HP Client Security

Aloitusopas

Ensimmäinen painos: elokuu 2013

Oppaan osanumero: 735339-351

Sisällysluettelo

1 Esittelyssä HP Client Security Manager

HP Client Security mahdollistaa tietojen, laitteiden ja henkilöllisyyden suojaamisen. Tämä pidentää tietokoneen suojausta.

Tietokoneellesi saatavilla olevat ohjelmiston moduulit voivat vaihdella mallista riippuen.

HP Client Security -ohjelmistomoduulit voivat olla valmiiksi asennettuja, esiasennettuja tai ladattavissa HP:n verkkosivustosta. Lisätietoja on kohdassa http://www.hp.com.

HUOMAUTUS: Tämän oppaan ohjeissa oletetaan, että olet jo asentanut asiaankuuluvat HP Client Security -ohjelmistomoduulit.

HP Client Securityn ominaisuudet

Seuraavassa taulukossa on HP Client Securityn moduulien tärkeimmät ominaisuudet.

Moduuli	Pääominaisuudet
HP Client Security Manager	Järjestelmänvalvojat voivat suorittaa seuraavat toiminnot: • Suojaa tietokoneesi ennen kuin Windows® käynnistyy • Suojaa Windows-tilisi vahvalla todennuksella • Hallitse Web-sivustojen ja sovellusten ja salasanoja • Vaihda helposti Windows- käyttöjärjestelmäsi salasana • Käytä sormenjälkiä tietoturvan ja käyttömukavuuden parantamiseksi • Määrittää älykortti, kontaktiton kortti tai lähikortti todennusta varten • Käyttää Bluetooth-puhelin tunnistamistapana • Määritä PIN-koodi laajentaaksesi todennusvaihtoehtoja • Määritä kirjautumis- ja istuntokäytännöt • Varmuuskopioi ja palauta ohjelmatiedot • Lisää sovelluksia, kuten HP Drive Encryption HP File Sanitizer, HP Trust Circles), HP Device Access Manager ja HP Computrace Yleiset käyttäjät voivat suorittaa seuraavat toiminnot: • Katso salaukseen tilan ja Device Access Managerin asetukset. • Aktivoi Computrace. • Määritä asetukset sekä varmuuskopiointi- ja palautusasetukset.

Moduuli	Pääominaisuudet
Password Manager	Yleiset käyttäjät voivat suorittaa seuraavat toiminnot: • Järjestää ja määrittää käyttäjänimet ja salasanat. • Luoda voimakkaampia salasanoja parempaa sähköpostien ja verkkotilien turvallisuutta varten. Password Manager täyttää ja lähettää tiedot automaattisesti. • Tehosta sisäänkirjautumistietoja prosessi ja kertakirjauspalvelulla, joka automaattisesti muistaa ja käyttää käyttäjätunnuksia. • Merkitse tilin tietosuoja vaarantuneeksi, jotta saat hälytyksiä muista käyttäjätileistä, joissa on samanlaiset tunnistetiedot. • Tuo sisäänkirjautumistiedot tuetusta selaimesta.
HP Drive Encryption (vain tietyt mallit)	• Tarjoaa täydellisen, koko kiintolevysalauksen. • Pakottaa käynnistystä edeltävän todennuksen tietojen salauksen purkamiseksi ja tietojen käyttämiseksi. • Antaa mahdollisuuden ottaa käyttöön itse salaavat asemat (vain tietyissä malleissa).
HP Device Access Manager	• Tämän avulla IT-päälliköt voivat valvoa laitteiden käyttöä käyttäjäprofiileihin perustuen. • Estää luvattomia käyttäjiä poistamasta tietoja käyttämällä ulkoisia tallennusvälineitä ja tuomasta viruksia järjestelmään ulkoisista tietovälineistä. • Tämän avulla järjestelmänvalvojat voivat poistaa käytöstä tietoliikennelaitteita tietyiltä käyttäjiltä tai käyttäjäryhmiltä.
HP Trust Circles	• Tarjoaa tiedostojen ja asiakirjojen tietoturvaa. • Salaa käyttäjän määrittämässä kansiossa olevat tiedostot ja suojaa ne trust circlen sisällä. • Mahdollistaa tiedostojen käytön ja jakamisen vain trust circlen jäsenten toimesta.
Varkauden selvittäminen (Computrace, myydään erikseen)	• Vaatii erikseen hankittavan seuranta- ja jäljitystilausten aktivoinnin. • Sisältää suojatun sisällönseurannan. • Valvoo käyttäjän toimintaa sekä laitteisto- ja ohjelmistomuutoksia. • Pysyy aktiivisena silloinkin, kun kiintolevy alustetaan tai vaihdetaan.

HP Client Securityn laitekuvaus ja yleisen käytön esimerkkejä

Useimmissa HP Client Security -tuotteissa on sekä käyttäjän todennus (tavallisesti salasana) ja järjestelmänvalvojan varmuuskopiointi, joita voidaan käyttää jos salasanat kadotetaan, jos ne eivät ole käytettävissä, jos ne unohtuvat tai kun yritysten tietoturvaa edellyttää niin.

HUOMAUTUS: Jotkin HP Client Security -tuotteet on suunniteltu rajoittamaan tietojen käyttöä. Tiedot pitäisi salata, kun on tärkeää että käyttäjä mieluummin menettää tietoja kuin että tietosuoja vaarantuu. On suositeltavaa, että kaikki tiedot varmuuskopioidaan turvalliseen paikkaan.

Password Manager

Password Manager tallentaa käyttäjänimiä ja salasanoja, ja sillä voidaan:

- Tallenna käyttäjänimet ja salasanat internet-yhteyttä tai sähköpostia varten.
- Kirjaa käyttäjän automaattisesti Web- sivustoon tai sähköpostiin.
- Hallitse ja järjestä todennuksia.
- Valitse web- tai verkkoresurssi ja käyttää linkkiä suoraan.
- Näytä nimet ja salasanat tarvittaessa.
- Merkitse tilin tietosuoja vaarantuneeksi, jotta saat hälytyksiä muista käyttäjätileistä, joissa on samanlaiset tunnistetiedot.
- Tuo sisäänkirjautumistiedot tuetusta selaimesta.

Esimerkki 1: Suuren valmistajan sisäänostaja tekee useimmat yritysostot internetin kautta. Ostaja myös vierailee useissa suosituissa verkkosivustoissa, jotka edellyttävät kirjautumistietoja. Hän on vahvasti tietoinen suojauksesta, joten hän ei käytä samaa salasanaa kaikille tileille. Sisäänostaja on päättänyt käyttää Password Manageria vastaamaan verkkolinkit eri käyttäjänimien ja salasanojen kanssa. Kun hän siirtyy verkkosivustolle kirjautuakseen sisään, Password Manager näyttää tunnistetiedot automaattisesti. Jos hän haluaa tarkastella käyttäjänimiä ja salasanoja, Password Manager voidaan määrittää näyttämään ne.

Password Manager voi myös hallita ja järjestää todennuksia. Tämän työkalun avulla voit valita web- tai verkkoresurssin ja käyttää linkkiä suoraan. Käyttäjä voi myös näyttää käyttäjänimet ja salasanat tarvittaessa.

Esimerkki 2: Ahkera työntekijä on ylennetty ja hän hallinnoi nyt koko laskutusosastoa. Tiimin pitää kirjautua useisiin asiakkaiden verkkotileihin, joista kukin käyttää eri kirjautumistietoja. Nämä kirjautumistiedot pitää jakaa muiden työntekijöiden kanssa, joten luottamuksellisuus on ongelma. Työntekijä päättää järjestää kaikki Web-linkit, yrityksen käyttäjätunnukset ja salasanat Password Managerissa. Kun tämä on suoritettu, työnantaja ottaa käyttöön Password Managerin työntekijöille niin, että he voivat työskennellä verkkotilien parissa tietämättä koskaan käyttämiään kirjautumistietoja.

HP Drive Encryption (vain tietyt mallit)

HP Drive Encryptionia käytetään rajoittamaan tietojen käyttöä koko tietokoneen kiintolevyllä tai toissijaisella asemalla. Drive Encryption voi hallita myös itse salaavia asemia.

Esimerkki 1: Lääkäri haluaa varmista, että hän voi käyttää kaikkia tietoja tietokoneensa kiintolevyllä. Lääkäri aktivoi Drive Encryptionin, joka vaatii käynnistystä edeltävää todennusta ennen Windows-kirjautumista. Asennuksen jälkeen, kiintolevyä ei voi käyttää ilman salasanaa ennen kuin käyttöjärjestelmä käynnistyy. Lääkäri voi parantaa aseman suojausta entisestään valitsemalla tietojen suojausta itse salaava asema -vaihtoehdolla.

Esimerkki 2: Sairaalavirkamies haluaa varmistaa, että vain lääkärit ja valtuutettu henkilöstö voi käyttää mitä tahansa tietoja paikallisella tietokoneella jakamatta henkilökohtaisia salasanojaan. IT-osasto lisää järjestelmänvalvojan lääkärit ja kaikki valtuutetut henkilöt Drive Encryption käyttäjiksi. Nyt vain valtuutettu henkilöstö voi käynnistää tietokoneen tai toimialueen uudelleen käyttämällä käyttäjätunnustaan ja salasanaansa.

HP Device Access Manager (vain tietyt mallit)

HP Device Access Managerin avulla järjestelmänvalvoja voi rajoittaa ja hallita laitteiston käyttöä. Device Access Managerin avulla voidaan estää luvaton pääsy USB-muistitikuille, josta tiedot voidaan

kopioida. Se voi myös rajoittaa pääsyä CD- ja DVD-asemiin, USB-laitteiden ohjausta, verkkoyhteyksiä jne. Esimerkiksi tilanne, jossa ulkopuolisten myyjien pitää käyttää yrityksen tietokoneita, mutta he eivät voi kopioida tietoja USB-asemaan.

Esimerkki 1: Sairaanhoitovälineyrityksen johtaja työskentelee usein henkilökohtaisten potilastietojen ja yritystietojen parissa. Työntekijöiden pitää käyttää näitä tietoja, mutta on kuitenkin erittäin tärkeää, että tietoja ei poisteta tietokoneelta USB-asemalla tai muulla ulkoisella tallennusvälineellä. Verkko on suojattu, mutta tietokoneissa on tallentavia CD-asemia ja USB-portit, jotka saattavat mahdollistaa tietojen kopioinnin tai varastamisen. Johtaja käyttää Device Access Manageria ja poistaa USB-portit ja tallentavat CD-asemat käytöstä niin, että niitä ei voi käyttää. Vaikka USB-portit on estetty, hiiri ja näppäimistö toimivat yhä.

Esimerkki 2: Vakuutusyhtiö ei halua työntekijänsä asentavan tai lataavan omia ohjelmia tai tietoja kotoaan. Joidenkin työntekijöiden tarvitsee käyttää USB-portteja kaikilla tietokoneilla. IT-johtaja käyttää Device Access Manageria antaakseen käyttöoikeuden joillekin työntekijöille samalla estäen käytön toisilta työntekijöiltä.

Computrace (hankittava erikseen)

Computrace (hankittava erikseen) on palvelu, jossa voidaan seurata varastetun tietokoneen sijaintia aina, kun käyttäjä käyttää internetiä. Computrace voi myös auttaa hallitsemaan etäkäytöllä ja etsimään tietokoneita, sekä valvomaan tietokoneen käyttöä ja sovelluksia.

Esimerkki 1: Koulun rehtori kehotti IT-osastoa seuraamaan kaikkia koulun tietokoneita. Kun tietokoneiden inventaari oli tehty, IT-järjestelmänvalvoja rekisteröi kaikki tietokoneet Computracella siten, että ne voidaan jäljittää, jos ne varastetaan. Äskettäin koulussa havaittiin, että useita tietokoneita puuttui, joten IT-järjestelmänvalvoja ilmoitti asiasta viranomaisille ja Computracen-henkilökunnalle. Tietokoneet löydettiin ja viranomaiset palauttivat ne koululle.

Esimerkki 2: Kiinteistöyhtiön pitää hallita ja päivittää tietokoneita ympäri maailmaa. He seuraavat ja päivittävät tietokoneita Computracen avulla lähettämättä IT-tukihenkilöä jokaiselle tietokoneelle.

Tärkeimpien suojatavoitteiden saavuttaminen.

HP Client Security -moduulit voivat työskennellä yhdessä tarjoamaan ratkaisuja eri suojaustoiminnoille, mukaan lukien seuraaville keskeisille suojaustavoitteille:

- Suojaaminen varkauksilta
- Luottamuksellisiin tietoihin pääsemisen rajoittaminen
- Luvattoman käytön estäminen sisäisistä tai ulkoisista sijainneista
- Tiukkojen salasanakäytäntöjen luominen

Suojaaminen varkauksilta

Varkaus voi olla esimerkiksi luottamuksellisia tietoja sisältävän tietokoneen varastaminen lentokentän turvatarkastuspisteestä. Seuraavat ominaisuudet auttavat suojaamaan varkauksilta:

- Jos käynnistystä edeltävä todennus on käytössä, se auttaa estämään pääsyä käyttöjärjestelmään.
  - HP Client Security—KatsoHP Client Security sivulla 12.
  - HP Drive Encryption—KatsoHP Drive Encryption (vain tietyt mallit) sivulla 28.
- Salaus auttaa varmistamaan, että tietoja ei voi käyttää silloinkin, kun kiintolevy on poistettu ja asennettu suojaamattomaan järjestelmään.
- Computrace avulla voidaan jäljittää tietokoneen sijaintia varkauden jälkeen.
  - Computrace - katso Varkauden selvittäminen (vain tietyissä malleissa) sivulla 52.

Luottamuksellisiin tietoihin pääsemisen rajoittaminen

Oletetaan, että ulkopuolinen tilintarkastaja työskentelee paikan päällä ja hänelle on annettu oikeus tarkastella arkaluontoisia taloustietoja tietokoneella. Et halua tilintarkastajan voivan tulostaa tiedostoja tai tallentaa niitä kirjoittavalle laitteelle kuten CD:lle. Seuraavat ominaisuudet auttavat rajoittamaan tietojen käyttöä:

- HP Device Access Managerin avulla IT- päälliköt voivat rajoittaa tietoliikennelaitteiden käyttöä niin että arkaluontoisia tietoja ei voi kopioida kiintolevyltä. Katso Järjestelmän näkymä sivulla 42.

Luvattoman käytön estäminen sisäisistä tai ulkoisista sijainneista

Suojaamattoman toimistotietokoneen luvaton käyttö on hyvin todellinen riski verkkoresursseille, kuten rahoituspalveluille, toimitusjohtajalle tai tutkimus- ja tuotekehitystiimille sekä yksityistiedoille, kuten potilaskertomuksille tai henkilökohtaiselle kirjanpidolle. Seuraavat ominaisuudet auttavat suojaamaan luvattomalta käytöltä:

- Jos käynnistystä edeltävä todennus on käytössä, se auttaa estämään pääsyä käyttöjärjestelmään. (katso HP Drive Encryption (vain tietyt mallit) sivulla 28.
- HP Client Security auttaa varmistamaan, että luvaton käyttäjä ei voi hakea salasanoja tai käyttää salasanasuojattuja sovelluksia. Katso HP Client Security sivulla 12.
- HP Device Access Managerin avulla IT- päälliköt voivat rajoittaa kirjoittavien laitteiden käyttöä niin, että arkaluontoisia tietoja ei voi kopioida kiintolevyltä. Katso HP Device Access Manager (vain tietyt mallit) sivulla 41.

Tiukkojen salasanakäytäntöjen luominen

Jos otetaan käyttöön yrityskäytäntö, joka vaatii vahvaa salasanakäytäntöä useille verkkopohjaisille sovelluksille ja tietokannoille, Password Manager toimii suojattuna salasanavarastona ja kertakirjauspalveluna. Katso Password Manager sivulla 17.

Ylimääräiset turvaratkaisut

Käyttöoikeusroolien määrittäminen

Tietokoneen suojauksen hallinnassa (erityisesti suurissa organisaatioissa), yksi tärkeä käytäntö on jakaa vastuualueita ja oikeuksia erityyppisille järjestelmänvalvojille ja käyttäjille.

HUOMAUTUS: Nämä roolit voivat olla yhdellä henkilöllä pienessä organisaatiossa tai omassa käytössä.

HP Client Securityn tietosuojavelvollisudet ja -oikeudet voidaan jakaa seuraaviin rooleihin:

- Turvallisuuspäällikkö- määrittää yrityksen tai verkon suojaustason ja määrittää käytettävät suojausasetukset, kuten Drive Encryptionin.

  HUOMAUTUS: Turvallisuuspäällikkö voi mukauttaa monia HP Client Securityn ominaisuuksia yhteistyössä HP:n kanssa. Lisätietoja on kohdassa http://www.hp.com.

- IT-järjestelmänvalvojan - käyttää ja hallitsee turvallisuuspäällikön määrittämiä suojausasetuksia. Voi myös ottaa käyttöön tai poistaa käytöstä tiettyjä toimintoja. Jos esimerkiksi turvallisuuspäällikkö on päättänyt ottaa käyttöön älykortit IT-järjestelmänvalvoja voi ottaa käyttöön sekä salasana- että älykorttitilan.

- Käyttäjä—käyttää suojausominaisuuksia. Jos esimerkiksi turvallisuuspäällikkö ja IT-järjestelmänvalvoja on ottanut käyttöön järjestelmän, käyttäjä voi asettaa älykortin PIN-koodin ja käyttää korttia todennusta varten.

VAROITUS: Järjestelmänvalvojia kannustetaan noudattamaan parhaita käytäntöjä loppukäyttäjän oikeuksien ja käyttäjän käytön rajoittamiseksi.

Luvattomille käyttäjille ei saa myöntää järjestelmänvalvojan oikeuksia.

HP Client Securityn salasanojen hallinta

Useimmat HP Client Security -ominaisuudet ovat salasanasuojattuja. Seuraavassa taulukossa on lueteltu yleisesti käytetyt salasanat, ohjelmistomoduuli, jossa salasana määritetään ja salasanatoiminto.

Vain IT-järjestelmänvalvojien määrittämät ja käyttämät salasanat on merkitty tässä taulukossa. Tavalliset käyttäjät tai järjestelmänvalvojat voivat asettaa kaikki muut salasanat.

HP Client Securityn salasana	Määritä seuraavassa moduulissa	Toiminto
Windowsin kirjautumissalasana	Windowsin ohjauspaneeli tai HP Client Security	Voidaan käyttää manuaaliseen kirjautumiseen ja HP Client Securityn eri toimintojen käyttöoikeuksien todentamiseen.
HP Client Securityn varmuuskopiointi- ja palautussalasana	HP Client Security, yksilöllisten käyttäjien mukaan	Suojaa HP Client Securityn varmuuskopiointi- ja palautustiedoston käyttöä.
Älykortin PIN	Credential Manager (Valtuustietojen hallinta)	Voidaan käyttää monivaiheisena todennuksena. Voidaan käyttää Windows-todennuksena. Todentaa Drive Encryptionin käyttäjät jos älykortti on valittu.

Suojatun salasanan luominen

Salasanoja luodessa pitää noudattaa ensin kaikkia ohjelman asettamia määrityksiä. Ota kuitenkin huomioon seuraavat ohjeet, joiden avulla voit luoda vahvoja salasanoja ja vähentää salasanojen vaarantumista.

- Käytä salasanoja, joissa on yli 6 merkkiä, mieluiten yli 8.
- Käytä salasanassa eri kirjainkokoja.
- Käytä aakkosnumeeristen merkkien yhdistelmää aina, kun se on mahdollista ja käytä erikoismerkkejä ja välimerkkejä.
- Käytä avainsanojen kirjaimien sijasta erikoismerkkejä tai numeroita. Voit esimerkiksi käyttää numeroa 1 kirjainta I tai L varten.
- Yhdistä kahden tai useamman kielen sanoja.
- Jaa sana tai lause numeroilla tai erikoismerkeillä kahtia, esimerkiksi "Mary2-2Cat45".
- Älä käytä salasanaa, joka esiintyy sanakirjassa.
- Älä käytä salasanana nimeäsi tai muita henkilökohtaisia tietoja, kuten syntymäpäivääsi, lemmikkieläinten nimiä tai äidin tyttönimeä vaikka se olisi kirjoitettu takaperin.
- Vaihda salasanoja säännöllisesti. Voit esimerkiksi muuttaa vain muutaman merkin arvoa.
- Jos kirjoitat salasanasi ylös, älä säilytä sitä näkyvässä paikassa tietokoneen lähellä.
- Älä tallenna salasanaa tiedostoon, kuten sähköpostiin tai tietokoneelle.
- Älä jaa tilejä tai paljasta salasanaasi kenellekään.

Tunnistetietojen ja asetusten varmuuskopiointi

Voit käyttää HP Client Securityn Backup and Recovery -työkalua keskeisenä paikkana, josta voit varmuuskopioida ja palauttaa valtuustiedot joistakin asennetuista HP Client Security -moduuleista.

2 Aloitusopas

Määrittääksesi HP Client Securityn käytettäväksi valtuustiedoillasi käynnistä HP Client Security yhdellä seuraavista tavoista. Kun ohjattu toiminto on suoritettu loppuun, käyttäjä ei voida käynnistää sitä uudelleen.

1. Napsauta tai napauta Käynnistä- tai Sovellukset-ruudulta **HP Client Security** -sovellusta (Windows 8).

   TAI

   Napsauta tai napauta Windowsin työpöydältä **HP Client Security Gadget** (Windows 7).

   TAI

   Kaksoisnapsauta tai kaksoisnapauta Windowsin työpöydällä, tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella sijaitsevaa **HP Client Security** -kuvaketta.

   TAI

   Kaksoisnapsauta tai kaksoisnapauta Windowsin työpöydällä **HP Client Security** -kuvaketta ilmoitusalueella, ja sen jälkeen valitse **Avaa HP Client Security**.

2. HP Client Securityn ohjattu asennus käynnistetään Aloitussivu näytettynä.

3. Lue Aloitusnäyttö, vahvista henkilöllisyytesi kirjoittamalla Windows-salasanasi, ja sen jälkeen napsauta tai napauta **Seuraava**.

   Jos et ole vielä luonut Windows-salasanaa, sinua kehotetaan luomaan se. Windows-salasana vaaditaan suojataksesi Windows-tilisi valtuuttomien henkilöiden pääsyltä käyttääkseen HP Client Security -ominaisuuksia.

4. Valitse HP SpareKey -sivulla kolme turvallisuuskysymystä. Anna vastaus kuhunkin kysymykseen ja sen jälkeen napsauta **Seuraava**. Mukautetut kysymykset ovat myös sallittuja. Lisätietoja on kohdassa HP SpareKey—Salasanan palautus sivulla 13.

5. Rekisteröi Sormenjäljet-sivulla vähintään minimimäärä tarvittavia sormenjälkiä, ja sen jälkeen napsauta tai napauta **Seuraava**. Lisätietoja on kohdassa Sormenjäljet sivulla 12.

6. Aktivoi salaus aseman salaussivulla, varmuuskopioi salausavain, ja sen jälkeen napsauta tai napauta **Seuraava**. Katso lisätietoja HP Client Security -ohjelmiston ohjeesta.

   HUOMAUTUS: Tämä pätee skenaarioon, miss käyttäjä on järjestelmänvalvoja, ja HP Client Securityn ohjattua käynnistystä järjestelmänvalvoja ei ole määrittänyt aikaisemmin.

7. Napsauta tai napauta ohjatun toiminnan viimeisellä sivulla **Lopeta**.

   Tämä sivu tarjoaa ominaisuuksien ja valtuustietojen tilan.

8. HP Client Securityn ohjattu käynnistys varmistaa Just In Time Authenticationin aktivoinnin ja File Sanitizer -ominaisuudet. Katso lisätietoja HP Client Security -ohjelmiston ohjeesta ja HP File Sanitizer -ohjelmiston ohjeesta.

   HUOMAUTUS: Tämä pätee skenaarioon, miss käyttäjä on järjestelmänvalvoja, ja HP Client Securityn ohjattua käynnistystä järjestelmänvalvoja ei ole määrittänyt aikaisemmin.

HP Client Securityn avaaminen

Voit avata HP Client Security -sovelluksen yhdellä seuraavista tavoista:

HUOMAUTUS: HP Client Securityn ohjattu käynnistys täytyy olla valmis ennen kuin HP Client Security -sovellus voidaan käynnistää.

- Napsauta tai napauta Käynnistä- tai Sovellukset-ruudulta **HP Client Security** -sovellus.

  TAI

  Napsauta tai napauta Windowsin työpöydältä **HP Client Security** Gadget (Windows 7).

  TAI

  Kaksoisnapsauta tai kaksoisnapauta Windowsin työpöydällä, tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella sijaitsevaa **HP Client Security** -kuvaketta.

  TAI

  Kaksoisnapsauta tai kaksoisnapauta Windowsin työpöydällä **HP Client Security** -kuvaketta ilmoitusalueella, ja sen jälkeen valitse **Avaa HP Client Security**.

3 Helppo asennusopas pienille yrityksille

Tässä luvussa esitellään perusvaiheet HP Client Security for Small Businessin yleisimpien ja hyödyllisimpien vaihtoehtoja aktivoimiseksi. Tämän ohjelman useiden työkalujen ja vaihtoehtojen avulla voit hienosäätää asetuksiasi ja määrittää käytön hallinnan. Tämän helpon asennusoppaan avulla saat kunkin moduulin käyttöön mahdollisimman helposti ja nopeasti. Jos haluat lisätietoja, valitse moduuli josta olet kiinnostunut ja napsauta sitten oikeassa yläkulmassa olevaa **?**- tai Ohje-painiketta. Tämä painike näyttää automaattisesti tiedot, jotka antavat ohjeita liittyen parhaillaan näytettyyn ikkunaan.

Aloitusopas

1. Avaa Windowsin työpöydällä HP Client Security kaksoisnapsauttamalla, tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella sijaitsevaa **HP Client Security** -kuvaketta.
2. Kirjoita Windows-salasanasi tai luo Windows-salasana.
3. HP Client Securityn asetuksen suorittaminen

HP Client Security edellyttää todennusta vain kerran aikana Windows-kirjautumisen aikana, katso Suojausominaisuudet sivulla 25.

Password Manager

Kaikilla on paljon salasanoja - erityisesti, jos käytät säännöllisesti verkkosivuja tai sovelluksia, jotka vaativat kirjautumisen. Tavallinen käyttäjä käyttää joko samaa salasanaa kullekin sovellukselle ja verkkosivulle tai unohtaa pian mikä salasana on määritetty millekin sovellukselle.

Password Manager voi automaattisesti muista salasanasi tai antaa sinulle mahdollisuuden hahmottaa mitkä sivustot kannattaa muistaa ja mitkä jättää huomioimatta. Kun olet kirjautunut sisään tietokoneeseen, Password Manager antaa salasanat tai tunnistetiedot osallistuaksesi sovelluksiin tai verkkosivustoihin.

Kun käytät sovellusta tai verkkosivua, joka vaatii tunnistetietoja, Password Manager tunnistaa automaattisesti sivuston ja kysyy haluatko ohjelman muistavan tietosi. Voit evätä pyynnön, jos haluat jättää tiettyjä sivuja huomioimatta.

Voit alkaa verkkosijainteja, käyttäjänimiä ja salasanoja:

1. Esimerkiksi siirry osallistuvaan tukisivustoon tai sovellukseen ja lisää verkkotodennus napsauttamalla Password Manager -kuvaketta verkkosivun vasemmassa yläkulmassa.
2. Nimeä linkki (valinnainen) ja kirjoita käyttäjänimi ja salasana Password Manageriin.
3. Kun olet valmis, napsauta **OK** painiketta.
4. Password Manager voi myös tallentaa käyttäjänimesi ja salasanasi verkkojakamista tai käyttöön otettuja verkkoasemia varten.

Tallennettujen todennusten katselu ja hallinta Password Managerissa

Password Managerin avulla voit tarkastella, hallita ja käynnistää todennuksia yhdestä paikasta. Password Manager tukee myös tallennettujen sivustojen käynnistämistä Windowsista.

Avaa Password Manager näppäimistöyhdistelmällä Ctrl+Windows- näppäin+h ja valitse sitten **Kirjaudu** käynnistääksesi ja todentaaksesi tallennetun pikakuvakkeen.

Password Managerin **Muokkaa**-vaihtoehdon avulla voit tarkastella ja muuttaa nimeä, kirjautumisnimeä ja jopa paljastaa salasanoja.

HP Client Security for Small Businessin avulla on mahdollista varmuuskopioida ja/tai kopioida kaikki tunnistetiedot ja asetukset toiseen tietokoneeseen.

HP Device Access Manager

Device Access Managerilla voidaan rajoittaa sisäisten ja ulkoisten tallennuslaitteiden käyttöä, jotta tietosi pysyvät suojattuna kiintolevyllä eivätkä joudu vääriin käsiin. Esimerkiksi kun käyttäjälle annetaan käyttöoikeus tietoihisi, mutta estät heitä kopioimasta tietoja CD-levylle, musiikkisoittimille tai USB-muistiin.

1. Avaa **Device Access Manager** (katso Device Access Manager -sovelluksen avaaminen sivulla 41).

   Nykyisen käyttäjän käyttöoikeudet tulee näyttöön.

2. Voit muuttaa käyttäjien, ryhmien tai laitteiden käyttöoikeutta valitsemalla tai napsauttamalla **Muuta**. Lisätietoja on kohdassa Järjestelmän näkymä sivulla 42.

HP Drive Encryption

HP Drive Encryptionia käytetään suojaamaan tietoja salaamalla koko kovalevyn. Kiintolevyllä olevat tiedot säilyvät suojattuina, jos tietokoneesi varastetaan ja/tai jos kiintolevy poistetaan alkuperäisestä tietokoneesta ja asetetaan toiseen tietokoneeseen.

Ylimääräinen Drive Encryptionin suojausominaisuus edellyttää oikeaa todennusta käyttämällä käyttäjätunnustasi ja salasanaasi ennen kuin käyttöjärjestelmä käynnistyy. Tätä kutsutaan käynnistystä edeltäväksi todennukseksi.

Tämän helpottamiseksi useat ohjelmistomoduulit synkronoivat salasanat automaattisesti, mukaan lukien Windows-käyttäjätilit, todennustoimialueet, HP Drive Encryptionin, Password Managerin ja HP Client Securityn.

Tietoja HP Drive Encryptionin asennuksesta alkuasennuksen aikana HP Client Securityllä on kohdassa Aloitusopas sivulla 8.

4 HP Client Security

HP Client Securityn etusivu on keskeinen sijainti helppoon pääsyyn HP Client Securityn ominaisuuksiin, sovelluksiin, ja asetuksiin. Kotisivu on jaettu kolmeen osaan:

- **TIETO**—Tarjoaa pääsyn sovelluksiin, joita käytetään tietoturvallisuuden hallintaan.
- **LAITE**—Tarjoaa pääsyn sovelluksiin, joita käytetään laiteturvallisuuden hallintaan
- **HENKILÖLLISYYS**—Tarjoaa todennuksen valtuustietojen rekisteröinnin ja hallinnan.

Siirrä kohdistin sovelluksen laatan päälle näyttämään sovelluksen kuvauksen.

HP Client Security voi tarjota linkkejä käyttäjän ja järjestelmänvalvojan asetuksiin sivun alaosassa. HP Client Security tarjoaa pääsyn Lisäasetuksiin ja ominaisuuksiin napauttamalla tai napsauttamalla **Gear** (asetukset) -kuvaketta.

Henkilöllisyysominaisuudet, sovellukset, ja asetukset

HP Client Securityn tarjoamat Henkilöllisyysominaisuudet, sovellukset, ja asetukset auttavat sinua digitaalisen henkilöllisyytesi erilaisten näkökohtien hallinnassa. Napsauta tai napauta yhtä seuraavista laatoista HP Client Securityn etusivulla, ja sen jälkeen anna Windows-salasanasi:

- **Sormenjäljet**—Rekisteröi ja hallitsee sormenjälkesi valtuustietoa.
- **SpareKey**—Asentaa ja hallitsee sinun HP SpareKey -valtuustietoa, mitä voidaan käyttää sisäänkirjautumiseen tietokoneeseesi, jos muut valtuustiedot ovat hävinneet tai tallennettu väärään paikkaan. Se myös sallii sinun palauttaa unohtuneen salasanasi.
- **Windows-salasana**—Tarjoaa helpon pääsyn muuttamaan Windows-salasanasi.
- **Bluetooth-laitteet**—Sallii sinun rekisteröidä ja hallita Bluetooth-laitteitasi.
- **Kortit**—Sallii sinun rekisteröidä ja hallita älykorttejasi, kontaktittomia korttejasi, ja lähestymiskorttejasi.
- **PIN**—Sallii sinun rekisteröidä ja hallita PIN-valtuustietojasi.
- **RSA SecurID**—Tämän avulla voit rekisteröidä ja hallita RSA SecurID -tunnistetietoja (jos asiaankuuluvat asetukset ovat paikallaan).
- **Salasananhallinta**—Sallii sinun hallita verkkotilejäsi ja sovelluksiasi.

Sormenjäljet

HP Client Securityn ohjattu käynnistys opastaa sinut asentamisen tai, "rekisteröimisen", sormenjälkesi prosessin läpi.

Voit myös rekisteröidä tai poistaa sormenjälkesi Sormenjäljet-sivulla, johon voit päästä napsauttamalla tai napauttamalla **Sormenjäljet**-kuvaketta HP Client Securityn etusivulla.

1. Sipaise Sormenjäljet-sivulla sormeasi kunnes se on onnistuneesti rekisteröity.

   Rekisteröitäväksi tarvittavien sormien lukumäärä osoitetaan sivulla. Etu- tai keskisormet ovat parempia.

2. Poistaaksesi aikaisemmin rekisteröityjä sormenjälkiä napsauta tai napauta **Poista**.

3. Rekisteröidäksesi lisää sormia napsauta tai napauta **Rekisteröi lisäsormenjälki**.

4. Napsauta tai napauta **Tallenna** ennen sivulta poistumista.

⚠ **VAROITUS:** Kun rekisteröit sormenjälkiä ohjatun toiminnon avulla, sormenjälkitietoja ei tallenneta, ennen kuin valitset **Next** (Seuraava). Jos tietokonetta ei käytetä vähään aikaan tai ohjelma suljetaan, muutoksia **ei** tallenneta.

- Päästäksesi Sormenjälkien järjestelmänvalvojan asetuksiin, missä järjestelmänvalvojat voivat määrittää rekisteröinnin, tarkkuuden, ja muita asetuksia, napsauta tai napauta **Järjestelmänvalvojan asetukset** (tarvitsee järjestelmänvalvojan oikeudet).
- Päästäksesi Sormenjälkien käyttäjän asetuksiin, missä voit määritellä asetukset, jotka ohjaavat sormenjälkien tunnistamisen esiintymistä ja käyttäytymistä, napsauta tai napauta **Käyttäjän asetukset**.

Sormenjälkien järjestelmänvalvojan asetukset

Järjestelmänvalvojat voivat määritellä rekisteröinnin, tarkkuuden, ja muita asetuksia sormenjälkilukijalle. Järjestelmänvalvojan oikeudet tarvitaan.

- Päästäksesi järjestelmänvalvojan asetuksiin sormenjälki-valtuustietoja varten napsauta tai napauta **Järjestelmänvalvojan asetukset** Sormenjäljet-sivulla.

- **Käyttäjän rekisteröinti**—Valitse sormenjälkien minimi- ja maksimimäärä, jolla käyttäjän on sallittua rekisteröityä.
- **Tunnistaminen**—Siirrä liukusäädintä asettaaksesi sormenjälkilukijan käyttämän herkkyyden sipaistessasi sormeasi.

  Jos sormenjälkeäsi ei tunnisteta yhtäpitävästi, voit joutua valitsemaan alemman tunnistamisasetuksen. Korkeampi asetus lisää herkkyyttä vaihteluihin sormenjälkisipaisussa ja siksi alentaa väärän hyväksynnän mahdollisuutta. **Keskitaso-korkea**-asetus tarjoaa hyvän sekoituksen turvallisuudesta ja mukavuudesta.

Sormenjälkien käyttäjän asetukset

Sormenjälkien käyttäjän asetukset -sivulla voit määritellä asetukset, jotka ohjaavat sormenjälkien tunnistamisen esiintymistä ja käyttäytymistä.

- Päästäksesi käyttäjän asetuksiin sormenjäljen valtuustietoja varten, napsauta tai napauta **Käyttäjän asetukset** Sormenjäljet-sivulla.

- **Ota käyttöön äänipalaute**—Oletuksena HP Client Security antaa sinulle äänipalautteen, kun sormenjälkesi on sipaistu toistaen erilaisia ääniä tietyille ohjelmatapahtumille. Voit kiinnittää uusia ääniä näille tapahtumille Äänet-välilehden kautta Ääni-asetuksessa Windowsin ohjauspaneelissa, tai poistaaksesi äänipalautteen käytöstä tyhjennä tämä valintaruutu.
- **Näytä tarkastuksen laadun palaute**—Näyttääksesi kaikki sipaisut, laadusta riippumatta, valitse valintaruutu. Näyttääksesi vain hyvän laadun sipaisut tyhjennä valintaruutu.

HP SpareKey—Salasanan palautus

HP SpareKey sallii sinun saada pääsyn tietokoneeseesi (tuetuilla alustoilla) vastaamalla kolmeen turvallisuuskysymykseen.

HP Client Security kehottaa sinua asentamaan henkilökohtaisen HP SpareKeysi aloitusasennuksen aikana HP Client Securityn ohjatussa asennuksessa.

HP SpareKeyn asentaminen:

1. Ohjatun toiminnon HP SpareKey -sivulla valitse kolme turvallisuuskysymystä, ja sen jälkeen anna vastaus kuhunkin kysymykseen.

   Voit valita kysymys ennalta määritetystä luettelosta tai kirjoittamalla oman kysymyksen.

2. Napsauta tai napauta **Rekisteröi**.

HP SpareKeysi poistaminen:

▲ Napsauta tai napauta **Poista SpareKeysi**.

Sen jälkeen kun SpareKeysi on asennettu, voit päästä tietokoneeseesi käyttämällä SpareKeytäsi Power-on authentication -kirjautumisnäytöstä tai Windowsin Aloitusnäytöstä.

Voit valita eri kysymyksiä tai muuttaa vastauksiasi SpareKey-sivulla, johon päästään Salasanan palautus -laatasta HP Client Securityn etusivulla.

Päästäksesi HP SpareKey -asetuksiin, missä järjestelmänvalvoja voi määritellä asetuksia liittyen HP SpareKeyn valtuustietoihin, napsauta **Asetukset** (tarvitsee järjestelmänvalvojan oikeudet).

HP SpareKey -asetukset

HP SpareKeyn asetukset -sivulla voit määritellä asetukset, jotka ohjaavat HP SpareKeyn valtuustietojen käyttäytymistä ja käyttöä.

▲ Käynnistääksesi HP SpareKeyn asetukset -sivun napsauta tai napauta **Asetukset** HP SpareKeyn sivulla (tarvitsee järjestelmänvalvojan oikeudet).

Järjestelmänvalvojat voivat valita seuraavat asetukset:

- Määritä kysymyksiä, jotka näkyvät kullekin käyttäjälle HP SpareKey -asetuksen aikana.
- Lisää enintään kolme mukautusturvallisuuskysymystä lisätäksesi käyttäjille esitettyyn luetteloon.
- Valitse sallitaanko vai ei käyttäjien kirjoittaa heidän omat turvallisuuskysymyksensä.
- Määrittele mitkä todennusympäristöt (Windows tai Power-on authentication) sallii HP SpareKeyn salasanan palautuksen käytön.

Windows-password

HP Client Security tekee Windows-salasanasi muuttamisen yksinkertaisemmaksi ja nopeammaksi kuin sen muuttaminen Windowsin ohjauspaneelin kautta.

Windows-salasanasi muuttaminen:

1. Napsauta tai napauta HP Client Securityn etusivulta **Windows-salasana**.
2. Anna nykyinen salasanasi **Nykyinen Windows-salasana** -tekstiruudussa.
3. Kirjoita uusi salasana **Uusi Windows-salasana** -tekstiruudussa, ja sen jälkeen kirjoita se uudelleen **Vahvista uusi salasana** -tekstiruudussa.
4. Napsauta tai napauta **Muuta** muuttaaksesi välittömästi nykyisen salasanasi uuteen, jonka annoit.

Bluetooth-laitteet

Jos järjestelmänvalvoja on ottanut Bluetoothin käyttöön todennus-valtuustietoina, voit asentaa Bluetooth-puhelimen yhdessä muiden valtuustietojen kanssa lisäturvallisuutta varten.

HUOMAUTUS: Vain Bluetooth-puhelinlaitteita tuetaan.

1. Varmista, että Bluetooth-toiminto on käytössä tietokoneella ja että Bluetooth-puhelin on tunnistustilassa. Yhdistääksesi puhelimen sinua voidaan pyytää kirjoittamaan automaattisesti luodun koodin Bluetooth-laitteessa. Riippuen Bluetooth-laitteen määrityksen asetuksista parin muodostuksen koodien vertailu tietokoneen ja puhelimen välillä voidaan tarvita.
2. Puhelimen rekisteröimiseksi valitse se, ja sen jälkeen napsauta tai napauta **Rekisteröi**.

Päästäksesi Bluetooth-laitteiden asetukset sivulla 15 -sivulle, missä järjestelmänvalvoja voi määritellä asetuksia Bluetooth-laitteille napsauta **Asetukset** (tarvitsee järjestelmänvalvojan oikeudet).

Bluetooth-laitteiden asetukset

Järjestelmänvalvojat voivat määritellä seuraavat asetukset, jotka ohjaavat Bluetooth-laitteiden valtuustietojen käyttäytymistä ja käyttöä:

Hiljainen todennus

- **Yhdistetyn rekisteröidyn Bluetooth-laitteesi automaattinen käyttö henkilöllisyytesi vahvistuksen aikana**—Valitse valintaruutu sallimaan käyttäjiä käyttämään Bluetooth-valtuustietoja todennukseen tarvitsematta käyttäjän toimenpidettä, tai tyhjennä valintaruutu poistaaksesi tämän valinnan käytöstä.

Bluetooth-lähialue

- **Lukitse tietokone kun rekisteröity Bluetooth-laite siirtyy tietokoneen kantaman ulkopuolelle**-Valitse valintaruutu lukitaksesi tietokoneen, kun Bluetooth-laite, joka oli yhdistetty sisäänkirjautumisen aikana, siirtyy alueen ulkopuolelle, tai tyhjennä valintaruutu poistaaksesi tämän valinnan käytöstä.

HUOMAUTUS: Tietokoneessasi olevan Bluetooth-moduulin täytyy tukea tätä ominaisuutta ottaakseen hyödyn tästä ominaisuudesta.

Kortit

HP Client Security voi tukea joukkoa eri tyyppisiä henkilökortteja, jotka ovat pieniä muovikortteja sisältäen tietokonesirun. Näihin kuuluvat älykortit, kontaktittomat kortit, ja lähestymiskortit. Jos yksi näistä korteista, ja sopiva kortinlukija, on liitetty tietokoneeseen, jos järjestelmänvalvoja on asentanut liittyvän laiteohjaimen valmistajalta, ja jos järjestelmänvalvoja on ottanut käyttöön kortin todennus-valtuustietoina, voit käyttää korttia todennus-valtuustietoina.

Älykorteille valmistajan tulisi tarjota työkalut asentaa turvallisuussertifikaatti ja PIN-hallinta, jota HP Client Security käyttää turvallisuusalgoritmissaan. PINinä käytettyjen merkkien määrä ja tyyppi voi vaihdella. Järjestelmänvalvoja täytyy alustaa älykortti ennen kuin sitä voidaan käyttää.

HP Client Security tukee seuraavia älykorttiformaatteja:

- CSP
- PKCS11

HP Client Security tukee seuraavan tyyppisiä kontaktittomia kortteja:

- Kontaktittomat HID iCLASS -muistikortit
- Kontaktittomat MiFare Classic 1k, 4k, ja minimuistikortit

HP Client Security tukee seuraavia lähestymiskortteja:

- HID-lähestymiskortit

Älykortin rekisteröiminen:

1. Laita kortti sisään liitettyyn älykortinlukijaan.
2. Kun kortti on tunnistettu, anna kortin PIN, ja sen jälkeen napsauta tai napauta **Rekisteröi**.

Älykortin PINin muuttaminen:

1. Laita kortti sisään liitettyyn älykortinlukijaan.
2. Kun kortti on tunnistettu, anna kortin PIN, ja sen jälkeen napsauta tai napauta **Todenna**.
3. Napsauta tai napauta **Muuta PIN**, ja sen jälkeen anna uusi PIN.

Kontaktittoman lähestymiskortin rekisteröiminen:

1. Laita kortti hyvin lähelle sopivaa lukijaa.
2. Kun kortti on tunnistettu, napsauta tai napauta **Rekisteröi**.

Rekisteröidyn kortin poistaminen:

1. Esitä kortti lukijalle.
2. Vain älykorteille anna korttiin kiinnitetty PIN, ja sen jälkeen napsauta tai napauta **Todenna**.
3. Napsauta tai napauta **Poista**.

Kun kortti on rekisteröity, tiedot kortista näytetään kohdassa **Rekisteröidyt kortit**. Kun kortti on poistettu, se poistetaan luettelosta.

Päästäksesi Lähestymis-, Kontaktittoman, ja Älykortin asetuksiin, missä järjestelmänvalvojat voivat määritellä asetuksia liittyen kortin valtuustietoihin, napsauta tai napauta **Asetukset** (tarvitsee järjestelmänvalvojan oikeudet).

Lähestymis-, Kontaktittoman, ja Älykortin asetukset

Päästäksesi asetuksiin kortille napsauta tai napauta luettelossa olevaa korttia, ja sen jälkeen napsauta tai napauta näytettävää nuolta.

Älykortin PINin muuttaminen:

1. Esitä kortti lukijalle
2. Anna korttiin kiinnitetty PIN, ja sen jälkeen napsauta tai napauta **Jatka**.
3. Anna ja vahvista uusi PIN, ja sen jälkeen napsauta tai napauta **Jatka**.

Älykortin PINin alustaminen:

1. Esitä kortti lukijalle
2. Anna korttiin kiinnitetty PIN, ja sen jälkeen napsauta tai napauta **Jatka**.
3. Anna ja vahvista uusi PIN, ja sen jälkeen napsauta tai napauta **Jatka**.
4. Napsauta tai napauta**Kyllä** alustuksen vahvistamiseksi.

Kortin tiedon tyhjentäminen:

1. Esitä kortti lukijalle
2. Anna korttiin kiinnitetty PIN (vain Älykorteille, ja sen jälkeen napsauta tai napauta **Jatka**.
3. Napsauta tai napauta **Kyllä** poistamisen vahvistamiseksi.

PIN-koodi

Jos järjestelmänvalvoja on ottanut käyttöön PINin todennus-valtuustietoina, voit asentaa PINin yhdessä muiden valtuustietojen kanssa lisäturvallisuutta varten.

Uuden PINin asettaminen:

▲ Anna PIN, anna se uudelleen vahvistaaksesi sen, ja sen jälkeen napsauta tai napauta **Käytä**.

PINin poistaminen:

▲ Napsauta tai napauta **Poista**, ja sen jälkeen napsauta tai napauta **Kyllä** vahvistukseksi.

Päästäksesi PIN-asetuksiin, missä järjestelmänvalvojat voivat määritellä asetuksia liittyen PIN-valtuustietoihin, napsauta tai napauta **Asetukset** (tarvitsee järjestelmänvalvojan oikeudet).

PIN-asetukset

PIN-asetukset-sivulla, voit määritellä hyväksytyille minimi- ja maksimipituuksille PIN-valtuustietoihin.

RSA SecurID

Jos järjestelmänvalvoja on ottanut käyttöön RSAn todennus-valtuustietoina, ja seuraavat ehdot ovat tosia, voit rekisteröidä tai poistaa RSA SecurID -valtuustiedot.

HUOMAUTUS: Sopiva asennus tarvitaan.

- Käyttäjän täytyy olla luonut RSA-palvelimella.
- RSA SecurID token kiinnitetty käyttäjään ja tietokoneen täytyy olla ollut kiinnitettynä RSA-palvelimen toimialueelle.
- SecurID-ohjelmisto on asennettu tietokoneeseen.
- Yhdistäminen on käytettävissä oikein määritetylle RSA-palvelimelle.

RSA SecurID -valtuustietojen rekisteröiminen:

▲ Anna RSA SecurID -käyttäjänimi ja salakoodi (RSA SecurID Token -koodi tai PIN+Token -koodi riippuen ympäristöstäsi), ja sen jälkeen napsauta tai napauta **Käytä**.

Onnistuneessa rekisteröinnissä näytetään viesti “RSA SecurID -valtuustietosi on onnistuneesti rekisteröity,” ja Poista-painike on otettu käyttöön.

RSA SecurID valtuustietosi poistaminen:

▲ Napsauta **Poista**, ja sen jälkeen **Kyllä** ponnahdusvalintaikkunaan, joka kysyy "Haluatko varmasti poistaa RSA SecurID -valtuustietosi?"

Password Manager

Sisäänkirjautuminen www-sivustoille ja sovelluksiin on helpompaa ja luotettavampaa, kun käytät Salasanojen hallintaa. Voit luoda vahvempia salasanoja, joita sinun ei ole kirjoitettava muistiin tai muistaa, ja sen jälkeen kirjaudu sisään helposti ja nopeasti sormenjäljellä, älykortilla,

lähestymiskortilla, kontaktittomalla kortilla, Bluetooth-puhelimella, PINillä, RSA-valtuustiedoilla, tai Windows-salasanalla.

HUOMAUTUS: Webin kirjautumisnäyttöjen jatkuvasti muuttuvan rakenteen takia Salasanojen hallinta ei ehkä kykene tukemaan kaikkia www-sivustoja kaikkina aikoina.

Salasanojen hallinta tarjoaa seuraavia valintoja:

Salasanojen hallinta -sivu

- Napsauta tai napauta tiliä käynnistääksesi automaattisesti www-sivun tai sovelluksen ja kirjaudu sisään.
- Käytä luokkia tiliesi järjestämiseen.

Salasanan vahvuus

- Katso yhdellä silmäyksellä onko mikään salasanoistasi turvallisuusriski.
- Kun lisätään sisäänkirjautumisen tietoa, tarkista yksittäisten www-sivuihin ja sovelluksiin käytettyjen salasanojen vahvuus.
- Salasanan vahvuus kuvataan punaisilla, keltaisilla, tai vihreillä tilailmaisimilla.

Salasanojen hallinta -kuvake näytetään ylhäällä www-sivun vasemmassa kulmassa tai kirjautumisnäytössä. Kun kirjautumista ei vielä ole luotu tuolle www-sivustolle tai sovellukseen, plus-merkki näytetään kuvakkeessa.

▲ Napsauta tai napauta **Salasanojen hallinta** -kuvaketta näyttääksesi pikavalikon, missä voit valita seuraavista valinnoista:

- Lisää [somedomain.com] Salasanojen hallintaan
- Avaa Salasanojen hallinta
- Kuvakeasetukset
- Ohje

WWW-sivuille tai ohjelmille, missä kirjautumista ei vielä ole luotu

Seuraavat valinnat näytetään pikavalikossa:

- **Lisää [somedomain.com] Salasanojen hallintaan**—Antaa sinun lisätä kirjautumisen nykyistä kirjautumisnäyttöä varten.
- **Avaa Salasanojen hallinta**—Käynnistää Salasanojen hallinnan.
- **Kuvakeasetukset**—Antaa sinun määritellä olosuhteet, joissa **Salasanojen hallinta** -kuvake näytetään.
- **Ohje**—Näyttää HP Client Securityn ohjeen.

WWW-sivuille tai ohjelmille, joissa kirjautuminen on jo luotu

Seuraavat valinnat näytetään pikavalikossa:

- **Täytä kirjautumistieto**—Näyttää **Varmista henkilöllisyytesi** -sivun. Jos onnistuneesti todennettu, kirjautumistietosi laitetaan kirjautumiskenttiin, ja sen jälkeen sivu lähetetään (jos lähettäminen oli määritelty, kun kirjautuminen oli luotu tai viimeksi muokattu).
- **Muokkaa kirjautumista**—Antaa sinun muokata kirjautumistietoasi tälle www-sivulle.

- **Lisää kirjautuminen**—Antaa sinun lisätä tilin Salasanojen hallintaan.
- **Avaa Salasanojen hallinta**—Käynnistää Salasanojen hallinnan.
- **Ohje**—Näyttää HP Client Securityn ohjeen.

HUOMAUTUS: Tämän tietokoneen järjestelmänvalvoja voi olla määrittänyt HP Client Securityn pyytämään enemmän kuin yhdet valtuustiedot kun henkilöllisyytesi varmistetaan.

Lisätään kirjautumisia

Voit helposti lisätä kirjautumisen www-sivustoa tai ohjelmaa varten antamalla kirjautumistiedot kerran. Siitä lähtien Salasanojen hallinta antaa automaattisesti tiedot sinulle. Voit käyttää näitä kirjautumisia selattuasi www-sivustolle tai ohjelmaan.

Kirjautumisten lisääminen:

1. Avaa kirjautumisnäyttö www-sivustoa tai ohjelmaa varten.
2. Napsauta tai napauta **Salasanojen hallinta** -kuvaketta, ja sen jälkeen napsauta tai napauta yhtä seuraavista, riippuen onko kirjautumisnäyttö www-sivustoa tai ohjelmaa varten:
   - www-sivustoa varten napsauta tai napauta **Lisää [toimialuenimi] Salasanojen hallintaan**.
   - www ohjelmaa varten napsauta tai napauta **Lisää tämä kirjautumisnäyttö Salasanojen hallintaan**.
3. Anna kirjautumistiedot. Kirjautumiskentät näytöllä, ja vastaavat kentät valintaruudussa, tunnistetaan lihavoidulla oranssilla rajalla.
   a. Täyttääksesi kirjautumiskentän yhdellä esiformatoiduista valinnoista napsauta tai napauta nuolia, jotka ovat kentästä oikealle.
   b. Katsoaksesi salasanan tälle kirjautumiselle napsauta tai napauta **Näytä salasana**.
   c. Jotta saat kirjautumiskentät täytetyiksi, mutta ei lähetetyksi, tyhjennä **Kirjautumistiedon automaattinen lähetys** -valintaruutu.
   d. Napsauta tai napauta **OK** valitaksesi todennusmenetelmän, jota haluat käyttää (sormenjäljet, älykortti, lähestymiskortti, kontaktiton kortti, Bluetooth-puhelin, PIN, tai salasana), ja sen jälkeen kirjaudu valitulla todennusmenetelmällä.

      Plus-merkki poistetaan **Salasanojen hallinta** -kuvakkeesta ilmoittamaan sinulle, että kirjautuminen on luotu.
   e. Jos Salasanojen hallinta ei löydä kirjautumiskenttiä, napsauta tai napauta **Enemmän kenttiä**.
      - Valitse kunkin kirjautumiseen vaadittavan kentän valintaruutu tai poista niiden kenttien valintaruudut, joita ei vaadita kirjautumiseen.
      - Napsauta tai napauta **Sulje**.

Joka kerta kun haet tuota www-sivustoa tai avaat tuon ohjelman, **Salasanojen hallinta** -kuvake näytetään ylhäällä www-sivun vasemmassa kulmassa tai sovelluksen kirjautumisnäytössä osoittaen, että voit käyttää rekisteröityjä valtuustietojasi kirjautumiseen.

Muokataan kirjautumisia

Kirjautumisen muokkaaminen:

1. Avaa kirjautumisnäyttö www-sivustoa tai ohjelmaa varten.
2. Näyttääksesi valintaruudun, missä voit muokata kirjautumistietojasi napsauta tai napauta **Salasanojen hallinta** -kuvaketta, ja sen jälkeen napsauta tai napauta **Muokkaa kirjautumista**.

   Kirjautumiskentät näytöllä, ja vastaavat kentät valintaruudussa, tunnistetaan lihavoidulla oranssilla rajalla.

   Voit myös muokata tilitietoja Salasanojen hallinta -sivulta napsauttamalla tai napauttamalla kirjautumista näyttämään muokkausvalinnat ja sen jälkeen valitsemalla **Muokkaa**.
3. Muokkaa kirjautumistietojasi.
   - Muokataksesi **Tilin nimi** -tietoa anna uusi nimi kenttään.
   - Lisätäksesi tai muokataksesi **Luokka**-nimeä anna tai muuta nimi **Luokka**-kentässä.
   - Valitaksesi **Käyttäjänimi**-kirjautumiskentän yhdellä esiformatoiduista kentistä napsauta tai napauta alas-nuolta kentän oikealla puolella.

     Esiformatoituja valintoja on käytettävissä vain, kun muokataan kirjautumista Muokkaa-komennosta Salasanojen hallinta -kuvakkeen pikavalikossa.
   - Valitaksesi **Salasana**-kirjautumiskentän yhdellä esiformatoiduista kentistä napsauta tai napauta alas-nuolta kentän oikealla puolella.

     Esiformatoituja valintoja on käytettävissä vain, kun muokataan kirjautumista Muokkaa-komennosta Salasanojen hallinta -kuvakkeen pikavalikossa.
   - Lisätäksesi lisäkenttiä näytöstä kirjautumiseesi napsauta tai napauta **Enemmän kenttiä**.
   - Katsoaksesi salasanan tälle kirjautumiselle napsauta tai napauta **Näytä salasana** -kuvake.
   - Jotta saat kirjautumiskentät täytetyiksi, mutta ei lähetetyksi, tyhjennä **Kirjautumistiedon automaattinen lähetys** -valintaruutu.
   - Merkitäksesi tämän kirjautumisen olevan epäilyttävä salasana valitse **Tämä salasana on epäilyttävä** -valintaruutu.

     Sen jälkeen kun muutokset on tallennettu, kaikki muut kirjautumiset jakaen saman salasanan merkitään myös epäilyttävinä. Voit sen jälkeen vierailla kullakin vaikutetulla tilillä ja muuttaa salasanat tarpeen mukaan.
4. Napsauta tai napauta **OK**.

Salasanojen hallinnan Pikalinkkien valikko

Salasanojen hallinta tarjoaa nopean, helpon keinon käynnistää www-sivut ja ohjelmat joita varten olet luonut kirjautumisia. Kaksoisnapsauta tai kaksoisnapauta ohjelmaa tai www-sivuston kirjautumista **Salasanojen hallinnan Pikalinkit** -valikosta, tai Salasanojen hallinnan sivulta HP Client Securityn sisällä avataksesi kirjautumisnäytön, ja sen jälkeen täytä kirjautumistietosi.

Kun luot kirjautumisen, se lisätään automaattisesti Salasanojen hallinnan **Pikalinkit**-valikkoon.

Pikalinkit-valikon näyttäminen:

- ▲ Paina **Password Manager** -pikanäppäinyhdistelmää. Tehdasasetus on (Ctrl+Windows-näppäin +h Pikanäppäinyhdistelmän muuttamiseksi napsauta HP Client Securityn etusivulta **Salasanojen hallinta**, ja sen jälkeen napsauta tai napauta **Asetukset**.

Kirjautumisten järjestäminen luokkiin

Luo yksi tai useampia luokkia pitämään kirjautumisesi järjestyksessä.

Kirjautumisen kiinnittäminen luokkaan:

1. Napsauta tai napauta HP Client Security -etusivulta **Salasanojen hallinta**.
2. Napsauta tai napauta tilin syöttöä ja sen jälkeen napsauta tai napauta **Muokkaa**.
3. Anna **Luokka**-kentässä luokan nimi.
4. Napsauta tai napauta **Tallenna**.

Tilin poistaminen luokasta:

1. Napsauta tai napauta HP Client Security -etusivulta **Salasanojen hallinta**.
2. Napsauta tai napauta tilin syöttöä ja sen jälkeen napsauta tai napauta **Muokkaa**.
3. Pyyhi pois **Luokka**-kentässä luokan nimi.
4. Napsauta tai napauta **Tallenna**.

Luokan nimeäminen uudelleen:

1. Napsauta tai napauta HP Client Security -etusivulta **Salasanojen hallinta**.
2. Napsauta tai napauta tilin syöttöä ja sen jälkeen napsauta tai napauta **Muokkaa**.
3. Muuta **Luokka**-kentässä luokan nimi.
4. Napsauta tai napauta **Tallenna**.

Kirjautumistesi hallinta

Salasanojen hallinta tekee helpoksi hallita kirjautumistietojasi käyttäjänimiä, salasanoja, ja useita kirjautumistilejä yhdestä keskussijaintipaikasta.

Kirjautumisesi luetteloidaan Salasanojen hallinta -sivulla.

Kirjautumistesi hallinta:

1. Napsauta tai napauta HP Client Security -etusivulta **Salasanojen hallinta**.
2. Napsauta tai napauta olemassa olevaa kirjautumista, ja sen jälkeen valitse yksi seuraavista valinnoista ja sen jälkeen seuraa näytöllä näkyviä ohjeita:
   - **Muokkaa**—Muokkaa kirjautumista. Lisätietoja on kohdassa Muokataan kirjautumisia sivulla 20.
   - **Kirjaudu sisään**—Kirjaudu sisään valitulle tilille.
   - **Poista**—Poista kirjautuminen valittua tiliä varten.

Lisä kirjautumisen lisääminen www-sivustoa tai ohjelmaa varten:

1. Avaa kirjautumisnäyttö www-sivustoa tai ohjelmaa varten.
2. Napsauta tai napauta **Salasanojen hallinta** -kuvaketta sen pikavalikon näyttämiseksi.
3. Napsauta tai napauta **Lisää kirjautuminen**, ja sen jälkeen seuraa näytöllä näkyviä ohjeita.

Salasanasi vahvuuden arvioiminen

Vahvojen salasanojen käyttäminen kirjautumiseen www-sivustoillesi ja ohjelmiin on tärkeä henkilöllisyytesi suojauksen näkökohta.

Salasanojen hallinta tekee turvallisuutesi valvonnan ja parantamisen helpoksi välittömällä ja automatisoidulla kunkin www-sivustolle ja ohjelmiin käytettyjen kirjautumisten salasanojen vahvuuden analyysillä.

Kun olet antamassa tilille salasanaa Salasanojen hallinnan kirjautumisen luomisen aikana, värillinen palkki näytetään salasanan alla osoittaen salasanan vahvuuden. Värit osoittava seuraavia arvoja:

- **Punainen**—Heikko
- **Keltainen**—Kohtalainen
- **Vihreä**—Vahva

Salasanojen hallinnan kuvakkeen asetukset

Salasanojen hallinta pyrkii tunnistamaan kirjautumisnäytöt www-sivustoille ja ohjelmille. Kun se tunnistaa kirjautumisnäytön, jolle et ole luonut kirjautumista, Salasanojen hallinta kehottaa sinua lisäämään kirjautumisen näytölle näyttäen **Salasanojen hallinta** -kuvakkeen plus-merkin kanssa.

1. Napsauta tai napauta kuvaketta, ja sen jälkeen napsauta tai napauta **Kuvakkeen asetukset** mukauttaaksesi kuinka Salasanojen hallinta käsittelee mahdollisia kirjautumissivustoja.
   - **Kehote lisätä kirjautumisia kirjautumisnäyttöjä varten**—Napsauta tai napauta tätä valintaa, jotta saat Salasanojen hallinnan kehottamaan sinua lisäämään kirjautumisen, kun näytetään kirjautumisnäyttö, jolla ei ennestään ole kirjautumisasetusta.
   - **Sulje tämä näyttö pois**—Valitse valintaruutu niin, että Salasanojen hallinta ei kehota sinua uudelleen lisäämään kirjautumisen tätä kirjautumisnäyttöä varten.
   - **Älä kehota lisäämään kirjautumisia kirjautumisnäyttöjä varten**—Valitse valintanappi.
2. Kirjautumisen lisääminen näytölle, joka on aikaisemmin ollut poissuljettu:
   a. Kirjaudu aikaisemmin poissuljetulle www-sivustolle.
   b. Saadaksesi Salasanojen hallinnan muistamaan salasanan tälle sivustolle napsauta tai napauta **Muista** ponnahdusvalintaikkunassa tallentaaksesi salasanan ja luodaksesi kirjautumisen näytölle.
3. Päästäksesi Salasanojen hallinnan lisäasetuksiin napsauta tai napauta Salasanojen hallinta -kuvaketta, napsauta tai napauta **Avaa Salasanojen hallinta**, ja sen jälkeen napsauta tai napauta **Asetukset** Salasanojen hallinnan sivulla.

Kirjautumisten tuominen ja vieminen

Salasanojen hallinnan Tuo- ja Vie-sivulla voit tuoda kirjauksia, joita www-selaimet ovat tallentaneet tietokoneessasi. Voit myös tuoda tietoa HP Client Securityn tallennuskopiointitiedostosta ja viedä tietoa HP Client Securityn tallennuskopiointitiedostoon.

▲ Käynnistääksesi Tuo- ja vie-sivun, napsauta tai napauta **Tuo- ja vie** Salasanojen hallinnan sivulla.

Salasanojen tuominen selaimelta:

1. Napsauta tai napauta selainta, jolta haluat tuoda salasanoja (vain asennetut selaimet näytetään).
2. Tyhjennä valintaruutu kaikista tileistä, joita varten et halua tuoda salasanoja.
3. Valitse tai napsauta **Tuo**.

Tiedon tuominen tai tiedon vieminen HP Client Securityn tallennuskopiointitiedostoon voidaan suorittaa liittyvien linkkien kautta (kohdassa **Muut valinnat)** Tuo- ja vie-sivulla.

HUOMAUTUS: Tämä ominaisuus tuo ja vie vain Salasanojen hallinnan tietoa. Katso tietoja Client Securityn lisätietojen varmuuskopioinnista ja palautuksesta kohdasta Tietojesi varmuuskopiointi ja palautus sivulla 26.

Tietojen tuominen HP Client Securityn tallennuskopiointitiedostosta:

1. Napsauta tai napauta HP Password Managerin Tuo- ja vie-sivulta **Tuo tietoa HP Client Securityn tallennuskopiointitiedostosta**.
2. Varmista henkilöllisyytesi.
3. Valitse aikaisemmin luotu tallennuskopiointitiedosto, tai anna polku tarjotussa kentässä, ja sen jälkeen napsauta tai napauta **Selaa**.
4. Anna tiedoston suojaamiseen käytetty salasana, ja sen jälkeen napsauta tai napauta **Seuraava**.
5. Napsauta tai napauta **Palautus**.

Tiedon vienti HP Client Securityn tallennuskopiointitiedostoon:

1. Napsauta tai napauta HP Password Managerin Tuo- ja vie-sivulta **Vie tietoa HP Client Securityn tallennuskopiointitiedostosta**.
2. Varmista henkilöllisyytesi, ja sen jälkeen napsauta tai napauta **Seuraava**.
3. Anna nimi varmuuskopiotiedostolle. Oletuksena tiedosto tallennetaan Asiakirjat-kansioosi. Eri sijaintipaikan määrittämiseksi napsauta tai napauta **Selaa**.
4. Anna ja vahvista tiedoston suojaamiseen käytetty salasana, ja sen jälkeen napsauta tai napauta **Tallenna**.

Asetukset

Voit määritellä asetuksia Salasanojen hallinnan henkilökohtaistamiseksi:

- **Kehote lisätä kirjautumisia kirjautumisnäyttöihin—Salasanojen hallinta** -kuvake plus-merkin kanssa näytetään aina kun www-sivun tai ohjelman kirjautumisnäyttö havaitaan osoittaen, että voit lisätä kirjautumisen tälle näyttöruudulle **Kirjautumiset**-valikkoon.

  Poistaaksesi tämän ominaisuuden käytöstä tyhjennä valintaruutu **Kehote lisätä kirjautumisia kirjautumisnäyttöihin** -toiminnon vieressä.

- **Avaa Password Manager näppäinyhdistelmällä Ctrl+Win+h** - Oletusnäppäinyhdistelmä, joka avaa **Password Managerin pikalinkit** -valikon, on Ctrl+Windows- näppäin+h.

  Pikanäppäimen muuttamiseksi napsauta tai napauta tätä valintaa, ja sen jälkeen anna uusi näppäinyhdistelmä. Yhdistelmät voivat sisältää yhden tai useampia seuraavista: ctrl, alt, tai vaihtonäppäin, ja mikä tahansa aakkosnumeerinen näppäin.

  Windowsiin tai Windows-sovelluksiin käytettyjä yhdistelmiä ei voida käyttää.

- Palauttaaksesi asetukset tehdasoletusarvoihin napsauta tai napauta **Palauta oletukset**.

Lisäasetukset

Järjestelmänvalvojat voivat päästä seuraaviin valintoihin valitsemalla **Gear** (asetukset) -kuvakkeen HP Client Securityn -etusivulta.

- **Järjestelmänvalvojan käytännöt**—Antaa sinun määrittää kirjautumisen ja istunnon käytännöt järjestelmänvalvojille.
- **Vakiokäyttäjän käytännöt**—Antaa sinun määrittää kirjautumisen ja istunnon käytännöt vakiokäyttäjille.
- **Suojausominaisuudet**—Antaa sinun lisätä tietokoneesi suojausta suojaamalla Windows-tilisi käyttämällä vahvaa todennusta ja/tai ottamalla todennuksen käyttöön ennen Windowsin käynnistämistä.
- **Käyttäjät**- tämän avulla voit hallita käyttäjiä ja heidän tunnistetietoja.
- **Omat käytännöt**—Antaa sinun tarkistaa todennuskäytäntösi ja rekisteröinnin tilan.
- **Varmuuskopiointi ja Palautus**—Antaa sinun varmuuskopioida ja palauttaa HP Client Securityn tiedon.
- **Tietoja HP Client Securitystä**- Näyttää HP Client Securityn versiotiedot.

Järjestelmänvalvojan käytännöt

Voit määrittää sisäänkirjautuminen- ja istuntokäytäntöjä tämän tietokoneen järjestelmänvalvojille. Tässä asetetut kirjautumiskäytännöt hallitsevat valtuustietoja, jotka paikalliselle järjestelmänvalvojalle tarvitaan Windowsiin kirjautumiseen. Tässä asetetut istuntokäytännöt hallitsevat valtuustietoja, jotka paikalliselle järjestelmänvalvojalle tarvitaan vahvistamaan henkilöllisyyden Windows-istunnon sisällä.

Oletuksena kaikki uudet tai muutetut käytännöt toimeenpannaan välittömästi **Käytä** napsauttamisen tai napauttamisen jälkeen.

Uuden käytännön lisääminen:

1. Napsauta tai napauta HP Client Securityn etusivulta **Gear**-kuvaketta.
2. Napsauta tai napauta Lisäasetukset-sivulta **Järjestelmänvalvojan käytännöt**.
3. Napsauta tai napauta **Lisää uusi käytäntö**.
4. Napsauta alas-nuolia valitaksesi ensisijaiset ja (valinnainen) toissijaiset valtuustiedot uudelle käytännölle, ja sen jälkeen napsauta tai napauta **Lisää**.
5. Valitse **Apply** (Käytä).

Uuden tai muutetun käytännön toimeenpanon viivästäminen:

1. Napsauta tai napauta **Toimeenpane tämä käytäntö välittömästi**.
2. Valitse **Toimeenpane tämä käytäntö tiettynä päivämääränä**.
3. Anna päivämäärä tai käytä ponnahduskalenteria valitaksesi päivämäärän, kun tämän käytännön tulee olla toimeenpantuna.
4. Halutessasi valitse milloin käyttäjiä muistutetaan uudesta käytännöstä.
5. Valitse **Apply** (Käytä).

Vakiokäyttäjän käytännöt

Voit määrittää kirjautumisen ja istunnon käytännöt tämän tietokoneen vakiokäyttäjille. Tässä asetetut kirjautumiskäytännöt hallitsevat valtuustietoja, jotka paikalliselle järjestelmänvalvojalle tarvitaan Windowsiin kirjautumiseen. Tässä asetetut istuntokäytännöt hallitsevat valtuustietoja, jotka paikalliselle järjestelmänvalvojalle tarvitaan vahvistamaan henkilöllisyyden Windows-istunnon sisällä.

Oletuksena kaikki uudet tai muutetut käytännöt toimeenpannaan välittömästi **Käytä** napsauttamisen tai napauttamisen jälkeen.

Uuden käytännön lisääminen:

1. Napsauta tai napauta HP Client Securityn etusivulta **Gear**-kuvaketta.
2. Napsauta tai napauta Lisäasetukset-sivulta **Vakiokäyttäjän käytännöt**.
3. Napsauta tai napauta **Lisää uusi käytäntö**.
4. Napsauta alas-nuolia valitaksesi ensisijaiset ja (valinnainen) toissijaiset valtuustiedot uudelle käytännölle, ja sen jälkeen napsauta tai napauta **Lisää**.
5. Valitse **Apply** (Käytä).

Uuden tai muutetun käytännön toimeenpanon viivästäminen:

1. Napsauta tai napauta **Toimeenpane tämä käytäntö välittömästi**.
2. Valitse **Toimeenpane tämä käytäntö tiettynä päivämääränä**.
3. Anna päivämäärä tai käytä ponnahduskalenteria valitaksesi päivämäärän, kun tämän käytännön tulee olla toimeenpantuna.
4. Halutessasi valitse milloin käyttäjiä muistutetaan uudesta käytännöstä.
5. Valitse **Apply** (Käytä).

Suojausominaisuudet

Voit ottaa käyttöön HP Client Securityn ominaisuudet, jotka auttavat suojaamaan luvattomalta pääsyltä tietokoneeseen:

Suojausominaisuuksien asettaminen:

1. Napsauta tai napauta HP Client Securityn etusivulta **Gear**-kuvaketta.
2. Napsauta tai napauta Lisäasetukset-sivulta **Suojausominaisuudet**.
3. Ota käyttöön suojausominaisuuksia valitsemalla valintaruudut, ja sen jälkeen napsauta tai napauta **Käytä**. Mitä enemmän ominaisuuksia valitset, sitä suojatumpi tietokoneesi on.

   Nämä asetukset pätevät kaikille käyttäjille.

   - **Windowsin kirjautumisen suojaus**—Suojaa Windows-tilisi vaatimalla HP Client Securityn valtuustiedot pääsyyn -toiminnon käytön.
   - **Pre-Boot Security (Power-on authentication)**—Suojaa tietokoneesi ennen Windowsin käynnistämistä. Tämä valinta ei ole käytettävissä, jos BIOS ei sitä tue.
   - **Salli yhden vaiheen kirjautuminen**—Tämä asetus sallii Windows-kirjautumisen ohittamisen, jos todennus oli aikaisemmin suoritettu Power–on-todennuksessa tai Drive Encryption -tasolla.
4. Valitse tai napauta **käyttäjät** ja napsauta tai napauta käyttäjän ruutua.

Users (Käyttäjät)

Voit valvoa ja hallita tämän tietokoneen HP Client Securityn käyttäjiä.

Toisen Windows-käyttäjän lisääminen HP Client Security -sovellukseen:

1. Napsauta tai napauta HP Client Securityn etusivulta **Gear**-kuvaketta.
2. Napsauta tai napauta Lisäasetukset-sivulta **Käyttäjät**.
3. Napsauta tai napauta **Lisää toinen Windows-käyttäjä HP Client Security -sovellukseen**.
4. Anna käyttäjän nimi, jonka haluat lisätä, ja sen jälkeen napsauta tai napauta **OK**.
5. Anna käyttäjän Windows-salasana.

   Lisätylle käyttäjälle näytetään laatta Käyttäjä-sivulla.

Windows-käyttäjän poistaminen HP Client Security -sovelluksesta:

1. Napsauta tai napauta HP Client Securityn etusivulta **Gear**-kuvaketta.
2. Napsauta tai napauta Lisäasetukset-sivulta **Käyttäjät**.
3. Napsauta tai napauta käyttäjän nimeä, jonka haluat poistaa.
4. Napsauta tai napauta **Poista käyttäjä** ja vahvista napsauttamalla tai napauttamalla **Kyllä**.

Kirjautumis- ja istuntokäytäntöjen yhteenvedon näyttäminen toimeenpantuna käyttäjälle:

▲ Valitse tai napauta **käyttäjät** ja napsauta tai napauta käyttäjän ruutua.

Omat käytännöt

Voit näyttää todennuskäytäntösi ja rekisteröinnin tilan. Omat käytännöt -sivu tarjoaa myös linkkejä Järjestelmänvalvojan käytännöt- ja Vakiokäyttäjän käytännöt -sivuille.

1. Napsauta tai napauta HP Client Securityn etusivulta **Gear**-kuvaketta.
2. Napsauta tai napauta Lisäasetukset-sivulta **Omat käytännöt**.

   Toimeenpannut kirjautumis- ja istuntokäytännöt parhaillaan kirjautuneena olevalle käyttäjälle näytetään.

Omat käytännöt -sivu tarjoaa myös linkit kohtaan Järjestelmänvalvojan käytännöt sivulla 24 ja Vakiokäyttäjän käytännöt sivulla 25.

Tietojesi varmuuskopiointi ja palautus

On suositeltavaa, että varmuuskopioit HP Client Security -tiedon säännöllisesti. Kuinka usein varmuuskopioit sen riippuu siitä kuinka usein tieto muuttuu. Jos esimerkiksi lisäät uusia kirjautumisia päivittäin, sinun tulisi varmuuskopioida tietosi päivittäin.

Varmuuskopiointeja voidaan käyttää myös siirtämään tietokoneesta toiseen, mitä nimitetään myös tuomiseksi ja viemiseksi.

HUOMAUTUS: Vain Salasanojen hallinta on varmuuskopioitu tällä ominaisuudella. Drive Encryptionilla on itsenäinen varmuuskopiointimenetelmä. Device Access Manager- ja sormenjälkitodennuksen tiedot eivät ole varmuuskopioituja.

HP Client Securityn täytyy olla asennettuna jokaiseen tietokoneeseen, jonka on vastaanotettava varmuuskopioitua tietoa ennen kuin tieto voidaan palauttaa varmuuskopiotiedostosta.

Tietosi varmuuskopioiminen:

1. Napsauta tai napauta HP Client Securityn etusivulta **Gear**-kuvaketta.
2. Napsauta tai napauta Lisäasetukset-sivulta **Järjestelmänvalvojan käytännöt**.
3. Napsauta tai napauta **Varmuuskopiointi ja Palautus**.
4. Napsauta tai napauta **Varmuuskopiointi**, ja sen jälkeen vahvista henkilöllisyytesi.
5. Valitse moduuli, jonka haluat sisältyvän varmuuskopiointiin, ja sen jälkeen napsauta tai napauta **Seuraava**.
6. Anna nimi tallennustiedostolle. Oletuksena tiedosto tallennetaan Asiakirjat-kansioosi. Eri sijaintipaikan määrittämiseksi napsauta tai napauta **Selaa**.
7. Anna ja vahvista tiedoston suojaamiseen käytetty salasana.
8. Napsauta tai napauta **Tallenna**.

Tietosi palauttaminen:

1. Napsauta tai napauta HP Client Securityn etusivulta **Gear**-kuvaketta.
2. Napsauta tai napauta Lisäasetukset-sivulta **Järjestelmänvalvojan käytännöt**.
3. Napsauta tai napauta **Varmuuskopiointi ja Palautus**.
4. Valitse **Palautus**, ja sen jälkeen vahvista henkilöllisyytesi.
5. Valitse aikaisemmin luotu tallennustiedosto. Anna polku tarjotussa kentässä. Eri sijaintipaikan määrittämiseksi napsauta tai napauta **Selaa**.
6. Anna tiedoston suojaamiseen käytetty salasana, ja sen jälkeen napsauta tai napauta **Seuraava**.
7. Valitse moduulit joista haluat palauttaa tiedon.
8. Napsauta tai napauta **Palautus**.

5 HP Drive Encryption (vain tietyt mallit)

HP Drive Encryption tarjoaa täydellisen tiedon suojauksen salaamalla tietokoneesi tiedot. Kun Drive Encryption on käytössä, sinun on kirjauduttava sisään Drive Encryption -kirjautumisnäytössä, joka tulee näyttöön ennen Windows®-käyttöjärjestelmän käynnistymistä.

HP Client Security Home -näyttöruutu sallii Windows-järjestelmänvalvojien aktivoida aseman salauksen, varmuuskopioida salausavaimen, ja valita tai valita pois asemia tai osioita salausta varten. Katso lisätietoja HP Client Security -ohjelmiston ohjeesta.

Seuraavat tehtävät voidaan suorittaa aseman salauksella:

- Aseman salauksen asetusten valitseminen:
  - Yksittäisten asemien tai osioiden salaaminen tai salauksen poistaminen ohjelmiston salausta käyttämällä
  - Yksittäisten itsesalaavien asemien salaaminen tai salauksen poistaminen laitteiston salausta käyttämällä
  - Lisäsuojauksen lisääminen poistamalla käytöstä lepotilan tai valmiustilan varmistamaan, että aseman salauksen esikäynnistyksen todennus aina tarvitaan

HUOMAUTUS: Vain sisäiset SATA- ja ulkoiset eSATA-kovalevyasemat voidaan salata.

- Varmuuskopiointiavainten luominen
- Pääsyn palauttaminen salattuun tietokoneeseen käyttämällä varmuuskopiointiavaimia ja HP SpareKey -sovellusta
- Aseman salauksen esikäynnistyksen todennuksen käyttöönottaminen käyttäen salasanaa, rekisteröityä sormenjälkeä, tai PINiä älykorttien valitsemiseen

Aseman salauksen avaaminen

Järjestelmänvalvojat voivat päästä aseman salaukseen avaamalla HP Client Security -sovelluksen:

1. Napsauta tai napauta Käynnistä-ruudulta **HP Client Security** -sovellusta (Windows 8).

   TAI

   Kaksoisnapsauta tai kaksoisnapauta Windowsin työpöydällä, tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella sijaitsevaa **HP Client Security** -kuvaketta.

2. Napsauta tai napauta **Aseman salaus** -kuvaketta.

Yleiset tehtävät

Aseman salauksen aktivointi vakiokovalevyasemille

Vakiokovalevyasemat salataan ohjelmiston salausta käyttämällä. Seuraa näitä vaiheita salataksesi aseman tai levyn osion:

1. Käynnistä **Aseman salaus**. Lisätietoja on kohdassa Aseman salauksen avaaminen sivulla 28.
2. Valitse valintaruutu asemalle tai osiolle, jonka haluat salata, ja sen jälkeen napsauta tai napauta **Varmuuskopiointiavain**.

HUOMAUTUS: Parempaa turvallisuutta varten valitse **Poista lepotila käytöstä lisättyä turvallisuutta varten** valintaruutu. Kun poistat lepotilan käytöstä, ei ehdottomasti ole vaaraa, että aseman avaamiseen käytetyt valtuustiedot on tallennettu muistiin.

3. Valitse yksi tai useampia varmuuskopioinnin valintoja, ja sen jälkeen napsauta tai napauta **Varmuuskopiointi**. Lisätietoja on kohdassa Varmuuskopioidaan salausavaimia sivulla 32.
4. Voit jatkaa työskentelyä samalla kun salausavainta ollaan varmuuskopioimassa. Älä käynnistä tietokonettasi uudelleen.

HUOMAUTUS: Sinua kehotetaan käynnistämään tietokoneesi uudelleen. Uudelleen käynnistämisen jälkeen aseman salauksen esikäynnistyksen näyttöruutu näytetään, tarvitaan todennus ennen kuin Windows käynnistyy.

Aseman salaus on aktivoitu. Valittujen aseman osioiden salaus voi viedä tunteja riippuen osioiden lukumäärästä ja koosta.

Katso lisätietoja HP Client Security -ohjelmiston ohjeesta.

Aseman salauksen aktivointi itsesalaaville asemille

Itsesalaavat asemat, jotka täyttävät Trusted Computing Group'in OPAL:in määritykset itsesalaavan aseman hallinnasta voidaan salata käyttämällä joko ohjelmiston salausta tai laitteiston salausta. Laitteiston salaus on paljon nopeampaa kuin ohjelmiston salaus. Et kuitenkaan voi valita mitkä levyn osiot salataan. Koko levy salataan, mukaan lukien mitkä tahansa levyn osiot.

Salataksesi tietyt osiot silloin sinun täytyy käyttää ohjelmiston salausta. Varmista, että tyhjennät **Salli vain laitteiston salaus itsesalaaville asemille (SEDit)** -valintaruudun.

Seuraa näitä vaiheita aktivoidaksesi aseman salauksen itsesalaaville asemille:

1. Käynnistä **Aseman salaus**. Lisätietoja on kohdassa Aseman salauksen avaaminen sivulla 28.
2. Valitse valintaruutu asemalle, jonka haluat salata, ja sen jälkeen napsauta tai napauta **Varmuuskopiointiavain**.

HUOMAUTUS: Parempaa turvallisuutta varten valitse **Poista lepotila käytöstä lisättyä turvallisuutta varten** -valintaruutu. Kun poistat lepotilan käytöstä, ei ehdottomasti ole vaaraa, että aseman avaamiseen käytetyt valtuustiedot on tallennettu muistiin.

3. Valitse yksi tai useampia varmuuskopioinnin valintoja, ja sen jälkeen napsauta tai napauta **Varmuuskopiointi**. Lisätietoja on kohdassa Varmuuskopioidaan salausavaimia sivulla 32.
4. Voit jatkaa työskentelyä samalla kun salausavainta ollaan varmuuskopioimassa. Älä käynnistä tietokonettasi uudelleen.

HUOMAUTUS: Itsesalaaville asemille sinua kehotetaan sammuttamaan tietokoneen.

Katso lisätietoja HP Client Security -ohjelmiston ohjeesta.

Aseman salauksen estäminen

1. Käynnistä **Aseman salaus**. Lisätietoja on kohdassa Aseman salauksen avaaminen sivulla 28.
2. Tyhjennä valintaruutu kaikilta salatuilta asemilta, ja sen jälkeen napsauta tai napauta **Käytä**.

   Aseman salauksen estäminen alkaa.

HUOMAUTUS: Jos käytettiin ohjelmiston salausta, salauksen purkaminen käynnistyy. Se voi viedä tunteja riippuen salatun kovalevyaseman osioiden koosta. Kun salauksen purku on valmis, aseman salaus estetään.

Jos käytettiin laitteiston salausta, aseman salaus puretaan hetkessä ja muutamien minuuttien kuluttua aseman salaus estetään.

Heti kun aseman salaus on estetty sinua kehotetaan sammuttamaan tietokone, jos laitteisto salattiin, tai käynnistä tietokone uudelleen, jos ohjelmisto salattiin.

Sisäänkirjautuminen aseman salauksen aktivoimisen jälkeen

Kun käynnistät tietokoneen aseman salauksen aktivoimisen jälkeen ja käyttäjätilisi ilmoitetaan, sinun täytyy sisäänkirjautua aseman salauksen sisäänkirjautumisen ruudulla:

HUOMAUTUS: Kun herätään lepotilasta tai valmiustilasta, aseman salauksen esikäynnistyksen todennusta ei näytetä ohjelmiston salausta tai laitteiston salausta varten. Laitteiston salaus tarjoaa **Poista lepotila käytöstä lisättyä turvallisuutta varten** -valinnan, mikä estää lepotilan tai valmiustilan tapahtumasta kun se otettiin käyttöön.

Kun herätään horrostilasta, aseman salauksen esikäynnistyksen todennusta ei näytetä ohjelmiston salausta eikä laitteiston salausta varten.

HUOMAUTUS: Jos Windows-järjestelmänvalvoja on ottanut käyttöön BIOS Pre-boot Security -sovelluksen HP Client Security -sovelluksessa ja jos One-Step Logon on otettu käyttöön (oletuksena), voit kirjautua sisään tietokoneeseen välittömästi BIOS-esikäynnistyksessä tapahtuvan todennuksen jälkeen tarvitsematta uudelleentodennusta aseman salauksen sisäänkirjautumisen ruudulla.

Yhden käyttäjän sisäänkirjautuminen:

- ▲ Anna **Sisäänkirjautuminen**-sivulla Windows-salasanasi, älykortin PIN, SpareKey, tai pyyhkäise rekisteröidyllä sormella.

Usean käyttäjän sisäänkirjautuminen:

1. Valitse **Valitse käyttäjä sisäänkirjautumiseen** -sivulla käyttäjä sisäänkirjautumiseen pudotusluettelosta ja sen jälkeen napsauta tai napauta **Seuraava**.
2. Anna **Sisäänkirjautuminen**-sivulla Windows-salasanasi tai älykortin PIN, tai pyyhkäise rekisteröidyllä sormella.

HUOMAUTUS: Seuraavia älykortteja tuetaan:

Tuetut älykortit

- Gemalto Cyberflex Access 64k V2c

HUOMAUTUS: Jos palautusavainta käytetään sisäänkirjutumiseen aseman salauksen sisäänkirjautumisen ruudulla, lisävaltuustietoja tarvitaan Windowsiin sisäänkirjautumiseen käyttäjän tileihin pääsyä varten.

Lisäkovalevyasemien salaaminen

On erittäin suositeltavaa, että käytät HP Drive Encryption -sovellusta suojaamaan tietosi salaamalla kovalevyasemasi. Minkä tahansa luotujen kovalevyasemien tai osioiden aktivoimisen jälkeen voidaan ne salata seuraamalla näitä vaiheita:

1. Käynnistä **Aseman salaus**. Lisätietoja on kohdassa Aseman salauksen avaaminen sivulla 28.
2. Valitse ohjelmistosuojatuille asemille salattavat aseman osiot.

HUOMAUTUS: Tämä pätee myös seka-asematapaukseen, missä läsnä on yksi tai useampi vakiokovalevyasema ja yksi tai useampi itsesalaava asema.

TAI

▲ Valitse laitteistosuojatuille asemille salattavat lisäasemat.

Lisätehtävät

Aseman salauksen hallinta (järjestelmänvalvojan tehtävä)

Järjestelmänvalvojat voivat käyttää aseman salausta näyttämään ja muuttamaan kaikkien tietokoneessa olevien kovalevyasemien salauksen tilaa (Ei salattu tai salattu).

- Jos tila on Otettu käyttöön, aseman salaus on aktivoitu ja määritetty. Asema on yhdessä seuraavista tiloista:

Ohjelmiston salaus

- Ei salattu
- Salattu
- Salataan
- Salaus poistetaan

Laitteiston salaus

- Salattu
- Ei salattu (lisäasemille)

Yksittäisten aseman osioiden salaus tai salauksen poisto (vain ohjelmiston salaus)

Järjestelmänvalvojat voivat käyttää aseman salausta salaamaan yhden tai useamman tietokoneessa olevan kovalevyaseman osion tai poistamaan salauksen mistä tahansa aseman osioista, jotka on jo salattu.

1. Käynnistä **Aseman salaus**. Lisätietoja on kohdassa Aseman salauksen avaaminen sivulla 28.
2. Valitse kohdassa **Aseman tila** tai tyhjennä valintaruutu kunkin kovalevyaseman osion vierestä, jonka haluat salata tai poistaa salauksen, ja sen jälkeen napsauta tai napauta **Käytä**.

HUOMAUTUS: Kun osiota ollaan salaamassa tai poistamassa salausta, edistymispalkki näyttää salatun osion prosentin.

HUOMAUTUS: Dynaamisia osioita ei tueta. Jos osio näytetään käytettävissä olevana, mutta sitä ei voida salata valittuna ollessa, osio on dynaaminen. Dynaaminen osio johtuu osion kutistumisesta luodakseen uuden osion Disk Management (Levyn hallinta) -toiminnon sisällä.

Varoitus näytetään, jos osio muunnetaan dynaamiseksi osioksi.

Disk management (Levyn hallinta)

- **Nickname** (Lempinimi)—Voit antaa asemillesi tai osioillesi nimiä helpompaa tunnistamista varten.
- **Irrotetut asemat**—Aseman salaus voi jäljittää levyjä, jotka on poistettu tietokoneesta. Tietokoneesta poistettu levy siirretään automaattisesti Disconnected (Irrotetut) -luetteloon. Jos levy palautetaan järjestelmään, se ilmestyy jälleen Connected (Liitetyt) -luetteloon.
- Jos sinun ei enää tarvitse jäljittää tai hallita irrotettua asemaa, voit poistaa irrotetun aseman Disconnected (Irrotetut) -luettelosta.
- Aseman salaus pysyy aktivoituna kunnes valintaruutu kaikille liitetyille asemille on tyhjennetty, ja Disconnected (Irrotetut) -luettelo on tyhjä.

Varmuuskopiointi ja palautus (järjestelmänvalvojan tehtävä)

Kun aseman salaus aktivoidaan, järjestelmänvalvojat voivat käyttää Encryption Key Backup -sivua varmuuskopioimaan salausavaimia siirrettävälle medialle ja suorittamaan palautuksen.

Varmuuskopioidaan salausavaimia

Järjestelmänvalvojat voivat varmuuskopioida salausavaimen salatulle asemalle siirrettävällä tallennuslaitteella.

VAROITUS: Varmista, että säilytät varmuuskopiointiavaimen sisältävän tallennuslaitteen turvallisessa paikassa, koska jos unohdat salasanasi, menetät älykorttisi, tai sinulla ei ole rekisteröityä sormea, vain tämä laite tarjoaa ainoan pääsysi tietokoneeseen. Tallennuspaikan tulisi myös olla turvallinen, koska tallennuslaite sallii pääsyn Windowsiin.

1. Käynnistä **Aseman salaus**. Lisätietoja on kohdassa Aseman salauksen avaaminen sivulla 28.
2. Valitse valintaruutu asemalle, sen jälkeen napsauta tai napauta**Varmuuskopiointiavain**.
3. Valitse kohdassa **Create HP Drive Encryption -palautusavain** yksi tai useampi seuraavista valinnoista:
   - **Siirrettävä tallennuspaikka**—Valitse valintaruutu, ja sen jälkeen valitse tallennuslaite, missä salausavain tallennetaan.
   - **SkyDrive**—Valitse valintaruutu. Sinun täytyy olla yhdistettynä internetiin. Kirjaudu sisään Microsoft SkyDriveen, ja sen jälkeen napsauta tai napauta **Kyllä**.

     HUOMAUTUS: Käyttääksesi HP Drive Encryption -varmuuskopiointiavainta, joka on tallennettuna SkyDrivessä, sinun täytyy ladata se SkyDrivestä siirrettävälle tallennuslaitteelle, ja sen jälkeen laittaa tallennuslaite sisään tässä tietokoneessa.
   - **TPM** (vain valitut mallit)—Sallii sinun palauttaa tietosi käyttämällä TPM-salasanaasi.

VAROITUS: Jos TPM on tyhjennetty tai tietokone on vaurioitunut, menetät pääsyn varmuuskopiointiin. Jos tämä on valittu, toinen varmuuskopiointimenetelmä pitää myös valita.

4. Napsauta tai napauta **Varmuuskopiointi**.

   Salausavain tallennetaan valitsemaasi tallennuslaitteeseen.

Pääsyn palauttaminen aktivoituun tietokoneeseen käyttämällä varmuuskopiointiavaimia

Järjestelmänvalvojat voivat suorittaa palautuksen käyttämällä aseman salausavainta, joka on varmuuskopioitu siirrettävälle tallennuslaitteelle aktivoinnissa tai valitsemalla **Varmuuskopiointiavain**-valinnan aseman salauksessa.

1. Laita sisään siirrettävä tallennuslaite, joka sisältää varmuuskopiointiavaimesi.
2. Käynnistä tietokone.
3. Kun HP Drive Encryption -sisäänkirjautumisen valintaruutu avautuu, napsauta tai napauta **Palautus**.
4. Anna tiedostopolku tai nimi, joka sisältää varmuuskopiointiavaimesi, ja sen jälkeen napsauta tai napauta **Palautus**.
5. Kun vahvistuksen valintaruutu avautuu, napsauta tai napauta **OK**.

   Windowsin sisäänkirjautuminen -ruutu näytetään.

HUOMAUTUS: Jos palautusavainta käytetään kirjautumaan sisään aseman salauksen sisäänkirjautumisen ruudulla, lisävaltuustietoja tarvitaan Windowsiin sisäänkirjautumiseen käyttäjän tileihin pääsyä varten. On erittäin suositeltavaa, että palautat salasanasi palautuksen suorittamisen jälkeen.

HP SpareKey -palautuksen suorittaminen

SpareKey -palautus aseman salauksen esikäynnistyksen sisällä pyytää sinua vastaamaan turvallisuuskysymyksiin oikein ennen kuin voit päästä tietokoneeseen. Katso lisätietoja SpareKey -palautuksen asettamisesta HP Client Security -ohjelmiston ohjeesta.

HP SpareKey -palautuksen suorittaminen, jos unohdat salasanasi:

1. Käynnistä tietokone.
2. Kun HP Drive Encryption sivu tulee näyttöön, siirry käyttäjän kirjautumissivulle.
3. Valitse **SpareKey**.

HUOMAUTUS: Jos sinun SpareKeytä ei ole alustettu HP Client Security -sovelluksessa, **SpareKey**-painike ei ole käytettävissä.

4. Kirjoita näyttöön tuleviin kysymyksiin oikeat vastaukset ja napsauta **sisäänkirjautuminen**.

   Windowsin sisäänkirjautuminen -ruutu näytetään.

HUOMAUTUS: Jos SpareKeytä käytetään sisäänkirjautumiseen aseman salauksen sisäänkirjautumisen ruudulla, lisävaltuustietoja tarvitaan Windowsiin sisäänkirjautumiseen käyttäjän tileihin pääsyä varten. On erittäin suositeltavaa, että palautat salasanasi palautuksen suorittamisen jälkeen.

6 HP File Sanitizer (vain tietyt mallit)

File Sanitizerin ansiosta voit turvallisesti hävittää resursseja (esimerkiksi: henkilötiedot tai tiedostot, historialliset tai verkkoon liittyvää tiedot, tai muut tietokomponentit) tietokoneen sisäisellä kovalevyasemalla ja määräajoin tyhjentää tietokoneen sisäinen kovalevyasema.

File Sanitizeria ei voida käyttää puhdistamaan tai tyhjentämään seuraavan tyyppisiä asemia:

- Solid-state-asemat (SSD), mukaan lukien RAID-asemat, jotka koostuvat SSD-laitteesta
- Ulkoiset asemat, jotka on liitetty USB:llä, Firewirellä, tai eSATA-liitännällä

Jos hävitys- tai tyhjennystoimintoa yritetään SSD:ssä varoitusviesti näkyy ja toimintoa ei suoriteta.

Hävittäminen

Hävittäminen poikkeaa vakio-Windows®:in poista-toiminnosta. Kun hävität omaisuutta File Sanitizeria käyttämällä, tiedostot korvataan merkityksettömällä tiedolla tehden virtuaalisesti mahdottomaksi hakea alkuperäinen omaisuus. Windowsin yksinkertainen poista-toiminto voi jättää tiedoston (tai omaisuuden) vahingoittumattomana kovalevyasemalle tai tilaan, missä oikeudellisia menetelmiä voitaisiin käyttää sen palauttamiseksi.

Voit aikatauluttaa tulevan hävitysajan, tai voit manuaalisesti aktivoida hävittämisen valitsemalla **File Sanitizer** -kuvakkeen HP Client Security Home -näyttöruudulla tai käyttämällä **File Sanitizer** -kuvaketta Windows-työpöydällä. Katso lisätietoja kohdasta Hävittämisen aikataulun asettaminen sivulla 36, Hävittäminen kakkospainikkeen napsautuksella sivulla 38, tai Hävitystoiminnon manuaalinen käynnistäminen sivulla 38.

HUOMAUTUS: .dll-tiedosto on hävitetty ja poistettu järjestelmästä vain, jos se on siirretty Roskakoriin.

Vapaan tilan tyhjennys

Omaisuuden poistaminen Windowsissa ei kokonaan poista omaisuuden sisältöä kovalevyasemaltasi. Windows poistaa vain viitteen omaisuuteen, tai sen sijaintipaikkaan kovalevyasemalla. Omaisuuden sisältö pysyy yhä kovalevyasemalla kunnes toinen omaisuus korvaa saman alueen kovalevyasemalla uudella tiedolla.

Vapaan tilan tyhjentäminen antaa sinun kirjoittaa satunnaista tietoa poistettujen omaisuuksien päälle estäen käyttäjiä katsomasta poistetun omaisuuden alkuperäistä sisältöä.

HUOMAUTUS: Vapaan tilan tyhjentäminen ei tarjoa lisäturvallisuutta hävitetyille omaisuuksille.

Voit asettaa tulevan vapaan tilan tyhjentämisen ajan, tai voit manuaalisesti aktivoida aikaisemmin hävitettyjen omaisuuksien vapaan tilan tyhjentämisen valitsemalla **File Sanitizer** -kuvakkeen HP Client Security Home -näyttöruudulla tai käyttämällä **File Sanitizer** -kuvaketta Windowsin työpöydällä. Katso lisätietoja kohdasta Vapaan tilan tyhjennysaikataulun asettaminen sivulla 36, Vapaan tilan tyhjentämisen manuaalinen käynnistäminen sivulla 38, tai File Sanitizer -kuvakkeen käyttäminen sivulla 37.

File Sanitizerin avaaminen

1. Napsauta tai napauta Käynnistä-ruudulta **HP Client Security** -sovellusta (Windows 8).

   TAI

   Kaksoisnapsauta tai kaksoisnapauta Windowsin työpöydällä, tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella sijaitsevaa **HP Client Security** -kuvaketta.

2. Kohdassa **Tieto** napauta **File Sanitizer**.

TAI

▲ Kaksoisnapsauta tai kaksoisnapauta **File Sanitizer** -kuvaketta Windowsin työpöydällä.

TAI

▲ Napsauta hiiren kakkospainikkeella tai napauta ja pidä **File Sanitizer** -kuvaketta Windowsin työpöydällä, ja sen jälkeen valitse **Avaa File Sanitizer**.

Asetusohjeita

Hävittäminen—File Sanitizer poistaa turvallisesti tai hävittää omaisuuksien valitut luokat.

1. Valitse kohdassa **Hävittäminen** valintaruutu kullekin hävitettävälle tiedostotyypille, tai tyhjennä valintaruutu, jos et halua hävittää noita tiedostoja.

   - **Roskakori**—hävittää kaikki roskakorin sisällä olevat kohdat.
   - **Tilapäiset järjestelmätiedostot**—hävittää kaikki järjestelmän tilapäisestä kansiosta löydetyt tiedostot. Seuraavat ympäristömuuttujat haetaan seuraavassa järjestyksessä, ja ensimmäistä löydettyä polkua pidetään järjestelmäkansiona:
     - TMP
     - TEMP
   - **Tilapäiset internet-tiedostot**—hävittää Web-sivujen kopiot, kuvat, ja median, jotka Web-selaimet ovat tallentaneet nopeampaa katselua varten.
   - **Evästeet**—hävittää kaikki tiedostot, jotka Web-sivustot ovat tallentaneet tietokoneeseen asetusten tallentamiseksi, kuten sisäänkirjautumisen tiedot.

2. Käynnistä hävittäminen napsauttamalla tai napauttamalla **Hävitä**.

Tyhjennys—kirjoittaa satunnaista tietoa vapaaseen tilaan ja estää poistettujen kohtien palautuksen.

▲ Käynnistä tyhjentäminen napsauttamalla tai napauttamalla **Tyhjennä**.

File Sanitizer -valinnat—valitse valintaruutu ottaaksesi käyttöön kunkin seuraavista valinnoista tai tyhjennä valintaruutu poistaaksesi valinnan käytöstä:

- **Ota työpöytä käyttöön -kuvake**—näyttää File Sanitizer -kuvakkeen Windowsin työpöydällä.
- **Ota käyttöön napsautus kakkospainikkeella**—antaa sinun napsauttaa kakkospainikkeella tai napauttaa ja pitää omaisuutta, ja sen jälkeen valitse **HP File Sanitizer – Hävitä**.
- **Kysy Windows-salasana ennen manuaalista hävittämistä**—tarvitsee todennuksen Windows-salasanalla ennen kohteen manuaalista hävittämistä.
- **Hävitä evästeet ja tilapäiset internet-tiedostot selaimella sulje**—hävittää kaikki valitut Webiin liittyvät omaisuudet, kuten selaimen URL-historia, kun suljet Web-selaimen.

Hävittämisen aikataulun asettaminen

Voit aikatauluttaa ajan hävittämisen suorittamisen automaattisesti, tai voit myös hävittää omaisuuksia manuaalisesti mihin aikaan tahansa. Lisätietoja on kohdassa Asetusohjeita sivulla 35.

1. Avaa File Sanitizer, ja sen jälkeen napsauta tai napauta **Asetukset**.
2. Aikatauluttaaksesi tulevan ajan valittujen omaisuuksien hävittämiseen, kohdassa **Hävitysaikataulu**, valitse **Ei milloinkaan**, **Kerran**, **Päivittäin**, **Viikoittain**, tai **Kuukausittain**, ja sen jälkeen valitse päivä ja aika:
   a. Napsauta tai napauta tunti, minuutti, tai AP/IP-kenttää.
   b. Vieritä kunnes haluttu arvo näytetään samalla tasolla kuin muut kentät.
   c. Napsauta tai napauta valkoista tilaa, joka ympäröi ajan asetuksen kenttiä.
   d. Toista kullekin kentälle kunnes oikea aikataulu on valittu.
3. Omaisuuksien seuraavat neljä tyyppiä luetellaan:
   - **Roskakori**—hävittää kaikki roskakorin sisällä olevat kohdat.
   - **Tilapäiset järjestelmätiedostot**—hävittää kaikki järjestelmän tilapäisestä kansiosta löydetyt tiedostot. Seuraavat ympäristömuuttujat haetaan seuraavassa järjestyksessä, ja ensimmäistä löydettyä polkua pidetään järjestelmäkansiona:
     - TMP
     - TEMP
   - **Tilapäiset internet-tiedostot**—hävittää Web-sivujen kopiot, kuvat, ja median, jotka Web-selaimet ovat tallentaneet nopeampaa katselua varten.
   - **Evästeet**—hävittää kaikki tiedostot, jotka Web-sivustot ovat tallentaneet tietokoneeseen asetusten tallentamiseksi, kuten sisäänkirjautumisen tiedot.

   Jos valittu, nämä omaisuudet hävitetään aikataulutetussa ajassa.
4. Lisämukautusomaisuuksien valitseminen hävitettäväksi:
   a. Kohdassa **Aikataulutettu hävitysluettelo** napsauta tai napauta **Lisää kansio**, ja sen jälkeen siirry tiedostoon tai kansioon.
   b. Napsauta tai napauta **Avaa**, ja sen jälkeen napsauta tai napauta **OK**.

   Poistaaksesi omaisuuden aikataulutetusta hävitysluettelosta tyhjennä omaisuuden valintaruutu.

Vapaan tilan tyhjennysaikataulun asettaminen

Vapaan tilan tyhjentäminen ei tarjoa lisäturvallisuutta hävitetyille omaisuuksille.

1. Avaa File Sanitizer, ja sen jälkeen napsauta tai napauta **Asetukset**.
2. Aikatauluttaaksesi tulevan ajan kovalevyasemasi hävittämiseen, kohdassa **Tyhjentämisen aikataulu**, valitse **Ei milloinkaan**, **Kerran**, **Päivittäin**, **Viikoittain**, tai **Kuukausittain**, ja sen jälkeen valitse päivä ja aika.
   a. Napsauta tai napauta tunti, minuutti, tai AP/IP-kenttää.
   b. Vieritä kunnes haluttu aika näytetään samalla tasolla kuin muut kentät.
   c. Napsauta tai napauta valkoista tilaa, joka ympäröi ajan asetuksen kenttiä.
   d. Toista kunnes oikea aikataulu on valittu.

HUOMAUTUS: Vapaan tilan tyhjennystoiminto voi ottaa huomattavan pitkän ajan. Varmista, että tietokoneesi on liitetty AC-virtaan. Vaikka vapaan tilan tyhjennys suoritetaan taustalla, lisääntynyt prosessorin käyttö voi vaikuttaa tietokoneesi suorituskykyyn. Vapaan tilan tyhjennys voidaan suorittaa tuntien kuluttua tai kun tietokone ei ole käytössä.

Tiedostojen suojaaminen hävittämiseltä

Tiedostojen tai kansioiden suojaaminen hävittämiseltä:

1. Avaa File Sanitizer, ja sen jälkeen napsauta tai napauta **Asetukset**.
2. Kohdassa **Älä milloinkaan hävitä luetteloa**, napsauta tai napauta **Lisää kansio**, ja sen jälkeen siirry tiedostoon tai kansioon.
3. Napsauta tai napauta **Avaa**, ja sen jälkeen napsauta tai napauta **OK**.

HUOMAUTUS: Tässä luettelossa olevat tiedostot ovat suojattuja niin kauan kuin ne pysyvät luettelossa.

Poistaaksesi omaisuuden poistamiset-luettelosta tyhjennä omaisuuden valintaruutu.

Yleiset tehtävät

Käytä File Sanitizeria seuraavien tehtävien suorittamiseen:

- **Käytä File Sanitizer -kuvaketta hävittämisen aloittamiseen**—Vedä tiedostot **File Sanitizer** -kuvakkeeseen Windowsin työpöydällä. Katso yksityiskohtia kohdasta File Sanitizer -kuvakkeen käyttäminen sivulla 37.
- **Hävitä manuaalisesti tietty omaisuus tai kaikki valitut omaisuudet**—Hävitä kohdat milloin tahansa odottamatta aikataulutettua hävitysaikaa. Katso yksityiskohtia kohdasta Hävittäminen kakkospainikkeen napsautuksella sivulla 38 tai Hävitystoiminnon manuaalinen käynnistäminen sivulla 38.
- **Aktivoi manuaalisesti vapaan tilan tyhjentäminen**—Aktivoi vapaan tilan tyhjentäminen mihin aikaan tahansa. Katso yksityiskohtia kohdasta Vapaan tilan tyhjentämisen manuaalinen käynnistäminen sivulla 38.
- **Näytä lokitiedostot**—Näytä hävityksen ja vapaan tilan tyhjentämisen lokitiedostot, jotka sisältävät mitkä tahansa virheet tai viat viimeksi hävitetyn tai vapaan tilan tyhjennystoiminnosta. Katso yksityiskohtia kohdasta Lokitiedostojen näyttäminen sivulla 40.

HUOMAUTUS: Hävitys tai vapaan tilan tyhjennystoiminto voi ottaa huomattavan pitkän ajan. Vaikka hävittäminen ja vapaan tilan tyhjennys suoritetaan taustalla, lisääntynyt prosessorin käyttö voi vaikuttaa tietokoneesi suorituskykyyn.

File Sanitizer -kuvakkeen käyttäminen

VAROITUS: Hävitettyä omaisuutta ei voi palauttaa. Harkitse huolellisesti mitkä kohdat valitset manuaaliseen hävittämiseen.

Kun käynnistät hävitystoiminnon manuaalisesti, vakiohävitysluettelo File Sanitizer -näkymässä hävitetään (katso Asetusohjeita sivulla 35).

Voit käynnistää hävitystoiminnon manuaalisesti yhdellä seuraavista tavoista:

1. Avaa File Sanitizer (katso File Sanitizerin avaaminen sivulla 35), ja sen jälkeen napsauta tai napauta **Hävitä**.
2. Kun vahvistuksen valintaruutu avautuu, varmista, että omaisuudet, jotka haluat hävittää on valittu, ja sen jälkeen napsauta tai napauta **OK**.

TAI

1. Napsauta tai napauta hiiren kakkospainikkeella ja pidä **File Sanitizer** -kuvaketta Windowsin työpöydällä, ja sen jälkeen napsauta tai napauta **Hävitä nyt**.
2. Kun vahvistuksen valintaruutu avautuu, varmista, että omaisuudet, jotka haluat hävittää on valittu, ja sen jälkeen napsauta tai napauta **Hävitä**.

Hävittäminen kakkospainikkeen napsautuksella

⚠ **VAROITUS:** Hävitettyä omaisuutta ei voi palauttaa. Harkitse huolellisesti mitkä kohdat valitset manuaaliseen hävittämiseen.

Jos **Ota käyttöön hävittäminen kakkospainikkeen napsautuksella** on valittu File Sanitizer -näkymässä, voit hävittää omaisuuden seuraavasti:

1. Siirry asiakirjaan tai kansioon, jonka haluat hävittää.
2. Napsauta tai napauta hiiren kakkospainikkeella ja pidä tiedostoa tai kansiota, ja sen jälkeen valitse **HP File Sanitizer – Hävitä**.

Hävitystoiminnon manuaalinen käynnistäminen

⚠ **VAROITUS:** Hävitettyä omaisuutta ei voi palauttaa. Harkitse huolellisesti mitkä kohdat valitset manuaaliseen hävittämiseen.

Kun käynnistät hävitystoiminnon manuaalisesti, vakiohävitysluettelo File Sanitizer -näkymässä hävitetään (katso Asetusohjeita sivulla 35).

Voit käynnistää hävitystoiminnon manuaalisesti yhdellä seuraavista tavoista:

1. Avaa File Sanitizer (katso File Sanitizerin avaaminen sivulla 35), ja sen jälkeen napsauta tai napauta **Hävitä**.
2. Kun vahvistuksen valintaruutu avautuu, varmista, että omaisuudet, jotka haluat hävittää on valittu, ja sen jälkeen napsauta tai napauta **OK**.

TAI

1. Napsauta tai napauta hiiren kakkospainikkeella ja pidä **File Sanitizer** -kuvaketta Windowsin työpöydällä, ja sen jälkeen napsauta tai napauta **Hävitä nyt**.
2. Kun vahvistuksen valintaruutu avautuu, varmista, että omaisuudet, jotka haluat hävittää on valittu, ja sen jälkeen napsauta tai napauta **Hävitä**.

Vapaan tilan tyhjentämisen manuaalinen käynnistäminen

Kun käynnistät tyhjennystoiminnon manuaalisesti, vakiohävitysluettelo File Sanitizer -näkymässä tyhjennetään (katso Asetusohjeita sivulla 35).

Voit käynnistää tyhjennystoiminnon manuaalisesti yhdellä seuraavista tavoista:

1. Avaa File Sanitizer (katso File Sanitizerin avaaminen sivulla 35), ja sen jälkeen napsauta tai napauta **Tyhjennä**.
2. Kun vahvistuksen valintaruutu avautuu, napsauta tai napauta **OK**.

TAI

1. Napsauta tai napauta hiiren kakkospainikkeella ja pidä **File Sanitizer** -kuvaketta Windowsin työpöydällä, ja sen jälkeen napsauta tai napauta **Tyhjennä nyt**.
2. Kun vahvistuksen valintaruutu avautuu, napsauta tai napauta **Tyhjennä**.

Lokitiedostojen näyttäminen

Joka kerta kun hävitys- tai vapaan tilan tyhjennystoiminto suoritetaan, minkä tahansa virheiden tai vikojen lokitiedostot luodaan. Lokitiedostot päivitetään aina viimeisimmän hävitys- tai vapaan tilan tyhjennystoiminnon mukaan.

HUOMAUTUS: Tiedostot, jotka hävitettiin tai tyhjennettiin onnistuneesti, eivät näy lokitiedostoissa.

Yksi lokitiedosto luodaan hävitystoiminnoille, ja toinen lokitiedosto luodaan vapaan tilan tyhjennystoiminnoille. Molemmat lokitiedostot sijaitsevat kovalevyasemalla seuraavissa kansioissa:

- C:\Program Files\Hewlett-Packard\File Sanitizer*[Username]*_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer*[Username]*_DiskBleachLog.txt

64-bittisille järjestelmille lokitiedostot sijaitsevat kovalevyasemalla seuraavissa kansioissa:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Username]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Username]*_DiskBleachLog.txt

7 HP Device Access Manager (vain tietyt mallit)

HP Device Access Manager ohjaa pääsyä tietoon poistamalla käytöstä tiedonsiirtolaitteita.

HUOMAUTUS: Jotkut käyttöliittymä-/syöttölaitteet, kuten hiiri, näppäimistö, TouchPad ja sormenjälkilukija eivät ole Device Access Manager -ohjelmiston ohjaamia. Lisätietoja on kohdassa Hallitsemattomat laiteluokat sivulla 44.

Windows®-käyttöjärjestelmän järjestelmänvalvojat käyttävät HP Device Access Manageria valvomaan järjestelmän laitteita ja estämään luvattoman käytön:

- Laiteprofiilit luodaan kullekin käyttäjälle määrittämään laitteet, joihin heille on sallittu pääsy tai kielletty lupa päästä.
- Just In Time Authentication (JITA) sallii esimääritettyjen käyttäjien todentaa itsensä päästäkseen laitteille, jotka joille on tavallisesti pääsy kielletty.
- Järjestelmänvalvojat ja luotetut käyttäjät voidaan jättää Device Access Managerin määrittämän laitteen käyttörajoitusten ulkopuolelle lisäämällä heidät Laitteen järjestelmänvalvojien ryhmään. Tämän ryhmän jäsenyyksiä hallitaan lisäasetuksista.
- Laitteeseen pääsy voidaan myöntää tai kieltää ryhmän käyttäjien perusteella tai yksittäisille käyttäjille.
- Joitakin laiteluokkia, kuten CD-ROM ja DVD, voidaan lisäksi ohjata sallimalla tai kieltämällä pääsyn erikseen luku- ja kirjoitustoimintoihin.

HP Device Access Manager määritetään automaattisesti seuraavilla asetuksilla HP Client Securityn ohjatun asennuksen suorituksen aikana:

- Just In Time Authentication (JITA) siirrettävä media otetaan käyttöön järjestelmänvalvojia ja käyttäjiä varten.
- Laitteen käytäntö sallii täyden pääsyn muille laitteille.

Device Access Manager -sovelluksen avaaminen

1. Napsauta tai napauta Käynnistä-ruudulta **HP Client Security** -sovellusta (Windows 8).

   TAI

   Kaksoisnapsauta tai kaksoisnapauta Windowsin työpöydällä, tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella sijaitsevaa **HP Client Security** -kuvaketta.

2. Kohdassa **Laite** napsauta tai napauta **Laitteen luvat**.

   - Vakiokäyttäjät voivat katsoa heidän nykyisen laitteen käytön (katso Käyttäjän näkymä sivulla 42).
   - Järjestelmänvalvojat voivat näyttää ja tehdä muutoksia käyttöön laitteelle, jota parhaillaan määritetään tietokoneeseen napsauttamalla tai napauttamalla **Muuta**, ja sen jälkeen antamalla järjestelmänvalvojan salasanan (katso Järjestelmän näkymä sivulla 42).

Käyttäjän näkymä

Kun **Laitteen luvat** on valittu, käyttäjän näkymä näytetään. Käytännöstä riippuen vakiokäyttäjät ja järjestelmänvalvojat voivat näyttää heidän oman pääsynsä laiteluokille tai yksittäisille laitteille tässä tietokoneessa.

- **Nykyinen käyttäjä**—Näytetään käyttäjän nimi, joka parhaillaan on kirjautuneena sisään.
- **Laiteluokka**—Laitteiden tyypit näytetään.
- **Pääsy**—Näytetään parhaillaan määritettynä oleva pääsy laitteiden tyyppeihin tai tiettyihin laitteisiin.
- **Kesto**—Näytetään aikaraja pääsyysi CD/DVD-ROM-asemille tai siirrettäville levyasemille.
- **Asetukset** —Järjestelmänvalvojat voivat muuttaa millä asemilla on Device Access Manager -ohjelmiston ohjaama pääsy.

Järjestelmän näkymä

Järjestelmän näkymässä järjestelmänvalvojat voivat sallia tai kieltää pääsyn laitteille tässä tietokoneessa käyttäjien ryhmälle tai järjestelmänvalvojien ryhmälle.

▲ Järjestelmänvalvojat voivat päästä järjestelmänäkymään napsauttamalla tai napauttamalla **Muuta**, antamalla järjestelmänvalvojan salasanan, ja sen jälkeen valitsemalla seuraavista valinnoista:

- **Device Access Manager**—Kääntääksesi HP Device Access Manager -ohjelmiston Just In Time Authentication -toiminnolla päälle tai pois, napsauta tai napauta **Päälle** tai **Pois**.
- **Käyttäjät ja ryhmät tässä PC:ssä**—Näyttää käyttäjien ryhmän tai järjestelmänvalvojien ryhmän, jotka ovat sallittuja tai kiellettyjä pääsemään valittuihin laiteluokkiin.
- **Laiteluokka**—Näyttää laiteluokat ja laitteet, jotka on asennettu järjestelmään, tai jotka voivat olla asennettuja järjestelmään aikaisemmin. Laajenna luetteloa napsauttamalla **+** -kuvaketta. Kaikki tietokoneeseen liitetyt laitteet näytetään, ja järjestelmänvalvojien sekä käyttäjien ryhmää laajennetaan näyttämään niiden jäsenyys. Päivitä laitteiden luettelo napsauttamalla pyöreää nuoli (päivitä) -kuvaketta.
  - Suojausta käytetään tavallisesti laiteluokalle. Jos pääsy on asetettu tilaan **Salli**, valittu käyttäjä tai ryhmä kykenee pääsemään mille tahansa laitteelle laiteluokassa.
  - Suojausta voidaan käyttää myös tietyille laitteille.
  - Määritä Just In Time authentication (JITA), sallien valittujen käyttäjien päästä DVD/CD-ROM -asemille tai siirrettäville levyasemille todentamalla itsensä. Lisätietoja on kohdassa JITA-määritys sivulla 43.
  - Salli tai kiellä pääsy muihin laiteluokkiin, kuten siirrettävä media (kuten USB flash -asemat), sarja- ja rinnakkaisportit, Bluetooth®-laitteet, modeemilaitteet, PCMCIA/ExpressCard -laitteet, 1394-laitteet, sormenjäljen lukija, ja älykortin lukija. Jos sormenjäljen lukija ja älykortin lukija ovat kiellettyjä, niitä voidaan käyttää todennuksen valtuustietoina, mutta niitä ei voi käyttää istunnon käytännön tasolla.

    HUOMAUTUS: Jos Bluetooth-laitteita käytetään todennuksen valtuustietoina, Bluetooth-laitteen pääsy ei tulisi olla rajoitettu Device Access Manager -ohjelmistön käytännössä.
  - Kun valitset asetuksen ryhmä- tai laiteluokka-tasolla, ja sinulta kysytään käytetäänkö asetusta lasten kohteisiin:

    Kyllä—Asetus mainostaa.

Ei—Asetus ei mainosta.

- Joitakin laiteluokkia, kuten DVD ja CD-ROM, voidaan lisäksi ohjata sallimalla tai kieltämällä pääsyn erikseen luku- ja kirjoitustoimintoihin.

HUOMAUTUS: Järjestelmänvalvojat-ryhmää ei voida lisätä Käyttäjäluetteloon.

- **Pääsy**—Napsauta tai napauta alas-nuolta, ja sen jälkeen valitse yksi seuraavasta pääsytyypistä sallimaan tai kieltämään pääsyn:
  - **Salli – Täysi pääsy**
  - **Salli – Vain luku**
  - **Salli – JITA vaaditaan**—Katso lisätietoja kohdasta JITA-määritys sivulla 43.

    Jos tämä pääsytyyppi valitaan, napsauta tai napauta kohdassa **Kesto** alas-nuolta valitaksesi aikarajan.
  - **Kiellä**
- **Kesto**—Napsauta tai napauta alas-nuolta valitaksesi aikarajan pääsyyn CD/DVD-ROM-asemille tai siirrettäville levyasemille (katso JITA-määritys sivulla 43).

JITA-määritys

JITA-määritys sallii järjestelmänvalvojan näyttää ja muuttaa käyttäjien ja ryhmien luetteloa, joille on sallittua päästä laitteisiin käyttäen Just In Time Authentication (JITA) -toimintoa.

JITA-mahdollistetut käyttäjät kykenevät pääsemään joihinkin laitteisiin, joille käytännöt luotiin **Laiteluokan määritys** -näkymässä on rajoitettu.

JITA-ajanjakso voidaan valtuuttaa minuuttien määräksi tai Rajattomaksi. Rajattomilla käyttäjillä on pääsy laitteeseen heidän todentamisajasta lähtien siihen saakka kunnes he kirjautuvat ulos järjestelmästä.

Jos käyttäjälle annetaan rajoitettu JITA-ajanjakso, yksi minuutti ennen JITA-ajanjakson umpeutumista käyttäjältä kysytään pidennetäänkö pääsyä. Heti kun käyttäjä kirjautuu ulos järjestelmästä tai toinen kirjautuu sisään, JITA-ajanjakso umpeutuu. Seuraavalla kertaa kun käyttäjä kirjautuu sisään ja yrittää päästä JITA-mahdollistetulle laitteelle, kehote antaa valtuustiedot näytetään.

JITA on käytettävissä seuraaviin laiteluokkiin:

- DVD/CD-ROM-asemat
- Siirrettävät levyasemat

JITA-käytännön luominen käyttäjälle tai ryhmälle

Järjestelmänvalvojat voivat sallia käyttäjien tai ryhmien päästä laitteisiin käyttämällä Just In Time Authentication (JITA) -toimintoa.

1. Käynnistä **Device Access Manager**, ja sen jälkeen napsauta tai napauta **Muuta**.
2. Valitse käyttäjä tai ryhmä, ja sitten kohdassa **Pääsy** joko **Siirrettävät levyasemat** tai **DVD/CD-ROM-asemat** napsauta tai napauta alas-nuolta, ja sen jälkeen valitse **Salli – JITA vaaditaan**.
3. Napsauta tai napauta alas-nuolta kohdassa **Kesto** valitaksesi ajanjakson JITA-pääsyä varten.

Käyttäjän täytyy kirjautua ulos ja sitten kirjautua uudelleen sisään uuden JITA-asetuksen käyttämiseksi.

JITA-käytännön poistaminen käytöstä käyttäjää tai ryhmää varten

Järjestelmänvalvojat voivat poistaa käytöstä käyttäjän tai ryhmän pääsyn laitteisiin käyttämällä Just In Time Authentication -toimintoa.

1. Käynnistä **Device Access Manager**, ja sen jälkeen napsauta tai napauta **Muuta**.
2. Valitse käyttäjä tai ryhmä, ja sitten kohdassa **Pääsy** joko **Siirrettävät levyasemat** tai **DVD/CD-ROM -asemat** napsauta tai napauta alas-nuolta, ja sen jälkeen valitse **Kiellä**.

Kun käyttäjä kirjautuu sisään ja yrittää päästä laitteeseen, pääsy kielletään.

Asetukset

Asetukset-näkymä sallii järjestelmänvalvojien näyttää ja muuttaa asemia, joilla on Device Access Manager -ohjelmistön ohjaama pääsy.

HUOMAUTUS: Device Access Manager -ohjelmiston täytyy olla otettuna käyttöön, kun asemakirjainten luettelo määritetään (katso Järjestelmän näkymä sivulla 42).

Hallitsemattomat laiteluokat

HP Device Access Manager ei hallitse seuraavia laiteluokkia:

- Tulo-/lähtölaitteet
  - CD-ROM
  - Levyasema
  - Floppy-levyohjain (FDC)
  - Kovalevyohjain (HDC)
  - Ihmisen liitäntälaite (HID) -luokka
  - Infrapunalla toimivat ihmisen liitäntälaitteet
  - hiiren.
  - Moniporti sarjamuotoinen
  - näppäimistö
  - Plug and play (PnP) -tulostimet
  - Tulostin
  - Tulostimen päivitys
- virta
  - Kehittynyt virranhallinta (APM) -tuki
  - Akku
- Sekalaista
  - Tietokone
  - Tallennin
  - Näyttö

- Intel® yhdistynyt näytönohjain
- Legacard
- Mediaohjain
- Keskitason vaihtaja
- Muistiteknologia
- Näyttö
- Monitoiminto
- Verkkoasiakas
- Verkkopalvelu
- Verkkokäännetty
- Suoritin
- SCSI-sovitin
- Turvakiihdytin
- Turvalaitteet
- Järjestelmä
- Tuntematon
- Asema
- Aseman tilannevedos

8 HP Trust Circles

HP Trust Circles on tiedosto- ja asiakirjaturvallisuuden sovellus, joka yhdistää kansion tiedostosalauksen mukavan trusted-circle asiakirja-jakamisen kyvyn kanssa. Sovellus salaa tiedostoja, jotka on laitettu käyttäjä-määriteltyihin kansioihin suojaten ne trust circlen sisällä. Suojattuina ollessaan tiedostoja voivat käyttää ja jakaa vain luottamuksen piirissä olevat jäsenet. Jos suojatun tiedoston vastaanottaa ei-jäsen, tiedosto pysyy salattuna, eikä ei-jäsen voi päästä sisältöihin.

Trust Circles -sovelluksen avaaminen

1. Napsauta tai napauta Käynnistä-ruudulla **HP Client Security** -sovellus.

   TAI

   Kaksoisnapsauta Windowsin työpöydältä **HP Client Security** -kuvaketta ilmoitusalueella, joka sijaitsee oikeanpuoleisimpana tehtäväpalkilla.

2. Kohdassa **Tieto**, napsauta tai napauta **Trust Circles**.

Aloitusopas

On kaksi keinoa lähettää sähköpostikutsuja ja vastata niihin:

- **Microsoft® Outlookin käyttäminen**—Trust Circlesin käyttäminen Microsoft Outlookin kanssa automatisoi mitkä tahansa Trust Circle -kutsujen ja vastausten käsittelyn muilta Trust Circle -käyttäjiltä.
- **Gmailin, Yahoon, Outlook.comin tai muiden sähköpostipalveluiden (SMTP) käyttäminen**—Kun annat nimesi, sähköpostiosoitteesi, ja salasanasi, Trust Circles käyttää sähköpostipalveluasi lähettämään sähköpostikutsuja jäsenille, jotka on valittu liittymään sinun trust circleen.

Perusprofiilisi asettaminen:

1. Anna nimesi ja sähköpostiosoitteesi, ja sen jälkeen napsauta tai napauta **Seuraava**.

   Nimi näkyy kaikille jäsenille, jotka on kutsuttu liittymään sinun trust circleen. Sähköpostiosoitetta käytetään lähettämään, vastaanottamaan, tai vastaamaan kutsuihin.

2. Anna salasana sähköpostitilille, ja sen jälkeen napsauta tai napauta **Seuraava**.

   Testisähköposti lähetetään varmistamaan, että sähköpostiasetukset ovat tarkkoja.

   HUOMAUTUS: Tietokoneen täytyy olla yhdistetty verkkoon.

3. Anna **Trust Circle Name** -kentässä nimi trust circlelle, ja sen jälkeen napsauta tai napauta **Seuraava**.

4. Lisää jäseniä ja kansioita, ja sen jälkeen napsauta tai napauta **Seuraava**. Trust circle luodaan minkä tahansa kansioiden kanssa, jotka oli valittu ja lähetetty sähköpostikutsuja kenelle tahansa valituille jäsenille. Jos mistä tahansa syystä kutsua ei voida lähettää, näytetään ilmoitus. Jäseniä voidaan kutsua uudelleen milloin tahansa Trust Circle -nakymästä napsauttamalla **Your Trust**

Circles, ja sen jälkeen kaksoisnapsauttamalla tai kaksoisnapauttamalla trust circleä. Lisätietoja on kohdassa Trust Circles sivulla 47.

Trust Circles

Voit luoda trust circlen aloitusasennuksen aikana annettuasi sähköpostiosoitteesi, tai Trust Circle -näkymässä:

▲ Napsauta tai napauta Trust Circle -näkymästä **Create Trust Circle**, ja sen jälkeen anna nimi trust circlelle.

- Lisätäksesi jäseniä trust circleen napsauta tai napauta **M+** -kuvaketta **Members** (Jäsenet) -valinnan vieressä, ja sen jälkeen seuraa näytöllä näkyviä ohjeita.
- Lisätäksesi kansioita trust circleen napsauta tai napauta **+** -kuvaketta **Folders** (Kansiot) -valinnan vieressä, ja sen jälkeen seuraa näytöllä näkyviä ohjeita.

Kansioiden lisääminen trust circleen

Kansioiden lisääminen uuteen trust circleen:

- Trust circlen luomisen aikana voit lisätä kansioita napsauttamalla tai napauttamalla **+** -kuvaketta **Folders** (Kansiot) -valinnan vieressä, ja sen jälkeen seuraa näytöllä näkyviä ohjeita.

  TAI

- Napsauta tai napauta hiiren kakkospainikkeella Windows Explorerissa ja pidä kansiota, joka parhaillaan ei ole trust circlen osa, valitse **Trust Circle**, ja sen jälkeen valitse **Luo Trust Circle kansiosta**.

VIHJE: Voit valita yhden tai useampia kansioita.

Kansioiden lisääminen olemassa olevaan Trust Circleen:

- Napsauta Trust Circle -näkymästä **Your Trust Circles**, kaksoisnapsauta tai kaksoisnapauta olemassa olevaa trust circleä näyttämään nykyiset kansiot, napsauta tai napauta **+** -kuvaketta **Folders** (Kansiot) -valinnan vieressä, ja sen jälkeen seuraa näytöllä näkyviä ohjeita.

  TAI

- Napsauta tai napauta hiiren kakkospainikkeella Windows Explorerissa ja pidä kansiota, joka parhaillaan ei ole trust circlen osa, valitse **Trust Circle**, ja sen jälkeen valitse **Lisää olemassa olevaan Trust Circleen kansiosta**.

VIHJE: Voit valita yhden tai useampia kansioita.

Heti kun kansio on lisätty trust circleen, Trust Circles salaa kansion ja sen sisällön automaattisesti. Heti kun kaikki tiedostot on salattu, näytetään ilmoitus. Lisäksi vihreä lukkosymboli näytetään kaikilla salatuilla kansiokuvakkeilla tiedostokuvakkeilla kansioiden sisällä osoittaen, että ne ovat täysin suojattuja.

Jäsenten lisääminen trust circleen

Tarvitaan kolme vaihetta lisätä jäseniä trust circleen:

1. **Kutsu**—Ensin trust circlen omistaja kutsuu jäseniä. Kutsusähköposti voidaan lähettää useille käyttäjille tai jakeluluetteloihin/ryhmiin.
2. **Hyväksy**—Kutsuttu vastaanottaa kutsun ja valitsee hyväksyykö vai hylkääkö. Jos kutsuttu hyväksyy kutsun, sähköpostivastaus lähetetään kutsujalle. Jos kutsu on lähetetty ryhmälle, kukin jäsen vastaanottaa kutsun ja valitsee hyväksyykö vai hylkääkö.
3. **Rekisteröi**—Kutsujalla on lopullinen mahdollisuus päättää lisätäkö jäsen trust circleen. Jos kutsuja päättää rekisteröidä jäsenen, sähköposti lähetetään kutsutulle todistaen vastauksen. Kutsuja ja kutsuttu voivat valinnaisesti varmistaa kutsuprosessin turvallisuuden. Vahvistuskoodi näytetään kutsutulle, joka täytyy lukea kutsujalle puhelimitse. Heti kun koodi on vahvistettu, kutsuja voi lähettää rekisteröitymissähköpostin.

Jäsenten lisääminen uuteen trust circleen:

▲ Trust circlen luomisen aikana voit lisätä jäseniä napsauttamalla tai napauttamalla **M+** -kuvaketta **Members** (Jäsenet) -valinnan vieressä, ja sen jälkeen seuraa näytöllä näkyviä ohjeita.

- Jos käytät Outlookia, valitse yhteystietoja Outlook-osoitteistosta, ja sen jälkeen napsauta **OK**
- Jos käytät muuta sähköpostipalvelua, joko lisää uusia osoitteita manuaalisesti Trust Circleen, tai voit saada ne haettua Trust Circleen rekisteröidystä sähköpostiosoitteesta.

Jäsenten lisääminen olemassa olevaan trust circleen:

▲ Napsauta Trust Circle -näkymästä **Your Trust Circles**, kaksoisnapsauta tai kaksoisnapauta olemassa olevaa trust circleä näyttämään nykyiset jäsenet, napsauta tai napauta **M+** -kuvaketta **Members** (Jäsenet) -valinnan vieressä, ja sen jälkeen seuraa näytöllä näkyviä ohjeita.

- Jos käytät Outlookia, valitse yhteystietoja Outlook-osoitteistosta, ja sen jälkeen napsauta **OK**.
- Jos käytät muuta sähköpostipalvelua, joko lisää uusia osoitteita manuaalisesti Trust Circleen, tai voit saada ne haettua Trust Circleen rekisteröidystä sähköpostiosoitteesta.

Tiedostojen lisääminen trust circleen

Voit lisätä tiedostoja trust circleen yhdellä seuraavista tavoista:

- Kopioi tai siirrä tiedosto olemassa olevaan trust circle -kansioon.

  TAI

- Napsauta tai napauta hiiren kakkospainikkeella Windows Explorerissa ja pidä tiedostoa, joka ei parhaillaan ole salattu, valitse **Trust Circle** ja valitse sitten **Salaa**. Näyttöön tulee kehotus valita trust circle, johon tiedosto tulisi lisätä.

VIHJE: Voit valita yhden tai useampia tiedostoja.

Salatut kansiot

Kuka tahansa trust circlen jäsen voi katsoa ja muokata tiedostoja, jotka kuuluvat tuohon trust circleen.

HUOMAUTUS: Trust Circle Manager/Reader ei synkronoi tiedostoja jäsenten välillä.

Tiedostot täytyy jakaa olemassa olevilla välineillä, kuten sähköposti, ftp, tai pilvitallennuspaikkatarjoajat. Tiedostot, jotka kopioitava, siirrettävä, tai luotuina trust circle -kansion sisällä suojataan välittömästi.

Kansioiden poistaminen trust circlestä

Kansion poistaminen trust circlestä purkaa kansion suojauksen ja kaikki sen sisällön sekä poistaen niiden suojauksen.

- Napsauta tai napauta Trust Circle -näkymästä **Your Trust Circles**, kaksoisnapsauta tai kaksoisnapauta olemassa olevaa trust circleä näyttämään nykyiset kansiot, ja sen jälkeen napsauta tai napauta **roska-astia** -kuvaketta tuon kansion vieressä.

  TAI

- Napsauta tai napauta hiiren kakkospainikkeella Windows Explorerissa ja pidä kansiota, joka parhaillaan on trust circlen osa, valitse **Trust Circle**, ja sen jälkeen valitse **Poista trust circlestä**.

VIHJE: Voit valita yhden tai useampia kansioita.

Tiedoston poistaminen trust circlestä

Poistaaksesi tiedoston trust circlestä Windows Explorerissa napsauta tai napauta hiiren kakkospainikkeella tiedostoa, joka parhaillaan on salattuna, valitse **Trust Circle** ja valitse sitten **Poista tiedoston salaus**.

Jäsenten poistaminen trust circlestä

Henkilöä, jota ei ole täysin rekisteröity, ei voi poistaa trust circlestä. Eräs vaihtoehto voisi olla luoda uusi trust circle kaikkien muiden jäsenten kanssa, siirtää kaikki tiedostot ja kansiot uuteen trust circleen, sekä sen jälkeen hävittää vanha trust circle. Tämä takaa, että mihinkään jäsenen vastaanottamaan tiedostoon ei ole pääsyä, mutta kaikki, jotka on aikaisemmin jaettu, säilyvät päästävissä olevina vanhan trust circlen jäsenille.

Jos jäsentä ei ole täysin salattu (joko jäsentä ei ole kutsuttu liittymään trust circleen, tai hän ei ole hyväksynyt kutsua trust circleen), voit poistaa jäsenen trust circlestä yhdellä seuraavista tavoista:

- Napsauta tai napauta Trust Circle -näkymästä **Your Trust Circles**, ja sen jälkeen kaksoisnapsauta tai kaksoisnapauta trust circleä näyttämään jäsenten nykyisen luettelon. Napsauta tai napauta **roska-astia**-kuvaketta poistettavan jäsenen nimen vieressä.
- Napsauta tai napauta Trust Circle -näkymästä **Members** (Jäsenet) -valintaa, ja sen jälkeen kaksoisnapsauta tai kaksoisnapauta jäsentä näyttämään trust circlet, missä he ovat jäseniä. Napsauta tai napauta **roska-astia**-kuvaketta trust circlen vieressä poistamaan jäsenen tuosta trust circlestä.

Trust circlen hävittäminen

Trust circlen hävittämiseksi tarvitaan omistajuus.

▲ Napsauta tai napauta Trust Circle -näkymästä **Your Trust Circles**, napsauta tai napauta **roska-astia**-kuvaketta hävitettävän trust circlen vieressä.

Tämä poistaa trust circlen sivulta ja lähettää sähköposteja kaikille trust circlen jäsenille tiedottaen heille, että trust circle on hävitetty. Kaikista tiedostoista tai kansioista, jotka sisältyivät tuohon trust circleen, poistetaan salaus.

Asetusten määrittäminen

Napsauta tai napauta Trust Circle -näkymästä **Määritykset**. Näytetään kolme välilehteä

- **Sähköpostin asetukset**

Asetus	Kuvaus
Käyttäjänimi	Parhaillaan käytössä oleva käyttäjänimi näytetään. Muuta se antamalla uuden käyttäjänimen tekstiruudussa. Muutokset tallennetaan automaattisesti.
Sähköpostiosoite	Parhaillaan käytetty sähköpostitili näytetään. Muuta se napsauttamalla tai napauttamalla **Muuta Sähköpostin asetuksia**, ja sen jälkeen seuraa näytöllä näkyviä ohjeita.
Uuden jäsenen vahvistus	Valitse seuraavista valinnoista: ◦ **Vahvista automaattisesti**—Vahvista vastaanoton hyväksyntä kutsutu(i)lta, ne vahvistetaan trust circleen ilman manuaalista syöttöä, ja vahvistussähköposti lähetetään kutsutu(i)lle. ◦ **Vahvista manuaalisesti**—Vastaanotettuasi hyväksynnän kutsutu(i)lta manuaalinen syöttö tarvitaan uusien jäsenten rekisteröimiseksi trust circleen, ja sen jälkeen vahvistussähköposti lähetetään kutsutu(i)lle. ◦ **Pyydä varmistus**—Vastaanotettuasi hyväksynnän kutsutu(i)lta varmistuskoodi tarvitaan kutsuttujen täyteen rekisteröintiin. Trust circlen omistajan täytyy ottaa yhteyden kutsuttuihin ja hankkia heiltä vahvistuskoodi. Annettuasi oikean koodin lähetetään vahvistussähköpostit.
Ajoittainen todennus	Ajoittainen todennus vaatii käyttäjää antamaan Windows-salasanan määritetyn aikakatkaisun (tallennettu minuuteissa) jälkeen ja myös suoritettaessa sensitiivisiä toimintoja. Tämä asetus sallii käyttäjille todennuksen päälle tai pois kääntämisen.
Todennuksen aikakatkaisu	Valitse määritetty aikakatkaisu (tallennettu minuuteissa) ennen todennuksen vaatimista.
Älä näytä vahvistusviestiä	Valitse valintaruutu poistaaksesi vahvistusviestien näyttämisen, tai tyhjennä valintaruutu vahvistusviestien näyttämiseksi.
Haluaisin auttaa parantamaan HP Trust Circleä anonyymillä käyttöjäljityksellä	Valitse valintaruutu osallistuaksesi ohjelmaan, tai tyhjennä valintaruutu, jos et halua osallistua.

- **Varmuuskopiointi/palautus**

Asetus	Kuvaus
Varmuuskopiointi	Kopioi Trust Circle Manager/Reader sovellustietosi (asetukset ja trust circlet) varmuuskopiointitiedostoon. Romahduksen tai järjestelmävian tapauksessa voit käyttää tätä tiedostoa palauttamaan uuden Trust Circles -sovelluksen asennuksen tallennettuun tilaan tiedostossa. **HUOMAUTUS:** Vain Trust Circle -sovelluksen tietosi tallennetaan (trust circlet, asetukset, ja jäsenet). Ajankohtaisia tiedostoja trust circle -kansioissa ei ole tallennuskopioitu. Noiden tiedostojen tulisi olla erillisesti tallennuskopioituja. Trust Circle -asetusten ja käyttäjän tiedon tallennuskopioiminen: **1.** Napsauta tai napauta **Varmuuskopiointi**. **2.** Valitse tiedostonimi ja hakemisto tallennuskopiointitiedostolle, ja sen jälkeen napsauta tai napauta **Tallenna**. **3.** Anna salasana, vahvista se, ja sen jälkeen napsauta tai napauta **OK**. Tämä salasana tarvitaan tämän tiedoston palauttamiseen.
Palauttaminen	Palauttaa asetukset ja trust circlet tallennuskopiointitiedostosta, tavallisesti järjestelmän romahduksen tai muuttoon toiseen tietokoneeseen. Trust Circle Managerin asetusten ja käyttäjän tietojen palauttaminen: **1.** Napsauta tai napauta **Palautus**. **2.** Siirry tallennuskopiointitiedoston hakemistoon ja tiedostonimeen, ja sen jälkeen napsauta tai napauta **Avaa**. **3.** Anna salasana, joka asetettiin tallennuskopiointia tehtäessä.

- **Tietoja**—Trust Circle Manager/Reader -ohjelmiston versio näytetään. Linkkejä näytetään sallimaan sinun päivittää Trust Circle Manager Pro-versioon tai näyttämään HP privacy statementin.

9 Varkauden selvittäminen (vain tietyissä malleissa)

Computracen (hankittava erikseen) avulla voit valvoa, hallita ja seurata tietokonetta etäkäytöllä.

Kun tämä on aktivoitu, Computrace määritetään Absolute-ohjelmiston asiakaspalvelukeskuksesta. Järjestelmänvalvoja voi määrittää asiakaspalvelukeskuksesta Computracen valvomaan ja ylläpitämään tietokonetta. Jos järjestelmä katoaa tai se varastetaan, asiakaspalvelukeskus voi auttaa löytämään ja palauttamaan tietokoneen. Jos Computrace on määritetty, se voi toimia silloinkin, kun kiintolevy tyhjennetään tai vaihdetaan.

Computracen aktivointi:

1. Internet-yhteyden muodostaminen.
2. Avaa HP Client Security. Lisätietoja on kohdassa HP Client Securityn avaaminen sivulla 9.
3. Napsauta **varkauden selvittäminen**.
4. Voit käynnistää Computracen aktivoinnin ohjatun toiminnon napsauttamalla **aloittaminen**.
5. Anna yhteystietosi ja luottokorttimaksutietosi tai anna ennalta ostettu tuotetunnus.

Aktivoinnin ohjattu toiminto käsittelee tapahtumat suojatusti ja määrittää käyttäjätilisi Absolute Software Customer Center -sivustossa. Kun tämä on tehty, saat vahvistusviestin, jossa on Customer Center -tilitietosi.

Jos olet aikaisemmin suorittanut ohjatun Computracen aktivoinnin ja Customer Center -käyttäjätili on jo olemassa, voit hankkia lisää lisenssejä ottamalla yhteyttä HP-asiakasedustaan.

Kirjautuminen Customer Centeriin:

1. Siirry osoitteeseen https://cc.absolute.com/.
2. Anna **kirjautumistunnus**- ja **salasana**-kentissä tunnistetiedot, jotka vastaanotit vahvistussähköpostissa, ja napsauta sitten **Kirjaudu sisään**.

Customer Centerin avulla voit:

- Valvoa tietokoneitasi.
- Suojaa etätietosi.
- Ilmoita Computracen suojaamien tietokoneiden varkaudet.

▲ Napsauta **Lisätietoja** saadaksesi lisätietoja Computracesta.

10 Lokalisoidut salasanapoikkeukset

Power-on todennustasolla ja HP Drive Encryption -tasolla salasanapoikkeusten tuki on rajoitettu. Lisätietoja on kohdassa Windows-IMEja ei tueta Power-on-todennustasolla tai Drive Encryption -tasolla sivulla 53.

Mitä tehdä, kun salasana hylätään

Salasanoja voidaan hylätä seuraavista syistä:

- Käyttäjä käyttää IMEä, jota ei tueta. Tämä on yleinen seikka kaksoistavukielissä (korea, japani, kiina). Tämän seikan ratkaiseminen:

  1. Käyttämällä **Ohjauspaneelia**, lisää tuettu näppäimistön layout (lisää US/English-näppäimistöt kiinan syöttökielen alle).
  2. Aseta tuettu näppäimistö oletussyötöksi.
  3. Käynnistä HP Client Security, ja sen jälkeen anna Windows-salasana.

- Käyttäjä käyttää merkkiä, jota ei tueta. Tämän seikan ratkaiseminen:

  1. Muuta Windows-salasanaa niin, että se käyttää vain tuettuja merkkejä. Katso lisätietoja tuettomista merkeistä kohdasta Erikoisnäppäimen käsittely sivulla 54.
  2. Käynnistä HP Client Security, ja sen jälkeen anna Windows-salasana.

Windows-IMEja ei tueta Power-on-todennustasolla tai Drive Encryption -tasolla

Windowsissa käyttäjä ei voi valita IMEä (tulomenetelmän editori) antaakseen monimutkaisia merkkejä ja symboleita, kuten japanilaiset tai kiinalaiset merkit käyttämällä länsimaista vakionäppäimistöä.

IMEja ei tueta Power-on-todennustasolla tai Drive Encryption -tasolla. Windows-salasanaa ei voida antaa IMEllä Power-on-todennuksessa tai HP Drive Encryption -kirjautumisnäytössä, ja niin tekeminen voi johtaa sulkemistilanteeseen. Joissakin tapauksissa Microsoft® Windows ei näytä IME:tä kun käyttäjä syöttää salasanan.

Ratkaisu on vaihtaa yhteen seuraavista tuetuista näppäimistö-layouteista, joka kääntää näppäimistö-layoutiin 00000411:

- Microsoft IME ja japania varten
- Japanilaisen näppäimistön layout
- Office 2007 IME japania varten—Jos Microsoft tai kolmas osapuoli käyttää termiä IME tai syöttömenetelmäeditoria, syöttömenetelmä ei todella voi olla IME. Tämä voi aiheuttaa sekaannuksen, mutta ohjelmisto lukee heksadesimaalikoodiesityksen. Täten jos IME kuvaa tuettuun näppäimistö-layoutiin, silloin HP Client Security voi tukea kokoonpanoa.

⚠ **VAARA** Kun HP Client Security sijoitetaan, Windows IMEllä annetut salasanat hylätään.

Salasanamuutokset käyttämällä näppäimistö-layoutia, jota myös tuetaan

Jos salasana on alunperin asetettu yhdellä näppäimistö-layoutilla, kuten U.S. English (409), ja sen jälkeen käyttäjä muuttaa salasanan käyttämällä eri näppäimistö-layoutia, jota myös tuetaan, kuten latinalaisamerikkalainen (080A), salasanamuutos toimii HP Drive Encryptionissa, mutta se kaatuu BIOSissa, jos käyttäjä käyttää merkkejä, jotka ovat myöhemmässä, mutta ei aikaisemmassa (esimerkiksi ē).

HUOMAUTUS: Järjestelmänvalvojat voivat ratkaista tämän ongelman käyttämällä HP Client Security Users -sivua (haettu **Gear**-kuvakkeesta etusivulla) poistamaan käyttäjän HP Client Securityn valitsemalla halutun näppäimistö-layoutin käyttöjärjestelmässä, ja sen jälkeen suorittamalla HP Client Securityn ohjatun asennuksen uudelleen samaa käyttäjää varten. BIOS-tallentaa halutun näppäimistö-layoutin ja salasanat, jotka voidaan kirjoittaa tällä näppäimistö-layoutilla, tulevat olemaan oikein asetettuja BIOSissa.

Toinen potentiaalinen seikka on eri näppäimistö-layoutien käyttö, jotka kaikki voivat tuottaa samat merkit. Esimerkiksi sekä U.S. International -näppäimistö-layout (20409) että latinalaisamerikkalainen näppäimistö-layout (080A) voivat tuottaa merkin é, vaikka erilaisia painallussekvenssejä voidaan tarvita. Jos salasana on alunperin asetettu latinalaisamerikkalaisella näppäimistö-layoutilla, silloin latinalaisamerikkalainen näppäimistö-layout asetetaan BIOSissa, vaikka jos salasana on myöhemmin muutettu käyttämällä U.S. International -näppäimistö-layoutia.

Erikoisnäppäimen käsittely

- Kiina, slovakia, kanadan ranska ja tsekki

  Kun käyttäjä valitsee yhden edellä olevista näppäimistöasetteluista ja antaa sitten salasanan (esimerkiksi abcdef), sama salasana on annettava samalla, kun vaihtonäppäintä painetaan pieniä kirjaimia varten ja vaihtonäppäintä ja caps lock -näppäintä painetaan isoja kirjaimia varten Power-on-todennuksessa ja HP Drive Encryptionissa. Numeeriset salasanat täytyy antaa käyttämällä numeerista näppäimistöä.

- Korea

  Kun käyttäjä valitsee tuetun koreankielisen näppäimistöasettelun ja antaa sitten salasanan, sama salasana on annettava samalla, kun oikeaa alt-näppäintä painetaan pieniä kirjaimia varten ja oikeaa alt-näppäintä ja caps lock -näppäintä painetaan isoja kirjaimia varten Power-on-todennuksessa ja HP Drive Encryptionissa.

- Tuettomat merkit luetellaan seuraavassa taulukossa:

Language (Kieli)	Windows	BIOS.	Drive Encryption
Arabia	٫ ,٬, ja ٭ -näppäimet luovat kaksi merkkiä.	٫ ,٬, ja ٭ -näppäimet luovat yhden merkin.	٫ ,٬, ja ٭ -näppäimet luovat yhden merkin.
Kanadan ranska	ç, è, à ja é + caps lock ovat Ç, È, À ja É Windowsissa.	ç, è, à ja é + caps lock ovat ç, è, à ja é Power-on-todennuksessa.	ç, è, à ja é + caps lock ovat ç, è, à ja é HP Drive Encryptionissa.

Language (Kieli)	Windows	BIOS.	Drive Encryption
Espanja	40a ei tueta. Se siitä huolimatta toimii, koska ohjelmisto muuntaa sen merkiksi c0a. Koska kuitenkin on vähäisiä eroja näppäimistö-layoutien välillä, on suositeltavaa, että espanjaa puhuvat käyttäjät muuttavat heidän Windows-näppäimistö-layoutinsa versioon 1040a (espanja-versio) tai versioon 080a (latinalaisamerikkalainen).	n/a	n/a
US international	◦ ¡, ¤, ‘, ’, ¥, ja × -näppäimet ylärivillä hylätään. ◦ å, ®, ja Þ -näppäimet toisella rivillä hylätään. ◦ á, ð, ja ø -näppäimet kolmannella rivillä hylätään. ◦ æ-näppäin alarivillä hylätään.	n/a	n/a
Tšekki	◦ ğ-näppäin hylätään. ◦ į-näppäin hylätään. ◦ ų-näppäin hylätään. ◦ ė, ı, ja ż -näppäimet hylätään. ◦ ģ, ķ, ļ, ņ, ja ţ -näppäimet hylätään.	n/a	n/a
Slovakia	ż-näppäin hylätään.	◦ š, ś, ja ş -näppäin hylätään kirjoitettaessa, mutta ne hyväksytään annettaessa soft-näppäimistöllä. ◦ Kuollut näppäin ţ luo kaksi merkkiä.	n/a
Unkari	ż-näppäin hylätään.	ţ-näppäin luo kaksi merkkiä.	n/a
sloveeni	żŻ-näppäin hylätään Windowsissa, ja alt-näppäin luo kuolleen näppäimen BIOSissa.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, ja Š -näppäimet hylätään BIOSissa.	n/a
Japanese	Kun käytettävissä, Microsoft Office 2007 IME on parempi valinta. IME-nimestä huolimatta se on todellisuudessa näppäimistö-layout 411, jota tuetaan.	n/a	n/a

Sanasto

aktivointi
Tehtävä, jonka täytyy olla valmis ennen kuin mihinkään aseman salauksen ominaisuuksiin on päästävissä. Järjestelmänvalvojat voivat aktivoida aseman salauksen HP Client Securityn ohjatulla käynnistyksellä tai HP Client Security -sovelluksella. Aktivointitapahtuma sisältää ohjelmiston aktivoinnin, aseman salauksen, ja aloitusvarmistuskopioinnin salausavaimen luomisen siirrettävällä tallennuslaitteella.

automaattinen hävitys
Hävittäminen, jonka aikataulutat File Sanitizerissa.

Bluetooth
Teknologia, joka tarjoaa radiolähetyksiä käyttöönottamaan Bluetooth-mahdollistettuja tietokoneita, tulostimia, hiiriä, matkapuhelimia, ja muita laitteita langattomaan tietoliikenteeseen lyhyellä etäisyydellä.

Drive Encryption
suojaa tietoja salaamalla kiintolevyt, minkä ansiosta muut kuin valtuutetut käyttäjät eivät pysty lukemaan niillä olevia tietoja.

Drive Encryptionin käynnistystä edeltäväksi todennus
Sisäänkirjautumisen ruutu näytetään ennen Windowsin käynnistymistä. Käyttäjien täytyy antaa heidän Windowsin käyttäjänimensä ja salasanansa tai älykortin PIN, tai pyyhkäistä rekisteröidyllä sormella. Jos yhden vaiheen sisäänkirjautuminen valitaan, sen jälkeen oikean tiedon antaminen aseman salauksen sisäänkirjautumisen ruudussa mahdollistaa suoran pääsyn Windowsiin tarvitsematta kirjoittautua uudelleen Windowsin sisäänkirjautumisen ruudulla.

Drive Encryption -kirjautumisnäyttö
Katso aseman salauksen esikäynnistyksen todennus.

DriveLock
Suojaustoiminto, joka yhdistää kiintolevyn käyttäjään ja vaatii käyttäjää kirjoittamaan oikein DriveLock-salasanan kun tietokone käynnistyy.

Encryption File System (EFS)
Järjestelmä, joka salaa kaikki valitun kansion tiedostot ja alikansiot.

Henkilökortti
Windows-työpöydän pienoisohjelma, joka tunnistaa visuaalisesti työpöytäsi käyttäjätunnuksesi ja valitun kuvasi kanssa.

HP SpareKey -palautus
Mahdollisuus käyttää tietokonetta vastaamalla turvallisuuskysymyksiin oikein.

hätäpalautusarkisto
Suojattu tallennuspaikka, joka sallii peruskäyttäjäavainten uudelleensalauksen yhden alustan omistajan avaimesta toiseen.

hävitys
Algoritmin suorittaminen, joka korvaa omaisuuden sisältämän tiedon merkityksettömällä tiedolla.

Just In Time Authentication
Katso HP Device Access Manager -ohjelmiston ohje.

järjestelmänvalvoja
Katso *Windows-järjestelmänvalvoja*.

kertakirjaustoiminto
Toiminto, joka tallentaa todennustiedot ja mahdollistaa HP Client Securityn käytön Internet-yhteyden muodostamista ja Windows-sovelluksia varten, jotka vaativat salasanatodennuksen.

kontaktiton kortti
Muovikortti sisältäen tietokonesirun, jota voidaan käyttää todennukseen.

Kotisivu
Keskuspaikka, missä voit päästä ja hallita ominaisuudet ja asetukset HP Client Securityssä.

kytketty laite
Laitteiston laite, joka on liitetty tietokoneessa olevaan porttiin.

käynnistystodennus
Turvallisuusominaisuus, joka edellyttää todennusta, kuten älykorttia, turvasirua, tai salasanaa, kun tietokone käynnistetään.

käyttäjä
Drive Encryptionia käyttävä henkilö. Muilla kuin järjestelmänvalvojilla on Drive Encryptionissa rajalliset oikeudet. He voivat ainoastaan rekisteröityä (järjestelmänvalvojan luvalla) ja kirjautua sisään.

laiteluokka
Kaikki erityisen tyyppiset laitteet, kuten asemat.

laitteeseen pääsyn käytäntö
Luettelo laitteista, joihin käyttäjä on sallittu tai kielletty pääsemään.

laitteiston salaus
Niiden itsesalaavien asemien käyttö, jotka täyttävät Trusted Computing Group'in OPAL:in määrityksen itsesalaavan aseman hallinnasta suorittamaan äkillisen salauksen. Laitteiston salaus on äkillistä ja voi viedä vain muutamia minuutteja, mutta ohjelmiston salaus voi viedä aikaa useita tunteja.

lähestymiskortti
Muovikortti sisältäen tietokonesirun, jota voidaan käyttää todennukseen yhdessä muiden valtuustietojen kanssa lisävarmistusta varten.

manuaalinen hävitys
Omaisuuden tai valittujen omaisuuksien välitön hävittäminen, mikä ohittaa aikataulutetun hävityksen.

ohjelmiston salaus
Ohjelmiston käyttö salaamaan kovalevyaseman sektori sektorilta. Tämä prosessi on hitaampi kuin laitteiston salaus.

omaisuus
Tietokomponentti, joka muodostuu henkilökohtaisista tiedoista tai tiedostoista, historiallisesta ja Webiin liittyvästä tiedosta, jne., mikä sijaitsee kovalevyasemalla.

omat tiedot
HP Client Securityssä tunnistetietojen ja asetusten joukkoa käsitellään kuten tietyn käyttäjän tiliä tai profiilia.

palauttaminen
Prosessi, joka kopioi ohjelman tietoja aikaisemmin ohjelmaan tallennetusta tallennuskopiointitiedostosta.

PIN-koodi
Henkilökohtainen tunnistusnumero rekisteröidylle käyttäjälle käytettäväksi todennukseen.

PKI
Public Key Infrastructure -standardi, joka määrittää varmenteiden ja salausavainten luomisen, käyttämisen ja hallinnan rajapinnat.

ryhmä
Käyttäjien ryhmä, jolla on sama pääsytaso tai kielto laiteluokkaan tai tiettyyn laitteeseen.

salaaminen
Salauksessa käytetty toiminto, kuten algoritmin käyttö, jolla muutetaan tavallinen teksti, jotta valtuuttamattomat vastaanottajat eivät voi lukea kyseisiä tietoja. On olemassa useita erityyppisiä tietojen salauksia ja ne ovat verkon suojauksen perusta. Yleisimpiä tyyppejä ovat mm. Data Encryption Standard ja julkisen avaimen salaus.

salauksen purkaminen
Salauksessa käytettävä toiminto, joka muokkaa salatut tiedot tavalliseksi tekstiksi.

sisäänkirjautuminen
Kohde HP Client Securityn sisällä, joka sisältää käyttäjänimen ja salasanan (ja mahdollisesti muita valittuja tietoja), joita voidaan käyttää kirjautumiseen www-sivustoille tai muihin ohjelmiin.

sormenjälki
Digitaalinen sormenjälkikuvasi ote. Todellista sormenjälkikuvaasi ei milloinkaan ole tallennettu HP Client Security-sovelluksella.

suojattu kirjautumistapa
Tietokoneeseen kirjautumiseen käytettävä menetelmä.

todentaminen
Vahvistamisprosessi, että olet väittämäsi henkilö valtuustietoja käyttämällä, mukaan lukien Windows-salasanasi, sormenjälkesi, älykortti, kontaktiton kortti, tai lähestymiskortti.

toimialue
Joukko tietokoneita, jotka ovat osa verkkoa ja jotka jakavat yhteisen hakemistotietokannan. Toimialueilla on yksilöllinen nimi ja kullakin on toimialueella on yleisten sääntöjen ja toimintojen joukko.

Trust Circle
Tarjoaa tietojen sitomisen sitomalla tiedot määritettyyn luotettujen käyttäjien ryhmään. Tämä estää tietojen joutumisen vääriin käsiin joko vahingossa tai tarkoituksellisesti. Varmistettu CryptoMill’s Zero Overhead Key Management -teknologialla, tiedot on salauksellisesti sidottu luottamuksen piiriin. Tämä ehkäisee asiakirjojen tai trust circlen ulkopuolella olevien muiden sensitiivisten tietojen salauksen purkamisen.

Trust Circle -kansio
Mikä tahansa trust circlellä suojattu kansio.

Trust Circle Manager/lukija
Trust Circle Reader voi hyväksyä vain kutsuja, jotka Trust Circle Manager on lähettänyt ulos. Kuitenkin Trust Circle Manager sallii trust circlejen luomisen. Ominaisuudet sisältävät jonkun kutsumisen sähköpostilla trust circleen ja trust circle -kutsujen hyväksymisen muilta. Heti kun trust circle on perustettu kumppaneiden joukossa, tuolla trust circlellä suojatut tiedostot voidaan jakaa turvallisesti.

Trusted Platform Module (TPM) Embedded Security -siru
TPM todentaa tietokoneen käyttäjän sijasta tallentamalla isäntäjärjestelmään liittyviä tietoja, kuten salausavain digitaalinen varmenne ja salasanat. TPM pienentää tietokoneen tietojen vaarantumisriskiä johtuen varkauksista tai ulkoisista hyökkäyksistä.

tunnistetiedot
Tietty pala tietoja tai laitteiston laite, jota käytetään yksittäisen käyttäjän todennukseen.

uudelleenkäynnistys
Tietokoneen uudelleenkäynnistys.

vapaan tilan tyhjennys
Satunnaisen tiedon kirjoittaminen poistettujen omaisuuksien ja käyttämättömän tilan päälle. Tämä prosessi vähentää poistetun omaisuuden olemassaoloa niin, että alkuperäistä omaisuutta on vaikeampi palauttaa.

varmuuskopiointi

Käyttämällä varmuuskopiointi-ominaisuutta tallentamaan tärkeän ohjelmatiedon kopion ohjelman ulkopuolella olevaan sijaintipaikkaan. Sitä voidaan sen jälkeen käyttää tietojen palauttamiseen myöhempänä päivänä samaan tai toiseen tietokoneeseen.

verkkokäyttäjätili
Paikallisessa tietokoneessa, työryhmässä tai toimialueessa oleva Windowsin käyttäjä- tai järjestelmänvalvojatili.

Windows-järjestelmänvalvoja
Käyttäjä täysillä oikeuksilla muunnella lupia ja hallita muita käyttäjiä.

Windows-käyttäjätili
Käyttäjä, joka on valtuutettu kirjautumaan sisään verkkoon tai yksittäiseen tietokoneeseen.

Windows Logon Security
Suojaa Windows-tilejä vaatimalla tiettyjä tunnistetietoja niiden käyttöä varten.

älykortti
Laitteiston laite, jota voidaan käyttää PIN-koodin kanssa todennukseen.

Hakemisto