HP ProtectTools
Käyttöopas

Ensimmäinen painos: marraskuu 2009

Asiakirjan osanumero: 593308-351

Sisällysluettelo

1 Johdanto: tietoturva

HP ProtectTools Security Manager -ohjelmiston suojausominaisuudet suojaavat tietokonetta, verkkoa ja kriittisiä tietoja luvattomalta käytöltä. HP ProtectTools Security Manager -ohjelmiston hallinta toteutetaan hallintakonsolitoiminnon avulla.

HP ProtectTools -hallintakonsolin avulla paikallinen järjestelmänvalvoja voi suorittaa seuraavat tehtävät:

- ottaa suojaustoiminnot käyttöön tai poistaa ne käytöstä
- rekisteröidä sormenjälkensä ja muiden tietokoneen käyttäjien sormenjäljet
- rekisteröidä yhden tai useamman kohteen kasvontunnistusta varten
- asentaa älykortin todennusta varten
- määrittää todennukseen vaadittavat valtuustiedot
- hallita tietokoneen käyttäjiä
- säätää laitekohtaisia parametreja
- määrittää asennettujen Security Manager -sovellusten asetukset
- lisätä uusia Security Manager -sovelluksia.

Security Managerin kojelaudan avulla paikallinen tavalliset käyttäjät voivat suorittaa seuraavat tehtävät:

- määrittää järjestelmänvalvojalta saadut asetukset
- hallita rajoitetusti joitakin HP ProtectTools -moduuleja.

Käytettävissä olevat ohjelmistomoduulit vaihtelevat tietokoneen mallin mukaan.

HP ProtectTools -ohjelmistomoduulit ovat esiasennettavissa, esiladattavissa tai saatavilla lataamista varten HP:n WWW-sivustosta. Lisätietoja on osoitteessa http://www.hp.com.

HUOMAUTUS: Tässä oppaassa oletetaan, että asianmukaiset HP ProtectTools -moduulit on jo asennettu tietokoneeseen.

HP ProtectTools -ominaisuudet

Seuraavassa taulukossa esitellään HP ProtectTools -moduulien tärkeimmät ominaisuudet.

Moduuli	Tärkeimmät ominaisuudet
HP ProtectTools Security Manager -hallintakonsoli (järjestelmänvalvojille)	• Ota käyttöön ja määritä suojaustasot ja suojatut kirjautumistavat Security Managerin ohjatun asennustoiminnon avulla. • Määritä peruskäyttäjiltä piilotetut asetukset. • Määritä Device Access Managerin kokoonpanot ja käyttöoikeudet. • Lisää ja poista HP ProtectTools -käyttäjiä sekä tarkastele käyttäjien tilaa järjestelmänvalvojan työkalujen avulla.
HP ProtectTools Security Manager (tavallisille käyttäjille)	• Järjestele, luo ja muuta käyttäjänimiä ja salasanoja. • Määritä ja muuta käyttäjien valtuustietoja, kuten Windows-salasanaa ja älykorttia. • Määritä ja muuta File Sanitizerin hävitys- ja tuhoamistoimintoja sekä asetuksia. • Tarkastele Device Access Managerin asetuksia. • Määritä ominaisuudet sekä varmuuskopiointi- ja palautusasetukset.
Credential Manager for HP ProtectTools (Password Manager)	• Tallenna, järjestele ja suojaa nimiä ja salasanoja. • Määritä sivustojen ja ohjelmien kirjautumisnäytöt nopeaa ja suojattua käyttöä varten. • Tallenna sivustojen käyttäjänimet ja salasanat kirjoittamalla ne Password Manageriin. Kun käyt sivustossa seuraavan kerran, Password Manager täyttää ne ja lähettää tiedot automaattisesti. • Paranna tilin suojausta luomalla entistä vahvempia salasanoja. Password Manager täyttää ja lähettää tiedot automaattisesti.
Drive Encryption for HP ProtectTools (vain tietyt mallit)	• Salaa koko kiintolevy täydellisesti. • Vaadi käynnistystä edeltävää todennusta tietojen salauksen purkamista ja niiden käyttöä varten.
Privacy Manager for HP ProtectTools (vain tietyt mallit)	• Käytä kehittyneitä kirjautumistekniikoita sähköpostiviestien, Microsoft® Office -asiakirjojen tai pikaviestien lähteen, eheyden ja turvallisuuden tarkistamiseen.
File Sanitizer for HP ProtectTools	• Hävitä tietokoneessa oleva digitaalinen omaisuus (arkaluonteiset tiedot, kuten sovellustiedostot, historialliset tai Internetin käyttöön liittyvät sisällöt tai muut luottamukselliset aineistot) ja tyhjennä kiintolevy säännöllisesti.
Device Access Manager for HP ProtectTools (vain tietyt mallit)	• Anna IT-päälliköiden hallita laitteiden käyttöä käyttäjäprofiilien perusteella. • Estä valtuuttamattomia käyttäjiä varastamasta tietoja ja siirtämästä viruksia järjestelmään ulkoisten tallennusvälineiden avulla. • Anna järjestelmänvalvojien estää tiettyjä henkilöitä tai käyttäjäryhmiä käyttämästä kirjoittavia laitteita.

Tärkeimpien tietoturvatavoitteiden saavuttaminen

HP ProtectTools -moduulit toimivat yhdessä tuottaen ratkaisuja erilaisiin tietoturvaongelmiin, kuten seuraaviin tärkeisiin tietoturvatavoitteisiin:

- suojautuminen varkauksilta
- arkaluontoisten tietojen käytön rajoittaminen
- luvattoman käytön estäminen sisäisistä tai ulkoisista sijainneista
- vahvojen salasanakäytäntöjen luominen

Suojautuminen kohdistettuja varkauksia vastaan

Esimerkki kohdistetusta varkaudesta on luottamuksellisia ja asiakkaan tietoja sisältävän tietokoneen varastaminen lentokentän turvatarkastuksessa. Voit suojautua kohdistettuja varkauksia vastaan seuraavien toimintojen avulla:

- Jos käynnistystä edeltävä todennustoiminto on otettu käyttöön, se auttaa estämään käyttöjärjestelmän käytön. Lisätietoja on seuraavissa toimintaohjeissa:
  - Security Manager
  - Drive Encryption

Arkaluonteisten tietojen käytön rajoittaminen

Kuvittele tilannetta, jossa tilintarkastaja työskentelee toimipisteessäsi ja hänelle on annettu oikeudet tarkastella arkaluonteisia taloudellisia tietoja, mutta et halua hänen tulostavan tiedostoja tai tallentavan niitä kirjoittavalla tallennuslaitteella esimerkiksi CD-levylle. Voit rajoittaa tietojen käyttöä seuraavan toiminnon avulla:

- Device Access Manager for HP ProtectTools -ohjelmiston avulla IT-päälliköt voivat rajoittaa kirjoittavien tallennuslaitteiden käyttöä, jotta arkaluonteisia tietoja ei voi tulostaa tai kopioida kiintolevyltä siirrettävälle tallennusvälineelle.

Luvattoman käytön estäminen sisäisistä tai ulkoisista sijainneista

Suojaamattoman yritystietokoneen luvaton käyttö aiheuttaa vakavan uhan paitsi yrityksen verkossa oleville resursseille, joihin kuuluvat muun muassa rahoituspalveluilta, johtohenkilöiltä tai tutkimus- ja kehitysryhmältä peräisin olevat tiedot, myös potilaskertomusten ja henkilökohtaisen taloudellisen tilanteen kaltaisille yksityisille tiedoille. Voit estää tietojen luvattoman käytön seuraavasti:

- Jos käynnistystä edeltävä todennustoiminto on otettu käyttöön, se auttaa estämään käyttöjärjestelmän käytön. Lisätietoja on seuraavissa toimintaohjeissa:
  - Password Manager
  - Drive Encryption
- Password Manager auttaa varmistamaan, että luvattomat käyttäjät eivät pysty hankkimaan salasanoja tai käyttämään salasanalla suojattuja sovelluksia.
- Device Access Manager for HP ProtectTools -ohjelmiston avulla IT-päälliköt voivat rajoittaa kirjoittavien tallennuslaitteiden käyttöä, jotta arkaluonteisia tietoja ei voi kopioida kiintolevyltä.

- File Sanitizerin avulla voit poistaa tiedot turvallisesti hävittämällä tärkeät tiedostot ja kansiot tai tyhjentämällä kiintolevyn (korvaamalla poistetut, mutta edelleen palautettavissa olevat tiedot).
- DriveLock auttaa varmistamaan, että tietoja ei voi käyttää, vaikka kiintolevy irrotetaan ja asennetaan suojaamattomaan järjestelmään.

Vahvojen salasanakäytäntöjen luominen

Jos yrityksessä aletaan soveltaa käytäntöä, joka edellyttää vahvojen salasanojen käyttöä monissa verkkopohjaisissa sovelluksissa ja tietokannoissa, Security Manager tarjoaa salasanoille suojatun säilön ja kertakirjautumisen mukavuuden.

Lisäsuojauselementit

Tietoturvaroolien määrittäminen

Etenkin suurten organisaatioiden tietokoneiden tietosuojan hallintaa suunniteltaessa on tärkeää jakaa vastuut oikein järjestelmänvalvojien ja käyttäjien kesken.

HUOMAUTUS: Pienissä organisaatioissa ja yksityisissä tietojärjestelmissä yksi henkilö voi hoitaa kaikki nämä roolit.

HP ProtectTools -järjestelmässä suojausvastuut ja -oikeudet voidaan jakaa seuraavasti:

- Tietosuojavastaava: Määrittelee yrityksen tai verkon suojaustason ja valitsee käytettävät tietosuojalaitteet, kuten Java™-kortit, biometriset tunnistimet tai USB-poletit.

  HUOMAUTUS: Yhteistyössä HP:n kanssa tietosuojavastaava voi mukauttaa monia HP ProtectToolsin toimintoja. Lisätietoja on HP:n WWW-sivustossa osoitteessa http://www.hp.com.

- Järjestelmänvalvoja: Käyttää ja määrittää tietosuojavastaavan valitsemia suojaustoimintoja. Järjestelmänvalvoja voi myös ottaa tiettyjä toimintoja käyttöön tai poistaa niitä käytöstä. Jos tietosuojavastaava on valinnut käytettäväksi esimerkiksi Java-kortit, järjestelmänvalvoja voi määrittää myös BIOS-järjestelmälle Java-korttisuojauksen.

- Käyttäjä: Käyttää suojaustoimintoja. Jos tietosuojavastaava ja järjestelmänvalvoja ovat ottaneet käyttöön esimerkiksi Java-kortit, käyttäjä voi määrittää Java-kortin PIN-koodin ja käyttää korttia käyttöoikeutensa todistamiseen.

VAROITUS: Järjestelmänvalvojia kehotetaan noudattamaan ”parhaita käytäntöjä” heidän rajoittaessaan loppukäyttäjien oikeuksia ja tietojen käyttömahdollisuuksia.

Luvattomille käyttäjille ei pidä myöntää järjestelmänvalvojan oikeuksia.

HP ProtectTools -salasanojen hallinta

Useimmat HP ProtectTools Security Manager -ohjelman toiminnot on suojattu salasanoilla. Seuraavassa taulukossa luetellaan yleiset salasanat, ohjelmistomoduulit, joissa salasanat määritetään, sekä salasanojen käyttötarkoitukset.

Taulukossa näkyvät myös vain järjestelmänvalvojien käyttöön tarkoitetut salasanat. Muita salasanoja voivat määrittää sekä käyttäjät että järjestelmänvalvojat.

HP ProtectTools -salasana	Aseta seuraava moduuli	Käyttötarkoitus
Windowsin kirjautumissalasana	Windowsin® ohjauspaneeli tai HP ProtectTools Security Manager	Voidaan käyttää manuaaliseen kirjautumiseen ja Security Managerin eri toimintojen käyttöoikeuksien todentamiseen.
Security Managerin varmuuskopiointi- ja palautussalasana	Security Manager, yksittäinen käyttäjä	Suojaa Security Managerin varmuuskopiointi- ja palautustiedostoa.
Java™-kortin PIN-koodi	Java Card Security	Suojaa Java-kortin sisältöä ja vahvistaa Java-kortin käyttäjän henkilöllisyyden. Kun Java-korttia käytetään käyttöoikeuden tarkistamiseen tietokonetta käynnistettäessä, PIN-koodi suojaa myös Tietokoneen asetukset -ohjelmaa ja tietokoneen sisältöä.

HP ProtectTools -salasana	Aseta seuraava moduuli	Käyttötarkoitus
		Todentaa Drive Encryption -käyttäjät, jos Java Card -poletti on valittu.

Suojatun salasanan valitseminen

Salasanoja luotaessa on noudatettava kyseisen ohjelman vaatimuksia. Seuraavassa on lueteltu joitakin yleisiä ohjeita, joita noudattamalla voit luoda luotettavia salasanoja ja pienentää salasanojen murtamisen riskiä.

- Käytä salasanoja, joissa on vähintään kuusi ja mieluiten enemmän kuin kahdeksan merkkiä.
- Käytä isoja ja pieniä kirjaimia.
- Käytä sekä kirjaimia että numeroita aina, kun se on mahdollista. Käytä myös erikoismerkkejä ja välimerkkejä.
- Vaihda sanoihin kirjainten tilalle erikoismerkkejä tai numeroita. Voit esimerkiksi vaihtaa I- tai L-kirjaimen tilalle numeron 1.
- Yhdistele eri kielten sanoja.
- Erota sanan tai lauseen osat numeroilla tai erikoismerkeillä, esimerkiksi Maija2-2Leena45.
- Älä käytä salasanana sanaa, joka löytyy sanakirjasta.
- Älä käytä salasanana nimeäsi tai mitään muuta henkilökohtaista tietoa, kuten syntymäaikaa, lemmikkieläimen nimeä tai äitisi tyttönimeä, älä edes takaperin kirjoitettuna.
- Vaihda salasanat säännöllisesti. Voit vaihtaa vaikkapa vain pari merkkiä.
- Jos kirjoitat salasanat muistiin, älä säilytä niitä näkyvässä paikassa tietokoneen lähellä.
- Älä tallenna salasanoja tietokoneeseen tai sähköpostiin.
- Älä käytä yhteistä käyttäjätiliä kenenkään kanssa äläkä kerro salasanaasi kenellekään.

HP ProtectToolsin valtuustietojen varmuuskopiointi ja palauttaminen

HP ProtectToolsin varmuuskopiointi- ja palautustoiminnon avulla voit valita ja varmuuskopioida HP ProtectToolsin valtuustiedot ja asetukset.

2 Ohjatun asennustoiminnon käytön aloittaminen

HP ProtectToolsin ohjattu asennustoiminto neuvoo Security Managerin useimmin käytettyjen toimintojen asennuksessa. HP ProtectToolsin hallintakonsolissa on kuitenkin lukuisia lisätoimintoja. Windowsin® Käynnistä-valikosta avattavassa konsolissa voidaan määrittää ohjatun toiminnon asetukset, kuten myös muita suojausominaisuuksia. Nämä asetukset koskevat tietokonetta ja kaikkia tietokoneen jakavia käyttäjiä.

1. Viikon kuluttua tietokoneen käyttöönotosta tai sen jälkeen, kun kirjaudut sisään tai järjestelmänvalvojan oikeudet saanut käyttäjä pyyhkäisee sormellaan sormenjäljenlukijaa ensimmäisen kerran, Security Managerin ohjattu asennustoiminto käynnistyy automaattisesti ja opastaa sinua ohjelman perusasetusten määrittämisessä. Tietokoneen asetusten määrittämistä käsittelevä video-opetusohjelma käynnistyy automaattisesti.

   TAI

   Avaa HP ProtectTools Security Manager Windowsin sivupalkin **Gadget** (Pienoisohjelma) -kuvakkeella tai tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen tehtäväpalkkikuvakkeella.

   

   Gadget (Pienoisohjelma) -kuvakkeen yläpalkin väri viittaa johonkin seuraavista tilanteista:

   - Punainen – HP ProtectToolsia ei ole otettu käyttöön tai jossakin ProtectTools-moduulissa on tapahtunut virhe.
   - Keltainen – Tarkista Security Managerin Applications Status (Sovellusten tila) -sivulta, mitä asetuksia on muutettava.
   - Sininen – HP ProtectTools on otettu käyttöön ja se toimii oikein.

   HUOMAUTUS: Gadget (Pienoisohjelma) -kuvake ei ole käytettävissä Windows XP:ssä.

   TAI

Valitse **Käynnistä**, **Kaikki ohjelmat** ja sitten **HP ProtectTools Administrative Console** (HP ProtectToolsin hallintakonsoli).

2. Lue Welcome (Tervetuloa) -näytön teksti ja valitse **Next** (Seuraava).

HUOMAUTUS: Welcome (Tervetuloa) -näytössä voit poistaa ohjatun toiminnon näkyvistä valitsemalla jonkin annetuista vaihtoehdoista.

3. Ohjattu asennustoiminto pyytää sinua vahvistamaan henkilöllisyytesi.

   Anna Windows-salasanasi tai lue sormenjälkesi sormenjäljenlukijalla ja valitse sitten **Next** (Seuraava).

   Jos sormenjäljenlukijaa tai älykorttia ei ole käytettävissä, sinua kehotetaan antamaan Windows-salasanasi. Sinun on käytettävä tätä salasanaa tulevaisuudessa aina todennusta vaadittaessa.

   Jos et ole vielä luonut Windows-salasanaa, sinua kehotetaan luomaan se. Windows-salasanaa tarvitaan suojaamaan Windows-tiliä luvattomalta käytöltä ja HP ProtectTools Security Managerin toimintojen käyttöön.

4. Ohjattu asennustoiminto opastaa kaikkia tietokoneen käyttäjiä koskevien suojausominaisuuksien käyttöönotossa.

   - Windows Logon Security suojaa Windows-tilejä vaatimalla tiettyjä valtuustietoja niiden käyttöä varten.
   - Drive Encryption suojaa tietoja salaamalla kiintolevyt, minkä ansiosta muut kuin valtuutetut käyttäjät eivät pysty lukemaan niillä olevia tietoja.
   - Pre-Boot Security suojaa tietokonetta estämällä sen luvattoman käytön ennen Windowsin käynnistymistä.

     HUOMAUTUS: Pre-Boot Security ei ole käytettävissä, jos tietokoneen BIOS ei tue sen käyttöä.

   Voit ottaa suojaustoiminnon käyttöön valitsemalla sitä vastaavan valintaruudun. Mitä enemmän toimintoja valitset, sitä suojatumpi tietokone on.

5. Valitse ohjatun toiminnon viimeisellä sivulla **Finish** (Valmis).

   Security Managerin kojelauta tulee näyttöön.

HUOMAUTUS: Jos et suorita ohjattua asennustoimintoa loppuun, se käynnistetään vielä kaksi kertaa automaattisesti uudelleen. Tämän jälkeen voit avata ohjatun asennustoiminnon ilmoituspuhekuplasta, joka ilmestyy tehtäväpalkin oikeassa reunassa olevalle ilmaisinalueelle (paitsi jos olet poistanut sen käytöstä) ja näkyy siellä, kunnes asennus on suoritettu loppuun.

3 HP ProtectTools Security Managerin hallintakonsoli

HP ProtectTools Security Managerin hallinta toteutetaan hallintakonsolin avulla.

HUOMAUTUS: HP ProtectToolsin hallintaan vaaditaan järjestelmänvalvojan oikeudet.

Konsolin avulla voit

- ottaa suojaustoiminnot käyttöön tai poistaa ne käytöstä
- hallita tietokoneen käyttäjiä
- säätää laitekohtaisia parametreja
- määrittää Security Manager -sovellusten asetukset
- lisätä uusia Security Manager -sovelluksia.

▲ Jos haluat käyttää HP ProtectTools Security Manager -sovelluksia, käynnistä HP ProtectTools Security Manager Käynnistä-valikosta tai napsauta hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella olevaa Security Manager -kuvaketta.

HP ProtectToolsin hallintakonsoli ja sen sovellukset ovat kaikkien tietokoneen jakavien käyttäjien käytettävissä.

Hallintakonsolin avaaminen

Avaa konsoli hallintatehtävien suorittamista, kuten järjestelmän käytäntöjen tai ohjelmiston asetusten määrittämistä varten seuraavasti:

- Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Administrative Console** (HP ProtectToolsin hallintakonsoli).

  TAI

  Valitse Security Managerin kojelaudan vasemmasta ruudusta **Administration** (Hallinta).

Avaa konsoli käyttäjätehtävien suorittamista, kuten sormenjälkien rekisteröintiä tai Security Managerin käyttöä varten seuraavasti:

- Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Security Manager**.

  TAI

  Kaksoisnapsauta tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **HP ProtectTools Security Manager** -kuvaketta.

Hallintakonsolin käyttäminen

HP ProtectTools Security Manageria hallitaan keskitetysti Security Managerin hallintakonsolin kautta.

Konsoli muodostuu seuraavista osista:

- **Tools** (Työkalut) – Näyttää seuraavat tietokoneen suojauksen määrittämiseen käytettävät luokat:
  - **Home** (Koti) – Mahdollistaa suoritettavien suojaustehtävien valinnan.
  - **System** (Järjestelmä) – Mahdollistaa suojaustoimintojen ja todennuksen määrittämisen käyttäjiä ja laitteita varten.
  - **Applications** (Sovellukset) – Näyttää HP ProtectTools Security Managerin ja Security Manager -sovellusten yleiset asetukset.
  - **Data** (Tiedot) – Näyttää tietoja suojaavien Security Manager -sovellusten linkkien avautuvan valikon.
- **Management Tools** (Hallintatyökalut) – Antaa tietoja muista työkaluista. Ruutu sisältää seuraavat vaihtoehdot:
  - **HP ProtectTools Security Manager Setup Wizard** (HP ProtectTools Security Managerin ohjattu asennustoiminto) – Opastaa HP ProtectTools Security Managerin käyttöönotossa.
  - **Help** (Ohje) – Näyttää ohjetiedoston, jossa on tietoja Security Managerista ja sen valmiiksi asennetuista sovelluksista. Myöhemmin lisättävien sovellusten ohjeet sisältyvät kyseisiin sovelluksiin.
  - **About** (Tietoja) – Näyttää tietoja HP ProtectTools Security Managerista, muun muassa versionumeron ja tekijänilmoitusilmoituksen.
- **Main area** (Pääalue) – Näyttää sovelluskohtaisia näyttöä.

4 Järjestelmän asetusten määrittäminen

System (Järjestelmä) -ryhmä avataan HP ProtectToolsin hallintakonsolinäytön vasemmalla puolella olevasta Tools (Työkalut) -valikkopaneelista. Tähän ryhmään kuuluvien sovellusten avulla voit hallita tietokoneen, sen käyttäjien ja sen laitteiden käytäntöjä ja asetuksia.

System (Järjestelmä) -ryhmään kuuluvat seuraavat sovellukset:

- **Security** (Suojaus) – Hallitse toimintoja, todennusta ja asetuksia, jotka määräävät, miten käyttäjät voivat käyttää tietokonetta.
- **Users** (Käyttäjät) – Määritä, hallitse ja rekisteröi tietokoneen käyttäjiä.
- **Devices** (Laitteet) – Hallitse tietokoneessa olevien tai siihen kytkettyjen suojauslaitteiden asetuksia.

Todennuksen ottaminen käyttöön tietokoneessa

Authentication (Todennus) -sovelluksen avulla voit valita tietokoneessa käytettävät suojausominaisuudet, asettaa tietokoneen käyttöä ohjaavat käytännöt ja määrittää muita lisäasetuksia. Voit määrittää valtuustiedot, joita käytetään eri käyttäjätyyppien todennukseen, kun käyttäjät kirjautuvat Windowsiin tai sivustoihin ja ohjelmiin käyttäjäistuntojen aikana.

Voit ottaa todennuksen tietokoneessa käyttöön seuraavasti:

1. Valitse Security (Suojaus) -valikosta **Authentication** (Todennus).
2. Jos haluat määrittää kirjautumisen todennuksen, valitse **Logon Policy** (Kirjautumiskäytäntö), tee muutokset ja valitse **Apply** (Käytä).
3. Jos haluat määrittää istunnon todennuksen, valitse **Session Policy** (Istuntokäytäntö), tee muutokset ja valitse **Apply** (Käytä).

Kirjautumiskäytäntö

Jos haluat määrittää käytännöt, jotka koskevat Windowsiin kirjauduttaessa tarvittavia käyttäjän valtuustietoja, toimi seuraavasti:

1. Valitse Tools (Työkalut) -valikosta **Security** (Suojaus) ja sitten **Authentication** (Todennus).
2. Valitse **Logon Policy** (Kirjautumiskäytäntö) -välilehti ja sitten käyttäjäluokka.
3. Määritä valitun käyttäjäluokan vaatimat todennusvaltuustiedot. Sinun on määritettävä ainakin yksi valtuustieto.
4. Valitse, vaaditaanko käyttäjän todennukseen MIKÄ TAHANSA (vain yksi) määritetyistä valtuustiedoista vai KAIKKI määritetyt valtuustiedot. Voit myös estää käyttäjiä käyttämästä tietokonetta.
5. Valitse **Apply** (Käytä).

Istuntokäytäntö

Jos haluat määrittää käytännöt, jotka koskevat HP ProtectTools -sovellusten käyttöä Windows-istunnon aikana, toimi seuraavasti:

1. Valitse Tools (Työkalut) -valikosta **Security** (Suojaus) ja sitten **Authentication** (Todennus).
2. Valitse **Session Policy** (Istuntokäytäntö) -välilehti ja sitten käyttäjäluokka.
3. Määritä valitun käyttäjäluokan vaatimat todennusvaltuustiedot.
4. Valitse, vaaditaanko käyttäjän todennukseen YKSI määritetyistä valtuustiedoista vai KAIKKI määritetyt valtuustiedot. Voit myös määrittää, että HP ProtectTools -ohjelmiston käyttöön ei vaadita todennusta.
5. Valitse **Apply** (Käytä).

Asetukset

Voit sallia yhden tai useampia seuraavista suojausasetuksista:

- **Allow One Step logon** (Salli yksivaiheinen kirjautuminen) – Tietokoneen käyttäjät voivat ohittaa Windows-kirjautumisen, jos todennus on suoritettu BIOSin tai salatun levyn tasolla.
- **Allow HP SpareKey authentication for Windows logon** (Salli HP SpareKey -todennus Windowsiin kirjauduttaessa) – Tietokoneen käyttäjät voivat käyttää HP SpareKey -toimintoa kirjautuessaan Windowsiin muihin Security Managerin vaatimiin todennuskäytäntöihin katsomatta.

Voit muuttaa asetuksia seuraavasti:

1. Ota haluamasi asetus käyttöön tai poista se käytöstä napsauttamalla sitä.
2. Tallenna muutokset valitsemalla **Apply** (Käytä).

Käyttäjien hallinta

Users (Käyttäjät) -sovelluksessa voit valvoa ja hallita tietokoneen HP ProtectTools -käyttäjiä.

Kaikki HP ProtectTools -käyttäjät on lueteltu ja heitä arvioidaan Security Managerissa määritettyjen käytäntöjen perusteella. Tavoitteena on tarkistaa, että ovatko he rekisteröineet käytäntöjä vastaavat valtuustiedot.

Voit hallita käyttäjiä seuraavien vaihtoehtojen avulla:

- Jos haluat lisätä uusia käyttäjiä, valitse **Add** (Lisää).
- Jos haluat poistaa käyttäjän, napsauta käyttäjää ja valitse **Delete** (Poista).
- Jos haluat rekisteröidä sormenjälkiä tai määrittää käyttäjälle muita valtuustietoja, napsauta käyttäjää ja valitse **Enroll** (Rekisteröi).
- Jos haluat tarkastella tietyn käyttäjän käytäntöjä, valitse käyttäjä ja tarkastele käytäntöjä alemmassa ikkunassa.

Laitteen asetusten määrittäminen

Device (Laite) -sovelluksessa voit määrittää asetukset, jotka ovat käytettävissä HP ProtectTools Security Managerin tunnistamissa sisäänrakennetuissa tai kytketyissä suojauslaitteissa.

Fingerprints (Sormenjäljet)

Fingerprints (Sormenjäljet) -sivulla on kolme välilehteä: Enrollment (Rekisteröinti), Sensitivity (Herkkyys) ja Advanced (Lisäasetukset).

Enrollment (Rekisteröinti)

Voit määrittää käyttäjän rekisteröitävissä olevien sormenjälkien vähimmäis- ja enimmäismäärän.

Voit myös poistaa kaikki sormenjäljenlukijassa olevat tiedot.

△ **VAROITUS:** Sormenjäljenlukijan kaikkien tietojen poistaminen poistaa kaikkien käyttäjien sormenjälkitiedot, järjestelmänvalvojat mukaan lukien. Jos kirjautumiskäytäntö vaatii vain sormenjälkiä, kaikkien käyttäjien kirjautuminen tietokoneeseen voidaan estää.

Sensitivity (Herkkyys)

Voit säätää sormenjäljenlukijan sormenjälkiä skannattaessa käyttämän herkkyyden liukusäätimellä.

Jos sormenjälkeä ei tunnisteta johdonmukaisesti, sinun on mahdollisesti käytettävä suurempaa herkkyysasetusta. Suurempi asetus lisää herkkyyttä havaita skannattujen sormenjälkien välillä olevia eroja ja siten vähentää virheellisen hyväksynnän mahdollisuutta. Medium-High (Keskisuuri) -asetuksessa yhdistyvät turvallisuus ja kätevyys.

Advanced (Lisäasetukset)

Voit määrittää sormenjäljenlukijan säästämään virtaa, kun tietokonetta käytetään akkuvirralla.

Smart card (Älykortti)

Voit määrittää tietokoneen lukkiutumaan automaattisesti, kun älykortti poistetaan. Tietokone lukitaan kuitenkin vain silloin, jos älykorttia käytettiin todennusvaltuustietona kirjauduttaessa Windowsiin. Tietokonetta ei lukita, jos poistettua älykorttia ei käytetty kirjautumiseen Windowsiin.

▲ Valitse valintaruutu, jos haluat ottaa tietokoneen lukituksen käyttöön tai poistaa sen käytöstä, kun älykortti poistetaan.

Kasvot

Voit määrittää kasvontunnistustoiminnon suojaustason painottamalla helppokäyttöisyyttä tai tietokoneen suojauksen murtamisen vaikeutta haluamallasi tavalla.

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Administrative Console** (HP ProtectToolsin hallintakonsoli).
2. Valitse **Devices** (Laitteet) ja sitten **Face** (Kasvot).

3. Voit parantaa käyttömukavuutta napsauttamalla liukusäädintä ja siirtämällä sitä vasemmalle tai lisätä tarkkuutta napsauttamalla liukusäädintä ja siirtämällä sitä oikealle.

   - **Convenience** (Käyttömukavuus) – Jos haluat helpottaa tietokoneen käyttöä epävarmoissa tilanteissa, napsauta liukusäädintä ja siirrä se **Convenience** (Käyttömukavuus) -asentoon.
   - **Balance** (Tasapaino) – Jos haluat varmistaa hyvän tasapainon suojauksen ja käytettävyyden välillä, tietokoneessa on arkaluonteisia tietoja tai tietokone on sellaisessa paikassa, jossa sitä voidaan käyttää luvattomasti, napsauta liukusäädintä ja siirrä se **Balance** (Tasapaino) -asentoon.
   - **Accuracy** (Tarkkuus) – Jos haluat vaikeuttaa tietokoneen käyttöä, kun rekisteröidyt kohteet tai vallitsevat valaistusolosuhteet ovat normaalia heikommat ja virheellinen hyväksyntä on tavallista epätodennäköisempää, napsauta liukusäädintä ja siirrä se **Accuracy** (Tarkkuus) -asentoon.

HUOMAUTUS: Suojaustaso koskee kaikkia käyttäjiä.

4. Valitse **Apply** (Käytä).

Lisäasetukset

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Administrative Console** (HP ProtectToolsin hallintakonsoli).
2. Valitse **Devices** (Laitteet) ja sitten **Face** (Kasvot).
3. Valitse **Advanced** (Lisäasetukset).

   - **Do not require user name for Windows logon. (Älä vaadi käyttäjänimeä Windows-kirjautumiseen.)**
     - Valitse valintaruutu, jos haluat antaa käyttäjille mahdollisuuden kirjautua Windowsiin ilman käyttäjänimeä.
     - Poista valintaruudun valinta, jos haluat vaatia käyttäjänimeä kirjautumiseen.
   - **Enforce the use of PIN for face logon** (Vaadi PIN-koodia kirjautumiseen kasvojen avulla) – Valitse valintaruutu, jos haluat, että jokainen käyttäjä määrittää PIN-koodin (Personal Identification Number) ja käyttää sitä kirjautumiseen.
     - **Minimum length allowed for PIN** (PIN-koodin pituuden vähimmäismäärä) – Napsauta ylänuolta, jos haluat lisätä PIN-koodiin vaadittavien merkkien vähimmäismäärää, tai alanuolta, jos haluat vähentää sitä.
     - **Maximum length allowed for PIN** (PIN-koodin pituuden enimmäismäärä) – Napsauta ylänuolta, jos haluat lisätä PIN-koodiin vaadittavien merkkien enimmäismäärää, tai alanuolta, jos haluat vähentää sitä.
     - **Maximum retries allowed for PIN** (PIN-koodin antamisyritysten enimmäismäärä) – Napsauta ylänuolta, jos haluat lisätä PIN-koodin antamisyritysten enimmäismäärää, tai alanuolta, jos haluat vähentää sitä.
4. Valitse **OK**.

5 Sovellusten asetusten määrittäminen

Applications (Sovellukset) -ryhmä avataan HP ProtectToolsin hallintakonsolin vasemmalla puolella olevasta Security Applications (Suojaussovellukset) -valikkopaneelista. Settings (Asetukset) -toiminnoilla voit mukauttaa asennettujen HP ProtectTools Security Manager -sovellusten toimintatapaa.

Voit muuttaa sovellusten asetuksia seuraavasti:

1. Valitse Tools (Työkalut) -valikon **Applications** (Sovellukset) -ryhmästä **Settings** (Asetukset).
2. Ota haluamasi asetus käyttöön tai poista se käytöstä napsauttamalla sitä.
3. Tallenna muutokset valitsemalla **Apply** (Käytä).

General (Yleiset) -välilehti

General (Yleiset) -välilehdessä ovat käytettävissä seuraavat asetukset:

- **Do not automatically launch the Setup Wizard for administrators** (Älä automaattisesti käynnistä ohjattua asennustoimintoa järjestelmänvalvojia varten) – Valitse tämä asetus, jos haluat estää ohjattua toimintoa avautumasta automaattisesti kirjauduttaessa.
- **Do not automatically launch the Getting Started for users** (Älä automaattisesti käynnistä ohjattua aloitustoimintoa käyttäjiä varten) – Valitse tämä asetus, jos haluat estää käyttäjien asetusten määritystoimintoa avautumasta automaattisesti kirjauduttaessa.

Applications (Sovellukset) -välilehti

Täällä näkyvien asetusten avulla voit määrittää, milloin Security Manageriin lisätään uusia sovelluksia. Oletusarvoisesti näytettävät vähimmäisasetukset ovat seuraavat:

- **Applications status** (Sovellusten tila) – Mahdollistaa kaikkien sovellusten tilan näyttämisen.
- **Password Manager** (Salasanojen hallinta) – Ottaa Password Manager (Salasanojen hallinta) -sovelluksen kaikille tietokoneen käyttäjille käyttöön.
- **Privacy Manager** (Yksityisyyden hallinta) – Ottaa Privacy Manager (Yksityisyyden hallinta) -sovelluksen kaikille tietokoneen käyttäjille käyttöön.
- **Enable the Discover more button** (Ota Discover More (Etsi lisää) -painike käyttöön) – Antaa tietokoneen käyttäjille mahdollisuuden lisätä sovelluksia HP ProtectTools Security Manageriin napsauttamalla **[+] Discover more** ([+] Etsi lisää) -painiketta.

Jos haluat palauttaa kaikkien sovellusten tehdasasetukset, napsauta **Restore Defaults** (Palauta oletukset) -painiketta.

6 Hallintatyökalut

Käytettävissä voi olla muitakin sovelluksia, joiden avulla Security Manageriin voidaan lisätä uusia hallintatyökaluja. Tietokoneen järjestelmänvalvoja poistaa tämän toiminnon käytöstä Settings (Asetukset) -sovelluksen kautta.

Jos haluat lisätä uusia hallintatyökaluja, valitse **[+] Management tools** ([+] Hallintatyökalut).

Päivitykset ja viestit

Jos käytettävissäsi on Internet-yhteys, DigitalPersona-sivustossa osoitteessa http://www.digitalpersona.com/ voit etsiä uusia sovelluksia tai ajoittaa automaattisia päivityksiä.

1. Jos haluat saada tietoja uusista sovelluksista ja päivityksistä, valitse **Keep me informed about new applications and updates** (Ilmoita uusista sovelluksista ja päivityksistä) -valintaruutu.
2. Jos haluat ajoittaa automaattisia päivityksiä, valitse päivien määrä.
3. Voit hakea päivityksiä valitsemalla **Check Now** (Hae nyt).

7 HP ProtectTools Security Manager

HP ProtectTools Security Manager parantaa merkittävästi tietokoneen suojausta.

Voit käyttää valmiiksi ladattuja Security Manager -sovelluksia sekä Internetistä välittömästi ladattavissa olevia muita sovelluksia, joiden avulla voit

- hallita kirjautumistunnusta ja salasanoja
- helposti vaihtaa Windows®-käyttöjärjestelmän salasanan
- määrittää ohjelman asetukset
- käyttää suojausta ja käyttömukavuutta parantavia sormenjälkiä
- rekisteröidä yhden tai useamman kohteen todennusta varten
- asentaa älykortin todennusta varten
- varmuuskopioida ja palauttaa ohjelmatietoja
- lisätä uusia sovelluksia.

HP ProtectTools Security Managerin avaaminen

Voit avata HP ProtectTools Security Managerin jollakin seuraavista tavoista:

- Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Security Manager**.
- Kaksoisnapsauta tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **HP ProtectTools** -kuvaketta.
- Napsauta hiiren kakkospainikkeella **HP ProtectTools** -kuvaketta ja valitse **Open HP ProtectTools Security Manager**.
- Napsauta Windowsin sivupalkissa olevaa **Security Manager ID Card** -pienoisohjelmaa.
- Avaa Security Manager Quick Links (Security Managerin pikalinkit) -valikko painamalla pikanäppäinyhdistelmää ctrl+Windows+h.

Security Managerin kojelaudan käyttäminen

Security Managerin kojelauta mahdollistaa Security Managerin toimintojen, sovellusten ja asetusten keskitetyn ja vaivattoman käytön.

▲ Voit avata Security Managerin kojelaudan valitsemalla **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Security Manager**.

Kojelauta muodostuu seuraavista osista:

- **ID Card** (Henkilökortti) – Näyttää Windowsin käyttäjänimen ja valitun kuvan, joita käytetään kirjautuneen käyttäjän tunnistamiseen.
- **Security Applications** (Suojaussovellukset) – Näyttää seuraavien suojausluokkien määrittämiseen käytettävien linkkien avautuvan valikon:
  - **Credential Manager (Valtuustietojen hallinta)**
  - **My Data (Omat tiedot)**
- **Discover more** (Etsi lisää) – Avaa sivun, jolta löydät lisää omien henkilötietojen, tietojen ja viestinnän suojausta parantavia sovelluksia.
- **Main area** (Pääalue) – Näyttää sovelluskohtaisia näyttöä.
- **Administration** (Hallinta) – Avaa HP ProtectToolsin hallintakonsolin.
- **Help button** (Ohje-painike) – Näyttää tietoja nykyisestä näytöstä.
- **Advanced** (Lisäasetukset) – Mahdollistaa seuraavien asetusten käytön:
  - **Preferences** (Asetukset) – Mahdollistaa Security Managerin asetusten mukauttamisen.
  - **Backup and Restore** (Varmuuskopiointi ja palautus) – Mahdollistaa tietojen varmuuskopioinnin tai palautuksen.
  - **About** (Tietoja) – Näyttää Security Managerin versiotiedot.

Asennusohjeet

Valtuustietojen rekisteröinti

My Identity (Omat henkilötiedot) -sivulla voit ottaa erilaisia todennustapoja tai valtuustietoja käyttöön. Kun ne on rekisteröity, voit käyttää niitä kirjautuessasi Security Manageriin.

Sormenjälkien rekisteröinti

Jos tietokoneessa on sormenjäljenlukija sisäänrakennettuna tai kytkettynä, HP ProtectTools Security Managerin ohjattu asennustoiminto antaa sormenjälkien käyttöönottoa tai rekisteröintiä koskevia neuvoja.

1. Näyttöön tulevat kahden käden ääriviivat. Aikaisemmin rekisteröidyt sormet on merkitty vihreällä. Napsauta ääriviivalla merkityllä alueella olevaa sormea.

   HUOMAUTUS: Jos haluat poistaa aikaisemmin rekisteröidyn sormenjäljen, napsauta sitä vastaavaa sormea.

2. Kun olet valinnut rekisteröitävän sormen, sinua kehotetaan skannaamaan sitä, kunnes sormenjäljen rekisteröinti onnistuu. Rekisteröity sormi näkyy ääriviivalla merkityllä alueella vihreänä.

3. Sinun on rekisteröitävä vähintään kaksi sormea, joista suositeltavimmat ovat etusormi ja keskisormi. Toista toisen sormen osalta vaiheet 1–3.

4. Valitse **Next** (Seuraava) ja toimi näyttöön tulevien ohjeiden mukaan.

HUOMAUTUS: Kun rekisteröit sormenjälkiä Getting Started (Käytön aloittaminen) -toiminnon avulla, sormenjälkitietoja ei tallenneta, ennen kuin valitset **Next** (Seuraava). Jos tietokonetta ei käytetä vähään aikaan tai ohjelma suljetaan, muutoksia **ei** tallenneta.

Kohteiden rekisteröinti

Sinun on rekisteröitävä vähintään yksi kohde, jos haluat kirjautua kasvojen avulla.

Voit rekisteröidä uuden kohteen HP ProtectTools Security Managerin ohjatun asennustoiminnon avulla seuraavasti:

1. Napsauta näytön oikeassa reunassa olevan sivupalkin **HP ProtectTools Security Manager** -kuvaketta.

2. Anna Windows®-salasanasi ja valitse **Next** (Seuraava).

3. Valitse **Enable security features** (Ota suojaustoiminnot käyttöön), **Windows Logon Security** (Windows-kirjautumisen suojaus) -valintaruutu ja sitten **Next** (Seuraava).

4. Valitse **Choose your credentials** (Valitse valtuustiedot) -kohdasta **Face** (Kasvot) -valintaruutu ja sitten **Next** (Seuraava).

5. Valitse **Enroll a new scene** (Rekisteröi uusi kohde).

Onnistuneen rekisteröinnin jälkeen voit rekisteröidä myös uuden kohteen, jos kirjautumisessa on ilmennyt ongelmia seuraavien olosuhteiden muuttumisen vuoksi:

- Kasvosi ovat muuttuneet merkittävästi edellisen rekisteröintikerran jälkeen.
- Valaistus on hyvin erilainen kuin edellisillä rekisteröintikerroilla.
- Käytit (tai et käyttänyt) silmälaseja edellisen rekisteröinnin aikana.

HUOMAUTUS: Jos kohteiden rekisteröinti on vaikeaa, yritä siirtyä lähemmäksi verkkokameraa. Valaistus ja kontrasti ovat erittäin tärkeitä, kuten valokuvauksessa ja videokuvauksessa yleensä. Varmista kuvauksen aikana, että valo tulee ensisijaisesti edestä eikä takaa. Jos huomaat, että kasvontunnistustoiminnolla on vaikeuksia todentaa sinua, yritä rekisteröidä kohde paremmassa valaistuksessa uudelleen.

Voit rekisteröidä uuden kohteen HP ProtectTools Security Managerin avulla seuraavasti:

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Security Manager**.
2. Valitse **Credentials** (Valtuustiedot) ja sitten **Face** (Kasvot).
3. Valitse **Enroll a new scene** (Rekisteröi uusi kohde).

Käyttäjien lisäasetukset

1. Valitse **Käynnistä**, **Kaikki ohjelmat** ja sitten **HP ProtectTools Security Manager**.
2. Valitse **Set up your authentication credentials** (Määritä todennukseen käytettävät valtuustiedot) ja sitten **Face** (Kasvot).
3. Napsauta **Advanced** (Lisäasetukset) -painiketta ja valitse jokin seuraavista vaihtoehdoista.

   a. Jos haluat vaatia PIN-koodia kirjautumiseen kasvojen avulla, valitse **Create PIN** (Luo PIN-koodi), anna Windows-salasanasi, anna uusi PIN-koodi ja vahvista uusi PIN-koodi antamalla se uudelleen.

   b. Valitse tarvittaessa myös muita asetuksia. Nämä asetukset koskevat vain nykyistä käyttäjää:

   - **Play sound on face recognition events (Toista ääni kasvontunnistustapahtumien yhteydessä)**
     - Valitse valintaruutu, jos haluat toistaa äänen kasvontunnistuksen onnistuessa tai epäonnistuessa.
     - Poista asetus käytöstä poistamalla valintaruudun valinta.
   - **Prompt to update scenes when logon fails (Kehota päivittämään kohteet kirjautumisen epäonnistuessa)**
     - Valitse valintaruutu, jos haluat sallia käyttäjälle kohteiden päivittämisen, jos kirjautuminen kasvojen avulla epäonnistuu. Jos todennus saavuttaa ”ehkä”-kynnyksen, käyttäjää kehotetaan päättämään, lisätäänkö ”epäonnistuneen” kirjautumisen suorat kuvat nykyiseen kohteeseen, mikä parantaa kirjautumisen onnistumismahdollisuuksia seuraavalla kerralla.
     - Poista asetus käytöstä poistamalla valintaruudun valinta.
   - **Prompt to enroll a new scene when logon fails (Kehota rekisteröimään uusi kohde kirjautumisen epäonnistuessa)**
     - Valitse valintaruutu, jos haluat näyttää käyttäjälle kehotteen rekisteröidä uusi kohde, jos kirjautuminen kasvojen avulla epäonnistuu eikä todennus saavuta ”ehkä”-kynnystä. Tämä voi parantaa kirjautumisen onnistumismahdollisuuksia seuraavalla kerralla.
     - Poista asetus käytöstä poistamalla valintaruudun valinta.

   c. Jos haluat rekisteröidä uuden kohteen, valitse **Enroll a new scene** (Rekisteröi uusi kohde) ja toimi näyttöön tulevien ohjeiden mukaan.

Windows-salasanan vaihtaminen

Security Managerin avulla voit vaihtaa Windows-salasanasi helpommin ja nopeammin kuin Windowsin Ohjauspaneelin kautta.

Voit vaihtaa Windows-salasanan seuraavasti:

1. Valitse Security Managerin kojelaudasta **Credentials** (Valtuustiedot) ja sitten **Password** (Salasana).
2. Kirjoita nykyinen salasana **Current Windows password** (Nykyinen Windows-salasana) -tekstiruutuun.

3. Kirjoita uusi salasana **New Windows password** (Uusi Windows-salasana) -tekstiruutuun ja sitten uudelleen **Confirm new password** (Vahvista uusi salasana) -tekstiruutuun.

4. Valitse **Change** (Vaihda), niin nykyisen salasanasi tilalle vaihdetaan välittömästi antamasi salasana.

Älykortin asentaminen

Jos valitset kirjautumisen älykortin avulla ja tietokoneessa on älykortinlukija sisäänrakennettuna tai kytkettynä, Security Managerin ohjattu asennustoiminto kehottaa sinua määrittämään älykortin PIN-koodin (Personal Identification Number).

Voit asentaa älykortin seuraavasti:

1. Anna ja vahvista PIN-koodi **Set up smart card** (Asenna älykortti) -kohdassa.

   Voit myös muuttaa PIN-koodia. Anna nykyinen PIN-koodi ja kirjoita sen tilalle uusi.

2. Jatka valitsemalla **Next** (Seuraava) ja toimi näyttöön tulevien ohjeiden mukaan.

TAI

▲ Valitse Security Managerin kojelaudasta **Credentials** (Valtuustiedot) ja sitten **Smart Card** (Älykortti).

- Älykortin PIN-koodin määrittäminen – Anna ja vahvista PIN-koodi **Set up smart card** (Asenna älykortti) -sivulla.
- PIN-koodin muuttaminen – Anna ensin nykyinen PIN-koodi, kirjoita sen tilalle uusi ja vahvista se.

Yleiset toiminnot

Tähän ryhmään kuuluvien sovellusten avulla voit hallita digitaalisen henkilöllisyytesi erilaisia aspekteja.

- **Security Manager** – Tällä toiminnolla voit luoda ja hallita pikalinkkejä, joiden avulla voit avata sivustoja ja ohjelmia sekä kirjautua niihin todentamalla henkilöllisyytesi Windows-salasanan, sormenjäljen tai älykortin avulla.
- **Credentials** (Valtuustiedot) – Tällä toiminnolla voit helposti vaihtaa Windows-salasanan, rekisteröidä sormenjälkiä tai asentaa älykortin.

Jos haluat lisätä muita sovelluksia, napsauta kojelaudan vasemmassa alakulmassa olevaa [+] **Discover more** (Tutustu tarkemmin) -painiketta. Järjestelmänvalvoja voi poistaa tämän painikkeen käytöstä.

Password Manager

Password Managerilla kirjautuminen Windowsiin, sivustoihin ja sovelluksiin on entistä helpompaa ja turvallisempaa. Sen avulla voit luoda aiempaa vahvempia salasanoja, joita ei tarvitse kirjoittaa ylös tai muistaa, ja sen jälkeen kirjautua nopeasti sormenjäljellä, älykortilla tai Windows-salasanalla.

Password Managerilla voit

- lisätä, muokata tai poistaa kirjautumistunnuksia Manage (Hallitse) -välilehdestä
- käynnistää oletusselaimen ja kirjautua mihin tahansa sivustoon tai ohjelmaan niiden asetusten määrittämisen jälkeen pikalinkkien avulla
- järjestellä pikalinkit luokkiin vetämällä ja pudottamalla
- tarkistaa yhdellä vilkaisulla, vaarantavatko salasanasi tietoturvan, ja luoda automaattisesti monimutkaisen vahvan salasanan käytettäväksi uusien sivustojen kanssa.

Monet Password Managerin toiminnoista ovat käytettävissä myös napsauttamalla Password Manager -kuvaketta, joka tulee näyttöön, kun verkkosivu tai ohjelman kirjautumisnäyttö on avattuna. Kuvaketta napsauttamalla voit avata pikavalikon, jossa voit valita jonkin seuraavista vaihtoehdoista.

Verkkosivut tai ohjelmat, joissa kirjautumistunnusta ei ole vielä luotu

Pikavalikossa näkyvät seuraavat vaihtoehdot:

- **Add [somedomain.com] to the Password Manager** (Lisää [jokintoimialue.com] Password Manageriin) – Mahdollistaa kirjautumistunnuksen luonnin nykyistä kirjautumisnäyttöä varten.
- **Open Password Manager** (Avaa Password Manager) – Käynnistää Password Managerin.
- **Icon settings** (Kuvakkeen asetukset) – Mahdollistaa niiden tilanteiden määrittämisen, joissa Password Manager -kuvake tulee näyttöön.
- **Help** (Ohje) – Näyttää Password Manager -ohjelmiston ohjeen.

Verkkosivut tai ohjelmat, joissa kirjautumistunnus on jo luotu

Pikavalikossa näkyvät seuraavat vaihtoehdot:

- **Fill in logon data** (Täytä kirjautumistiedot) – Lisää kirjautumistiedot kirjautumiskenttiin ja lähettää sivun (jos lähetys määritettiin, kun kirjautumistunnus luotiin tai sitä viimeksi muokattiin).
- **Edit logon** (Muokkaa kirjautumistunnusta) – Mahdollistaa tämän sivuston kirjautumistietojen muokkaamisen.
- **Add a New Account** (Lisää uusi tili) – Mahdollistaa tilin lisäämisen kirjautumistunnukseen.
- **Open Password Manager** (Avaa Password Manager) – Käynnistää Password Manager -sovelluksen.
- **Help** (Ohje) – Näyttää Password Manager -ohjelmiston ohjeen.

HUOMAUTUS: Tietokoneen järjestelmänvalvoja on voinut määrittää Security Managerin vaatimaan useita valtuustietoja henkilöllisyyttä tarkistettaessa.

Kirjautumistunnusten lisääminen

Voit helposti lisätä sivuston tai ohjelman kirjautumistunnuksen antamalla kirjautumistiedot kerran. Tämän jälkeen Password Manager lisää tiedot puolestasi automaattisesti. Voit käyttää näitä kirjautumistunnuksia sen jälkeen, kun olet avannut sivuston tai ohjelman, tai napsauttaa **Logons** (Kirjautumistunnukset) -valikossa olevaa kirjautumistunnusta, jolloin Password Manager avaa sivuston tai ohjelman ja kirjaa sinut sisään.

Voit lisätä kirjautumistunnuksen seuraavasti:

1. Avaa sivuston tai ohjelman kirjautumisnäyttö.
2. Napsauta **Password Manager** -kuvakkeen päällä olevaa kuvaketta ja sitten jotakin seuraavista sen mukaan, onko kyseessä sivuston vai ohjelman kirjautumisnäyttö.
   - Jos kyseessä on sivusto, valitse **Add [domain name] to Password Manager** (Lisää [toimialueen nimi] Password Manageriin).
   - Jos kyseessä on ohjelma, valitse **Add this logon screen to Password Manager** (Lisää tämä kirjautumisnäyttö Password Manageriin).
3. Anna kirjautumistiedot. Näytön kirjautumiskentät ja niitä vastaavat valintaikkunan kentät on osoitettu paksulla oranssilla kehyksellä. Voit avata tämän valintaikkunan myös napsauttamalla **Password Manager Manage** (Password Managerin hallinta) -välilehden **Add Logon** (Lisää kirjautumistunnus) -painiketta. Jotkin asetukset vaihtelevat tietokoneeseen kytkettyjen suojauslaitteiden mukaan, esimerkiksi ctrl+Windows+h-pikanäppäintä käytetään sormenjäljen skannaamiseen tai älykortin asettamiseen.
   a. Jos haluat täyttää kirjautumiskentän jollakin valmiiksi muotoillulla vaihtoehdolla, napsauta kentän oikealla puolella olevia nuolia.
   b. Jos haluat tarkastella kirjautumistunnuksen salasanaa, valitse **Show password** (Näytä salasana).
   c. Jos haluat täyttää kirjautumiskentät, mutta et lähettää niitä, poista **Automatically submit logon data** (Lähetä kirjautumistiedot automaattisesti) -valintaruudun valinta.

d. Valitse **OK**, napsauta haluamaasi todennustapaa vaihtoehdoista **Fingerprints** (Sormenjäljet), **Password** (Salasana) tai **Face** (Kasvot) ja kirjaudu valittua todennustapaa käyttäen.

   Plusmerkki poistetaan Password Manager -kuvakkeen päältä, mikä osoittaa, että kirjautumistunnus on luotu.

e. Jos Password Manager ei tunnista kirjautumiskenttiä, valitse **More fields** (Lisää kenttiä).

   i. Valitse kunkin kirjautumiseen vaadittavan kentän valintaruutu tai poista niiden kenttien valintaruudut, joita ei vaadita kirjautumiseen.

   ii. Jos Password Manager ei tunnista kaikkia kirjautumiskenttiä, näyttöön tulee viesti, jossa kysytään, että haluatko jatkaa. Valitse **Yes** (Kyllä).

   iii. Näyttöön tulee valintaikkuna, jonka kirjautumiskentät on täytetty. Napsauta kunkin kentän kuvaketta, vedä kuvakkeet oikeisiin kirjautumiskenttiin ja kirjaudu sivustoon napsauttamalla painiketta.

   HUOMAUTUS: Jos olet antanut sivuston kirjautumistiedot manuaalisessa tilassa, sinun on myös myöhemmin kirjauduttava sivustoon samalla tavalla.

   HUOMAUTUS: Kirjautumistiedot voidaan antaa manuaalisessa tilassa vain Internet Explorer 8:ssa.

   iv. Valitse **Close** (Sulje).

Kun avaat kyseisen sivuston tai ohjelman, Password Manager -kuvake tulee näkyviin ja osoittaa, että voit kirjautua rekisteröimilläsi valtuustiedoilla.

Kirjautumistunnusten muokkaaminen

Voit muokata kirjautumistunnusta seuraavasti:

1. Avaa sivuston tai ohjelman kirjautumisnäyttö.
2. Avaa kirjautumistietojen muokkausvalintaikkuna napsauttamalla **Password Manager** -kuvakkeen päällä olevaa nuolta ja valitsemalla sitten **Edit logon** (Muokkaa kirjautumistunnusta). Näytön kirjautumiskentät ja niitä vastaavat valintaikkunan kentät on osoitettu paksulla oranssilla kehyksellä.

   Voit avata tämän valintaikkunan myös napsauttamalla **Password Manager Manage** (Password Managerin hallinta) -välilehden **Edit for the desired logon** (Muokkaa haluttua kirjautumistunnusta) -painiketta.
3. Muokkaa kirjautumistietoja.

   - Jos haluat täyttää kirjautumiskentän jollakin valmiiksi muotoillulla vaihtoehdolla, napsauta kentän oikealla puolella olevia nuolia.
   - Jos haluat lisätä kenttiä näytöstä kirjautumistunnukseen, napsauta **More fields** (Lisää kenttiä) -painiketta.

- Jos haluat täyttää kirjautumiskentät, mutta et lähettää niitä, poista **Submit logon data** (Lähetä kirjautumistiedot) -valintaruudun valinta.
- Jos haluat tarkastella kirjautumistunnuksen salasanaa, valitse **Show password** (Näytä salasana).

4. Valitse **OK**.

Logons (Kirjautumistunnukset) -valikon käyttäminen

Password Manager tarjoaa nopean ja helpon tavan avata sivustot ja ohjelmat, joita varten olet luonut kirjautumistunnukset. Avaa kirjautumisnäyttö kaksoisnapsauttamalla ohjelman tai sivuston kirjautumistunnusta **Logons** (Kirjautumistunnukset) -valikossa tai **Password Manager** -sovelluksen **Manage** (Hallinta) -välilehdessä.

Kun luot kirjautumistunnuksen, se lisätään automaattisesti Password Manager Logons (Password Managerin kirjautumistunnukset) -valikkoon.

Voit avata Logons (Kirjautumistunnukset) -valikon seuraavasti:

1. Paina **Password Manager** -pikanäppäinyhdistelmää. Tehdasasetus on ctrl+Windows+h. Jos haluat vaihtaa pikanäppäinyhdistelmää, valitse **Password Manager** ja sitten **Settings** (Asetukset).
2. Skannaa sormenjälkesi (tietokoneissa, joissa on sormenjäljenlukija sisäänrakennettuna tai kytkettynä).

Kirjautumistunnusten järjesteleminen luokkiin

Luomalla yhden tai useamman luokan voit pitää kirjautumistunnukset järjestyksessä. Vedä ja pudota sen jälkeen kirjautumistunnukset haluamiisi luokkiin.

Voit lisätä luokan seuraavasti:

1. Valitse Security Managerin kojelaudasta **Password Manager**.
2. Valitse **Manage** (Hallinta) -välilehti ja sitten **Add Category** (Lisää luokka).
3. Anna luokalle nimi.
4. Valitse **OK**.

Voit lisätä kirjautumistunnuksen luokkaan seuraavasti:

1. Aseta hiiren osoitin haluamasi kirjautumistunnuksen päälle.
2. Paina hiiren ykköspainiketta ja pidä sitä painettuna.
3. Vedä kirjautumistunnus luokkien luettelon päälle. Luokat korostetaan, kun siirrät hiiren niiden päälle.
4. Vapauta hiiren painike, kun haluttu luokka on korostettuna.

Kirjautumistunnuksia ei siirretä, vaan ne ainoastaan kopioidaan valittuun luokkaan. Voit lisätä saman kirjautumistunnuksen useampaan kuin yhteen luokkaan ja näyttää kaikki kirjautumistunnukset valitsemalla **All** (Kaikki).

Kirjautumistunnusten hallinta

Password Managerin avulla voit hallita kirjautumistietoja, kuten käyttäjänimiä, salasanoja ja useita kirjautumistilejä, helposti yhdestä keskitetystä paikasta.

Kirjautumistunnukset on lueteltu Manage (Hallinta) -välilehdessä. Jos samaa sivustoa varten on luotu useita kirjautumistunnuksia, jokainen kirjautumistunnus on annettu sivuston nimen kohdalla ja sisennetty kirjautumisluettelossa.

Voit hallita kirjautumistunnuksia seuraavasti:

Valitse Security Managerin kojelaudasta **Password Manager** ja sitten **Manage** (Hallinta) -välilehti.

- **Add a logon** (Lisää kirjautumistunnus) – Valitse **Add Logon** (Lisää kirjautumistunnus) ja toimi näyttöön tulevien ohjeiden mukaan.
- **Edit a logon** (Muokkaa kirjautumistunnusta) – Valitse **Edit** (Muokkaa) ja muuta kirjautumistietoja.
- **Delete a logon** (Poista kirjautumistunnus) – Valitse kirjautumistunnus ja sitten **Delete** (Poista).

Voit lisätä sivustoa tai ohjelmaa varten toisen kirjautumistunnuksen seuraavasti:

1. Avaa sivuston tai ohjelman kirjautumisnäyttö.
2. Avaa pikavalikko napsauttamalla **Password manager** -kuvaketta.
3. Valitse **Add additional logon** (Lisää toinen kirjautumistunnus) ja toimi näyttöön tulevien ohjeiden mukaan.

Salasanan vahvuuden arvioiminen

Vahvojen salasanojen käytöllä sivustoihin ja ohjelmiin kirjauduttaessa on tärkeä tehtävä yksityisyytesi suojaamisessa.

Password Manager helpottaa suojauksen valvontaa ja tehostamista arvioimalla välittömästi ja automaattisesti sivustoihin ja ohjelmiin kirjautumiseen käytettävien salasanojen vahvuutta.

Password Manager -kuvakkeen asetukset

Password Manager yrittää tunnistaa sivustojen ja ohjelmien kirjautumisnäytöt. Kun Password Manager havaitsee kirjautumisnäytön, jota varten et ole luonut kirjautumistunnusta, se kehottaa sinua lisäämään kirjautumistunnuksen näyttöön lisäämällä Password Manager -kuvakkeeseen plusmerkin (+).

Napsauta kuvakkeen nuolta ja valitse **Icon Settings** (Kuvakkeen asetukset), jolloin voit määrittää, miten **Password Manager** käsittelee mahdollisia kirjautumissivustoja.

- **Prompt to add logons for logon screens** (Kehota lisäämään kirjautumistunnuksia kirjautumisnäyttöihin) – Valitse tämä vaihtoehto, jos haluat Password Managerin kehottavan sinua lisäämään kirjautumistunnuksen, kun näyttöön avautuu kirjautumisnäyttö, jota varten ei ole vielä luotu kirjautumistunnusta.
- **Exclude this screen** (Ohita tämä näyttö) – Jos valitset tämän valintaruudun, Password Manager ei enää kehota sinua lisäämään kirjautumistunnusta tätä kirjautumisnäyttöä varten.

Jos haluat avata muut Password Managerin asetukset, valitse **Password Manager** ja sitten Security Managerin kojelaudasta **Settings** (Asetukset).

Asetukset

Voit mukauttaa HP ProtectTools Security Managerin toimintatapaa määrittämällä sen asetukset:

1. **Prompt to add logons for logon screens** (Kehota lisäämään kirjautumistunnuksia kirjautumisnäyttöihin) – Kun sovellus havaitsee sivuston tai ohjelman kirjautumisnäytön, Password Manager -kuvake ja plusmerkki tulevat näyttöön. Tämä osoittaa, että voit määrittää kirjautumistunnuksen sivustoa varten ja lisätä sen salasanasäilöön. Voit poistaa tämän toiminnon käytöstä poistamalla **Icon Settings** (Kuvakkeen asetukset) -valintaikkunassa olevan **Prompt to add logons for logon screens** (Kehota lisäämään kirjautumistunnuksia kirjautumisnäyttöihin) -valintaruudun valinnan.
2. **Open Password Manager with ctrl+Windows+h** (Avaa Password Manager painamalla ctrl +Windows+h) – Password Managerin pikalinkkivalikko avataan oletusarvoisesti pikanäppäimellä ctrl+Windows+h. Jos haluat vaihtaa pikanäppäintä, napsauta tätä vaihtoehtoa ja määritä uusi näppäinyhdistelmä. Yhdistelmässä voi olla yksi tai useampi seuraavista: ctrl, alt tai shift ja mikä tahansa kirjain- tai numeronäppäin.
3. Tallenna muutokset valitsemalla **Apply** (Käytä).

Valtuustiedot

Security Managerin valtuustietojen avulla varmistetaan, että sinä olet todellakin sinä. Tietokoneen paikallinen järjestelmänvalvoja voi määrittää, mitä valtuustietoja henkilöllisyytesi todentamiseen käytetään, kun kirjaudut Windows-tilillesi, sivustoihin tai ohjelmiin.

Käytettävissä olevat valtuustiedot voivat vaihdella tietokoneessa olevien tai siihen kytkettyjen suojauslaitteiden mukaan. Jokaisesta tuetusta valtuustiedosta on merkintä **My Identity, Credentials** (Oma henkilöllisyys, valtuustiedot) -ryhmässä.

Sovelluksessa on annettu käytettävissä olevat valtuustiedot sekä niiden vaatimukset ja nykyinen tila. Niihin voivat kuulua

- sormenjäljet
- salasana
- älykortti
- kasvot.

Voit rekisteröidä valtuustiedon tai muuttaa sitä napsauttamalla linkkiä ja toimimalla näyttöön tulevien ohjeiden mukaan.

Oma henkilökorttisi

Oma henkilökorttisi, jossa näkyvät nimesi ja haluamasi kuva, osoittaa yksilöllisellä tavalla, että olet tämän Windows-tilin omistaja. Se näkyy selvästi Security Manager -sivujen vasemmassa yläkulmassa ja Windowsin sivupalkin pienoisohjelmana.

Henkilökortin napsauttaminen Windowsin sivupalkissa on yksi monista tavoista, joilla voit käyttää Security Manageria nopeasti.

Voit muuttaa kuvaa ja nimesi näyttötapaa. Oletusarvoisesti käytetään Windowsin täydellistä käyttäjänimeä ja Windowsin asennuksen yhteydessä valittua kuvaa.

Voit muuttaa näytössä näkyvää nimeä seuraavasti:

1. Valitse Security Managerin kojelaudan vasemmasta yläkulmasta **ID Card** (Henkilökortti) -kuvake.
2. Napsauta valintaruutua, jossa näkyy Windows-tilille antamasi nimi. Järjestelmä näyttää tälle tilille määritetyn Windowsin käyttäjänimen.
3. Jos haluat muuttaa tätä nimeä, kirjoita uusi nimi ja napsauta **Save** (Tallenna) -painiketta.

Voit muuttaa näytössä näkyvää kuvaa seuraavasti:

1. Valitse Security Managerin kojelaudan vasemmasta yläkulmasta **ID Card** (Henkilökortti).
2. Napsauta **Choose picture** (Valitse kuva) -painiketta, valitse kuva ja napsauta **Save** (Tallenna) -painiketta.

Omien asetusten määrittäminen

Voit mukauttaa HP ProtectTools Security Managerin asetukset. Valitse Security Managerin kojelaudasta **Advanced** (Lisäasetukset) ja sitten **Preferences** (Omat asetukset). Käytettävissä olevat asetukset näkyvät kahdessa välilehdessä: General (Yleiset) ja Fingerprint (Sormenjälki).

General (Yleiset)

General (Yleiset) -välilehdessä ovat käytettävissä seuraavat asetukset:

Appearance (Ulkoasu) – **Show icon on taskbar** (Näytä kuvake tehtäväpalkissa)

- Valitse valintaruutu, jos haluat näyttää kuvakkeen tehtäväpalkissa.
- Poista valintaruudun valinta, jos et halua näyttää kuvaketta tehtäväpalkissa.

Fingerprint (Sormenjälki)

Fingerprint (Sormenjälki) -välilehdessä ovat käytettävissä seuraavat asetukset:

- **Quick Actions** (Pikatoiminnot) – Quick Actions (Pikatoiminnot) -toiminnon avulla voit valita Security Manager -tehtävän, joka suoritetaan, kun painat tiettyä näppäintä sormenjäljen skannaamisen aikana.

  Jos haluat määrittää pikatoiminnon luettelossa oleville näppäimille, valitse **(Key)+Fingerprint** ((Näppäin)+Sormenjälki) -vaihtoehto ja sitten jokin valikon käytettävissä olevista toiminnoista.

- **Fingerprint Scan Feedback** (Sormenjäljen skannauksen palaute) – Näkyy vain silloin, jos sormenjäljenlukija on käytettävissä. Tämän asetuksen avulla voit säätää sormenjälkeä skannattaessa annettavaa palautetta.

  - **Enable sound feedback** (Ota äänipalaute käyttöön) – Security Manager antaa sinulle mahdollisuuden käyttää äänipalautetta sormenjäljen skannaamisen jälkeen toistamalla erilaisia ääniä tiettyjen ohjelmatapahtumien jälkeen. Voit liittää näihin tapahtumiin uusia ääniä Windowsin Ohjauspaneelin Äänet-välilehdessä tai poistaa äänipalautteen käytöstä poistamalla tämän asetuksen valinnan.

  - **Show scan quality feedback (Näytä skannauksen laatupalaute)**

    Valitse valintaruutu, jos haluat näyttää kaikki skannaukset niiden laatuun katsomatta.

    Poista valintaruudun valinta, jos haluat näyttää vain hyvänlaatuiset skannaukset.

Tietojen varmuuskopiointi ja palauttaminen

Suosittelemme, että varmuuskopioit Security Managerin tiedot säännöllisin väliajoin. Varmuuskopioinnin tiheysväli vaihtelee sen mukaan, kuinka usein tiedot muuttuvat. Esimerkiksi jos lisäät uusia kirjautumistunnuksia päivittäin, tiedot kannattaa todennäköisesti varmuuskopioida päivittäin.

Varmuuskopioiden avulla tietoja voidaan siirtää myös tietokoneiden välillä. Tätä kutsutaan tuonniksi ja vienniksi.

HUOMAUTUS: Tätä toimintoa käytettäessä kopioidaan vain tiedot.

HP ProtectTools Security Manager on asennettava kaikkiin tietokoneisiin, joihin varmuuskopioituja tietoja ollaan siirtämässä, ennen kuin tietoja voidaan palauttaa varmuuskopiotiedostosta.

Voit varmuuskopioida tiedot seuraavasti:

1. Valitse vasemmasta ruudusta **Advanced** (Lisäasetukset) ja sitten **Backup and Restore** (Varmuuskopiointi ja palauttaminen).
2. Valitse **Back up data** (Varmuuskopioi tiedot).
3. Valitse moduulit, jotka haluat lisätä varmuuskopioon. Useimmissa tapauksissa haluat todennäköisesti valita ne kaikki.
4. Anna tallennustiedostolle nimi. Oletusarvoisesti tiedosto tallennetaan Tiedostot-kansioon. Valitse **Browse** (Selaa), jos haluat määrittää toisen sijainnin.
5. Anna tiedostoa suojaava salasana.

6. Vahvista henkilöllisyytesi.
7. Valitse **Finish** (Valmis).

Voit palauttaa tiedot seuraavasti:

1. Valitse vasemmasta ruudusta **Advanced** (Lisäasetukset) ja sitten **Backup and Restore** (Varmuuskopiointi ja palauttaminen).
2. Valitse **Restore data** (Palauta tiedot).
3. Valitse aikaisemmin luotu tallennustiedosto. Voit kirjoittaa polun tähän tarkoitukseen varattuun kenttään tai valita **Browse** (Selaa).
4. Anna tiedostoa suojaava salasana.
5. Valitse moduulit, joiden tiedot haluat palauttaa. Useimmissa tapauksissa tämä tarkoittaa kaikkia annettuja moduuleita.
6. Valitse **Finish** (Valmis).

Discover more (Etsi lisää)

Saatavilla voi olla lisäsovelluksia, jotka lisäävät ohjelmaan uusia toimintoja.

Voit hakea lisäsovelluksia valitsemalla Security Managerin kojelaudasta **[+] Discover more** ([+] Etsi lisää).

HUOMAUTUS: Jos kojelaudan vasemmassa alakulmassa ei ole **[+] Discover more** ([+] Etsi lisää) -linkkiä, tietokoneen järjestelmänvalvoja on poistanut sen käytöstä.

Päivitykset ja viestit

1. Jos haluat saada tietoja uusista sovelluksista ja päivityksistä, valitse **Keep me informed about new applications and updates** (Ilmoita uusista sovelluksista ja päivityksistä) -valintaruutu.
2. Jos haluat ajoittaa automaattisia päivityksiä, valitse päivien määrä.
3. Voit hakea päivityksiä valitsemalla **Check Now** (Hae nyt).

Suojaussovellusten tila

Security Managerin Applications Status (Sovellusten tila) -sivulla näkyy asennettujen suojaussovellusten yleinen tila. Sivulla näkyvät asennetut sovellukset ja niiden asennuksen tila. Yhteenveto tulee automaattisesti näyttöön, kun avaat Security Managerin kojelaudan ja valitset **Check the status of the security applications** (Tarkista suojaussovellusten tila), kun valitset **Security Applications** (Suojaussovellukset) tai kun napsautat näytön oikeassa reunassa olevan Windowsin sivupalkin **Gadget** (Pienoisohjelma) -kuvakkeen **Check Now** (Tarkista nyt) -vaihtoehtoa.

8 Drive Encryption for HP ProtectTools (vain tietyt mallit)

△ **VAROITUS:** Jos päätät poistaa Drive Encryption -moduulin asennuksen, sinun on ensin purettava kaikkien salattujen kiintolevyjen salaus. Jos et tee niin, et voi käyttää salatuilla kiintolevyillä olevia tietoja, ennen kuin olet rekisteröitynyt Drive Encryption -palautuspalveluun. Vaikka Drive Encryption -moduuli asennetaan uudelleen, salattujen kiintolevyjen sisältöä ei voi käyttää.

Drive Encryption for HP ProtectTools on kokonaisvaltainen ratkaisu tietokoneen kiintolevyn tietojen suojaamiseen salaamalla. Kun Drive Encryption on käytössä, sinun on kirjauduttava sisään Drive Encryption -kirjautumisnäytössä, joka tulee näyttöön ennen Windows®-käyttöjärjestelmän käynnistymistä.

HP ProtectTools Setup Wizard (HP ProtectToolsin ohjattu asennustoiminto) antaa järjestelmänvalvojille mahdollisuuden ottaa Drive Encryption käyttöön, varmuuskopioida salausavain, lisätä ja poistaa käyttäjiä sekä poistaa Drive Encryption käytöstä. Lisätietoja on HP ProtectTools Security Manager -ohjelmiston ohjeessa.

Drive Encryptionilla voi suorittaa seuraavat tehtävät:

- Salauksen hallinta

  Yksittäisten kiintolevyjen salaaminen tai niiden salauksen purkaminen

  HUOMAUTUS: Vain sisäiset kiintolevyt voidaan salata.

- Palautus
  - Varmuuskopioavainten luominen
  - Palautuksen suorittaminen

Asennusohjeet

Drive Encryptionin avaaminen

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Administrative Console**.
2. Valitse vasemmasta ruudusta **Drive Encryption**.

Yleiset tehtävät

Drive Encryptionin ottaminen käyttöön

Ota Drive Encryption käyttöön HP ProtectToolsin ohjatun asennustoiminnon avulla.

HUOMAUTUS: Ohjatun toiminnon avulla voit myös lisätä ja poistaa käyttäjiä.

TAI

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Administrative Console**.
2. Valitse vasemmasta ruudusta **Security** (Suojaus) ja sitten **Features** (Toiminnot).
3. Valitse **Drive Encryption** (Aseman salaus) -valintaruutu ja sitten **Next** (Seuraava).
4. Valitse **Drives to be encrypted** (Salattavat asemat) -kohdasta sen kiintolevyn valintaruutu, jonka haluat salata.
5. Aseta tallennuslaite sille varattuun paikkaan.

   HUOMAUTUS: Jos haluat tallentaa salausavaimen, sinun on käytettävä FAT32-muodossa olevaa USB-tallennuslaitetta.

6. Valitse **External storage device on which to save encryption key** (Ulkoinen tallennuslaite, jonne salausavain tallennetaan) -kohdasta sen tallennuslaitteen valintaruutu, johon salausavain tallennetaan.
7. Valitse **Apply** (Käytä).

   Aseman salaaminen alkaa.

Lisätietoja on HP ProtectTools Security Manager -ohjelmiston ohjeessa.

Drive Encryptionin poistaminen käytöstä

Poista Drive Encryption käytöstä HP ProtectToolsin ohjatun asennustoiminnon avulla. Lisätietoja on HP ProtectTools Security Manager -ohjelmiston ohjeessa.

TAI

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Administrative Console**.
2. Valitse vasemmasta ruudusta **Security** (Suojaus) ja sitten **Features** (Toiminnot).
3. Poista **Drive Encryption** (Aseman salaus) -valintaruudun valinta ja valitse **Apply** (Käytä).

   Aseman salaamisen purkaminen alkaa.

Sisäänkirjautuminen Drive Encryptionin käyttöönoton jälkeen

Kun käynnistät tietokoneen Drive Encryptionin käyttöönoton jälkeen ja käyttäjätilisi on rekisteröity, sinun on kirjauduttava sisään Drive Encryption -kirjautumisnäytössä:

HUOMAUTUS: Jos Windowsin järjestelmänvalvoja on ottanut HP ProtectTools Security Managerin Pre-boot Security (Käynnistystä edeltävä suojaus) -toiminnon, sinut kirjataan sisään tietokoneeseen välittömästi tietokoneen käynnistämisen jälkeen Drive Encryption -kirjautumisnäytön sijaan.

1. Valitse käyttäjätunnuksesi ja kirjoita Windowsin salasana tai Java™-kortin PIN-koodi, tai pyyhkäise rekisteröidyllä sormellasi.
2. Valitse **OK**.

HUOMAUTUS: Jos kirjaudut Drive Encryption -kirjautumisnäytössä palautusavaimella, sinua kehotetaan myös valitsemaan Windowsin käyttäjätunnus ja kirjoittamaan salasanasi Windowsin kirjautumisnäyttöön.

Suojaa tietojasi salaamalla kiintolevysi

HP ProtectToolsin ohjatun asennustoiminnon avulla voit suojata tietojasi salaamalla kiintolevysi:

1. Valitse Security Managerista **Getting Started** (Käytön aloittaminen) ja napsauta **Security Manager Setup** (Security Managerin asennus) -kuvaketta. Security Managerin toimintoja kuvaileva lyhyt esittely käynnistyy. (Voit käynnistää Security Managerin myös Drive Encryption (Aseman salaus) -sivulta.)
2. Valitse vasemmasta ruudusta **Drive Encryption** (Aseman salaus) ja sitten **Encryption Management** (Salauksen hallinta).
3. Valitse **Change Encryption** (Muuta salausta).
4. Valitse yksi tai useampi salattava asema.

HUOMAUTUS: Kiintolevyn salaaminen on erittäin suositeltavaa.

Salauksen tilan näyttäminen

Käyttäjät voivat näyttää HP ProtectTools Security Managerissa salauksen tilan.

HUOMAUTUS: Aseman salauksen tilan muutokset on tehtävä HP ProtectToolsin hallintakonsolissa.

1. Avaa **HP ProtectTools Security Manager**.
2. Valitse **My Data** (Omat tiedot) -kohdasta **Encryption Status** (Salauksen tila).

   Jos Drive Encryption on käytössä, aseman tilan koodina on jokin seuraavista:

   - Active (Aktiivinen)
   - Inactive (Passiivinen)
   - Not encrypted (Salaamaton)
   - Encrypted (Salattu)
   - Encrypting (Salataan)
   - Decrypting (Salausta puretaan)

   Jos kiintolevyä salataan tai sen salausta puretaan, tilanneilmaisin näyttää valmiusasteen prosentteina ja salauksesta tai salauksen purkamisesta jäljellä olevan ajan.

Lisätoiminnot

Drive Encryptionin hallinta (järjestelmänvalvojan tehtävä)

Encryption Management (Salauksen hallinta) -sivulla järjestelmänvalvojat voivat tarkastella ja muuttaa Drive Encryptionin tilaa (käytössä tai ei käytössä) sekä tarkastella tietokoneen kaikkien kiintolevyjen salauksen tilaa.

- Jos tilana on Inactive (Passiivinen), Windows-järjestelmänvalvoja ei ole vielä ottanut Drive Encryptionia HP ProtectTools Security Managerissa käyttöön eikä se suojaa kiintolevyä. Ota Drive Encryption käyttöön HP ProtectTools Security Managerin ohjatun asennustoiminnon avulla.
- Jos tilana on Active (Aktiivinen), Drive Encryption on otettu käyttöön ja määritetty. Aseman tilana on jokin seuraavista:
  - Not encrypted (Salaamaton)
  - Encrypted (Salattu)
  - Encrypting (Salataan)
  - Decrypting (Salausta puretaan)

Yksittäisten kiintolevyjen salaaminen tai niiden salauksen purkaminen

Jos haluat salata yhden tai useamman tietokoneen kiintolevyn tai purkaa salatun kiintolevyn salauksen, käytä Change Encryption (Muuta salausta) -toimintoa.

1. Avaa **HP ProtectTools Administrative Console**, valitse **Drive Encryption** (Aseman salaus) ja sitten **Encryption Management** (Salauksen hallinta).
2. Valitse **Change Encryption** (Muuta salausta).
3. Valitse Change Encryption (Muuta salausta) -valintaikkunassa niiden kiintolevyjen vieressä olevat valintaruudut tai poista niiden kiintolevyjen vieressä olevien valintaruutujen valinnat, jotka haluat salata tai joiden salauksen haluat purkaa, ja valitse **OK**.

HUOMAUTUS: Kun kiintolevyä salataan tai sen salausta puretaan, tilanneilmaisin näyttää nykyisen istunnon aikana suoritettavasta prosessista jäljellä olevan ajan. Jos tietokone sammutetaan tai se siirtyy lepo-, valmius- tai horrostilaan salauksen aikana ja käynnistyy uudelleen, Time Remaining (Jäljellä oleva aika) -näyttö nollautuu, mutta salaus jatkuu siitä kohdasta, jossa se keskeytyi. Jäljellä oleva aika ja tilanneilmaisin muuttuvat tavallista nopeammin aikaisemman tilanteen mukaan.

Varmuuskopiointi ja palautus (järjestelmänvalvojan tehtävä)

Recovery (Palautus) -sivulla järjestelmänvalvojat voivat varmuuskopioida ja palauttaa salausavaimia.

Local Drive Encryption Key Backup (Paikallisen aseman salausavaimen varmuuskopiointi) – Voit varmuuskopioida salausavaimia siirrettäville tallennusvälineille, kun Drive Encryption on otettu käyttöön.

Varmuuskopioavainten luominen

Voit varmuuskopioida salatun aseman salausavaimen siirrettävään tallennuslaitteeseen:

△ **VAROITUS:** Säilytä varmuuskopioavaimen sisältävää tallennuslaitetta turvallisessa paikassa, sillä jos unohdat salasanasi tai kadotat Java-korttisi, voit käyttää kiintolevyn tietoja vain tämän laitteen avulla.

1. Avaa **HP ProtectTools Administrative Console**, valitse **Drive Encryption** (Aseman salaus) ja sitten **Recovery** (Palautus).
2. Valitse **Backup Keys** (Varmuuskopioi avaimet).
3. Valitse Select Backup Disk (Valitse varmuuskopiolevy) -sivulla sen laitteen valintaruutu, johon haluat varmuuskopioida salausavaimen, ja valitse **Next** (Seuraava).
4. Lue seuraavalla sivulla olevat tiedot ja valitse **Next** (Seuraava) Salausavain tallennetaan valittuun tallennuslaitteeseen.
5. Kun vahvistusvalintaikkuna avautuu, valitse **Finish** (Valmis).

Palautuksen suorittaminen

Salasanan unohtuessa voit suorittaa palautuksen seuraavasti:

1. Käynnistä tietokone.
2. Aseta varmuuskopioavaimen sisältävä siirrettävä tallennuslaite paikalleen.
3. Kun Drive Encryption for HP ProtectTools -kirjautumisvalintaikkuna avautuu, valitse **Cancel** (Peruuta).
4. Valitse näytön vasemmasta alakulmasta **Options** (Asetukset) ja sitten **Recovery** (Palautus).
5. Valitse varmuuskopioavaimen sisältävä tiedosto tai etsi se napsauttamalla **Browse** (Selaa), ja valitse **Next** (Seuraava).
6. Kun vahvistusvalintaikkuna avautuu, valitse **OK**.

   Tietokone käynnistyy.

HUOMAUTUS: Suosittelemme, että palautat salasanasi palautuksen suorittamisen jälkeen.

9 Privacy Manager for HP ProtectTools (vain tietyt mallit)

Privacy Manager for HP ProtectToolsin avulla voit käyttää kehittyneitä kirjautumistekniikoita (todennustekniikoita) tietojen lähteen, eheyden ja turvallisuuden tarkistamiseen sähköpostia, Microsoft® Office -asiakirjoja tai pikaviestejä (IM) käytettäessä.

Privacy Manager hyödyntää HP ProtectTools Security Managerin suojausinfrastruktuuria, johon kuuluvat seuraavat suojatut kirjautumistavat:

- sormenjälkitodennus
- Windowsin® salasana
- HP ProtectTools Java™ -kortti.

Privacy Managerissa voit käyttää mitä tahansa edellä mainituista suojatuista kirjautumistavoista

Privacy Managerin vaatimukset ovat seuraavat:

- HP ProtectTools Security Manager 5.00 tai uudempi
- Windows® 7-, Windows Vista®- tai Windows XP -käyttöjärjestelmä
- Microsoft Outlook 2007 tai Microsoft Outlook 2003
- voimassa oleva sähköpostitili

HUOMAUTUS: Privacy Manager -varmenne (digitaalinen varmenne) on pyydettävä ja asennettava Privacy Managerista, ennen kuin suojausominaisuuksia voi käyttää. Tietoja Privacy Manager -varmenteen pyytämisestä on kohdassa Privacy Manager -varmenteen pyytäminen ja asentaminen sivulla 47.

Asennusohjeet

Privacy Managerin avaaminen

Voit avata Privacy Managerin seuraavasti:

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Security Manager**.
2. Valitse **Privacy Manager**.

TAI

Napsauta hiiren kakkospainikkeella ilmaisinalueella, tehtäväpalkin oikeassa reunassa olevaa **HP ProtectTools** -kuvaketta, valitse **Privacy Manager** (Yksityisyyden hallinta) ja napsauta **Configuration** (Kokoonpano) -painiketta.

TAI

Napsauta Microsoft Outlook -sähköpostiviestin työkalurivillä, **Send Securely** (Lähetä turvallisesti) -kohdan vieressä olevaa alanuolta ja valitse **Certificates** (Varmenteet) tai **Trusted Contacts** (Luotetut yhteyshenkilöt).

TAI

Napsauta Microsoft Office -asiakirjan työkalurivillä, **Sign and Encrypt** (Allekirjoita ja salaa) -kohdan vieressä olevaa alanuolta ja valitse **Certificates** (Varmenteet) tai **Trusted Contacts** (Luotetut yhteyshenkilöt).

Privacy Manager -varmenteiden hallinta

Privacy Manager -varmenteet suojaavat tietoja ja viestejä julkisen avaimen infrastruktuuriksi (PKI) kutsutun salaustekniikan avulla. PKI edellyttää, että käyttäjät hankkivat varmenteiden myöntäjän (CA) myöntämät salausavaimet ja Privacy Manager -varmenteen. Toisin kuin useimmat tietojen salaus- ja todennusohjelmistot, jotka vaativat todennusta vain tietyin väliajoin, Privacy Manager vaatii todennusta aina, kun allekirjoitat sähköpostiviestin tai Microsoft Office -asiakirjan salausavaimella. Privacy Managerin avulla tärkeät tiedot voidaan tallentaa ja lähettää turvallisesti.

Voit suorittaa seuraavat tehtävät:

- pyytää ja asentaa Privacy Manager -varmenteen
- tarkastella Privacy Manager -varmenteen tietoja
- uudistaa Privacy Manager -varmenteita
- kun käytettävissä on useita varmenteita, määrittää Privacy Managerin käyttämän oletusarvoisen Privacy Manager -varmenteen
- poistaa ja kumota Privacy Manager -varmenteen (lisätoiminto)

Privacy Manager -varmenteen pyytäminen ja asentaminen

Ennen kuin voit käyttää Privacy Managerin toimintoja, sinun on pyydettävä ja asennettava Privacy Manager -varmenne (Privacy Managerista) käyttämällä kelvollista sähköpostiosoitetta. Sähköpostiosoite on määritettävä Microsoft Outlook -tiliksi samassa tietokoneessa kuin mistä olet pyytämässä Privacy Manager -varmennetta.

Privacy Manager -varmenteen pyytäminen

1. Avaa Privacy Manager ja valitse **Certificates** (Varmenteet).
2. Valitse **Request a Privacy Manager certificate** (Pyydä Privacy Manager -varmenne).
3. Lue Welcome (Tervetuloa) -sivun teksti ja valitse **Next** (Seuraava).
4. Lue License Agreement (Käyttöoikeus) -sivulla oleva käyttöoikeussopimus.
5. Varmista, että **Check here to accept the terms of this license agreement** (Hyväksy tämän käyttöoikeussopimuksen ehdot valitsemalla tämä) -valintaruutu on valittuna, ja valitse **Next** (Seuraava).
6. Anna Your Certificate Details (Varmenteen tiedot) -sivulla tarvittavat tiedot ja valitse **Next** (Seuraava).
7. Valitse Certificate Request Accepted (Varmennepyyntö hyväksytty) -sivulla **Finish** (Valmis).
8. Sulje varmenne valitsemalla **OK**.

Saat Microsoft Outlookiin Privacy Manager -varmenteen sisältävän sähköpostiviestin.

Valmiiksi määritetyn Privacy Manager -yritysvarmenteen hankkiminen

1. Avaa Outlookissa saamasi sähköpostiviesti, jossa ilmoitetaan, että olet saanut valmiiksi määritetyn yritysvarmenteen.
2. Valitse **Obtain** (Hanki).
3. Saat Microsoft Outlookiin Privacy Manager -varmenteen sisältävän sähköpostiviestin.
4. Lisätietoja varmenteen asentamisesta on kohdassa Privacy Manager -varmenteen asentaminen sivulla 48

Privacy Manager -varmenteen asentaminen

1. Kun saat Privacy Manager -varmenteen sisältävän sähköpostiviestin, avaa se ja napsauta Outlook 2007:ssä sen oikeassa alakulmassa tai Outlook 2003:ssa sen vasemmassa yläkulmassa olevaa **Setup** (Asennus) -painiketta.
2. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.
3. Valitse Certificate Installed (Varmenne asennettu) -sivulla **Next** (Seuraava).
4. Anna Certificate Backup (Varmenteen varmuuskopio) -sivulla varmuuskopiotiedoston sijainti ja nimi, tai etsi sijainti valitsemalla **Browse** (Selaa).

   △ **VAROITUS:** Tallenna tiedosto muualle kuin kiintolevylle ja säilytä sitä turvallisessa paikassa. Tiedosto on tarkoitettu vain omaan käyttöösi ja tarvitset sitä, jos haluat palauttaa Privacy Manager -varmenteesi ja siihen liittyvät avaimet.

5. Anna salasana, vahvista se ja valitse **Next** (Seuraava).
6. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.
7. Jos päätät aloittaa Trusted Contact (Luotettu yhteyshenkilö) -kutsuprosessin, toimi näyttöön tulevien ohjeiden mukaan. Aloita kohdan Luotettujen yhteyshenkilöiden lisääminen Microsoft Outlookin yhteystietojen avulla sivulla 52 toisesta vaiheesta.

TAI

Jos valitset **Cancel** (Peruuta), perehdy kohtaan Luotetun yhteyshenkilön lisääminen sivulla 51, joka sisältää lisätietoja luotettujen yhteyshenkilöiden lisäämisestä myöhemmin.

Privacy Manager -varmenteen tietojen tarkasteleminen

1. Avaa Privacy Manager ja valitse **Certificates** (Varmenteet).
2. Valitse Privacy Manager -varmenne.
3. Valitse **Certificate details** (Varmenteen tiedot).
4. Kun olet lopettanut tietojen tarkastelun, valitse **OK**.

Privacy Manager -varmenteen uudistaminen

Kun Privacy Manager -varmenteen voimassaoloaika on umpeutumassa, saat tästä kertovan ilmoituksen:

1. Avaa Privacy Manager ja valitse **Certificates** (Varmenteet).
2. Valitse **Renew certificate** (Uudista varmenne).
3. Osta uusi Privacy Manager -varmenne toimimalla näyttöön tulevien ohjeiden mukaan.

HUOMAUTUS: Privacy Manager -varmenteen uudistamisprosessi ei korvaa vanhaa Privacy Manager -varmennetta. Sinun on hankittava uusi Privacy Manager -varmenne ja asennettava se kohdassa Privacy Manager -varmenteen pyytäminen ja asentaminen sivulla 47 kuvatulla tavalla.

Oletusarvoisen Privacy Manager -varmenteen määrittäminen

Privacy Managerissa voi tarkastella vain Privacy Manager -varmenteita, vaikka tietokoneeseen olisi asennettu myös muiden varmenteiden myöntäjien varmenteita.

Jos tietokoneeseen on asennettu useampia Privacy Manager -varmenteita Privacy Managerista, voit määrittää niistä yhden oletusvarmenteeksi seuraavalla tavalla:

1. Avaa Privacy Manager ja valitse **Certificates** (Varmenteet).
2. Valitse oletusarvoisesti käytettävä Privacy Manager -varmenne ja sitten **Set default** (Aseta oletukseksi).
3. Valitse **OK**.

HUOMAUTUS: Sinun ei tarvitse käyttää oletusarvoista Privacy Manager -varmennetta. Voit valita Privacy Manager -toiminnoista minkä tahansa Privacy Manager -varmenteen.

Privacy Manager -varmenteen poistaminen

Jos poistat Privacy Manager -varmenteen, et voi avata tiedostoja tai tarkastella tietoja, jotka on salattu kyseisellä varmenteella. Jos olet vahingossa poistanut Privacy Manager -varmenteen, voit palauttaa sen varmenteen asentamisen yhteydessä luodun varmuuskopiotiedoston avulla. Lisätietoja on kohdassa Privacy Manager -varmenteen palauttaminen sivulla 50.

Voit poistaa Privacy Manager -varmenteen seuraavasti:

1. Avaa Privacy Manager ja valitse **Certificates** (Varmenteet).
2. Valitse poistettava Privacy Manager -varmenne ja sitten **Advanced** (Lisäasetukset).
3. Valitse **Delete** (Poista).
4. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).
5. Valitse **Close** (Sulje) ja sitten **Apply** (Käytä).

Privacy Manager -varmenteen palauttaminen

Privacy Manager -varmenteen asentamisen aikana sinua kehotetaan luomaan varmuuskopio varmenteesta. Voit luoda varmuuskopion myös Migration (Siirto) -sivulla. Tätä varmuuskopiota voi käyttää, kun siirryt käyttämään toista tietokonetta tai palautat varmenteen samaan tietokoneeseen.

1. Avaa Privacy Manager ja valitse **Migration** (Siirto).
2. Valitse **Restore** (Palauta).
3. Etsi varmuuskopiointiprosessin yhteydessä luotu .dppsm-tiedosto valitsemalla Migration File (Siirtotiedosto) -sivulta **Browse** (Selaa) ja sitten **Next** (Seuraava).
4. Anna varmuuskopion luonnin yhteydessä käytetty salasana ja valitse **Next** (Seuraava).
5. Valitse **Finish** (Valmis).
6. Valitse **OK**.

Lisätietoja on kohdassa Privacy Manager -varmenteen asentaminen sivulla 48 tai Privacy Manager -varmenteiden ja luotettujen yhteyshenkilöiden varmuuskopiointi sivulla 66.

Privacy Manager -varmenteen kumoaminen

Jos uskot Privacy Manager -varmenteesi turvallisuuden olevan uhattuna, voit kumota oman varmenteesi seuraavasti:

HUOMAUTUS: Kumottua Privacy Manager -varmennetta ei poisteta. Varmennetta voidaan edelleen käyttää salattujen tiedostojen tarkasteluun.

1. Avaa Privacy Manager ja valitse **Certificates** (Varmenteet).
2. Valitse **Advanced** (Lisäasetukset).
3. Valitse kumottava Privacy Manager -varmenne ja sitten **Revoke** (Kumoa).
4. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).
5. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.
6. Toimi näyttöön tulevien ohjeiden mukaan.

Luotettujen yhteyshenkilöiden hallinta

Luotetut yhteyshenkilöt ovat käyttäjiä, joiden kanssa olet vaihtanut Privacy Manager -varmenteita, mikä mahdollistaa turvallisen viestinnän kahden osapuolen välillä.

Trusted Contacts Managerin avulla voit suorittaa seuraavat tehtävät:

- tarkastella luotettujen yhteyshenkilöiden tietoja
- poistaa luotettuja yhteyshenkilöitä
- tarkastella luotettujen yhteyshenkilöiden kumoustilaa (lisätoiminto).

Luotettujen yhteyshenkilöiden lisääminen

Luotettujen yhteyshenkilöiden lisääminen on kolmivaiheinen prosessi:

1. Voit lähettää sähköpostikutsun luotettuihin yhteyshenkilöihin kuuluvalle vastaanottajalle.
2. Luotettuihin yhteyshenkilöihin kuuluva vastaanottaja vastaa sähköpostiviestiin.
3. Kun saat sähköpostivastauksen luotettuihin yhteyshenkilöihin kuuluvalta vastaanottajalta, valitse **Accept** (Hyväksy).

Voit lähettää luotettujen yhteyshenkilöiden sähköpostikutsuja yksittäisille vastaanottajille tai lähettää kutsun kaikille Microsoft Outlookin osoitteistossa oleville yhteyshenkilöille.

Jos haluat lisätä luotettuja yhteyshenkilöitä, perehdy seuraaviin kohtiin.

HUOMAUTUS: Luotettuihin yhteyshenkilöihin kuuluvien vastaanottajien on asennettava Privacy Manager tai vaihtoehtoinen asiakas tietokoneisiinsa, ennen kuin he voivat vastata pyyntöön ja heidät voidaan lisätä luotetuiksi yhteyshenkilöiksi. Lisätietoja vaihtoehtoisen asiakkaan asentamisesta on DigitalPersonan sivustossa osoitteessa http://DigitalPersona.com/PrivacyManager.

Luotetun yhteyshenkilön lisääminen

1. Avaa Privacy Manager, valitse **Trusted Contacts Manager** (Luotettujen yhteyshenkilöiden hallinta) ja sitten **Invite Contacts** (Kutsu yhteyshenkilöitä).

   TAI

   Napsauta Microsoft Outlookissa, **Send Securely** (Lähetä turvallisesti) -kohdan vieressä olevaa alanuolta ja valitse **Invite Contacts** (Kutsu yhteyshenkilöitä).

2. Jos Select Certificate (Valitse varmenne) -valintaikkuna avautuu, valitse käytettävä Privacy Manager -varmenne ja sitten **OK**.
3. Kun Trusted Contact Invitation (Luotettujen yhteyshenkilöiden kutsuminen) -valintaikkuna avautuu, lue siinä oleva teksti ja valitse **OK**.

   Sähköpostiviesti luodaan automaattisesti.

4. Anna yhden tai useamman vastaanottajan sähköpostiosoite, jotka haluat lisätä luotettuihin yhteyshenkilöihin.
5. Muokkaa tekstiä ja allekirjoita nimesi (valinnainen).
6. Valitse **Send** (Lähetä).

HUOMAUTUS: Jos et ole vielä hankkinut Privacy Manager -varmennetta, näyttöön tulee viesti, jossa kerrotaan, että luotetun yhteyshenkilön pyynnön lähettämiseen tarvitaan Privacy Manager -varmennetta. Käynnistä Certificate Request Wizard (Ohjattu varmennepyyntö) -toiminto valitsemalla **OK**. Lisätietoja on kohdassa Privacy Manager -varmenteen pyytäminen ja asentaminen sivulla 47.

7. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

HUOMAUTUS: Kun luotettuihin yhteyshenkilöihin kuuluva vastaanottaja saa sähköpostiviestin, hänen on avattava se, napsautettava sen oikeassa alakulmassa olevaa **Accept** (Hyväksy) -painiketta ja valittava **OK**, kun vahvistusvalintanäyttö avautuu.

8. Kun saat sähköpostivastauksen vastaanottajalta, jossa hän ilmoittaa hyväksyvänsä, että lisäät hänet luotettuihin yhteyshenkilöihin, valitse sähköpostiviestin oikeasta alakulmasta **Accept** (Hyväksy).

   Näyttöön tulee valintaikkuna, jossa kerrotaan, että vastaanottaja on lisätty luotettujen yhteyshenkilöiden luetteloon.

9. Valitse **OK**.

Luotettujen yhteyshenkilöiden lisääminen Microsoft Outlookin yhteystietojen avulla

1. Avaa Privacy Manager, valitse **Trusted Contacts Manager** (Luotettujen yhteyshenkilöiden hallinta) ja sitten **Invite Contacts** (Kutsu yhteyshenkilöitä).

   TAI

   Napsauta Microsoft Outlookissa, **Send Securely** (Lähetä turvallisesti) -kohdan vieressä olevaa alanuolta ja valitse **Invite All My Outlook Contacts** (Kutsu kaikki Outlookin yhteyshenkilöt).

2. Kun Trusted Contact Invitation (Luotettujen yhteyshenkilöiden kutsuminen) -sivu avautuu, valitse niiden vastaanottajien sähköpostiosoitteet, jotka haluat lisätä luotettuihin yhteyshenkilöihin, ja valitse **Next** (Seuraava).

3. Kun Sending Invitation (Lähetetään kutsua) -sivu avautuu, valitse **Finish** (Valmis).

   Valituista Microsoft Outlookin sähköpostiosoitteista luodaan automaattisesti luettelo sähköpostiviestin muodossa.

4. Muokkaa tekstiä ja allekirjoita nimesi (valinnainen).

5. Valitse **Send** (Lähetä).

HUOMAUTUS: Jos et ole vielä hankkinut Privacy Manager -varmennetta, näyttöön tulee viesti, jossa kerrotaan, että luotetun yhteyshenkilön pyynnön lähettämiseen tarvitaan Privacy Manager -varmennetta. Käynnistä Certificate Request Wizard (Ohjattu varmennepyyntö) -toiminto valitsemalla **OK**. Lisätietoja on kohdassa Privacy Manager -varmenteen pyytäminen ja asentaminen sivulla 47.

6. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

HUOMAUTUS: Kun luotettuihin yhteyshenkilöihin kuuluva vastaanottaja saa sähköpostiviestin, hänen on avattava se, napsautettava sen oikeassa alakulmassa olevaa **Accept** (Hyväksy) -painiketta ja valittava **OK**, kun vahvistusvalintanäyttö avautuu.

7. Kun saat sähköpostivastauksen vastaanottajalta, jossa hän ilmoittaa hyväksyvänsä, että lisäät hänet luotettuihin yhteyshenkilöihin, valitse sähköpostiviestin oikeasta alakulmasta **Accept** (Hyväksy).

   Näyttöön tulee valintaikkuna, jossa kerrotaan, että vastaanottaja on lisätty luotettujen yhteyshenkilöiden luetteloon.

8. Valitse **OK**.

Luotettujen yhteyshenkilöiden tietojen tarkasteleminen

1. Avaa Privacy Manager ja valitse **Trusted Contacts** (Luotetut yhteyshenkilöt).
2. Napsauta luotettua yhteyshenkilöä.
3. Valitse **Contact details** (Yhteyshenkilön tiedot).
4. Kun olet lopettanut tietojen tarkastelun, valitse **OK**.

Luotetun yhteyshenkilön poistaminen

1. Avaa Privacy Manager ja valitse **Trusted Contacts** (Luotetut yhteyshenkilöt).
2. Napsauta luotettua yhteyshenkilöä, jonka haluat poistaa.
3. Valitse **Delete contact** (Poista yhteyshenkilö).
4. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

Luotetun yhteyshenkilön kumoustilan tarkistaminen

Jos haluat tarkistaa, onko luotettu yhteyshenkilö kumonnut Privacy Manager -varmenteensa, toimi seuraavasti:

1. Avaa Privacy Manager ja valitse **Trusted Contacts** (Luotetut yhteyshenkilöt).
2. Napsauta luotettua yhteyshenkilöä.
3. Napsauta **Advanced** (Lisäasetukset) -painiketta.

   Advanced Trusted Contact Management (Luotettujen yhteyshenkilöiden hallinnan lisäasetukset) -valintaikkuna tulee näyttöön.
4. Valitse **Check Revocation** (Tarkista kumous).
5. Valitse **Sulje**.

Yleiset tehtävät

Voit käyttää Privacy Manageria seuraavien Microsoft-tuotteiden kanssa:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Privacy Managerin käyttäminen Microsoft Outlookissa

Kun Privacy Manager on asennettu, Microsoft Outlookin työkalurivillä näkyy Privacy (Yksityisyys) -painike ja jokaisen Microsoft Outlook -sähköpostiviestin työkalurivillä näkyy Send Securely (Lähetä turvallisesti) -painike. Kun napsautat **Privacy** (Yksityisyys)- tai **Send Securely** (Lähetä turvallisesti) -kohdan vieressä olevaa alanuolta, voit valita seuraavista vaihtoehdoista:

- Sign and Send (Send Securely button only) (Allekirjoita ja lähetä (vain Lähetä turvallisesti -painike)) – Tämä toiminto lisää sähköpostiviestiin digitaalisen allekirjoituksen ja lähettää sähköpostiviestin, kun olet todentanut sen valitsemaasi suojattua kirjautumistapaa käyttäen.
- Seal for Trusted Contacts and Send (Send Securely button only) (Sinetöi luotettuja yhteyshenkilöitä varten ja lähetä (vain Lähetä turvallisesti -painike)) – Tämä toiminto lisää sähköpostiviestiin digitaalisen allekirjoituksen, salaa sähköpostiviestin ja lähettää sen, kun olet todentanut sen valitsemaasi suojattua kirjautumistapaa käyttäen.
- Invite Contacts (Kutsu yhteyshenkilöitä) – Tämän toiminnon avulla voit lähettää luotetun yhteyshenkilön kutsun. Lisätietoja on kohdassa Luotetun yhteyshenkilön lisääminen sivulla 51.
- Invite Outlook Contacts (Kutsu Outlook-yhteyshenkilöitä) – Tämän toiminnon avulla voit lähettää luotetun yhteyshenkilön kutsun kaikille Microsoft Outlook -osoitekirjassa oleville yhteyshenkilöille. Lisätietoja on kohdassa Luotettujen yhteyshenkilöiden lisääminen Microsoft Outlookin yhteystietojen avulla sivulla 52.
- Open the Privacy Manager software (Avaa Privacy Manager -ohjelmisto) – Certificates (Varmenteet)-, Trusted Contacts (Luotetut yhteyshenkilöt)- ja Settings (Asetukset) -toimintojen avulla voit avata Privacy Manager -ohjelmiston asetusten lisäämistä, tarkastelemista tai muuttamista varten. Lisätietoja on kohdassa Privacy Managerin asetusten määrittäminen Microsoft Outlookia varten sivulla 54.

Privacy Managerin asetusten määrittäminen Microsoft Outlookia varten

1. Avaa Privacy Manager, valitse **Settings** (Asetukset) ja napsauta **E-mail** (Sähköposti) -välilehteä.

   TAI

   Napsauta Microsoft Office -päätyökalurivillä, **Send Securely** (Lähetä turvallisesti) -kohdan vieressä olevaa alanuolta (Outlook 2003:ssa **Privacy** (Yksityisyys)) ja valitse **Settings** (Asetukset).

   TAI

   Napsauta Microsoft Office -sähköpostiviestin työkalurivillä, **Send Securely** (Lähetä turvallisesti) -kohdan vieressä olevaa alanuolta ja valitse **Settings** (Asetukset).

2. Valitse suojatun sähköpostiviestin lähettämisen yhteydessä suoritettavat toimenpiteet ja valitse **OK**.

Sähköpostiviestin allekirjoittaminen ja lähettäminen

1. Valitse Microsoft Outlookissa **Uusi** tai **Vastaa**.
2. Kirjoita sähköpostiviesti.
3. Napsauta **Send Securely** (Lähetä turvallisesti) -kohdan vieressä olevaa alanuolta (Outlook 2003:ssa **Privacy** (Yksityisyys)) ja valitse **Sign and Send** (Allekirjoita ja lähetä).
4. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

Sähköpostiviestin sinetöiminen ja lähettäminen

Digitaalisesti allekirjoitettuja ja sinetöityjä (salattuja) sähköpostiviestejä voivat tarkastella vain luotettujen yhteyshenkilöiden luettelosta valitsemasi henkilöt.

Voit sinetöidä sähköpostiviestin ja lähettää sen luotetulle yhteyshenkilölle seuraavasti:

1. Valitse Microsoft Outlookissa **Uusi** tai **Vastaa**.
2. Kirjoita sähköpostiviesti.
3. Napsauta **Send Securely** (Lähetä turvallisesti) -kohdan vieressä olevaa alanuolta (Outlook 2003:ssa **Privacy** (Yksityisyys)) ja valitse **Seal for Trusted Contacts and Send** (Sinetöi luotettuja yhteyshenkilöitä varten ja lähetä).
4. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

Sinetöidyn sähköpostiviestin tarkasteleminen

Kun avaat sinetöidyn sähköpostiviestin, suojausmerkintä näkyy sähköpostiviestin otsikossa. Suojausmerkintä sisältää seuraavat tiedot:

- sähköpostiviestin allekirjoittaneen henkilön henkilöllisyyden todentamiseen käytetyt valtuustiedot
- sähköpostiviestin allekirjoittaneen henkilön valtuustietojen todentamiseen käytetty tuote.

Privacy Managerin käyttäminen Microsoft Office 2007 -asiakirjassa

HUOMAUTUS: Privacy Manageria voi käyttää vain Microsoft Office 2007 -asiakirjojen kanssa.

Privacy Manager -varmenteen asentamisen jälkeen kaikkien Microsoft Word-, Microsoft Excel- ja Microsoft PowerPoint -asiakirjojen työkalurivin oikealle puolelle ilmestyy Sign and Encrypt (Allekirjoita ja salaa) -painike. Kun napsautat **Sign and Encrypt** (Allekirjoita ja salaa) -kohdan vieressä olevaa alanuolta, voit valita seuraavista vaihtoehdoista:

- Sign Document (Allekirjoita asiakirja) – Tämä toiminto lisää asiakirjaan digitaalisen allekirjoituksen.
- Add Signature Line Before Signing (Lisää allekirjoitusrivi ennen allekirjoitusta) (vain Microsoft Word ja Microsoft Excel) – Oletusarvoisesti allekirjoitusrivi lisätään, kun Microsoft Word- tai Microsoft Excel -asiakirja allekirjoitetaan tai salataan. Voit poistaa tämän toiminnon käytöstä poistamalla **Add Signature Line** (Lisää allekirjoitusrivi) -valintaruudun valinnan.
- Encrypt Document (Salaa asiakirja) – Tämä toiminto lisää asiakirjaan digitaalisen allekirjoituksen ja salaa asiakirjan.

- Remove Encryption (Poista salaus) – Tämä toiminto purkaa asiakirjan salauksen.
- Open the Privacy Manager software (Avaa Privacy Manager -ohjelmisto) – Certificates (Varmenteet)-, Trusted Contacts (Luotetut yhteyshenkilöt)- ja Settings (Asetukset) -toimintojen avulla voit avata Privacy Manager -ohjelmiston asetusten lisäämistä, tarkastelemista tai muuttamista varten. Lisätietoja on kohdassa Privacy Manager -varmenteiden hallinta sivulla 47, Luotettujen yhteyshenkilöiden hallinta sivulla 50 tai Privacy Managerin asetusten määrittäminen Microsoft Officea varten sivulla 56.

Privacy Managerin asetusten määrittäminen Microsoft Officea varten

1. Avaa Privacy Manager, valitse **Settings** (Asetukset) ja napsauta **Documents** (Asiakirjat) -välilehteä.

   TAI

   Napsauta Microsoft Office -asiakirjan työkalurivillä, **Sign and Encrypt** (Allekirjoita ja salaa) -kohdan vieressä olevaa alanuolta ja valitse **Settings** (Asetukset).

2. Valitse määritettävät toimenpiteet ja sitten **OK**.

Microsoft Office -asiakirjan allekirjoittaminen

1. Luo ja tallenna asiakirja Microsoft Word-, Microsoft Excel- tai Microsoft PowerPoint -muodossa.
2. Napsauta **Sign and Encrypt** (Allekirjoita ja salaa) -kohdan vieressä olevaa alanuolta ja valitse **Sign Document** (Allekirjoita asiakirja).
3. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.
4. Kun vahvistusvalintaikkuna avautuu, lue siinä oleva teksti ja valitse **OK**.

Jos päätät muokata asiakirjaa myöhemmin, toimi seuraavasti:

1. Napsauta näytön vasemmassa yläkulmassa olevaa **Office** (Toimisto) -painiketta.
2. Valitse **Prepare** (Valmistele) ja sitten **Mark as Final** (Merkitse lopulliseksi).
3. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä) ja jatka työskentelyä.
4. Kun olet lopettanut muokkauksen, allekirjoita asiakirja uudelleen.

Allekirjoitusrivin lisääminen Microsoft Word- tai Microsoft Excel -asiakirjoja allekirjoitettaessa

Privacy Managerissa voit lisätä allekirjoitusrivin, kun allekirjoitat Microsoft Word- tai Microsoft Excel -asiakirjoja:

1. Luo ja tallenna asiakirja Microsoft Word- tai Microsoft Excel -muodossa.
2. Valitse **Home** (Koti) -valikko.
3. Napsauta **Sign and Encrypt** (Allekirjoita ja salaa) -kohdan vieressä olevaa alanuolta ja valitse **Add Signature Line Before Signing** (Lisää allekirjoitusrivi ennen allekirjoitusta).

HUOMAUTUS: Add Signature Line Before Signing (Lisää allekirjoitusrivi ennen allekirjoitusta) -kohdan viereen ilmestyy valintamerkki, kun tämä asetus on valittuna. Oletusarvoisesti tämä asetus on käytössä.

4. Napsauta **Sign and Encrypt** (Allekirjoita ja salaa) -kohdan vieressä olevaa alanuolta ja valitse **Sign Document** (Allekirjoita asiakirja).

5. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

Ehdotettujen allekirjoittajien lisääminen Microsoft Word- tai Microsoft Excel -asiakirjaan

Ehdotettuja allekirjoittajia määrittämällä voit lisätä asiakirjaan useita allekirjoitusrivejä. Ehdotettu allekirjoittaja on käyttäjä, jonka Microsoft Word- tai Microsoft Excel -asiakirjan tekijä on määrittänyt lisäämään asiakirjaan allekirjoitusrivin. Ehdotettuna allekirjoittajana voit toimia sinä itse tai joku muu henkilö, jonka haluat allekirjoittavan asiakirjan. Esimerkiksi jos valmistelet asiakirjan, joka jokaisen osastosi työntekijän on allekirjoitettava, voit lisätä asiakirjan viimeiselle sivulle allekirjoitusrivit näitä käyttäjiä varten ja kehottaa heitä allekirjoittamaan asiakirjan tiettynä päivänä.

Voit lisätä ehdotetun allekirjoittajan Microsoft Word- tai Microsoft Excel -asiakirjaan seuraavasti:

1. Luo ja tallenna asiakirja Microsoft Word- tai Microsoft Excel -muodossa.

2. Valitse **Insert** (Lisää) -valikko.

3. Napsauta **Text** (Teksti) -ryhmän työkalurivillä, **Signature Line** (Allekirjoitusrivi) -kohdan vieressä olevaa nuolta ja valitse **Privacy Manager Signature Provider** (Privacy Managerin allekirjoittaja).

   Signature Setup (Allekirjoituksen asetukset) -valintaikkuna tulee näyttöön.

4. Kirjoita ehdotetun allekirjoittajan nimi **Suggested signer** (Ehdotettu allekirjoittaja) -kohdan alla olevaan tekstiruutuun.

5. Kirjoita ehdotetulle allekirjoittajalle viesti **Instructions to the signer** (Ohjeita allekirjoittajalle) -kohdan alla olevaan tekstiruutuun.

   HUOMAUTUS: Tämä viesti näkyy otsikon tilalla, ja se poistetaan tai korvataan käyttäjän asemalla, kun asiakirja allekirjoitetaan.

6. Näytä päivämäärä valitsemalla **Show sign date in signature line** (Näytä allekirjoituksen päivämäärä allekirjoitusrivillä) -valintaruutu.

7. Näytä otsikko valitsemalla **Show signer's title in signature line** (Näytä allekirjoittajan asema allekirjoitusrivillä) -valintaruutu.

   HUOMAUTUS: Jos **Show sign date in signature line** (Näytä allekirjoituksen päivämäärä allekirjoitusrivillä)- ja/tai **Show signer's title in signature line** (Näytä allekirjoittajan asema allekirjoitusrivillä) -valintaruudut eivät ole valittuina, ehdotettu allekirjoittaja ei pysty näyttämään päivämäärää ja/tai asemaa otsikkorivillä, vaikka ehdotetun allekirjoittajan asiakirjan asetukset olisi määritetty niin, sillä asiakirjan tekijä määrittää asiakirjalleen ehdotettuja allekirjoittajia.

8. Valitse **OK**.

Ehdotetun allekirjoittajan allekirjoitusrivin lisääminen

Kun ehdotetut allekirjoittajat avaavat asiakirjan, he näkevät nimensä sulkeissa, mikä merkitsee, että heidän on allekirjoitettava kyseinen asiakirja.

Voit allekirjoittaa asiakirjan seuraavasti:

1. Kaksoisnapsauta asianmukaista allekirjoitusriviä.

2. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

Allekirjoitusrivi näytetään asiakirjan tekijän määrittämien asetusten mukaisesti.

Microsoft Office -asiakirjan salaaminen

Voit salata Microsoft Office -asiakirjan itseäsi ja luotettuja yhteyshenkilöitäsi varten. Kun salaat asiakirjan ja suljet sen, sinun ja luettelosta valitsemiesi luotettujen yhteyshenkilöiden on todennettava henkilöllisyytensä ennen asiakirjan avaamista.

Voit salata Microsoft Office -asiakirjan seuraavasti:

1. Luo ja tallenna asiakirja Microsoft Word-, Microsoft Excel- tai Microsoft PowerPoint -muodossa.
2. Valitse **Home** (Koti) -valikko.
3. Napsauta **Sign and Encrypt** (Allekirjoita ja salaa) -kohdan vieressä olevaa alanuolta ja valitse **Encrypt Document** (Salaa asiakirja).

   Select Trusted Contacts (Valitse luotetut yhteyshenkilöt) -valintaikkuna tulee näyttöön.
4. Napsauta sen luotetun yhteyshenkilön nimeä, jolle haluat antaa luvan avata asiakirjan ja tarkastella sen sisältöä.

HUOMAUTUS: Jos haluat valita useita luotettuja yhteyshenkilöitä, pidä ctrl-näppäintä painettuna ja napsauta yksittäisiä nimiä.

5. Valitse **OK**.

Jos päätät muokata asiakirjaa myöhemmin, toimi kohdassa Microsoft Office -asiakirjan salauksen poistaminen sivulla 58 annettujen ohjeiden mukaisesti. Voit muokata asiakirjaa salauksen poistamisen jälkeen. Voit salata asiakirjan uudelleen toimimalla tämän kohdan ohjeiden mukaan.

Microsoft Office -asiakirjan salauksen poistaminen

Kun poistat Microsoft Office -asiakirjan salauksen, sinun ja luotettujen yhteyshenkilöiden ei enää tarvitse todentaa henkilöllisyyttään asiakirjan avaamista ja sen sisällön tarkastelemista varten.

Voit poistaa Microsoft Office -asiakirjan salauksen seuraavasti:

1. Avaa salattu Microsoft Word-, Microsoft Excel- tai Microsoft PowerPoint -asiakirja.
2. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.
3. Valitse **Home** (Koti) -valikko.
4. Napsauta **Sign and Encrypt** (Allekirjoita ja salaa) -kohdan vieressä olevaa alanuolta ja valitse **Remove Encryption** (Poista salaus).

Salatun Microsoft Office -asiakirjan lähettäminen

Voit liittää salatun Microsoft Office -asiakirjan sähköpostiviestiin ilman itse sähköpostiviestin allekirjoittamista tai salaamista. Sinun ei tarvitse tehdä muuta kuin luoda salatun asiakirjan sisältävä sähköpostiviesti ja lähettää se aivan samalla tavalla kuin mikä tahansa liitetiedoston sisältävä sähköpostiviesti.

Parhaan mahdollisen suojauksen varmistamiseksi on kuitenkin suositeltavaa salata sähköpostiviesti, kun siihen liitetään allekirjoitettu tai salattu Microsoft Office -asiakirja.

Voit lähettää allekirjoitetun ja/tai salatun Microsoft Office -asiakirjan sisältävän sinetöidyn sähköpostiviestin seuraavasti:

1. Valitse Microsoft Outlookissa **Uusi** tai **Vastaa**.
2. Kirjoita sähköpostiviesti.
3. Liitä Microsoft Office -asiakirja.
4. Lisäohjeita löydät kohdasta Sähköpostiviestin sinetöiminen ja lähettäminen sivulla 55.

Allekirjoitetun Microsoft Office -asiakirjan tarkasteleminen

HUOMAUTUS: Allekirjoitetun Microsoft Office -asiakirjan tarkastelemiseen ei tarvita Privacy Manager -varmennetta.

Kun allekirjoitettu Microsoft Office -asiakirja avataan, asiakirjaikkunan alareunassa olevalle tilariville ilmestyy Digital Signature (Digitaalinen allekirjoitus) -kuvake.

1. Napsauta **Digital Signatures** (Digitaaliset allekirjoitukset) -kuvaketta, jos haluat vaihdella Signatures (Allekirjoitukset) -valintaikkunaa, jossa näkyvät kaikkien asiakirjan allekirjoittaneiden käyttäjien nimet ja allekirjoituspäivät.
2. Jos haluat näyttää lisätietoja kustakin allekirjoituksesta, napsauta nimeä Signatures (Allekirjoitukset) -valintaikkunassa hiiren kakkospainikkeella ja valitse Signature Details (Allekirjoituksen tiedot).

Salatun Microsoft Office -asiakirjan tarkasteleminen

Toisesta tietokoneesta peräisin olevan salatun Microsoft Office -asiakirjan tarkasteleminen edellyttää, että Privacy Manager on asennettu siihen tietokoneeseen, jossa asiakirjaa tarkastellaan. Lisäksi on palautettava tiedoston salaamiseen käytetty Privacy Manager -varmenne.

Jos luotettu yhteyshenkilö haluaa tarkastella salattua Microsoft Office -asiakirjaa, hänen tietokoneessaan on oltava Privacy Manager ja Privacy Manager -varmenne. Lisäksi salatun Microsoft Office -asiakirjan tekijän on valittava kyseinen henkilö luotetuksi yhteyshenkilöksi.

Privacy Managerin käyttäminen Windows Live Messengerissä

Privacy Manager lisää seuraavat suojatut tietoliikenneominaisuudet Windows Live Messengeriin:

- **Secure chat** (Suojattu keskustelu) – Viestit lähetetään SSL/TLS (Secure Sockets Layer/Transport Layer Security) over XML -protokollan välityksellä. Tällä samalla tekniikalla varmistetaan myös sähköisten kaupankäyntitapahtumien turvallisuus.
- **Recipient identification** (Vastaanottajien tunnistus) – Voit tarkistaa henkilön läsnäolon ja henkilöllisyyden ennen viestin lähettämistä.
- **Signed messages** (Allekirjoitetut viestit) – Voit allekirjoittaa viestit sähköisesti. Jos viestiä peukaloidaan, se merkitään virheelliseksi, kun vastaanottaja saa sen.
- **Hide/show feature** (Piilota/näytä-toiminto) – Voit piilottaa minkä tahansa viestin tai kaikki viestit Privacy Manager Chat -välilehdessä. Voit lähettää myös viestin, jonka sisältö on piilotettu. Todennus on suoritettava ennen viestin näyttämistä.

- **Secure chat history** (Suojattu keskusteluhistoria) – Keskusteluistuntojen lokit salataan ennen tallennusta ja ne vaativat todennusta, ennen kuin niitä voidaan tarkastella.
- **Automatic locking/unlocking** (Automaattinen lukitseminen / lukituksen poistaminen) – Voit lukita Privacy Manager Chat -ikkunan ja poistaa sen lukituksen tai määrittää sen lukittumaan automaattisesti, kun sitä ei ole käytetty tiettyyn aikaan.

Privacy Manager Chat -istunnon käynnistäminen

HUOMAUTUS: Privacy Manager Chatin käyttäminen edellyttää, että molemmat osapuolet ovat asentaneet Privacy Managerin ja Privacy Manager -varmenteen. Lisätietoja Privacy Manager -varmenteen asentamisesta on kohdassa Privacy Manager -varmenteen pyytäminen ja asentaminen sivulla 47.

1. Voit käynnistää Privacy Manager Chatin Windows Live Messengerissä jollakin seuraavista tavoista:

   a. Napsauta hiiren kakkospainikkeella Live Messengerin online-tilassa olevaa yhteyshenkilöä ja valitse **Start an Activity** (Aloita aktiviteetti).

   b. Valitse **Start Chat** (Aloita keskustelu).

   TAI

   a. Kaksoisnapsauta Live Messengerin online-tilassa olevaa yhteyshenkilöä ja valitse **See a list of activities** (Katso toimintojen luettelo) -valikko.

   b. Valitse **Action** (Toiminto) ja sitten **Start Chat** (Aloita keskustelu).

   TAI

   a. Napsauta tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **ProtectTools**-kuvaketta hiiren kakkospainikkeella, valitse **Privacy Manager for HP ProtectTools** ja napsauta **Start Chat** (Aloita keskustelu) -painiketta.

   b. Valitse Live Messengerissä **Actions: Start an Activity** (Toiminnot: aloita aktiviteetti) ja sitten **Privacy Manager Chat**.

   HUOMAUTUS: Jokaisen käyttäjän on oltava Live Messengerissä online-tilassa ja käyttäjien on näyttävä toistensa Live Messengerin online-ikkunassa. Valitse online-tilassa oleva käyttäjä napsauttamalla.

   Privacy Manager lähettää yhteyshenkilölle kutsun käynnistää Privacy Manager Chat. Kun kutsuttu yhteyshenkilö hyväksyy pyynnön, Privacy Manager Chat -ikkuna avautuu. Jos kutsutulla yhteyshenkilöllä ei ole Privacy Manageria, häntä kehotetaan lataamaan se.

2. Aloita suojattu keskustelu valitsemalla **Start** (Aloita).

Privacy Managerin asetusten määrittäminen Windows Live Messengeriä varten

1. Napsauta Privacy Manager Chatissa **Settings** (Asetukset) -painiketta.

   TAI

   Valitse Privacy Managerissa **Settings** (Asetukset) ja napsauta **Chat** (Keskustelu) -välilehteä.

   TAI

   Napsauta Privacy Manager Live Messenger History Viewerissa **Settings** (Asetukset) -painiketta.

2. Määritä aika, jonka Privacy Manager Chat odottaa ennen istunnon lukitsemista, valitsemalla numero **Lock session after _ minutes of activity** (Lukitse istunto _ minuutin toiminnan jälkeen) -luettelosta.

3. Jos haluat määrittää keskusteluistuntojen historian sisältävän kansion, etsi kansio valitsemalla **Browse** (Selaa) ja valitse **OK**.

4. Valitsemalla **Automatically save secure chat history** (Tallenna suojatun keskustelun historia automaattisesti) -valintaruudun voit salata ja tallentaa istunnot automaattisesti, kun ne suljetaan.

5. Valitse **OK**.

Keskusteleminen Privacy Manager Chat -ikkunassa

Privacy Manager Chatin käynnistämisen jälkeen Windows Live Messengeriin avautuu Privacy Manager Chat -ikkuna. Privacy Manager Chatin käyttö muistuttaa Windows Live Messengerin peruskäyttöä, mutta Privacy Manager Chatin ikkunassa ovat käytettävissä seuraavat lisätoiminnot:

- **Save** (Tallenna) – Tätä painiketta napsauttamalla voit tallentaa keskusteluistunnon kokoonpanoasetuksissa määritettyyn kansioon. Voit myös määrittää Privacy Manager Chatin tallentamaan jokaisen istunnon automaattisesti, kun se suljetaan.

- **Hide all** (Piilota kaikki) ja **Show all** (Näytä kaikki) – Asianmukaista painiketta napsauttamalla voit laajentaa tai kutistaa Secure Communications (Suojattu tietoliikenne) -ikkunassa näkyvät viestit. Voit myös piilottaa tai näyttää yksittäisiä viestejä napsauttamalla niiden otsikoita.

- **Are you there?** (Oletko siellä?) – Tätä painiketta napsauttamalla voit pyytää yhteyshenkilöä todentamaan henkilöllisyytensä.

- **Lock** (Lukitse) – Tätä painiketta napsauttamalla voit sulkea Privacy Manager Chat -ikkunan ja palata Chat Entry (Keskustelun syöttö) -ikkunaan. Jos haluat näyttää Secure Communications (Suojattu tietoliikenne) -ikkunan uudelleen, valitse **Resume the session** (Jatka istuntoa) ja todenna henkilöllisyytesi valitsemaasi suojattua kirjautumistapaa käyttäen.

- **Send** (Lähetä) – Tätä painiketta napsauttamalla voit lähettää yhteyshenkilölle salatun viestin.

- **Send signed** (Lähetä allekirjoitettuna) – Valitse tämä valintaruutu, jos haluat allekirjoittaa ja salata viestisi sähköisesti. Jos viestiä peukaloidaan, se merkitään virheelliseksi, kun vastaanottaja saa sen. Sinun on todennettava henkilöllisyytesi aina, kun lähetät allekirjoitetun viestin.

- **Send hidden** (Lähetä piilotettuna) – Valitse tämä valintaruutu, jos haluat salata ja lähettää viestin, josta näkyy vain otsikko. Yhteyshenkilön on todennettava henkilöllisyytensä, ennen kuin hän pystyy lukemaan viestin sisällön.

Keskusteluhistorian tarkasteleminen

Privacy Manager Chat: Live Messenger History Viewer näyttää salattujen Privacy Manager Chat -istuntojen tiedostot. Voit tallentaa istunnot napsauttamalla Privacy Manager Chat -ikkunassa **Save** (Tallenna) tai määrittämällä automaattisen tallennuksen Privacy Managerin Chat (Keskustelu) -välilehdessä. Katseluohjelmassa jokaisesta istunnosta näytetään (salattu) yhteyshenkilön näyttönimi sekä istunnon alkamis- ja päättymispäivämäärä ja -aika. Oletusarvoisesti näytetään kaikkien määrittämiesi sähköpostitilien istunnot. **Display history for** (Näytä historia) -valikossa voit valita tarkasteltaviksi vain tiettyjä tilejä.

Katseluohjelman avulla voit suorittaa seuraavat tehtävät:

- Paljasta kaikki istunnot sivulla 62
- Paljasta tietyn tilin istunnot sivulla 62
- Näytä istunnon tunnus sivulla 63
- Näytä istunto sivulla 63
- Hae istunnoista tiettyä tekstiä sivulla 63
- Poista istunto sivulla 63
- Lisää tai poista sarakkeita sivulla 64
- Suodata näytettyjä istuntoja sivulla 64

Voit käynnistää Live Messenger History Viewerin seuraavasti:

▲ Napsauta hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **HP ProtectTools** -kuvaketta, valitse **Privacy Manager: for HP ProtectTools** ja napsauta **Live Messenger History Viewer** -painiketta.

TAI

▲ Valitse keskusteluistunnon aikana **History Viewer** (Historian katseluohjelma) tai **History** (Historia).

Paljasta kaikki istunnot

Paljastamalla kaikki istunnot voit näyttää valittujen istuntojen ja samalla tilillä olevien istuntojen yhteyshenkilön näyttönimen salaamattomana.

Voit paljastaa kaikki tallennetut keskusteluhistoriaistunnot seuraavasti:

1. Napsauta Live Messenger History Viewerissa mitä tahansa istuntoa hiiren kakkospainikkeella ja valitse **Reveal All Sessions** (Paljasta kaikki istunnot).
2. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

   Yhteyshenkilöiden näyttönimien salaus puretaan.
3. Kaksoisnapsauta istuntoa, jonka sisältöä haluat tarkastella.

Paljasta tietyn tilin istunnot

Paljastamalla istunnon voit näyttää valittuna olevan istunnon yhteyshenkilön näyttönimen salaamattomana.

Voit paljastaa tietyn keskusteluhistoriaistunnon seuraavasti:

1. Napsauta Live Messenger History Viewerissa mitä tahansa istuntoa hiiren kakkospainikkeella ja valitse **Reveal Session** (Paljasta istunto).
2. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

   Yhteyshenkilön näyttönimen salaus puretaan.
3. Kaksoisnapsauta paljastettua istuntoa, jonka sisältöä haluat tarkastella.

HUOMAUTUS: Muiden samalla varmenteella salattujen istuntojen vieressä näkyy lukitsematon kuvake, joka osoittaa, että voit tarkastella kyseisiä istuntoja kaksoisnapsauttamalla ilman lisätodennusta. Eri varmenteella salattujen istuntojen vieressä näkyy lukittu kuvake, joka osoittaa, että kyseiset istunnot vaativat lisätodennusta, ennen kuin yhteyshenkilön näyttönimeä tai istunnon sisältöä voidaan tarkastella.

Näytä istunnon tunnus

Voit näyttää istunnon tunnuksen seuraavasti:

- Napsauta Live Messenger History Viewerissa mitä tahansa paljastettua istuntoa hiiren kakkospainikkeella ja valitse **View session ID** (Näytä istunnon tunnus).

Näytä istunto

Istuntoa tarkasteltaessa tiedosto avautuu tarkastelemista varten. Jos istuntoa ei ole vielä paljastettu (salaamatonta yhteyshenkilön näyttönimeä ei ole vielä näytetty), se paljastetaan samalla kertaa.

Voit tarkastella Live Messengerin historiaistuntoa seuraavasti:

1. Napsauta Live Messenger History Viewerissa mitä tahansa istuntoa hiiren kakkospainikkeella ja valitse **View** (Näytä).
2. Suorita pyydettäessä todennus valitsemaasi suojattua kirjautumistapaa käyttäen.

   Istunnon sisällön salaus puretaan.

Hae istunnoista tiettyä tekstiä

Voit hakea tekstiä vain katseluohjelman ikkunassa näkyvistä istunnoista, jotka on paljastettu (joiden salaus on purettu). Näissä istunnoissa yhteyshenkilön näyttönimi näkyy tavallisena tekstinä.

Voit hakea tekstiä keskusteluhistoriaistunnoista seuraavasti:

1. Napsauta Live Messenger History Viewerissa **Search** (Hae) -painiketta.
2. Anna haettava teksti, määritä haluamasi hakuparametrit ja valitse **OK**.

   Tekstiä sisältävät istunnot korostetaan katseluohjelman ikkunassa.

Poista istunto

1. Valitse keskusteluhistoriaistunto.
2. Valitse **Delete** (Poista).

Lisää tai poista sarakkeita

Oletusarvoisesti Live Messenger History Viewer näyttää kolme yleisimmin käytettyä saraketta. Voit lisätä näyttöön uusia sarakkeita tai poistaa sarakkeita näytöstä.

Voit lisätä sarakkeita näyttöön seuraavasti:

1. Napsauta hiiren kakkospainikkeella minkä tahansa sarakkeen otsikkoa ja valitse **Add/Remove Columns** (Lisää/poista sarakkeita).
2. Valitse sarakkeen otsikko vasemmasta ruudusta ja siirrä se oikeaan ruutuun valitsemalla **Add** (Lisää).

Voit poistaa sarakkeita näytöstä seuraavasti:

1. Napsauta hiiren kakkospainikkeella minkä tahansa sarakkeen otsikkoa ja valitse **Add/Remove Columns** (Lisää/poista sarakkeita).
2. Valitse sarakkeen otsikko oikeasta ruudusta ja siirrä se vasempaan ruutuun valitsemalla **Remove** (Poista).

Suodata näytettyjä istuntoja

Live Messenger History Viewer näyttää kaikkien tilien istuntojen luettelon. Voit myös suodattaa näytettäviä istuntoja seuraavasti:

- Tietyt tilit. Lisätietoja on kohdassa Tietyn tilin istuntojen näyttäminen sivulla 64.
- Päivämääräalueet. Lisätietoja on kohdassa Tietyllä aikavälillä olevien istuntojen näyttäminen sivulla 64.
- Eri kansiot. Lisätietoja on kohdassa Muuhun kuin oletuskansioon tallennettujen istuntojen näyttäminen sivulla 64.

Tietyn tilin istuntojen näyttäminen

▲ Valitse tili Live Messenger History Viewerin **Display history for** (Näytä historia) -valikosta.

Tietyllä aikavälillä olevien istuntojen näyttäminen

1. Napsauta Live Messenger History Viewerissa **Advanced Filter** (Erikoissuodatus) -kuvaketta.

   Advanced Filter (Erikoissuodatus) -valintaikkuna tulee näyttöön.

2. Valitse **Display only sessions within specified date range** (Näytä vain määrätyllä aikavälillä olevat istunnot) -valintaruutu.
3. Valitse päivämäärät kirjoittamalla päivä, kuukausi ja/tai vuosi **From date** (Alkamispäivämäärä)- ja **To date** (Päättymispäivämäärä) -tekstiruutuihin tai napsauttamalla kalenterin vieressä olevaa nuolta.
4. Valitse **OK**.

Muuhun kuin oletuskansioon tallennettujen istuntojen näyttäminen

1. Napsauta Live Messenger History Viewerissa **Advanced Filter** (Erikoissuodatus) -kuvaketta.
2. Valitse **Use an alternate history files folder** (Käytä vaihtoehtoista historiatiedostojen kansiota) -valintaruutu.

3. Hae kansio antamalla kansion sijainti tai valitsemalla **Browse** (Selaa).
4. Valitse **OK**.

Lisätoiminnot

Privacy Manager -varmenteiden ja luotettujen yhteyshenkilöiden siirtäminen toiseen tietokoneeseen

Voit siirtää Privacy Manager -varmenteet ja luotetut yhteyshenkilöt turvallisesti toiseen tietokoneeseen tai varmuuskopioida tiedot varmuuden vuoksi. Voit tehdä tämän varmuuskopioimalla tiedot salasanalla suojattuna tiedostona verkkosijaintiin tai siirrettävään tallennusvälineeseen ja palauttamalla tiedoston uuteen tietokoneeseen.

Privacy Manager -varmenteiden ja luotettujen yhteyshenkilöiden varmuuskopiointi

Voit varmuuskopioida Privacy Manager -varmenteet ja luotetut yhteyshenkilöt salasanalla suojattuun tiedostoon seuraavasti:

1. Avaa Privacy Manager ja valitse **Migration** (Siirto).
2. Valitse **Backup** (Varmuuskopioi).
3. Valitse Select Data (Valitse tiedot) -sivulla siirtotiedostoon sisällytettävien tietojen luokat ja valitse **Next** (Seuraava).
4. Anna Migration File (Siirtotiedosto) -sivulla tiedoston nimi tai etsi sijainti valitsemalla **Browse** (Selaa), ja valitse **Next** (Seuraava).
5. Anna salasana, vahvista se ja valitse **Next** (Seuraava).

   HUOMAUTUS: Tallenna salasana turvalliseen paikkaan, sillä tarvitset sitä siirtotiedoston palauttamiseen.

6. Suorita todennus valitsemaasi suojattua kirjautumistapaa käyttäen.
7. Valitse Migration File Saved (Siirtotiedosto tallennettu) -sivulta **Finish** (Valmis).

Privacy Manager -varmenteiden ja luotettujen yhteyshenkilöiden palauttaminen

Voit palauttaa Privacy Manager -varmenteet ja luotetut yhteyshenkilöt toiseen tietokoneeseen osana siirtoprosessia tai samaan tietokoneeseen seuraavasti:

1. Avaa Privacy Manager ja valitse **Migration** (Siirto).
2. Valitse **Restore** (Palauta).
3. Hae tiedosto valitsemalla Migration File (Siirtotiedosto) -sivulta **Browse** (Selaa), ja valitse **Next** (Seuraava).
4. Anna varmuuskopiotiedoston luonnin yhteydessä käytetty salasana ja valitse **Next** (Seuraava).
5. Valitse Migration File (Siirtotiedosto) -sivulta **Finish** (Valmis).

Privacy Managerin keskitetty hallinta

Privacy Manager -asennus voi kuulua järjestelmänvalvojan mukauttamaan keskitettyyn asennukseen. Yksi tai useampi seuraavista toiminnoista on ehkä otettu käyttöön tai poistettu käytöstä:

- **Certificate use policy** (Varmenteen käyttökäytäntö) – Voit ehkä käyttää vain Comodon myöntämiä Privacy Manager -varmenteita tai käyttää myös muiden myöntäjien digitaalisia varmenteita.
- **Encryption policy** (Salauskäytäntö) – Salaustoiminnot on ehkä otettu yksilöllisesti käyttöön tai poistettu käytöstä Microsoft Officessa tai Outlookissa ja Windows Live Messengerissä.

10 File Sanitizer for HP ProtectTools

File Sanitizer on työkalu, jonka avulla voit turvallisesti hävittää tietokoneessa olevan omaisuuden (henkilökohtaiset tiedot tai tiedostot, historiallisen tai Internetin käyttöön liittyvän sisällön tai muut aineistot) ja tyhjentää kiintolevyn säännöllisesti.

HUOMAUTUS: Tämä File Sanitizerin versio tukee vain järjestelmän kiintolevyn käyttöä.

Hävittäminen

Hävittäminen eroaa Windowsin® tavallisesta poistotoiminnosta (jota File Sanitizerissa kutsutaan tavalliseksi poistamiseksi) siinä, että File Sanitizerilla omaisuutta hävitettäessä käytetään algoritmia, joka sekoittaa haetut tiedot ja tekee alkuperäisen omaisuuden käytön lähes mahdottomaksi. Windowsin tavallinen poistotoiminto voi jättää tiedoston (tai omaisuuden) kiintolevylle ehjänä tai sellaiseen tilaan, jossa tiedosto (tai omaisuus) voidaan palauttaa rikosteknisin keinoin.

Kun valitset hävitysprofiilin (vahva suojaus, keskitasoinen suojaus tai heikko suojaus), hävittämistä varten valitaan automaattisesti valmiiksi määritetty omaisuusluettelo ja poistotapa. Voit myös mukauttaa hävitysprofiilia ja määrittää hävitysjaksojen määrän, hävitykseen sisällytettävän omaisuuden, ennen hävitystä vahvistettavan omaisuuden ja hävityksessä ohitettavan omaisuuden. Lisätietoja on kohdassa Hävitysprofiilin valitseminen tai luominen sivulla 72.

Voit määrittää automaattisen hävitysaikataulun ja hävittää omaisuutta manuaalisesti milloin tahansa. Lisätietoja on kohdassa Hävitysaikataulun määrittäminen sivulla 71, Yhden pääoman manuaalinen hävittäminen sivulla 76 tai Kaikkien valittujen kohteiden manuaalinen hävittäminen sivulla 77.

HUOMAUTUS: .dll-tiedosto hävitetään ja poistetaan järjestelmästä vain silloin, jos se on siirretty roskakoriin.

Vapaan tilan tyhjennys

Omaisuuden hävittäminen Windowsissa ei poista omaisuuden sisältöä kiintolevyltä kokonaan. Windows poistaa vain viittauksen omaisuuteen. Omaisuuden sisältö jää kiintolevylle, kunnes kiintolevyn samalle alueelle tallennettava omaisuus korvaa sisällön uusilla tiedoilla.

Vapaan tilan tyhjennyksen avulla voit kirjoittaa sattumanvaraista tietoa poistetun omaisuuden päälle, mikä estää poistetun omaisuuden alkuperäisen sisällön tarkastelun.

HUOMAUTUS: Vapaan tilan tyhjennys on tarkoitettu Windowsin roskakorin avulla tai manuaalisesti poistetulle omaisuudelle. Vapaan tilan tyhjennys ei paranna hävitetyn omaisuuden suojausta.

Voit määrittää vapaan tilan tyhjennykselle automaattisen aikataulun tai ottaa sen manuaalisesti käyttöön napsauttamalla tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **HP ProtectTools** -kuvaketta. Lisätietoja on kohdassa Vapaan tilan tyhjennyksen aikataulun määrittäminen sivulla 72 tai Vapaan tilan tyhjennyksen manuaalinen käynnistäminen sivulla 77.

Asennusohjeet

File Sanitizerin avaaminen

Voit avata File Sanitizerin seuraavasti:

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Security Manager**.
2. Valitse **File Sanitizer**.

TAI

▲ Kaksoisnapsauta työpöydällä olevaa **File Sanitizer** -kuvaketta.

TAI

▲ Napsauta hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **HP ProtectTools** -kuvaketta, valitse **File Sanitizer** ja sitten **Open File Sanitizer** (Avaa File Sanitizer).

Hävitysaikataulun määrittäminen

HUOMAUTUS: Lisätietoja valmiiksi määritetyn hävitysprofiilin valitsemisesta tai hävitysprofiilin luomisesta on kohdassa Hävitysprofiilin valitseminen tai luominen sivulla 72.

HUOMAUTUS: Lisätietoja omaisuuden manuaalisesta hävittämisestä on kohdassa Yhden pääoman manuaalinen hävittäminen sivulla 76.

1. Avaa File Sanitizer ja valitse **Shred** (Hävitä).
2. Valitse hävitysvaihtoehto:
   - **Windows shutdown** (Windowsin sammutus) – Valitse tämä vaihtoehto, jos haluat hävittää kaiken valitun omaisuuden Windowsin sammutuksen yhteydessä.

     HUOMAUTUS: Kun tämä vaihtoehto on valittuna, näyttöön tulee tietokonetta sammutettaessa valintaikkuna, jossa kysytään, että haluatko jatkaa valitun omaisuuden hävittämistä vai ohittaa toiminnon. Valitse **Yes** (Kyllä), jos haluat ohittaa hävittämisen, ja **No** (Ei), jos haluat jatkaa hävittämistä.
   - **Web browser open** (Web-selainen avaus) – Valitse tämä vaihtoehto, jos haluat hävittää kaiken Web-omaisuuden, kuten selaimen URL-osoitteiden historian, kun avaat Web-selaimen.
   - **Web browser quit** (Web-selaimen lopetus) – Valitse tämä vaihtoehto, jos haluat hävittää kaiken Web-omaisuuden, kuten selaimen URL-osoitteiden historian, kun suljet Web-selaimen.
   - **Key sequence** (Näppäinyhdistelmä) – Valitse tämä vaihtoehto, jos haluat käynnistää hävittämisen näppäinyhdistelmän avulla.
   - **Scheduler** (Ajoitus) – Valitse **Activate Scheduler** (Ota ajoitus käyttöön) -valintaruutu, anna Windowsin salasana ja määritä valitun omaisuuden hävitysajankohta antamalla päivä ja aika.

   HUOMAUTUS: .dll-tiedosto hävitetään ja poistetaan järjestelmästä vain silloin, jos se on siirretty roskakoriin.
3. Valitse **Apply** (Käytä) ja sitten **OK**.

Vapaan tilan tyhjennyksen aikataulun määrittäminen

HUOMAUTUS: Vapaan tilan tyhjennys on tarkoitettu Windowsin roskakorin avulla tai manuaalisesti poistetulle omaisuudelle. Vapaan tilan tyhjennys ei paranna hävitetyn omaisuuden suojausta.

Voit määrittää vapaan tilan tyhjennyksen aikataulun seuraavasti:

1. Avaa File Sanitizer ja valitse **Free Space Bleaching** (Vapaan tilan tyhjennys).
2. Valitse **Activate Scheduler** (Ota ajoitus käyttöön) -valintaruutu, anna Windowsin salasana ja määritä kiintolevyn tyhjennysajankohta antamalla päivä ja aika.
3. Valitse **Apply** (Käytä) ja sitten **OK**.

HUOMAUTUS: Vapaan tilan tyhjennys voi kestää pitkään. Vaikka vapaan tilan tyhjennys suoritetaan taustalla, tietokone voi hidastua suorittimen lisääntyneen kuormituksen seurauksena.

Hävitysprofiilin valitseminen tai luominen

Voit määrittää tyhjennystavan ja valita hävitettävän omaisuuden valitsemalla valmiiksi määritetyn profiilin tai luomalla oman profiilin.

Valmiiksi määritetyn hävitysprofiilin valitseminen

Kun valitset valmiiksi määritetyn hävitysprofiilin (vahva suojaus, keskitasoinen suojaus tai heikko suojaus), hävittämistä varten valitaan automaattisesti valmiiksi määritetty poistotapa ja omaisuusluettelo. Napsauttamalla **View Details** (Näytä tiedot) -painiketta voit tarkastella hävittämistä varten valitun omaisuuden valmiiksi määritettyä luetteloa.

Voit valita valmiiksi määritetyn hävitysprofiilin seuraavasti:

1. Avaa File Sanitizer ja valitse **Settings** (Asetukset).
2. Napsauta valmiiksi määritettyä hävitysprofiilia.
3. Napsauta **View Details** (Näytä tiedot) -painiketta ja tarkastele hävittämistä varten valitun omaisuuden luetteloa.
4. Valitse **Shred the following** (Hävitä seuraavat) -kohdasta niiden omaisuuksien valintaruudut, jotka haluat vahvistaa ennen hävittämistä.
5. Valitse **Apply** (Käytä) ja sitten **OK**.

Hävitysprofiilin mukauttaminen

Kun luot hävitysprofiilin, määrität hävitysjaksojen määrän, hävitykseen sisällytettävän omaisuuden, ennen hävitystä vahvistettavan omaisuuden ja hävityksessä ohitettavan omaisuuden.

1. Avaa File Sanitizer, valitse **Settings** (Asetukset), sitten **Advanced Security Settings** (Suojauksen lisäasetukset) ja lopuksi **View Details** (Näytä tiedot).
2. Määritä hävitysjaksojen määrä.

HUOMAUTUS: Jokaiselle omaisuudelle suoritetaan valittu hävitysjaksojen määrä. Jos esimerkiksi valitset kolme hävitysjaksoa, tiedot sekoittava algoritmi suoritetaan kolme kertaa. Jos valitset vahvan suojauksen hävitysjaksot, hävittäminen voi kestää pitkään. Hävitysjaksojen määrää lisäämisen myötä on kuitenkin entistä epätodennäköisempää, että tiedot voidaan palauttaa.

3. Valitse hävitettävä omaisuus:

   a. Napsauta omaisuutta **Available shred options** (Käytettävissä olevat hävitysvaihtoehdot) -kohdassa ja valitse **Add** (Lisää).

   b. Jos haluat lisätä mukautettavan omaisuuden, valitse **Add Custom Option** (Lisää mukautettu vaihtoehto) ja etsi tai kirjoita tiedoston tai kansion polku. Valitse **Open** (Avaa) ja sitten **OK**. Napsauta mukautettavaa omaisuutta **Available shred options** (Käytettävissä olevat hävitysvaihtoehdot) -kohdassa ja valitse **Add** (Lisää).

HUOMAUTUS: Jos haluat poistaa omaisuuden käytettävissä olevien hävitysvaihtoehtojen luettelosta, napsauta omaisuutta ja valitse **Delete** (Poista).

4. Valitse **Shred the following** (Hävitä seuraavat) -kohdasta niiden omaisuuksien valintaruudut, jotka haluat vahvistaa ennen hävittämistä.

HUOMAUTUS: Jos haluat poistaa omaisuuden hävitettävien omaisuuksien luettelosta, napsauta omaisuutta ja valitse **Remove** (Poista).

5. Jos haluat suojata tiedostot tai kansiot automaattiselta hävittämiseltä, valitse **Do not shred the following** (Älä hävitä seuraavia) -kohdasta **Add** (Lisää) ja valitse tai kirjoita sen jälkeen tiedoston tai kansion polku. Valitse **Open** (Avaa) ja sitten **OK**.

HUOMAUTUS: Jos haluat poistaa omaisuuden poikkeusluettelosta, napsauta omaisuutta ja valitse **Delete** (Poista).

6. Kun olet määrittänyt hävitysprofiilin, valitse **Apply** (Käytä) ja sitten **OK**.

Tavallisen poistoprofiilin mukauttaminen

Tavallinen poistoprofiili poistaa omaisuuden tavalliseen tapaan sitä hävittämättä. Kun mukautat tavallista poistoprofiilia, määrität tavalliseen poistamiseen sisällytettävän omaisuuden, ennen tavallista poistamista vahvistettavan omaisuuden ja tavallisessa poistamisessa ohitettavan omaisuuden.

HUOMAUTUS: Jos käytät tavallista poistotoimintoa, vapaan tilan tyhjennys voidaan ajoittain suorittaa manuaalisesti tai Windowsin roskakorin avulla poistetulle omaisuudelle.

Voit mukauttaa tavallista poistoprofiilia seuraavasti:

1. Avaa File Sanitizer, valitse **Settings** (Asetukset), sitten **Simple Delete Setting** (Tavallisen poiston asetukset) ja lopuksi **View Details** (Näytä tiedot).

2. Valitse poistettava omaisuus:

   a. Napsauta omaisuutta **Available delete options** (Käytettävissä olevat poistovaihtoehdot) -kohdassa ja valitse **Add** (Lisää).

   b. Jos haluat lisätä mukautettavan omaisuuden, valitse **Add Custom Option** (Lisää mukautettu vaihtoehto), anna tiedoston tai kansion nimi ja valitse **OK**. Napsauta mukautettua omaisuutta ja valitse **Add** (Lisää).

HUOMAUTUS: Jos haluat poistaa omaisuuden käytettävissä olevien poistovaihtoehtojen luettelosta, napsauta omaisuutta ja valitse **Delete** (Poista).

3. Valitse **Delete the following** (Poista seuraavat) -kohdasta niiden omaisuuksien valintaruudut, jotka haluat vahvistaa ennen poistamista.

HUOMAUTUS: Jos haluat poistaa omaisuuden poistettavien omaisuuksien luettelosta, napsauta omaisuutta ja valitse **Remove** (Poista).

4. Napsauta **Do not delete the following** (Älä poista seuraavia) -kohdassa **Add** (Lisää) ja valitse niiden omaisuuksien valintaruudut, jotka haluat ohittaa poistamisessa.

HUOMAUTUS: Jos haluat poistaa omaisuuden poikkeusluettelosta, napsauta omaisuutta ja valitse **Delete** (Poista).

5. Kun olet määrittänyt tavallisen poistoprofiilin, valitse **Apply** (Käytä) ja sitten **OK**.

Yleiset tehtävät

Voit suorittaa File Sanitizerin avulla seuraavat tehtävät:

- Use a key sequence to initiate shredding (Käytä näppäinyhdistelmää hävittämisen käynnistämiseen) – Tämän toiminnon avulla voit luoda näppäinyhdistelmän (esimerkiksi ctrl+alt +s) hävittämisen käynnistämiseen. Lisätietoja on kohdassa Hävittämisen käynnistäminen näppäinyhdistelmän avulla sivulla 75.
- Use the File Sanitizer icon to initiate shredding (Käytä File Sanitizer -kuvaketta hävittämisen käynnistämiseen) – Tämä toiminto vastaa Windowsin vedä ja pudota -toimintoa. Lisätietoja on kohdassa File Sanitizer -kuvakkeen käyttäminen sivulla 76.
- Manually shred a specific asset or all selected assets (Hävitä tietty omaisuus tai kaikki valitut omaisuudet manuaalisesti) – Näiden toimintojen avulla voit hävittää kohteet manuaalisesti ilman säännöllisen hävitysaikataulun avaamista. Lisätietoja on kohdassa Yhden pääoman manuaalinen hävittäminen sivulla 76 tai Kaikkien valittujen kohteiden manuaalinen hävittäminen sivulla 77.
- Manually activate free space bleaching (Ota vapaan tilan tyhjennys manuaalisesti käyttöön) – Tämän toiminnon avulla voit ottaa vapaan tilan tyhjennyksen manuaalisesti käyttöön. Lisätietoja on kohdassa Vapaan tilan tyhjennyksen manuaalinen käynnistäminen sivulla 77.
- Abort a shred or free space bleaching operation (Keskeytä hävitys- tai vapaan tilan tyhjennystoiminto) – Tämän toiminnon avulla voit pysäyttää hävitys- tai vapaan tilan tyhjennystoiminnon. Lisätietoja on kohdassa Hävittämisen tai vapaan tilan tyhjennyksen keskeyttäminen sivulla 77.
- View the log files (Näytä lokitiedostot) – Tämän toiminnon avulla voit näyttää hävityksen ja vapaan tilan tyhjennyksen lokitiedostot, jotka sisältävät edellisen hävitys- tai vapaan tilan tyhjennystoiminnon suorittamisen aikana ilmenneet virheet. Lisätietoja on kohdassa Lokitiedostojen tarkasteleminen sivulla 77.

HUOMAUTUS: Hävitys- tai vapaan tilan tyhjennystoiminnon suorittaminen voi kestää pitkään. Vaikka hävitys ja vapaan tilan tyhjennys suoritetaan taustalla, tietokone voi hidastua suorittimen lisääntyneen kuormituksen seurauksena.

Hävittämisen käynnistäminen näppäinyhdistelmän avulla

Määritä näppäinyhdistelmä seuraavasti:

1. Avaa File Sanitizer ja valitse **Shred** (Hävitä).
2. Valitse **Key sequence** (Näppäinyhdistelmä) -valintaruutu.
3. Kirjoita merkki tekstiruutuun.
4. Valitse **CTRL**- tai **ALT**-tekstiruutu ja sitten **SHIFT**-tekstiruutu.

   Jos haluat käynnistää hävittämisen esimerkiksi s-näppäimellä ja painamalla ctrl+shift, kirjoita tekstiruutuun `s` ja valitse **CTRL**- ja **SHIFT**-valintaruudut.

HUOMAUTUS: Valitse näppäinyhdistelmä, joka eroaa muista määrittämistäsi näppäinyhdistelmistä.

Voit käynnistää hävittämisen näppäinyhdistelmän avulla seuraavasti:

1. Pidä shift-näppäintä ja ctrl-näppäintä tai alt-näppäintä (tai muuta määrittämääsi näppäinyhdistelmää) painettuna, samalla kun painat valitsemaasi merkkiä.
2. Jos vahvistusvalintaikkuna tulee näyttöön, valitse **Yes** (Kyllä).

File Sanitizer -kuvakkeen käyttäminen

△ **VAROITUS:** Hävitettyä omaisuutta ei voi palauttaa. Harkitse huolellisesti, mitkä kohteet haluat hävittää manuaalisesti.

1. Etsi asiakirja tai kansio, jonka haluat hävittää.
2. Vedä omaisuus työpöydällä olevan **File Sanitizer** -kuvakkeen päälle.
3. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

Yhden pääoman manuaalinen hävittäminen

△ **VAROITUS:** Hävitettyä omaisuutta ei voi palauttaa. Harkitse huolellisesti, mitkä kohteet haluat hävittää manuaalisesti.

1. Napsauta hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **HP ProtectTools** -kuvaketta, valitse **File Sanitizer** ja sitten **Shred One** (Hävitä yksi).
2. Kun Browse (Selaa) -valintaikkuna avautuu, siirry hävitettävän omaisuuden kohdalle ja valitse **OK**.

   HUOMAUTUS: Valittava omaisuus voi olla yksittäinen tiedosto tai kansio.

3. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

TAI

1. Napsauta hiiren kakkospainikkeella työpöydällä olevaa **File Sanitizer** -kuvaketta ja valitse **Shred One** (Hävitä yksi).
2. Kun Browse (Selaa) -valintaikkuna avautuu, siirry hävitettävän omaisuuden kohdalle ja valitse **OK**.
3. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

TAI

1. Avaa File Sanitizer ja valitse **Shred** (Hävitä).
2. Napsauta **Browse** (Selaa) -painiketta.
3. Kun Browse (Selaa) -valintaikkuna avautuu, siirry hävitettävän omaisuuden kohdalle ja valitse **OK**.
4. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

Kaikkien valittujen kohteiden manuaalinen hävittäminen

1. Napsauta hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **HP ProtectTools** -kuvaketta, valitse **File Sanitizer** ja sitten **Shred Now** (Hävitä nyt).
2. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

TAI

1. Napsauta hiiren kakkospainikkeella työpöydällä olevaa **File Sanitizer** -kuvaketta ja valitse **Shred Now** (Hävitä nyt).
2. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

TAI

1. Avaa File Sanitizer ja valitse **Shred** (Hävitä).
2. Napsauta **Shred now** (Hävitä nyt) -painiketta.
3. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

Vapaan tilan tyhjennyksen manuaalinen käynnistäminen

1. Napsauta hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen **HP ProtectTools** -kuvaketta, valitse **File Sanitizer** ja sitten **Bleach Now** (Tyhjennä nyt).
2. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

TAI

1. Avaa File Sanitizer ja valitse **Free Space Bleaching** (Vapaan tilan tyhjennys).
2. Valitse **Bleach Now** (Tyhjennä nyt).
3. Kun vahvistusvalintaikkuna avautuu, valitse **Yes** (Kyllä).

Hävittämisen tai vapaan tilan tyhjennyksen keskeyttäminen

Kun hävitys tai vapaan tilan tyhjennys on käynnissä, ilmaisinalueella olevan HP ProtectTools Security Manager -kuvakkeen yläpuolella on tästä kertova viesti. Viesti sisältää tietoja hävitys- tai vapaan tilan tyhjennysprosessista (edistymisestä prosentteina) ja antaa sinulle mahdollisuuden toiminnon keskeyttämiseen.

Voit keskeyttää toiminnon seuraavasti:

- Napsauta viestiä ja pysäytä toiminto valitsemalla **Stop** (Pysäytä).

Lokitiedostojen tarkasteleminen

Mahdollisista virheistä tai toimintahäiriöistä luodaan lokitiedosto jokaisen hävitys- tai vapaan tilan tyhjennystoiminnon suorittamisen yhteydessä. Lokitiedostot päivitetään aina viimeisimmän hävitys- tai vapaan tilan tyhjennystoiminnon mukaan.

HUOMAUTUS: Onnistuneesti hävitetyt tai tyhjennetyt tiedostot eivät näy lokitiedostoissa.

Yksi lokitiedosto luodaan hävitystoimintoja ja toinen lokitiedosto vapaan tilan tyhjennystoimintoja varten. Molemmat lokitiedostot sijaitsevat kiintolevyllä seuraavissa sijainneissa:

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

11 Device Access Manager for HP ProtectTools (vain tietyt mallit)

Device Access Manager for HP ProtectToolsin avulla Windows®-käyttöjärjestelmän järjestelmänvalvojat voivat hallita järjestelmässä olevien laitteiden käyttöä ja suojata niitä luvattomalta käytöltä:

- Jokaiselle käyttäjälle luodaan laiteprofiili, joka määrittää, mitä laitteita käyttäjällä on oikeus käyttää.
- Käyttäjät on myös järjestelty ryhmiin. Yksi ryhmistä on esimerkiksi laitteiden ylläpitäjät, joka on valmiiksi määritetty ryhmä. Ryhmiä voidaan määrittää myös Ohjauspaneelin Valvontatyökalujen Tietokoneen hallinta -kohdassa.
- Laitteen käyttöoikeus voidaan myöntää tai estää ryhmän jäsenyyden mukaan.
- Laiteluokkien, kuten CD-asemien ja DVD-asemien osalta luku- ja kirjoitusoikeus voidaan myöntää tai estää erikseen.

Rajoitetuille käyttäjille voidaan myös myöntää lupa laitteiden käytön hallintakäytännön lukemiseen ja muokkaamiseen.

Asennusohjeet

Device Access Managerin avaaminen

Voit avata Device Access Managerin seuraavasti:

1. Valitse **Käynnistä**, **Kaikki ohjelmat**, **HP** ja sitten **HP ProtectTools Administrative Console**.
2. Valitse vasemmasta ruudusta **Device Access Manager** (Laitteiden käytön hallinta).

Laitteiden käytön määrittäminen

Device Access Manager for HP ProtectToolsissa on kolme näkymää:

- Simple Configuration (Yksinkertaiset määritykset) -näkymässä voidaan sallia tai estää laiteluokkien käyttö laitteiden järjestelmänvalvojien ryhmän jäsenille.
- Device Class Configuration (Laiteluokkien määritykset) -näkymässä voidaan sallia tai estää laitetyyppien tai tiettyjen laitteiden käyttö tietyille käyttäjille tai ryhmille.
- User Access Settings (Käyttäjien käyttöoikeusasetukset) -näkymässä voidaan määrittää, mitkä käyttäjät voivat tarkastella tai muuttaa Simple Configuration (Yksinkertaiset määritykset)- tai Device Class Configuration (Laiteluokkien määritykset) -näkymän tietoja.

Laitteiden järjestelmänvalvojien ryhmä

Device Access Managerin asentamisen jälkeen luodaan Device Administrators (Laitteiden järjestelmänvalvojat) -ryhmä.

Järjestelmänvalvoja voi ottaa yksinkertaisen laitteiden käytön hallintakäytännön käyttöön estämällä tiettyjen laiteluokkien käytön muilta kuin luotetuilta käyttäjiltä (laitteiden käyttöoikeuden osalta). Suositeltu tapa erottaa laitteiden luotetut ja luottamattomat käyttäjät on lisätä laitteiden luotetut käyttäjät Device Administrators (Laitteiden järjestelmänvalvojat) -ryhmään. Käyttöoikeuden myöntäminen Device Administrators (Laitteiden järjestelmänvalvojat) -ryhmän jäsenille laitteiden käyttöön Simple Configuration (Yksinkertaiset määritykset)- tai Device Class Configuration (Laiteluokkien määritykset) -näkymän kautta takaa, että laitteiden luotetuilla käyttäjillä on täydelliset oikeudet määritettyjen laiteluokkien käyttöön.

HUOMAUTUS: Käyttäjän lisääminen Device Administrators (Laitteiden järjestelmänvalvojat) -ryhmään ei automaattisesti anna käyttäjälle oikeutta laitteiden käyttöön. Simple Configuration (Yksinkertaiset määritykset) -näkymässä laitteiden luotetuille käyttäjille voidaan kuitenkin myöntää oikeus vaadittavien laiteluokkien käyttöön.

Voit lisätä käyttäjiä Device Administrators (Laitteiden järjestelmänvalvojat) -ryhmään seuraavasti:

- Jos käytät Windows 7-, Vista- tai XP Professional -käyttöjärjestelmää, käytä tavallista Paikalliset käyttäjät ja ryhmät -MMC-laajennusta.
- Jos käytät Windows 7-, Vista®- tai XP-käyttöjärjestelmän kotiversiota tai etuoikeutettua tiliä, kirjoita seuraava komento komentokehoteikkunaan:

```
c:\> net localgroup "Device Administrators" username /ADD
```

Yksinkertainen kokoonpano

Järjestelmänvalvojat ja valtuutetut käyttäjät voivat yksinkertaisen määrityksen avulla muokata seuraavien laiteluokkien käyttöoikeuksia muiden kuin laitteiden järjestelmänvalvojien osalta:

HUOMAUTUS: Jotta käyttäjä tai ryhmä pystyy käyttämään tätä näkymää laitteiden käyttöoikeustietojen lukemiseen, sille on myönnettävä lukuoikeudet **User Access Settings** (Käyttäjien käyttöoikeusasetukset) -näkymässä. Jotta käyttäjä tai ryhmä pystyy käyttämään tätä näkymää laitteiden käyttöoikeustietojen muuttamiseen, sille on myönnettävä muutosoikeudet **User Access Settings** (Käyttäjien käyttöoikeusasetukset) -näkymässä.

- kaikki siirrettävät tietovälineet (esimerkiksi levykkeet ja muistitikut)
- kaikki DVD/CD-asemat
- kaikki sarja- ja rinnakkaisportit
- kaikki Bluetooth®-laitteet
- kaikki infrapunalaitteet
- kaikki modeemilaitteet
- kaikki PCMCIA-laitteet
- kaikki 1394-laitteet.

Jos haluat sallia tai estää muita kuin laitteiden järjestelmänvalvojia käyttämästä tietyn luokan laitteita, toimi seuraavasti:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **Simple Configuration** (Yksinkertaiset määritykset).
2. Valitse oikeasta ruudusta sen laiteluokan tai laitteen valintaruutu, jonka käytön haluat estää. Poista valintaruudun valinta, jos haluat sallia laiteluokan tai tietyn laitteen käytön.

   Jos valintaruutu on harmaa, käyttöoikeuksia koskevia arvoja on muutettu Device Class Configuration (Laiteluokkien määritykset) -näkymässä. Jos haluat palauttaa arvot tavallisiksi asetuksiksi, tyhjennä tai valitse valintaruutu napsauttamalla sitä ja vahvista valintasi valitsemalla **Yes** (Kyllä).
3. Napsauta **Save** (Tallenna) -kuvaketta.

   HUOMAUTUS: Jos taustapalvelu ei ole käynnissä, näyttöön tulee valintaikkuna, jossa kysytään, että haluatko käynnistää sen. Valitse **Yes** (Kyllä).
4. Valitse **OK**.

Taustapalvelun käynnistäminen

Ennen kuin laiteprofiileja voidaan käyttää, HP ProtectTools Security Manager avaa valintaikkunan, jossa kysytään, että haluatko käynnistää HP ProtectTools Device Locking/Auditing -taustapalvelun. Valitse **Yes** (Kyllä). Taustapalvelu käynnistetään ja se käynnistyy tämän jälkeen aina järjestelmän käynnistyessä.

HUOMAUTUS: Laiteprofiili on määritettävä, ennen kuin taustapalvelun kehote tulee näyttöön.

Järjestelmänvalvojat voivat myös käynnistää tai pysäyttää tämän palvelun:

1. Valitse **Käynnistä** ja sitten **Ohjauspaneeli**.
2. Valitse **Valvontatyökalut** ja sitten **Palvelut**.
3. Etsi **HP ProtectTools Device Locking/Auditing** -palvelu.

Device Locking/Auditing -palvelun pysäyttäminen ei pysäytä laitteen lukitusta. Laitteen lukituksesta vastaa kaksi komponenttia:

- Device Locking/Auditing -palvelu
- DAMDrv.sys-ohjain

Palvelun käynnistäminen käynnistää laiteohjaimen, mutta palvelun pysäyttäminen ei pysäytä ohjainta.

Jos haluat määrittää, onko taustapalvelu käynnissä, avaa komentokehoteikkuna ja kirjoita sc query flcdlock.

Jos haluat määrittää, onko laiteohjain käynnissä, avaa komentokehoteikkuna ja kirjoita sc query damdrv.

Laiteluokkien määritykset

Järjestelmänvalvojat ja valtuutetut käyttäjät voivat tarkastella ja muokata luetteloita käyttäjistä ja ryhmistä, joilla on oikeus tai joilla ei ole oikeutta laiteluokkien tai tiettyjen laitteiden käyttöön.

HUOMAUTUS: Jotta käyttäjä tai ryhmä pystyy käyttämään tätä näkymää laitteiden käyttöoikeustietojen lukemiseen, sille on myönnettävä lukuoikeudet **User Access Settings** (Käyttäjien käyttöoikeusasetukset) -näkymässä. Jotta käyttäjä tai ryhmä pystyy käyttämään tätä näkymää laitteiden käyttöoikeustietojen muuttamiseen, sille on myönnettävä muutosoikeudet **User Access Settings** (Käyttäjien käyttöoikeusasetukset) -näkymässä.

Device Class Configuration (Laiteluokkien määritykset) -näkymä muodostuu seuraavista osista:

- **Device List** (Laiteluettelo) – Näyttää kaikki laiteluokat ja laitteet, jotka on asennettu järjestelmään tai jotka on mahdollisesti asennettu järjestelmään aikaisemmin.
  - Suojaus koskee tavallisesti laiteluokkaa. Valittu käyttäjä tai ryhmä voi käyttää mitä tahansa laiteluokkaan kuuluvaa laitetta.
  - Suojaus voi koskea myös tiettyjä laitteita.
- **User List** (Käyttäjäluettelo) – Näyttää kaikki käyttäjät ja ryhmät, joilla on oikeus tai joilla ei ole oikeutta tietyn laiteluokan tai laitteen käyttöön.
  - Käyttäjäluettelomerkintä voi koskea tiettyä käyttäjää tai ryhmää, johon käyttäjä kuuluu.
  - Jos käyttäjäluetteloon ei voi tehdä käyttäjä- tai ryhmämerkintää, asetus on peritty laiteluettelossa tai luokkakansiossa olevalta laiteluokalta.
  - Joidenkin laiteluokkien, kuten DVD- ja CD-asemien, osalta luku- ja kirjoitustoiminnot voidaan sallia tai estää erikseen.

    Muiden laitteiden ja luokkien tapauksessa luku- ja kirjoitusoikeudet voidaan periä. Esimerkiksi lukuoikeus voidaan periä ylemmältä luokalta, mutta kirjoitusoikeus voidaan estää tietyltä käyttäjältä tai ryhmältä.

    HUOMAUTUS: Jos Read (Luku) -valintaruutu on tyhjä, käyttöoikeuksien hallintaa koskevalla merkinnällä ei ole vaikutusta laitteen lukuoikeuksiin. Se ei evää tai myönnä laitteen lukuoikeuksia.

    Esimerkki 1 – Jos käyttäjältä tai ryhmältä evätään laitteen tai laiteluokan kirjoitusoikeudet:

    Samalle käyttäjälle, samalle ryhmälle tai saman ryhmän jäsenelle voidaan myöntää kirjoitusoikeudet tai luku- ja kirjoitusoikeudet vain laitehierarkiassa alemmalle laitteelle.

Esimerkki 2 – Jos käyttäjälle tai ryhmälle myönnetään laitteen tai laiteluokan kirjoitusoikeudet:

Samalta käyttäjältä, samalta ryhmältä tai saman ryhmän jäseneltä voidaan evätä kirjoitusoikeudet tai luku- ja kirjoitusoikeudet vain samalle laitteelle tai laitehierarkiassa alemmalle laitteelle.

Esimerkki 3 – Jos käyttäjälle tai ryhmälle myönnetään laitteen tai laiteluokan lukuoikeudet:

Samalta käyttäjältä, samalta ryhmältä tai saman ryhmän jäseneltä voidaan evätä lukuoikeudet tai luku- ja kirjoitusoikeudet vain samalle laitteelle tai laitehierarkiassa alemmalle laitteelle.

Esimerkki 4 – Jos käyttäjältä tai ryhmältä evätään laitteen tai laiteluokan lukuoikeudet:

Samalle käyttäjälle, samalle ryhmälle tai saman ryhmän jäsenelle voidaan myöntää lukuoikeudet tai luku- ja kirjoitusoikeudet vain laitehierarkiassa alemmalle laitteelle.

Esimerkki 5 – Jos käyttäjälle tai ryhmälle myönnetään laitteen tai laiteluokan luku- ja kirjoitusoikeudet:

Samalta käyttäjältä, samalta ryhmältä tai saman ryhmän jäseneltä voidaan evätä kirjoitusoikeudet tai luku- ja kirjoitusoikeudet vain samalle laitteelle tai laitehierarkiassa alemmalle laitteelle.

Esimerkki 6 – Jos käyttäjältä tai ryhmältä evätään laitteen tai laiteluokan luku- ja kirjoitusoikeudet:

Samalle käyttäjälle, samalle ryhmälle tai saman ryhmän jäsenelle voidaan myöntää lukuoikeudet tai luku- ja kirjoitusoikeudet vain laitehierarkiassa alemmalle laitteelle.

Käyttäjän tai ryhmän käytön estäminen

Toimi seuraavasti, jos haluat estää käyttäjää tai ryhmää käyttämästä laitetta tai laiteluokkaa:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **Device Class Configuration** (Laiteluokkien määritykset).
2. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää.
   - Device class (Laiteluokka)
   - All devices (Kaikki laitteet)
   - Individual device (Yksittäinen laite)
3. Valitse **User/Groups** (Käyttäjä/ryhmät) -kohdasta käyttäjä tai ryhmä, jonka käyttöoikeudet haluat kieltää.
4. Valitse käyttäjän tai ryhmän vierestä **Deny** (Estä).
5. Napsauta **Save** (Tallenna) -kuvaketta.

HUOMAUTUS: Kun käyttäjälle määritetään saman laitetason esto- ja sallimisasetukset, käyttöoikeuksien esto ohittaa käyttöoikeuksien sallimisen.

Käyttäjän tai ryhmän käytön salliminen

Toimi seuraavasti, jos haluat myöntää käyttäjälle tai ryhmälle oikeudet laitteen tai laiteluokan käyttöön:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **Device Class Configuration** (Laiteluokkien määritykset).
2. Valitse laiteluettelosta jokin seuraavista:
   - Device class (Laiteluokka)
   - All devices (Kaikki laitteet)
   - Individual device (Yksittäinen laite)
3. Valitse **Add** (Lisää).

   Select Users or Groups (Valitse käyttäjät tai ryhmät) -valintaikkuna avautuu.
4. Valitse **Advanced** (Lisäasetukset) ja hae lisättäviä käyttäjiä tai ryhmiä valitsemalla **Find Now** (Hae nyt).
5. Napsauta käyttäjää tai ryhmää, jonka haluat lisätä käytettävissä olevien käyttäjien ja ryhmien luetteloon, ja valitse **OK**.
6. Valitse **OK** uudelleen.
7. Myönnä käyttäjälle tai ryhmälle käyttöoikeus valitsemalla **Allow** (Salli).
8. Napsauta **Save** (Tallenna) -kuvaketta.

Käyttäjän tai ryhmän käytön estäminen

Toimi seuraavasti, jos haluat poistaa käyttäjän tai ryhmän oikeudet laitteen tai laiteluokan käyttöön:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **Device Class Configuration** (Laiteluokkien määritykset).
2. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää.
   - Device class (Laiteluokka)
   - All devices (Kaikki laitteet)
   - Individual device (Yksittäinen laite)
3. Valitse **User/Groups** (Käyttäjä/ryhmät) -kohdasta käyttäjä tai ryhmä, jonka haluat poistaa, ja valitse **Remove** (Poista).
4. Napsauta **Save** (Tallenna) -kuvaketta.

Laiteluokan käyttöoikeuden myöntäminen yhdelle käyttäjälle tai ryhmälle

Toimi seuraavasti, jos haluat myöntää käyttäjälle laiteluokan käyttöoikeuden ja estää laiteluokan käytön kaikilta muilta saman käyttäjäryhmän jäseniltä:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **Device Class Configuration** (Laiteluokkien määritykset).
2. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää.
   - Device class (Laiteluokka)
   - All devices (Kaikki laitteet)
   - Individual device (Yksittäinen laite)
3. Valitse **User/Groups** (Käyttäjä/ryhmät) -kohdasta ryhmä, jonka käyttöoikeudet haluat kieltää, ja valitse **Deny** (Estä).
4. Siirry halutun luokan alla olevaan kansioon ja lisää yksittäinen käyttäjä kansioon.
5. Myönnä käyttäjälle käyttöoikeus valitsemalla **Allow** (Salli).
6. Napsauta **Save** (Tallenna) -kuvaketta.

Tietyn laitteen käyttöoikeuden myöntäminen yhdelle käyttäjälle tai ryhmälle

Järjestelmänvalvojat voivat myöntää yhdelle käyttäjälle tietyn laitteen käyttöoikeuden ja estää koko laiteluokan käytön kaikilta muilta saman käyttäjäryhmän jäseniltä:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **Device Class Configuration** (Laiteluokkien määritykset).
2. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää. Siirry sitten sen alla olevaan kansioon.
3. Valitse **Add** (Lisää). **Select Users or Groups** (Valitse käyttäjät tai ryhmät) -valintaikkuna avautuu.
4. Valitse **Advanced** (Lisäasetukset) ja sitten **Find Now** (Hae nyt), jos haluat hakea käyttäjäryhmän, jolta estetään kaikkien laiteluokkaan kuuluvien laitteiden käyttö.
5. Valitse ryhmä ja sitten **OK**.
6. Siirry laiteluokassa sen laitteen kohdalle, jonka käyttöoikeudet haluat myöntää käyttäjälle.
7. Valitse **Add** (Lisää). **Select Users or Groups** (Valitse käyttäjät tai ryhmät) -valintaikkuna avautuu.
8. Valitse **Advanced** (Lisäasetukset) ja hae lisättäviä käyttäjiä tai ryhmiä valitsemalla **Find Now** (Hae nyt).
9. Napsauta käyttäjää, jolle haluat myöntää laitteen käyttöoikeuden. Valitse sitten **OK**.
10. Myönnä käyttäjälle käyttöoikeus valitsemalla **Allow** (Salli).
11. Napsauta **Save** (Tallenna) -kuvaketta.

Määritysten palauttaminen

△ **VAROITUS:** Määritysten palauttaminen tarkoittaa sitä, että kaikki laitekokoonpanoon tehdyt muutokset hylätään ja tehdasasetukset palautetaan.

Voit palauttaa kokoonpanoasetusten alkuperäiset arvot seuraavasti:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **Device Class Configuration** (Laiteluokkien määritykset).
2. Napsauta **Reset** (Palauta) -painiketta.
3. Vahvista valinta valitsemalla **Yes** (Kyllä).
4. Napsauta **Save** (Tallenna) -kuvaketta.

Lisätoiminnot

Kokoonpanoasetusten käyttöoikeuksien hallinta

User Access Settings (Käyttäjien käyttöoikeusasetukset) -näkymässä järjestelmänvalvojat voivat määrittää ryhmät tai käyttäjät, jotka voivat käyttää Simple Configuration (Yksinkertaiset määritykset)- ja Device Class Configuration (Laiteluokkien määritykset) -sivuja.

HUOMAUTUS: Käyttäjällä tai ryhmällä on oltava Full User Administrator rights (Täydelliset järjestelmänvalvojan oikeudet) -tason oikeudet User Access Settings (Käyttäjien käyttöoikeusasetukset) -näkymän asetusten muuttamista varten.

- Käyttäjälle tai ryhmälle on myönnettävä View (Read-only) Configuration Settings (Näytä kokoonpanoasetukset (vain luku)) -oikeudet Simple Configuration (Yksinkertaiset määritykset)- ja Device Class Configuration (Laiteluokkien määritykset) -näkymän tietojen tarkastelemista varten.
- Käyttäjälle tai ryhmälle on myönnettävä Change Configuration Settings (Muuta kokoonpanoasetukset) -oikeudet Simple Configuration (Yksinkertaiset määritykset)- ja Device Class Configuration (Laiteluokkien määritykset) -näkymän tietojen tarkastelemista varten.

HUOMAUTUS: Jopa järjestelmänvalvojien ryhmälle on myönnettävä lukuoikeudet Simple Configuration (Yksinkertaiset määritykset)- ja Device Class Configuration (Laiteluokkien määritykset) -näkymän tietojen tarkastelemista varten ja myönnettävä muutosoikeudet Simple Configuration (Yksinkertaiset määritykset)- ja Device Class Configuration (Laiteluokkien määritykset) -näkymän tietojen muuttamista varten.

HUOMAUTUS: Jos käyttäjälle ei ole valittu tiettyä käyttöoikeustasoa varten asetukseksi Allow (Salli) tai Deny (Estä) kaikkien käyttäjien ja ryhmien käyttöoikeustasojen arvioinnin jälkeen, käyttäjältä estetään oikeudet kyseisen tason käyttöön.

Oikeuksien myöntäminen olemassa olevalle käyttäjälle tai ryhmälle

Toimi seuraavasti, jos haluat myöntää olemassa olevalle ryhmälle tai käyttäjälle oikeudet kokoonpanoasetusten tarkastelemiseen tai muuttamiseen:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **User Access Settings** (Käyttäjien käyttöoikeusasetukset).
2. Valitse ryhmä tai käyttäjä, jolle haluat myöntää oikeudet.
3. Valitse **Permissions** (Oikeudet) -kohdasta **Allow** (Salli) kaikkien oikeuksien kohdalla, jotka haluat myöntää valitulle ryhmälle tai käyttäjälle:

   HUOMAUTUS: Myönnetyt oikeudet ovat kumulatiivisia. Esimerkiksi käyttäjä, joka on saanut Change Configuration Settings (Muuta kokoonpanoasetukset) -oikeudet, saa automaattisesti View (Read-only) Configuration Settings (Näytä kokoonpanoasetukset (vain luku)) -oikeudet. Käyttäjä, joka on saanut Full User Administrator Rights (Täydelliset järjestelmänvalvojan oikeudet) -tason oikeudet, saa myös View (Read-only) Configuration Settings (Näytä kokoonpanoasetukset (vain luku)) -oikeudet.

   - Full User Administrator Rights (Täydelliset järjestelmänvalvojan oikeudet)
   - Change Configuration Settings (Muuta kokoonpanoasetukset)
   - View (Read-only) Configuration Settings (Näytä kokoonpanoasetukset (vain luku))
4. Napsauta **Save** (Tallenna) -kuvaketta.

Oikeuksien epääminen olemassa olevalta käyttäjältä tai ryhmältä

Toimi seuraavasti, jos haluat evätä olemassa olevan ryhmän tai käyttäjän oikeudet kokoonpanoasetusten tarkastelemiseen tai muuttamiseen:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **User Access Settings** (Käyttäjien käyttöoikeusasetukset).
2. Valitse ryhmä tai käyttäjä, jolta haluat evätä oikeudet.
3. Valitse **Permissions** (Oikeudet) -kohdasta **Deny** (Estä) kaikkien oikeuksien kohdalla, jotka haluat evätä valitulta ryhmältä tai käyttäjältä:
   - Full User Administrator Rights (Täydelliset järjestelmänvalvojan oikeudet)
   - Change Configuration Settings (Muuta kokoonpanoasetukset)
   - View (Read-only) Configuration Settings (Näytä kokoonpanoasetukset (vain luku))
4. Napsauta **Save** (Tallenna) -kuvaketta.

Uuden ryhmän tai käyttäjän lisääminen

Toimi seuraavasti, jos haluat myöntää uudelle ryhmälle tai käyttäjälle oikeudet kokoonpanoasetusten tarkastelemiseen tai muuttamiseen:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **User Access Settings** (Käyttäjien käyttöoikeusasetukset).
2. Valitse **Add** (Lisää). **Select Users or Groups** (Valitse käyttäjät tai ryhmät) -valintaikkuna avautuu.
3. Valitse **Advanced** (Lisäasetukset) ja hae lisättäviä käyttäjiä tai ryhmiä valitsemalla **Find Now** (Hae nyt).
4. Valitse ryhmä tai käyttäjä, **OK** ja sitten **OK** uudelleen.
5. Myönnä käyttäjälle käyttöoikeus valitsemalla **Allow** (Salli).
6. Napsauta **Save** (Tallenna) -kuvaketta.

Ryhmän tai käyttäjän oikeuksien poistaminen

Toimi seuraavasti, jos haluat poistaa ryhmän tai käyttäjän oikeudet kokoonpanoasetusten tarkastelemiseen tai muuttamiseen:

1. Valitse **HP ProtectTools Administrative Console** -valintaikkunan vasemmasta ruudusta **Device Access Manager** ja sitten **User Access Settings** (Käyttäjien käyttöoikeusasetukset).
2. Valitse ryhmä tai käyttäjä ja sitten **Remove** (Poista).
3. Napsauta **Save** (Tallenna) -kuvaketta.

Aiheeseen liittyvät aineistot

Device Access Manager for HP ProtectTools on yhteensopiva HP ProtectTools Enterprise Device Access Manager -yritystuotteen kanssa. Kun käytät yritystuotetta, Device Access Manager for HP ProtectTools myöntää omiin toimintoihinsa vain lukuoikeudet.

Lisätietoja Device Access Manager for HP ProtectToolsista on Internetissä osoitteessa http://www.hp.com/hps/security/products.

12 LoJack Pro for HP ProtectTools

Absolute Softwaren Computrace-tuotteiden avulla käyttäjät voivat jäljittää HP-tietokoneensa ja parantaa tietojen suojausta. Computrace LoJack -tuotteet vähentävät myös laitteiden katoamista ja helpottavat varastettujen laitteiden palauttamista.

Voit ottaa Computrace-tuotteen käyttöön toimimalla seuraavien ohjeiden mukaan:

1. Valitse **Käynnistä**, **Kaikki ohjelmat** ja sitten **HP ProtectTools Security Manager**.
2. Valitse **Theft Recovery** (Varkauden selvittäminen) ja sitten **Activate Now** (Ota käyttöön nyt).

   Oletusverkkoselaimesi avaa tilaussivuston, jossa voit valita ja ostaa yhden kolmesta HP ProtectToolsiin saatavasta Computrace-tuotteesta:

   - **Computrace Data Delete** – Sisältää tietojen etäpoistomahdollisuuden, laitteen käytön eston sekä perustason omaisuuden seuranta- ja raportointitoiminnot.
   - **Computrace LoJack Pro** – Sisältää tietojen etäpoistomahdollisuuden, laitteen käytön eston, perustason omaisuuden seuranta- ja raportointitoiminnot sekä hallitun varkauden selvittämisen.
   - **Computrace LoJack Pro Premium** – Sisältää tietojen etäpoistomahdollisuuden, laitteen käytön eston, edistyneet omaisuuden seuranta- ja raportointitoiminnot, maantieteellisen paikannuksen ja alueseurannan sekä hallitun varkauden selvittämisen.

Computrace-agentti on sulautettu HP:n kannettavien yritystietokoneiden BIOSiin, vaikka agentti on tietokoneen toimitushetkellä poistettu käytöstä. Voit aktivoida agentin tilauksen hankinnan jälkeen. Sulautettu agentti pystyy asentamaan käyttöjärjestelmän ja alustamaan kiintolevyt uudelleen.

HUOMAUTUS: Saatavilla on 1–5 vuoden tilausjaksoja. Lisätietoja on Absolute Softwaren tilaussopimuksessa. Palautustoiminnon käytettävyys vaihtelee maantieteellisen sijainnin mukaan. GPS-seurantaa tuetaan joissakin WWAN-toiminnolla varustetuissa malleissa.

13 Vianmääritys

HP ProtectTools Security Manager

Lyhyt kuvaus	Tiedot	Ratkaisu
Älykortit ja USB-poletit eivät ole käytettävissä Security Managerissa, jos ne on asennettu Security Managerin asennuksen jälkeen.	Jos haluat käyttää älykortteja tai USB-poletteja Security Managerissa, niitä tukeva ohjelmistot (esimerkiksi ohjaimet ja PKCS#11-sovellukset) on asennettava ennen Security Managerin asennusta. Jos Security Manager on jo asennettu, toimi seuraavasti älykorttia tai polettia tukevan ohjelmiston asennuksen jälkeen:	Kirjaudu Security Manageriin. Valitse HP ProtectTools Security Managerista **Password Manager**, **Credentials** (Valtuustiedot) ja sitten **Smart Card** (Älykortti). Käynnistä tietokone pyydettäessä uudelleen.
Jotkin Web-sovellussivut luovat virheitä, jotka estävät käyttäjää suorittamasta tai viimeistelemästä tehtäviä.	Jotkin Web-pohjaiset sovellukset lakkaavat toimimasta ja raportoivat virheistä kertakirjaustoiminnon käytöstä poistamiseen liittyvien toimintojen vuoksi. Esimerkiksi Internet Explorer -selaimeen voi ilmestyä keltaisen kolmion sisällä oleva huutomerkki **!**, joka ilmaisee virhettä.	Security Managerin kertakirjaustoiminto ei tue kaikkien verkkopohjaisten käyttöliittymien käyttöä. Voit poistaa yksittäisten sivustojen kertakirjaustoiminnon käytöstä poistamalla kertakirjauksen tuen käytöstä. Lisätietoja on Security Manager -ohjelman ohjeessa olevassa kertakirjaustoiminnon täydellisessä ohjeessa. Jos jotakin tiettyä kertakirjaustoimintoa ei voi poistaa käytöstä tietyssä sovelluksessa, ota yhteys HP:n tekniseen tukeen ja pyydä kolmannen tason tukea HP-yhteyshenkilöltä.
Vaihtoehto **Browse for Virtual Token** (Etsi virtuaalinen poletti selaamalla) ei näy kirjautumisen aikana.	Käyttäjä ei voi vaihtaa rekisteröidyn virtuaalisen poletin sijaintia Password Managerissa, sillä selaustoiminto on poistettu tietoturvariskien vähentämiseksi.	Selaamisvaihtoehto on poistettu, koska sen avulla muut kuin varsinaiset käyttäjät pystyivät poistamaan tiedostoja ja nimeämään niitä uudelleen ja ottamaan Windowsin hallintaansa.
Toimialueen järjestelmänvalvojat eivät voi muuttaa Windows-salasanaa, vaikka heillä olisi valtuudet siihen.	Näin käy, kun toimialueen järjestelmänvalvoja kirjautuu toimialueeseen ja rekisteröi toimialueen tiedot Password Manageriin järjestelmänvalvojan oikeuksilla toimialueeseen ja paikalliseen tietokoneeseen. Kun toimialueen järjestelmänvalvoja yrittää vaihtaa Windowsin salasanaa Password Managerissa, hän saa ilmoituksen kirjautumisessa tapahtuneesta virheestä: **User account restriction** (Käyttäjätilin rajoitus).	Password Manager ei pysty muuttamaan toimialueen käyttäjän tilin salasanaa **Change Windows password** (Vaihda Windowsin salasana) -toiminnolla. Security Manager pystyy muuttamaan vain paikallisessa tietokoneessa olevien tilien salasanoja. Toimialueen käyttäjä voi muuttaa omaa salasanaansa **Windows security** (Windowsin suojaus) -toiminnon **Change password** (Vaihda salasana) -asetuksen avulla, mutta koska toimialueen käyttäjällä ei ole fyysistä tiliä paikallisessa tietokoneessa, Password Manager pystyy vaihtamaan vain kirjautumiseen käytetyn salasanan.
Password Managerissa on yhteensopivuusongelmia	Jos käyttäjä kirjautuu Password Manageriin, luo asiakirjan WordPerfectissä ja tallentaa sen	HP pyrkii ratkaisemaan ongelman tulevien tuoteparannusten myötä.

Lyhyt kuvaus	Tiedot	Ratkaisu
Corel WordPerfect 12:n salasanan GINA kanssa.	salasanasuojauksella, Password Manager ei manuaalisesti tai automaattisesti tunnista salasanaa GINA.	
Password Manager ei tunnista näytössä olevaa **Connect** (Yhdistä) -painiketta.	Jos RDP (Remote Desktop Connection) -kertakirjaustavaksi on määritetty **Yhdistä**, kertakirjaustoiminto siirtyy aina uudelleenkäynnistyksen yhteydessä **Save As** (Tallenna nimellä) -tilaan **Yhdistä**-tilan sijasta.	HP pyrkii ratkaisemaan ongelman tulevien tuoteparannusten myötä.
Käyttäjä ei pysty kirjautumaan Password Manageriin siirryttyään valmiustilasta lepotilaan (vain Windows XP Service Pack 1).	Järjestelmän siirryttyä horros- ja lepotilaan järjestelmänvalvoja tai käyttäjä ei pysty kirjautumaan Password Manageriin ja Windowsin kirjautumisnäyttö jää näyttöön siihen katsomatta, mitkä kirjautumisvaltuudet on valittu (salasana, sormenjälki tai Java-kortti).	Asenna Windowsiin Service Pack 2 -päivitys Windows Update -toiminnon avulla. Lisätietoja ongelman syistä on Microsoftin Knowledge Base -artikkelissa 813301 osoitteessa http://www.microsoft.com. Käyttäjän on kirjautumista varten valittava Password Manager ja kirjauduttava sisään. Password Manageriin kirjautumisen jälkeen käyttäjää kehotetaan kirjautumaan Windowsiin (käyttäjän on mahdollisesti valittava Windowsin kirjautumistoiminto) ja suorittamaan kirjautumisprosessi loppuun. Jos käyttäjä kirjautuu ensin Windowsiin, hänen on sen jälkeen kirjauduttava manuaalisesti Password Manageriin.
Virtuaalisen poletin liitos häviää käytettäessä suojauksen **Restore Identity** (Palauta omat tiedot) -toimintoa.	Kun käyttäjä palauttaa henkilötiedot, Password Manager voi menettää liitoksen kirjautumisnäytössä olevan virtuaalisen poletin sijaintiin. Vaikka virtuaalinen poletti on rekisteröity Password Managerissa, käyttäjän on rekisteröitävä poletti uudelleen liitoksen palauttamista varten.	Tämä on tarkoituksellista nykyisessä versiossa. Kun Security Managerin asennus poistetaan henkilötietoja tallentamatta, poletin järjestelmän (palvelimen) puolella oleva osa tuhotaan. Polettia ei tämän jälkeen voi käyttää kirjautumiseen, vaikka poletin asiakkaan puoleinen osa palautetaan henkilötietojen palautustoiminnon avulla. HP tutkii tulevia vaihtoehtoja tämän ratkaisemiseksi.

Device Access Manager for HP ProtectTools

Käyttäjiltä on evätty laitteiden käyttöoikeudet Device Access Managerin kautta, mutta laitteet ovat edelleen käytettävissä.

- **Selitys** – Laitteiden käyttöoikeus Device Access Managerin kautta on evätty Simple Configuration (Yksinkertaiset määritykset)- tai Device Class Configuration (Laiteluokkien määritykset) -näkymässä. Vaikka käyttöoikeudet on evätty, käyttäjät voivat edelleen käyttää laitteita.
- **Ratkaisu:**
  - Varmista, että HP ProtectTools Device Locking -palvelu on käynnissä.
  - Valitse järjestelmänvalvojatason käyttäjänä **Ohjauspaneeli** ja sitten **Järjestelmä ja ylläpito**. Valitse Valvontatyökalut-ikkunasta **Palvelut** ja etsi **HP ProtectTools Device Locking/Auditing** -palvelu. Varmista, että palvelu on käynnissä ja että sen asetuksena on **Automaattinen**.

Käyttäjälle on yllättäen myönnetty oikeudet laitteen käyttöön tai evätty ne.

- **Selitys** – Device Access Managerin avulla on evätty käyttöoikeus joihinkin laitteisiin ja myönnetty käyttöoikeus toisiin laitteisiin. Kun käyttäjät käyttävät järjestelmää, he voivat käyttää laitteita, joiden käyttöoikeudet he uskovat Device Access Managerin evänneen, ja he eivät pysty käyttämään laitteita, jotka Device Access Managerin pitäisi heidän mielestään sallia.
- **Ratkaisu:**
  - Tutki laitteen asetukset Device Access Managerin Device Class Configuration (Laiteluokkien määritykset) -toiminnon avulla.
  - Valitse **Security Manager**, **Device Access Manager** ja **Device Class Configuration** (Laiteluokkien määritykset). Laajenna Device Class (Laiteluokka) -puun tasot ja tarkista käyttäjää koskevat asetukset. Tarkista, että käyttäjään tai niihin Windowsin ryhmiin, joihin käyttäjä voi kuulua (esimerkiksi käyttäjät tai järjestelmänvalvojat), ei liity käyttöoikeuksien rajoituksia.

Salli tai estä – kumpi on etusijalla?

- **Selitys** – Device Class Configuration (Laiteluokkien määritykset) -näkymässä on määritetty seuraava kokoonpano:
  - Salli-lupa on myönnetty Windows-ryhmälle (esim. BUILTIN\Järjestelmänvalvojat) ja Estä-lupa taas laitehierarkiassa (esim. DVD- ja CD-asemat) samalla tasolla olevalle toiselle Windows-ryhmälle (esim. BUILTIN\Käyttäjät).
  - Jos käyttäjä on molempien ryhmien jäsen (esimerkiksi järjestelmänvalvoja), kumpi on etusijalla?
- **Ratkaisu:**
  - Käyttäjältä estetään laitteen käyttö. Estä-komento on etusijalla Salli-komentoon nähden.
  - Käytön estäminen johtuu Windowsin tavasta ratkaista lupa laitteen käyttöön. Yksi ryhmä estetään, toinen ryhmä sallitaan, mutta käyttäjä on molempien ryhmien jäsen. Käyttäjältä evätään oikeudet, sillä oikeuksien epääminen on etusijalla oikeuksien myöntämiseen nähden.

- Yksi tapa kiertää ongelma on evätä oikeudet käyttäjien ryhmältä DVD- ja CD-asemien tasolla ja myöntää oikeudet järjestelmänvalvojien ryhmälle DVD- ja CD-asemia alemmille tasoille.
- Toinen tapa kiertää ongelma on luoda erityisiä Windows-ryhmiä, joista yksi sallii DVD- ja CD-asemien käytön, kun taas toinen estää sen. Käyttäjät voidaan sitten lisätä asianomaisiin ryhmiin.

Laitteiden käytön hallintakäytäntö on määritetty Simple Configuration (Yksinkertaiset määritykset) -näkymässä, mutta järjestelmänvalvojatason käyttäjät eivät pysty käyttämään laitteita.

- **Selitys** – Simple Configuration (Yksinkertaiset määritykset) -toiminto estää käytön käyttäjiltä ja vierailta, mutta sallii sen laitteiden järjestelmänvalvojille.
- **Ratkaisu:** Lisää järjestelmänvalvojatason käyttäjä Device Administrators (Laitteiden järjestelmänvalvojat) -ryhmään.

Muut

Ohjelmisto, johon ongelma vaikuttaa – Lyhyt kuvaus	Tiedot	Ratkaisu
Security Manager – Varoitus: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (Tietoturvasovellusta ei voi asentaa, ennen kuin HP Protect Tools Security Manager on asennettu).	Kaikki tietoturvasovellukset, kuten Java Card Security ja biometriikka, ovat Security Manager -liittymän laajennettavia laajennuksia. Security Manager on asennettava ennen HP:n hyväksymän tietoturvalaajennuksen lataamista.	Security Manager -ohjelmisto on asennettava, ennen kuin mitään tietoturvalaajennusosaa voi ladata.
HP ProtectTools Security Manager – Security Manager -liittymän sulkemisen yhteydessä palautetaan ajoittain virhe.	Virhe ilmenee ajoittain (noin joka 12. kerta), kun Security Manager suljetaan näytön oikeassa yläkulmassa olevalla sulkemispainikkeella, ennen kuin kaikki laajennussovellukset on ladattu kokonaan.	Tämä liittyy laajennuspalvelujen latausaikojen ajoitusriippuvuuteen Security Managerin sulkemisen ja uudelleenkäynnistyksen yhteydessä. Koska PTHOST.exe on muita sovelluksia (laajennuksia) isännöivä komentoliittymä, se on riippuvainen laajennuksen latauksen loppuun saattamisesta (palvelut). Ongelma johtuu pääosin siitä, että komentoliittymä suljetaan, ennen kuin laajennusosaa on ehditty ladata. Salli Security Managerin viimeistellä palvelujen lataussanoma (näkyvissä Security Manager -ikkunan yläosassa) ja kaikki vasemmassa sarakkeessa olevat laajennusosat. Virheen välttämiseksi näille laajennusosille pitää varata riittävästi latautumisaikaa.
HP ProtectTools – Rajoittamaton käyttö tai hallitsemattomat järjestelmänvalvojan oikeudet ovat tietoturvariski.	Asiakastietokoneen rajoittamattomassa käytössä piilee useita riskejä. Näitä ovat muun muassa seuraavat: • PSD:n poistaminen • Käyttäjäasetusten haitallinen muokkaaminen • Tietoturvakäytäntöjen ja -toimintojen käytöstä poistaminen	Järjestelmänvalvojia kehotetaan noudattamaan ”parhaita käytäntöjä” heidän rajoittaessaan loppukäyttäjien oikeuksia ja tietojen käyttömahdollisuuksia. Luvattomille käyttäjille ei pidä myöntää järjestelmänvalvojan oikeuksia.

Sanasto

aktivointi Tehtävä on suoritettava loppuun, ennen kuin Drive Encryption -toiminnot ovat käytettävissä. Drive Encryption otetaan käyttöön HP ProtectToolsin ohjatun asennustoiminnon avulla. Drive Encryptionin voi ottaa käyttöön vain järjestelmänvalvoja. Aktivointi muodostuu ohjelmiston ottamisesta käyttöön, kiintolevyn salaamisesta, käyttäjätilin luomisesta ja ensimmäisen varmuuskopion salausavaimen luomisesta siirrettävään tallennuslaitteeseen.

allekirjoitusrivi Digitaalisen allekirjoituksen visuaalista näyttämistä varten varattu paikkamerkki. Kun asiakirja allekirjoitetaan, siinä näkyvät allekirjoittajan nimi ja todennustapa. Asiakirjaan voidaan lisätä myös allekirjoituspäivä ja allekirjoittajan työtehtävä.

ATM Automatic Technology Manager, joka antaa verkonvalvojille mahdollisuuden järjestelmien BIOS-tason etähallintaan.

automaattinen hävitys Ajoitettu hävitys, jonka käyttäjä ottaa käyttöön File Sanitizer -toiminnon avulla.

biometriikka Käyttöoikeuden tarkistustapa, joka tunnistaa käyttäjän fyysisen ominaisuuden, kuten sormenjäljen, perusteella.

digitaalinen allekirjoitus Tiedoston kanssa lähetettävät tiedot, jotka vahvistavat aineiston lähettäjän henkilöllisyyden ja sen, että tiedostoa ei ole muutettu allekirjoittamisen jälkeen.

digitaalinen varmenne Sähköiset tunnistetiedot, jotka vahvistavat henkilön tai yrityksen henkilöllisyyden yhdistämällä digitaalisen varmenteen omistajan henkilöllisyyden digitaalisten tietojen allekirjoittamiseen käytettävään sähköiseen avainpariin.

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

Drive Encryption -kirjautumisnäyttö Kirjautumisnäyttö, joka avautuu ennen Windowsin käynnistymistä. Käyttäjien on annettava Windowsin käyttäjätunnus ja salasana tai Java-kortin PIN-koodi. Useimmissa tapauksissa Windowsia voi käyttää suoraan, eikä Windowsin kirjautumisnäytössä tarvitse kirjautua sisään uudelleen, jos Drive Encryption -kirjautumisnäytössä annetaan salasana oikein.

DriveLock Suojausominaisuus, joka yhdistää kiintolevyn käyttäjään. DriveLock-salasana on annettava oikein, ennen kuin tietokone käynnistyy.

ehdotettu allekirjoittaja Käyttäjä, jonka Microsoft Word- tai Microsoft Excel -asiakirjan tekijä on määrittänyt lisäämään asiakirjaan allekirjoitusrivin.

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

henkilökortti Windowsin sivupalkin pienoisohjelma, jota käytetään tietokoneen tunnistamiseen käyttäjänimen ja valitun kuvan perusteella. Avaa HP ProtectToolsin hallintakonsoli napsauttamalla henkilökorttia.

HP SpareKey Kiintolevyn salausavaimen varmuuskopio.

hätäpalautusarkisto Suojattu tallennusalue, jonka avulla peruskäyttäjän avaimia voidaan salata uudelleen käyttöympäristön omistajan avainten välillä.

hävitys Omaisuuden sisältämät tiedot sekoittavan algoritmin suorittaminen.

hävitysjakso Ilmaisee, kuinka monta kertaa hävitysalgoritmi suoritetaan omaisuudelle. Hävitysjaksojen määrää lisäämällä voit parantaa tietokoneen turvallisuutta.

hävitysprofiili Määritetty poistotapa ja omaisuusluettelo.

Java-kortti Siirrettävä kortti, joka asetetaan tietokoneeseen. Sisältää kirjautumiseen tarvittavia tunnistetietoja. Jos Drive Encryption -kirjautumisnäytössä kirjaudutaan Java-kortilla, käyttäjän on asetettava Java-kortti laitteeseen ja annettava käyttäjätunnus sekä Java-kortin PIN-koodi.

järjestelmänvalvoja *Katso* Windows-järjestelmänvalvoja.

kertakirjaustoiminto Todennustiedot tallentava toiminto, joka mahdollistaa Internetin ja salasanatodennusta vaativien Windows-sovellusten käytön Security Managerilla.

keskusteluhistoriaistunto Salattu tiedosto, joka sisältää tallenteen keskusteluistunnon molempien osapuolten keskustelusta.

kirjautumistavat Tapa, jolla käyttäjän käyttöoikeus todistetaan eli todennetaan jotakin tiettyä tehtävää varten.

kirjautumistunnus Security Managerin objekti, joka muodostuu käyttäjänimestä ja salasanasta (ja mahdollisesti muista valituista tiedoista). Kirjautumistunnusta käytetään sivustoihin ja muihin ohjelmiin kirjautumiseen.

kohde Rekisteröidyn käyttäjän valokuva, jota käytetään henkilöllisyyden todentamiseen.

kojelauta Keskitetty sijainti, jonka kautta voit käyttää ja hallita HP ProtectTools Security Managerin toimintoja ja asetuksia.

konsoli Keskitetty sijainti, jonka kautta voit käyttää ja hallita HP ProtectToolsin hallintakonsolin toimintoja ja asetuksia.

kryptografia Tietojen salaamisen ja salauksen purkamisen tapa, joka varmistaa, että vain tietyt käyttäjät saavat tiedot käyttöönsä.

kryptografinen palveluntarjoaja (CSP) Salausalgoritmien tarjoaja tai kirjasto. Algoritmeja voidaan käyttää tarkkaan määritetyn liittymän avulla tiettyjen salaustoimintojen suorittamiseen.

käynnistystodennus Suojaustoiminto. Kun tämä toiminto on käytössä, käyttäjän on todistettava käyttöoikeutensa esimerkiksi Java-kortilla, suojaussirulla tai salasanalla, 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 tietyntyyppiset laitteet, esimerkiksi asemat.

laitteiden käytön hallintakäytäntö Luettelo laitteista, joita käyttäjällä on oikeus käyttää.

Live Messenger History Viewer Privacy Manager Chat -komponentti, jonka avulla voit hakea ja tarkastella salattuja keskusteluhistoriaistuntoja.

luotettuihin yhteyshenkilöihin kuuluva vastaanottaja Henkilö, joka on saanut luotetun yhteyshenkilön kutsun.

luotettujen yhteyshenkilöiden luettelo Luettelo luotetuista yhteyshenkilöistä.

luotettujen yhteyshenkilöiden sinetti Tehtävä, joka lisää digitaalisen allekirjoituksen, salaa sähköpostiviestin ja lähettää sen, kun olet todentanut sen valitsemaasi suojattua kirjautumistapaa käyttäen.

luotettu lähettäjä Luotettu yhteyshenkilö, joka lähettää allekirjoitettuja ja/tai salattuja sähköpostiviestejä ja Microsoft Office -asiakirjoja.

luotettu pikaviestiviestintä Viestintäistunto, jonka aikana vaihdetaan luotettuja viestejä luotetun lähettäjän ja luotetun yhteyshenkilön välillä.

luotettu viesti Viestintäistunto, jonka aikana vaihdetaan luotettuja viestejä luotetun lähettäjän ja luotetun yhteyshenkilön välillä.

luotettu yhteyshenkilö Henkilö, joka on hyväksynyt luotetun yhteyshenkilön kutsun.

luotetun yhteyshenkilön kutsu Sähköpostiviesti, jossa vastaanottajaa pyydetään hyväksymään, että hänet lisätään luotetuksi yhteyshenkilöksi.

manuaalinen hävitys Valitun omaisuuden tai valittujen omaisuuksien välitön hävitys, joka ohittaa automaattisen hävitysaikataulun.

näppäinyhdistelmä Tiettyjen näppäinten yhdistelmä, joka käynnistää automaattisen hävityksen (esimerkiksi ctrl+alt+s).

omaisuus Tietokomponentti, joka muodostuu kiintolevylle tallennetuista henkilökohtaisista tiedoista tai tiedostoista sekä historiallisesta ja Internetin käyttöön liittyvästä sisällöstä.

omat tiedot HP ProtectTools Security Managerissa käytettävä kirjautumistapojen ja käyttöoikeusasetusten joukko, joka vastaa tietyn käyttäjän käyttäjätiliä tai profiilia.

palautus Prosessi, jossa ohjelmatiedot kopioidaan aikaisemmin tallennetusta varmuuskopiotiedostosta tähän ohjelmaan.

paljastaminen Tehtävä, jonka avulla käyttäjä voi purkaa yhden tai useamman keskusteluhistoriaistunnon salauksen, näyttää yhteyshenkilön näyttönimen tavallisena tekstinä ja mahdollistaa istunnon tarkastelun.

peruutussalasana Salasana, joka luodaan käyttäjän pyytäessä digitaalista varmennetta. Salasanaa tarvitaan, kun käyttäjä haluaa peruuttaa digitaalisen varmenteensa. Tällä varmistetaan, että vain käyttäjä voi peruuttaa varmenteen.

PIN-koodi Personal Identification Number.

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

poletti Katso suojattu kirjautumistapa.

Privacy Manager -varmenne Digitaalinen varmenne, joka vaatii todennusta aina salaustoimintoja käytettäessä, esimerkiksi sähköpostiviestejä ja Microsoft Office -asiakirjoja allekirjoitettaessa ja salattaessa.

PSD Henkilökohtainen suojattu levyasema, arkaluontoisten tietojen suojattu tallennusalue.

ryhmä Ryhmä käyttäjiä, joilla on samanlaiset oikeudet laiteluokan tai tietyn laitteen käyttöön.

salaaminen Normaalin tekstin muuntaminen salatekstiksi esimerkiksi algoritmin avulla, jotta luvattomat vastaanottajat eivät voi lukea tietoja. Tietojen salaukseen on olemassa monia eri tapoja. Ne muodostavat tietoverkkojen tietoturvan perustan. Yleisiä salaustapoja ovat Data Encryption Standard sekä julkista avainta käyttävä salaus.

salauksen purkaminen Salattujen tietojen muuntaminen normaaliksi tekstiksi.

SATA-laitetila Tietokoneen ja massamuistilaitteiden, kuten kiintolevyjen ja optisten asemien, välinen tiedonsiirtotila.

Send Securely (Lähetä turvallisesti) -painike Ohjelmiston painike, joka näkyy Microsoft Outlook -sähköpostiviestien työkalurivillä. Painiketta napsauttamalla voit allekirjoittaa ja/tai salata Microsoft Outlook -sähköpostiviestin.

Sign and Encrypt (Allekirjoita ja salaa) -painike Ohjelmiston painike, joka näkyy Microsoft Office -sovellusten työkalurivillä. Painiketta napsauttamalla voit allekirjoittaa ja salata Microsoft Office -asiakirjan sekä purkaa sen salauksen.

siirto Privacy Manager -varmenteiden ja luotettujen yhteyshenkilöiden hallintaan, palauttamiseen ja siirtoon tarkoitettu tehtävä.

sormenjälki Digitaalinen vedos sormenjälkikuvasta. Security Manager ei koskaan tallenna todellista sormenjälkikuvaa.

suojattu kirjautumistapa Tietokoneeseen kirjautumiseen käytettävä menetelmä.

taustapalvelu HP ProtectTools Device Locking/Auditing -taustapalvelu, jonka on oltava käynnissä, jotta laitteiden käytön hallintakäytäntöjä voidaan käyttää. Sitä voidaan tarkastella Ohjauspaneelin Valvontatyökalut-toiminnon Palvelut-sovelluksen kautta. Jos taustapalvelu ei ole käynnissä, HP ProtectTools Security Manager yrittää käynnistää sen laitteiden käytön hallintakäytäntöjä sovellettaessa.

tavallinen poisto Omaisuuden Windows-viittauksen poistaminen. Omaisuuden sisältö jää kiintolevylle, kunnes tiedot sekoitetaan vapaan tilan tyhjennyksen avulla.

todentaminen Prosessi, jonka tarkoituksena on tarkistaa, että käyttäjällä on oikeudet tietyn tehtävän suorittamiseen, kuten tietokoneen käyttöön, tietyn ohjelman asetusten muokkaamiseen tai suojattujen tietojen tarkastelemiseen.

toimialue Samaan verkkoon kuuluvien ja yhteisen hakemistotietokannan jakavien tietokoneiden ryhmä. Toimialueilla on yksilölliset nimet sekä yhteiset säännöt ja menettelytavat.

TXT Trusted Execution Technology.

USB-poletti Suojauslaite, johon on tallennettu käyttäjään liittyviä tunnistetietoja. Sitä käytetään Java-kortin tai biometrisen lukulaitteen tapaan tietokoneen käyttöoikeuden todentamiseen.

uudelleenkäynnistys Tietokoneen käynnistäminen uudelleen.

valtuutettu käyttäjä Käyttäjä, jolle on annettu oikeudet User Access Settings (Käyttäjien käyttöoikeusasetukset) -näkymässä Simple Configuration (Yksinkertaiset määritykset)- tai Device Class Configuration (Laiteluokkien määritykset) -näkymän kokoonpanoasetusten tarkastelemiseen tai muuttamiseen.

vapaan tilan tyhjennys Sattumanvaraisten tietojen turvallinen kirjoittaminen poistetun omaisuuden päälle, minkä tarkoituksena on vääristää poistetun omaisuuden sisältö.

varmenteen myöntäjä Palvelu, joka myöntää sertifikaatteja julkista avainta käyttävän rakenteen ylläpitämistä varten.

varmuuskopiointi Varmuuskopiointitoiminnon käyttäminen, jonka tarkoituksena on tallentaa kopio tärkeistä ohjelmatiedoista ohjelman ulkopuolelle. Varmuuskopion avulla tiedot voidaan myöhemmin palauttaa samaan tai toiseen tietokoneeseen.

verkkokäyttäjätili Käyttäjän tai järjestelmänvalvojan Windows-käyttäjätili paikallisessa tietokoneessa, työryhmässä tai verkkotoimialueessa.

Windows-järjestelmänvalvoja Käyttäjä, jolla on kokonaisvaltaiset oikeudet muuttaa käyttöoikeuksia ja hallita muita käyttäjiä.

Windows-käyttäjätili Tietoverkon tai yksittäisen tietokoneen käyttäjän profiili.

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

virtuaalinen poletti Suojausominaisuus, joka toimii Java-kortin ja kortin lukulaitteen tapaan. Poletti tallennetaan tietokoneen kiintolevylle tai Windowsin rekisteriin. Kun kirjaudut sisään virtuaalisella poletilla, sinua kehotetaan antamaan käyttäjän PIN-koodi todennuksen suorittamista varten.

älykortti Luottokortin kokoinen kortti, johon tallennetaan kortin omistajan tunnistustiedot. Korttia käytetään tietokoneen käyttöoikeuden vahvistamiseen (todentamiseen).

Hakemisto