HP ProtectTools

Aloitusopas

Ensimmäinen painos: Tammikuu 2007

Oppaan osanumero: 419699-351

Sisällysluettelo

1 Johdanto

HP ProtectTools Security Manager -ohjelma sisältää suojaustoimintoja, joilla tietokone, tietoverkko ja tärkeät tiedot voidaan suojata luvattomalta käytöltä. Seuraavat ohjelmistomoduulit tarjoavat käyttäjälle tehokkaat suojausominaisuudet:

- Smart Card Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Credential Manager for HP ProtectTools
- Device Access Manager for HP ProtectTools.

Käytettävissä olevat ohjelmistomoduulit vaihtelevat tietokoneen mallin mukaan. Esimerkiksi Embedded Security for HP ProtectTools -ohjelmaa voi käyttää vain, jos tietokoneessa on TPM (Trusted Platform Module) Embedded Security -siru (käytettävissä vain tietyissä malleissa). Smart Card Security for HP ProtectTools -ohjelmaa varten käytettävissä on oltava sirukortti ja kortinlukija.

HP ProtectTools-ohjelmistomoduulit saattavat kuulua tietokoneen esiasennukseen, ne on ehkä ladattu valmiiksi tai niitä voidaan ladata HP:n Web-sivustosta. Lisätietoja on osoitteessa http://www.hp.com.

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

HP ProtectTools Security Manager -ohjelman avaaminen

HP ProtectTools Security Manager -ohjelman avaaminen Windows®-ohjauspaneelista

▲ Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.

Huomautus Kun olet määrittänyt Credential Manager -moduulin asetukset, voit avata HP ProtectTools -ohjelman myös kirjautumalla Credential Manager -ohjelmaan suoraan Windows-käyttöjärjestelmän kirjautumisnäytössä. Lisätietoja on luvun 6 Credential Manager for HP ProtectTools kohdassa Kirjautuminen Windowsiin Credential Manager -ohjelman avulla.

Tietosuojavastuut

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 sirukortit, biometriset tunnistimet tai USB-poletit.

Huomautus Tietosuojavastaava voi mukauttaa monia HP ProtectTools -ohjelmiston ominaisuuksia yhteistyössä HP:n kanssa. Lisätietoja on 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 sirukortit, järjestelmänvalvoja voi määrittää myös BIOS-järjestelmälle sirukorttisuojauksen.
- Käyttäjä: Käyttää suojaustoimintoja. Jos tietosuojavastaava ja järjestelmänvalvoja ovat ottaneet käyttöön esimerkiksi sirukortit, käyttäjä voi määrittää sirukortin PIN-koodin ja käyttää korttia käyttöoikeutensa todistamiseen.

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	HP ProtectTools -moduuli, jossa salasana määritetään	Käyttötarkoitus
Tietokoneen asetukset -ohjelman asetussalasana **Huomautus** Vaihtoehtoinen nimitys: BIOS-järjestelmänvalvojan, f10-asetusten tai suojausasetusten salasana.	BIOS Configuration, järjestelmänvalvoja	Estää Tietokoneen asetukset -ohjelman luvattoman käytön.
Käynnistyssalasana	BIOS Configuration	Estää tietokoneen sisällön käsittelemisen, kun tietokone käynnistetään (uudelleen) tai palautetaan lepotilasta.
Sirukortin järjestelmänvalvojan salasana **Huomautus** Vaihtoehtoinen nimitys: BIOS-järjestelmänvalvojan korttisalasana	Smart Card Security, järjestelmänvalvoja	Käytetään sirukorttitodennuksen yhteydessä tietokonetta (BIOS-järjestelmää) käynnistettäessä. Sallii Tietokoneen asetukset -ohjelman käyttämisen ja tietokoneen sisällön käsittelemisen, kun tietokone käynnistetään (uudelleen) tai palautetaan lepotilasta. Sallii myös palautustiedostojen luomisen käyttäjien tai järjestelmänvalvojien korttien tietojen palauttamista varten.
Sirukortin käyttäjän salasana **Huomautus** Vaihtoehtoinen nimitys: BIOS-käyttäjän korttisalasana	Smart Card Security	Käytetään sirukorttitodennuksen yhteydessä tietokonetta (BIOS-järjestelmää) käynnistettäessä. Sallii tietokoneen sisällön käsittelemisen, kun tietokone käynnistetään (uudelleen) tai palautetaan lepotilasta.
Sirukortin PIN-koodi	Smart Card Security	Suojaa sirukortin sisältöä ja vahvistaa sirukortin käyttäjän henkilöllisyyden. Kun sirukorttia käytetään käyttöoikeuden tarkistamiseen tietokonetta käynnistettäessä, PIN-koodi suojaa myös Tietokoneen asetukset -ohjelmaa ja tietokoneen sisältöä.
Sirukortin palautustiedoston salasana	Smart Card Security	Suojaa palautustiedostoa, joka sisältää BIOS-salasanat.
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

HP ProtectTools -salasana	HP ProtectTools -moduuli, jossa salasana määritetään	Käyttötarkoitus
		Tietokoneen asetukset -ohjelmaa ja tietokoneen sisältöä.
Peruskäyttäjän avaimen salasana **Huomautus** Vaihtoehtoinen nimitys: Embedded Security -salasana	Embedded Security	Sallii Embedded Security -toimintojen käytön. Tällaisia toimintoja ovat esimerkiksi suojattu sähköposti sekä tiedostojen ja kansioiden salaus. Kun tätä salasanaa käytetään käyttöoikeuden tarkistamiseen tietokoneen käynnistyksen tai lepotilasta palauttamisen yhteydessä, se suojaa myös tietokoneen sisältöä.
Tietojen palautuksen salasana **Huomautus** Vaihtoehtoinen nimitys: Tietojen palautuksen avainsalasana	Embedded Security, järjestelmänvalvoja	Suojaa tietojen palautustiedostoa (Emergency Recovery Token), joka on upotetun suojaussirun varmuuskopiotiedosto.
Pääkäyttäjän salasana	Embedded Security, järjestelmänvalvoja	Suojaa järjestelmää ja TPM-sirua Embedded Security -ohjelman pääkäyttäjän toimintojen luvattomalta käytöltä.
Credential Manager -ohjelman salasana	Credential Manager	Salasanalla on kaksi käyttötapaa: • Salasanan avulla voidaan kirjautua Credential Manager -ohjelmaan, kun käyttäjä on jo kirjautuneena Windows-järjestelmään. • Salasanaa voidaan käyttää Windows-järjestelmään kirjauduttaessa, jolloin käyttäjä kirjautuu samanaikaisesti sekä Credential Manager -ohjelmaan että Windows-järjestelmään.
Credential Manager -ohjelman palautustiedoston salasana	Credential Manager, järjestelmänvalvoja	Suojaa Credential Manager -ohjelman palautustiedostoa.
Windows-salasana	Windows-käyttöjärjestelmän Ohjauspaneeli	Salasanaa voidaan käyttää manuaaliseen kirjautumiseen tai se voidaan tallentaa sirukorttiin.

Turvallisen 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.

2 Smart Card Security for HP ProtectTools

Smart Card Security for HP ProtectTools ohjelmalla hallitaan sirukortin asetuksia ja kokoonpanoa tietokoneissa, joissa on valinnainen sirukortin lukija.

Kun käytettävissä on Smart Card Security -ohjelma, voit

- käsitellä sirukorttien suojausominaisuuksia.
- alustaa sirukortin, jotta sitä voidaan käyttää muiden HP ProtectTools -moduulien, kuten Credential Manager for HP ProtectTools -ohjelman kanssa.
- ottaa Tietokoneen asetukset -ohjelmassa käyttöön käyttöoikeuden tarkistuksen sirukortilla tietokonetta käynnistettäessä. Voit myös määrittää erilliset sirukortit järjestelmänvalvojille ja käyttäjille. Tämä toiminto edellyttää, että käyttäjä asettaa sirukortin kortinlukijaan tai kirjoittaa myös PIN-koodin ennen käyttöjärjestelmän lataamista.
- määrittää ja vaihtaa salasanan, jota käytetään sirukortin käyttäjien todentamisessa.
- varmuuskopioida ja palauttaa sirukorttiin tallennettuja sirukortin BIOS-salasanoja.

Sirukortin alustaminen

Sirukorttia voi käyttää vasta, kun se on alustettu.

Sirukortin alustaminen

1. Aseta sirukortti kortinlukijaan.
2. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
3. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **Smart Card** (Älykortti).
4. Valitse oikeassa ruudussa **Initialize** (Alusta).
5. Kirjoita nimesi **Initialize the smart card** (Alusta älykortti) -valintaikkunan ensimmäiseen ruutuun.
6. Määritä ja vahvista sirukortin PIN-koodi asianmukaisissa ruuduissa. PIN-koodissa on oltava 4–8 numeroa.

   VARO On tärkeää, että et unohda sirukortin PIN-koodia. Jos unohdat PIN-koodin, et ehkä enää voi käyttää tietokonetta. Sirukortti lukittuu eikä sitä voi enää käyttää, jos PIN-koodi annetaan väärin viisi kertaa peräkkäin. Kun PIN-koodi annetaan oikein, väärien yritysten laskuri nollautuu.

7. Suorita alustus loppuun valitsemalla **OK**.

BIOS-järjestelmän sirukorttisuojaus

Kun tämä toiminto on otettu käyttöön, tietokonetta käynnistettäessä on käytettävä sirukorttia.

BIOS-järjestelmän sirukorttisuojauksen käyttöönotto sisältää seuraavat vaiheet:

1. Ota sirukortilla suoritettava käynnistystodennus käyttöön BIOS Configuration -moduulissa. Lisätietoja on luvussa 5 BIOS Configuration for HP ProtectTools kohdassa Sirukortin ja Java-kortin käynnistystodennuksen tuen ottaminen käyttöön tai poistaminen käytöstä.

   Huomautus Kun tämä toiminto on otettu käyttöön, käynnistystodennuksessa voidaan käyttää sirukorttia. BIOS-järjestelmän sirukorttisuojauksen toiminnot ovat käytettävissä vasta, kun sirukortilla suoritettava käynnistystodistus on otettu käyttöön.

2. Ota BIOS-järjestelmän sirukorttisuojaus käyttöön Smart Card Security -ohjelmassa. Lisätietoja on jäljempänä tämän luvun kohdassa BIOS-järjestelmän sirukorttisuojauksen ottaminen käyttöön ja sirukortin järjestelmänvalvojan salasanan määrittäminen.

3. Määritä sirukortin järjestelmänvalvojan salasana.

   Huomautus Sirukortin järjestelmänvalvojan salasanan määritys on osa BIOS-järjestelmän sirukorttisuojauksen käyttöönottoa.

Sirukortin järjestelmänvalvojan salasana ei ole sama kuin Tietokoneen asetukset -ohjelman asetussalasana. Sirukortin järjestelmänvalvojan salasana mahdollistaa sirukortin käyttämisen tietokoneen käyttöoikeuksien tarkistamiseen. Sen avulla voit myös

- avata Tietokoneen asetukset -ohjelman sekä käyttää tietokoneeseen tallennettuja tietoja, kun tietokone on käynnistetty
- luoda uusia järjestelmänvalvojien ja käyttäjien sirukortteja
- luoda palautustiedoston käyttäjän tai järjestelmänvalvojan sirukortin tietojen palauttamista varten.

BIOS-järjestelmän sirukorttisuojauksen ottaminen käyttöön ja sirukortin järjestelmänvalvojan salasanan määrittäminen

BIOS-järjestelmän sirukorttisuojauksen ottaminen käyttöön ja sirukortin järjestelmänvalvojan salasanan määrittäminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **BIOS**.
3. Valitse oikean ruudun BIOS Security mode (BIOS-järjestelmän suojaus) -kohdassa **Ota käyttöön**.
4. Valitse **Seuraava**.

5. Kirjoita Tietokoneen asetukset -ohjelman asetussalasana, kun ohjelma pyytää sitä, ja valitse sitten **Seuraava**.

6. Aseta uusi järjestelmänvalvojan sirukortti kortinlukijaan ja noudata näyttöön tulevia ohjeita. Ohjeet vaihtelevat tilanteen mukaan ja saattavat sisältää seuraavia tehtäviä:

   - Sirukortin alustaminen. Lisätietoja on kohdassa Sirukortin alustaminen.
   - Sirukortin järjestelmänvalvojan salasanan määrittäminen. Lisätietoja on kohdassa Järjestelmänvalvojan tai käyttäjän salasanan tallentaminen korttiin.
   - Palautustiedoston luominen. Lisätietoja on kohdassa Palautustiedoston luominen.

BIOS-järjestelmän sirukorttisuojauksen poistaminen käytöstä

Kun BIOS-järjestelmän sirukorttisuojaus on poistettu käytöstä, sirukortin järjestelmänvalvojan ja käyttäjän salasanat eivät ole enää käytössä eikä sirukorttia enää tarvita tietokoneen käynnistämiseen.

Huomautus Jos BIOS-järjestelmän sirukorttisuojaus on aiemmin otettu käyttöön, Smart Card Security BIOS (BIOS-järjestelmän sirukorttisuojaus) -sivulla on Poista käytöstä -painike.

Sirukorttisuojauksen poistaminen käytöstä

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **BIOS**.
3. Valitse oikean ruudun **BIOS Security mode** (BIOS-järjestelmän suojaus) -kohdassa **Poista käytöstä**.
4. Aseta nykyistä sirukortin järjestelmänvalvojan salasanaa käyttävä kortti kortinlukijaan ja valitse sitten **Seuraava**.
5. Anna sirukortin PIN-koodi, kun järjestelmä kysyy sitä, ja valitse sitten **Valmis**.

Sirukortin järjestelmänvalvojan salasanan muuttaminen

Sirukortin järjestelmänvalvojan salasanan määritys on osa BIOS-järjestelmän sirukorttisuojauksen käyttöönottoa. Voit muuttaa sirukortin järjestelmänvalvojan salasanaa, kun se on ensin määritetty. Lisätietoja sirukortin järjestelmänvalvojan salasanasta on edellä tämän luvun kohdassa BIOS-järjestelmän sirukorttisuojaus.

Huomautus Näiden ohjeiden avulla voit muuttaa korttiin ja Tietokoneen asetukset -ohjelmaan tallennetun sirukortin järjestelmänvalvojan salasanan.

Järjestelmänvalvojan salasanan muuttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **BIOS**.
3. Napsauta oikean ruudun **BIOS Security Mode** (BIOS-järjestelmän suojaus) -kohdassa **BIOS administrator card** (BIOS-järjestelmänvalvojan kortti) -kohdan vieressä olevaa **Muuta**-painiketta.
4. Anna sirukortin PIN-koodi ja valitse sitten **Seuraava**.

5. Aseta uusi järjestelmänvalvojan kortti kortinlukijaan ja valitse sitten **Seuraava**.
6. Anna sirukortin PIN-koodi ja valitse sitten **Valmis**.

Sirukortin käyttäjän salasanan määrittäminen ja muuttaminen

Sirukortin käyttäjän salasanan määrittäminen ja muuttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **BIOS**.
3. Napsauta oikean ruudun **BIOS Security Mode** (BIOS-järjestelmän suojaus) -kohdassa **BIOS user card** (BIOS-käyttäjän kortti) -kohdan vieressä olevaa **Aseta**-painiketta.

   Huomautus Jos Tietokoneen asetukset -ohjelmassa on jo määritetty käyttäjän salasana, napsauta **Muuta**-painiketta.

4. Anna sirukortin PIN-koodi ja valitse sitten **Seuraava**.
5. Aseta uusi käyttäjän kortti kortinlukijaan ja valitse sitten **Seuraava**.
   - Jos kortille on jo määritetty käyttäjän salasana, näyttöön tulee **Valmis**-valintaikkuna. Jätä vaiheet 6 - 8 suorittamatta ja siirry suoraan vaiheeseen 9.
   - Jos kortille ei ole määritetty käyttäjän salasanaa, ohjattu BIOS-salasanojen määritystoiminto tulee näyttöön.
6. Ohjatussa BIOS-salasanojen määritystoiminnossa (BIOS Password Wizard) voit
   - määrittää salasanan manuaalisesti
   - luoda satunnaisen 32-tavuisen salasanan.

   Huomautus Jos käytät tunnettua salasanaa, voit luoda kortista kaksoiskappaleen ilman palautustiedostoa. Satunnaisesti luotu salasana lisää tietoturvaa. Tällöin kaksoiskappaleiden luomiseen tarvitaan kuitenkin palautustiedosto.

7. Valitse **Boot Requirements** (Käynnistysvaatimukset) -kohdassa valintaruutu, jos haluat määrittää sirukortin PIN-koodin pakolliseksi tietokonetta käynnistettäessä.

   Huomautus Jos et halua määrittää sirukortin PIN-koodia pakolliseksi tietokonetta käynnistettäessä, poista valinta valintaruudusta.

8. Anna sirukortin PIN-koodi ja valitse sitten **OK**. Järjestelmä kehottaa sinua luomaan palautustiedoston.

   Huomautus Palautustiedoston luominen on erittäin suositeltavaa. Lisätietoja on tämän luvun kohdassa Palautustiedoston luominen.

9. Anna sirukortin PIN-koodi **Valmis**-valintaikkunassa ja valitse sitten **Valmis**.

Järjestelmänvalvojan tai käyttäjän salasanan tallentaminen korttiin

Jos haluat luoda varmuuskopiokortin ja järjestelmänvalvojan salasana on jo määritetty, voit tallentaa salasanan uuteen korttiin.

VARO Näiden ohjeiden avulla voit muuttaa vain korttiin tallennetun salasanan. Tietokoneen asetukset -ohjelmassa tallennettu salasana ei muutu. Uutta korttia ei voi käyttää tietokoneeseen kirjautumiseen.

Järjestelmänvalvojan tai käyttäjän salasanan tallentaminen korttiin

1. Aseta sirukortti kortinlukijaan.
2. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
3. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **BIOS**.
4. Valitse oikean ruudun **BIOS Password on Smart Card** (BIOS-salasana sirukorttiin) -kohdassa **Store** (Tallenna).
5. Ohjatussa BIOS-salasanojen määritystoiminnossa (BIOS Password Wizard) voit
   - määrittää salasanan manuaalisesti
   - luoda satunnaisen 32-tavuisen salasanan.

   Huomautus Jos käytät tunnettua salasanaa, voit luoda kortista kaksoiskappaleen ilman palautustiedostoa. Satunnaisesti luotu salasana lisää tietoturvaa. Tällöin kaksoiskappaleiden luomiseen tarvitaan kuitenkin palautustiedosto.
6. Valitse **Access Privilege** (Käyttöoikeustaso) -kohdassa kortin tyypiksi **Administrator** (Järjestelmänvalvoja) tai **User** (Käyttäjä).
7. Valitse **Boot Requirements** (Käynnistysvaatimukset) -kohdassa valintaruutu, jos haluat määrittää sirukortin PIN-koodin pakolliseksi tietokonetta käynnistettäessä.

   Huomautus Jos et halua määrittää sirukortin PIN-koodia pakolliseksi tietokonetta käynnistettäessä, poista valinta valintaruudusta.
8. Anna sirukortin PIN-koodi ja valitse sitten **OK**.
9. Anna sirukortin PIN-koodi uudelleen **Valmis**-valintaikkunassa ja valitse sitten **Valmis**.

   Järjestelmä kehottaa sinua luomaan palautustiedoston.

   Huomautus Sirukortin palautustiedoston luominen on erittäin suositeltavaa. Lisätietoja on tämän luvun kohdassa Palautustiedoston luominen.

Yleiset toiminnot

BIOS-järjestelmän sirukorttiasetusten päivittäminen

Sirukortin PIN-koodin määrittäminen pakolliseksi tietokonetta käynnistettäessä

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **BIOS**.
3. Valitse oikean ruudun **Smart Card BIOS Password Properties** (Sirukortin BIOS-salasanaominaisuudet) -kohdassa **Asetukset** (Tallenna).
4. Valitse valintaruutu, jos haluat määrittää PIN-koodin pakolliseksi käynnistettäessä tietokonetta uudelleen.

   Huomautus Jos et halua määrittää PIN-koodia pakolliseksi, poista valinta valintaruudusta.

5. Anna sirukortin PIN-koodi ja valitse sitten **OK**.

Sirukortin lukijan valitseminen

Varmista, että Smart Card Security -ohjelmassa on valittu oikea kortinlukulaite, ennen kuin käytät sirukorttia. Jos Smart Card Security -ohjelmassa on valittu väärä kortinlukulaite, jotkin toiminnot eivät ehkä ole käytettävissä tai niiden näytössä on virheitä.

Sirukortin lukijan valitseminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **Yleistä**.
3. Valitse oikean ruudun **Smart Card Reader** (Sirukortin lukija) -kohdasta oikea lukulaite.
4. Aseta sirukortti kortinlukijaan. Laitteen tiedot päivittyvät automaattisesti.

Sirukortin PIN-koodin muuttaminen

Sirukortin PIN-koodin muuttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **Smart Card** (Älykortti).
3. Valitse oikean ruudun **Muuta PIN-koodi** -kohdassa **Muuta PIN-koodi**.
4. Kirjoita käytössä oleva sirukortin PIN-koodi.
5. Määritä uusi PIN-koodi ja vahvista se.
6. Valitse vahvistusikkunassa **OK**.

Sirukorttien tietojen varmuuskopioiminen ja palauttaminen

Kun sirukortti on alustettu ja se on valmis käytettäväksi, on suositeltavaa luoda siitä palautustiedosto. Palautustiedoston avulla yhden sirukortin tiedot voidaan siirtää toiseen sirukorttiin. Tiedosto on myös

sirukortin tietojen varmuuskopio, ja sen avulla varastetun tai kadonneen sirukortin tiedot voidaan siirtää toiseen korttiin.

VARO Jotta palautustiedoston tiedot olisivat aina ajan tasalla, luo sirukortista uusi palautustiedosto aina, kun tietoja on päivitetty. Säilytä palautustiedostoa huolellisesti. Jos käytät varmuuskopiona toista sirukorttia, muista siirtää päivitetyt tiedot aina myös siihen. Siirrä tiedot uuden palautustiedoston avulla.

Palautustiedoston luominen

Palautustiedoston luominen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **Smart Card** (Älykortti).
3. Valitse oikean ruudun **Palautus**-kohdassa **Luo**.
4. Anna sirukortin PIN-koodi ja valitse sitten **OK**.
5. Määritä tiedostopolku ja tiedoston nimi **Tiedostonimi**-ruudussa.

   VARO Älä tallenna palautustiedostoa tietokoneen kiintolevylle. Jos palautustiedosto on kiintolevyllä, et voi käyttää sitä ilman sirukorttia. Kiintolevylle tallennettu palautustiedosto saattaa olla myös toisten käyttäjien käytettävissä. Tämä on tietoturvariski.

6. Määritä ja vahvista palautustiedoston salasana ja valitse sitten **OK**.

VARO On tärkeää, että et unohda palautustiedoston salasanaa. Kortin tietoja ei voi palauttaa palautustiedostosta ilman salasanaa.

Sirukortin tietojen palauttaminen

Voit palauttaa sirukortin tiedot palautustiedostosta. Tämä toiminto on erityisen hyödyllinen silloin, kun kortti katoaa tai se varastetaan. Toiminnon avulla voi myös luoda varmuuskopiona toimivan sirukortin. Jos käsiteltävänä olevassa kortissa on jo tietoja, ne korvautuvat uusilla tiedoilla.

Varmista ennen toiminnon suorittamista, että käytettävissäsi on

- tietokone, johon on asennettu Smart Card Security -ohjelma
- sirukortin palautustiedosto
- sirukortin palautustiedoston salasana
- sirukortti.

Sirukortin tietojen palauttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Älykortin suojaus** ja valitse sitten **Smart Card** (Älykortti).
3. Aseta tietokoneeseen levyke tai muu tallennusväline, joka sisältää sirukortin palautustiedoston.
4. Aseta sirukortti kortinlukijaan. Jos korttia ei ole alustettu, järjestelmä kehottaa sinua alustamaan sen. Lisätietoja sirukortin alustamisesta on edellä tämän luvun kohdassa Sirukortin alustaminen.

5. Valitse oikean ruudun **Palautus**-kohdassa **Palauta**.
6. Varmista, että oikea palautustiedosto on valittuna, ja anna palautustiedoston salasana.
7. Anna sirukortin PIN-koodi.
8. Valitse **OK**. Alkuperäisen sirukortin tiedot tallentuvat uuteen sirukorttiin.

Varmuuskopiona toimivan sirukortin luominen

On suositeltavaa luoda sirukorteista kaksoiskappaleet, jotka toimivat varmuuskopioina. Varmuuskopiokortti voidaan luoda kahdella eri tavalla. Käytettävä tapa määräytyy sen mukaan, onko sirukortin salasana muodostettu manuaalisesti vai satunnaisesti.

Sirukortin kaksoiskappaleen luominen, kun salasana on muodostettu satunnaisesti

- Aseta sirukortti kortinlukulaitteeseen ja lataa korttiin asianmukainen palautustiedosto. Lisätietoja on edellä tämän luvun kohdassa Sirukortin tietojen palauttaminen.

Sirukortin kaksoiskappaleen luominen, kun salasana on muodostettu manuaalisesti

1. Alusta uusi sirukortti. Lisätietoja on edellä tämän luvun kohdassa Sirukortin alustaminen.
2. Tallenna järjestelmänvalvojan tai käyttäjän korttisalasana uuteen sirukorttiin. Lisätietoja on edellä tämän luvun kohdassa Järjestelmänvalvojan tai käyttäjän salasanan tallentaminen korttiin.

3 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools -ohjelmalla hallitaan Java-kortin asetuksia tietokoneissa, joissa on lisävarusteena saatava sirukortin lukija.

Kun käytettävissä on Java Card Security -ohjelma, voit

- käsitellä Java-korttien suojausominaisuuksia.
- ottaa Tietokoneen asetukset -ohjelmassa käyttöön käyttöoikeuden tarkistuksen Java-kortilla tietokonetta käynnistettäessä. Voit myös määrittää erilliset Java-kortit järjestelmänvalvojille ja käyttäjille. Kun tämä toiminto on otettu käyttöön, käyttöjärjestelmä latautuu vasta, kun käyttäjä on asettanut Java-kortin kortinlukijaan ja antanut PIN-koodin.
- määrittää ja vaihtaa PIN-koodin, jolla Java-kortin käyttäjä vahvistaa käyttöoikeutensa.
- varmuuskopioida ja palauttaa Java-korttiin liittyviä käynnistyksen yhteydessä tapahtuvan käyttöoikeuden tarkistuksen (käynnistystodennuksen) tietoja.

Yleiset toiminnot

Yleistä-sivulla voit suorittaa seuraavat tehtävät:

- Muuttaa Java-kortin PIN-koodin.
- Valita sirukortin lukijan.

Huomautus Sirukortin lukijassa voidaan käyttää sekä Java-kortteja että sirukortteja. Tämä toiminto on käytettävissä, jos tietokoneeseen on kytketty vähintään kaksi sirukortin lukijaa.

Java-kortin PIN-koodin muuttaminen

Java-kortin PIN-koodin muuttaminen

Huomautus Java-kortin PIN-koodissa on oltava 4 - 8 numeroa.

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Yleistä**.
3. Aseta kortinlukulaitteeseen Java-kortti, jossa on vielä käytössä vanha PIN-koodi.
4. Valitse oikeassa ruudussa **Muuta**.
5. Kirjoita vanha PIN-koodi **Muuta PIN-koodi** -valintaikkunan **Nykyinen PIN-koodi** -ruutuun.
6. Kirjoita uusi PIN-koodi **Uusi PIN-koodi** -ruutuun ja kirjoita se sitten uudelleen Vahvista uusi PIN-koodi -ruutuun.
7. Valitse **OK**.

Sirukortin lukijan valitseminen

Varmista, että Java Card Security -ohjelmassa on valittu oikea kortinlukulaite, ennen kuin käytät Java-korttia. Jos Java Card Security -ohjelmassa on valittu väärä kortinlukulaite, jotkin toiminnot eivät ehkä ole käytettävissä tai niiden näytössä on virheitä.

Sirukortin lukijan valitseminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Yleistä**.
3. Aseta Java-kortti sirukortin lukijaan.
4. Valitse oikean ruudun **Smart Card Reader** (Sirukortin lukija) -kohdasta oikea lukulaite.

Lisätoiminnot (vain järjestelmänvalvojille)

Lisäasetukset-sivulla voit suorittaa seuraavat tehtävät:

- Määrittää Java-kortin PIN-koodin.
- Määrittää Java-kortille uuden nimen.
- Määrittää käynnistystodennuksen (käyttöoikeuden tarkistuksen käynnistyksen yhteydessä).
- Varmuuskopioida ja palauttaa Java-korttien tietoja.

Huomautus Lisäasetukset-sivun avaamiseen tarvitaan Tietokoneen asetukset -ohjelman asetussalasana.

Java-kortin PIN-koodin määrittäminen

Java-korttia voi käyttää käynnistystodennukseen vasta, kun sille on määritetty PIN-koodi.

Java-kortin PIN-koodin määrittäminen

Huomautus Java-kortin PIN-koodissa on oltava 4 - 8 numeroa.

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Yleistä**.
3. Aseta uusi Java-kortti sirukortin lukijaan.
4. Kun **Muuta PIN-koodi** -valintaikkuna tulee näyttöön, kirjoita uusi PIN-koodi **Uusi PIN-koodi** -ruutuun. Kirjoita sitten PIN-koodi uudelleen **Vahvista uusi PIN-koodi** -ruutuun.
5. Valitse **OK**.

Java-kortin nimen määrittäminen

Java-korttia voi käyttää käynnistystodennukseen vasta, kun sille on määritetty nimi.

Java-kortin nimen määrittäminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Lisäasetukset**.
3. Kun **Asetussalasana**-valintaikkuna tulee näyttöön, anna Tietokoneen asetukset -ohjelman asetussalasana ja valitse sitten **OK**.
4. Aseta Java-kortti sirukortin lukijaan.

   Huomautus Jos kortille ei ole määritetty PIN-koodia, Muuta PIN-koodi -valintaikkuna tulee näyttöön. Määritä uusi PIN-koodi tässä valintaikkunassa.

5. Valitse oikean ruudun **Java Card** -kohdassa **Muuta**.
6. Määritä Java-kortille nimi **Nimi**-ruudussa.

7. Kirjoita Java-kortin nykyinen PIN-koodi **PIN-koodi**-ruutuun.
8. Valitse **OK**.

Käynnistystodennuksen määrittäminen

Kun tämä toiminto on otettu käyttöön, käynnistystodennuksessa on käytettävä Java-korttia.

Java-kortin käynnistystodennuksen käyttöönotto sisältää seuraavat vaiheet:

1. Ota Java-kortin käynnistystodennuksen tuki käyttöön BIOS Configuration -ohjelmassa tai Tietokoneen asetukset -ohjelmassa. Lisätietoja on luvussa 5 BIOS Configuration for HP ProtectTools kohdassa Sirukortin ja Java-kortin käynnistystodennuksen tuen ottaminen käyttöön tai poistaminen käytöstä.
2. Ota Java-kortin käynnistystodennuksen tuki käyttöön Java Card Security -ohjelmassa. Lisätietoja on jäljempänä tämän luvun kohdassa Java-kortin käynnistystodennuksen tuen ottaminen käyttöön ja järjestelmänvalvojan Java-kortin luominen.
3. Luo ja ota käyttöön järjestelmänvalvojan Java-kortti.

Java-kortin käynnistystodennuksen tuen ottaminen käyttöön ja järjestelmänvalvojan Java-kortin luominen

Java-kortin käynnistystodennuksen tuen ottaminen käyttöön

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Lisäasetukset**.
3. Kun **Tietokoneen asetussalasana** -valintaikkuna tulee näyttöön, anna Tietokoneen asetukset -ohjelman asetussalasana ja valitse sitten **OK**.
4. Aseta Java-kortti sirukortin lukijaan.

   Huomautus Jos kortille ei ole määritetty PIN-koodia, **Muuta PIN-koodi** -valintaikkuna tulee näyttöön. Määritä uusi PIN-koodi tässä valintaikkunassa.

5. Valitse oikean ruudun **Käynnistystodennus**-kohdassa oleva **Ota käyttöön** -valintaruutu.
6. Jos DriveLock ei ole käytössä, anna Java-kortin PIN-koodi ja valitse sitten **OK**.

   TAI

Jos DriveLock on käytössä, toimi seuraavasti:

a. Valitse **Tee Java-kortin käyttäjätiedoista ainutlaatuiset**.

   TAI

   Valitse **Muuta Java-kortin käyttäjätiedot DriveLock-salasanaa vastaaviksi**.

   Huomautus Jos DriveLock on otettu käyttöön tietokoneessa, voit määrittää Java-kortin käyttäjätiedot vastaamaan DriveLock-salasanaa. Tällöin voit suorittaa sekä DriveLock-todennuksen että Java-korttitodennuksen Java-kortilla, kun käynnistät tietokoneen.

b. Jos DriveLock-salasana on käytössä, kirjoita se **DriveLock-salasana** -ruutuun ja kirjoita se sitten uudelleen **Vahvista salasana** -ruutuun.

c. Anna Java-kortin PIN-koodi.

d. Valitse **OK**.

7. Jos järjestelmä kehottaa sinua luomaan palautustiedoston, katso lisäohjeita kohdasta Palautustiedoston luominen. Voit myös valita **Peruuta** ja luoda palautustiedoston myöhemmin.

Käyttäjän Java-kortin luominen

Huomautus Käyttäjän Java-kortin voi luoda vasta, kun käynnistystodennuksen tuki on otettu käyttöön ja järjestelmänvalvojan Java-kortti on luotu.

Käyttäjän Java-kortin luominen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Lisäasetukset**.
3. Kun **Asetussalasana**-valintaikkuna tulee näyttöön, anna Tietokoneen asetukset -ohjelman asetussalasana ja valitse sitten **OK**.
4. Aseta kortinlukijaan Java-kortti, jonka haluat määrittää käyttäjän kortiksi.
5. Napsauta oikean ruudun **Käynnistystodennus**-kohdassa **Käyttäjän kortin käyttäjätiedot** -kohdan vieressä olevaa **Luo**-painiketta.
6. Määritä Java-kortille PIN-koodi ja valitse sitten OK.

Java-kortin käynnistystodennuksen tuen poistaminen käytöstä

Kun käynnistystodennuksen tuki on poistettu käytöstä, Java-korttia ei enää tarvita tietokonetta käynnistettäessä.

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Lisäasetukset**.
3. Kun **Asetussalasana**-valintaikkuna tulee näyttöön, anna Tietokoneen asetukset -ohjelman asetussalasana ja valitse sitten **OK**.

4. Aseta Java-kortti kortinlukijaan, anna PIN-koodi ja valitse sitten **OK**.
5. Poista valinta oikean ruudun **Käynnistystodennus**-kohdassa olevasta **Ota käyttöön** -;valintaruudusta.

Java-korttien tietojen varmuuskopioiminen ja palauttaminen

Kun Java-kortille on määritetty käynnistystodennuksessa tarvittavat tiedot, on suositeltavaa luoda siitä palautustiedosto. Palautustiedoston avulla yhden Java-kortin käynnistystodennustiedot voidaan siirtää toiselle Java-kortille. Tiedosto on myös Java-kortin tietojen varmuuskopio, ja sen avulla varastetun tai kadonneen Java-kortin tiedot voidaan siirtää toiseen korttiin.

VARO Jotta palautustiedoston tiedot olisivat aina ajan tasalla, luo Java-kortista uusi palautustiedosto aina, kun tietoja on päivitetty. Tallenna tiedot siirrettävään tallennusvälineeseen ja säilytä sitä huolella. Jos käytät varmuuskopiona toista Java-korttia, muista siirtää päivitetyt tiedot aina myös siihen. Siirrä tiedot uuden palautustiedoston avulla.

Palautustiedoston luominen

Palautustiedoston luominen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Lisäasetukset**.
3. Kun **Asetussalasana**-valintaikkuna tulee näyttöön, anna Tietokoneen asetukset -ohjelman asetussalasana ja valitse sitten **OK**.
4. Valitse oikean ruudun **Palautus**-kohdassa **Luo**.
5. Määritä tiedostopolku ja tiedoston nimi **Tiedostonimi**-ruudussa.

   VARO Älä tallenna palautustiedostoa tietokoneen kiintolevylle. Jos palautustiedosto on kiintolevyllä, et voi käyttää sitä ilman Java-korttia. Kiintolevylle tallennettu palautustiedosto saattaa olla myös toisten käyttäjien käytettävissä. Tämä on tietoturvariski.

6. Kirjoita palautustiedolle salasana **Palautustiedoston salasana** -ruutuun ja kirjoita se sitten uudelleen **Vahvista salasana** -ruutuun.
7. Anna Java-kortin PIN-koodi ja valitse sitten **OK**.

VARO On tärkeää, että et unohda palautustiedoston salasanaa. Kortin tietoja ei voi palauttaa palautustiedostosta ilman salasanaa.

Java-kortin tietojen palauttaminen

Voit palauttaa Java-kortin tiedot palautustiedostosta. Tämä toiminto on erityisen hyödyllinen silloin, kun kortti katoaa tai se varastetaan. Toiminnon avulla voi myös luoda varmuuskopiona toimivan Java-kortin. Jos käsiteltävänä olevassa kortissa on jo tietoja, ne korvautuvat uusilla tiedoilla.

Varmista ennen toiminnon suorittamista, että käytettävissäsi on

- tietokone, johon on asennettu Java Card Security -ohjelma
- Java-kortin palautustiedosto

- Java-kortin palautustiedoston salasana
- Java-kortti.

Java-kortin tietojen palauttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Java Card Security** ja valitse sitten **Lisäasetukset**.
3. Kun **Asetussalasana**-valintaikkuna tulee näyttöön, anna Tietokoneen asetukset -ohjelman asetussalasana ja valitse sitten **OK**.
4. Aseta tietokoneeseen levyke tai muu tallennusväline, joka sisältää Java-kortin palautustiedoston.
5. Aseta Java-kortti sirukortin lukijaan. Jos kortille ei ole määritetty PIN-koodia, järjestelmä kehottaa sinua määrittämään sen. Lisätietoja Java-kortin PIN-koodin määrittämisestä on edellä tämän luvun kohdassa Java-kortin PIN-koodin määrittäminen.
6. Valitse oikean ruudun Palautus-kohdassa **Palauta**.
7. Varmista, että oikea palautustiedosto on valittuna, ja anna palautustiedoston salasana.
8. Anna Java-kortin PIN-koodi.
9. Valitse **OK**.

   Alkuperäisen Java-kortin tiedot tallentuvat uuteen Java-korttiin.

Varmuuskopiona toimivan Java-kortin luominen

On suositeltavaa luoda Java-korteista kaksoiskappaleet, jotka toimivat varmuuskopioina.

Java-kortin kaksoiskappaleen luominen

▲ Aseta Java-kortti kortinlukulaitteeseen ja lataa korttiin asianmukainen palautustiedosto. Lisätietoja on edellä tämän luvun kohdassa Java-kortin tietojen palauttaminen.

4 Embedded Security for HP ProtectTools

Huomautus Tietokoneessa on oltava TPM (Trusted Platform Module) Embedded Security -siru (upotettu suojaussiru), jotta voit käyttää Embedded Security for HP ProtectTools -ohjelmaa.

Embedded Security for HP ProtectTools -ohjelma suojaa käyttäjän tietoja ja käyttöoikeuksia luvattomalta käytöltä. Ohjelmisto sisältää seuraavat suojausominaisuudet:

- Enhanced Microsoft Encryption File System (EFS) -järjestelmä tiedostojen ja kansioiden salaamiseen
- käyttäjätietojen suojaus henkilökohtaisen suojatun levyaseman (PSD) avulla
- tiedonhallintatoiminnot, kuten hierarkian varmuuskopiointi ja palauttaminen
- muiden toimittajien sovellusten (esimerkiksi Microsoft® Outlook ja Internet Explorer) tuki suojatun varmenteen toimintoja varten Embedded Security -ohjelmaa käytettäessä.

Valinnainen TPM Embedded Security -siru ottaa käyttöön ja tehostaa muita HP ProtectTools Security Manager -ohjelman suojaustoimintoja. Credential Manager for HP ProtectTools voi esimerkiksi käyttää tätä sirua todennuksessa, kun käyttäjä kirjautuu Windowsiin. Tietyissä tietokoneen malleissa TPM Embedded Security -siru ottaa käyttöön myös tehostettuja BIOS-suojaustoimintoja, jotka avataan BIOS Configuration for HP ProtectTools -ohjelman kautta.

Asetusten määrittäminen

VARO Järjestelmänvalvojan tulee alustaa upotettu suojaussiru välittömästi. Näin vältetään monia tietoturvariskejä. Jos sirua ei oteta käyttöön, tietokone voi joutua luvattoman käyttäjän, madon tai viruksen hyökkäyksen kohteeksi. Tunkeutuja voi ottaa tietokoneen käyttöönsä ja päästä esimerkiksi käsittelemään varmistustiedostoja tai määrittämään käyttäjien käyttöoikeusasetuksia.

Ota upotettu suojaussiru käyttöön ja alusta se noudattamalla tässä annettuja kaksivaiheisia ohjeita.

Upotetun suojaussirun käyttöön ottaminen

Upotettu suojaussiru otetaan käyttöön Tietokoneen asetukset -ohjelmassa. Sirua ei voi ottaa käyttöön BIOS Configuration for HP ProtectTools -ohjelmassa.

Upotetun suojaussirun ottaminen käyttöön

1. Avaa Tietokoneen asetukset käynnistämällä tai uudelleenkäynnistämällä tietokone ja painamalla f10-näppäintä, kun näytön vasemmassa alakulmassa näkyy teksti f10 = ROM Based Setup.
2. Jos et ole määrittänyt järjestelmänvalvojan salasanaa, valitse nuolinäppäimillä **Turvallisuus > Asetussalasana** ja paina enter-näppäintä.
3. Kirjoita salasana **Uusi salasana**- ja **Vahvista uusi salasana** -ruutuihin ja paina sitten f10-näppäintä.
4. Valitse nuolinäppäinten avulla **Turvallisuus**-valikosta **TPM Sulautettu suojaus** ja paina sitten enter-näppäintä.
5. Jos laite on piilotettuna, valitse **Sulautettu suojaus** -kohdassa **Available** (Käytettävissä).
6. Valitse **Embedded security device state** (Sulautetun suojauslaitteen tila) -asetus ja muuta sen arvoksi **Ota käyttöön**.
7. Hyväksy muutokset sulautetun suojauksen asetuksiin painamalla f10-näppäintä.
8. Jos haluat tallentaa tekemäsi asetukset ja lopettaa Tietokoneen asetukset -ohjelman, valitse nuolinäppäimillä **File > Save Changes and Exit** (Tiedosto > Tallenna muutokset ja lopeta). Noudata sitten näyttöön tulevia ohjeita.

Upotetun suojaussirun alustaminen

Upotetun suojaussirun alustukseen kuuluvat seuraavat vaiheet:

- Upotetun suojaussirun pääkäyttäjän salasanan määrittäminen. Salasanalla suojataan kaikki sirun pääkäyttäjän toiminnot luvattomalta käytöltä.
- Varmistustiedostojen määrittäminen. Varmistustiedostot ovat suojattuja tallennuspaikkoja, joiden avulla kaikkien käyttäjien perusavaimet voidaan tarvittaessa salata uudelleen.

Upotetun suojaussirun alustaminen

1. Napsauta tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen HP ProtectTools Security Manager -kuvaketta hiiren kakkospainikkeella ja valitse sitten **Embedded Security Initialization** (Sulautetun suojauksen alustus).

   Näyttöön tulee ohjattu HP ProtectTools Embedded Security -alustustoiminto.

2. Valitse **Seuraava**.

3. Määritä ja vahvista pääkäyttäjän salasana ja valitse sitten **Seuraava**.

   Näyttöön tulee Setup Emergency Recovery (Määritä varmistustiedostot) -valintaikkuna.

4. Jos haluat ottaa käyttöön varmistustiedostojen oletussijainnin, valitse **Seuraava**. Jos haluat valita toisen sijainnin, valitse ensin **Selaa** ja sitten **Seuraava**.

5. Määritä ja vahvista tietojen palautuksessa tarvittava salasana ja valitse sitten **Seuraava**.

6. Valitse **Selaa** ja määritä varmistustiedostojen sijainti. Valitse sitten **Seuraava**.

7. Valitse Summary (Yhteenveto) -sivulta **Seuraava**.

   - Jos et halua määrittää nyt peruskäyttäjätiliä, poista valinta **Start the Embedded Security User Initialization Wizard** (Käynnistä ohjattu sulautetun suojauksen käyttäjän alustustoiminto) -valintaruudusta ja valitse sitten **Valmis**. Voit käynnistää ohjatun toiminnon manuaalisesti ja määrittää peruskäyttäjätilin milloin tahansa noudattamalla seuraavassa osassa annettuja ohjeita.

   - Jos haluat määrittää peruskäyttäjätilin, valitse **Start the Embedded Security User Initialization Wizard** (Käynnistä ohjattu sulautetun suojauksen käyttäjän alustustoiminto) -valintaruutu ja valitse sitten **Valmis**. Embedded Security User Initialization Wizard (Ohjattu sulautetun suojauksen käyttäjän alustustoiminto) tulee näyttöön. Lisätietoja on tämän luvun seuraavassa osassa.

Peruskäyttäjätilin määrittäminen

Embedded Security -ohjelman peruskäyttäjätilin määritystoiminnolla

- luodaan peruskäyttäjäavain, joka suojaa salattuja tietoja, ja määritetään peruskäyttäjän avaimen salasana, joka suojaa peruskäyttäjän avainta
- määritetään henkilökohtainen suojattu levyasema (PSD), johon voidaan tallentaa salattuja tiedostoja ja kansioita.

VARO Säilytä peruskäyttäjän avaimen salasana huolellisesti. Salattuja tietoja ei voi käyttää tai palauttaa ilman salasanaa.

Peruskäyttäjätilin määrittäminen ja käyttäjän suojausominaisuuksien käyttöön ottaminen

1. Jos Embedded Security User Initialization Wizard (Ohjattu sulautetun suojauksen käyttäjän alustustoiminto) ei ole käynnissä, valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.

2. Valitse vasemmasta ruudusta **Sulautettu suojaus** ja valitse sitten **User Settings** (Käyttäjän asetukset).

3. Valitse oikean ruudun **Embedded Security Features** (Sulautetun suojauksen ominaisuudet) -kohdassa **Määritä**.

   Embedded Security User Initialization Wizard (Ohjattu sulautetun suojauksen käyttäjän alustustoiminto) tulee näyttöön.

4. Valitse **Seuraava**.

5. Määritä ja vahvista peruskäyttäjän avaimen salasana ja valitse sitten **Seuraava**.

6. Vahvista asetukset valitsemalla **Seuraava**.

7. Valitse tarvittavat suojausominaisuudet ja valitse sitten **Seuraava**.

8. Valitse uudelleen **Seuraava**.

   Huomautus Jos haluat käyttää suojattua sähköpostia, määritä ensin sähköpostiohjelman asetukset niin, että ohjelma käyttää Embedded Security -ohjelmalla luotua digitaalista varmennetta. Jos digitaalista varmennetta ei ole käytettävissä, pyydä se sertifikaatin myöntäjältä. Sähköpostiohjelman Ohjeessa on lisätietoja asetusten määrittämisestä ja digitaalisen varmenteen (sertifikaatin) hankkimisesta.

9. Jos käytettävissä on useita salausvarmenteita, valitse tarvittava varmenne ja valitse sitten **Seuraava**.

10. Valitse henkilökohtaisen suojatun levyaseman (PSD) kirjain ja nimi ja valitse sitten **Seuraava**.

11. Valitse henkilökohtaisen suojatun levyaseman sijainti ja koko ja valitse sitten **Seuraava**.

12. Valitse Summary (Yhteenveto) -sivulta **Seuraava**.

13. Valitse **Valmis**.

Yleiset toiminnot

Kun peruskäyttäjätili on määritetty, käytettävissä on seuraavat toiminnot:

- Tiedostojen ja kansioiden salaaminen
- Salatun sähköpostin lähettäminen ja vastaanottaminen

Henkilökohtaisen suojatun levyaseman käyttäminen

Kun levyasema on määritetty, järjestelmä pyytää seuraavan kirjautumisen yhteydessä käyttäjää antamaan peruskäyttäjän avaimen salasanan. Jos peruskäyttäjän avaimen salasana on oikein, henkilökohtainen suojattu levyasema on käytettävissä Resurssienhallinnassa.

Tiedostojen ja kansioiden salaaminen

Kun käsitellään salattuja tiedostoja, on otettava huomioon seuraavat säännöt:

- Vain NTFS-osioihin tallennettuja tiedostoja ja kansioita voi salata. FAT-osioihin tallennettuja tiedostoja ja kansioita ei voi salata.
- Järjestelmätiedostoja ja pakattuja tiedostoja ei voi salata. Salattuja tiedostoja ei voi pakata.
- Väliaikaistiedostot tulee salata, koska luvattomat käyttäjät saattavat olla kiinnostuneita niistä.
- Kun tiedosto tai kansio salataan ensimmäisen kerran, järjestelmä määrittää automaattisesti palautuskäytännön. Näin varmistetaan, että salausvarmenteen ja käyttäjän avainten mahdollisesti tuhoutuessa tietojen salaus voidaan purkaa palautusagentin avulla.

Tiedostojen ja kansioiden salaaminen

1. Napsauta salattavaa tiedostoa tai kansiota hiiren kakkospainikkeella.
2. Valitse **Encrypt** (Salaa).
3. Valitse jompikumpi seuraavista vaihtoehdoista:
   - **Apply changes to this folder only** (Tee muutokset vain tämän kansion asetuksiin)
   - **Apply changes to this folder, subfolders, and files** (Tee muutokset tämän kansion, alikansioiden ja tiedostojen asetuksiin).
4. Valitse **OK**.

Salatun sähköpostin lähettäminen ja vastaanottaminen

Embedded Security -ohjelman avulla voit lähettää ja vastaanottaa salattua sähköpostia. Toimintatavat vaihtelevat kuitenkin käytössä olevan sähköpostiohjelman mukaan. Lisätietoja on Embedded Security -ohjelman käytönaikaisessa ohjeessa sekä sähköpostiohjelman Ohjeessa.

Peruskäyttäjän avaimen salasanan muuttaminen

Peruskäyttäjän avaimen salasanan muuttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Sulautettu suojaus** ja valitse sitten **User Settings** (Käyttäjän asetukset).
3. Valitse oikean ruudun **Basic User Key password** (Peruskäyttäjän avaimen salasana) -kohdassa **Muuta**.
4. Kirjoita vanha salasana ja määritä ja vahvista sitten uusi salasana.
5. Valitse **OK**.

Lisätoiminnot

Tietojen varmuuskopiointi ja palauttaminen

Embedded Security -ohjelman varmuuskopiointitoiminto luo arkiston, joka sisältää varmennetiedot. Varmuuskopion avulla tiedot voidaan palauttaa tarvittaessa käyttöön.

Varmuuskopiotiedoston luominen

Varmuuskopiotiedoston luominen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Sulautettu suojaus** ja valitse sitten **Backup** (Varmuuskopio).
3. Valitse oikeassa ruudussa **Backup** (Varmuuskopio).
4. Napsauta **Browse** (Selaa) -painiketta ja valitse varmuuskopiotiedoston tallennuskohde.
5. Valitse, lisätäänkö varmuuskopiotietoihin varmistustiedostot.
6. Valitse **Seuraava**.
7. Valitse **Valmis**.

Varmennetietojen palauttaminen varmuuskopiotiedostosta

Tietojen palauttaminen varmuuskopiotiedostosta

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Sulautettu suojaus** ja valitse sitten **Backup** (Varmuuskopio).
3. Valitse oikeassa ruudussa **Palauta**.
4. Napsauta **Browse** (Selaa) -painiketta sekä etsi ja valitse varmuuskopiotiedosto.

5. Valitse **Seuraava**.
6. Valitse, käynnistetäänkö Embedded Security User Initialization Wizard (Ohjattu sulautetun suojauksen käyttäjän alustustoiminto).
   - Jos haluat käynnistää ohjatun alustustoiminnon, valitse Valmis ja suorita sitten alustus loppuun noudattamalla näyttöön tulevia ohjeita. Lisätietoja on edellä tämän luvun kohdassa Peruskäyttäjätilin määrittäminen.
   - Jos et halua käynnistää ohjattua alustustoimintoa, valitse **Valmis**.

Pääkäyttäjän salasanan muuttaminen

Pääkäyttäjän salasanan muuttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Sulautettu suojaus** ja valitse sitten **Lisäasetukset**.
3. Valitse oikean ruudun **Owner Password** (Pääkäyttäjän salasana) -kohdassa **Muuta**.
4. Kirjoita vanha pääkäyttäjän salasana ja määritä ja vahvista sitten uusi salasana.
5. Valitse **OK**.

Käyttäjän salasanan määrittäminen uudelleen

Järjestelmänvalvoja voi määrittää salasanan uudelleen, jos käyttäjä on unohtanut sen. Lisätietoja on ohjelman käytönaikaisessa ohjeessa.

Embedded Security -ohjelman ottaminen käyttöön ja poistaminen käytöstä

Voit poistaa Embedded Security -toiminnot käytöstä, jos haluat työskennellä ilman suojaustoimintoja.

Valittavana on kaksi tasoa Embedded Security -toimintojen käytöstä poistamiseen. Valittu taso vaikuttaa myös siihen, kuinka toiminnot saadaan takaisin käyttöön.

- Tilapäinen käytöstä poisto: Tätä vaihtoehtoa käytettäessä Embedded Security -ohjelma tulee automaattisesti uudelleen käyttöön, kun Windows käynnistetään. Oletuksena on, että tämä vaihtoehto on kaikkien käyttäjien käytettävissä.
- Pysyvä käytöstä poisto: Tätä vaihtoehtoa käytettäessä Embedded Security -ohjelman käyttöönottoon tarvitaan pääkäyttäjän salasana. Tämä vaihtoehto on vain pääkäyttäjien käytettävissä.

Embedded Security -ohjelman poistaminen pysyvästi käytöstä

Embedded Security -ohjelman poistaminen pysyvästi käytöstä

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Sulautettu suojaus** ja valitse sitten **Lisäasetukset**.
3. Valitse oikean ruudun **Sulautettu suojaus** -kohdassa **Poista käytöstä**.
4. Kirjoita pääkäyttäjän salasanasi, kun ohjelma pyytää sitä, ja valitse sitten **OK**.

Embedded Security -ohjelman ottaminen käyttöön pysyvän käytöstä poistamisen jälkeen

Embedded Security -ohjelman ottaminen käyttöön pysyvän käytöstä poistamisen jälkeen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Sulautettu suojaus** ja valitse sitten **Lisäasetukset**.
3. Valitse oikean ruudun **Sulautettu suojaus** -kohdassa **Ota käyttöön**.
4. Kirjoita pääkäyttäjän salasanasi, kun ohjelma pyytää sitä, ja valitse sitten **OK**.

Avainten siirtäminen ohjatulla siirtotoiminnolla (Migration Wizard)

Järjestelmänvalvoja voi hallita, palauttaa ja siirtää avaimia ja varmenteita.

Lisätietoja näistä toiminnoista on Embedded Security -ohjelman käytönaikaisessa ohjeessa.

5 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools -ohjelman avulla voit käsitellä Tietokoneen asetukset -apuohjelman suojaus- ja kokoonpanoasetuksia. Tämän ominaisuuden ansiosta käyttäjät voivat käsitellä sellaisia Windows-järjestelmän suojausominaisuuksia, joita hallitaan Tietokoneen asetukset -apuohjelmalla.

BIOS-määritysten avulla voit

- hallita käynnistyssalasanoja ja järjestelmänvalvojan salasanoja
- määrittää muita käynnistyksen todennusominaisuuksia, kuten sirukorttien salasanojen käyttöönoton ja sulautetun suojaustodennuksen tuen
- ottaa käyttöön ja poistaa käytöstä laitteisto-ominaisuuksia (kuten käynnistyksen CD-levyltä tai eri laiteporteista)
- määrittää käynnistysasetuksia, kuten MultiBoot-apuohjelman käyttöönoton ja käynnistysjärjestyksen muuttamisen.

Huomautus Monia BIOS Configuration for HP ProtectTools -ohjelman ominaisuuksia voidaan käyttää myös Tietokoneen asetukset -apuohjelmassa.

Yleiset toiminnot

BIOS-määritysten avulla voit hallita monia tietokoneasetuksia, jotka muutoin olisivat käytettävissä vain, kun käynnistyksen yhteydessä painetaan f10-näppäintä ja näyttöön tulee Tietokoneen asetukset -apuohjelma.

Käynnistysasetusten hallinta

BIOS-määritysten avulla voit hallita monia sellaisten tehtävien asetuksia, jotka suoritetaan tietokoneen virran kytkemisen tai uudelleenkäynnistyksen yhteydessä.

Voit käsitellä käynnistysasetuksia seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **BIOS-määritykset**.
3. Kirjoita BIOS-järjestelmänvalvojan salasanakehotteeseen Tietokoneen asetukset -apuohjelman järjestelmänvalvojan salasana ja valitse sitten **OK**.

   Huomautus BIOS-järjestelmänvalvojan salasanakehote tulee näkyviin vain, jos Tietokoneen asetukset -apuohjelman asetussalasana on määritetty. Lisätietoja Tietokoneen asetukset -apuohjelman asetussalasanan määrittämisestä on jäljempänä kohdassa Asetussalasanan määrittäminen.

4. Valitse vasemmasta ruudusta **Järjestelmän kokoonpano**.
5. Valitse f9-, f10- ja f12-näppäinten **Pikakäynnistysvalikon viive (sekunteina)** -asetuksen viiveet (sekunteina).
6. Ota **MultiBoot** käyttöön tai poista se käytöstä.
7. Jos MultiBoot-toiminto on käytössä, valitse käynnistysjärjestys valitsemalla käynnistyslaite ja muuttamalla tarvittaessa luettelon järjestystä ala- tai ylänuolinäppäimillä.
8. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Järjestelmän kokoonpanoasetusten ottaminen käyttöön ja käytöstä poistaminen

Huomautus Tietokoneesi ei ehkä tue kaikkia taulukossa mainittuja asetuksia.

Voit ottaa laitteita tai suojausasetuksia käyttöön tai poistaa niitä käytöstä seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **BIOS-määritykset**.
3. Kirjoita BIOS-järjestelmänvalvojan salasanakehotteeseen Tietokoneen asetukset -apuohjelman järjestelmänvalvojan salasana ja valitse sitten **OK**.

4. Valitse vasemmasta ruudusta **Järjestelmän kokoonpano** ja ota sitten käyttöön haluamasi järjestelmän kokoonpanoasetus tai poista se käytöstä tai määritä järjestelmän kokoonpanoasetus oikeassa ruudussa:

   - Porttiasetukset
     - Sarjaportti
     - Infrapunaportti
     - Rinnakkaisportti
     - SD Slot (SD-korttipaikka)
     - USB-portti
     - 1394-portti
     - Cardbus-korttipaikka
     - ExpressCard-korttipaikka
   - Boot Options (Käynnistysasetukset)
     - f9-, f10- ja f12-toimintojen viive (sekunteina)
     - MultiBoot
     - Pikakäynnistysvalikon viive (sekunteina)
     - CD-levyltä käynnistys
     - Levykkeeltä käynnistys
     - Käynnistys sisäisen verkkokortin avulla
     - Käynnistys sisäisen verkkokortin avulla -tila (PXE tai RPL)
     - Käynnistysjärjestys
   - Laitekokoonpanot
     - NumLock at Boot (NumLock käynnistyksen yhteydessä)
     - Vaihda fn/ctrl-näppäimet
     - Useita osoitinlaitteita
     - Vanhojen USB-laitteiden tuki
     - Rinnakkaisporttitila (vakio, kaksisuuntainen, EPP tai ECP)
     - Tietojen suorittamisen estäminen
     - SATA- oma tila
     - Dual Core -suoritin
     - Automaattinen Intel® SpeedStep -toiminnan tuki
     - Tuuletin päällä aina kytkettäessä verkkovirtaa

- BIOS DMA -tiedonsiirrot
- Intel tai AMD PSAE Execution Disable

- Sisäiset laiteasetukset
  - Embedded WLAN Device Radio (Sulautettu WLAN-laiteradio)
  - Embedded WWAN Device Radio (Sulautettu WWAN-laiteradio)
  - Sisäinen Bluetooth®-radio
  - LAN/WLAN-järjestelmävaihto
  - Käynnistäminen lähiverkon kautta sammutuksen jälkeen

5. Tallenna muutokset ja lopeta ohjelma valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Lisätoiminnot

HP ProtectTools -asetusten hallinta

BIOS-määrityksissä voidaan hallita joitakin HP ProtectTools Security Manager -ohjelmiston ominaisuuksia.

Sirukortin ja Java-kortin käynnistystodennuksen tuen ottaminen käyttöön tai poistaminen käytöstä

Kun tämä asetus on käytössä, voit käyttää sirukorttia tai Java-korttia käyttäjän todentamisessa, kun tietokoneeseen kytketään virta.

Huomautus Jos haluat ottaa käynnistystodennuksen kaikki ominaisuudet käyttöön, myös sirukortti tulisi määrittää käyttämällä Smart Card Security for HP ProtectTools- tai Java Card Security for HP ProtectTools -moduulia.

Voit ottaa käyttöön tai poistaa käytöstä käynnistystodennuksen tuen seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **BIOS-määritykset**.
3. Kirjoita BIOS-järjestelmänvalvojan salasanakehotteeseen Tietokoneen asetukset -apuohjelman järjestelmänvalvojan salasana ja valitse sitten **OK**.
4. Valitse vasemmasta ruudusta **Suojaus**.
5. Valitse **Älykortin suojaus** -kohdasta **Ota käyttöön**.

Huomautus Voit poistaa sirukortin käynnistystodennuksen käytöstä valitsemalla **Poista käytöstä**.

6. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Sulautetun suojauksen käynnistystodennuksen tuen ottaminen käyttöön tai poistaminen käytöstä

Kun tämä asetus on käytössä, järjestelmä voi käyttää TPM-upotettua suojaussirua (jos käytettävissä) käyttäjän todentamisessa, kun tietokoneeseen kytketään virta.

Huomautus Jos haluat ottaa käynnistystodennuksen kaikki ominaisuudet käyttöön, myös TPM-upotettu suojaussiru tulisi määrittää käyttämällä Embedded Security for HP ProtectTools -moduulia.

Ota sulautetun suojauksen käynnistystodennuksen tuki käyttöön seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **BIOS-määritykset**.
3. Kirjoita BIOS-järjestelmänvalvojan salasanakehotteeseen Tietokoneen asetukset -apuohjelman järjestelmänvalvojan salasana ja valitse sitten **OK**.
4. Valitse vasemmasta ruudusta **Suojaus**.
5. Valitse **Sulautettu suojaus** -kohdasta **Ota käynnistystodennus käyttöön**.

   Huomautus Voit poistaa sulautetun suojauksen käynnistystodennuksen käytöstä valitsemalla **Poista käytöstä**.

6. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Automaattisen DriveLock-kiintolevysuojauksen ottaminen käyttöön ja poistaminen käytöstä

Kun tämä asetus on käytössä, DriveLock-salasanat luodaan automaattisesti ja määritetään levyasemalle sekä suojataan TPM-upotetun suojaussirun avulla.

Huomautus Automaattisesti luodut salasanat määritetään levyasemalle vasta sitten, kun olet käynnistänyt tietokoneen uudelleen ja kirjoittanut salasanakehotteeseen TPM-upotetun suojaussalasanan.

Automaattinen DriveLock -asetusta ei voi ottaa käyttöön, ellei

- tietokoneeseen ole asennettu ja alustettu TMP-suojaussirua. Lisätietoja TMP-suojaussirun käyttöön ottamisesta ja alustamisesta on luvun 4, Embedded Security for HP ProtectTools, kohdissa Upotetun suojaussirun käyttöön ottaminen ja Upotetun suojaussirun alustaminen.
- DriveLock-sanasanoja ei ole vielä otettu käyttöön.

Huomautus Jos olet määrittänyt tietokoneen DriveLock-salasanat manuaalisesti, sinun täytyy ensin poistaa ne käytöstä, ennen kuin voit määrittää automaattisen Drivelock-suojauksen.

Voit ottaa automaattisen DriveLock-suojauksen käyttöön tai poistaa sen käytöstä seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **BIOS-määritykset**.
3. Kirjoita BIOS-järjestelmänvalvojan salasanakehotteeseen Tietokoneen asetukset -apuohjelman järjestelmänvalvojan salasana ja valitse sitten **OK**.

4. Valitse vasemmasta ruudusta **Suojaus**.

5. Valitse **Sulautettu suojaus** ja napsauta sitten **Automatic DriveLock Support** -kohdan vieressä olevaa **Ota käyttöön** -painiketta.

   Huomautus Voit poistaa sulautetun suojauksen automaattisen DriveLock-suojaustoiminnon käytöstä valitsemalla **Poista käytöstä**.

6. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Tietokoneen asetukset -apuohjelman salasanojen hallinta

BIOS-määritysten avulla voit määrittää ja vaihtaa käynnistys- ja asetussalasanoja Tietokoneen asetukset -apuohjelmassa. Voit myös hallita erilaisia salasana-asetuksia.

VARO BIOS-määritysten Salasanat-sivulla määrittämäsi salasanat tallentuvat heti, kun napsautat ProtectTools-ikkunan **Käytä**- tai **OK**-painiketta. Varmista, että muistat määrittämäsi salasanan, koska salasana-asetusta ei voi perua ilman edellistä salasanaa.

Käynnistyssalasanalla voit estää kannettavan tietokoneen luvattoman käytön.

Huomautus Kun olet määrittänyt käynnistyssalasanan, Salasanat-sivulla oleva Aseta-painike korvautuu Muuta-painikkeella.

Tietokoneen asetukset -apuohjelman salasanalla voit suojata Tietokoneen asetukset -apuohjelmassa määritetyt kokoonpanoasetukset ja järjestelmän tunnistustiedot. Kun salasana on määritetty, se kysytään aina Tietokoneen asetukset -apuohjelman käynnistyksen yhteydessä. Jos olet määrittänyt asetussalasanan, näkyviin tulee salasanakehote ennen HP ProtectTools -ohjelman BIOS-määritysosan avaamista.

Huomautus Kun olet määrittänyt asetussalasanan, Salasanat-sivulla oleva Aseta-painike korvautuu Muuta-painikkeella.

Käynnistyssalasanan määrittäminen

Määritä käynnistyssalasana seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta ensin **BIOS-määritykset** ja valitse sitten **Suojaus**.
3. Napsauta oikean ruudun **Käynnistyssalasana**-kohdan vieressä olevaa **Aseta**-painiketta.
4. Kirjoita ja vahvista salasana **Anna salasana**- ja **Vahvista salasana** -ruutuihin.
5. Valitse Salasanat-valintaikkunassa **OK**.
6. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Käynnistyssalasanan vaihtaminen

Vaihda käynnistyssalasana seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta ensin **BIOS-määritykset** ja valitse sitten **Suojaus**.

3. Napsauta oikean ruudun **Käynnistyssalasana**-kohdan vieressä olevaa **Muuta**-painiketta.
4. Kirjoita nykyinen salasana **Vanha salasana** -ruutuun.
5. Määritä ja vahvista uusi salasana **Anna uusi salasana** -ruutuun.
6. Valitse **Salasanat**-valintaikkunassa **OK**.
7. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Asetussalasanan määrittäminen

Määritä Tietokoneen asetukset -apuohjelman asetussalasana seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta ensin **BIOS-määritykset** ja valitse sitten **Suojaus**.
3. Napsauta oikean ruudun **Asetussalasana**-kohdan vieressä olevaa **Aseta**-painiketta.
4. Kirjoita ja vahvista salasana **Anna salasana**- ja **Vahvista salasana** -ruutuihin.
5. Valitse **Salasanat**-valintaikkunassa **OK**.
6. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Asetussalasanan vaihtaminen

Vaihda Tietokoneen asetukset -apuohjelman asetussalasana seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta ensin **BIOS-määritykset** ja valitse sitten **Suojaus**.
3. Napsauta oikean ruudun **Asetussalasana**-kohdan vieressä olevaa **Muuta**-painiketta.
4. Kirjoita nykyinen salasana **Vanha salasana** -ruutuun.
5. Kirjoita ja vahvista uusi salasana **Anna uusi salasana**- ja **Vahvista uusi salasana** -ruutuihin.
6. Valitse **Salasanat**-valintaikkunassa **OK**.
7. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Salasana-asetusten määrittäminen

Voit parantaa järjestelmän suojausta määrittämällä salasana-asetuksia BIOS Configuration for HP ProtectTools -ohjelmassa.

Tiukan suojauksen ottaminen käyttöön tai poistaminen käytöstä

VARO Voit estää tietokonetta tulemasta pysyvästi käyttökelvottomaksi kirjoittamalla määrittämäsi asetussalasanan, käynnistyssalasanan tai sirukortin PIN-koodin muistiin ja säilyttämällä ne turvallisessa paikassa erillään tietokoneesta. Tietokoneen lukitusta ei voi avata ilman näitä salasanoja tai PIN-koodia.

Tiukan suojauksen käyttöön ottaminen parantaa käynnistys- ja pääkäyttäjäsalasanojen ja muiden käynnistystodennuksen lomakkeiden suojausta.

Voit ottaa tiukan suojauksen käyttöön tai poistaa se käytöstä seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta ensin **BIOS-määritykset** ja valitse sitten **Suojaus**.
3. Ota käyttöön **Vahva suojaus** -asetus oikean ruudun **Salasana-asetukset**-kohdasta tai poista se käytöstä.

   

   Huomautus Jos haluat poistaa vahvan suojauksen käytöstä, poista **Enable Stringent Security** (Ota vahva suojaus käyttöön) -valintaruudun valinta.

4. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

Windowsin uudelleenkäynnistyksen yhteydessä tapahtuvan käynnistystodennuksen käyttöön ottaminen tai käytöstä poistaminen

Tällä asetuksella voit parantaa suojausta vaatimalla käyttäjiä määrittämään käynnistys-, TPM- tai sirukorttisalasana aina, kun Windows käynnistetään uudelleen.

Voit ottaa käyttöön Windowsin uudelleenkäynnistyksen yhteydessä tapahtuvan käynnistystodennuksen tai poistaa sen käytöstä seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta ensin **BIOS-määritykset** ja valitse sitten **Suojaus**.
3. Ota käyttöön **Vaadi salasana uudelleenkäynnistyksessä** -asetus oikean ruudun **Salasana-asetukset**-kohdasta tai poista se käytöstä.
4. Tallenna muutokset valitsemalla HP ProtectTools -ikkunasta **Käytä** ja valitsemalla sitten **OK**.

6 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools -ohjelman suojausominaisuudet suojaavat tietokonetta luvattomalta käytöltä. Suojausominaisuuksia ovat esimerkiksi seuraavat ominaisuudet:

- Windowsiin kirjautuminen muun kuin salasanan avulla, esimerkiksi sirukortin tai biometrisen tunnisteen avulla. Lisätietoja on tämän luvun kohdassa Kirjautumistapojen määrittäminen.
- Kertakirjaustoiminto, joka muistaa automaattisesti Web-sivustojen, sovellusten ja suojattujen verkkoresurssien käyttöoikeustiedot.
- Valinnaisten suojauslaitteiden (kuten sirukorttien ja biometristen tunnistimien) tuki.
- Muiden tietoturva-asetusten tuki. Tietokoneen lukituksen avaamiseen saatetaan esimerkiksi määrittää pakollinen tunnistautuminen valinnaisella tietoturvalaitteella.

Asetusten määrittäminen

Kirjautuminen Credential Manager -ohjelmaan

Credential Manager -ohjelmaan voidaan kirjautua seuraavilla tavoilla sen mukaan, mitkä tavat on otettu käyttöön:

- Ohjattu Credential Manager -kirjautuminen (suositeltava tapa)
- Ilmoitusalueella oleva HP ProtectTools Security Manager -kuvake
- HP ProtectTools Security Manager

Huomautus Kun kirjaudut Credential Manager -ohjelmaan käyttäen ohjelman kirjautumiskehotetta Windows-kirjautumisnäytössä, järjestelmä kirjaa sinut samalla sisään myös Windows-käyttöjärjestelmään.

Kun avaat Credential Manager -ohjelman ensimmäisen kerran, kirjaudu sisään Windows-salasanallasi. Tällöin järjestelmä luo sinulle automaattisesti Credential Manager -tilin, jossa käytetään Windows-tunnuksiasi.

Kun olet kirjautunut Credential Manager -ohjelmaan, voit ottaa käyttöön muita kirjautumistapoja, kuten sormenjälkitunnistuksen tai sirukortin. Lisätietoja on tämän luvun kohdassa Kirjautumistapojen määrittäminen.

Kun kirjaudut ohjelmaan seuraavan kerran, voit valita kirjautumiskäytännön ja käyttää mitä tahansa käytössä olevien kirjautumistapojen yhdistelmää.

Ohjatun Credential Manager -kirjautumisen käyttäminen

Kirjautuminen Credential Manager -ohjelmaan ohjattua toimintoa käyttämällä

1. Avaa Ohjattu Credential Manager -kirjautuminen jollakin seuraavista tavoista:
   - Windows-kirjautumisnäytön avulla
   - kaksoisnapsauttamalla ilmoitusalueen **HP ProtectTools Security Manager** -kuvaketta
   - napsauttamalla ProtectTools Security Manager -ohjelman Credential Manager -sivun oikeassa ylälaidassa olevaa **Kirjaudu**-linkkiä.
2. Valitse **Seuraava**.
3. Kirjoita käyttäjänimesi **User name** (Käyttäjänimi) -ruutuun.
4. Kirjoita salasanasi **Password** (Salasana) -ruutuun ja valitse sitten **Seuraava**.
5. Valitse **Valmis**.

Kirjautuminen ensimmäisen kerran

Kirjaudu ensin Windows-käyttöjärjestelmään järjestelmänvalvojana. Älä kuitenkaan kirjaudu Credential Manager -ohjelmaan.

1. Avaa HP ProtectTools Security Manager kaksoisnapsauttamalla ilmoitusalueen HP ProtectTools Security Manager -kuvaketta. HP ProtectTools Security Manager -ikkuna avautuu.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten oikean ruudun oikeasta yläkulmasta **Kirjaudu**. Ohjattu Credential Manager -kirjautuminen tulee näyttöön.
3. Kirjoita Windows-salasanasi **Salasana**-ruutuun ja valitse sitten **Seuraava**.

Kirjautumistapojen määrittäminen

Voit ottaa kirjautumistapoja käyttöön Omat tiedot -sivulla. Kun kirjautumistavat on määritetty, voit käyttää niitä kirjautuessasi Credential Manager -ohjelmaan.

Sormenjälkien rekisteröiminen

Sormenjälkitunnistinta käyttämällä voit kirjautua Windows-käyttöjärjestelmään rekisteröidyn sormenjäljen avulla ilman Windows-salasanaa.

Sormenjälkitunnistimen asetusten määrittäminen

1. Kun olet kirjautunut Credential Manager -ohjelmaan, pyyhkäise sormella sormenjälkitunnistimien yli. Ohjattu Credential Manager -rekisteröinti tulee näyttöön.
2. Valitse **Seuraava**.

   Huomautus Credential Manager -ohjelmassa on oletusarvon mukaan rekisteröitävä *vähintään* kahden sormen jälki.

   Ensimmäisen sormenjäljen rekisteröinnissä käytetään oletusarvoisesti oikean käden etusormea. Voit vaihtaa tämän oletusasetuksen napsauttamalla sen sormen kuvaa, jonka haluat rekisteröidä ensiksi. Tämä sormi voi olla vasemman tai oikean käden sormi. Kun napsautat sormen kuvaa, sen ympärille ilmestyy kehys merkiksi siitä, että se on valittu.
3. Vedä sormeasi hitaasti alaspäin sormenjälkitunnistimen päällä. Noudata ohjatun toiminnon ohjeita ja jatka saman sormen vetämistä sormenjälkitunnistimen yli, kunnes näytössä oleva sormi muuttuu vihreäksi.

   Huomautus Sormenjäljen rekisteröintiä varten sormea on vedettävä useita kertoja tunnistimen päällä.

   Jos joudut aloittamaan sormenjäljen rekisteröimisen uudelleen, napsauta hiiren kakkospainikkeella näytössä olevaa korostettua sormen kuvaa ja valitse **Poista** tai **Poista kaikki**.
4. Rekisteröi toinen sormenjälki noudattamalla ohjatun toiminnon ohjeita.

   Huomautus Jos valitset **Valmis** ennen kuin vähintään kahden sormen jälki on rekisteröity, näyttöön tulee virheilmoitus. Jatka valitsemalla **OK**.
5. Kun olet rekisteröinyt vähintään kahden sormen sormenjäljet, valitse **Seuraava**.

6. Jos haluat kirjautua Windowsiin käyttämällä sormenjälkitunnistusta, varmista, että **Yes, I want to use Credential Manager to logon to Windows** (Kyllä, haluan kirjautua Windowsiin Credential Manager -ohjelmalla) -valintaruutu on valittu. Valitse **Valmis**.

7. Jos haluat määrittää toisen Windows-käyttäjän sormenjälkiasetukset, kirjaudu Windowsiin kyseisenä käyttäjänä ja toista vaiheet 1–6.

Windowsiin kirjautuminen rekisteröidyn sormenjäljen avulla

1. Kun olet rekisteröinyt sormenjälkesi, käynnistä Windows uudestaan.

2. Voit kirjautua Windowsiin vetämällä jonkin rekisteröidyistä sormista tunnistimen yli.

Java- tai sirukortin, poletin tai virtuaalisen poletin määrittäminen

Huomautus Toimenpide edellyttää, että käytettävissä on määritetty sirukortin lukija. Jos tietokoneeseen ei ole asennettu lukijaa, voit määrittää virtuaalisen poletin kohdassa Virtuaalisen poletin luominen olevien ohjeiden mukaan

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.

2. Valitse vasemmasta ruudusta **Credential Manager**.

3. Valitse oikeasta ruudusta **Register Smart Card or Token** (Rekisteröidä sirukortin tai tunnuspoletin). Ohjattu Credential Manager -rekisteröinti tulee näyttöön.

4. Valitse **Seuraava**.

5. Napsauta sitä kirjautumistapaa, jonka haluat ottaa käyttöön. Valitse sitten **Seuraava**.

6. Suorita rekisteröinti loppuun näyttöön tulevien ohjeiden mukaan.

USB eToken -poletin määrittäminen

1. Varmista, että järjestelmään on asennettu USB eToken -ohjaimet.

Huomautus Lisätietoja on USB eToken -käyttöoppaassa.

2. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.

3. Valitse vasemmasta ruudusta **Credential Manager**.

4. Valitse oikeasta ruudusta **Register Smart Card or Token** (Rekisteröidä sirukortin tai tunnuspoletin). Ohjattu Credential Manager -rekisteröinti tulee näyttöön.

5. Valitse **Seuraava**.

6. Valitse **Device Type** (Laitetyyppi) -kohdasta **USB eToken** (USB eToken -poletti) ja valitse sitten **Seuraava**.

7. Suorita rekisteröinti loppuun näyttöön tulevien ohjeiden mukaan.

Muiden kirjautumistapojen määrittäminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager**.
3. Valitse oikeasta ruudussa **Register Credentials** (Rekisteröi kirjautumistavat). Ohjattu Credential Manager -rekisteröinti tulee näyttöön.
4. Valitse **Seuraava**.
5. Napsauta sitä kirjautumistapaa, jonka haluat ottaa käyttöön. Valitse sitten **Seuraava**.
6. Suorita rekisteröinti loppuun näyttöön tulevien ohjeiden mukaan.

Yleiset toiminnot

Kaikki käyttäjät voivat käyttää Credential Manager -ohjelman Omat tiedot -sivua. Omat tiedot -sivulla voit suorittaa seuraavat tehtävät:

- Virtuaalisen poletin luominen
- Windows-salasanan muuttaminen
- Poletin PIN-koodin hallitseminen
- Omien tietojen hallinta
- Tietokoneen lukitseminen

Huomautus Tämä vaihtoehto on käytettävissä vain, jos käytössä on Credential Manager -ohjelman perinteinen kirjautumiskehote. Lisätietoja on kohdassa Esimerkki 1: Advanced Settings (Lisäasetukset) -sivulla määritetään Credential Manager -ohjelma hoitamaan myös Windows-kirjautuminen.

Virtuaalisen poletin luominen

Virtuaalinen poletti toimii lähes samalla tavoin kuin sirukortti tai USB-poletti. Poletti tallennetaan tietokoneen kiintolevylle tai Windows-käyttöjärjestelmän rekisteriin. Kun kirjaudut virtuaalista polettia käyttämällä, sinun on annettava PIN-koodi.

Uuden virtuaalisen poletin luominen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager**.
3. Valitse oikeasta ruudussa **Virtual Token** (Virtuaalinen poletti). Ohjattu Credential Manager -rekisteröinti tulee näyttöön.

   Huomautus Jos Virtual Token (Virtuaalinen poletti) -asetus ei ole käytettävissä, noudata kohdassa Muiden kirjautumistapojen määrittäminen olevia ohjeita.
4. Valitse **Seuraava**.
5. Valitse **Virtual Token** (Virtuaalinen poletti) ja valitse sitten **Seuraava**.

6. Määritä virtuaalisen poletin tiedostonimi ja sijainti tai etsi tiedosto valitsemalla **Selaa**. Valitse sitten **Seuraava**.
7. Määritä ja vahvista pääkäyttäjän ja käyttäjän PIN-koodit.
8. Valitse **Valmis**.

Windows-salasanan muuttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager**.
3. Valitse oikeasta ruudussa **Change Windows Password** (Muuttaa Windows-salasanan).
4. Kirjoita vanha salasana **Vanha salasana** -ruutuun.
5. Kirjoita uusi salasana **Uusi salasana**- ja **Vahvista uusi salasana** -ruutuihin.
6. Valitse **Valmis**.

Poletin PIN-koodin muuttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager**.
3. Valitse oikeasta ruudusta **Change Token PIN** (Muuta poletin PIN-koodi).
4. Valitse se poletti, jonka PIN-koodin haluat muuttaa, ja valitse sitten **Seuraava**.
5. Suorita toiminto loppuun näyttöön tulevien ohjeiden mukaan.

Omien tietojen hallinta

Omien tietojen varmuuskopiointi

On suositeltavaa ottaa omista tiedoista varmuuskopio Credential Manager -ohjelmassa, jotta tiedot eivät katoa ja jotta niitä ei poistettaisi vahingossa.

Varmuuskopion tekeminen omista tiedoista

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager**.
3. Valitse oikeasta ruudusta **Backup Identity** (Varmuuskopioda omat tiedostot).
4. Valitse kopioitavat tiedot ja valitse sitten **Seuraava**.
5. Valitse Device Type (Laitetyyppi) -sivulla laite, johon haluat tallentaa varmuuskopion, ja valitse sitten **Seuraava**.

   Huomautus Tarvitset valitun laitteen salasanan tai PIN-koodin.

6. Suorita toiminto loppuun näyttöön tulevien ohjeiden mukaan. Valitse sitten **Valmis**.

Omien tietojen palauttaminen

Omien tietojen palauttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager**.
3. Valitse oikeasta ruudusta **Restore Identity** (Palauttaa omat tiedot).
4. Valitse Device Type (Laitetyyppi) -sivulla laite, johon varmuuskopio on tallennettu, ja valitse sitten **Seuraava**.

   Huomautus Tarvitset valitun laitteen salasanan tai PIN-koodin.

5. Suorita toiminto loppuun näyttöön tulevien ohjeiden mukaan. Valitse sitten **Valmis**.
6. Valitse vahvistusikkunassa **Kyllä**.

Omien tietojen poistaminen järjestelmästä

Huomautus Tietojen poistaminen ei vaikuta Windows-käyttäjätiliisi.

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager**.
3. Valitse oikeasta ruudusta **Clear Identity for this Account** (Poistaa tilin omat tiedot).
4. Valitse vahvistusikkunassa **Kyllä**. Järjestelmä kirjaa käyttäjän ulos ja poistaa tiedot.

Tietokoneen lukitseminen

Tämä toiminto on käytettävissä, jos kirjaudut Windowsiin Credential Manager -ohjelmaa käyttämällä. Kun poistut työpöytäsi äärestä, voit suojata tietokoneen lukitustoiminnolla. Tällöin asiattomat käyttäjät eivät pääse käyttämään tietokonettasi. Sinun itsesi lisäksi vain tietokoneen järjestelmänvalvojien ryhmään kuuluvat käyttäjät voivat avata tietokoneen lukituksen.

Huomautus Tämä vaihtoehto on käytettävissä vain, jos käytössä on Credential Manager -ohjelman perinteinen kirjautumiskehote. Lisätietoja on kohdassa Esimerkki 1: Advanced Settings (Lisäasetukset) -sivulla määritetään Credential Manager -ohjelma hoitamaan myös Windows-kirjautuminen.

Voit vahvistaa suojaa määrittämällä sirukortin, biometrisen tunnisteen tai poletin käytön pakolliseksi tietokoneen lukitusta avattaessa. Lisätietoja on tämän luvun kohdassa Credential Manager -ohjelman asetusten määrittäminen.

Tietokoneen lukitseminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager**.
3. Valitse oikeasta ruudusta **Lock Workstation** (Lukita työaseman). Windows-kirjautumisnäyttö avautuu. Voit avata tietokoneen lukituksen käyttämällä joko ohjattua Credential Manager -kirjautumistoimintoa tai Windows-salasanaa.

Windows-kirjautumisen käyttäminen

Voit käyttää Credential Manager -ohjelmaa Windows-käyttöjärjestelmään kirjautumiseen sekä paikallisessa tietokoneessa että verkkotoimialueessa. Kun kirjaudut Credential Manager -ohjelmaan ensimmäisen kerran, järjestelmä lisää paikallisen Windows-käyttäjätilisi automaattisesti Windows-kirjautumispalvelun käyttäjätiliksi.

Kirjautuminen Windowsiin Credential Manager -ohjelman avulla

Voit käyttää Credential Manager -ohjelmaa Windows-käyttöjärjestelmään kirjautumiseen sekä paikallisessa tietokoneessa että verkkotoimialueessa.

1. Jos olet rekisteröinyt sormenjälkesi Windowsiin kirjautumista varten, kirjaudu järjestelmään lukemalla sormi sormenjälkitunnistimella.
2. Jos et ole rekisteröinyt sormenjälkeäsi Windowsiin kirjautumista varten, napsauta näytön vasemmassa yläkulmassa sormenjälkikuvakkeen vieressä olevaa näppäimistökuvaketta. Ohjattu Credential Manager -kirjautuminen tulee näyttöön.
3. Napsauta **User name** (Käyttäjänimi) -nuolta ja valitse sitten nimesi.
4. Kirjoita salasanasi **Salasana**-ruutuun ja valitse sitten **Seuraava**.
5. Valitse **More > Wizard Options** (Lisää > Ohjatun toiminnon asetukset).
   a. Jos haluat määrittää käyttäjänimen seuraavalla kirjautumiskerralla käytettäväksi oletukseksi, valitse **Use last user name on next logon** (Käytä edellistä nimeä kirjautuessasi seuraavan kerran) -valintaruutu.
   b. Jos haluat määrittää valitsemasi kirjautumistavan oletusasetukseksi, valitse **Use last policy on next logon** (Käytä edellistä kirjautumistapaa, kun kirjaudut seuraavan kerran) -valintaruutu.
6. Noudata näyttöön tulevia ohjeita. Jos kirjautumistietosi ovat oikein, järjestelmä kirjaa sinut sisään Windows-käyttöjärjestelmään ja Credential Manager -ohjelmaan.

Tilin lisääminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikeasta ruudusta **Microsoft Network Logon** (Microsoft Network -kirjautuminen) -kohdasta **Add a Network Account** (Lisää verkkokäyttäjätili). Ohjattu verkkokäyttäjätilin lisääminen käynnistyy.
4. Kirjoita uuden käyttäjätilin käyttäjänimi **User name** (Käyttäjänimi) -ruutuun tai etsi käyttäjänimi valitsemalla **Selaa**.
5. Valitse toimialue käytettävissä olevien toimialueiden luettelosta.
6. Kirjoita salasana ja vahvista se.

Huomautus Jos haluat, että Credential Manager tarkistaa tämän tilin, varmista, että **Validate network account when Next or Finish button clicked** (Tarkista verkkokäyttäjätili, kun Seuraava- tai Valmis-painiketta napsautetaan) -valintaruutu on valittu.

7. Valitse **Valmis**.

Tilin poistaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Windows Logon** (Windowsiin kirjautuminen) -kohdasta **Manage Network Accounts** (Verkkokäyttäjätilien hallinta). **Manage Network Accounts** (Verkkokäyttäjätilien hallinta) -valintaikkuna avautuu.
4. Napsauta poistettavaa käyttäjätiliä ja valitse **Poista**.
5. Valitse vahvistusikkunassa **Kyllä**.
6. Valitse **OK**.

Kertakirjaustoiminnon käyttäminen

Credential Manager -ohjelmassa on kertakirjaustoiminto, joka tallentaa eri Internet- ja Windows-ohjelmissa käytettävät käyttäjänimet ja salasanat ja antaa ne sitten automaattisesti, kun käyttäjä avaa rekisteröidyn ohjelman.

Huomautus Tietoturva ja omien tietojen suojaus ovat kertakirjaustoiminnon keskeisiä ominaisuuksia. Kaikki käyttäjätunnukset ja salasanat säilytetään salatussa muodossa ja niitä voi muokata vain Credential Manager -ohjelmaan kirjautumisen jälkeen.

Huomautus Suojattuun sivustoon tai ohjelmaan kirjauduttaessa tarvittava käyttöoikeuden vahvistaminen sirukortilla, sormenjäljen tunnistuksella tai poletilla voidaan määrittää pakolliseksi myös kertakirjaustoimintoa käytettäessä. Tämä ominaisuus on erityisen hyödyllinen silloin, kun kirjaudutaan ohjelmiin tai Web-sivustoihin, jotka sisältävät henkilökohtaisia tietoja, kuten pankkitilien numeroita. Lisätietoja on tämän luvun kohdassa Credential Manager -ohjelman asetusten määrittäminen.

Uuden sovelluksen määrittäminen

Kun käynnistät jonkin sovelluksen ollessasi kirjautuneena Credential Manager -ohjelmaan, ohjelma kehottaa sinua rekisteröimään sen. Voit rekisteröidä sovelluksen myös manuaalisesti.

Automaattisen rekisteröinnin käyttäminen

1. Avaa sovellus, joka vaatii käyttäjätunnuksen ja salasanan.
2. Napsauta Credential Manager -ohjelman kertakirjauskuvaketta ohjelmassa tai Web-sivuston salasanaikkunassa.
3. Kirjoita ohjelman tai Web-sivuston salasana ja valitse sitten **OK**. Credential Manager -ohjelman kertakirjaustoiminnon valintaikkuna tulee näyttöön.

4. Valitse **More** (Lisää) ja valitse jokin seuraavista vaihtoehdoista:

   - Do not use SSO for this site or application (Älä ehdota kertakirjaustoiminnon käyttämistä tätä sivustoa tai sovellusta avattaessa)
   - Prompt to select account for this application (Valitse tili tälle sovellukselle erikseen)
   - Fill in credentials but do not submit (Täytä tiedot, mutta älä lähetä niitä)
   - Authenticate user before submitting credentials (Tarkista käyttöoikeus ennen tietojen lähettämistä)
   - Show SSO shortcut for this application (Näytä tämän sovelluksen kertakirjaustoiminnon kuvake).

5. Lopeta rekisteröinti valitsemalla **Kyllä**.

Manuaalisen rekisteröinnin käyttäminen (vedä ja pudota -toiminto)

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Single Sign On** (Kertakirjaustoiminto) -kohdasta **Register new Application** (Rekisteröi uusi sovellus). Kertakirjaustoiminnon ohjattu käyttöönotto käynnistyy.
4. Käynnistä rekisteröitävä sovellus ja odota, kunnes sovellus pyytää salasanaa.
5. Valitse kertakirjaustoiminnon ohjatun käyttöönoton Drag and Drop Registration (Vedä ja pudota -rekisteröinti) -sivulta toiminto, jonka haluat automatisoida.

   Huomautus Useimmissa tapauksissa automatisoitava toiminto on **Logon simple dialog** (Yksinkertainen kirjautumisikkuna).

6. Napsauta ohjatun toiminnon sivulla olevaa kuvaketta ja vedä se sovelluksen salasanaruudun päälle. Pudota kuvake, kun salasanaruudun alue näkyy valittuna.
7. Kirjoita sovelluksen nimi ja kuvaus ohjatun kertakirjaustoiminnon käyttöönoton Application Information (Sovelluksen tiedot) -sivulle.
8. Valitse **Valmis**.
9. Kirjoita sovelluksen ruutuun kirjautumistiedot, kuten käyttäjänimi ja salasana.
10. Vahvista kirjautumistietojen nimi tai napsauta nimeä hiiren kakkospainikkeella ja muokkaa sitä Credential Manager Single Sign On (Crential Manager -ohjelman kertakirjaustoiminto) -valintaikkunassa. Valitse **Kyllä**.
11. Valitse **More** (Lisää) ja valitse jokin seuraavista vaihtoehdoista:

    - Do not use SSO for this site or application (Älä ehdota kertakirjaustoiminnon käyttämistä tätä sivustoa tai sovellusta avattaessa)
    - Prompt to select account for this application (Valitse tili tälle sovellukselle erikseen)
    - Fill in credentials but do not submit (Täytä tiedot, mutta älä lähetä niitä)

- Authenticate user before submitting credentials (Tarkista käyttöoikeus ennen tietojen lähettämistä)
- Show SSO shortcut for this application (Näytä tämän sovelluksen kertakirjaustoiminnon kuvake).

12. Lopeta rekisteröinti valitsemalla **Kyllä**.

Sovellusten ja kirjautumistietojen hallinta

Sovelluksen ominaisuuksien muokkaaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Single Sign On** (Kertakirjaustoiminto) -kohdassa **Manage Applications and Credentials** (Sovellusten ja kirjautumistietojen hallinta).
4. Napsauta sovellusta, jota haluat muokata, ja valitse **Ominaisuudet**.
5. Jos haluat muokata sovelluksen nimeä ja kuvausta, valitse **Yleistä**-välilehti. Voit muuttaa asetuksia valitsemalla valintaruudun tai poistamalla valinnan.
6. Jos haluat katsoa tai muokata kertakirjaustoiminnon sovelluskomentosarjaa, valitse **Script** (Komentosarja) -välilehti.
7. Tallenna muutokset valitsemalla **OK**.

Sovelluksen poistaminen kertakirjaustoiminnosta

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Single Sign On** (Kertakirjaustoiminto) -kohdassa **Manage Applications and Credentials** (Sovellusten ja kirjautumistietojen hallinta).
4. Napsauta sovellusta, jonka haluat poistaa toiminnosta, ja valitse **Remove** (Poista).
5. Valitse vahvistusikkunassa **Kyllä**.
6. Valitse **OK**.

Sovellustietojen vieminen

Voit luoda kertakirjaustoiminnon sovelluskomentosarjoista varmuuskopiot viemällä tiedot toiseen tiedostomuotoon. Kertakirjaustoiminnon tiedot voidaan tarvittaessa palauttaa vientitiedostosta. Tiedosto täydentää omien tietojen varmuuskopiotiedostoa, joka sisältää vain kirjautumistietoja.

Sovellustietojen vieminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).

3. Valitse oikean ruudun **Single Sign On** (Kertakirjaustoiminto) -kohdassa **Manage Applications and Credentials** (Sovellusten ja kirjautumistietojen hallinta).
4. Napsauta sovellusta, jonka tiedot haluat viedä. Valitse sitten **More > Applications > Export Application** (Lisää > Sovellukset > Vie komentosarja).
5. Suorita toiminto loppuun näyttöön tulevien ohjeiden mukaan.
6. Valitse **OK**.

Sovellustietojen tuominen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Single Sign On** (Kertakirjaustoiminto) -kohdassa **Manage Applications and Credentials** (Sovellusten ja kirjautumistietojen hallinta).
4. Napsauta sovellusta, jonka tiedot haluat tuoda. Valitse sitten **More > Applications > Import Script** (Lisää > Sovellukset > Tuo komentosarja).
5. Suorita toiminto loppuun näyttöön tulevien ohjeiden mukaan.
6. Valitse **OK**.

Kirjautumistapojen muokkaaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Single Sign On** (Kertakirjaustoiminto) -kohdassa **Manage Applications and Credentials** (Sovellusten ja kirjautumistietojen hallinta).
4. Napsauta sovellusta, jota haluat muokata, ja valitse **More** (Lisää).
5. Valitse jokin seuraavista vaihtoehdoista:
   - Applications (Sovellukset)
     - Add New (Lisää uusi)
     - Remove (Poista)
     - Ominaisuudet
     - Import Script (Tuo komentosarja)
     - Export Script (Vie komentosarja)
   - Credentials (Kirjautumistavat)
     - Create New (Luo uusi)
   - View Password (Näytä salasana).

Huomautus Ennen salasanan näyttämistä käyttöoikeutesi on tarkistettava.

6. Noudata näyttöön tulevia ohjeita.
7. Tallenna muutokset valitsemalla **OK**.

Sovelluksen suojauksen käyttäminen

Tämän toiminnon avulla voit määrittää sovellusten käyttöoikeudet. Voit rajoittaa käyttöoikeuksia seuraavien perusteiden mukaan:

- käyttäjän luokka
- käytön ajankohta
- käyttäjän toimettomuus.

Sovelluksen käyttöoikeuden rajoittaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Application Protection** (Sovelluksen suojaus) -kohdasta **Manage Protected Applications** (Suojattujen sovellusten hallinta). Application Protection Service (Sovellusten suojauspalvelu) -valintaikkuna avautuu.
4. Valitse käyttäjäluokka, jonka käyttöoikeuksia haluat muokata.

Huomautus Jos luokan asetus ei ole Everyone (Kaikki), sinun on ehkä ohitettava Everyone (Kaikki) -luokan asetukset valitsemalla **Override default settings** (Korvaa oletusasetukset) -asetus.

5. Valitse **Add** (Lisää). Ohjattu ohjelman lisääminen käynnistyy.
6. Napsauta suojattavaa sovellusta ja valitse sitten **OK**. Valitun sovelluksen Ominaisuudet-valintaikkuna avautuu.
7. Napsauta **Yleistä**-välilehteä. Valitse jokin seuraavista asetuksista:
   - Disabled (Cannot be used) (Ei käytössä [ei voi käytttää])
   - Enabled (Can be used without restrictions) (Käytössä [rajoitukseton käyttö])
   - Restricted (Usage depends on settings) (Rajoitettu [käyttö asetusten mukaan]).
8. Jos otat käyttöön rajoitetut käyttöoikeudet, käytettävissä ovat seuraavat asetukset:
   a. Jos haluat rajoittaa käyttöoikeuksia kellonajan, päivän tai päivämäärän mukaan, napsauta **Schedule** (Ajoitus) -välilehteä ja määritä asetukset.
   b. Jos haluat rajoittaa käyttöoikeuksia käyttämättömyyden keston mukaan, napsauta **Lisäasetukset**-välilehteä ja valitse käyttämättömyyden kesto.
9. Sulje sovelluksen Ominaisuudet-valintaikkuna valitsemalla **OK**.
10. Valitse **OK**.

Sovelluksen suojauksen poistaminen käytöstä

Poista sovelluksen käyttöoikeusrajoitukset käytöstä seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Application Protection** (Sovelluksen suojaus) -kohdasta **Manage Protected Applications** (Suojattujen sovellusten hallinta). Application Protection Service (Sovellusten suojauspalvelu) -valintaikkuna avautuu.
4. Valitse käyttäjäluokka, jonka käyttöoikeuksia haluat muokata.

   Huomautus Jos luokan asetus ei ole Everyone (Kaikki), sinun on ehkä ohitettava Everyone (Kaikki) -luokan asetukset valitsemalla **Override default settings** (Korvaa oletusasetukset) -asetus.

5. Napsauta sovellusta, jonka haluat poistaa toiminnosta, ja valitse **Remove** (Poista).
6. Valitse **OK**.

Suojatun sovelluksen käyttöoikeusrajoitusten muuttaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Services and Applications** (Palvelut ja sovellukset).
3. Valitse oikean ruudun **Application Protection** (Sovelluksen suojaus) -kohdasta **Manage Protected Applications** (Suojattujen sovellusten hallinta). Application Protection Service (Sovellusten suojauspalvelu) -valintaikkuna avautuu.
4. Valitse käyttäjäluokka, jonka käyttöoikeuksia haluat muokata.

   Huomautus Jos luokan asetus ei ole Everyone (Kaikki), sinun on ehkä ohitettava Everyone (Kaikki) -luokan asetukset valitsemalla **Override default settings** (Korvaa oletusasetukset) -asetus.

5. Napsauta muokattavaa sovellusta ja valitse sitten **Ominaisuudet**. Valitun sovelluksen Ominaisuudet-valintaikkuna avautuu.
6. Napsauta **Yleistä**-välilehteä. Valitse jokin seuraavista asetuksista:
   - Disabled (Cannot be used) (Ei käytössä [ei voi käytttää])
   - Enabled (Can be used without restrictions) (Käytössä [rajoitukseton käyttö])
   - Restricted (Usage depends on settings) (Rajoitettu [käyttö asetusten mukaan]).
7. Jos otat käyttöön Rajoitettu-asetuksen, käytettävissä ovat seuraavat asetukset:
   a. Jos haluat rajoittaa käyttöoikeuksia kellonajan, päivän tai päivämäärän mukaan, napsauta **Schedule** (Ajoitus) -välilehteä ja määritä asetukset.
   b. Jos haluat rajoittaa käyttöoikeuksia käyttämättömyyden keston mukaan, napsauta **Lisäasetukset**-välilehteä ja valitse käyttämättömyyden kesto.

8. Sulje sovelluksen Ominaisuudet-valintaikkuna valitsemalla **OK**.
9. Valitse **OK**.

Lisätoiminnot (vain järjestelmänvalvojille)

Vain järjestelmänvalvojat voivat käyttää Credential Manager -ohjelman Authentication and Credentials (Käyttöoikeuksien tarkistus ja kirjautumistavat)- ja Advanced Settings (Lisäasetukset) -sivuja. Näillä sivuilla voit suorittaa seuraavat tehtävät:

- Käyttäjien ja järjestelmänvalvojien kirjautumistapojen määrittäminen
- Mukautettujen kirjautumisvaatimusten määrittäminen
- Kirjautumistapojen asetusten määrittäminen
- Credential Manager -ohjelman asetusten määrittäminen

Käyttäjien ja järjestelmänvalvojien kirjautumistapojen määrittäminen

Authentication and Credentials (Käyttöoikeuksien tarkistus ja kirjautumistavat) -sivulla voit määrittää, mitä kirjautumistapaa tai tapojen yhdistelmää käyttäjien tai järjestelmänvalvojien on käytettävä.

Käyttäjien ja järjestelmänvalvojien kirjautumistapojen määrittäminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja sitten **Authentication and Credentials** (Käyttöoikeuksien tarkistus ja kirjautumistavat).
3. Valitse oikeassa ruudussa **Authentication** (Käyttöoikeuksien tarkistus) -välilehti.
4. Valitse käyttäjäluokkaluettelosta **Users** (Käyttäjät) tai **Administrators** (Järjestelmänvalvojat).
5. Valitse luettelosta kirjautumistapa tai tapojen yhdistelmä.
6. Valitse **Käytä** ja tallenna sitten muutokset valitsemalla **OK**.

Mukautettujen kirjautumisvaatimusten määrittäminen

Jos Authentication and Credentials (Käyttöoikeuksien tarkistus ja kirjautumistavat) -sivulla ei ole haluamaasi käyttöoikeuden tarkistustapojen yhdistelmää, voit määrittää oman yhdistelmän.

Mukautettujen vaatimusten määrittäminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja sitten **Authentication and Credentials** (Käyttöoikeuksien tarkistus ja kirjautumistavat).
3. Valitse oikeassa ruudussa **Authentication** (Käyttöoikeuksien tarkistus) -välilehti.
4. Valitse käyttäjäluokkaluettelosta **Users** (Käyttäjät) tai **Administrators** (Järjestelmänvalvojat).
5. Valitse käyttöoikeuden tarkistustapojen luettelosta **Custom** (Mukautettu).
6. Valitse **Configure** (Määritä).
7. Valitse haluamasi käyttöoikeuden tarkistustavat.

8. Valitse kirjautumistapojen yhdistelmä valitsemalla jompikumpi seuraavista:

   - Valitse yhdistämistavaksi AND

     (Käyttäjien on kirjauduttava kaikkia valittuja kirjautumistapoja käyttäen.)

   - Valitse yhdistämistavaksi OR, jo haluat, että käyttöoikeuden tarkistamistapa valitaan vähintään kahdesta käyttöoikeuden tarkistamistavasta

     (Käyttäjät voivat valita, mitä käytettävissä olevaa kirjautumistapaa he käyttävät.)

9. Valitse **OK**.

10. Valitse **Käytä** ja tallenna sitten muutokset valitsemalla **OK**.

Kirjautumistapojen asetusten määrittäminen

Voit katsoa käytettävissä olevien kirjautumistapojen luetteloa ja muokata asetuksia Authentication and Credentials (Käyttöoikeuksien tarkistus ja kirjautumistavat) -sivun Credentials (Kirjautumistavat) välilehdessä.

Kirjautumistapojen asetusten määrittäminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.

2. Valitse vasemmasta ruudusta **Credential Manager** ja sitten **Authentication and Credentials** (Käyttöoikeuksien tarkistus ja kirjautumistavat).

3. Valitse oikeassa ruudussa **Credentials** (Kirjautumistavat) -välilehti.

4. Napsauta kirjautumistapaa, jota haluat muokata.

   - Voit rekisteröidä kirjautumistavan valitsemalla **Rekisteröi** ja noudattamalla sitten näyttöön tulevia ohjeita.

   - Voit poistaa kirjautumistavan valitsemalla **Clear** (Tyhjennä) ja valitsemalla sitten vahvistusikkunassa **Kyllä**.

   - Voit muokata kirjautumistapojen ominaisuuksia valitsemalla **Ominaisuudet** ja noudattamalla sitten näyttöön tulevia ohjeita.

5. Valitse **Käytä** ja valitse sitten **OK**.

Credential Manager -ohjelman asetusten määrittäminen

Asetukset-sivulla voit tarkastella ja muokata asetuksia seuraavia välilehtiä käyttämällä:

- Yleistä: Voit muokata perusasetuksia.

- Single Sign On (Kertakirjaustoiminto): Voit muokata nykyisen käyttäjän kertakirjausasetuksia, kuten kirjautumisnäyttöjen käsittelyä, automaattista kirjautumista rekisteröityihin kirjautumisikkunoihin sekä salasanan näyttötapaa.

- Services and Applications (Palvelut ja sovellukset): Voit katsoa käytettävissä olevia palveluja ja muokata palvelujen asetuksia.

- Suojaus: Voit valita sormenjälkitunnistimen ohjelmiston ja säätää tunnistimen suojaustasoa.
- Smart Cards and Tokens (Sirukortit ja poletit): Voit katsoa ja muokata kaikkien käytettävissä olevien sirukorttien ja polettien ominaisuuksia.

Credential Manager -ohjelman asetusten muokkaaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Asetukset**.
3. Valitse oikeassa ruudussa se välilehti, jolla olevia asetuksia haluat muokata.
4. Muokkaa asetuksia näyttöön tulevien ohjeiden mukaan.
5. Valitse **Käytä** ja tallenna sitten muutokset valitsemalla **OK**.

Esimerkki 1: Advanced Settings (Lisäasetukset) -sivulla määritetään Credential Manager -ohjelma hoitamaan myös Windows-kirjautuminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Asetukset**.
3. Valitse oikeassa ruudussa **Yleistä**-välilehti.
4. Valitse **Select the way users log on to Windows (requires restart)** (Valitse käyttäjien Windows-kirjautumistapa [edellyttää uudelleenkäynnistystä]) -kohdasta **Use Credential Manager with classic logon prompt** (Käytä Credential Manager -ohjelmaa ja perinteistä kirjautumiskehotetta) -valintaruutu.
5. Valitse **Käytä** ja tallenna sitten muutokset valitsemalla **OK**.
6. Käynnistä tietokone uudelleen.

Huomautus Kun valitset **Use Credential Manager with classic logon prompt** (Käytä Credential Manager -ohjelmaa ja perinteistä kirjautumiskehotetta) -valintaruudun, voit lukita tietokoneen. Lisätietoja on kohdassa Tietokoneen lukitseminen.

Esimerkki 2: Advanced Settings (Lisäasetukset) -sivulla määritetään pakollinen käyttäjätunnistus ennen kertakirjaustoiminnon käyttämistä.

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Credential Manager** ja valitse sitten **Asetukset**.
3. Valitse oikeassa ruudussa **Single Sign On** (Kertakirjaustoiminto) -välilehti.
4. Valitse **When registered logon dialog or Web page is visited** (Siirryttäessä rekisteröityyn kirjautumisikkunaan tai Web-sivustoon) -kohdasta **Authenticate user before submitting credentials** (Tarkista käyttöoikeus ennen tietojen lähettämistä) -valintaruutu.
5. Valitse **Käytä** ja tallenna sitten muutokset valitsemalla **OK**.
6. Käynnistä tietokone uudelleen.

7 Device Access Manager for HP ProtectTools

Tämä suojaustyökalu on vain pääkäyttäjien käytettävissä. Device Access Manager for HP ProtectTools -ohjelman suojausominaisuudet suojaavat tietokoneeseen liitettyjä laitteita luvattomalta käytöltä. Suojausominaisuuksia ovat esimerkiksi seuraavat ominaisuudet:

- laitteiden käyttöoikeudet määrittävien laiteprofiilien luominen kaikille käyttäjälle
- laitteen käyttöoikeuden myöntäminen tai estäminen ryhmän jäsenyyden mukaan.

Taustapalvelun käynnistäminen

Laiteprofiilien käyttäminen edellyttää, että HP ProtectTools Device Locking/Auditing -taustapalvelu on käynnissä. Kun ensimmäisen kerran yrität ottaa laiteprofiilit käyttöön, HP ProtectTools Security Manager avaa valintaikkunan. Valitse valintaikkunassa, haluatko käynnistää taustapalvelun. Käynnistä taustapalvelu ja määritä se käynnistymään automaattisesti aina, kun järjestelmä käynnistyy, valitsemalla **Kyllä**.

Yksinkertainen kokoonpano

Tämän toiminnon avulla voit estää seuraaviin luokkiin kuuluvien laitteiden käytön:

- USB-laitteet (muilta kuin järjestelmänvalvojilta)
- siirrettävät tietovälineet kuten levykkeet ja USB-muistit (muilta kuin järjestelmänvalvojilta)
- DVD- ja CD-ROM-laitteet (muilta kuin järjestelmänvalvojilta)
- kaikki sarja- ja rinnakkaisportit (muilta kuin järjestelmänvalvojilta).

Voit estää muita kuin järjestelmänvalvojia käyttämästä tietyn luokan laitteita seuraavasti:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Device Access Manager** ja valitse sitten **Simple Configuration** (Yksinkertainen kokoonpano).
3. Valitse oikeasta ruudusta sen laitteen valintaruutu, jonka käytön haluat estää.
4. Valitse **Käytä**.

   Huomautus Jos taustapalvelu ei ole käynnissä, se yrittää nyt käynnistyä. Salli käynnistyminen valitsemalla **Kyllä**.

5. Valitse **OK**.

Laiteluokan kokoonpano (lisäasetus)

Käyttöoikeuksien myöntämiseen tietyille käyttäjille tai ryhmille sekä käytön kieltämiseen on käytettävissä lisäasetuksia.

Käyttäjän tai ryhmän lisääminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Device Access Manager** ja valitse sitten **Device Class Configuration** (Laiteluokan kokoonpano).
3. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää.
4. Valitse **Add** (Lisää). Select Users or Groups (Valitse käyttäjät tai ryhmät) -valintaikkuna avautuu.
5. Etsi lisättävät käyttäjät ja ryhmät valitsemalla **Lisäasetukset > Find Now** (Etsi nyt).

6. Napsauta käyttäjää, jolta haluat estää laitteen käytön. Valitse sitten **OK**.
7. Valitse **OK**.

Käyttäjän tai ryhmän poistaminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Device Access Manager** ja valitse sitten **Device Class Configuration** (Laiteluokan kokoonpano).
3. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää.
4. Napsauta poistettavaa käyttäjää tai ryhmää. Valitse sitten **Poista**.
5. Valitse **Käytä** ja valitse sitten **OK**.

Käyttäjän tai ryhmän käytön estäminen

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Device Access Manager** ja valitse sitten **Device Class Configuration** (Laiteluokan kokoonpano).
3. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää.
4. Lisää **User/Groups** (Käyttäjä/ryhmät) -kohtaan käyttäjä tai ryhmä, jonka käyttöoikeudet haluat kieltää.
5. Valitse **Deny** (Estä) sen käyttäjän tai ryhmän vierestä, jonka käyttöoikeudet haluat kieltää.
6. Valitse **Käytä** ja valitse sitten **OK**.

Laiteluokan käyttöoikeuden myöntäminen yhdelle käyttäjälle tai ryhmälle

Voit myöntää yhdelle käyttäjälle laiteluokan käyttöoikeuden ja estää laiteluokan käytön kaikilta muilta saman käyttäjäryhmän jäseniltä.

Myönnä seuraavasti käyttöoikeus käyttäjälle, mutta ei ryhmälle:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Device Access Manager** ja valitse sitten **Device Class Configuration** (Laiteluokan kokoonpano).
3. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää.
4. Lisää **User/Groups** (Käyttäjä/ryhmät) -kohtaan ryhmä, jonka käyttöoikeudet haluat kieltää.
5. Valitse **Deny** (Estä) sen ryhmän vierestä, jonka käyttöoikeudet haluat kieltää.
6. Siirry halutun luokan alla olevaan kansioon ja lisää yksittäinen käyttäjä kansioon. Myönnä käyttäjälle käyttöoikeus valitsemalla **Allow** (Salli).
7. Valitse **Käytä** ja valitse sitten **OK**.

Tietyn laitteen käyttöoikeuden myöntäminen yhdelle käyttäjälle tai ryhmälle

Voit myöntää yhdelle käyttäjälle tietyn laitteen käyttöoikeuden ja estää koko laiteluokan käytön kaikilta muilta saman käyttäjäryhmän jäseniltä.

Myönnä seuraavasti tietyn laitteen käyttöoikeus käyttäjälle, mutta ei ryhmälle:

1. Valitse **Käynnistä > Kaikki ohjelmat > HP ProtectTools Security Manager**.
2. Valitse vasemmasta ruudusta **Device Access Manager** ja valitse sitten **Device Class Configuration** (Laiteluokan kokoonpano).
3. Valitse laiteluettelosta laiteluokka, jonka asetukset haluat määrittää. Siirry sitten sen alla olevaan kansioon.
4. Lisää **User/Groups** (Käyttäjä/ryhmät) -kohtaan ryhmä, jonka käyttöoikeudet haluat kieltää.
5. Valitse **Deny** (Estä) sen ryhmän vierestä, jonka käyttöoikeudet haluat kieltää.
6. Siirry laiteluettelossa sen laitteen kohtaan, jonka käyttöoikeudet haluat myöntää käyttäjälle.
7. Valitse **Add** (Lisää). Select Users or Groups (Valitse käyttäjät tai ryhmät) -valintaikkuna avautuu.
8. Etsi lisättävät käyttäjät ja ryhmät valitsemalla **Lisäasetukset > Find Now** (Etsi nyt).
9. Napsauta käyttäjää, jolle haluat myöntää laitteen käyttöoikeuden. Valitse sitten **OK**.
10. Myönnä käyttäjälle käyttöoikeus valitsemalla **Allow** (Salli).
11. Valitse **Käytä** ja valitse sitten **OK**.

Sanasto

automaattinen DriveLock-lukitus Suojaustoiminto, joka mahdollistaa DriveLock-salasanojen luomisen ja suojaamisen TPM Embedded Security -sirun (upotetun suojaussirun) avulla. Kun käyttäjä vahvistaa käyttöoikeutensa TPM Embedded Security -sirun avulla ja antaa oikean TPM-peruskäyttäjän avaimen salasanan, BIOS poistaa kiintolevyn lukituksen kyseistä käyttäjää varten.

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

BIOS-järjestelmän sirukorttisuojaus Kun tämä toiminto on otettu käyttöön Smart Card Security -ohjelmassa, käyttäjän todennuksessa on käytettävä sirukorttia ja oikeaa PIN-koodia.

BIOS-profiili Joukko BIOS-asetuksia, jotka voidaan tallentaa ja joita voidaan sitten käyttää muissa käyttäjätileissä.

digitaalinen allekirjoitus Tiedoston mukana lähetetyt tiedot, jotka vahvistavat aineiston lähettäjän sekä sen, että tiedostoa ei ole muokattu allekirjoittamisen jälkeen.

digitaalinen varmenne (sertifikaatti) Sähköinen käyttöoikeustieto, joka yksilöi ja todentaa käyttäjän tai yrityksen kytkemällä digitaalisen varmenteen omistajan sähköiseen avainpariin, jota käytetään sähköisten tietojen allekirjoittamiseen.

DriveLock Suojaustoiminto, joka yksilöi kiintolevyn käyttäjät. Kun tämä toiminto on käytössä, käyttäjän on annettava oikea DriveLock-salasana tietokonetta käynnistettäessä.

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

henkilökohtainen suojattu levyasema (Personal secure drive, PSD) Arkaluontoisten tietojen suojattu tallennusalue.

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

julkista avainta käyttävä rakenne (Public Key Infrastructure, PKI) Standardi, joka määrittää varmenteiden ja salausavainten luomisen, käyttämisen ja hallinnan rajapinnat.

kertakirjaustoiminto Toiminto, joka tallentaa kirjautumistietoja ja jonka avulla Credential Manager -ohjelma voi antaa salasanat automaattisesti, kun käyttäjä avaa Web- tai Windows-sovelluksen, joka on suojattu salasanalla.

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

käynnistystodennus Suojaustoiminto. Kun tämä toiminto on käytössä, käyttäjän on todistettava käyttöoikeutensa esimerkiksi sirukortilla, suojaussirulla tai salasanalla, kun tietokone käynnistetään.

omat tiedot HP ProtectTools Credential Manager -ohjelmassa käytettävä kirjautumistapojen ja käyttöoikeusasetusten joukko, joka vastaa tietyn käyttäjän käyttäjätiliä tai profiilia.

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.

salauspalvelun tarjoaja (Cryptographic service provider, CSP) Salausalgoritmien tarjoaja tai kirjasto. Algoritmeja voidaan käyttää tarkkaan määritetyn liittymän avulla tiettyjen salaustoimintojen suorittamiseen.

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

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

siirtäminen Avaimia ja varmenteita voidaan hallita, palauttaa ja siirtää.

sirukortin järjestelmänvalvojan salasana Salasana, joka on määritetty järjestelmänvalvojan sirukortille Tietokoneen asetukset -ohjelmassa ja jonka avulla järjestelmänvalvojan henkilöllisyys tarkastetaan, kun tietokone käynnistetään tai käynnistetään uudelleen. Järjestelmänvalvoja voi määrittää salasanan manuaalisesti, tai salasana voidaan muodostaa automaattisesti.

sirukortin käyttäjän salasana Salasana, joka on määritetty käyttäjän sirukortille Tietokoneen asetukset -ohjelmassa ja jonka avulla käyttäjän henkilöllisyys tarkastetaan, kun tietokone käynnistetään tai käynnistetään uudelleen. Järjestelmänvalvoja voi määrittää salasanan manuaalisesti, tai salasana voidaan muodostaa automaattisesti.

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

tiukka suojaus BIOS Configuration -ohjelman suojaustoiminto, joka tarjoaa lisäsuojaa järjestelmänvalvojan ja käynnistyksen salasanoille sekä muille käynnistystodennustavoille.

todennus Käyttöoikeuden tarkistus; prosessi, jossa tarkistetaan, onko käyttäjällä esimerkiksi oikeus käyttää tietokonetta, muokata jonkin ohjelman asetuksia tai katsoa suojattuja tietoja.

toimialue Tietokoneet, jotka kuuluvat tiettyyn verkon osaan ja joilla on yhteinen hakemistotietokanta. Toimialueet on nimetty yksilöivästi, ja kullakin toimialueella on omat säännöt ja prosessit.

TPM (Trusted Platform Module) Embedded Security -siru (vain tietyt mallit) Sisäinen suojaussiru, jolla voidaan suojata arkaluontoisia käyttäjätietoja tietomurroilta. Se on käyttöympäristön murtosuojauksen ydin. TPM tarjoaa salausalgoritmeja, jotka vastaavat Trusted Computing Group (TCG) -vaatimuksia.

USB-poletti Tietoturvalaite, johon tallennetaan käyttäjän tunnistustiedot. Sitä käytetään tietokoneen omistajan todennukseen samaan tapaan kuin sirukorttia ja biometristä tunnistusta.

uudelleen käynnistäminen Tietokone sammuu ja käynnistyy sitten uudelleen.

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

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

Windows-käyttäjätili Tietoverkon tai yksittäisen tietokoneen käyttäjän profiili.

virtuaalinen poletti Suojaustoiminto, joka toimii lähes samalla tavoin kuin sirukortti ja kortinlukija. Poletti tallennetaan tietokoneen kiintolevylle tai Windows-käyttöjärjestelmän rekisteriin. Kun kirjaudut virtuaalista polettia käyttämällä, sinun on annettava PIN-koodi.

Hakemisto