Dell Data Protection | Access -aloitusnäyttö

Dell Data Protection | Access -aloitusnäyttö on lähtöpaikka, jonka kautta sovelluksen eri toimintoja voidaan käyttää. Tästä ikkunasta voit avata seuraavat ikkunat:

System Access Wizard (Ohjattu asennustoiminto)
Kirjautumisasetukset
Itsesalaava asema
Lisäasetukset

Ikkunan oikeassa alakulmassa on **advanced** (lisäasetukset) -linkki, jota napsauttamalla pääset lisäasetusnäyttöön.

Kun napsautat advanced options (lisäasetukset) -sivun oikeassa alakulmassa olevaa **home** (aloitus) -linkkiä, pääset takaisin aloitusnäyttöön.

System Access Wizard (Ohjattu asennustoiminto)

Ohjattu System Access Wizard -toiminto käynnistyy automaattisesti, kun **Dell Data Protection | Access** -sovellus käynnistetään ensimmäisen kerran. Ohjattu toiminto opastaa järjestelmän turvallisuusasetusten määrittämisessä. Voit määrittää, miten (esimerkiksi vain salasana tai sormenjälki ja salasana) ja milloin (Windows-kirjautumisessa, ennen Windowsin käynnistystä tai molemmissa vaiheissa) järjestelmään kirjaudutaan. Jos järjestelmässä on itsesalaava asema (SED-asema), voit määrittää kyseisen aseman asetukset tämän ohjatun toiminnon avulla.

Pääkäyttäjän toiminnot

Käyttäjät, joille on järjestelmässä määritetty Windowsin pääkäyttäjän oikeudet, voivat käyttää seuraavia **Dell Data Access | Protection** -sovelluksen toimintoja, jotka eivät ole tavallisten käyttäjien käytettävissä:

- Asettaa/vaihtaa järjestelmän (Windowsin käynnistystä edeltävän) salasanan
- Asettaa/vaihtaa kiintolevyn salasanan
- Asettaa/vaihtaa pääkäyttäjän salasanan
- Asettaa/vaihtaa TPM-omistajan salasanan
- Asettaa/vaihtaa ControlVault-pääkäyttäjän salasanan
- Palauttaa järjestelmän
- Arkistoida ja palauttaa tunnistetietoja
- Asettaa/vaihtaa älykortin pääkäyttäjän PIN-koodin
- Poistaa/palauttaa älykortin
- Ottaa käyttöön / poistaa käytöstä Dellin suojatun Windows-kirjautumisen
- Asettaa Windowsin kirjautumiskäytännön
- Hallita itsesalaavia asemia mm. seuraavasti:
    - Ottaa käyttöön / poistaa käytöstä itsesalaavan aseman lukituksen
    - Ottaa käyttöön / poistaa käytöstä Windows-salasanojen synkronoinnin (WPS-toiminnon)
    - Ottaa käyttöön / poistaa käytöstä Single Sign On -sisäänkirjauksen (SSO)
    - Suorittaa salauksen poiston

Etähallinta

Organisaatiot voivat määrittää käyttöympäristön siten, että useissa alustoissa käytettävän **Dell Data Protection | Access** -sovelluksen suojaustoimintoja voidaan hallita keskitetysti (etähallinta). Tässä tapauksessa Windowsin tietoturvainfrastruktuuria, kuten Active Directory -palvelua, voidaan käyttää **Dell Data Protection | Access** -sovelluksen toimintojen turvalliseen hallitsemiseen.

Kun tietokonetta hallitaan etäyhteyden kautta (etäpääkäyttäjä "omistaa" laitteen), **Dell Data Protection | Access** -sovelluksen paikallinen hallinta poistetaan käytöstä. Toisin sanoen sovelluksen hallintaikkunat eivät ole käytettävissä paikallisesti. Seuraavia toimintoja voidaan hallita etäyhteyden kautta:

- Trusted Platform Module (TPM)
- ControlVault
- Windowsin käynnistystä edeltävä kirjautuminen
- Järjestelmän palautus
- BIOS-salasanat
- Windows-kirjautumiskäytäntö
- Itsesalaavat asemat
- Sormenjäljen ja älykortin rekisteröinti.

Lisätietoja etähallinnasta Wave Systemsin EMBASSY® Remote Administration Server (ERAS) -palvelimen avulla saat ottamalla yhteyttä Dellin myyntihenkilöstöön tai käymällä osoitteessa dell.com.

Kirjautumisasetukset

Access Options (Kirjautumisasetukset) -ikkunan avulla voidaan määrittää järjestelmän kirjautumisasetukset.

Jos olet määrittänyt **Dell Data Protection | Access** -sovelluksen asetuksia, nämä asetukset ja niiden sisältämät asetusvaihtoehdot näkyvät aloitussivulla (esim. change password for Pre-Windows login (vaihda Windowsin käynnistystä edeltävää kirjautumissalasanaa)). Käytettävissä olevat valinnat ovat pikavalintoja. Niitä napsauttamalla pääset ikkunaan, jossa voit tehdä tietyn tehtävän (esimerkiksi vaihtaa Windowsin käynnistystä edeltävää salasanan tai rekisteröidä toisen sormenjäljen).

Yleiset
Voit määrittää, milloin kirjautuminen tapahtuu (Windowsissa, ennen Windowsia tai molemmissa kohdissa) ja miten kirjautuminen tehdään (esimerkiksi salasanalla tai sormenjäljen avulla). Voit valita yhden kirjautumisvaihtoehdon tai kaksi kirjautumisvaihtoehtoa. Näitä ovat sormenjäljen, älykortin ja salasanan yhdistelmät. Näytössä näkyvät käytettävissä olevat kirjautumisvaihtoehdot perustuvat käyttöympäristön kirjautumiskäytäntöihin ja alustan tukemiin kirjautumismenetelmiin.

Sormenjälki
Jos järjestelmässä on sormenjälkilukija, voit rekisteröidä tai päivittää sormenjälkiä järjestelmään kirjautumista varten. Kun olet rekisteröinyt sormenjäljet, voit kirjautua järjestelmään Windows-tasolla, ennen Windowsin käynnistymistä tai molemmissa vaiheissa pyyhkäisemällä järjestelmään liitettyä sormenjälkilukijaa rekisteröidyllä sormenjäljellä. Lisätietoja on kohdassa Käyttäjän sormenjälkien rekisteröiminen.

Windowsin käynnistystä edeltävä kirjautuminen
Jos olet määrittänyt, että käyttäjien on kirjauduttava ennen Windowsin käynnistymistä, sinun on määritettävä järjestelmän salasana (kutsutaan myös Windowsin käynnistystä edeltäväksi salasanaksi) Windowsin käynnistystä edeltävää kirjautumista varten. Kun salasana on määritetty, pääkäyttäjä voi milloin tahansa vaihtaa tätä salasanaa.

Tämän näytön avulla voit myös poistaa käytöstä Windowsin käynnistystä edeltävän kirjautumisen. Voit poistaa kirjautumisen käytöstä antamalla nykyisen järjestelmän salasanan, vahvistamalla nykyisen salasanan ja napsauttamalla sitten **Disable** (Poista käytöstä) -painiketta.

Älykortti
Jos olet määrittänyt, että käyttäjien on kirjauduttava älykortin avulla, vähintään yksi perinteinen (kontaktillinen) tai etäluettava älykortti on rekisteröitävä järjestelmään. Käynnistä ohjattu älykortin rekisteröimistoiminto napsauttamalla **Enroll another smartcard** (Rekisteröi toinen älykortti) -linkkiä. Rekisteröiminen tarkoittaa älykortin määrittämistä kirjautumista varten.

Kun olet rekisteröinyt älykortin, voit vaihtaa tai määrittää kortin PIN-koodin **Change or setup my smartcard PIN** (Vaihda tai aseta älykortin PIN-koodi) -linkin kautta.

Windowsin käynnistystä edeltävä kirjautuminen

Kun järjestelmään on määritetty Windowsin käynnistystä edeltävä kirjautuminen, käyttäjien on tunnistauduttava (salasanan, sormenjäljen tai älykortin avulla) ennen Windowsin käynnistystä, kun järjestelmä käynnistetään. Windowsin käynnistystä edeltävä kirjautumistoiminto parantaa järjestelmän suojausta. Luvattomat käyttäjät eivät pysty käynnistämään Windowsia eivätkä käyttämään tietokonetta (jos tietokone esimerkiksi varastetaan).

Pre-Windows Login (Windowsin käynnistystä edeltävä kirjautuminen) -ikkunan avulla pääkäyttäjät voivat määrittää Windowsin käynnistystä edeltävän kirjautumisen asetukset ja luoda tai vaihtaa Windowsin käynnistystä edeltävää (järjestelmän) salasanan. Jos salasanaa ei ole määritetty, Windowsin käynnistystä edeltävä kirjautuminen voidaan poistaa käytöstä tästä ikkunasta. Windowsin käynnistystä edeltävän kirjautumisen määrittäminen käynnistää ohjatun toiminnon, jonka avulla voidaan tehdä seuraavaa:

- Järjestelmän salasana: Määritä järjestelmän salasana (Windowsin käynnistystä edeltävä salasana) Windowsin käynnistystä edeltävää kirjautumista varten. Tätä salasanaa käytetään myös varmuussalasanana, jos käytössä on muita todennusmenetelmiä. (Salasanan avulla voidaan kirjautua järjestelmään, jos esimerkiksi sormenjälkianturi ei toimi.)
- Sormenjälki tai älykortti: Määritä sormenjälki tai älykortti Windowsin käynnistystä edeltävää kirjautumista varten. Määritä myös, käytetäänkö tätä todennusmenetelmää Windowsin käynnistystä edeltävän salasanan sijaan tai sen lisäksi.
- Single Sign On -kertakirjautuminen: Oletusarvoisesti Windowsin käynnistystä edeltävä todennus (salasanan, sormenjäljen tai älykortin avulla) kirjaa käyttäjän automaattisesti myös Windowsiin (toiminnon nimi on Single Sign On). Toiminnon voi poistaa käytöstä lisäämällä valinnan I want to login again at Windows (Haluan kirjautua myös Windows-tasolla) -valintaruutuun.
- Jos BIOS-kiintolevyn salasana on otettu käyttöön Windowsin käynnistystä edeltävän salasanan lisäksi, käytössä on myös asetus, jonka avulla voit vaihtaa kiintolevyn salasanaa tai poistaa sen käytöstä.

HUOMAUTUS: Kaikkia sormenjälkilukijoita ei voi käyttää Windowsin käynnistystä edeltävässä todennuksessa. Jos sormenjälkilukija ei ole yhteensopiva, voit rekisteröidä sormenjälkiä ainoastaan Windows-kirjautumista varten. Voit tarkistaa, onko tietty sormenjälkilukija yhteensopiva, ottamalla yhteyttä järjestelmän pääkäyttäjään tai tutustumalla tuettujen sormenjälkilukijoiden luetteloon osoitteessa support.dell.com.

Windowsin käynnistystä edeltävän kirjautumisen poistaminen käytöstä
Tämän ikkunan avulla voit myös poistaa käytöstä Windowsin käynnistystä edeltävän kirjautumisen. Voit poistaa kirjautumisen käytöstä antamalla nykyisen Windowsin käynnistystä edeltävän (järjestelmän) salasanan, vahvistamalla kyseisen salasanan ja napsauttamalla sitten **Disable** (Poista käytöstä) -painiketta. Huomaa, että Windowsin käynnistystä edeltävän kirjautumisen poistaminen käytöstä ei poista rekisteröityjä sormenjälkiä tai älykortteja.

Sormenjälkien rekisteröiminen / poistaminen

Käyttäjät voivat rekisteröidä tai päivittää sormenjälkiä, joita käytetään käyttäjän todennukseen Windowsin käynnistystä edeltävässä kirjautumisessa tai Windows-kirjautumisessa. Fingerprint (Sormenjälki) -välilehdessä näkyvät käsien kuvat osoittavat, mitkä käyttäjän sormet on rekisteröity. **Enroll another** (Rekisteröi uusi) -linkin valitseminen käynnistää ohjatun sormenjälkien rekisteröintitoiminnon, joka opastaa sormenjäljen rekisteröintiprosessissa. Rekisteröiminen tarkoittaa kirjautumiseen käytettävän sormenjäljen tallentamista. Järjestelmässä on oltava toimiva sormenjälkilukija, joka on asennettu ja määritetty oikein, jotta sormenjälkiä voidaan rekisteröidä.

HUOMAUTUS: Kaikkia sormenjälkilukijoita ei voi käyttää Windowsin käynnistystä edeltävässä kirjautumisessa. Näyttöön tulee virheviesti, jos yrität rekisteröidä sormenjälkeä Windowsin käynnistystä edeltävää kirjautumista varten yhteensopimattomalla sormenjälkilukijalla. Voit tarkistaa, onko laite yhteensopiva, ottamalla yhteyttä järjestelmän pääkäyttäjään tai tutustumalla tuettujen sormenjälkilukijoiden luetteloon osoitteessa support.dell.com.

Sormenjälkien rekisteröimisen aikana järjestelmä pyytää antamaan Windows-salasanan henkilöllisyyden vahvistamista varten. Jos kirjautumiskäytäntö edellyttää järjestelmän salasanaa, järjestelmä pyytää antamaan myös Windowsin käynnistystä edeltävän (järjestelmän) salasanan. Windowsin käynnistystä edeltävän salasanan avulla voidaan kirjautua järjestelmään, jos sormenjälkilukija ei toimi.

HUOMAUTUKSET:

- Jokaisen käyttäjän tulisi rekisteröidä ainakin kaksi sormenjälkeä rekisteröintiprosessin aikana.
- Varmista, että sormenjäljet on rekisteröity kunnolla, ennen kuin sormenjälkitodennusominaisuudet otetaan käyttöön.
- Jos vaihdat järjestelmän sormenjälkilukijaa, sormenjäljet on rekisteröitävä uudelleen uudella lukijalla. Eri sormenjälkilukijoiden käyttämistä vuorotellen ei suositella.
- Jos sormenjälkien rekisteröimisen aikana näyttöön tulee toistuvasti viesti sensor lost focus (anturin tarkennus epäonnistui), tämä voi tarkoittaa, että tietokone ei tunnista sormenjälkilukijaa. Jos käytössä on ulkoinen sormenjälkilukija, sormenjälkilukijan irrottaminen ja uudelleen kytkeminen ratkaisee usein tällaisen ongelman.

Rekisteröityjen sormenjälkien tyhjentäminen

Voit poistaa rekisteröityjä sormenjälkiä napsauttamalla **Remove fingerprint** (Poista sormenjälki) -linkkiä tai napsauttamalla rekisteröityä sormea ohjatussa sormenjäljen rekisteröintitoiminnossa (poistaa valinnan).

Jos haluat poistaa tietyn käyttäjän, joka on rekisteröinyt sormenjälkiä Windowsin käynnistystä edeltävää todennusta varten, pääkäyttäjän on poistettava kyseisen käyttäjän kaikki rekisteröidyt sormenjäljet.

HUOMAUTUS: Jos sormenjäljen rekisteröintiprosessin aikana ilmenee ongelmia, katso lisätietoja osoitteesta wave.com/support/Dell.

Älykorttien rekisteröiminen

Dell Data Protection | Access -sovelluksen avulla voidaan määrittää, käytetäänkö perinteisiä (kontaktillisia) vai etäluettavia älykortteja Windows-tiliin kirjautumiseen tai Windowsin käynnistystä edeltävään todentamiseen. Napsauttamalla Smartcard (Älykortti) -välilehden **Enroll another smartcard** (Rekisteröi uusi älykortti) -linkkiä voit käynnistää ohjatun älykortin rekisteröimistoiminnon. Toiminto opastaa rekisteröintiprosessin vaiheissa. Rekisteröiminen tarkoittaa älykortin määrittämistä kirjautumista varten.

Järjestelmässä on oltava toimiva älykortintodennuslaite, joka on asennettu ja määritetty oikein, jotta rekisteröiminen voidaan suorittaa.

HUOMAUTUS: Voit tarkistaa, onko tietty laite yhteensopiva, ottamalla yhteyttä järjestelmänvalvojaan tai tutustumalla tuettujen älykorttien luetteloon osoitteessa support.dell.com.

Rekisteröinti
Älykortin rekisteröimisen aikana järjestelmä pyytää antamaan Windows-salasanan henkilöllisyyden vahvistamista varten. Jos kirjautumiskäytäntö edellyttää järjestelmän salasanaa, järjestelmä pyytää antamaan myös Windowsin käynnistystä edeltävän (järjestelmän) salasanan. Windowsin käynnistystä edeltävän salasanan avulla voidaan kirjautua järjestelmään, jos älykortinlukija ei toimi.

Rekisteröimisen aikana järjestelmä pyytää älykortin PIN-koodia, jos sellainen on asetettu. Jos kirjautumiskäytäntö edellyttää PIN-koodia eikä sitä ole asetettu, järjestelmä pyytää luomaan PIN-koodin.

HUOMAUTUKSET:

- Kun käyttäjä on rekisteröity käyttämään älykorttia Windowsin käynnistystä edeltävässä kirjautumisessa, käyttäjää ei voi poistaa.
- Tavalliset käyttäjät voivat vaihtaa älykortin käyttäjän PIN-koodin. Pääkäyttäjä voi vaihtaa pääkäyttäjän PIN-koodin ja käyttäjän PIN-koodin.
- Pääkäyttäjä voi nollata älykortin. Kun älykortti on nollattu, sitä ei voi käyttää Windows-kirjautumiseen tai Windowsin käynnistystä edeltävään kirjautumiseen, ennen kuin se on rekisteröity uudelleen.

HUOMAUTUS: TPM:n varmenteen kanssa suoritettavaa todennusta varten pääkäyttäjät voivat rekisteröidä TPM:n varmenteita Windowsin älykorttien rekisteröintiprosessin avulla. Pääkäyttäjien on valittava salauspalvelun tarjoajaksi (Cryptographic Service Provider, CSP) Wave TCG-Enabled CSP älykortin CSP:n sijasta, jotta voidaan taata toimivuus tämän sovelluksen kanssa. Lisäksi suojatun Dell-kirjautumisen ja sopivan todennustyyppikäytännön on oltava käytössä.

HUOMAUTUS: Jos näyttöön tulee virheilmoitus, ettei älykorttipalvelu ole käytössä, voit käynnistää palvelun (uudelleen) seuraavalla tavalla:

- Avaa Ohjauspaneelin Valvontatyökalut-ikkuna, valitse Palvelut ja napsauta Älykortti-kuvaketta hiiren kakkospainikkeella. Valitse sitten Käynnistä tai Käynnistä uudelleen.
- Tiettyyn virheviestiin liittyviä lisätietoja on osoitteessa wave.com/support/Dell.

Itsesalaava asema

Dell Data Protection | Access -sovellus hallitsee sisäänrakennettuja tietojensalausominaisuuksia sisältävien itsesalaavien asemien laitteistopohjaisia suojaustoimintoja. Tällä toiminnallisuudella voidaan varmistaa, että vain luvan saaneet käyttäjät voivat käyttää salattuja tietoja (kun aseman lukitus on käytössä).

Self-Encryping Drive (Itsesalaava asema) -ikkuna voidaan avata napsauttamalla näytön alapalkissa olevaa **Self-Encrypting Drive** (Itsesalaava asema) -kohtaa . Tämä palkki on näkyvissä vain, jos järjestelmään on kytketty vähintään yksi itsesalaava asema (SED-asema).

Käynnistä ohjattu Self-Encrypting Drive Setup Wizard -asetustoiminto napsauttamalla **Setup** (Asetukset) -linkkiä. Ohjatun toiminnon avulla voidaan luoda aseman pääkäyttäjän salasana, varmuuskopioida tämä salasana ja määrittää aseman salausasetukset. Vain järjestelmän pääkäyttäjät voivat käyttää ohjattua Self-Encryping Drive Setup Wizard -toimintoa.

Tärkeää! Kun asema on määritetty, tietojen suojaus ja aseman lukitus ovat käytössä. Kun asema lukitaan, se käyttäytyy seuraavasti:

- Asema siirtyy *lukittuun* tilaan, kun aseman virta katkaistaan.
- Asema ei käynnisty, ellei käyttäjä anna oikeaa käyttäjätunnusta ja salasanaa (tai sormenjälkeä) Windowsin käynnistystä edeltävässä kirjautumisnäytössä. Ennen kuin aseman lukitus otetaan käyttöön, aseman sisältämät tiedot ovat kaikkien tietokoneen käyttäjien käytettävissä.
- Asema on suojattu, vaikka se kytkettäisiin toisen tietokoneen toissijaiseksi asemaksi. Aseman tietojen käyttö edellyttää todennusta.

Kun asema on määritetty, Self-Encrypting Drive (Itsesalaava asema) -ikkunassa näkyy käytettävissä olevat asemat ja linkki aseman käyttäjän salasanan vaihtamista varten. Jos olet aseman pääkäyttäjä, voit tämän ikkunan kautta lisätä tai poistaa aseman käyttäjiä. Jos järjestelmään on määritetty ulkoinen asema, se näkyy tässä ikkunassa ja sen lukitus voidaan poistaa.

HUOMAUTUS: Jos haluat lukita toissijaisen, ulkoisen aseman, aseman virta on katkaistava erillään tietokoneesta.

Aseman pääkäyttäjä voi hallita aseman asetuksia kohdassa **Advanced > Devices** (Lisäasetukset > Laitteet). Lisätietoja on kohdassa Laitehallinta – Itsesalaavat asemat.

Aseman asetukset

Ohjattu Self-Encrypting Drive Setup Wizard -toiminto opastaa asemien määrittämisessä. Seuraavat käsitteet on hyvä pitää mielessä asennustoiminnon aikana.

Drive Administrator (Aseman pääkäyttäjä)
Ensimmäisestä käyttäjästä, jolla on järjestelmän pääkäyttäjän oikeudet ja joka määrittää aseman kirjautumisasetukset (ja asettaa aseman pääkäyttäjän salasanan), tulee aseman pääkäyttäjä. Ainostaan tällä käyttäjällä on oikeudet muuttaa aseman kirjautumisasetuksia. Vahvista, että ensimmäinen käyttäjä määritetään aseman pääkäyttäjäksi valitsemalla I understand (Ymmärrän) -valintaruutu.

Drive Administrator Password Aseman pääkäyttäjän salasana
Ohjattu toiminto pyytää luomaan aseman pääkäyttäjän salasanan ja vahvistamaan sen. Henkilöllisyys on vahvistettava antamalla Windows-salasana, ennen kuin aseman pääkäyttäjän salasana voidaan luoda. Salasanan luominen edellyttää, että kirjautuneena olevalla Windows-käyttäjällä on pääkäyttäjän oikeudet.

Backup Drive Credentials (Varmuuskopioi aseman tunnistetiedot)
Valitse sijainti kirjoittamalla sijainti kenttään tai napsauttamalla **Browse** (Selaa) -painiketta ja tallenna varmuuskopio aseman pääkäyttäjän tunnistetiedoista.

TÄRKEÄÄ**!**

- On erittäin suositeltavaa varmuuskopioida aseman pääkäyttäjän tunnistetiedot ja tallentaa ne muulle kuin ensisijaiselle kiintolevylle (esimerkiksi siirrettävälle tallennusvälineelle). Muutoin jos et pysty käyttämään asemaa ja varmuuskopio on tallennettu siihen, varmuuskopio ei ole käytettävissä.
- Kun aseman asetukset on määritetty,käyttäjien on ennen Windowsin käynnistystä annettava kelvollinen käyttäjätunnus ja salasana (tai sormenjälki), jotta he voivat käyttää järjestelmää, kun järjestelmä käynnistetään seuraavan kerran.

Add Drive User (Lisää aseman käyttäjä)
Aseman pääkäyttäjä voi lisätä asemaan uusia käyttäjiä, jotka ovat sallittuja Windows-käyttäjiä. Pääkäyttäjä voi halutessaan määrittää käyttäjän lisäämisen yhteydessä, että käyttäjän on vaihdettava salasanaa ensimmäisen kirjautumisen aikana. Käyttäjän on vaihdettava uusi salasana Windowsin käynnistystä edeltävässä todennusnäytössä, ennen kuin aseman lukitus poistetaan.

Lisäasetukset

- *Single Sign On* - Oletusarvoisesti ennen Windowsin käynnistystä annettavan itsesalaavan aseman salasanaa käytetään automaattisesti myös Windows-kirjautumiseen (toiminnon nimi on Single Sign On). Voit poistaa tämän toiminnon käytöstä valitsemalla aseman asetuksista I want to login again when Windows starts (Haluan kirjautua uudelleen, kun Windows käynnistyy) -valintaruudun.
- *Sormenjälkikirjautuminen* - Tuetuissa alustoissa voit määrittää, että kirjautuminen itsesalaavaan asemaan tapahtuu sormenjäljen avulla salasanan sijaan.
- *Lepotila/Valmiustila (S3) -tuki* (jos alusta tukee toimintoa) - Jos toiminto on käytössä, itsesalaava asema voidaan asettaa turvallisesti lepotilaan/valmiustilaan (kutsutaan myös S3-tilaksi). Tällöin aseman palauttaminen lepotilasta/valmiustilasta edellyttää Windowsin käynnistystä edeltävää todennusta.

HUOMAUTUKSET:

- Jos S3-tuki on käytössä, aseman salaussalasanoihin sovelletaan mahdollisesti käytössä olevia BIOSin salasanarajoitteita. Lisätietoja BIOSin salasanarajoitteista saat järjestelmän laitteiston valmistajalta.
- Kaikki itsesalaavat asemat eivät tue S3-tilaa. Aseman määrittämisen aikana saat ilmoituksen, tukeeko asema lepotilaa/valmiustilaa. Jos asema ei tue kyseistä tilaa, Windowsin S3-pyynnöt muunnetaan automaattisesti horrostilapyynnöiksi, jos horrostila on käytössä. (On erittäin suositeltavaa ottaa horrostila käyttöön tietokoneessa.)
- Kun kirjaudut ensimmäisen kerran Single Sign On (SSO) -toiminnon käyttöönoton jälkeen, käynnistymisprosessi pysähtyy Windowsin-kirjautumisnäyttöön. Käyttäjän pitää antaa Windows-todennuksensa, joka tallennetaan turvallisesti tulevia Windows-kirjautumisia varten. Kun järjestelmä käynnistetään seuraavan kerran, SSO-toiminto kirjaa käyttäjän automaattisesti Windowsiin. Sama prosessi on suoritettava, jos käyttäjän Windows-todennusta (salasana, sormenjälki, älykortin PIN-koodi) muutetaan. Jos tietokone on osa verkkoaluetta ja verkkoalueen käytäntö edellyttää ctrl+alt+del-näppäinyhdistelmän painamista kirjauduttaessa Windowsiin, sovellus käyttää samaa käytäntöä.

VAROITUS! Jos poistat **Dell Data Protection | Access** -sovelluksen asennuksen, itsesalaavan aseman tietojen suojaus ja aseman lukitus on ensin poistettava käytöstä.

Itsesalaavien asemien (SED) käyttäjätoiminnot

Itsesalaavien asemien pääkäyttäjät voivat hallita aseman suojausta ja käyttäjiä. Aseman käyttäjät, jotka eivät ole aseman pääkäyttäjiä, voivat käyttää vain seuraavia toimintoja:

- vaihtaa omaa aseman salasanaa
- poistaa aseman lukituksen.

Nämä toiminnot ovat käytettävissä **Dell Data Protection | Access** -sovelluksen **Self-Encrypting Drive** (Itsesalaava asema) -välilehdestä.

Change Password (Vaihda salasana)
Tämän toiminnon avulla rekisteröity käyttäjä voi luoda uuden aseman todennussalasanan. Nykyinen itsesalaavan aseman salasana on annettava ennen uuden salasana-arvon asettamista.

HUOMAUTUKSET:

- Sovellus käyttää Windows-salasanojen pituus- ja muotokäytäntöjä, jos nämä toiminnot on otettu käyttöön. Jos Windows-salasanakäytännöt eivät ole käytössä, itsesalaavan aseman salasanan enimmäispituus on 32 merkkiä. Huomaa, että enimmäispituus on 127 merkkiä, jos S3 (lepotila/valmiustila) ei ole käytössä.
- Käyttäjän itsesalaavan aseman salasana on eri salasana kuin käyttäjän Windows-salasana. Jos käyttäjän Windows-salasana muutetaan tai nollataan, se ei vaikuta käyttäjän aseman salasanaan, ellei Windowsin salasanan synkronointi ole käytössä. Lisätietoja on kohdassa Laitteet: Itsesalaavat asemat.
- Muissa kuin englantilaisissa näppäimistöissä esiintyy joskus merkkejä, joita ei voi käyttää itsesalaavan aseman salasanassa. Jos Windows-salasanassa on jokin rajoitetuista merkeistä ja Windowsin salasanan synkronisointi on käytössä, synkronisointi epäonnistuu ja näyttöön tulee virheviesti.

Drive Unlock (Aseman lukituksen poisto)
Aseman lukituksen poiston avulla rekisteröity aseman käyttäjä voi poistaa lukitun aseman lukituksen. Kun aseman lukitus on käytössä, asema siirtyy lukitustilaan, kun tietokoneen virta katkaistaan. Kun järjestelmän käynnistetään seuraavan kerran, käyttäjän on tunnistauduttava aseman käyttäjäksi antamalla salasanansa ennen Windowsin käynnistystä näyttöön tulevassa todennusruudussa.

HUOMAUTUKSET:

- Jos tietokoneella on aktiivisena yhtä aikaa useita itsesalaavan aseman käyttäjätilejä, virransäästötilaan (esim. lepotila/valmiustila tai horrostila) siirtyminen ei välttämättä ole mahdollista.
- Ennen Windowsin käynnistystä näyttöön tulevassa todennusruudussa Käyttäjä 1, Käyttäjä 2, Käyttäjä 3 ja Käyttäjä 4 korvataan aseman käyttäjänimillä sovelluksen versioissa, jotka on lokalisoitu seuraaville kielille: kiina, japani, korea ja venäjä.

Lisäasetukset

Dell Data Protection | Access -sovelluksen lisäasetusten avulla käyttäjä, jolla on järjestelmänvalvojan oikeudet, voi hallita seuraavia sovelluksen osia:

Ylläpito
Salasanat
Laitteet

HUOMAUTUS: Vain käyttäjät, joilla on järjestelmänvalvojan oikeudet, voivat tehdä muutoksia lisäasetuksiin. Tavalliset käyttäjät voivat tarkastella näitä asetuksia, mutta eivät voi tehdä muutoksia niihin.

Maintenance (Ylläpito) -ikkunan yleiskatsaus

Maintenance (Ylläpito) -ikkunan avulla pääkäyttäjät voivat määrittää Windows-kirjautumisen asetukset, palauttaa järjestelmän uutta käyttötarkoitusta varten tai arkistoida käyttäjän tunnistetietoja järjestelmän suojauslaitteistoon tai palauttaa niitä. Lisätietoja on seuraavissa aiheissa:

Kirjautumisen asetukset
Järjestelmän palautus
Tunnistetietojen arkistointi ja palautus

Kirjautumisen asetukset

Access Preferences (Kirjautumisen asetukset) -ikkunan avulla pääkäyttäjät voivat määrittää kaikkia järjestelmän käyttäjiä koskevat Windows-kirjautumisen asetukset.

Enable Dell Secure login (Ota käyttöön suojattu Dell-kirjautuminen)
Mahdollisuus korvata tavallinen Windowsin ctrl-alt-delete-näyttö tuo käyttöön useita todennustapoja Windows-kirjautumista varten Windows-salasanan sijaan (tai sen lisäksi). Voit vahvistaa Windows-kirjautumisen suojausta lisäämällä sormenjälkitunnistuksen toiseksi todennusmenetelmäksi. Windows-kirjautumista varten voidaan lisätä myös muita todentamistapoja, joita ovat muun muassa älykortti ja TPM-varmenne.

HUOMAUTUKSET:

- Suojatun Dell-kirjautumisen käyttöönotto vaikuttaa kaikkiin järjestelmän käyttäjiin.
- On suositeltavaa, että toiminto otetaan käyttöön vasta käyttäjien sormenjälkien tai älykorttien rekisteröimisen JÄLKEEN.
- Kun kirjaudut järjestelmään ensimmäisen kerran toiminnon käyttöönoton jälkeen, järjestelmä pyytää kirjautumaan Windowsiin vakiokäytännön mukaan. Seuraavan käynnistämisen yhteydessä kirjautuminen tapahtuu käyttämällä uutta todennusmenetelmää.

Disable Dell Secure login (Poista käytöstä suojattu Dell-kirjautuminen)
Tämä asetus poistaa käytöstä kaikki **Dell Data Protection | Access** -sovelluksen Windows-kirjautumistoiminnot. Kun asetus on valittuna, käytössä on tavallinen Windows-kirjautumiskäytäntö.

HUOMAUTUKSET:

- Jos kirjautumisen aikana näyttöön tulee suojattua Windows-kirjautumista koskeva virheviesti, poista käytöstä suojattu Dell-kirjautuminen ja ota se sitten käyttöön uudelleen.
- Tiettyyn virheviestiin liittyviä lisätietoja on osoitteessa wave.com/support/Dell.

Järjestelmän palautus

Reset System (Palauta järjestelmä) -toiminnon avulla voidaan poistaa alustan suojauslaitteistojen sisältämät käyttäjätiedot. Toimintoa voidaan käyttää esimerkiksi, kun tietokoneen käyttötarkoitus muuttuu. Toiminto poistaa kaikki järjestelmään tallennetut salasanat, lukuun ottamatta Windowsin käyttäjäsalasanoja, ja kaikki suojauslaitteiden (esim. ControlVault, TPM ja sormenjälkilaitteet) sisältämät tiedot. Tämä toiminto poistaa käytöstä myös itsesalaavien asemien tietojen suojauksen siten, että aseman tiedot ovat käytettävissä.

Vahvista, että haluat varmasti palauttaa järjestelmän, ja valitse sitten **Next** (Seuraava). Kun palautat järjestelmän, sinun on annettava jokaisen suojauslaitteen salasana, jos sellainen on asetettu:

- TPM-omistaja
- ControlVault-pääkäyttäjä
- BIOS -pääkäyttäjä
- BIOS-järjestelmä (Windowsin käynnistystä edeltävä)
- Kiintolevy (BIOS)
- Itsesalaavan aseman pääkäyttäjä

HUOMAUTUS: Vain itsesalaavan aseman pääkäyttäjän salasana on annettava. Aseman käyttäjien salasanoja ei tarvitse antaa.

Tärkeää! Ainoa tapa palauttaa järjestelmän palauttamisen yhteydessä poistetut tiedot on palauttaa ne aiemmin tallennetusta arkistosta. Jos tietoja ei ole arkistoitu, niitä ei voi palauttaa. Itsesalaavista asemista poistetaan vain asetustiedot. Näiden asemien sisältämiä henkilökohtaisia tietoja ei poisteta.

Tunnistetietojen arkistointi ja palautus

Tunnistetietojen arkistointi- ja palautustoimintojen avulla voidaan varmuuskopioida ja palauttaa kaikki käyttäjien tunnistetiedot (kirjautumis- ja salaustiedot), jotka on tallennettu ControlVault-tallennuspaikkaan tai TPM (Trusted Platform Module) -turvapiiriin. Tietojen varmuuskopioiminen on tärkeää, kun tietokone alustetaan uudelleen. Tiedot on myös hyvä varmuuskopioida, jotta ne voidaan palauttaa laitteistovian jälkeen. Jos tiedot on arkistoitu, voit palauttaa kaikki tunnistetiedot uuteen tietokoneeseen tallennetusta arkistotiedostosta.

Voit arkistoida tai palauttaa yhden käyttäjän tai järjestelmän kaikkien käyttäjien tunnistetiedot.

Käyttäjän tunnistetiedot koostuvat Windowsin käynnistystä edeltävistä tunnistetiedoista (esim. rekisteröidyt sormenjäljet ja älykorttitiedot) ja TPM-turvapiiriin tallennetuista avaimista. TPM luo avaimia suojattujen sovellusten pyyntöjen mukaan. Esimerkiksi digitaalisen varmenteen luominen luo avaimet TPM-turvapiiriin.

HUOMAUTUS: Tarkista suojatun sovelluksen ohjeista, voiko **Dell Data Protection | Access** arkistoida TPM-avaimia vai ei. Yleensä Wave TCG-Enabled CSP -ohjelmaa käyttävien sovellusten luomia avaimia tuetaan.

Tunnistetietojen arkistoiminen

Voit arkistoida tunnistetiedot seuraavalla tavalla:

- Määritä, arkistoidaanko vain omat vai järjestelmän kaikkien käyttäjien tunnistetiedot.
- Kirjaudu suojauslaitteeseen antamalla järjestelmän (Windowsin käynnistystä edeltävä) salasana, ControlVault-pääkäyttäjän salasana ja TPM-omistajan salasana.
- Luo tunnistetietojen varmuuskopion salasana.
- Määritä arkiston sijainti **Broswe** (Selaa) -painikkeen avulla. Arkiston sijainnin on oltava siirrettävä tallennusväline, kuten USB flash -asema tai verkkoasema, jotta salasanat olisivat suojassa myös kiintolevyn vikaantuessa.

Tärkeitä huomautuksia:

- Merkitse arkiston sijainti muistiin, sillä käyttäjä tarvitsee sijaintitietoa tunnistetietojen palauttamiseen.
- Merkitse tunnistetietojen varmuuskopion salasana muistiin, jotta tiedot voidaan palauttaa. Tämä on erittäin tärkeää, sillä salasanaa ei voi palauttaa.
- Jos et tiedä TPM-omistajan salasanaa, ota yhteyttä järjestelmän pääkäyttäjään tai katso lisätietoja tietokoneen TPM-asennusohjeista.

Tunnistetietojen palauttaminen

Voit palauttaa tunnistetiedot seuraavalla tavalla:

- Määritä, palautetaanko vain omat vai järjestelmän kaikkien käyttäjien tunnistetiedot.
- Selaa arkistointisijaintiin ja valitse arkistotiedosto.
- Anna tunnistetietojen varmuuskopion salasana, joka luotiin arkistoinnin yhteydessä.
- Kirjaudu suojauslaitteeseen antamalla järjestelmän (Windowsin käynnistystä edeltävä) salasana, ControlVault-pääkäyttäjän salasana ja TPM-omistajan salasana.

HUOMAUTUKSET:

- Jos näyttöön tulee tunnistetietojen palautuksen epäonnistumisesta ilmoittava virheviesti ja olet yrittänyt palautusta useita kertoja, yritä palauttaa jokin muu arkistotiedosto. Jos tämä ei onnistu, luo uusi tunnistetietojen arkisto ja yritä palauttaa tiedot uudesta arkistosta.
- Jos näyttöön tulee virheilmoitus, joka ilmoittaa, että TPM -avaimia ei voi palauttaa, luo uusi tunnistetietojen arkisto ja tyhjennä sitten TPM BIOS-järjestelmässä. Jos haluat tyhjentää

TPM:n, käynnistä tietokone uudelleen ja paina **F2**-näppäintä käynnistysprosessin aikana, jotta pääset BIOS-asetuksiin. Siirry kohtaan Security (Suojaus)>TPM>Security (TPM-suojaus). Määritä TPM:n omistajuus uudelleen ja yritä sitten palauttaa tunnistetiedot uudelleen.

- Tiettyyn virheviestiin liittyviä lisätietoja on osoitteessa wave.com/support/Dell.

Salasananhallinta

Password Management (Salasananhallinta) -ikkunan avulla pääkäyttäjä voi luoda tai vaihtaa seuraavia järjestelmän suojaussalasanoja:

- järjestelmän (Windowsin käynnistystä edeltävä) salasana*
- pääkäyttäjän salasana*
- kiintolevyn salasana*
- ControlVault-salasana
- TPM-omistajan salasana
- TPM-pääsalasana
- TPM-salasanasäiliön salasana
- itsesalaavan aseman salasana.

HUOMAUTUKSET:

- Sovelluksen näytössä näkyvät vain nykyiseen alustakokoonpanoon soveltuvat salasanat. Ikkunan sisältö perustuu siis järjestelmän kokoonpanoon ja tilaan.
- Salasanat, joiden vieressä on tähtimerkintä (*), ovat BIOS-salasanoja. Kyseisiä salasanoja voi vaihtaa myös järjestelmän BIOSin kautta.
- BIOS-tason salasanoja ei voi luoda tai vaihtaa, jos BIOS-pääkäyttäjä on estänyt salasanojen vaihtamisen.
- Itsesalaavan aseman **setup** (asetukset) -linkin napsauttaminen käynnistää ohjatun Self-Encrypting Drive Setup Wizard -asetustoiminnon. Napsauttamalla **manage** (hallitse) -linkkiä käyttäjä voi vaihtaa yhtä tai useampaa itsesalaavan aseman salasanaa.
- TPM-salasanasäiliön **manage** (hallitse) -linkin napsauttaminen avaa näyttöön ikkunan, jonka kautta voidaan tarkastella tai vaihtaa TPM-avaimia suojaavia salasanoja. Jos TPM-avain edellyttää salasanan luomista, salasana luodaan satunnaisesti ja tallennetaan salasanasäiliöön. TPM-salasanasäiliötä ei voi hallita ennen TPM-pääsalasanan luomista.

Windows-salasanan muodostussäännöt

Dell Data Protection | Access -sovellus varmistaa, että seuraavat salasanat ovat Windowsin salasanasääntöjen mukaisia:

- TPM-omistajan salasana

Tietokoneen Windows-salasanan säännöt voi määrittää seuraavasti:

1. Avaa Ohjauspaneeli.
2. Kaksoisnapsauta Valvontatyökalut-kuvaketta.
3. Kaksoisnapsauta Paikallinen suojauskäytäntö -kuvaketta.
4. Laajenna Tilikäytännöt ja valitse Salasanakäytäntö.

Devices (Laitteet) -ikkunan yleiskatsaus

Devices (Laitteet) -ikkunan avulla pääkäyttäjät voivat hallita kaikkia järjestelmään asennettuja suojauslaitteita. Ikkunan avulla voidaan tarkastella kunkin laitteen tilaa ja laitteeseen liittyviä lisätietoja, kuten laitteen laiteohjelmistoversiota. Saat näkyviin laitteita koskevat lisätiedot valitsemalla **show** (näytä). Voit piilottaa tiedot valitsemalla **hide** (piilota). Alustan mukaan hallittavissa olevia laitteita ovat seuraavat:

Trusted Platform Module (TPM)
ControlVault®
SED-asema(t)
Todennuslaitetiedot

Trusted Platform Module (TPM)

TPM-turvapiiri on otettava käyttöön ja TPM-omistajuus on määritettävä, jotta **Dell Data Protection | Access** -sovelluksen ja TPM-turvapiirin laajennettuja tietoturvaominaisuuksia voidaan käyttää.

Device Management (Laitehallinta) -näytön Trusted Platform Module -ikkuna on näkyvissä vain, jos järjestelmässä havaitaan TPM -turvapiiri.

TPM Management (TPM-hallinta)

Seuraavien toimintojen avulla järjestelmän pääkäyttäjä voi hallita TPM-turvapiiriä.

Status (Tila)
Näyttää, onko TPM:n tila aktiivinen (*active*) vai passiivinen (*inactive*). Aktiivinen tila tarkoittaa, että TPM on otettu käyttöön BIOS-asetuksista ja sen omistajuus voidaan määrittää. TPM-turvapiiriä ei voi hallita eikä sen tietoturvaominaisuuksia voi käyttää, jos TPM ei ole aktiivinen (käytössä).

Jos järjestelmässä havaitaan TPM, mutta se ei ole aktiivinen (käytössä), voit ottaa TPM:n käyttöön avaamatta BIOS-järjestelmää napsauttamalla tässä ikkunassa näkyvää **activate** (ota käyttöön) -linkkiä. Kun TPM on otettu käyttöön tämän toiminnon avulla, tietokone on käynnistettävä uudelleen. Uudelleen käynnistämisen aikana näyttöön saattaa tulla ikkuna, jossa pyydetään hyväksymään muutokset.

HUOMAUTUS: TPM:n aktivointitoiminto sovelluksen avulla ei välttämättä ole käytettävissä kaikissa alustoissa. Jos toiminto ei ole käytettävissä, TPM on otettava käyttöön järjestelmän BIOS-asetuksista. Voit tehdä tämän käynnistämällä tietokoneen uudelleen ja painamalla **F2**-näppäintä ennen Windowsin käynnistymistä, jolloin BIOS -asetukset avautuvat näyttöön. Avaa BIOSissaSecurity (Suojaus)>TPM Security (TPM-suojaus) ja ota TPM käyttöön.

Voit myös *poistaa käytöstä* TPM-turvapiirin napsauttamalla **deactivate** (poista käytöstä) -linkkiä. Jos TPM poistetaan käytöstä, laajennetut tietoturvaominaisuudet eivät ole käytettävissä. TPM:n poistaminen käytöstä ei kuitenkaan muuta TPM-asetuksia tai poista tai muuta TPM-turvapiiriin tallennettuja tietoja tai avaimia.

Owned (Omistettu)
Näyttää omistajuuden tilan (esim. omistettu). Toiminnon avulla voidaan myös määrittää TPM-omistaja tai vaihtaa omistajaa. TPM-omistajuus on määritettävä, jotta tietoturvaominaisuudet ovat käytettävissä. TPM on otettava käyttöön (aktivoitava) ennen omistajuuden määrittämistä.

Omistajuuden määrittämisprosessin aikana käyttäjä (jolla on pääkäyttäjän oikeudet) luo TPM-omistajan salasanan. Kun tämä salasana on määritetty, omistajuus määritetään ja TPM on käyttövalmis.

HUOMAUTUS: TPM-omistajan salasanan on noudatettava järjestelmän Windows-salasanan muodostussääntöjä.

Tärkeää! Älä hävitä tai unohda TPM-omistajan salasanaa, sillä sitä tarvitaan **Dell Data Protection | Access** -sovelluksessa TPM:n laajennettujen tietoturvatoimintojen käyttämiseen.

Locked (Lukittu)
Näyttää, onko TPM:n tila *lukittu* vai *lukitsematon*. Lukitseminen on TPM:n tietoturvaominaisuus. TPM siirtyy lukittuun tilaan, kun TPM-omistajan salasana on annettu väärin määritetyn monta kertaa. TPM-omistaja voi poistaa TPM:n lukituksen tästä ikkunasta. Lukituksen poistaminen edellyttää TPM-omistajan salasanaa.

HUOMAUTUKSET:

- Jos näyttöön tulee virheviesti, joka ilmoittaa, että TPM-omistajuutta ei voi määrittää, tyhjennä TPM järjestelmän BIOS-asetuksista ja yritä määrittää omistajuus uudelleen. Jos haluat tyhjentää TPM:n, käynnistä tietokone uudelleen ja paina **F2**-näppäintä käynnistysprosessin aikana, jotta pääset BIOS-asetuksiin. Siirry kohtaan Security (Suojaus) > TPM Security (TPM-suojaus).
- Jos näyttöön tulee virheviesti, joka ilmoittaa, että TPM-omistajan salasanaa ei voi muuttaa, arkistoi TPM-tiedot (tunnistetietojen arkistointi), tyhjennä TPM järjestelmän BIOSin kautta, määritä TPM-omistajuus uudelleen ja palauta TPM-tiedot (palauta tunnistetiedot).
- Tiettyyn virheviestiin liittyviä lisätietoja on osoitteessa wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) on suojattu tallennuspaikka Windowsin käynnistystä edeltävien tunnistetietojen tallentamista varten (esim. käyttäjäsalasanat tai sormenjälkitiedot). **Device Management** (Laitehallinta) -näytön ControlVault-ikkuna on näkyvissä vain, jos järjestelmässä havaitaan ControlVault .

ControlVault Management (ControlVault-hallinta)

Seuraavien toimintojen avulla järjestelmänvalvoja voi hallita järjestelmän ControlVault-toimintoa.

Status (Tila)
Näyttää, onko ControlVaultin tila aktiivinen (*active*) vai passiivinen (*inactive*). Passiivinen tila tarkoittaa, että ControlVault ei ole käytettävissä järjestelmässä tallennusta varten. Tarkista Dell-järjestelmän dokumentaatiosta, onko järjestelmässä ControlVault-ominaisuutta.

Password (Salasana)
Osoittaa, onko määritetty. Toiminnon avulla voidaan asettaa salasana tai vaihtaa salasanaa (jos salasana on jo asetettu). Ainoastaan järjestelmän pääkäyttäjät voivat asettaa tai vaihtaa tätä salasanaa. ControlVault-pääkäyttäjän salasana tarvitaan seuraavien toimintojen tekemiseen:

- tunnistetietojen arkistoimiseen tai palauttamiseen
- kaikkien käyttäjien käyttäjätietojen tyhjentämiseen.

HUOMAUTUS: Jos tietoja yritetään arkistoida tai palauttaa, mutta ControlVault-pääkäyttäjän salasanaa ei ole määritetty, käyttäjä saa kehotteen luoda kyseinen salasana (jos käyttäjä on pääkäyttäjä).

Enrolled Users (Rekisteröidyt käyttäjät)
Osoittaa, onko käyttäjillä rekisteröityjä kirjautumistunnistetietoja (kuten salasanoja ja sormenjälki- tai älykorttitietoja), jotka on tallennettu ControlVaultiin.

Clear User Data (Tyhjennä käyttäjätiedot)
ControlVaultin sisältämät tiedot on ehkä tyhjennettävä joissakin tilanteissa, esimerkiksi, jos käyttäjillä on vaikeuksia käyttää tai rekisteröidä Windowsin käynnistystä edeltävän todennuksen tunnistetietoja. Kaikki ControlVaultiin tallennetut (yhden käyttäjän tai kaikkien käyttäjien) tiedot voidaan tyhjentää tästä ikkunasta.

ControlVault-pääkäyttäjän salasana on annettava, jotta alustan kaikkien käyttäjien tiedot voidaan tyhjentää. Järjestelmä pyytää antamaan myös järjestelmän (Windowsin käynnistystä edeltävän) salasanan, jos Windowsin käynnistystä edeltäviä tunnistetietoja on rekisteröity. Kun kaikkien käyttäjien tiedot tyhjennetään, ControlVault-pääkäyttäjän salasana ja järjestelmän salasana palautetaan. Huomaa, että tämä on ainoa tapa tyhjentää ControlVault-pääkäyttäjän salasana.

HUOMAUTUS: Kun kaikki käyttäjätiedot on tyhjennetty, järjestelmä kehottaa käynnistämään tietokoneen uudelleen. Tietokone on käynnistettävä uudelleen, jotta järjestelmä toimii oikein.

ControlVault-pääkäyttäjän salasanaa ei tarvitse määrittää, jos halutaan tyhjentää vain yhden käyttäjän tunnistetiedot. Kun valitset **clear user data** (tyhjennä käyttäjätiedot), järjestelmä pyytää valitsemaan käyttäjän, jonka ControlVault-tunnistetiedot halutaan tyhjentää. Kun käyttäjä on valittu, järjestelmä pyytää järjestelmän salasanaa (vain jos Windowsin käynnistystä edeltäviä tunnistetietoja on rekisteröity).

HUOMAUTUKSET:

- Jos näyttöön tulee virheilmoitus, ettei ControlVault-järjestelmänvalvojan salasanaa voi luoda, arkistoi tunnistetiedot ja tyhjennä kaikki käyttäjätiedot ControlVaultista. Käynnistä tietokone sitten uudelleen ja yritä luoda salasana uudelleen.
- Jos näyttöön tulee virheilmoitus, ettei tietyn käyttäjän tunnistetietoja voi tyhjentää ControlVaultista, arkistoi tunnistetiedot ja yritä tyhjentää kaikkien käyttäjien tiedot. Yritä sitten tyhjentää tietyn käyttäjän tiedot uudelleen.
- Jos näyttöön tulee virheilmoitus, ettei kaikkien käyttäjien tietoja voi tyhjentää ControlVaultista, kannattaa harkita järjestelmän palautusta. **Tärkeää!** Tutustu ohjeen Järjestelmän palautus -aiheeseen ennen järjestelmän palauttamista, sillä palautustoiminto tyhjentää KAIKKI käyttäjien suojaustiedot.
- Jos näyttöön tulee virheilmoitus, ettei ControlVault- ja TPM-tietoja voi varmuuskopioida, poista TPM käytöstä järjestelmän BIOSin kautta. Tämä tehdään käynnistämällä tietokone uudelleen ja painamalla **F2**-näppäintä tietokoneen käynnistymisen aikana, jolloin BIOS-asetukset avautuvat näyttöön. Avaa BIOSissa Security (Suojaus) > TPM Security (TPM-suojaus). Ota TPM käyttöön uudelleen ja yritä arkistoida ControlVault-tiedot uudelleen.
- Tiettyyn virheviestiin liittyviä lisätietoja on osoitteessa wave.com/support/Dell.

Itsesalaavat asemat: Lisäasetukset

Dell Data Protection |Access -sovellus hallitsee sisäänrakennettuja tietojensalausominaisuuksia sisältävien itsesalaavien asemien laitteistopohjaisia suojaustoimintoja. Aseman hallinnalla voidaan varmistaa, että vain luvan saaneet käyttäjät voivat käyttää salattuja tietoja (kun aseman lukitus on käytössä).

Self-Encrypting Drive (Itsesalaava asema) -ikkuna näkyy **Device Management** (Laitehallinta) -näytössä vain, jos järjestelmään on liitetty vähintään yksi itsesalaava asema (SED-asema).

Tärkeää! Kun asema on määritetty, itsesalaavan aseman tietojen suojaus ja aseman lukitus ovat käytössä.

Drive Management (Aseman hallinta)
Tämän osion toimintojen avulla aseman pääkäyttäjä voi hallita aseman tietoturva-asetuksia. Aseman tietoturva-asetusten muutokset tulevat voimaan sen jälkeen, kun aseman virta on katkaistu.

Data Protection (Tietojen suojaus)
Näyttää itsesalaavan aseman tietojen suojauksen tilan: *enabled* (käytössä) tai *disabled* (poistettu käytöstä). Käytössä-tila tarkoittaa, että aseman suojaus on määritetty. Käyttäjien ei kuitenkaan tarvitse tunnistautua asemaan Windowsin käynnistustä edeltävässä kirjautumisessa, ennen kuin aseman *lukitus* on otettu käyttöön.

Voit poistaa itsesalaavan aseman tietojen suojauksen tästä ikkunasta. Kun tietojen suojaus poistetaan käytöstä, kaikki itsesalaavan aseman laajennetut suojaustoiminnot poistetaan käytöstä ja asema toimii kuin tavallinen asema. Tietojen suojauksen poistaminen käytöstä poistaa kaikki tietoturva-asetukset, mukaan lukien aseman pääkäyttäjien ja käyttäjien tunnistetiedot. Tämä toiminto ei kuitenkaan muuta tai poista mitään asemassa olevia käyttäjien tietoja.

Locking (Lukitus)
Näyttää itsesalaavan aseman lukituksen tilan: *enabled* (käytössä) tai *disabled* (poistettu käytöstä). Lisätietoja aseman lukitustoiminnosta on aiheessa Itsesalaava asema.

Jos aseman lukitus on jostain syystä poistettava käytöstä, se voidaan tehdä tästä ikkunasta. Lukituksen poistaminen ei ole suositeltavaa, sillä kun lukitus on poistettu, asemaan kirjautuminen ei edellytä tunnistetietojen antamista, joten kaikki alustan käyttäjät voivat käyttää aseman tietoja. Aseman lukituksen poistaminen käytöstä eipoista tietoturva-asetuksia, kuten aseman pääkäyttäjän ja käyttäjien tunnistetietoja eikä aseman sisältämiä käyttäjien tietoja.

VAROITUS! Jos poistat **Dell Data Protection | Access** -sovelluksen asennuksen, itsesalaavan aseman tietojen suojaus ja aseman lukitus on ensin poistettava käytöstä.

Drive Administrator (Aseman pääkäyttäjä)

Näyttää nykyisen aseman pääkäyttäjän. Aseman pääkäyttäjä voi tästä kohdasta määrittää uuden aseman pääkäyttäjän. Uuden pääkäyttäjän on oltava sallittu Windows-käyttäjä, jolla on järjestelmän pääkäyttäjän oikeudet. Järjestelmässä voi olla vain yksi aseman pääkäyttäjä.

Drive Users (Aseman käyttäjät)

Näyttää rekisteröidyt aseman käyttäjät ja nykyisten rekisteröityjen käyttäjien määrän. Tuettujen käyttäjien enimmäismäärä riippuu itsesalaavasta asemasta (nykyisin neljä käyttäjää Seagate-asemissa ja 24 käyttäjää Samsung-asemissa).

Windowsin salasanan synkronointi

Windowsin salasanan synkronointitoiminto (WPS) määrittää käyttäjien itsesalaavan aseman salasanat automaattisesti samoiksi kuin heidän Windows-salasanansa. Toiminnon ei tarvitse koskea aseman pääkäyttäjää, vaan ainoastaan aseman käyttäjiä. WPS-toiminnallisuutta voidaan käyttää yritysympäristöissä, joissa salasanoja on vaihdettava tietyin välein (esimerkiksi 90 päivän välein). Kun toiminto on käytössä, käyttäjien itsesalaavan aseman salasanat päivittyvät automaattisesti, kun Windows-salasanoja vaihdetaan.

HUOMAUTUS: Kun Windowsin salasanan synkronointi (WPS-toiminto) on käytössä, käyttäjän itsesalaavan aseman salasanaa ei voi vaihtaa. Tällöin itsesalaavan salasanan voi päivittää vain vaihtamalla Windows-salasanan.

Remember Last Username (Muista edellinen käyttäjätunnus)

Kun tämä asetus on käytössä, viimeiseksi annettu käyttäjätunnus näkyy oletusarvoisesti Windowsin käynnistystä edeltävän tunnistautumisnäytön **Username** (Käyttäjätunnus) -kentässä.

Username Selection (Käyttäjätunnuksen valinta)

Kun tämä asetus on käytössä, käyttäjät voivat tarkastella kaikkia aseman käyttäjätunnuksia Windowsin käynnistystä edeltävän tunnistautumisnäytön **Username** (Käyttäjätunnus) -kentässä.

Cryptographic Erase (Salauksen poisto)

Tämän asetuksen avulla kaikki itsesalaavan aseman tiedot voidaan "poistaa". Tietoja ei itse asiassa poisteta, mutta tietojen salaamiseen käytetyt avaimet poistetaan, joten tietoja ei voi käyttää. Salauksen poiston jälkeen aseman tietoja ei voi palauttaa. Salauksen poisto poistaa käytöstä myös itsesalaavan aseman tietojen suojauksen, ja asema on valmis uutta käyttötarkoitusta varten.

HUOMAUTUKSET:

- Jos näyttöön tulee itsesalaavan aseman hallintatoimintoihin liittyviä virheilmoituksia, katkaise tietokoneen virta täysin (älä valitse uudelleenkäynnistystä) ja käynnistä tietokone sitten uudelleen.
- Tiettyyn virheviestiin liittyviä lisätietoja on osoitteessa wave.com/support/Dell.

Todennuslaitetiedot

Device Management (Laitehallinta) -kohdan Authentication Device Information (Todennuslaitetiedot) -ikkunassa näkyvät kaikkien järjestelmään liitetyjen todennuslaitteiden (kuten sormenjälkilukijan, perinteisen tai etäluettavan älykortinlukijan) tiedot ja tila.

Tekninen tuki

Dell Data Protection | Access -ohjelmistoa koskevia teknisiä tukitietoja on osoitteessa http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP -ohjelma

Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) -ohjelma on osa **Dell Data Protection | Access** -sovellusta, ja se on käytettävissä aina, kun CSP-palvelua tarvitaan. Ohjelma voidaan avata suoraan sovelluksesta tai valita asennettujen CSP-ohjelmien luettelosta. Jos mahdollista, valitse "Wave TCG-Enabled CSP". Näin varmistat, että TPM luo avaimet ja että **Dell Data Protection | Access** hallinnoi avaimia ja niiden salasanoja.

Wave Systems TCG-Enabled CSP:n avulla sovellukset voivat käyttää TCG-yhteensopivien alustojen käytettävissä olevia toimintoja suoraan MSCAPI:n kautta. Kyseessä on TCG-ominaisuuksia sisältävä MSCAPI CSP -moduuli, joka mahdollistaa asymmetriset avaintoiminnot TPM:ssä ja parantaa TPM:n sisältämiä suojausominaisuuksia riippumatta siitä, mitkä Trusted Software Stack (TSS) -toimittajaa koskevat ohjelmistotoimittajan vaatimukset ovat.

HUOMAUTUS: Jos Wave TCG-enabled CSP -ohjelman luomat TPM-avaimet edellyttävät salasanaa ja käyttäjä on luonut TPM-pääsalasanan, yksittäiset avainsalasanat luodaan satunnaisesti ja tallennetaan TPM-salasanasäiliöön.