HP Client Security

Alustamine

Esimene väljaanne: august 2013

Dokumendi number: 735339-E41

Sisukord

1 Klienditurbesüsteemi HP Client Security Manager tutvustus

HP Client Security võimaldab teil kaitsta oma teavet, seadet, identiteeti, tõstes selleks teie arvuti turvalisust.

Arvutile mõeldud tarkvaramoodulid võivad erineda sõltuvalt arvutimudelist.

HP Client Security tarkvaramoodulid on võimalik eelinstallida ja eellaadida või allalaadida HP veebilehelt. Lisateavet leiate jaotisest http://www.hp.com.

MÄRKUS. Käesolevas juhendis antud juhised on toodud eeldusel, et olete juba installinud saadaolevad HP Client Security tarkvaramoodulid.

HP Client Security funktsioonid

Järgnevas tabelis on täpsemalt kirjeldatud HP Client Security moodulite põhifunktsioone.

Moodul	Põhifunktsioonid
Klienditurbesüsteem HP Client Security	Haldurid saavad sooritada järgmisi funktsioone: • kaitsta arvutit enne Windows®-i käivitumist; • kaitsta oma Windowsi kontot tugeva autentimise abil; • hallata oma veebisaitide ja rakenduste sisselogimisandmeid ja paroole; • muuta hõlpsasti Windowsi operatsioonisüsteemi parooli; • kasutada lisaturvalisuse ja mugavuse tagamiseks sõrmejälge; • määrata autentimiseks kiipkaardi, kontaktivaba kaardi või viipekaardi; • kasutada identifitseerimiseks oma Bluetooth-telefoni; • määrata oma autentimisvalikute laiendamiseks PIN-i; • konfigureerida sisselogimis- ja seansipoliitikat; • varundada ja taastada oma programmiteavet; • lisada täiendavaid rakendusi, näiteks HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager ja HP Computrace. Tavakasutajad saavad sooritada järgmisi funktsioone: • Vaadata krüptimisoleku ning Device Access Manageri seadeid. • Aktiveerida rakenduse Computrace. • Konfigureerida eelistusi ning varundamise ja taastamise suvandeid.

Moodul	Põhifunktsioonid
Password Manager	Tavakasutajad saavad sooritada järgmisi funktsioone: • Korraldada ning häälestada kasutajanimesid ja paroole. • Luua täiustatud turbeks tugevamaid paroole e-posti kontodele ja veebikontodele. Password Manager sisestab ning edastab teabe automaatselt. • Muuta sisselogimisprotsessi sujuvamaks ühekordse sisselogimise funktsiooni abil, mis peab kasutajamandaadi meeles ja kasutab seda automaatselt. • Konto märkimiseks kahtlasena, et saada teavitus teistest sarnaste mandaatidega kontodest. • Sisselogimisandmete importimiseks toetatud brauserist.
HP Drive Encryption (ainult teatud mudelitel)	• Võimaldab kõvaketta täieliku krüptimise. • Rakendab andmete dekrüptimiseks ja nendele ligipääsemiseks buudieelse autentimise. • Pakub võimaluse aktiveerida draivide isekrüptimine (ainult teatud mudelitel).
HP Device Access Manager	• Võimaldab IT halduritel kontrollida ligipääsu kasutajaprofiilidel põhinevatele seadmetele. • Takistab volitamata kasutajatel andmete eemaldamise väliselt salvestuskandjalt ning viiruste kandumise väliselt salvestuskandjalt süsteemi. • Võimaldab halduritel keelata teatud üksikkasutajate või kasutajarühmade ligipääs sideseadmetele.
HP Trust Circles	• Tagab failide ja dokumentide turvalisuse. • Krüptib faile, mis asuvad kasutajapõhistes kaustades, andes neile usaldusringi kaitse. • Võimaldab failide kasutamise ja jagamise üksnes usaldusringis olevate liikmete vahel.
Theft Recovery (Computrace eraldi ostetav)	• Aktiveerimiseks on vajalik eraldi ostetav jälgimise ja jälitamise tellimine. • Võimaldab üksuse turvalist jälgimist. • Jälgib kasutajaaktiivsust, samuti riistvara ja tarkvara muutusi. • Püsib aktiivsena isegi siis, kui kõvaketas on ümber vormindatud või asendatud.

Klienditurbesüsteemi HP Client Security tootekirjeldus ja üldised näited selle kasutamiseks

Enamikel HP Client Security toodetel on nii kasutaja autentimise (tavaliselt parool) kui ka halduslikku varunduse võimalus, et ligipääs oleks võimalik ka siis, kui paroolid on kadunud, ei ole kättesaadavad, on ununenud või vajalikud ettevõtte turvalisuse tõttu.

MÄRKUS. Mõned HP Client Security klienditurbesüsteemi tooted on kujundatud andmetele ligipääsu piiramiseks. Andmed peavad olema krüptitud juhul, kui nad on niivõrd olulised, et kasutaja pigem kaotaks selle teabe, kui laseks sellel ohtu sattuda. Soovitav on kõik andmed varundada turvalisse kohta.

Password Manager

Password Manager talletab kasutajanimed ja paroolid ja seda on võimalik kasutada:

- Sisselogimisnimede ja paroolide salvestamiseks, et pääseda Internetti või e-postkasti.
- Kasutaja automaatseks sisselogimiseks veebilehele või e-postkasti.
- Autentimise haldamiseks ja korraldamiseks.
- Valige lingile otse juurdepääsuks veebi- või võrguüksus.
- Vajadusel nimede ja paroolide vaatamiseks.
- Konto märkimiseks kahtlasena, et saada teavitus teistest sarnaste mandaatidega kontodest.
- Sisselogimisandmete importimiseks toetatud brauserist.

Esimene näide: Suure tootja ostuagent teeb suure osa oma äritehingutest Interneti kaudu. Ta külastab tihti populaarseid veebilehekülgi, mis nõuavad logimisteavet. Ta on turvalisusest vägagi teadlik, seega ta ei kasuta iga konto jaoks sama parooli. Ostuagent on otsustanud Password Manageri abil siduda veebilehed erinevate kasutajanimede ja paroolidega. Kui ta avab sisselogimiseks veebilehe, pakub Password Manager mandaadi automaatselt. Kui ta soovib näha kasutajanimesid ja paroole, on võimalik Password Manager konfigureerida neid kuvama.

Password Manageri saab kasutada autentimise haldamiseks ja korraldamiseks. See tööriist võimaldab kasutajal lingile otse juurdepääsuks valida veebi- või võrguüksus. Samuti saab kasutaja vajadusel näha nimesid ja paroole.

Teine näide: Töökas töötaja on edutatud ning haldab nüüd kogu raamatupidamisosakonda. Meeskond peab sisse logima paljude klientide veebikontodesse ning kõikide kontode logimisteave on erinev. Logimisteavet tuleb jagada kõikide töötajatega, seega tähtis on konfidentsiaalsus. Töötaja otsustab veebilingid, ettevõtte kasutajanimed ja paroolid organiseerida Password Manageri abil. Kui see on tehtud, juurutab töötaja teised Password Manageri kasutama nii, et nad saavad töötada veebikontodega, kui ei tea, millist sisselogimismandaati nad kasutavad.

HP Drive Encryption (ainult teatud mudelitel)

Krüpteerimistarkvara HP Drive Encryptioni kasutatakse andmetele ligipääsu piiramiseks kogu arvuti kõvakettal või lisadraivil. Drive Encryption haldab ka isekrüptivaid draive.

Esimene näide: Arst tahab olla kindel, et ainult tema pääseb ligi oma arvuti kõvakettal olevatele andmetele. Arst aktiveerib Drive Encryptioni, mis vajab enne Windowsi sisselogimist buudieelset autentimist. Kui Drive Encryption on häälestatud, ei ole kõvakettale võimalik ligipääseda ilma paroolita enne, kui operatsioonisüsteem käivitub. Arstil on võimalik veelgi draivi turvalisust suurendada, valides andmete krüptimiseks draivi isekrüptimise võimaluse.

Teine näide: Haigla haldur soovib olla kindel, et üksnes arstid ning volitatud töötajad pääseksid andmetele ligi oma kohalikest arvutitest, ilma et nad peaksid jagama oma isiklikke paroole. IT osakond lisab halduri, arstid ning kõik volitatud töötajad Drive Encryptioni kasutajate hulka. Nüüd saavad üksnes volitatud töötajad arvuti või domeeni algkäivitada, kasutades selleks oma isikliku kasutajanime ja parooli.

HP Device Access Manager (ainult teatud mudelitel)

HP Device Access Manager võimaldab halduril piirata ja hallata ligipääsu riistvarale. Device Access Manageri saab kasutada volitamata ligipääsu blokeerimiseks USB-mälupulkadele, kuhu on võimalik andmeid kopeerida. Samuti saab seda kasutada ligipääsu piiramiseks CD/DVD-draividele, USB-seadmete ning võrguühenduste kontrolliks jne. Näiteks on olukord, kus välised tarnijad vajavad ligipääsu ettevõtte arvutitele, kui ei peaks saama kopeerida andmeid USB-draivile.

Esimene näide: Meditsiinitarvikutega tegeleva ettevõtte juhataja puutub oma töös lisaks ettevõttega seotud teabele tihti kokku ka isiklike haiguslugudega. Töötajatel on vajalik ligipääs nendele andmetele, kui on üliloluline, et neid andmeid ei eemaldata arvutist USB-draivile või teistele välistele salvestuskandjatele. Võrk on turvaline, kuid arvutitel on CD-kirjutid ja USB-pordid, mis võimaldavad andmete kopeerimist või varastamist. Juhataja kasutab Device Access Manageri, et keelata USB-pordid ja CD-kirjutid nii, et neid pole võimalik kasutada. Kuigi USB-pordid on blokeeritud, siis hiir ja klaviatuur töötavad.

Teine näide: Kindlustuskompanii ei soovi, et töötajad installiksid või laadiksid isiklikku tarkvara või andmeid koduarvutist. Mõned töötajad vajavad ligipääsu kõikide arvutite USB-portidele. IT-haldur kasutab Device Access Manageri, et võimaldada teatud töötajatele ligipääs ning takistada teistele ligipääs väljastpoolt.

Computrace (eraldi ostetav)

Computrace (eraldi ostetav) on teenus, mille abil on võimalik jälgida varastatud arvuti asukohta iga kord, kui kasutaja siseneb Internetti. Computrace aitab arvuteid eemalt hallata ja otsida, samuti jälgida arvuti ning rakenduste kasutamist.

Esimene näide: Koolidirektor palus IT-osakonnal jälgida kõiki koolis olevaid arvuteid. Kui arvutite inventuur oli tehtud, registreeris IT haldur kõik arvutid, kasutades selleks Computrace teenust nii, et arvuteid on võimalik jälitada juhul, kui need kunagi varastatakse. Hiljuti avastas kool, et mitu arvutit on kadunud ning IT haldur teavitas sellest ametkondi ja Computrace töötajaid. Arvutite asukoht tehti ametnike poolt kindlaks ning arvutid tagastati koolile.

Teine näide: Kinnisvaraettevõte tahab hallata ja värskendada arvuteid üle kogu maailma. Nad kasutavad arvutite jälgimiseks ja värskendamiseks Computrace teenust ning ei pea saatma IT haldurit iga arvuti juurde.

Peamiste turbe eesmärkide saavutamine

HP Client Security mooduleid saab kasutada koos, et leida lahendused erinevatele turbeprobleemidele, sealhulgas järgmiste peamiste turbe eesmärkide saavutamiseks:

- Kaitse sihipärase varguse vastu
- Juurdepääsu piiramine tundlikele andmetele
- Volitamata juurdepääsu takistamine välistelt või sisemistelt asukohtadelt
- Tugeva paroolipoliitika loomine

Kaitse sihipärase varguse vastu

Näide sihipärasest vargusest on konfidentsiaalseid andmeid ja klienditeavet sisaldava arvuti vargus lennujaama turvakontrollis. Sihipärase varguse vastu annavad kaitse järgnevad funktsioonid:

- Kui buudieelne autentimine on lubatud aitab see takistada ligipääsu operatsioonisüsteemile.
  - HP Client Security — vt Klienditurbesüsteem HP Client Security lk 12.
  - HP Drive Encryption — vt HP Drive Encryption (ainult teatud mudelitel) lk 29.
- Krüptimine ei võimalda andmetele juurde pääseda isegi siis, kui kõvaketas on eemaldatud ja installitud ebaturvalisse süsteemi.
- Computrace abil saab jälitada arvuti asukoha peale vargust.
  - Computrace — vt Theft recovery (ainult teatud mudelitel) lk 51.

Juurdepääsu piiramine tundlikele andmetele

Lepinguline audiitor töötab kohapeal ning talle on antud ligipääs tundlike finantsandmete vaatamiseks arvutis. Te ei soovi, et audiitor saaks faile printida või salvestada neid kirjutatavale seadmele, näiteks CD-le. Järgnev funktsioon aitab piirata ligipääsu andmetele:

- HP Device Access Manager võimaldab IT-halduritel piirata ligipääsu sideseadmetele nii, et tundlikku teavet pole võimalik kõvakettale kopeerida. Vt Süsteemivaade lk 42.

Volitamata juurdepääsu takistamine välistelt või sisemistelt asukohtadelt.

Volitamata juurdepääs ebaturvalistele äriarvutitele kujutab endast vägagi reaalset ohtu ettevõtte võrgu ressurssidele, näiteks teave finantsosakonnalt, juhatuselt või teadus- ja arendustegevuse meeskonnalt ja salajasele teabele, näiteks patsientide andmed või isiklikud finantsandmed. Järgnev funktsioon aitab takistada volitamata ligipääsu:

- Kui buudieelne autentimine on lubatud aitab see takistada ligipääsu operatsioonisüsteemile. (vt HP Drive Encryption (ainult teatud mudelitel) lk 29.
- HP Client Security aitab tagada, et volitamata kasutaja ei saa kätte paroole ning ei pääse ligi parooliga kaitstud rakendustele. Vt Klienditurbesüsteem HP Client Security lk 12.
- HP Device Access Manager võimaldab IT-halduritel piirata ligipääsu kirjutatavatele seadmetele nii, et tundlikku teavet pole võimalik kõvakettale kopeerida. Vt HP Device Access Manager (ainult teatud mudelitel) lk 41.

Tugeva paroolipoliitika loomine

Kui ettevõte rakendab poliitikat, mis nõuab tugevat paroolipoliitikat tuhandetele veebipõhistele rakendustele ja andmebaasidele, siis Password Manager tagab paroolide kaitstud hoidla ja mugava ühekordse sisselogimise. Vt Password Manager lk 18.

Täiendavad turvaelemendid

Turberollide määramine

Arvuti turvalisuse haldamisel (eriti suurtes organisatsioonides) on üks oluline tava jaotada vastutused ja õigused erinevat tüüpi haldurite ja kasutajate vahel.

MÄRKUS. Väikeses organisatsioonis või isikliku kasutamise korral võib neid rolle täita üks ja seesama inimene.

HP Client Security puhul saab turbekohustused ja privileegid jagada järgmistesse rollide vahel:

- Turbeametnik - määrab ettevõtte või võrgu turbetaseme ning otsustab, millised turbefunktsioone näiteks Drive Encryption, juurutada.

MÄRKUS. Turbeametnik saab koostöös HP-ga kohandada mitmeid HP Client Security funktsioone saab funktsioone. Lisateavet leiate jaotisest http://www.hp.com.

- IT-haldur - rakendab ning haldab turbeametniku poolt määratud turbefunktsioone. IT-haldur saab teatud funktsioone lubada ja keelata. Näiteks, kui turbeametnik on otsustanud juurutada kiipkaardid, saab IT-haldur lubada nii paroolirežiimi kui ka kiipkaardi režiimi.
- Kasutaja - kasutab turbefunktsioone. Näiteks juhul, kui turbeametnik ja IT-haldur on lubanud süsteemis kiipkaardid, saab kasutaja seadistada kiipkaardi PIN-koodi ja kasutada kaarti autentimiseks.

ETTEVAATUST. Halduritel on soovitav järgida lõppkasutaja privileegide ja kasutaja juurdepääsu piiramisel nn "häid tavasid".

Volitamata kasutajatele ei tohi olla antud halduri eesõigusi.

HP Client Security Manageri paroolide haldamine

Enamik HP Client Security funktsioonidest on kaitstud paroolidega. Järgnevas tabelis on loetletud enimkasutatavad paroolid, parooliga tarkvaramoodulid ning paroolifunktsioonid.

Samuti on tabelis märgitud paroolid, mille on seadnud ja mida kasutavad üksnes IT-haldurid. Kõiki teisi paroole saavad seada tavakasutajad või haldurid.

HP Client Security parool	Seatud moodulile	Funktsioon
Windowsi sisselogimise parool	Windowsi juhtpaneel või HP Client Security	Võimalik kasutada käsitsi sisselogimiseks ja autentimiseks, et pääseda ligi erinevatele HP Client Security funktsioonidele.
HP Client Security varundamine ja taasteparool	HP Client Security, üksikkasutaja poolt	Kaitseb juurdepääsu HP Client Security varundusele ja taastefailile.
Kiipkaardi PIN-kood	Credential Manager	Võimalik kasutada multiautentimiseks. Võimalik kasutada Windowsi autentimiseks. Autendib Drive Encryptioni kasutajad juhul, kui valitud on kiipkaart.

Turvalise parooli loomine

Parooli loomisel tuleb eelkõige jälgida programmi poolt seatud spetsifikatsioone. Reeglina võtke arvesse järgnevaid näpunäiteid, mis aitavad luua tugevaid paroole ja vähendada parooli ohtusattumise võimalusi.

- Kasutage rohkem kui 6-tähemärgilist, soovitavalt rohkem kui 8-tähemärgilist parooli.
- Kombineerige läbivalt paroolis suurtähti.
- Igal võimalikul juhul kombineerige tähtnumbrilisi koode ja kasutage erimärke ja kirjavahemärke.
- Asendage märksõna tähed erimärkide või numbritega. Näiteks, kasutage number 1 tähtede l või L asemel.

- Kombineerige sõnad kahest või enamast keelest.
- Poolitage sõna või fraas numbrite või erimärkidega keskel, näiteks “Mary2-2Cat45.”
- Ärge kasutage parooli, mis on kirjas sõnaraamatus.
- Ärge kasutage paroolina oma nime või muud isiklikku teavet, näiteks oma sünniaega, lemmikloomade nimesid või ema neiupõlvenime, isegi mitte tagurpidi kirjutades.
- Vahetage parooli regulaarselt. Võite lisada üksnes mõned tähemärgid.
- Kui panete oma parooli kirja, ärge hoidke seda liiga arvuti lähedal üldiselt nähtavas kohas.
- Ärge salvestage parooli arvutis olevas failis, näiteks e-kirjas.
- Ärge jagage kontosid ega öelge kellelegi oma parooli.

Mandaatide varundamine ja sätted

HP Client Security varundus- ja taastetööriista saab kasutada keskse kohana, kus varundada ja taastada installitud HP Client Security moodulite turbemandaate.

2 Alustamine

HP Client Security konfigureerimiseks oma mandaate kasutades käivitage HP Client Security ühel järgmistest viisidest. Kui kasutaja on viisardi läbinud, ei saa sama kasutaja seda enam käivitada.

1. Klõpsake või koputage ava- või rakenduste kuval üksust **HP Client Security** (Windows 8).

   või

   Klõpsake või koputage Windowsi töölaual üksust **HP Client Security Gadget** (Windows 7).

   või

   Topeltklõpsake või topeltkoputage Windowsi töölaua teadete alal ikooni **HP Client Security**, mis asub tegumiriba parempoolses servas.

   või

   Klõpsake või koputage Windowsi töölaua teadete alal ikooni **HP Client Security** ja valige siis üksus **Open HP Client Security** (Ava HP Client Security).

2. Kuvatakse tervitusleheküIg koos HP Client Security häälestusviisardiga.

3. Tutvuge tervituskuvaga, kinnitage oma identiteet Windowsi parooliga ja klõpsake või koputage seejärel valikut **Edasi**.

   Kui te pole veel Windowsi parooli loonud, palutakse teil seda teha. Windowsi parooli läheb tarvis teie Windowsi konto kaitsmiseks volitamata isikute eest ja HP Client Security funktsioonide kasutamiseks.

4. Valige HP SpareKey leheküljel kolm turvaküsimust. Sisestage iga küsimuse vastus ja klõpsake siis **Edasi**. Lubatud on ka kohandatud küsimused. Lisateavet leiate jaotisest HP SpareKey – paroolitaaste lk 14.

5. Registreerige sõrmejälgede lehel minimaalne nõutud hulk sõrmejälgi ja klõpsake või koputage **Edasi**. Lisateavet leiate jaotisest Sõrmejäljed lk 12.

6. Aktiveerige Drive Encryptioni lehel krüptimine, varundage krüptimiskood ja klõpsake või koputage **Edasi**. Lisateavet leiate HP Drive Encryptioni tarkvara spikrist.

   MÄRKUS. See kehtib juhul, kui kasutajal on halduri õigused ja HP Client Security häälestusviisard ei ole halduri poolt hiljuti konfigureeritud.

7. Klõpsake või koputage viisardi viimasel lehel käsku **Valmis**.

   See leht sisaldab funktsioonide ja mandaatide olekut.

8. HP Client Security häälestusviisard tagab rakenduste Just In Time autentimine ja File Sanitizer funktsioonide käivitamise. Lisateavet leiate HP Device Access Manageri tarkvaraspikrist ja HP File Sanitizeri tarkvaraspikrist.

   MÄRKUS. See kehtib juhul, kui kasutajal on halduri õigused ja HP Client Security häälestusviisard ei ole halduri poolt hiljuti konfigureeritud.

HP Client Security avamine

Rakendust HP Client Security võib avada ühel järgmistest viisidest.

MÄRKUS. Enne HP Client Security käivitamist peab HP Client Security häälestusviisard olema lõpetatud.

- Klõpsake või koputage ava- või rakenduste kuval üksust **HP Client Security**.

  või

  Klõpsake või koputage Windowsi töölaual **HP Client Security** vidinat (Windows 7).

  või

  Topeltklõpsake või topeltkoputage Windowsi töölaua teadete alal ikooni **HP Client Security**, mis asub tegumiriba parempoolses servas.

  või

  Klõpsake või koputage Windowsi töölaua teadete alal ikooni **HP Client Security** ja valige siis üksus **Open HP Client Security** (Ava HP Client Security).

3 Lihtne häälestusjuhend väikeettevõtetele

Käesolev peatükk kirjeldab põhilisi samme, kuidas aktiveerida HP Client Security kõige tavalisemad ja kasulikumad funktsioonid väikeettevõtetele. Mitmed selle tarkvara tööriistad ja suvandid võimaldavad viimistleda teie eelistusi ja häälestada juurdepääsu kontrolli. Selle häälestusjuhendi fookuses on iga mooduli käivitamine võimalikult väikse häälestusele kuluva pingutuse ja ajakuluga. Lisateabe saamiseks valige teid huvitav moodul ja klõpsake üleval paremas nurgas olevale **?** või spikrinupule. See nupp kuvab automaatselt abistava teabe hetkel avatud aknas.

Alustamine

1. HP Client Security avamiseks topeltklõpsake Windowsi töölaual tegumiriba parempoolses otsas asuval teavitusalal ikooni **HP Client Security**.
2. Sisestage oma Windowsi parool või looge see.
3. Viige HP Client Security häälestus lõpuni.

Kui soovite, et HP Client Security nõuaks autentimist üks kord Windowsi sisselogimise jooksul, vt Turbefunktsioonid lk 26.

Password Manager

Igaühel on üsna palju paroole - eriti siis, kui pidevalt käia veebilehekülgedel ja kasutada rakendusi, mis nõuavad sisselogimist. Tavakasutaja kasutab sama parooli iga rakenduse või veebilehe jaoks või on loov ning unustab koheselt, milline parool on millise rakenduse jaoks.

Password Manager jätab automaatselt meelde paroolid või annab võimaluse eristada, milliseid saite mäletada ja millised välja jätta. Kui olete arvutisse sisse loginud, pakub Password Manager rakenduste või veebilehekülgede avamiseks paroolid või mandaadid,

Kui avate mistahes rakenduse või veebilehe, mis nõuab mandaati, tunneb Password Manager saidi automaatselt ära ning küsib, kas soovite, et tarkvara peaks teie kohta käiva teabe meeles. Kui soovite teatud saidid välja jätta, saate sellest päringust keelduda.

Veebiasukohtade, kasutajanimede ja paroolide salvestamine.

1. Näiteks navigeerige kasutatavale veebileheni või rakenduseni ning klõpsake veebi autentimiseks Password Manageri ikoonil veebilehe üleval vasakul nurgas.
2. Andke lingile nimi (valikuline) ja sisestage Password Manageri kasutajanimi ja parool.
3. Kui olete lõpetanud, klõpsake nuppu **OK**.
4. Password Manager salvestab ka ühisvõrgukohtade ja ühendatud võrgudraivide kasutajanimed ja paroolid.

Salvestatud autentimiste kuvamine ja haldamine Password Manageris

Password Manager võimaldab kesksest kohast autentimisi vaadata, hallata, varundada ja käivitada. Password Manager toetab ka salvestatud saitide käivitamist Windowsis.

Password Manageri avamiseks kasutage klaviatuuril kombinatsiooni Ctrl+Windowsi klahv+h ja seejärel klõpsake salvestatud otsetee käivitamiseks ja autentimiseks **Log in** (Logi sisse).

Password Manageri suvand **Edit** (Redigeeri) võimaldab nime ja sisselogimisnime vaadata ja muuta ning isegi paroole avaldada.

HP Client Security väikeettevõtetele võimaldab kõik mandaadid ja sätted kokku pakkida ja/või kopeerida teise arvutisse.

HP Device Access Manager

Device Access Manageri on võimalik kasutada erinevate sisemiste ja välimiste talletusseadmete kasutamise piiramiseks nii, et andmed jäävad turvaliselt kõvakettale ning ei sattu ettevõtte seinte vahelt välja. Näiteks on võimalik lubada kasutaja juurdepääs andmetele, kuid takistada andmete kopeerimist CD-le, isiklikku muusikapleierisse või USB-mäluseadmele.

1. Avage **Device Access Manager** (vt Device Access Manageri avamine lk 41).

   Kuvatakse ligipääs praegusele kasutajale.

2. Ligipääsu muutmiseks kasutajatele, rühmadele või seadmetele, klõpsake või koputage **Change** (Muuda). Lisateavet leiate jaotisest Süsteemivaade lk 42.

HP Drive Encryption

HP Drive Encryption kasutatakse andmete kaitsmiseks kogu kõvaketta krüptimise kaudu. Andmed arvuti kõvakettal on kaitstud isegi siis, kui arvuti varastatakse ja/või kõvaketas eemaldatakse algsest arvutist ning sisestatakse teise arvutisse.

Täiendava turvaeelisena nõuab Drive Encryption enne operatsioonisüsteemi käivitamist täielikku autentimist kasutajanime ja parooli abil. Seda protsessi nimetatakse buudieelseks autentimiseks.

Et seda lihtsustada, sünkroonivad erinevad tarkvaramoodulid paroolid automaatselt, sealhulgas Windowsi kasutajakontod, autentimisdomeenid, HP Drive Encryption, Password Manager ning HP Client Security.

HP Drive Encryption häälestamiseks esmasel käivitamisel koos HP Client Security häälestusviisardiga, vt Alustamine lk 8.

4 Klienditurbesüsteem HP Client Security

HP Client Security avaleht on keskne koht, kust pääseb juurde HP Client Security funktsioonidele, rakendustele ja sätetele. Avaleht koosneb kolmest sektsioonist:

- **ANDMED** – pakub juurdepääsu andmeturbega seotud rakendustele.
- **SEADE** – pakub juurdepääsu seadmeturbega seotud rakendustele.
- **IDENTITEET** – pakub autentimismandaatide registreerimist ja autentimist.

Rakenduse kirjelduse kuvamiseks liigutage kursorit üle rakenduste loendi.

Lehe allosas võib HP Client Security pakkuda linke kasutajale ning haldussätteid. HP Client Security pakub juurdepääsu täpsematele sätetele ja funktsioonidele, kui klõpsate või koputate ikooni **Hammasratas** (sätted).

Identiteedifunktsioonid, -rakendused ja -sätted

HP Client Security pakutavad identiteedifunktsioonid, -rakendused ja sätted aitavad teil oma digitaalset ID-d mitmeti hallata. Klõpsake või koputage HP Client Security avalehel ühte järgmistest paanidest ja sisestage oma Windowsi parool:

- **Sõrmejäljed** – registreerib ja haldab sõrmejäljemandaati.
- **SpareKey** – seadistab ja haldab teie HP SpareKey mandaati, mida saab kasutada arvutisse sisselogimisel, kui teised mandaadid on kadunud. Samuti saate lähtestada oma unustatud parooli.
- **Windowsi parool** – võimaldab lihtsa juurdepääsu abil muuta Windowsi parooli.
- **Bluetooth-seadmed** – saate registreerida ja hallata oma Bluetooth-seadmeid.
- **Kaardid** – saate registreerida ja hallata oma kiipkaarte, kontaktivabu kaarte ja viipekaarte.
- **PIN** – saate registreerida ja hallata oma PIN-mandaate.
- **RSA SecurID** – saate registreerida ja hallata oma RSASecurID mandaati (kui sobiv seadistus on tehtud).
- **Password Manager** – saate hallata oma võrgukontode ja -rakenduste paroole.

Sõrmejäljed

HP Client Security häälestusviisard juhendab teid läbi häälestustoimingute ehk sõrmejälgede "registreerimise".

Oma sõrmejälgi võite registreerida või kustutada ka sõrmejälgede lehel, mille saate avada, kui klõpsate või koputate HP Client Security avalehel ikooni **Fingerprints** (Sõrmejäljed).

1. Libistage sõrmega sõrmejälgede lehel, kuni registreerumine õnnestub.

   Registreerimiseks vajaminevate sõrmede arv on lehel ära toodud. Soovitatav on kasutada nimetissõrme ja keskmist sõrme.

2. Varem registreeritud sõrmejälgede kustutamiseks klõpsake või koputage **Delete** (Kustuta).

3. Lisasõrmede registreerimiseks klõpsake või koputage **Enroll an additional fingerprint** (Täiendava sõrmejälje registreerimine).

4. Enne lehelt lahkumist klõpsake või koputage **Salvesta**.

⚠ **ETTEVAATUST.** Kui registreerite sõrmejälgi viisardi kaudu, ei salvestata sõrmejäljeandmeid enne, kui klõpsate **Edasi**. Kui lahkute mõneks ajaks arvuti juurest või sulgete programmi, siis tehtud muutusi **ei** salvestata.

- Kui soovite pääseda sõrmejälgede haldussätete juurde, kus haldurid saavad teha täpsustusi registreerimise, täpsuse ja muude sätete kohta, klõpsake või koputage **Administrative Settings** (Haldussätted) (vaja läheb halduri õigusi).
- Sõrmejäljetuvastuse kasutajasätetele juurdepääsuks, kus saate täpsustada sõrmejäljetuvastuse erinevaid sätteid, klõpsake või koputage **User Settings** (Kasutajasätted).

Sõrmejäljetuvastuse haldussätted

Haldurid saavad täpsustada sõrmejäljelugeja registreerimist, täpsust ja muid sätteid. Nõutavad on halduriõigused.

- Sõrmejäljemandaadi haldussätetele juurdepääsuks klõpsake või koputage sõrmejälgede lehel **Administrative Settings** (Haldussätted).

- **User enrollment** (Kasutaja registreerimine) – valige minimaalne ja maksimaalne sõrmejälgede arv, mida kasutaja võib registreerida.
- **Recognition** (Tuvastus) – libistage liugurit, et reguleerida sõrmejäljelugeja tundlikkust sõrme libistamisel.

  Kui teie sõrmejälge järjest ei tuvastata, peaksite valima madalama tuvastussätte. Kõrgem säte suurendab sõrmejäljetundlikkust eri sõrmejäljeversioonide tuvastamisel ja seetõttu vähendab ka tuvastusvea võimalusi. **Medium-High** (Keskmine-kõrge) säte pakub nii turvalisust kui ka mugavust.

Sõrmejäljetuvastuse kasutajasätted

Sõrmejäljetuvastuse kasutajasätete lehel saate valida sätted, mis määravad sõrmejäljetuvastuse välimust ja toimimist.

- Sõrmejäljemandaadi kasutajasätetele juurdepääsuks klõpsake või koputage sõrmejälgede lehel **User Settings** (Kasutajasätted).

- **Enable sound feedback** (Luba heliga tagasiside) – vaikimisi annab HP Client Security sõrmejälje andmisel helilist tagasisidet, esitades erinevate sündmuste korral erinevaid helisid. Sündmustele saab määrata uusi helisid Windowsi juhtpaneeli helide vahekaardil helisätete jaotises, või juhul, kui soovite heli välja lülitada, tühjendage vastav ruut.
- **Show scan quality feedback** (Kuva tagasiside skannimise kvaliteedi kohta) – kvaliteedist olenemata kõigi liigutuste kuvamiseks märkige ruut. Ainult kvaliteetsete liigutuste kuvamiseks tühjendage ruut.

HP SpareKey – paroolitaaste

HP SpareKey annab teile juurdepääsu oma arvutile (toetatud platvormide puhul), vastates kolmele turbeküsimusele.

HP Client Security palub teil HP Client Security häälestusviisardis algse käivitamise ajal määrata oma isiklik HP SpareKey.

HP SpareKey loomiseks:

1. Valige viisardi HP SpareKey leht, valige kolm turbeküsimust ja sisestage kõigi jaoks vastus.

   Võite valida mõne olemasoleva küsimuse või selle ise kirjutada.

2. Klõpsake või koputage **Enroll** (Registreeri).

HP SpareKey kustutamiseks:

▲ Klõpsake või koputage **Delete your SpareKey** (SpareKey kustutamine).

Kui SpareKey on häälestatud, pääsete oma arvutile juurde, kasutades oma SpareKey'd sisselülitusautentimisel või Windowsi tervituskuval.

SpareKey lehel võite valida erinevaid küsimusi või muuta oma vastuseid; lehele pääsete HP Client Security avalehe paroolitaaste paanilt.

HP SpareKey sätete avamiseks, kus haldur saab HP SpareKey mandaadiga seotuid sätteid muuta, klõpsake valikut **Sätted** (nõuab halduriõigusi).

HP SpareKey sätted

HP SpareKey sätete lehel saate täpsustada, milliste sätetega reguleeritakse HP SpareKey mandaadi käitumist ja kasutamist.

▲ HP SpareKey sätete lehe käivitamiseks klõpsake või koputage HP SpareKey lehel üksust **Sätted** (nõuab halduriõigusi).

Haldurid saavad valida järgmised sätted:

- Määrata küsimused, mis esitatakse kõigile kasutajatele HP SpareKey häälestamisel.
- Lisada kolm kohandatud turbeküsimust, mis lisatakse kasutajatele esitatavasse loendisse.
- Valida, kas lubada kasutajatel ise turbeküsimusi koostada.
- Määrata, milline autentimiskeskkond (Windows või sisselülitusautentimine) lubab paroolitaasteks HP SpareKey kasutamist.

Windowsi parool

HP Client Security teeb Windowsi parooli muutmise lihtsamaks ja kiiremaks kui Windowsi juhtpaneelil.

Windowsi parooli muutmiseks:

1. Klõpsake või koputage HP Client Security avakuval valikut **Windowsi parool**.
2. Sisestage kehtiv parool tekstiboksi **Current Windows password** (Windowsi praegune parool).
3. Tippige uus parool tekstiboksi **New Windows password** (Windowsi uus parool) ja seejärel tippige see uuesti tekstiboksi **Confirm new password** (Kinnita uus parool).
4. Klõpsake või koputage valikut **Muuda**, et kohe vahetada olemasolev parool uue parooli vastu, mille te sisestasite.

Bluetooth-seadmed

Kui haldur on lubanud autentimismandaadina Bluetooth-seadme, võite teiste mandaatide kõrval täiendava turvalisuse tagamiseks häälestada ka Bluetooth-telefoni.

MÄRKUS. Toetatud on ainult Bluetooth-mobiiliseadmed.

1. Veenduge, et arvutis oleks Bluetoothi funktsioon lubatud ja et Bluetooth-telefon on otsingurežiimis. Telefoni ühendamiseks võidaks teilt nõuda Bluetooth-telefonis automaatselt loodud koodi sisestamist. Olenevalt Bluetooth-seadme konfiguratsioonisätetest võidakse nõuda arvuti ja telefoni sidumiskoodide võrdlust.
2. Telefoni registreerimiseks valige see ja klõpsake või koputage valikut **Enroll** (Registreeri).

Lehe Bluetooth-seadmete sätted lk 15 avamiseks, kus haldur saab täpsustada Bluetooth-seadmete sätteid, klõpsake **Settings** (Sätted) (nõuab halduriõigusi).

Bluetooth-seadmete sätted

Haldurid saavad Bluetooth-seadme mandaadi toimimise ja kasutamise reguleerimiseks määrata järgmised sätted:

Vaikne autentimine

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Ühendatud registreeritud Bluetooth-seadme automaatne kasutamine identiteedi kontrollimiseks) – valige ruut, et lubada kasutajatel autentimiseks Bluetoothi mandaadi kasutamine ilma kasutajatoiminguta või tühjendage ruut, et see valik keelata.

Bluetoothi ühendusulatus

- **Lock computer when your enrolled Bluetooth device moves out of range of your computer** (Arvuti lukustamine juhul, kui registreeritud Bluetooth-seade väljub arvuti ühendusulatusest) – märkige ruut, et arvuti lukustada, kui sisselogimisel ühendatud Bluetooth-seade väljub ühendusulatusest või tühjendage ruut, kui soovite selle valiku keelata.

MÄRKUS. Selle valiku eeliste kasutamiseks peab teie arvuti Bluetooth-moodul seda võimalust toetama.

Kaardid

HP Client Security võib toetada mitmeid eri tüüpi identifitseerimiskaarte, mis on väikesed arvutikiipi sisaldavad plastkaardid. Nende hulka kuuluvad kiipkaardid, kontaktivabad kaardid ja viipekaardid. Kui mõni selline kaart ja sobiv kaardilugeja on arvutiga ühendatud ning kui haldur on installinud tootja vastava draiveri ja kui ta on lubanud kaardi autentimismandaadina, võitegi kaarti autentimismandaadina kasutada.

Kiipkaartide puhul peaks tootja tagama ka tööriistad turvasertifikaadi installimiseks ja PIN-halduseks, mida HP Client Security oma turvaalgoritmis kasutab. PIN-ina kasutatavad numbrid ja tähed võivad muutuda. Enne kiikaardi kasutamist peab haldur selle lähtestama.

HP Client Security toetab järgmisi kiipkaardivorminguid:

- CSP
- PKCS11

HP Client Security toetab järgmisi kontaktivaba kaardi vorminguid:

- Kontaktivabad HID iCLASS mälukaardid
- Kontaktivabad MiFare Classic 1k, 4k ja mini-mälukaardid

HP Client Security toetab järgmisi viipekaardivorminguid:

- HID viipekaardid

Kiipkaardi registreerimiseks:

1. Sisestage kaart kiipkaardilugejasse.
2. Kui kaart on tuvastatud, sisestage kaardi PIN-kood ja klõpsake või koputage **Enroll** (Registreeri).

Kiipkaardi PIN-koodi muutmiseks:

1. Sisestage kaart kiipkaardilugejasse.
2. Kui kaart on tuvastatud, sisestage kaardi PIN-kood ja klõpsake või koputage **Authenticate** (Autendi).
3. Klõpsake või koputage **Change PIN** (Muuda PIN-koodi) ja sisestage uus PIN-kood.

Kontaktivaba või viipekaardi registreerimiseks:

1. Pange kaart lugejale hästi lähedale.
2. Kui kaart tuvastatakse, klõpsake või koputage **Enroll** (Registreeri).

Registreeritud kaardi kustutamiseks:

1. Esitage kaart lugejale.
2. Kui tegu on kiipkaardiga, sisestage kaardile omistatud PIN-kood ja klõpsake või koputage **Authenticate** (Autendi).
3. Klõpsake või koputage **Kustuta**.

Kui kaart on registreeritud, kuvatakse kaardi üksikasjad jaotises **Enrolled Cards** (Registreeritud kaardid). Kui kaart on kustutatud, eemaldatakse see loendist.

Juurdepääsuks viipe-, kontaktivaba ja kiipkaardi sätetele, kus haldurid saavad määrata kaardimandaatidega seotud sätteid klõpsake või koputage **Sätted** (nõuab halduriõigusi).

Viipe-, kontaktivabade ja kiipkaartide sätted

Kaardisätetele juurdepääsuks klõpsake või koputage loendis kaarti ja klõpsake või koputage kuvatavat noolt.

Kiipkaardi PIN-koodi muutmiseks:

1. Esitage kaart lugejale
2. Sisestage kaardile omistatud PIN-kood ja klõpsake või koputage **Jätka**.
3. Sisestage ja kinnitage uus PIN-kood ja klõpsake või koputage **Jätka**.

Kiipkaardi PIN-koodi lähtestamiseks:

1. Esitage kaart lugejale
2. Sisestage kaardile omistatud PIN-kood ja klõpsake või koputage **Jätka**.

3. Sisestage ja kinnitage uus PIN-kood ja klõpsake või koputage **Jätka**.
4. Lähtestamise kinnitamiseks klõpsake või koputage **Jah**.

Kaardiandmete kustutamiseks:

1. Esitage kaart lugejale
2. Sisestage kaardile omistatud PIN-kood (ainult kiipkaartidel) ja klõpsake või koputage **Continue** (Jätka).
3. Kustutamise kinnitamiseks klõpsake või koputage **Jah**.

PIN

Kui haldur on lubanud autentimismandaadina PIN-koodi, võite teiste mandaatide kõrval täiendava turvalisuse tagamiseks häälestada ka PIN-koodi.

Uue PIN-koodi määramiseks:

▲ Sisestage PIN-kood, sisestage see kinnitamiseks uuesti ja klõpsake ja koputage **Apply** (Rakenda).

PIN-koodi kustutamiseks:

▲ Klõpsake või koputage **Kustuta** ja seejärel klõpsake või koputage kinnitamiseks **Jah**.

Juurdepääsuks PIN-koodi sätetele, kus haldurid saavad määrata PIN-koodi mandaatidega seotud sätteid, klõpsake või koputage **Sätted** (nõuab halduriõigusi).

PIN-koodi sätted

PIN-koodi sätete lehel saate määrata PIN-koodi mandaadile minimaalse ja maksimaalse lubatud pikkuse.

RSA SecurID

Kui haldur on lubanud autentimismandaadina RSA ja järgmised tingimused on täidetud, võite RSA SecurID mandaadi registreerida või kustutada.

MÄRKUS. Nõutav on sobiv seadistus.

- Kasutaja peab olema loodud RSA Serveris.
- Kasutajale ja arvutile omistatud RSA SecurID luba peab olema liidetud RSA Serveri domeeniga.
- SecurID tarkvara on arvutisse installitud.
- Õigesti konfigureeritud RSA Serveri jaoks on ühendus saadaval.

RSA SecurID mandaadi registreerimiseks:

▲ Sisestage oma RSA SecurID kasutajanimi ja pääsukood (RSA SecurID loa kood või PIN+Token kood, olenevalt teie keskkonnast) ja klõpsake või koputage **Rakenda**.

Edukal registreerimisel kuvatakse teade "Your RSA SecurID credential has been successfully enrolled" (Teie RSA SecurID mandaat on edukalt registreeritud) ja nupp Kustuta on saadaval.

RSA SecurID mandaadi kustutamiseks:

▲ Klõpsake **Kustuta** ja valige hüpikdialoogi küsimusele "Are you sure you want to delete your RSA SecurID credential?" (Kas oled kindel, et soovid oma RSA SecurID mandaadi kustutada?) vastuseks **Jah**.

Password Manager

Password Manageri kasutades on veebisaitidele ja rakendustesse sisselogimine lihtsam ja turvalisem. Võite luua tugevamaid paroole, mida te ei pea üles kirjutama ega meelde jätma; logida kiiresti ja lihtsalt sisse sõrmejäljega, kiipkaardiga, viipekaardiga, kontaktivaba kaardiga, Bluetooth-telefoniga, PIN-koodiga, RSA mandaadiga või oma Windowsi parooliga.

MÄRKUS. Kuna sisselogimisekraanide struktuur on pidevas muutumises, ei pruugi Password Manager kõiki veebisaite alati toetada.

Password Manager pakub järgmisi võimalusi:

Password Manageri leht

- Klõpsake või koputage kontot, et veebileht või rakendus automaatselt käivitada ja logige sisse.
- Kasutage oma kontode organiseerimisel kategooriaid.

Parooli tugevus

- Vaadake kiirelt, kas teie paroolid on turvalised.
- Sisselogimisandmete lisamisel kontrollige veebisaitide ja rakenduste jaoks mõeldud üksikute paroolide tugevust.
- Parooli tugevust väljendatakse punase, kollase või rohelise olekuindikaatoriga.

Rakenduse **Password Manager** ikoon kuvatakse veebilehe või rakenduse sisselogimisekraani ülemises vasakpoolses nurgas. Kui veebisaidi või rakenduse sisselogimist pole veel loodud, kuvatakse ikoonil plussmärk.

▲ Klõpsake või koputage ikooni **Password Manager**, et kuvada kontekstimenüü, kus saab valida järgmist:

- Lisa [mingidomeen.com] Password Manageri
- Ava Password Manager
- Ikoonisätted
- Spikker

Veebisaidid või programmid, kus sisselogimist pole veel loodud

Kontekstimenüüs kuvatakse järgmised valikud:

- **Add [somedomain.com] to the Password Manager** (Lisa [mingidomeen.com] Password Manageri) – võimaldab lisada praegusele sisselogimisekraanile sisselogimise.
- **Open Password Manager** (Ava Password Manager) – käivitab Password Manageri.
- **Icon Settings** (Ikoonisätted) – lubab määrata tingimused, millistel ikoon **Password Manager** kuvatakse.
- **Spikker** – kuvab HP Client Security spikri.

Veebisaidid või programmid, kus sisselogimine on juba loodud

Kontekstimenüüs kuvatakse järgmised valikud:

- **Fill in logon data** (Sisestage sisselogimisandmed) – kuvab lehe **Verify your identity** (Kinnitage oma identiteet). Edukal autentimisel paigutatakse teie sisselogimisandmed sisselogimisväljadele ja seejärel leht esitatakse (kui esitamisel täpsustati, millal sisselogimine loodi või seda viimati muudeti).
- **Edit Logon** (Redigeeri sisselogimist) – võimaldab muuta selle veebisaidi sisselogimisandmeid.
- **Add Logon** (Lisa sisselogimine) – võimaldab lisada Password Manageri konto.
- **Open Password Manager** (Ava Password Manager) – käivitab Password Manageri.
- **Spikker** – kuvab HP Client Security spikri.

MÄRKUS. Selle arvuti haldur võis konfigureerida HP Client Security nii, et identiteedi kinnitamisel nõutakse rohkem kui üht mandaati.

Sisselogimiste lisamine

Saate kergelt lisada veebisaidile või programmile sisselogimise, sisestades sisselogimisteabe vaid üks kord. Edaspidi sisestab Password Manager automaatselt teabe teie eest. Neid sisselogimisi saate kasutada pärast veebisaidi või programmi avamist.

Sisselogimise lisamiseks:

1. Avage veebisaidi või programmi sisselogimisekraan.
2. Klõpsake ikooni **Password Manager** ja klõpsake või koputage seejärel ühte järgmistest valikutest, olenevalt sellest, kas tegemist on veebisaidi või programmiga:
   - Veebisaidi puhul klõpsake või koputage **Add [domain name] to Password Manager** (Lisa [domeeni nimi] Password Manageri).
   - Programmi puhul klõpsake või koputage **Add this logon screen to Password Manager** (Lisa see sisselogimisekraan Password Manageri).
3. Sisestage oma sisselogimisandmed. Ekraanil olevad sisselogimisväljad ja vastavad väljad dialoogiboksis identifitseeritakse laia oranži joonega.
   a. Sisselogimisvälja täitmiseks ühe eelvormindatud valikuga klõpsake või koputage välja paremal serval olevaid nooli.
   b. Selle sisselogimise parooli kuvamiseks klõpsake või koputage **Show password** (Kuva parool).
   c. Sisselogimisväljade täitmiseks, kuid mitte esitamiseks tühjendage ruut **Automatically submit logon data** (Edasta sisselogimisandmed automaatselt).

d. Klõpsake või koputage **OK** , et valida soovitud autentimismeetod (sõrmejäljed, kiipkaart, viipekaart, kontaktivaba kaart, Bluetooth-telefon, PIN-kood või parool) ja logige valitud autentimismeetodi abil sisse.

   Ikoonilt **Password Manager** eemaldatakse plussmärk, andmaks märku loodud sisselogimisest.

e. Kui Password Manager sisselogimisvälju ei tuvasta, klõpsake või koputage **More fields** (Veel välju).

   - Valige kõigi sisselogimiseks nõutud väljade ruudud või tühjendage nende väljade ruudud, mida sisselogimiseks ei vajata.
   - Klõpsake või koputage **Sule**.

Iga kord, kui te seda veebisaiti soovite külastada või programmi avada, kuvatakse veebisaidi või rakenduse sisselogimisekraani ülemises vasakpoolses nurgas ikoon **Password Manager**, tähistades seda, et te võite sisselogimiseks kasutada oma registreeritud mandaate.

Sisselogimiste redigeerimine

Sisselogimise redigeerimiseks:

1. Avage veebisaidi või programmi sisselogimisekraan.
2. Et kuvada sisselogimisteabe redigeerimiseks vajalik dialoogiboks, klõpsake või koputage ikooni **Password Manager** ja seejärel klõpsake või koputage **Edit Logon** (Redigeeri sisselogimist).

   Ekraanil olevad sisselogimisväljad ja vastavad väljad dialoogiboksis identifitseeritakse laia oranži joonega.

   Password Manageri lehel saate redigeerida ka kontoteavet, kui klõpsate või koputate sisselogimist, et kuvada redigeerimisvalikuid ja valite seejärel **Edit** (Redigeeri).
3. Redigeerige oma sisselogimisteavet.

   - Et redigeerida üksust **Account name** (Konto nimi), sisestage väljale uus nimi.
   - Kui soovite lisada või redigeerida üksust **Category** (Kategooria), sisestage või muutke nime väljal **Category** (Kategooria).
   - Et valida üksuse **Username** (Kasutajanimi) sisselogimisväli ühe eelvormindatud valikuga, klõpsake või koputage välja paremal serval olevaid nooli.

     Eelvormindatud valikud on saadaval vaid siis, kui redigeerida sisselogimist redigeerimiskäsu abil Password Manageri ikooni kontekstimenüüst.
   - Et valida üksuse **Password** (Parool) sisselogimisväli ühe eelvormindatud valikuga, klõpsake või koputage välja paremal serval olevaid nooli.

     Eelvormindatud valikud on saadaval vaid siis, kui redigeerida sisselogimist redigeerimiskäsu abil Password Manageri ikooni kontekstimenüüst.
   - Sisselogimisele ekraanilt lisaväljade lisamiseks klõpsake või koputage **More fields** (Veel välju).
   - Selle sisselogimise parooli kuvamiseks klõpsake või koputage ikooni **Show password** (Kuva parool).

- Sisselogimisväljade täitmiseks, kuid mitte esitamiseks tühjendage ruut **Automatically submit logon data** (Edasta sisselogimisandmed automaatselt).
- Selle sisselogimise turvariskiga parooli tähistamiseks märkige ruut **This password is compromised** (See parool on turvariskiga).

  Kui muudatused on salvestatud, tähistatakse ka kõik teised sama parooli kasutavad sisselogimised turvariskiga üksusteks. Sel juhul külastage kõiki turvariskiga kontosid ja muutke paroolid nii nagu vaja.

4. Klõpsake või koputage **OK**.

Password Manageri kiirlinkide menüü

Password Manager pakub kiiret ja lihtsat võimalust veebisaitide ja programmide käivitamiseks, millele olete loonud sisselogimised. Topeltklõpsake või topeltkoputage menüüs **Password Manager Quick Links** (Password Manageri kiirlingid) programmi või veebisaiti või HP Client Security Password Manageri lehel sisselogimisekraani ja seejärel täitke sisselogimisandmed.

Sisselogimise loomisel lisatakse see automaatselt Password Manageri menüüsse **Quick Links** (Kiirlingid).

Menüü **Quick Links** (Kiirlingid) kuvamiseks:

▲ Vajutage **Password Manager** kiirklahvikombinatsiooni (tehasesätted on Ctrl+Windows klahv+h). Klahvikombinatsiooni muutmiseks klõpsake HP Client Security avalehel **Password Manager** ja seejärel klõpsake või koputage **Sätted**.

Sisselogimiste kategooriatesse paigutamine

Sisselogimiste korrashoidmiseks looge üks või mitu kategooriat.

Sisselogimisele kategooria määramiseks:

1. Klõpsake või koputage HP Client Security avakuval valikut **Password Manager**.
2. Klõpsake või koputage kontot ning seejärel **Edit** (Redigeeri).
3. Sisestage kategooria nimi väljale **Category** (Kategooria).
4. Klõpsake või koputage **Salvesta**.

Kategooriast konto eemaldamiseks:

1. Klõpsake või koputage HP Client Security avalehel **Password Manager**.
2. Klõpsake või koputage kontot ning seejärel **Edit** (Redigeeri).
3. Kustutage väljal **Category** (Kategooria) kategooria nimi.
4. Klõpsake või koputage **Salvesta**.

Kategooria ümbernimetamiseks:

1. Klõpsake või koputage HP Client Security avalehel **Password Manager**.
2. Klõpsake või koputage kontot ning seejärel **Edit** (Redigeeri).
3. Muutke väljal **Category** (Kategooria) kategooria nimi.
4. Klõpsake või koputage **Salvesta**.

Sisselogimiste haldus

Password Manager teeb sisselogimisteabe (kasutajanimed, paroolid ja mitme sisselogimisega kontod) halduse ühest kesksest kohast lihtsaks.

Teie sisselogimised kuvatakse Password Manageri lehel.

Sisselogimiste halduseks:

1. Klõpsake või koputage HP Client Security avalehel **Password Manager**.
2. Klõpsake või koputage olemasolevat sisselogimiskontot, valige üks järgnevatest üksustest ja järgige ekraanijuhiseid:
   - **Redigeeri** – sisselogimise redigeerimine. Lisateavet leiate jaotisest Sisselogimiste redigeerimine lk 20.
   - **Logi sisse** – valitud kontole sisselogimine.
   - **Kustuta** – valitud kasutaja sisselogimisandmete kustutamine.

Veebilehele või programmile täiendava sisselogimise lisamiseks:

1. Avage veebilehe või programmi sisselogimiskuva.
2. Klõpsake või koputage ikooni **Password Manager** rakenduse kontekstimenüü kuvamiseks.
3. Klõpsake või koputage valikut **Add Logon** (Sisselogimise lisamine) ning järgige ekraanijuhiseid.

Parooli tugevuse hindamine

Veebilehtedele ja programmidele sisselogimisel on tugeva parooli kasutamine oluline osa identiteedi kaitsest.

Password Manager muudab turvalisuse jälgimise ja tõhustamise lihtsamaks, analüüsides koheselt ning automaatselt iga veebisaitidele ja programmidele sisselogimiseks kasutatava parooli tugevust.

Password Manageris sisselogimise loomisel ja parooli sisestamisel kuvatakse parooli all värviline riba, mis näitab parooli tugevust. Värvid näitavad alljärgnevat:

- **Punane** – nõrk
- **Kollane** – keskmine
- **Roheline** – tugev

Password Manageri ikoonisätted

Password Manager üritab tuvastada veebisaitide ja programmide sisselogimiskuvasid. Sisselogimisteabeta sisselogimiskuva tuvastamisel pakub Password Manager võimaluse sisselogimise loomiseks, kuvades ikooni **Password Manager** koos plussmärgiga.

1. Klõpsake või koputage ikooni ning seejärel klõpsake või koputage **Icon Settings** (Ikoonisätted), et kohandada Password Manageri toimimist võimalikel sisselogimislehtedel.

   - **Prompt to add logons for logon screens** (Küsi sisselogimise lisamist sisselogimisekraanidel) – klõpsake või koputage seda võimalust, et Password Manager küsiks sisselogimisteabeta sisselogimisekraani kuvamisel sisselogimise lisamist.
   - **Exclude this screen** (Arva ekraan valikust välja) – märkige ruut, et Password Manager enam sellel sisselogimisekraanil sisselogimise lisamist ei küsiks.
   - **Do not prompt to add logons for logon screens** (Ära küsi sisselogimise lisamist sisselogimisekraanidel) – valige raadionupp.

2. Varem välja arvatud sisselogimiskuvale sisselogimise lisamiseks:

   a. Logige sisse varem välja arvatud veebilehele.

   b. Klõpsake või koputage hüpikdialoogi valikut **Remember** (Jäta meelde), et Password Manager parooli salvestaks ning looks ekraanile sisselogimise.

3. Password Manageri lisasätetele juurdepääsuks klõpsake või koputage Password Manageri ikooni, klõpsake või koputage **Open Password Manager** (Ava Password Manager) ning seejärel klõpsake või koputage Password Manageri lehel valikut **Sätted**.

Sisselogimiste import ja eksport

HP Password Manageri impordi- ja ekspordilehel saate importida brauseri poolt salvestatud sisselogimisi. Andmeid saab importida ka HP Client Security varufaililt ning eksportida HP Client Security varufailile.

▲ Impordi- ja ekspordilehe kuvamiseks klõpsake või koputage Password Manageri lehel **Import and export** (Import ja eksport).

Brauserist paroolide importimiseks:

1. Klõpsake või koputage brauserit, millest paroole importida (kuvatakse ainult installitud brauserid).
2. Tühjendage kõigi kontode ruut, mille puhul te paroole importida ei soovi.
3. Klõpsake või koputage **Import** (Impordi).

HP Client Security varufaili andmete importimine või eksportimine toimub läbi seotud linkide impordi- ja ekspordilehel (jaotises **Other Options** (Muud suvandid)).

MÄRKUS. See funktsioon impordib ja ekspordib ainult Password Manageri andmeid. Täiendavate HP Client Security andmete varunduseks ja taasteks vt Andmete varundus ja taaste lk 27.

Andmete importimiseks HP Client Security varufailist:

1. Klõpsake või koputage HP Password Manager impordi- ja ekspordilehel **Import data from an HP Client Security backup file** (Impordi andmeid HP Client Security varufailist).
2. Kinnitage oma identiteet.
3. Valige varemloodud varufail või sisestage väljale selle tee ning klõpsake või koputage **Sirvi**.

4. Sisestage faili parool ja klõpsake või koputage seejärel **Edasi**.
5. Klõpsake või koputage üksust **Restore** (Taasta).

Andmete eksportimiseks HP Client Security varufaili:

1. Klõpsake või koputage HP Password Manager impordi- ja ekspordilehel **Export data from an HP Client Security backup file** (Ekspordi andmeid HP Client Security varufailist).
2. Kinnitage oma identiteet ning klõpsake või koputage **Edasi**.
3. Sisestage varufaili nimi. Vaikesättena salvestatakse fail teie dokumentide kausta. Teise sihtkoha valimiseks klõpsake või koputage **Sirvi**.
4. Sisestage ja kinnitage faili parool ja klõpsake või koputage **Salvesta**.

Sätted

Password Manager isikustamiseks saate sätteid muuta:

- **Prompt to add logons for logon screens** (Küsi sisselogimiskuvadel, kas lisada sisselogimine) – plussmärgiga ikoon **Password Manager** kuvatakse iga kord, kui tuvastatakse veebilehe või programmi sisselogimisekraan, mis võimaldab lisada sisselogimise menüü **Logons** (Sisselogimised) kaudu.

  Selle funktsiooni väljalülitamiseks tühjendage ruut valiku **Prompt to add logons for logon screens** (Küsi sisselogimiskuvadel, kas lisada sisselogimine) kõrval.

- **Open Password Manager with Ctrl+Win+h** (Ava Password Manager kombinatsiooniga Ctrl +Win+h) – vaikimisi kiirklahv, mis avab menüü **Password Manager Quick Links** (Password Manageri kiirlingid) on Ctrl+Windowsi klahv +h.

  Kiirklahvi vahetamiseks klõpsake või koputage valikut ning sisestage uus klahvikombinatsioon. Kombinatsioonid võivad sisaldada ühte või mitut alljärgnevatest: ctrl, alt või shift ja suvaline tähe- või numbriklahv.

  Windowsile või Windowsi rakendustele ette nähtud kombinatsioone ei saa kasutada.

- Tehase vaikeseadete juurde tagasipöördumiseks klõpsake või koputage **Restore defaults** (Taasta vaikesätted).

Täpsemad sätted

Haldurid pääsevad järgmistesse valikutesse sisse, valides ikooni **Hammasratas** HP Client Security avalehel.

- **Administrator Policies** (Halduripoliitikad) – võimaldab hallata haldurite sisselogimis- ja seansipoliitikaid.
- **Standard User Policies** (Tavakasutaja poliitikad) – võimaldab hallata tavakasutaja sisselogimis- ja seansipoliitikaid.
- **Security Features** (Turvafunktsioonid) – võimaldab arvuti turvalisust suurendada, kaitstes teie Windowsi kontot tugeva autentimisega ja/või autentimise lubamisega enne Windowsi käivitumist.
- **Users** (Kasutajad) – võimaldab hallata kasutajaid ja nende mandaate.
- **My Policies** (Minu poliitikad) – võimaldab üle vaadata autentimispoliitikaid ja registreerimiste olekut.

- **Backup and Restore** (Varundus ja taaste) – võimaldab HP Client Security andmeid varundada ja taastada.
- **About HP Client Security** (Teave HP Client Security kohta) – kuvab HP Client Security versiooniteabe.

Halduripoliitikad

Selle arvuti haldurite sisselogimis- ja seansipoliitikaid saab konfigureerida. Siin määratud sisselogimispoliitikad määratlevad kohalike haldurite nõutavad Windowsi sisselogimismandaadid. Siin määratud seansipoliitikad määravad kohalike haldurite nõutavad Windowsi seansil identiteedituvastamiseks vajalikud mandaadid.

Vaikesättena on kõik uued või muudetud poliitikad rakendatud pärast valiku **Apply** (Rakenda) klõpsamist või koputamist.

Uue poliitika lisamiseks:

1. Klõpsake või koputage HP Client Security avalehel ikooni **Hammasratas**.
2. Täpsemate sätete lehel klõpsake või koputage **Administrator Policies** (Halduripoliitikad).
3. Klõpsake või koputage **Add new policy** (Lisa uus poliitika).
4. Klõpsake allanooli, et valida uue poliitika esmane ja (vajadusel) teisene mandaat ning klõpsake või koputage **Lisa**.
5. Klõpsake nuppu **Rakenda**.

Uue või muudetud poliitika jõustamise edasilükkamiseks:

1. Klõpsake või koputage **Enforce this policy immediately** (Jõusta poliitika koheselt).
2. Valige **Enforce this policy on the specific date** (Jõusta see poliitika konkreetsel kuupäeval).
3. Sisestage kuupäev või kasutage hüpikkalendrit, et valida poliitika jõustamise kuupäev.
4. Vajadusel valige kasutajale uue poliitika meeldetuletus.
5. Klõpsake nuppu **Rakenda**.

Tavakasutajate poliitikad

Selle arvuti tavakasutajate sisselogimis- ja seansipoliitikaid saab konfigureerida. Siin määratud sisselogimispoliitikad määravad tavakasutajate nõutavad Windowsi sisselogimismandaadid. Siin määratud seansipoliitikad määravad tavakasutajate Windowsi seansil identiteedituvastamiseks vajalikud mandaadid.

Vaikesättena on kõik uued või muudetud poliitikad rakendatud pärast valiku **Apply** (Rakenda) klõpsamist või koputamist.

Uue poliitika lisamiseks:

1. Klõpsake või koputage HP Client Security avalehel ikooni **Hammasratas**.
2. Täpsemate seadete lehel klõpsake või koputage **Standard User Policies** (Tavakasutajate poliitikad).
3. Klõpsake või koputage **Add new policy** (Lisa uus poliitika).

4. Klõpsake allanooli, et valida uue poliitika esmane ja (vajadusel) teisene mandaat ning klõpsake või koputage **Lisa**.
5. Klõpsake nuppu **Rakenda**.

Uue või muudetud poliitika jõustamise edasilükkamiseks:

1. Klõpsake või koputage **Enforce this policy immediately** (Jõusta poliitika koheselt).
2. Valige **Enforce this policy on the specific date** (Jõusta see poliitika konkreetsel kuupäeval).
3. Sisestage kuupäev või kasutage hüpikkalendrit, et valida poliitika jõustamise kuupäev.
4. Vajadusel valige kasutajale uue poliitika meeldetuletus.
5. Klõpsake nuppu **Rakenda**.

Turbefunktsioonid

HP Client Security funktsioonide lubamine aitab kaitsta arvutit volitamata juurdepääsu eest.

Turbefunktsioonide seadistamiseks:

1. Klõpsake või koputage HP Client Security avalehel ikooni **Hammasratas**.
2. Täpsemate seadete lehel klõpsake või koputage **Security Features** (Turbefunktsioonid).
3. Lubage turbefunktsioonid, märkides ruudud ning klõpsates või koputades **Apply** (Rakenda). Mida rohkem funktsioone valite, seda turvalisem teie arvuti on.

   Need sätted kehtivad kõigile kasutajatele.

   - **Windows Logon Security** (Windowsi sisselogimisturvalisus) – kaitseb Windowsi kontosid HP Client Security turvamandaatide nõudmisega juurdepääsu saamiseks.
   - **Pre-Boot Security (Power-on authentication)** (Buudieelne turvalisus (Sisselülitusautentimine)) – kaitseb arvutit enne Windowsi käivitamist. Valik ei ole saadaval, kui BIOS seda ei toeta.
   - **Allow One Step logon** (Luba üheetapiline sisselogimine) – see säte võimaldab Windowsi sisselogimise vahele jätta, kui autentimine toimus sisselülitusautentimisega või Drive Encryptioni tasemel.
4. Klõpsake või koputage esmalt valikut **Users** (Kasutajad) ning seejärel kasutaja paani.

Kasutajad

Selle arvuti HP Client Security kasutajaid saab jälgida ja hallata.

Uue Windowsi kasutaja lisamiseks HP Client Securitysse:

1. Klõpsake või koputage HP Client Security avalehel ikooni **Hammasratas**.
2. Täpsemate seadete lehel klõpsake või koputage **Users** (Kasutajad).
3. Klõpsake või koputage valikut **Add another Windows user to HP Client Security** (Täiendava Windowsi kasutaja lisamine rakendusse HP Client Security).
4. Sisestage lisatava kasutaja nimi ning klõpsake või koputage **OK**.
5. Sisestage kasutaja Windowsi parool.

   Lisatud kasutaja paan kuvatakse kasutajate lehel.

Windowsi kasutaja kustutamiseks HP Client Securityst:

1. Klõpsake või koputage HP Client Security avalehel ikooni **Hammasratas**.
2. Täpsemate seadete lehel klõpsake või koputage **Users** (Kasutajad).
3. Klõpsake või koputage kustutatava kasutaja nimel.
4. Klõpsake või koputage esmalt **Delete User** (Kustuta kasutaja) ning seejärel kinnituseks valikut **Yes** (Jah).

Kasutaja jõustatud sisselogimis- ja seansipoliitikate kokkuvõtte kuvamiseks:

▲ Klõpsake või koputage esmalt valikut **Users** (Kasutajad) ning seejärel kasutaja paani.

Minu poliitikad

Võite kuvada oma autentimispoliitikaid ja registreerimise olekuid. Leht My Policies (Minu poliitikad) pakub linke ka lehtedele Administrators Policies (Halduripoliitikad) ja Standard User Policies (Tavakasutajate poliitikad).

1. Klõpsake või koputage HP Client Security avalehel ikooni **Hammasratas**.
2. Täpsemate seadete lehel klõpsake või koputage **My Policies** (Minu poliitikad).

   Kuvatakse parajasti sisselogitud kasutaja jõustatud sisselogimis- ja seansipoliitikad.

Minu poliitikate lehel on ka lingid juurdepääsuks lehtedele Halduripoliitikad lk 25 ja Tavakasutajate poliitikad lk 25.

Andmete varundus ja taaste

HP Client Security andmete regulaarne varundus on soovitatav. Varunduse sagedus sõltub andmete muutumise sagedusest. Näiteks igapäevasel uute sisselogimiste lisamisel tuleks andmeid varundada iga päev.

Varundusi saab ühest arvutist teise viia; seda nimetatakse ka importimiseks ja eksportimiseks.

MÄRKUS. See funktsioon varundab ainult Password Manageri. Drive Encryptionil on teistsugune varundusmeetod. Device Access Manageri ja sõrmejäljeautentimisteavet ei varundata.

HP Client Security peab olema installitud arvutisse, kuhu varundatud teave kogutakse enne kui seda varufaili kasutada saab.

Andmete varundamiseks:

1. Klõpsake või koputage HP Client Security avalehel ikooni **Hammasratas**.
2. Täpsemate sätete lehel klõpsake või koputage **Administrator Policies** (Halduripoliitikad).
3. Klõpsake või koputage üksust **Backup and Restore** (Varunda ja taasta).
4. Klõpsake või koputage **Backup** (Varunda) ja seejärel kinnitage oma identiteet.
5. Valige varundatav moodul ning klõpsake või koputage **Edasi**.
6. Sisestage salvestatava faili nimi. Vaikesättena salvestatakse fail teie dokumentide kausta. Teise sihtkoha valimiseks klõpsake või koputage **Sirvi**.
7. Faili kaitsmiseks sisestage ja kinnitage parool.
8. Klõpsake või koputage **Salvesta**.

Andmete taastamiseks:

1. Klõpsake või koputage HP Client Security avalehel ikooni **Hammasratas**.
2. Täpsemate sätete lehel klõpsake või koputage **Administrator Policies** (Halduripoliitikad).
3. Klõpsake või koputage üksust **Backup and Restore** (Varunda ja taasta).
4. Valige üksus **Restore** (Taasta) ning kinnitage oma identiteet.
5. Valige varem loodud varufail. Sisestage tee vastavale väljale. Teise sihtkoha valimiseks klõpsake või koputage **Sirvi**.
6. Sisestage faili parool ja klõpsake või koputage seejärel **Edasi**.
7. Valige moodulid, millele te soovite andmed taastada.
8. Klõpsake või koputage üksust **Restore** (Taasta).

5 HP Drive Encryption (ainult teatud mudelitel)

HP Drive Encryption pakub täielikku andmekaitset, krüptides teie arvuti andmed. Kui Drive Encryption on aktiveeritud, tuleb sisse logida Drive Encryptioni sisselogimisekraanil, mis kuvatakse enne Windows® operatsioonisüsteemi käivitumist.

HP Client Security avakuva võimaldab Windowsi halduritel aktiveerida rakendus Drive Encryption, talletada krüptimisvõti ja valida või tühistada krüptitavad draivid või sektsioonid. Lisateavet vt HP Client Security tarkvaraspikrist.

Drive Encryptioniga saab teostada järgmisi toiminguid:

- Drive Encryptioni sätete valimine:
  - Üksikute draivide või sektsioonide krüptimine või dekrüptimine tarkvarakrüptimist kasutades.
  - Üksikute isekrüptivate draivide krüptimine või dekrüptimine riistvarakrüptimist kasutades.
  - Unerežiimi või puhkerežiimi keelamisega turvalisuse lisamine, et buudieelne Drive Encryptioni autentimine toimuks igakordselt.

MÄRKUS. Krüptida saab ainult sisemisi SATA ja välimisi eSATA kõvakettaid.

- Tagavaravõtmete loomine.
- Krüptitud arvutile juurdepääsu taastamine, kasutades tagavaravõtmeid ja rakendust HP SpareKey.
- Drive Encryptioni buudieelse autentimise lubamine, kasutades parooli, registreeritud sõrmejälge või valitud kiipkaartide PIN-koode.

Drive Encryptioni avamine

Haldurid pääsevad Drive Encryptioni juurde, avades HP Client Security:

1. Klõpsake või koputage avakuval **HP Client Security** (Windows 8).

   või

   Topeltklõpsake või topeltkoputage Windowsi töölaua teadete alal ikooni **HP Client Security**, mis asub tegumiriba parempoolses servas.

2. Klõpsake või koputage ikooni **Drive Encryption**.

Põhiülesanded

Drive Encryptioni käivitamine standardsete kõvaketaste puhul

Standardsed kõvakettad krüptitakse tarkvarakrüptimise abil. Draivi või sektsiooni krüptimiseks tehke järgmist.

1. Käivitage **Drive Encryption**. Lisateavet leiate jaotisest Drive Encryptioni avamine lk 29.
2. Märkige esmalt soovitud draivi või sektsiooni ruut ning klõpsake või koputage valikut **Backup Key** (Tagavaravõti).

MÄRKUS. Paremaks turvalisuseks märkige ruut **Disable sleep mode for increased security** (Unerežiimi keelamine turvalisuse suurendamiseks). Unerežiimi keelamisel ei ole mingit ohtu, et draivi lahtilukustamisel vajalikud andmed mällu salvestuksid.

3. Valige üks või rohkem tagavaravariante ning klõpsake või koputage **Backup** (Varunda). Lisateavet leiate jaotisest Krüptimisvõtmete varundamine lk 33.
4. Krüptimisvõtme varundamise ajal võite tööd jätkata. Ärge arvutit taaskäivitage.

MÄRKUS. Vajadusel palutakse teil arvuti taaskäivitada. Pärast taaskäivitamist kuvatakse enne Windowsi käivitamist draivi krüptimise buudieelne ekraan.

Drive Encryption on aktiveeritud. Valitud sektsioonide krüptimine võib võtta mitmeid tunde, sõltuvalt sektsioonide arvust ja suurusest.

Lisateavet vt HP Client Security tarkvaraspikrist.

Drive Encryptioni käivitamine isekrüptivate kõvaketaste puhul

Trusted Computing Group isekrüptivate draivihalduse OPAL-spetsifikatsioonidele vastavaid isekrüptivaid draive saab krüptida nii tarkvarakrüptimise kui ka riistvarakrüptimisega. Riistvarakrüptimine on palju kiirem kui tarkvarakrüptimine. Samas ei saa te valida, milliseid sektsioone krüptida. Terve ketas, sh kõik sektsioonid krüptitakse.

Kindlate sektsioonide krüptimiseks peate kasutama tarkvarakrüptimist. Tühjendage ruut **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Luba isekrüptivatel ketastel (SED) ainult riistvarakrüptimine).

Drive Encryptioni aktiveerimiseks isekrüptivate ketaste puhul tehke järgmist.

1. Käivitage **Drive Encryption**. Lisateavet leiate jaotisest Drive Encryptioni avamine lk 29.
2. Märkige krüptitava draivi ruut ning klõpsake või koputage valikut **Backup Key** (Tagavaravõti).

MÄRKUS. Paremaks turvalisuseks märkige ruut **Disable Sleep Mode for added security** (Unerežiimi keelamine turvalisuse suurendamiseks). Unerežiimi keelamisel ei ole mingit ohtu, et draivi lahtilukustamisel vajalikud andmed mällu salvestuksid.

3. Valige üks või rohkem tagavaravariante ning klõpsake või koputage **Backup** (Varunda). Lisateavet leiate jaotisest Krüptimisvõtmete varundamine lk 33.
4. Krüptimisvõtme varundamise ajal võite tööd jätkata. Ärge arvutit taaskäivitage.

MÄRKUS. Isekrüptivate ketaste puhul ilmub arvuti väljalülitamise kohta teatis.

Lisateavet vt HP Client Security tarkvaraspikrist.

Drive Encryptioni desaktiveerimine

1. Käivitage **Drive Encryption**. Lisateavet leiate jaotisest Drive Encryptioni avamine lk 29.
2. Tühjendage kõigi krüptitud draivide ruut ning klõpsake või koputage **Apply** (Rakenda).

   Drive Encryptioni desaktiveerimine algab.

MÄRKUS. Kui kasutati tarkvarakrüptimist, algab dekrüptimine. Sõltuvalt krüptitud ketta sektsioonide suurusest võib toiming võtta mitu tundi. Dekrüptimise lõppedes on Drive Encryption desaktiveeritud.

Kui kasutati riistvarakrüptimist, krüptitakse draiv koheselt ning paari minuti pärast on Drive Encryption desaktiveeritud.

Kui Drive Encryption on desaktiveeritud, palutakse riistvarakrüptimise puhul arvuti välja lülitada või tarkvarakrüptimise puhul arvuti taaskäivitada.

Sisselogimine pärast Drive Encryptioni aktiveerimist

Aktiveeritud Drive Encryptioniga ning registreeritud kasutajanimega arvuti käivitamisel peate esmalt sisse logima Drive Encryptioni sisselogimisekraanil:

MÄRKUS. Une- või puhkerežiimist väljudes ei kuvata Drive Encryptioni buudieelset autentimist tarkvara- ega riistvarakrüptimise puhul. Riistvarakrüptimisel on saadaval valik **Disable sleep mode for increased security** (Unerežiimi keelamine turvalisuse suurendamiseks), mis takistab arvutil une- ja puhkerežiimidesse minekut.

Talveunerežiimist väljudes kuvatakse Drive Encryptioni buudieelne autentimine nii tarkvara- kui ka riistvarakrüptimisel.

MÄRKUS. Kui Windowsi haldur on lubanud BIOSi buudieelse turbe rakenduses HP Client Security ja kui üheetapiline sisselogimine on lubatud (vaikesäte), saate pärast BIOSi buudieelset autentimist koheselt arvutisse sisse logida ilma Drive Encryptioni aknas uuesti autentimata.

Ühe kasutaja sisselogimine:

- ▲ Sisestage lehel **Sisselogimine** oma Windowsi parool, kiipkaardi PIN-kood, SpareKey või logige sisse registreeritud sõrmejäljega.

Mitme kasutaja sisselogimine:

1. Valige lehel **Valige kasutaja** rippmenüüst sisselogitav kasutaja, seejärel klõpsake või koputage valikut **Edasi**.
2. Lehel **Sisselogimine** sisestage oma Windowsi parool, kiipkaardi PIN-kood või logige sisse registreeritud sõrmejäljega.

MÄRKUS. Toetatud on järgmised kiipkaardid:

toetatud kiipkaardid

- Gemalto Cyberflex Access 64k V2c

MÄRKUS. Kui Drive Encryptioni sisselogimisekraanil kasutatakse varuvõtit, küsitakse kasutajakontoni jõudmiseks Windowsi sisselogimisel lisamandaate.

Täiendavate kõvaketaste krüptimine

Soovitatav on kasutada rakendust HP Drive Encryption, et kõvaketta krüptimise teel oma andmeid kaitsta. Pärast käivitamist saab täiendavaid kõvakettaid või loodud sektsioone krüptida järgnevate sammudega:

1. Käivitage **Drive Encryption**. Lisateavet leiate jaotisest Drive Encryptioni avamine lk 29.
2. Tarkvarakrüptimisega draivide puhul valige krüptitavad draivi sektsioonid.

MÄRKUS. See kehtib ka kombineeritud draivide puhul, kui kasutatakse korraga ühte või enamat standardset kõvaketast ning ühte või enamat isekrüptivat ketast.

või

- Riistvarakrüptimisega draivide puhul valige lisanduvad krüptitavad draivid.

Lisaülesanded

Drive Encryption haldus (halduritele)

Haldurid saavad kasutada Drive Encryptionit krüptimise oleku nägemiseks ja muutmiseks (mittekrüptitud või krüptitud) arvuti kõigil kõvaketastel.

- Kui olek on lubatud, on Drive Encryption aktiveeritud ja konfigureeritud. Draiv on ühes järgnevatest olekutest:

Tarkvarakrüptimine

- Mittekrüptitud
- Krüptitud
- Krüptimine
- Dekrüptimine

Riistvarakrüptimine

- Krüptitud
- Mittekrüptitud (täiendavatele draividele)

Üksikute sektsioonide krüptimine või dekrüptimine (ainult tarkvarakrüptimine)

Haldurid saavad Drive Encryptionit kasutada ühe või enamate kettasektsioonide krüptimiseks või krüptitud sektsioonide dekrüptimiseks.

1. Käivitage **Drive Encryption**. Lisateavet leiate jaotisest Drive Encryptioni avamine lk 29.
2. Märkige või tühjendage jaotises **Drive Status** (Draivi olek) krüptitava või dekrüptitava kettasektsiooni ruut ning seejärel klõpsake või koputage **Apply** (Rakenda).

MÄRKUS. Kui sektsiooni krüptitakse või dekrüptitakse, kuvab edenemisriba krüptitud sektsiooni protsente.

MÄRKUS. Dünaamilisi sektsioone ei toetata. Kui sektsioon on saadaval, kuid valimisel ei saa seda krüptida, on tegu dünaamilise sektsioon. Dünaamiline sektsioon tekib kettahalduse rakenduses uue sektsiooni loomisel teist sektsiooni vähendades.

Kui sektsioon muudetakse dünaamiliseks, kuvatakse hoiatus.

Kettahaldus

- **Nickname** (Hüüdnimi) – draividele ja sektsioonidele saab lihtsamaks tuvastamiseks anda nimed.
- **Disconnected drives** (Lahtiühendatud draivid) – Drive Encryption saab jälgida arvutist eemaldatud kettaid. Arvutist eemaldatud ketas liigutatakse kohe lahtiühendatud ketaste loendisse. Kui ketas ühendatakse süsteemiga, ilmub see uuesti ühendatud ketaste loendis.
- Kui lahtiühendatud ketast ei ole tarvis enam jälgida või hallata, võite lahtiühendatud ketta lahtiühendatud ketaste loendist eemaldada.
- Drive Encryption jääb aktiivseks niikauaks, kuni kõigi ühendatud ketaste ruudud tühjendatakse ning lahtiühendatud ketaste nimekiri on tühi.

Varundamine ja taaste (haldurile)

Kui Drive Encryption on aktiveeritud, saavad haldurid kasutada krüptimisvõtme varundamise lehte, et varundada krüptimisvõtmeid irdtalletusseadmele ning viia läbi taastamine.

Krüptimisvõtmete varundamine

Haldurid saavad krüptitud ketta krüptimisvõtme varundada irdtalletusseadmele.

⚠ **ETTEVAATUST.** Hoidke tagavaravõtmega irdtalletusseadet kindlas kohas, sest parooli unustamisel, kiipkaardi kaotamisel või juhul, kui sõrmejälge ei ole registreeritud, on see ainuke juurdepääs arvutile. Talletuskoht peaks samuti olema turvaline, sest talletusseade lubab juurdepääsu Windowsile.

1. Käivitage **Drive Encryption**. Lisateavet leiate jaotisest Drive Encryptioni avamine lk 29.
2. Märkige kettale vastav ruut ning seejärel klõpsake või koputage **Backup Key** (Tagavaravõti).
3. Valige jaotises **Create HP Drive Encryption recovery key** (Loo HP Drive Encryptioni taastevõti) ja tehke üks või rohkem järgmistest valikutest:
   - **Removable Storage** (Irdtalletusseade) – märkige ruut ning valige talletusseade, kuhu krüptimisvõti salvestatakse.
   - **SkyDrive** – märkige ruut. Vajalik on internetiühendus. Logige sisse rakendusse Microsoft SkyDrive ning klõpsake või koputage **Yes** (Jah).

     MÄRKUS. Rakendusse SkyDrive talletatud HP Drive Encryptioni varuvõtme kasutamiseks on tarvis see rakendusest SkyDrive alla laadida irdtalletusseadmele ning seejärel ühendada talletusseade arvutiga.

   - **TPM** (ainult teatud mudelitel) – võimaldab taastada andmeid, kasutades teie TPM parooli.

     ⚠ **ETTEVAATUST.** Kui TPM-i sisu peaks kaotsi minema või teie arvuti viga saama, ei pääse te enam sellele varukoopiale ligi. Selle meetodi valimisel peaks olema valitud ka teine varumeetod.
4. Klõpsake või koputage üksust **Backup** (Varundus).

   Krüptimisvõti salvestatakse valitud talletusseadmele.

Aktiveeritud arvutile varuvõtmega juurdepääsu taastamine

Haldurid saavad Drive Encryptioni aktiveerimisel taastada irdtalletusseadmele juurdepääsu varundatud võtmega, valides Drive Encryptionis **Backup Key** (Varuvõti).

1. Sisestage varuvõtit sisaldav irdtalletusseade.
2. Lülitage arvuti sisse.
3. Kui HP Drive Encryption sisselogimise dialoogiboks avaneb, klõpsake või koputage **Recovery** (Taaste).
4. Sisestage varuvõtme failitee või nimi ning klõpsake või koputage **Recovery** (Taaste).
5. Kui kinnitamise dialoogiboks avaneb, klõpsake või koputage **OK**.

   Kuvatakse Windowsi sisselogimisekraan.

MÄRKUS. Kui Drive Encryptioni sisselogimisekraanil kasutatakse varuvõtit, küsitakse kasutajakontodeni jõudmiseks Windowsi sisselogimisel lisamandaate. Pärast taastet on väga soovitatav parool lähtestada.

HP SpareKey taaste läbiviimine

Drive Encryptioni buudieelse taaste raames läbiviidav SpareKey taaste eeldab enne arvutile juurdepääsu turvaküsimustele vastamist. Lisateavet SpareKey taaste kohta leiate HP Client Security tarkvaraspikrist.

HP SpareKey taasteks parooli unustamise korral:

1. Lülitage arvuti sisse.
2. HP Drive Encryptioni lehekülje kuvamisel valige kasutaja sisselogimise lehekülg.
3. Klõpsake nuppu **SpareKey**.

   MÄRKUS. Kui SpareKey ei ole lähtestatud HP Client Security kaudu, ei ole **SpareKey** nupp saadaval.

4. Tippige küsimustele õiged vastused ning klõpsake **Logon** (Sisselogimine).

   Kuvatakse Windowsi sisselogimisekraan.

MÄRKUS. Kui Drive Encryptioni sisselogimisekraanil kasutatakse valikut SpareKey, küsitakse kasutajakontoni jõudmiseks Windowsi sisselogimisel lisamandaate. Pärast taastet on väga soovitatav parool lähtestada.

6 HP File Sanitizer (ainult teatud mudelitel)

File Sanitizer võimaldab arvuti kõvakettal olevate üksuste turvalist ribastamist (näiteks: isikliku teabe või failide, sirvimisajaloo ja -teabe või muude andmekomponentide) ning arvuti kõvaketta perioodilist pleegitamist.

Rakendust File Sanitizer ei saa kasutada järgmiste kõvakettatüüpide puhastamisel või pleegitamisel:

- välkdraivid (SSD), sealhulgas RAID-draivid, mida kasutati SSD-seadmega
- USB-, Firewire- või eSATA-ühendusega välised draivid

Kui SSD-seadmel üritatakse läbi viia andmete ribastamise või ketta pleegitamise toimingut, kuvatakse hoiatus ning toimingut ei viida läbi.

Ribastamine

Ribastamine erineb standardsest Windows® kustutamise toimingust. File Sanitizeriga üksuste ribastamisel kirjutatakse failid üle tähenduseta andmetega, mis muudab esialgsete andmete taastamise võimatuks. Windowsi kustutamise toiming võib jätta faili (või üksuse) kõvakettale olukorda, kus neid saab erinevate meetoditega taastada.

Ribastamise saab ajastada või käsitsi käivitada, valides HP Client Security avakuval rakenduse **File Sanitizer** või kasutades ikooni **File Sanitizer** Windowsi töölaual. Lisateabe saamiseks vaadake Ribastamise ajastamise häälestamine lk 37, Paremklõpsuga ribastamine lk 39 või Ribastamise käsitsi käivitamine lk 39.

MÄRKUS. Fail .dll ribastatakse ja eemaldatakse süsteemist ainult siis, kui see on teisaldatud prügikasti.

Vaba ruumi pleegitamine

Windowsis üksuse kustutamine ei eemalda andmete sisu kõvakettalt täielikult. Windows kustutab ainult viite üksusele või selle asukohale kõvakettal. Üksuse sisu säilib kõvakettal seni, kuni kõvaketta vastav koht kirjutatakse uute andmetega üle.

Vaba ruumi pleegitamine võimaldab kirjutada kustutatud üksuse üle juhusliku sisuga, mis takistab kasutajatel kustutatud andmete originaalsisu nägemist.

MÄRKUS. Vaba ruumi pleegitamine ei paku ribastatud üksusele lisaturvalisust.

Vaba ruumi pleegitamist saab ajastada või käivitada käsitsi varem ribastatud üksuse pleegitamise, valides rakenduse **File Sanitizer** ikooni HP Client Security avakuval või kasutades **File Sanitizer** ikooni Windowsi töölaual. Lisateabe saamiseks vaadake Vaba ruumi pleegitamise ajastamise seadistamine lk 38, Vaba ruumi pleegitamise käsitsi käivitamine lk 40 või File Sanitizeri ikooni kasutamine lk 39.

File Sanitizeri avamine

1. Klõpsake või koputage avakuval **HP Client Security** (Windows 8).

   või

   Topeltklõpsake või topeltkoputage Windowsi töölaua teadete alal ikooni **HP Client Security**, mis asub tegumiriba parempoolses servas.

2. Klõpsake või koputage jaotises **Data** (Andmed) üksust **File Sanitizer**.

või

▲ Topeltklõpsake või topeltkoputage Windowsi töölaual ikooni **File Sanitizer**.

või

▲ Paremklõpsake või koputage ja hoidke Windowsi töölaual ikooni **File Sanitizer**, seejärel valige **Open File Sanitizer** (Ava File Sanitizer).

Häälestustoimingud

Shredding (Ribastamine) – File Sanitizer kustutab või ribastab valitud üksuste kategooriad turvaliselt.

1. Märkige üksuses **Shredding** (Ribastamine) iga soovitud ribastatava failitüübi ruut või tühjendage see, kui te neid faile ribastada ei taha.
   - **Recycle Bin** (Prügikast) – ribastab kõik prügikastis olevad üksused.
   - **Temporary system files** (Ajutised süsteemifailid) – ribastab kõik failid süsteemi ajutises kaustas. Järgnevaid keskkonnamuutujaid otsitakse alltoodud järjekorras ja esimene leitud tee loetakse süsteemikaustaks:
     - TMP
     - TEMP
   - **Ajutised Internetifailid** – ribastab veebisaitide koopiad, pildid ja meediumid, mille brauserid salvestavad kiiremaks kasutamiseks.
   - **Küpsised** – ribastab arvutis kõik veebisaitide failid, mis salvestavad eelistusi, näiteks sisselogimisteave.
2. Ribastamise alustamiseks klõpsake või koputage üksust **Shred** (Ribasta).

Bleaching (Pleegitamine) – kirjutab ruumi vabastamiseks suvalist sisu ja takistab kustutatud objektide taastamist.

▲ Pleegitamise alustamiseks klõpsake või koputage üksust **Bleach** (Pleegita).

File Sanitizer Options (File Sanitizeri valikud) – suvandi lubamiseks märkige vastav ruut; tühjendage ruut suvandi keelamiseks:

- **Enable Desktop icon** (Luba töölaua ikoon) – kuvab File Sanitizeri ikooni Windowsi töölaual.
- **Enable right-click** (Luba paremklõps) – võimaldab paremklõpsata või koputada ja hoida vara ning seejärel valida **HP File Sanitizer – Shred** (HP File Sanitizer – ribasta).

- **Ask for Windows password before manual shredding** (Enne käsitsiribastamise alustamist küsi Windowsi parooli) – nõuab Windowsi parooliga tuvastamist enne käsitsiribastamise alustamist.
- **Shred Cookies and Temporary Internet Files on browser close** (Ribasta küpsised ja ajutised Interneti-failid brauseri sulgemisel) – ribastab brauseri sulgemisel kõik valitud veebiandmed, nt brauseri aadresside mälu.

Ribastamise ajastamise häälestamine

Saate ajastada automaatse ribastamise või üksuste käsitsi ribastamine igal ajal. Lisateavet leiate teemast Häälestustoimingud lk 36.

1. Avage File Sanitizer ning klõpsake või koputage **Sätted**.
2. Valitud üksuste ribastamise ajastamiseks valige jaotises **Shred Schedule** (Ribastamise ajastamine) üksus **Never** (Mitte kunagi), **Once** (Üks kord), **Daily** (Iga päev), **Weekly** (Kord nädalas) või **Monthly** (Kord kuus), seejärel valige päev ja aeg:
   a. Klõpsake või koputage tunni, minuti või AM/PM väljal.
   b. Kerige, kuni soovitud väärtus kuvatakse samal tasemel kui teised väljad.
   c. Klõpsake või koputage ajaväljade kõrval asuvat valget ala.
   d. Korrake toimingut igal väljal, kuni õige aeg on valitud.
3. Loendatud on järgmised neli üksusetüüpi:
   - **Recycle Bin** (Prügikast) – ribastab kõik prügikastis olevad üksused.
   - **Temporary system files** (Ajutised süsteemifailid) – ribastab kõik failid süsteemi ajutises kaustas. Järgnevaid keskkonnamuutujaid otsitakse alltoodud järjekorras ja esimene leitud tee loetakse süsteemikaustaks:
     - TMP
     - TEMP
   - **Ajutised Internetifailid** – ribastab veebisaitide koopiad, pildid ja meediumid, mille brauserid salvestavad kiiremaks kasutamiseks.
   - **Küpsised** – ribastab arvutis kõik veebisaitide failid, mis salvestavad eelistusi, näiteks sisselogimisteave.

   Kui ruudud on valitud, ribastatakse need üksused määratud ajal.
4. Täiendavate ribastatavate üksuste lisamiseks:
   a. Klõpsake või koputage üksust **Scheduled Shred List** (Ajastatud ribastavate üksuste loend), valikut **Add folder** (Lisa kaust) ning seejärel valige fail või kaust.
   b. Esmalt klõpsake või koputage **Ava**, seejärel **OK**.

   Objekti eemaldamiseks ajastatud ribastavate üksuste loendist tühjendage üksuse ruut.

Vaba ruumi pleegitamise ajastamise seadistamine

Vaba ruumi pleegitamine ei paku ribastatud üksusele lisaturvalisust.

1. Avage File Sanitizer ning klõpsake või koputage **Sätted**.
2. Kõvaketta ruumi pleegitamiseks valige jaotises **Bleach Schedule** (Pleegitamise ajastamine) kas **Never** (Mitte kunagi), **Once** (Üks kord), **Daily** (Iga päev), **Weekly** (Kord nädalas) või **Monthly** (Kord kuus) ning seejärel valige päev ja aeg:
   a. Klõpsake või koputage tunni, minuti või AM/PM väljal.
   b. Kerige kuni soovitud aeg kuvatakse samal kõrgusel kui teised väljad.
   c. Klõpsake või koputage ajaväljade kõrval asuvat valget ala.
   d. Korrake kuni soovitud ajastus on valitud.

MÄRKUS. Vaba ruumi pleegitamise toiming võib kesta mõnda aega. Veenduge, et teie arvuti oleks ühendatud vooluvõrku. Kuigi vaba ruumi pleegitamine toimub muu taustal, võib lisanduv protsessorikasutus mõjutada arvuti kasutusomadusi. Vaba ruumi pleegitamine võib toimuda öösel või ajal, kui arvuti ei ole kasutuses.

Failide kaitsmine ribastamise eest

Failide või kaustade kaitsmiseks ribastamise eest:

1. Avage File Sanitizer ning klõpsake või koputage **Sätted**.
2. Klõpsake või koputage jaotises **Never Shred List** (Mitte kunagi ribastatavate üksuste loend) valikut **Add folder** (Lisa kaust), seejärel valige fail või kaust.
3. Esmalt klõpsake või koputage **Ava**, seejärel **OK**.

MÄRKUS. Selles loendis olevad failid on kaitstud seni, kuni nad on loendis.

Üksuse eemaldamiseks mitte kunagi ribastavate üksuste loendist tühjendage üksuse ruut.

Põhiülesanded

Kasutage File Sanitizerit järgmiste ülesannete läbiviimiseks:

- **Kasutage File Sanitizeri ikooni ribastamise alustamiseks** – lohistage failid Windowsi töölaual olevale ikoonile **File Sanitizer**. Lisateavet vt File Sanitizeri ikooni kasutamine lk 39.
- **Kindla üksuse ribastamine või kõigi valitud üksuste ribastamine** – ribastage üksused mis tahes ajal, ajastatud ribastamist ootamata. Lisateavet vt Paremklõpsuga ribastamine lk 39 või Ribastamise käsitsi käivitamine lk 39.
- **Vaba ruumi pleegitamise käsitsi käivitamine** – käivitage vaba ruumi pleegitamine mis tahes ajal. Lisateavet vt Vaba ruumi pleegitamise käsitsi käivitamine lk 40.
- **Logifailide vaatamine** – vaadake ribastamise ja vaba ruumi pleegitamise logifaile, mis sisaldavad kõiki tõrkeid või rikkeid viimastest ribastamistest või vaba ruumi pleegitamistest. Lisateavet vt Logifailide vaatamine lk 40.

MÄRKUS. Ribastamine või vaba ruumi pleegitamine võib kesta mõnda aega. Ehkki ribastamine ja vaba ruumi pleegitamine toimub muude toimingute taustal, võib lisanduv protsessorikasutus mõjutada arvuti kasutusomadusi.

File Sanitizeri ikooni kasutamine

⚠ **ETTEVAATUST.** Ribastatud üksusi ei saa taastada. Valige hoolikalt, milliseid üksusi soovite käsitsi ribastada.

Ribastamise käsitsi alustamisel ribastatakse File Sanitizeri vaates asuvate tavaliste ribastavate üksuste loend (vt Häälestustoimingud lk 36).

Ribastamist saab käsitsi käivitada ühel järgnevatest viisidest:

1. Avage File Sanitizer (vt File Sanitizeri avamine lk 36) ning seejärel klõpsake või koputage **Shred** (Ribasta).
2. Kui kinnitamise dialoogiboks avaneb, veenduge, et soovitud ribastatava üksuse ruut oleks märgitud ning seejärel klõpsake või koputage **OK**.

või

1. Paremklõpsake või koputage ja hoidke Windowsi töölaual ikooni **File Sanitizer**, seejärel klõpsake või koputage **Shred Now** (Ribasta kohe).
2. Kui kinnitamise dialoogiboks avaneb, veenduge, et soovitud ribastatava üksuse ruut oleks märgitud ning seejärel klõpsake või koputage **Shred** (Ribasta).

Paremklõpsuga ribastamine

⚠ **ETTEVAATUST.** Ribastatud üksusi ei saa taastada. Valige hoolikalt, milliseid üksusi soovite käsitsi ribastada.

Kui File Sanitizeri vaates on valitud **Enable right-click shredding** (Luba paremklõpsuga ribastamine), saate üksusi ribastada järgmiselt:

1. Liikuge dokumendi või kaustani, mida soovite ribastada.
2. Paremklõpsake või koputage ja hoidke faili või kausta ning valige **HP File Sanitizer – Shred** (HP File Sanitizer – Ribasta).

Ribastamise käsitsi käivitamine

⚠ **ETTEVAATUST.** Ribastatud üksusi ei saa taastada. Valige hoolikalt, milliseid üksusi soovite käsitsi ribastada.

Ribastamise käsitsi alustamisel ribastatakse File Sanitizeri vaates asuvate tavaliste ribastavate üksuste loend (vt Häälestustoimingud lk 36).

Ribastamist saab käsitsi käivitada ühel järgnevatest viisidest:

1. Avage File Sanitizer (vt File Sanitizeri avamine lk 36) ning seejärel klõpsake või koputage **Shred** (Ribasta).
2. Kui kinnitamise dialoogiboks avaneb, veenduge, et soovitud ribastatava üksuse ruut oleks märgitud ning seejärel klõpsake või koputage **OK**.

või

1. Paremklõpsake või koputage ja hoidke Windowsi töölaual ikooni **File Sanitizer**, seejärel klõpsake või koputage **Shred Now** (Ribasta kohe).
2. Kui kinnitamise dialoogiboks avaneb, veenduge, et soovitud ribastatava üksuse ruut oleks märgitud ning seejärel klõpsake või koputage **Shred** (Ribasta).

Vaba ruumi pleegitamise käsitsi käivitamine

Pleegitamise käsitsi alustamisel pleegitatakse File Sanitizeri vaates asuv tavaliste ribastavate üksuste loend (vt Häälestustoimingud lk 36).

Pleegitamistoimingut saab käsitsi käivitada ühel järgnevatest viisidest:

1. Avage File Sanitizer (vt File Sanitizeri avamine lk 36) ning seejärel klõpsake või koputage **Bleach** (Pleegita).
2. Kui kinnitamise dialoogiboks avaneb, klõpsake või koputage **OK**.

või

1. Paremklõpsake või koputage ja hoidke Windowsi töölaual ikooni **File Sanitizer** ning seejärel klõpsake või koputage **Bleach Now** (Pleegita kohe).
2. Kui kinnitamise dialoogiboks avaneb, klõpsake või koputage **OK**.

Logifailide vaatamine

Iga kord, kui ribastamist või pleegitamist teostatakse, luuakse võimalikke tõrkeid kajastavad logifailid. Logifaile uuendatakse alati vastavalt viimase ribastamise või vaba ruumi pleegitamise toimingule.

MÄRKUS. Edukalt ribastatud või pleegitatud failid logifailides ei kajastu.

Üks logifail on ribastamistoimingute kohta ning teine logifail vaba ruumi pleegitamise toimingute kohta. Mõlemad logifailid asuvad kõvakettal järgmistes kaustades:

- C:\Programmifailid\Hewlett-Packard\File Sanitizer*[Kasutajanimi]*_ShredderLog.txt
- C:\Programmifailid\Hewlett-Packard\File Sanitizer*[Kasutajanimi]*_DiskBleachLog.txt

64-bitistel süsteemidel asuvad mõlemad logifailid kõvakettal järgmistes kaustades:

- C:\Programmifailid (x86)\Hewlett-Packard\File Sanitizer*[Kasutajanimi]*_ShredderLog.txt
- C:\Programmifailid (x86)\Hewlett-Packard\File Sanitizer*[Kasutajanimi]*_DiskBleachLog.txt

7 HP Device Access Manager (ainult teatud mudelitel)

HP Device Access Manager kontrollib juurdepääsu andmetele, keelates andmete edastamise andmeedastusseadmetega.

MÄRKUS. Mõni kasutajaliides/sisendseadmed, nt hiir, klaviatuur, puuteplaat ja sõrmejäljelugeja ei ole Device Access Manageri kontrolli all. Lisateavet leiate jaotisest Haldamata seadmeklassid lk 44.

Windows®operatsioonisüsteemi haldurid kasutavad HP Device Access Manageri süsteemi seadmete juurdepääsu kontrollimiseks ning loata juurdepääsu eest kaitsmiseks:

- Seadme profiilid luuakse igale kasutajale, et määrata lubatud või keelatud juurdepääs seadmetele.
- Just In Time autentimine (JITA) võimaldab varem määratud kasutajatel end autentida juurdepääsuks seadmetele, mis vastasel juhul oleksid keelatud.
- Halduritele ja usaldusväärsetele kasutajatele ei pea kehtima Device Access Manageri poolt seatud seadmetele ligipääsemise piirangud, kui nad on lisatud seadme haldurite rühma. Rühma kuuluvust saab hallata täpsemate sätete lehel.
- Seadme juurdepääsu lubamine või keelamine võib tuleneda rühma liikmelisusest või sõltuda individuaalsetest kasutajatest.
- Seadmeklasside puhul, näiteks CD-ROM-draivid ja DVD-draivid, on võimalik lugemis- ja kirjutamisõigust eraldi lubada või keelata.

HP Device Access Manager on HP Client Security häälestusviisardi järel automaatselt konfigureeritud järgnevalt:

- Just In Time autentimise (JITA) irdtalletusseadmed on haldurite ja kasutajate poolt lubatud.
- Seadmepoliitika lubab muudele seadmetele täieliku juurdepääsu.

Device Access Manageri avamine

1. Klõpsake või koputage avakuval **HP Client Security** (Windows 8).

   või

   Topeltklõpsake või topeltkoputage Windowsi töölaua teadete alal ikooni **HP Client Security**, mis asub tegumiriba parempoolses servas.

2. Klõpsake või koputage jaotises **Device** (Seade) üksust **Device Permissions** (Seadme load).

   - Tavakasutajad saavad vaadata oma olemasolevat seadme juurdepääsu (vt Kasutaja vaade lk 42).
   - Haldurid saavad arvutile konfigureeritud seadmete juurdepääsuõigusi vaadata ja neid muuta, klõpsates või koputades üksust **Change** (Muuda) ja sisestades halduri parooli (vt Süsteemivaade lk 42).

Kasutaja vaade

Kui valitud on **Device Permission** (Seadme load), kuvatakse kasutaja vaade. Sõltuvalt poliitikast saavad tavakasutajad ja haldurid vaadata juurdepääsu nii seadmeklassile kui ka üksikutele arvutiga seotud seadmetele.

- **Current user** (Praegune kasutaja) – kuvatakse praegu sisse logitud kasutaja nimi.
- **Device Class** (Seadmeklass) – kuvatakse seadmete tüübid.
- **Access** (Juurdepääs) – kuvatakse praegu konfigureeritud juurdepääs seadme tüüpidele või kindlatele seadmetele.
- **Duration** (Kestus) – kuvatakse teie juurdepääsu ajalimiit CD/DVD-ROM-draividele või irdketastele.
- **Settings** (Sätted) – haldurid saavad muuta, millistele draividele kehtib juurdepääs Device Access Manageri abil.

Süsteemivaade

Süsteemivaates saavad haldurid lubada või keelata juurdepääsu selle arvutiga seotud seadmetele kasutajarühmale või halduriühmale.

▲ Haldurid pääsevad süsteemivaatesse, klõpsates või koputades üksust **Change** (Muuda), sisestades halduri parooli ja valides siis ühe järgnevatest valikutest:

- **Device Access Manager** – et HP Device Access Manager koos Just In Time autentimisega sisse või välja lülitada, klõpsake või koputage **Sisse** või **Välja**.
- **Users and groups on this PC** (Selle arvuti kasutajad ja rühmad) – kuvab kasutajarühma või halduriühma, kellel on lubatud või keelatud juurdepääs valitud seadmeklassidele.
- **Device Class** (Seadmeklass) – kuvab seadmeklassid ja seadmed, mis on süsteemi installitud või mis võivad olla varem süsteemi installitud. Loendi laiendamiseks klõpsake ikooni **+**. Kuvatakse kõik arvutiga ühendatud seadmed ning liikmelisuse kuvamiseks on halduri- ja kasutajarühmad laiendatud. Seadmeloendi värskendamiseks klõpsake ümarnoolega (värskendamise) ikooni.
  - Kaitset rakendatakse tavaliselt seadmeklassile. Kui juurdepääsutasemeks on **Allow** (Luba), pääseb valitud kasutaja või rühm juurde kõigile selle seadmeklassi seadmetele.
  - Kaitset saab rakendada ka kindlatele seadmetele.
  - Konfigureerige Just In Time autentimine (JITA), lubades valitud kasutajatel autentimise abil juurdepääsu DVD/CD-ROM-draividele või irdketastele. Lisateavet leiate jaotisest JITA konfigureerimine lk 43.
  - Lubage või keelake juurdepääs teistele seadmeklassidele, näiteks irdseadmetele (USB-välkdraivid), jada- ja paralleelportidele, Bluetooth® seadmetele, modemiseadmetele, PCMCIA/ExpressCard-seadmetele, 1394-seadmetele, sõrmejäljelugejale ja kiipkaardilugejale. Kui sõrmejäljelugeja ja kiipkaardilugeja on keelatud, võib neid kasutada autentimismandaatidena, kuid neid ei saa kasutada seansipoliitika tasemel.

    MÄRKUS. Kui Bluetooth-seadmeid kasutatakse autentimismandaatidena, ei tohiks Bluetooth-seadmete juurdepääs olla Device Access Manageri poliitikaga piiratud.

  - Kui valite rühma- või seadmeklassi tasemel sätte ja teilt küsitakse, kas rakendada sätet laste puhul:

    Jah – sätet levitatakse.

Ei – sätet ei levitata.

- Mõne seadmeklassi puhul, näiteks DVD ja CD-ROM, võidakse rakendada ka täpsemaid sätteid, lubades või keelates eraldi lugemis- või kirjutusjuurdepääsu.

MÄRKUS. Halduririihma ei saa kasutajaloendisse lisada.

- **Access** (Juurdepääs) – klõpsake või koputage allanoolt ja valige juurdepääsu lubamiseks või keelamiseks üks järgmistest juurdepääsutüüpidest:
  - **Luba − täielik juurdepääs**
  - **Luba − kirjutuskaitstud**
  - **Allow – JITA Required** (Luba – JITA nõutav) – lisateavet vt JITA konfigureerimine lk 43.

    Selle juurdepääsutüübi valimisel klõpsake või koputage ajalimiidi valimiseks jaotises **Duration** (Kestus) allanoolt.
  - **Keela**
- **Duration** (Kestus) – klõpsake või koputage allanoolt, et valida ajalimiit juurdepääsuks CD/DVD-ROM-idele või irdketastele (vt JITA konfigureerimine lk 43).

JITA konfigureerimine

JITA konfigureerimine võimaldab halduril vaadata ja muuta kasutaja- ja rühmaloendeid, millele on lubatud juurdepääs Just In Time autentimist (JITA) kasutavatele seadmetele.

Kasutajad, kellel on JITA aktiveeritud, pääsevad juurde seadmetele, mille puhul vaates **Device Class Configuration** (Seadmeklassi konfiguratsioon) loodud poliitika on piiratud.

JITA perioodiks võivad olla määratud minutid kuni piiramatu aeg. Piiramatu ajalimiidiga kasutajad pääsevad seadmele juurde alates autentimisest kuni süsteemist väljalogimiseni.

Kui kasutajale on antud piiratud JITA periood, küsitakse kasutajalt üks minut enne JITA perioodi lõppemist, kas ta soovib juurdepääsu pikendada. Niipea kui kasutaja süsteemist välja ja uus kasutaja sisse logib, aegub JITA periood. Kui kasutaja järgmine kord sisse logib ja üritab juurde pääseda JITA-t kasutavale seadmele, palutakse tal sisestada mandaat.

JITA on saadaval järgmiste seadmeklassidega:

- DVD/CD-ROM-draivid
- Irdkettad

JITA poliitika loomine kasutajale või rühmale

Haldurid saavad lubada kasutajatel või rühmadel juurdepääsu Just In Time autentimise (JITA) abil.

1. Käivitage **Device Access Manager** ja klõpsake või koputage **Change** (Muuda).
2. Valige kasutaja või rühm ja klõpsake või koputage jaotise **Access** (Juurdepääs) all kas **Removable Disk drives** (Irdkettad) või **DVD/CD-ROM drives** (DVD/CD-ROM-draivid) allanoolt ja valige siis **Allow – JITA Required** (Luba – JITA nõutav).
3. Klõpsake või koputage jaotises **Duration** (Kestus) allanoolt, et valida JITA juurdepääsu kestus.

Kasutajal tuleb uue JITA sätte jõustumiseks välja ja uuesti sisse logida.

JITA poliitika keelamine kasutajale või rühmale

Haldurid saavad keelata kasutajatel või rühmadel seadmele juurdepääsu Just In Time autentimise abil.

1. Käivitage **Device Access Manager** ja klõpsake või koputage **Change** (Muuda).
2. Valige kasutaja või rühm ja klõpsake või koputage jaotise **Access** (Juurdepääs) all kas **Removable Disk drives** (Irdkettad) või **DVD/CD-ROM drives** (DVD/CD-ROM-draivid) allanoolt ja valige siis **Keela**.

Kui kasutaja logib sisse ja üritab seadmele juurdepääsu, keelatakse see.

Sätted

Vaade **Sätted** lubab halduritel vaadata ja muuta seda, millistele draividele juhib juurdepääsu Device Access Manager.

MÄRKUS. Device Access Manager peab olema lubatud, kui draivitähtede loendit konfigureeritakse (vt Süsteemivaade lk 42).

Haldamata seadmeklassid

HP Device Access Manager ei halda järgmisi seadmeklasse:

- sisend/väljundseadmed
  - CD-ROM
  - Kettadraiv
  - Disketikontroller (FDC)
  - Kõvakettakontroller (HDC)
  - Inimliidese seadme (HID) klass
  - Inimliidese infrapunaseadmed
  - Hiir
  - Mitmepordised jadaseadmed
  - Klaviatuur
  - Plug and play (PnP) printerid
  - Printer
  - Printeri värskendus
- toide
  - Täiustatud toitehalduse (APM) tugi
  - Aku
- Mitmesugused
  - Arvuti
  - Dekooder
  - Ekraan

- Intel® ühendatud kuvadraiver
- Legacard
- Kandjadraiver
- Kandja muutja
- Mälutehnoloogia
- Monitor
- Multifunktsionaalsed
- Võrguklient
- Võrguteenus
- Võrguedastus
- Protsessor
- SCSI adapter
- Turvakiirendi
- Turvaseadmed
- Süsteem
- Tundmatu
- Draiv
- Draivi hetktõmmis

8 HP Trust Circles

HP Trust Circles on failide ja dokumentide turvarakendus, mis kombineerib kaustafailide krüptimise käepärase usaldusringi dokumendijagamise võimalustega. Rakendus krüptib faile, mis asuvad kasutajapõhistes kaustades, andes neile usaldusringi kaitse. Juba kaitse all olevaid faile saavad kasutada ainult usaldusringi liikmed. Kui kaitse all oleva faili saab usaldusringi mitte kuuluv kasutaja, jääb fail krüptituks ja mitte-liige ei pääse faili sisule juurde.

Rakenduse Trust Circles avamine

1. Klõpsake või koputage avakuval rakendust **HP Client Security**.

   või

   Topeltklõpsake Windowsi töölaua teadete alal ikooni **HP Client Security**, mis asub tegumiriba parempoolses servas.

2. Klõpsake või koputage üksuses **Data** (Andmed) valikut **Trust Circles**.

Alustamine

Meilikutsete saatmiseks ja neile vastamiseks on kaks võimalust:

- **Using Microsoft® Outlook** (Microsoft® Outlooki kasutamine) – rakenduse Trust Circles kasutamisel Microsoft Outlookis toimub teiste Trust Circle'i kasutajate Trust Circle'i kutsete ja vastuste töötlemine automaatselt.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)** (Gmaili, Yahoo, Outlook.com ja teiste meiliteenuste (SMTP) kasutamine) – kui sisestate oma nime, meiliaadressi ja parooli, kasutab Trust Circles teie meiliteenust valitud liikmetele kutsete saatmiseks teie usaldusringiga ühinemiseks.

Põhiprofiili loomiseks:

1. Sisestage oma nimi ja meiliaadress ja klõpsake või koputage **Edasi**.

   Nimi on nähtav kõigile liikmetele, kes saavad kutse liituda teie usaldusringiga. Meiliaadressi kasutatakse kutsete saatmiseks, vastuvõtmiseks või neile vastamiseks.

2. Sisestage meilikonto parool ja klõpsake või koputage seejärel **Edasi**.

   Meilisätete õigsuse kontrollimiseks saadetakse proovimeil.

   MÄRKUS. Arvuti peab olema ühendatud Internetti.

3. Sisestage väljale **Trust Circle Name** (Usaldusringi nimi) usaldusringi nimi ja klõpsake või koputage seejärel **Edasi**.

4. Lisage liikmed ja kaustad ning klõpsake või koputage **Edasi**. Usaldusringi loomisel kaasatakse kõik valitud kaustad ning saadetakse meilikutsed kõigile valitud liikmetele. Kui kutset mingil põhjusel saata ei saa, kuvatakse sellekohane teade. Vaates Trust Circle saab liikmeid alati uuesti kutsuda, kui klõpsate valikut **Your Trust Circles** (Teie usaldusringid) ning topeltklõpsate või topeltkoputate seejärel usaldusringi. Lisateavet leiate jaotisest Trust Circles lk 47.

Trust Circles

Usaldusringi saab luua esmasel käivitamisel pärast meiliaadressi sisestamist, või Trust Circle'i vaates:

▲ Klõpsake või koputage Trust Circle'i vaates **Create Trust Circle** (Loo usaldusring) ja sisestage seejärel usaldusringi nimi.

- Liikmete lisamiseks usaldusringi klõpsake või koputage üksuse **Members** (Liikmed) kõrval olevat ikooni **M+** ja järgige seejärel ekraanijuhiseid.
- Kaustade lisamiseks usaldusringi klõpsake või koputage üksuse **Folders** (Kaustad) kõrval olevat ikooni **+** ja järgige seejärel ekraanijuhiseid.

Kaustade lisamine usaldusringi

Kaustade lisamine uude usaldusringi:

- Usaldusringi loomise ajal kaustade lisamiseks klõpsake üksuse **Folders** (Kaustad) kõrval olevat ikooni **+** ja järgige seejärel ekraanijuhiseid.

  või

- Windows Exploreris paremklõpsake või koputage ja hoidke usaldusringi mitte kuuluvat kausta, valige **Trust Circle** ja seejärel **Create Trust Circle from Folder** (Loo kaustast usaldusring).

NÄPUNÄIDE. Valida saab ühe või mitu kausta.

Kaustade lisamine olemasolevasse usaldusringi:

- Klõpsake vaates Trust Circle'i üksust **Your Trust Circles** (Teie usaldusringid), topeltklõpsake või topeltkoputage olemasolevat usaldusringi olemasolevate kaustade kuvamiseks, klõpsake või koputage üksuse **Folders** (Kaustad) kõrval olevat ikooni **+** ja järgige seejärel ekraanijuhiseid.

  või

- Windows Exploreris paremklõpsake või koputage ja hoidke usaldusringi mitte kuuluvat kausta, valige **Trust Circle** (usaldusring) ja seejärel **Add to existing Trust Circle from Folder** (Lisa kaustast olemasolevasse usaldusringi).

NÄPUNÄIDE. Valida saab ühe või mitu kausta.

Kui kaust on usaldusringi lisatud, krüptib Trust Circles selle koos sisuga automaatselt. Kui kõik failid on krüptitud, kuvatakse sellekohane teade. Lisaks ilmub kõigi krüptitud kausta- ja failiikoonide juurde roheline lukusümbol, mis näitab, et need on täielikult kaitstud.

Liikmete lisamine usaldusringi

Liikmete lisamine usaldusringi eeldab kolme sammu:

1. **Kutsu** – kõigepealt kutsub usaldusringi omanik liikme(id). Meilikutse võib saata mitmele kasutajale või levinimistule/rühmale.
2. **Nõustu** – kutsutav saab kutse ja nõustub või lükkab selle tagasi. Kui kutsutav võtab kutse vastu, saadetakse kutsujale meilisõnum. Kui kutse on saadetud rühmale, saab iga liige kutse ja kas nõustub või lükkab selle tagasi.
3. **Registreeri** – kutsujal on viimane võimalus otsustada, kas lisada liige usaldusringi. Kui kutsuja otsustab liikme registreerida, saadetakse kutsutavale vastav teade. Kutsuja ja kutsutav võivad

soovi korral kontrollida kutsumistoimingu turvalisust. Kutsutava jaoks kuvatakse kontrollkood, mille ta peab kutsujale telefoni teel ette lugema. Kui kood on kontrollitud, võib kutsuja saata lõpliku registreerimismeili.

Liikmete lisamine uude usaldusringi:

▲ Usaldusringi loomise ajal liikmete lisamiseks klõpsake üksuse **Members** (Liikmed) kõrval olevat ikooni **M+** ja järgige seejärel ekraanijuhiseid.

- Kui kasutate Outlooki, valige kontaktid Outlooki aadressiraamatust ja klõpsake siis **OK**.
- Kui kasutate muid meiliteenuseid, lisage uued meiliaadressid Trust Circle'isse käsitsi või lisage Trust Circle'is registreeritud meiliaadresside kaudu.

Liikmete lisamine olemasolevasse usaldusringi:

▲ Klõpsake vaates Trust Circle üksust **Your Trust Circles** (Teie usaldusringid), topeltklõpsake või topeltkoputage olemasolevat usaldusringi olemasolevate liikmete kuvamiseks, klõpsake või koputage üksuse **Members** (Liikmed) kõrval olevat ikooni **M+** ja järgige seejärel ekraanijuhiseid.

- Kui kasutate Outlooki, valige kontaktid Outlooki aadressiraamatust ja klõpsake siis **OK**.
- Kui kasutate muid meiliteenuseid, lisage uued meiliaadressid Trust Circle'isse käsitsi või lisage Trust Circle'is registreeritud meiliaadresside kaudu.

Failide lisamine usaldusringi

Faile võite usaldusringi lisada ühel järgmistest viisidest:

- Kopeerige või teisaldage fail olemasolevasse usaldusringi kausta.

  või

- Windows Exploreris paremklõpsake või koputage ja hoidke krüptimata faili, valige üksus **Trust Circle** ja seejärel **Encrypt** (Krüpti). Teil palutakse valida usaldusring, kuhu fail lisada.

NÄPUNÄIDE. Valida saab ühe või mitu faili.

Krüptitud kaustad

Kõik usaldusringi liikmed võivad usaldusringi kuuluvaid faile vaadata ja muuta.

MÄRKUS. Trust Circle Manager/Reader ei sünkrooni faile liikmete vahel.

Faile tuleb jagada olemasolevate vahenditega – meili teel, ftp või pilveteenuste kaudu. Failid, mida usaldusringi kaustades kopeeritakse, teisaldatakse või luuakse, saavad kohese kaitse.

Kaustade eemaldamine usaldusringist

Kausta eemaldamisel usaldusringist dekrüptitakse kaust ja kogu selle sisu, eemaldades sealt kaitse.

- Klõpsake vaates Trust Circle üksust **Your Trust Circles** (Teie usaldusringid), topeltklõpsake või topeltkoputage olemasolevat usaldusringi seal leiduvate kaustade kuvamiseks, klõpsake või koputage kausta kõrval olevat ikooni **prügikast**.

  või

- Windows Exploreris paremklõpsake või koputage ja hoidke usaldusringi kuuluvat kausta, valige **Trust Circle** ja seejärel **Remove from trust circle** (Eemalda usaldusringist).

NÄPUNÄIDE. Valida saab ühe või mitu kausta.

Faili eemaldamine usaldusringist

Faili usaldusringist eemaldamiseks paremklõpsake või koputage ja hoidke Windows Exploreris krüptitud faili, valige üksus **Trust Circle** ja seejärel **Decrypt File** (Dekrüpti fail).

Liikmete eemaldamine usaldusringist

Täielikult registreeritud liiget usaldusringist eemaldada ei saa. Alternatiivseks võimaluseks on luua kõigi teiste liikmetega uus usaldusring, teisaldada kõik failid ja kaustad uude usaldusringi ja seejärel vana usaldusring kustutada. See tagab, et uutele failidele, mida see liige saab, ta enam juurde ei pääse, kuid kõik varem jagatud failid jäävad vana usaldusringi liikmele siiski kättesaadavaks.

Kui liige pole täielikult registreeritud (kui ta on saanud kutse liituda usaldusringiga või pole ta usaldusringi kutset vastu võtnud), saate selle liikme usaldusringist eemaldada ühel järgmistest viisidest:

- Klõpsake või koputage Trust Circle'i vaates üksust **Your Trust Circles** (Teie usaldusringid) ja topeltklõpsake või koputage olemasolevate liikmete loendi nägemiseks usaldusringi. Klõpsake eemaldatava liikme nime kõrval ikooni **prügikast**.
- Klõpsake või koputage Trust Circle'i vaates üksust **Members** (Liikmed) ja topeltklõpsake või koputage liikmel, et näha, millisesse usaldusringi ta kuulub. Liikme sellest usaldusringist eemaldamiseks klõpsake usaldusringi kõrval olevat ikooni **prügikast**.

Usaldusringi kustutamine

Usaldusringi kustutamine eeldab omanikuõigust.

▲ Klõpsake või koputage Trust Circle'i vaates üksust **Your Trust Circles** (Teie usaldusringid) ja seejärel kustutatava usaldusringi kõrval olevat **prügikasti** ikooni.

Sellega eemaldatakse leheküljelt usaldusring ja saadetakse kõigile selle liikmetele teade usaldusringi kustutamise kohta. Kõik usaldusringi kuulunud failid ja kaustad dekrüptitakse.

Eelistuste määramine

Klõpsake või koputage Trust Circle'i vaates üksust **Preferences** (Eelistused). Kuvatakse kolm vahekaarti

- **Meilisätted**

Valik	Kirjeldus
Kasutajanimi	Kuvatakse kasutuselolev kasutajanimi. Muutmiseks sisestage tekstiväljale uus kasutajanimi. Muudatused salvestatakse automaatselt.
Meiliaadress	Kuvatakse kasutuselolev meiliaadress. Selle muutmiseks klõpsake või koputage valikut **Change Email Settings** (Muuda meilisätteid) ja järgige ekraanijuhiseid.

Valik	Kirjeldus
Uue liikme kinnitamine	Valige järgmiste võimaluste vahel: ◦ **Confirm Automatically** (Kinnita automaatselt) – pärast kutsutavalt nõusoleku saamist kinnitatakse ta usaldusringi liikmeks ilma täiendavate toiminguteta ja talle saadetakse kinnitusmeil. ◦ **Confirm Manually** (Kinnita käsitsi) – pärast kutsutavalt nõusoleku saamist nõutakse uue liikme usaldusringi registreerimiseks käsitsi kinnitamist, mispeale saadetakse talle kinnitusmeil. ◦ **Require Verification** (Nõua kinnitamist) – pärast kutsutavalt nõusoleku saamist nõutakse kutsutava täielikuks registreerimiseks kontrollkoodi. Usaldusringi omanik peab kutsutavaga ühendust võtma ja küsima temalt kontrollkoodi. Pärast õige koodi sisestamist saadetakse kutsutavale kinnitusmeil.
Perioodiline autentimine	Perioodiline autentimine nõuab kasutajalt kindlaksmääratud aja (arvestatakse minutites) tagant ja tundlike toimingute teostamisel Windowsi parooli sisestamist. See säte võimaldab kasutajatel autentimist sisse ja välja lülitada.
Autentimise ajalõpp	Valige kindel ajalõpuperiood (minutites), millal autentimist nõuda.
Ära kuva kinnitusteadet	Märkige ruut, et keelata kinnitusteadete kuvamine või tühjendage ruut, et kinnitusteated kuvada.
Soovin anonüümse kasutuse jälgimise abil aidata HP Trust Circle'it paremaks muuta	Märkige ruut, kui soovite programmis osaleda või tühjendage ruut, kui te seda ei soovi.

- **Varundus/taaste**

Valik	Kirjeldus
Varundamine	Kopeerib teie Trust Circle Manageri/Readeri andmed (sätted ja usaldusringid) varufailile. Rikke või süsteemitõrke korral saate seda faili kasutada rakenduse Trust Circles uuesti installimiseks samas olekus, kui te faili salvestasite. **MÄRKUS.** Salvestatakse ainult teie rakenduse Trust Circle andmed (usaldusringid, sätted ja liikmed). Usaldusringi kaustades olevaid faile ei varundata. Need failid tuleb varundada eraldi. Trust Circle'i sätete ja kasutusandmete varundamiseks: **1.** Klõpsake või koputage üksust **Backup** (Varundus). **2.** Valige varufaili kaust ja failinimi, seejärel klõpsake või koputage **Save** (Salvesta). **3.** Sisestage parool, kinnitage see ja klõpsake või koputage **OK**. Parooli nõutakse selle faili taastamiseks.
Taastamine	Taastab varufaililt sätted ja usaldusringid, tavaliselt pärast süsteemiriket või teise arvuti kasutuselevõttu. Trust Circle Manageri sätete ja kasutusandmete taastamiseks: **1.** Klõpsake või koputage üksust **Restore** (Taasta). **2.** Liikuge varufaili kausta ja failinimeni, klõpsake või koputage **Ava**. **3.** Sisestage parool, mille varundamisel valisite.

- **About** (Teave) – kuvatakse Trust Circle Manager/Readeri tarkvaraversioon. Kuvatakse lingid, mis võimaldavad Trust Circle Manageri Pro-versiooniks uuendamist või HP privaatsusavalduse kuvamist.

9 Theft recovery (ainult teatud mudelitel)

Computrace (eraldi ostetav) võimaldab arvutit eemalt jälgida, hallata ja jälitada.

Kui Computrace on aktiveeritud konfigureeritakse seda Absolute Software kliendikeskusest. Kliendikeskuse haldur saab konfigureerida Computrace abil arvutit jälgima või haldama. Kliendikeskuse haldur saab kohalikel ametkondadel aidata arvutit otsida ja tagasi saada, juhul kui süsteem on kadunud või varastatud. Kui Computrace on konfigureeritud jätkab see töötamist isegi siis, kui kõvaketas on kustutatud või asendatud.

Computrace aktiveerimine

1. Looge internetiühendus
2. Avage HP Client Security Lisateavet leiate jaotisest HP Client Security avamine lk 8.
3. Klõpsake **Theft Recovery**.
4. Computrace aktiveerimisviisardi käivitamiseks klõpsake **Get Started** (Alustamine).
5. Sisestage oma kontaktteave ja krediitkaardi makseteave või sisestage eelnevalt ostetud tootevõti.

Aktiveerimisviisard töötleb turvaliselt tehingu ning häälestab teie kasutajakonto Absolute Software kliendikeskuse veebilehel. Kui see on tehtud, saate kliendikeskuse kontoteavet sisaldava kinnitava meilisõnumi.

Kui olete eelnevalt Computrace aktiveerimisviisardi käivitanud ja kliendikeskuses on kasutajakonto juba olemas, saate HP konto esindajaga ühendust võttes osta täiendavad litsentse.

Kliendikeskusesse sisselogimine

1. Külastage veebisaiti https://cc.absolute.com/.
2. Sisestage **Login ID** (Sisselogimise ID) ja **Password** (Parool) väljadele mandaadid, mis saadeti kinnitava meilisõnumiga ja seejärel klõpsake **Log in** (Logi sisse).

Kliendikeskus abil saate:

- Jälgida oma arvuteid
- Kaitsta oma kaugandmeid
- Teatage iga Computrace abil kaitstud arvuti vargusest.

▲ Lisateabe saamiseks Computrace kohta klõpsake üksust **Learn More** (Lisateave).

10 Kohandatud paroolide erandid

Sisselülitusautentimise ja HP Drive Encryptioni tasemetel on paroolide kohanduse toetamine piiratud. Lisateavet leiate jaotisest Windows IME ei ole sisselülitusautentimise või Drive Encryptioni tasemel toetatud lk 52.

Mida teha parooli tagasilükkamisel

Paroole võib tagasi lükata järgmistel põhjustel:

- Kasutaja kasutab toetuseta IME-t. Seda tuleb rohkem ette kahebaidistel keeltel (korea, jaapani ja hiina keel). Probleemi lahendamiseks:
  1. Lisage **Juhtpaneelil** toetatud klaviatuuripaigutus (lisage hiina keele sisendi alla US/inglise klaviatuurid).
  2. Valige vaikesisendiks toetatud klaviatuur.
  3. Käivitage HP Client Security ning seejärel sisestage Windowsi parool.
- Kasutaja kasutab toetuseta tähte. Probleemi lahendamiseks:
  1. Muutke Windowsi parooli nii, et see sisaldaks ainult toetatud tähti. Lisateavet toetamata tähtedest vt Eriliste klahvide kasutamine lk 53.
  2. Käivitage HP Client Security ning seejärel sisestage Windowsi parool.

Windows IME ei ole sisselülitusautentimise või Drive Encryptioni tasemel toetatud

Windowsis võib kasutaja valida IME (sisestusmeetodi redaktor), et sisestada keerukamaid märke ja sümboleid, nt jaapani või hiina tähti, kasutades standardset lääne klaviatuuri.

IME ei ole sisselülitusautentimise või Drive Encryptioni tasemel toetatud. Windowsi parooli ei saa sisestada IMEga sisselülitusautentimise või HP Drive Encryptioni sisselogimisekraanil ning selle katsetamine võib põhjustada lukustumist. Teatud juhtudel ei kuva Microsoft® Windows IME kasutaja paroolisisestamisel

Probleemi lahendamiseks tuleb lülitada ühele toetatavatest klaviatuuripaigutustest, mis vastavad klaviatuuripaigutusele 00000411:

- Microsoft IME jaapani keelele
- Jaapani klaviatuuri paigutus
- Office 2007 IME jaapani keelele – kui Microsoft või mõni kolmas osapool kasutab terminit IME või sisestusmeetodi redaktorit, ei pruugi sisestusmeetod tegelikult olla IME. See võib põhjustada segadust, kuid tarkvara loeb kuueteistkümnendikkoodi esitust. Seega, kui IME vastab toetatava klaviatuuri paigutusele, saab HP Client Security toetada konfiguratsiooni.

⚠ **HOIATUS!** Kui HP Client Security on paigutatud, siis Windows IMEga sisestatud paroolid lükatakse tagasi.

Paroolimuutused, kasutades toetatavat klaviatuuripaigutust

Kui parool on alguses määratud ühe klaviatuuripaigutusega, nt U.S. English (409) ja kasutaja muudab oma parooli teise klaviatuuripaigutusega, nt Latin American (080A), toimib muudetud parool HP Drive Encryptionis, kuid lükatakse tagasi BIOSis, kui kasutaja on parooli sisestanud märke, mis esinevad viimases paigutuses, kuid mitte esimeses (nt ē).

MÄRKUS. Haldurid saavad seda probleemi lahendada, kasutades HP Client Security kasutajate lehekülge (kasutades avalehel ikooni **Hammasratas**), et eemaldada kasutaja rakendusest HP Client Security, valides soovitud klaviatuuripaigutuse operatsioonisüsteemis ning seejärel sama kasutaja kohta HP Client Security häälestusviisardi käivitamisel. BIOS salvestab soovitud klaviatuuripaigutuse ning selle klaviatuuripaigutusega kirjutatavad paroolid jäävad õigesti BIOSi.

Teine võimalik probleem on erinevate klaviatuuripaigutuste kasutamine, mis võivad toota samu märke. Näiteks nii U.S. International klaviatuuripaigutus (20409) ja Latin American klaviatuuripaigutus (080A) sisaldavad märki é, kuigi selle kirjutamiseks on tarvis erinevaid tähekombinatsioone. Kui parool on esmalt salvestatud Latin American klaviatuuripaigutusega, siis Latin American klaviatuuripaigutus on määratud ka BIOSis, isegi kui paroole muudetakse korduvalt, kasutades U.S. International klaviatuuripaigutust.

Eriliste klahvide kasutamine

- Hiina, slovakkia, kanada prantsuse ja tšehhi

  Kui kasutaja valib ühe eelmainitud klaviatuuripaigutustest ja sisestab parooli (nt abcdef), tuleb sama parool sisestada, vajutades samal ajal shift klahvi väiketäheks ja shift klahvi ja caps lock klahvi suurtäheks sisselülitusautentimisel ja HP Drive Encryptioniga. Numbrilised paroolid tuleb sisestada numbriklahve kasutades.

- Korea keel

  Kui kasutaja valib toetatud Koera klaviatuuripaigutuse ja sisestab parooli, tuleb sama parool sisestada, vajutades samal ajal paremat alt klahvi väiketäheks ja paremat alt klahvi ja caps lock klahvi suurtäheks sisselülitusautentimisel ja HP Drive Encryptioniga.

- Toetamata märgid on loendatud järgnevas tabelis:

Keel	Windows	BIOS	Drive Encryption
Araabia keel	ﻻ ,ﻷ, ja ﻹ klahvid tekitavad kaks märki.	ﻻ ,ﻷ, ja ﻹ klahvid tekitavad ühe märgi.	ﻻ ,ﻷ, ja ﻹ klahvid tekitavad ühe märgi.
Kanada prantsuse keel	ç, è, à ja é koos klahviga caps lock on Windowsis Ç, È, À ja É.	ç, è, à ja é koos klahviga caps lock on Windowsi sisselülitusautentimisel ç, è, à ja é.	ç, è, à ja é koos klahviga caps lock on HP Drive Encryptioniga ç, è, à ja é.

Keel	Windows	BIOS	Drive Encryption
Hispaania keel	40a ei ole toetatud. See töötab sellegipoolest, sest tarkvara teisendab selle süsteemi c0a. Sellegipoolest, tulenevalt väikestest erinevustest klaviatuuride paigutustes, on soovitatav, et hispaaniakeelsed kasutajad valiksid oma Windowsi klaviatuuripaigutuseks kas 1040a (Spanish Variation) või 080a (Latin American).	pole saadaval	pole saadaval
US international	◦ Ülemise rea märgid ¡, ¤, ‘, ’, ¥ ja × lükatakse tagasi. ◦ Teise rea märgid å, ®, ja Þ lükatakse tagasi. ◦ Kolmanda rea á, ð, ja ø märgid lükatakse tagasi. ◦ Alumise rea æ märk lükatakse tagasi.	pole saadaval	pole saadaval
Tšehhi keel	◦ Märk ğ lükatakse tagasi. ◦ Märk į lükatakse tagasi. ◦ Märk ų lükatakse tagasi. ◦ Märgid ė, ı, ja ż lükatakse tagasi. ◦ Märgid ģ, ķ, ļ, ņ, ja ţ lükatakse tagasi.	pole saadaval	pole saadaval
Slovaki keel	Märk ż lükatakse tagasi.	◦ Märgid š, ś, ja ş lükatakse tippimisel tagasi, kuid pehme klaviatuuriga sisestamisel võetakse vastu. ◦ Sammuta klahv ţ tekitab kahte märki.	pole saadaval
Ungari keel	Märk ż lükatakse tagasi.	Klahv ţ tekitab kaks märki.	pole saadaval
Sloveeni keel	Klahv żŻ lükatakse Windowsis tagasi ning klahv alt tekitab sammuta klahvi BIOSis.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, ja Š märgid lükatakse BIOSis tagasi.	pole saadaval
Jaapani keel	Saadavuse korral on Microsoft Office 2007 IME parem valik. Sõltumata IME nimest on see tegelikult toetatav klaviatuuripaigutus 411.	pole saadaval	pole saadaval

Sõnastik

Aktiveerimine:
toiming, mis tuleb läbi viia enne Drive Encryptioni funktsioonide kasutama hakkamist. Haldurid saavad aktiveerida Drive Encryptioni HP Client Security häälestusviisardi või HP Client Security kaudu. Aktiveerimisprotsess koosneb tarkvara aktiveerimisest, ketta krüptimisest ja irdtalletusseadmele algse krüptimise varuvõtme loomisest.

Autentimine:
isikutuvastamise toiming, mille käigus kasutatakse teie tuvastamiseks mandaate nagu Windowsi parool, sõrmejälg, kiipkaart, puutevaba kaart või viipekaart.

Automaatne ribastamine:
File Sanitizeris ajastatud ribastamine.

Avaleht:
keskne koht HP Client Security funktsioonide ja sätete juurdepääsuks ja halduseks.

Bluetooth:
tehnoloogia, mis võimaldab Bluetoothi kasutavaid arvuteid, printereid, hiiri, mobiiltelefone ja teisi seadmeid väikse vahemaa tagant raadiolainetega juhtmevabalt ühendada.

Dekrüptimine:
toiming, mida kasutatakse krüptograafias krüptitud andmete teisendamisel lihttekstiks.

Domeen:
rühm arvuteid, mis on osa võrgust ja jagavad ühist kaustade andmebaasi. Igal domeenil on unikaalne nimi ja oma üldised reeglid ning toimingud.

Drive Encryption:
Kaitseb andmeid kõvaketta või kõvaketaste krüptimise kaudu, muutes nii teabe ilma vastava volituseta inimestele loetamatuks.

Drive Encryptioni buudieelne autentimine:
sisselogimisekraan, mis kuvatakse enne Windowsi käivitamist. Kasutajad peavad sisestama oma Windowsi kasutajanime ja parooli või kiipkaardi PIN-koodi või registreeritud sõrmejälje. Kui valitud on üheetapiline sisselogimine, võimaldab Drive Encryption sisselogimisekraanil õige info sisestamisel kohest juurdepääsu ilma Windowsi sisselogimisekraanil uuesti sisse logimata.

Drive Encryptioni sisselogimisekraan:
vt Drive Encryptioni buudieelne autentimine.

DriveLock:
turbefunktsioon, mis lingib kõvaketta kasutajaga ning nõuab arvuti käivitamisel kasutajalt õige DriveLock parooli sisestamist.

Encryption File System (EFS):
süsteem, mis krüptib valitud kaustas kõik failid ja alamkaustad.

Haldur:
Vt *Windowsi haldur*.

HP SpareKey taaste
võimalus arvutile juurdepääsuks vastates õigesti turvaküsimustele.

Hädataastearhiiv:

kaitstud talletusala, mis võimaldab ühe platvormi omaniku tavakasutaja koodi uuesti krüptimist teiseks.

Identiteet:
HP Client Security rühm mandaate ja seadeid, mida käsitletakse nagu konkreetse kasutaja kontot või profiili.

ID-kaart:
Windowsi töölaua vidin, mille eesmärgiks on töölaua visuaalne tuvastamine kasutajanime ja valitud pildid abil.

Just In Time autentimine:
vt HP Device Access Manager tarkvara spikrit.

Kasutaja:
kõik, kes on Drive Encryptionis registreeritud. Halduriõigusteta kasutajatel on Drive Encryptionis piiratud õigused. Nad saavad vaid (halduri loal) registreeruda ning sisse logida.

Kiipkaart:
riistvaraseade, mida saab kasutada autentimisel koos PIN-koodiga.

Kontaktivaba kaart:
kiibiga plastkaart, mida saab kasutada autentimisel.

Krüptimine:
toiming, näiteks algoritmi kasutamine krüptograafias, et teisaldada lihttekst krüpteeritud tekstiks eesmärgiga takistada volitamata adressaate andmeid lugemast. Andmete krüptimise tüüpe on mitmesuguseid ning need on võrguturbe põhialuseks. Levinumate tüüpide hulka kuuluvad andmekrüpteerimise standard ja avaliku koodi krüptimine.

Käsitsi ribastamine:
üksuste või valitud üksuste kohene ribastamine väljaspool ajastatud ribastamist.

Mandaat:
kindel teave riistvaral, mis võimaldab kasutajat autentida.

PIN:
registreeritud kasutajale antud isiklik identifitseerimisnumber, mida kasutatakse autentimisel.

PKI:
avaliku võtme taristu standard, mis määratleb liidesed sertifikaatide ja krüptograafiliste võtmete loomiseks, kasutamiseks ja haldamiseks.

Ribastamine:
algoritmi rakendamine, mis kirjutab üksuses olevad andmed üle suvaliste andmetega.

Riistvarakrüptimine:
Trusted Computing Group'i isekrüptivate ketaste halduse OPAL-spetsifikatsioonidele vastavate isekrüptivate ketaste kasutamine kohese krüptimise läbiviimiseks. Riistvarakrüptimine toimub kohe ning võib aega võtta mõne minuti, tarkvarakrüptimine võib võtta mitmeid tunde.

Rühm:
kasutajate rühm, kellel on samal tasemel juurdepääs või juurdepääsukeeld seadmeklassile või kindlatele seadmetele.

Seadme juurdepääsupoliitika:
seadmete loend, millele kasutajal on lubatud või keelatud juurdepääs.

Seadmeklass:
kõik kindlat tüüpi seadmed, nt draivid.

Sisselogimine:
üksus HP Client Security rakenduses, mis koosneb kasutajanimest ja paroolist (ning mõnikord muust valitud teabest) ja võimaldab juurdepääsu veebisaitidele või teistele programmidele.

Sisselülitusautentimine:
turbefunktsioon, mis nõuab teatud arvuti käivitamisel teatud tüüpi autentimist, näiteks kiipkaarti, turvakiipi või parooli.

Sõrmejälg:
digitaalne väljavõte sõrmejälje pildist. HP Client Security ei salvesta kunagi teie tegelikku sõrmejälge.

Taaskäivitamine:
arvuti taaskäivitamise protsess.

Taaste:
toiming, mille käigus kopeeritakse programmiteave varemsalvestatud varufailist programmi.

Tarkvarakrüptimine:
tarkvara kasutamine kõvaketta sektorhaaval krüpteerimiseks. See toiming on aeglasem kui riistvarakrüptimine.

Trust Circle:
pakub andmetõket, koondades andmed usaldusväärse määratud rühma kasutusse. See takistab andmete juhuslikku või tahtlikku sattumist võõrastesse kätesse. Tehnoloogia CryptoMill's Zero Overhead Key Management seob andmed krüptograafiliselt usaldusringi kasutusse. See tõkestab dokumentide või muu tundliku teabe dekrüptimist väljaspool usaldusringi.

Trust Circle Manager/Reader:
Trust Circle Reader saab vastu võtta ainult Trust Circle Manageri kasutajate saadetud kutseid. Trust Circle Manager võimaldab siiski ka usaldusringide loomist. Funktsioonid sisaldavad võimalust kutsuda liikmeid usaldusringi ja võtta teistelt usaldusringi liikmetelt kutseid vastu ka meili teel. Kui kasutajad on usaldusringi loonud, saab usaldusringiga kaitstud faile jagada turvaliselt.

Turvalise sisselogimise meetod:
meetod, mida kasutatakse arvutisse sisselogimisel.

Usaldusringi kaust:
kõik usaldusringiga kaitstud kaustad.

Usaldusväärse platvormi mooduli (TPM) sisseehitatud turvakiip:
TPM autendib eelkõige arvuti, mitte kasutaja, salvestades hostsüsteemi spetsiifilise teabe, näiteks krüptimiskoodid, digitaalserdid ja paroolid. TPM vähendab riski, et arvutis olev teave sattub ohtu füüsilise varguse või välise häkkeri rünnaku tagajärjel.

vaba ruumi pleegitamine
suvaliste andmete kirjutamine kustutatud varale ja kasutamata ruumile. See toiming vähendab kustutatud üksusi nii, et originaalüksust on keerulisem taastada.

Varundus:
varundusfunktsiooni kasutamine tähtsa programmiteabe koopia salvestamiseks asukohta väljaspool programmi. Koopiat saab hiljem kasutada teabe taasteks samal arvutil või mõnel teisel arvutil.

Viipekaart:
kiibiga plastkaart, mida kasutatakse autentimisel koos teiste lisaturvalisust andvate mandaatidega.

Windowsi haldur:
kasutaja, kellel on täielik õigus muuta lube ja hallata teisi kasutajaid.

Windowsi kasutajakonto:
kasutaja, kellel on õigus võrku või kindlasse arvutisse sisse logida.

Windowsi sisselogimise turvalisus:
kaitseb Windowsi kontot nõudes ligipääsuks spetsiifilisi mandaate.

Võrgukonto:
Windowsi kasutaja või halduri konto kohalikus arvutis, töögrupis või domeenis.

Ühekordne sisselogimine:
funktsioon, mis salvestab autentimisteabe ja võimaldab kasutada klienditurbesüsteemi HP Client Security ligipääsuks Internetile ja Windowsi rakendusele, mis nõuavad autentimist parooli abil.

Ühendatud seade:
riistvaraline seade, mis on ühendatud mõnda arvuti porti.

Üksus:
andmekomponent, mis koosneb isiklikust teabest või failidest, sirvimisajaloost ja seotud andmetest jne, mis asuvad kõvakettal.

Tähestikuline register