HP Client Security

Darbo pradžia

„Bluetooth“ – atitinkamo savininko prekės ženklas, kuriuo pagal licenciją naudojasi „Hewlett-Packard“. „Intel“ yra „Intel Corporation“ prekės ženklas JAV ir kitose šalyse ir yra naudojamas pagal licenciją. „Microsoft“ ir „Windows“ yra JAV registruoti „Microsoft Corporation“ prekių ženklai.

Čia pateikta informacija gali būti pakeista apie tai nepranešus. Vienintelės produktų ir paslaugų garantijos yra išdėstytos raštiškuose garantijų patvirtinimuose, pateikiamuose su tam tikrais produktais ir paslaugomis. Nė vienas iš išdėstytų dalykų negali būti laikomas papildoma garantija. HP neprisiima atsakomybės už šio dokumento techninės ar redagavimo klaidas ar praleidimus.

Pirmasis leidimas: 2013 m. rugpjūčio mėn.

Dokumento numeris: 735339-E21

Turinys

1 Įvadas į „HP Client Security Manager“

„HP Client Security“ leidžia apsaugoti savo duomenis, įrenginį ir tapatybę, taip pagerinant jūsų kompiuterio saugą.

Jūsų kompiuteriui tinkantys programinės įrangos moduliai gali skirtis priklausomai nuo jūsų kompiuterio modelio.

„HP Client Security“ programinės įrangos moduliai gali būti iš anksto įdiegti ar įkelti arba juos galima atsisiųsti iš HP svetainės. Norėdami gauti daugiau informacijos, eikite į http://www.hp.com.

PASTABA: Šiame vadove pateikti nurodymai tariant, kad jūs jau esate įdiegę reikiamus „HP Client Security“ programinės įrangos modulius.

„HP Client Security“ funkcijos

Toliau pateiktoje lentelėje aprašytos pagrindinės „HP Client Security“ modulių funkcijos.

Modulis	Pagrindinės funkcijos
„HP Client Security Manager“	Administratoriai gali atlikti šias funkcijas: • Apsaugoti savo kompiuterį prieš paleidžiant „Windows®“. • Apsaugoti savo „Windows“ abonementą naudojant griežtą autentifikavimą • Valdyti prisijungimą prie tinklalapių ir programų bei valdyti savo slaptažodžius • Lengvai pakeisti savo „Windows“ operacinės sistemos slaptažodį • Naudoti pirštų atspaudus dar geresniam saugumui ir patogumui • Nustatyti autentifikavimui lustinę kortelę, bekontaktę kortelę ar judesio kortelę • Identifikuojant naudoti savo „Bluetooth“ telefoną • Nustatyti PIN ir taip išplėsti autentifikavimo galimybes • Konfigūruoti prisijungimo ir seanso strategijas • Sukurti atsarginę programos duomenų kopiją ir atkurti programos duomenis • Įtraukti daugiau programų, pvz., „HP Drive Encryption“, „HP File Sanitizer“, „HP Trust Circles“, „HP Device Access Manager“ ir „HP Computrace“ Bendrieji vartotojai gali atlikti šias funkcijas: • Peržiūrėti šifravimo būklės ir „Device Access Manager“ nuostatas. • Suaktyvinti „Computrace“. • Konfigūruoti nustatymus ir atsarginių kopijų kūrimo ir atkūrimo parinktis.

Modulis	Pagrindinės funkcijos
„Password Manager“	Bendrieji vartotojai gali atlikti šias funkcijas: • Sutvarkyti ir nustatyti vartotojo vardus ir slaptažodžius. • Sukurti sudėtingesnius slaptažodžius ir taip patobulinti el. pašto ir žiniatinklio abonementų saugą. „Password Manager“ užpildo ir pateikia informaciją automatiškai. • Supaprastinti prisijungimo procesą naudojant vienintelės registracijos funkciją, kuri automatiškai įsimena ir pritaiko vartotojo kredencialus. • Pažymėti, kad abonementas yra pažeistas - jūs būsite įspėti apie kitą (-us) abonementą (-us) su panašiais kredencialais. • Importuoti prisijungimo duomenis iš palaikomos naršyklės.
„HP Drive Encryption“ (tik tam tikruose modeliuose)	• Suteikia pilną viso standžiojo disko šifravimą. • Pradeda išankstinės įkrovos autentifikavimą, kad po to būtų galima iškoduoti ir pasiekti duomenis. • Suteikia galimybę suaktyvinti užsišifruojančius diskų įrenginius (tik tam tikruose modeliuose).
„HP Device Access Manager“	• IT valdytojams leidžia valdyti prieigą prie įrenginių atsižvelgiant į vartotojų profilius. • Neleidžia nesankcionuotiems vartotojams pašalinti duomenų naudojant išorinę saugojimo laikmeną ir saugo, kad į sistemą iš išorinių laikmenų nepatektų virusai. • Administratoriams leidžia išjungti konkrečių vartotojų ar vartotojų grupių prieigą prie ryšio įrenginių.
„HP Trust Circles“	• Apsaugoja failus ir dokumentus. • Užšifruoja failus, esančius vartotojo nurodytuose aplankuose ir juos apsaugo patikimame rate. • Failus naudoti ir bendrinti leidžia tik patikimame rate esantiems vartotojams.
„Theft Recovery“ („Computrace“, įsigyjama atskirai)	• Norint suaktyvinti, stebėjimo ir sekimo prenumeratą reikia įsigyti atskirai. • Suteikia saugų išteklių stebėjimą. • Stebi vartotojo veiklą ir aparatūros bei programinės įrangos pakeitimus. • Priemonė yra aktyvi net tada, kai standusis diskas yra suformuotas iš naujo arba pakeistas kitu.

„HP Client Security“ produkto aprašymas ir įprastinio naudojimo pavyzdžiai

Daugumoje „HP Client Security“ produktų yra vartotojo autentifikavimas (dažniausiai slaptažodis) ir administratoriaus atsarginė kopija, kuri suteikia prieigą tais atvejais, kai slaptažodžiai yra prarasti, jų nėra arba jie pamiršti, o taip pat tuomet, kai prieiga reikalinga bendrajai saugai.

PASTABA: Kai kurie „HP Client Security“ produktai sukurti riboti prieigą prie duomenų. Jei duomenys vartotojui yra tokie svarbūs, kad juos vartotojas verčiau prarastų, nei rizikuotų, kad jie būtų pažeisti, tuomet šiuos duomenis reikėtų užšifruoti. Rekomenduojama saugioje vietoje sukurti visų duomenų atsargines kopijas.

„Password Manager“

„Password Manager“ išsaugoja vartotojų vardus ir slaptažodžius ir šią priemonę galima naudoti norint:

- Išsaugoti prisijungimo vardus ir slaptažodžius prieigai prie interneto ar el. pašto.
- Vartotoją automatiškai prijungti prie žiniatinklio svetainės ar el. pašto.
- Valdyti ir tvarkyti autentifikavimus.
- Pasirinkti žiniatinklio arba tinklo išteklius ir tiesiogiai pasinaudoti saitu.
- Prireikus peržiūrėti vardus ir slaptažodžius.
- Pažymėti, kad abonementas yra pažeistas - jūs būsite įspėti apie kitą (-us) abonementą (-us) su panašiais kredencialais.
- Importuoti prisijungimo duomenis iš palaikomos naršyklės.

1 pavyzdys: Pirkimų agentė, dirbanti stambiam gamintojui, didžiausią dalį verslo sandorių sudaro internetu. Ji taip pat dažnai lanko keletą populiarių žiniatinklio svetainių, prie kurių reikia prisijungti naudojant prisijungimo informaciją. Ji daug nusimano apie saugą, todėl skirtingiems abonementams nenaudoja to pačio slaptažodžio. Pirkimų agentė nusprendė naudoti „Password Manager“ ir žiniatinklio saitus susieti su skirtingais vartotojo vardais ir slaptažodžiais. Kai ji nueina į žiniatinklio svetainę prisijungti, „Password Manager“ kredencialus pateikia automatiškai. Jei ji pageidauja peržiūrėti vartotojo vardus ir slaptažodžius, „Password Manager“ gali sukonfigūruoti taip, kad jie būtų parodyti.

„Password Manager“ taip pat galima naudoti norint valdyti ir tvarkyti autentifikavimus. Ši priemonė vartotojui leidžia pasirinkti žiniatinklio arba tinklo išteklius ir tiesiogiai pasinaudoti saitu. Vartotojas prireikus taip pat gali peržiūrėti vartotojo vardus ir slaptažodžius.

2 pavyzdys: Darbštus darbuotojas buvo paaukštintas pareigose ir dabar valdys visą buhalterinės apskaitos skyrių. Skyriaus darbuotojai turi prisijungti prie daug klientų abonementų žiniatinklyje, kurių kiekvienas naudoja skirtingą prisijungimo informaciją. Šia informacija turi bendrai naudotis ir kiti darbuotojai, todėl konfidencialumas kelia problemų. Darbuotojas nusprendžia naudojant „Password Manager“ sutvarkyti visus žiniatinklio saitus, įmonės vartotojų vardus ir slaptažodžius. Tai atlikęs darbuotojas „Password Manager“ priemonę įdiegia kitiems darbuotojams ir šie gali dirbti su žiniatinklio abonementais ir niekada nesužinoti naudojamų prisijungimo kredencialų.

„HP Drive Encryption“ (tik tam tikruose modeliuose)

„HP Drive Encryption“ priemonė naudojama siekiant apriboti prieigą prie duomenų visame kompiuterio standžiajame diske arba papildomame diskų įrenginyje. „Drive Encryption“ taip pat gali valdyti užsišifruojančius diskus.

1 pavyzdys: Gydytojas nori užtikrinti, kad duomenis kompiuterio standžiajame diske pasiekti galėtų tik jis. Gydytojas suaktyvina „Drive Encryption“ priemonę, kuri prieš prisijungiant prie „Windows“ reikalauja išankstinės įkrovos autentifikavomo. Priemonę nustačius, standusis diskas nebus pasiekiamas neįvedus slaptažodžio prieš paleidžiant operacinę sistemą. Gydytojas gali dar labiau sustiprinti diskų įrenginio saugą pasirinkdamas duomenų užšifravimo užsišifruojančiais diskais parinktį.

2 pavyzdys: Ligoninės administratorius nori užtikrinti, kad jo vietiniame kompiuteryje esantys duomenys būtų pasiekiami tik gydytojams ir įgaliotiesiems darbuotojams, tačiau nenori atskleisti savo asmeninio slaptažodžio. IT skyriaus darbuotojai administratorių, gydytojus ir visus įgaliotuosius darbuotojus įtraukia kaip „Drive Encryption“ vartotojus. Nuo šiol tik įgaliotieji asmenys gali įkrauti kompiuterį arba domeną naudodami asmeninius vartotojo vardus ir slaptažodžius.

„HP Device Access Manager“ (tik tam tikruose modeliuose)

„HP Device Access Manager“ administratoriui leidžia riboti ir valdyti prieigą prie aparatūros. Naudojant „Device Access Manager“ galima užblokuoti nesankcionuotą prieigą prie USB „flash“ disko. Ši priemonė taip pat gali apriboti prieigą prie CD / DVD diskų įrenginių, USB įrenginių valdymo, tinklo ryšių ir t. t. Pavyzdžiu galėtų būti toks atvejis, kai išorės tiekėjui yra reikalinga prieiga prie įmonės kompiuterių, tačiau jis negali duomenų nukopijuoti į USB atmintinę.

1 pavyzdys: Medicinos reikmenis tiekiančios įmonės vadybininkas dažnai kartu dirba su asmeniniais medicininiais įrašais ir savo įmonės informacija. Darbuotojams reikalinga prieiga prie šių duomenų, tačiau nepaprastai svarbu, kad duomenys nebūtų perkelti iš kompiuterio į USB atmintinę ar kitą išorinę saugojimo laikmeną. Tinklas yra saugus, tačiau kompiuteriuose yra įrašymo į kompaktinį diską įrenginiai ir USB prievadai, kuriuos naudojant duomenys gali būti nukopijuoti arba pavogti. Vadybininkas norėdamas išjungti USB prievadus ir įrašymo į kompaktinį diską įrenginius naudoja „Device Access Manager“ priemonę. Nors USB prievadai yra užblokuoti, pelė ir klaviatūra ir toliau veiks.

2 pavyzdys: Draudimo įmonė nenori, kad jos darbuotojai įdiegtų ar įkeltų programinę įrangą ar duomenis iš namų. Kai kuriems darbuotojams yra reikalinga prieiga prie visų kompiuterių USB prievadų. IT valdytojas norėdamas įjungti prieigą vieniems darbuotojams, tačiau užblokuoti išorinę prieigą kitiems, naudoja „Device Access Manager“ priemonę.

„Computrace“ (įsigyjama atskirai)

„Computrace“ (įsigyjama atskirai) yra paslauga, kurios dėka vartotojui prisijungus prie interneto galima susekti pavogtą kompiuterį. Bet to „Computrace“ gali padėti nuotoliniu būdu valdyti kompiuterius ir nustatyti jų buvimo vietą, o taip pat stebėti kompiuterio naudojimą ir programas.

1 pavyzdys: Mokyklos direktorius IT skyriui davė nurodymus stebėti visus kompiuterius jo mokykloje. Atlikus kompiuterių inventorizaciją, IT administratorius visus kompiuterius užregistravo „Computrace“ priemone, kad juos būtų galima susekti, jei kompiuteriai būtų pavogti. Neseniai buvo pastebėta, kad dingo keletas kompiuterių, todėl IT administratorius apie tai įspėjo valdžios organus ir „Computrace“ darbuotojus. Kompiuteriai valdžios organų buvo surasti ir sugrąžinti mokyklai.

2 pavyzdys: Nekilnojamo turto agentūra turi valdyti ir naujinti kompiuterius visame pasaulyje. Agentūros darbuotojai kompiuterius stebi ir naujina naudodamiesi „Computrace“ priemone, todėl dėl kiekvieno atskiro kompiuterio nebereikia siųsti IT darbuotojo.

Svarbiausių saugos tikslų pasiekimas

„HP Client Security“ moduliai gali veikti kartu ir pateikti įvairių saugos problemų sprendimus, įskaitant šiuos svarbiausius saugos tikslus:

- Apsaugą nuo suplanuotų vagysčių
- Prieigos prie slaptų duomenų apribojimą
- Apsisaugojimą nuo nesankcionuotos prieigos iš vidinės arba išorinės vietos
- Sudėtingesnių slaptažodžių sukūrimo strategijas

Apsauga nuo suplanuotų vagysčių

Suplanuotos vagystės pavyzdžiu galėtų būti kompiuterio su konfidencialiais duomenimis ir klientų informacija vagystė oro uosto saugos kontrolės punkte. Šios funkcijos padeda apsisaugoti nuo suplanuotų vagysčių:

- Autentifikavimas prieš įkraunant sistemą, jei įjungtas, padeda užkirsti kelią prieigai prie operacinės sistemos.
  - „HP Client Security“ – žr. „„HP Client Security““ 12 puslapyje.
  - „HP Drive Encryption“ – žr. „„HP Drive Encryption“ (tik tam tikruose modeliuose)“ 31 puslapyje.
- Šifravimas padeda užtikrinti, kad duomenys nebūtų pasiekiami net ir tuomet, kai standusis diskas yra išimtas ir įdiegtas neapsaugotoje sistemoje.
- „Computrace“ gali susekti pavogto kompiuterio buvimo vietą.
  - „Computrace“ – žr. „„Theft Recovery“ (tik tam tikruose modeliuose)“ 55 puslapyje.

Prieigos prie slaptų duomenų apribojimas

Tarkime, kad sutarčių auditorius dirba audituojamoje įmonėje ir jam yra suteikta prieiga kompiuteryje prie slaptų finansinių duomenų. Nenorėtumėte, kad auditorius galėtų atsispausdinti failus arba išsaugoti juos rašomajame įrenginyje, pvz., kompaktiniame diske. Ši funkcija padeda apriboti prieigą prie duomenų:

- „HP Device Access Manager“ IT valdytojams leidžia apriboti prieigą prie ryšio įrenginių, kad slaptos informacijos nebūtų galima nukopijuoti iš standžiojo disko. Žr. „Sistemos rodinys“ 45 puslapyje.

Apsisaugojimas nuo nesankcionuotos prieigos iš vidinės arba išorinės vietos

Nesankcionuota prieiga prie neapsaugoto verslo kompiuterio kelia rimtą riziką įmonės tinklo ištekliams, pvz., finansinių tarnybų informacijai, vadovui arba mokslinių tyrimų ir plėtros komandai, asmeninei informacijai, tokiai kaip pacientų įrašai ar asmeniniai finansiniai įrašai. Šios funkcijos padeda apsisaugoti nuo nesankcionuotos prieigos:

- Autentifikavimas prieš įkraunant sistemą, jei įjungtas, padeda užkirsti kelią prieigai prie operacinės sistemos. (žr. skyrių „„HP Drive Encryption“ (tik tam tikruose modeliuose)“ 31 puslapyje.
- „HP Client Security“ padeda užtikrinti, kad nesankcionuoti vartotojai negalėtų gauti slaptažodžių ar prieigos prie slaptažodžiu apsaugotų programų. Žr. „„HP Client Security““ 12 puslapyje.
- „HP Device Access Manager“ IT valdytojams leidžia apriboti prieigą prie rašomųjų įrenginių, kad slaptos informacijos nebūtų galima nukopijuoti iš standžiojo disko. Žr. „„HP Device Access Manager“ (tik tam tikruose modeliuose)“ 44 puslapyje.

Sudėtingesnių slaptažodžių sukūrimo strategijos

Jei įsigalioja įmonės strategija, reikalaujanti, kad naudojant daugelį internetinių programų būtų taikoma sudėtingesnio slaptažodžio politika, „Password Manager“ priemonė pateikia apsaugotą slaptažodžių saugyklą ir patogią vienintelės registracijos funkciją. Žr. „„Password Manager““ 18 puslapyje.

Papildomi saugos elementai

Saugos vaidmenų priskyrimas

Valdant kompiuterių saugą (ypač stambiose organizacijose) atsakomybę ir teises svarbu paskirstyti tarp įvairaus rango administratorių ir vartotojų.

PASTABA: Mažose organizacijose ar asmeninio vartojimo atveju šį vaidmenį gali atlikti vienas ir tas pats asmuo.

Naudojant „HP Client Security“ priemonę, saugos prievolės ir teisės gali būti suskirstytos į šiuos vaidmenis:

- Saugos pareigūnas – nustato įmonės arba tinklo saugos lygmenį ir nusprendžia, kurias saugos priemones įdiegti, pvz., „Drive Encryption“.

  PASTABA: Saugos pareigūnas, bendradarbiaudamas su HP, gali individualizuoti daugelį „HP Client Security“ funkcijų. Norėdami gauti daugiau informacijos, eikite į http://www.hp.com.

- IT administratorius – pritaiko ir valdo saugos priemones, kurias nustato saugos pareigūnas. Taip pat gali įjungti ir išjungti kai kurias funkcijas. Pavyzdžiui, jei saugos pareigūnas nusprendė įdiegti lustines korteles, IT administratorius gali įjungti ir slaptažodį, ir lustinės kortelės režimą.
- Vartotojas – naudojasi saugos priemonėmis. Pavyzdžiui, jei saugos pareigūnas ir IT administratorius sistemoje įjungė lustines korteles, vartotojas gali nustatyti lustinių kortelių PIN ir kortelę naudoti autentifikuojant.

ĮSPĖJIMAS: Administratoriai yra skatinami laikytis „geriausios praktikos“ ribojant galutinio vartotojo teises bei ribojant vartotojo prieigą.

Nesankcionuotiems vartotojams neturėtų būti suteiktos administratoriaus teisės.

„HP Client Security“ slaptažodžių valdymas

Dauguma „HP Client Security“ funkcijų yra apsaugotos slaptažodžiais. Toliau pateiktoje lentelėje nurodyti dažniausiai vartojami slaptažodžiai, programinės įrangos moduliai, kai yra nustatytas slaptažodis ir slaptažodžio funkcija.

Slaptažodžiai, kuriuos nustato ir naudoja tik IT administratoriai, taip pat yra nurodyti šioje lentelėje. Visus kitus slaptažodžius gali nustatyti įprastiniai vartotojai arba administratoriai.

„HP Client Security“ slaptažodis	Nustatytas šiame modulyje	Funkcija
„Windows“ registravimosi slaptažodis	„Windows“ valdymo skyde arba „HP Client Security“ priemonėje	Gali būti naudojamas prisijungiant rankiniu būdu ir atliekant autentifikavimą norint pasiekti įvairias „HP Client Security“ funkcijas
„HP Client Security“ atsarginių kopijų kūrimo ir atkūrimo slaptažodis	„HP Client Security“ priemonėje, nustatomas atskiro vartotojo	Apsaugo prieigą prie „HP Client Security“ atsarginių kopijų kūrimo ir atkūrimo failo.
Lustinės kortelės PIN	„Credential Manager“ priemonėje	Gali būti naudojamas kaip daugelio dalių autentifikavimas. Gali būti naudojamas kaip „Windows“ autentifikavimas. Autentifikuoja „Drive Encryption“ vartotojus, jei pasirinkta lustinė kortelė.

Saugaus slaptažodžio kūrimas

Kurdami slaptažodžius turite pirmiausia laikytis programos nustatytų nurodymų. Vis dėlto atsižvelkite į šias rekomendacijas, kurios jums padės sukurti sudėtingesnius slaptažodžius ir sumažinti pažeistų slaptažodžių riziką:

- Naudokite slaptažodžius, kurie susideda iš daugiau nei 6 simbolių, o geriausia daugiau nei 8.
- Visame slaptažodyje naudokite mažąsias ir didžiąsias raides.
- Jei įmanoma, visuomet naudokite raidžių ir skaičių derinius ir įtraukite specialiuosius simbolius bei skyrybos ženklus.
- Raktinio žodžio raides pakeiskite specialiaisiais simboliais arba skaičiais. Pavyzdžiui, vietoje L raidės galite naudoti skaičių 1.
- Naudokite dviejų skirtingų kalbų žodžius.
- Žodžio arba frazės viduryje įveskite skaičius arba specialiosius simbolius, pvz., „Mary2-2Cat45.“
- Nenaudokite slaptažodžio iš žodyno.
- Slaptažodžiu nepasirinkite savo vardo ar kitos asmeninės informacijos, pvz., gimimo datos, augintinių vardų ar motinos mergautinės pavardės, net jei šiuos žodžius įrašytumėte atbuline tvarka.
- Slaptažodį reguliariai keiskite. Galite pakeisti tik keletą daugėjančių simbolių.
- Jei slaptažodį užsirašysite, nelaikykite jo visiems matomoje vietoje netoliese kompiuterio.
- Slaptažodžio neišsaugokite faile, pvz., el. pašte, kompiuteryje.
- Nebendrinkite abonementų ir niekam nepasakykite savo slaptažodžio.

Kredencialų ir nustatymų atsarginių kopijų kūrimas

„HP Client Security“ priemonės atsarginių kopijų kūrimo ir atkūrimo įrankį galite naudoti kaip centrinę vietą, kurioje iš įdiegtų „HP Client Security“ modulių galite sukurti atsarginę saugos kredencialų kopiją ir juos atkurti.

2 Darbo pradžia

Norėdami sukonfigūruoti „HP Client Security“ programą, kad ją būtų galima naudoti su jūsų kredencialais, „HP Client Security“ paleiskite vienu iš šių būdų. Kai vedlį vartotojas užbaigs, jo dar kartą paleisti tas pats vartotojas nebegalės.

1. Pradžios arba programėlių ekrane spustelėkite arba bakstelėkite **„HP Client Security“** programėlę („Windows 8“).

   – arba –

   „Windows“ darbalaukyje spustelėkite arba bakstelėkite **„HP Client Security Gadget“** („Windows 7“).

   – arba –

   „Windows“ darbalaukyje, pranešimų srityje, esančioje užduočių juostos dešinėje pusėje, dukart spustelėkite arba dukart bakstelėkite **„HP Client Security“** piktogramą.

   – arba –

   „Windows“ darbalaukyje, pranešimų srityje spustelėkite arba bakstelėkite **„HP Client Security“** piktogramą ir tada pasirinkite **„Open HP Client Security“** (atidaryti „HP Client Security“).

2. Paleidžiamas „HP Client Security“ sąrankos vedlys ir parodomas pasveikinimo puslapis.

3. Perskaitykite pasveikinimo ekraną, įvesdami „Windows“ slaptažodį patvirtinkite savo tapatybę ir tada spustelėkite arba bakstelėkite **Toliau**.

   Jei dar nesate susikūrę „Windows“ slaptažodžio, būsite paraginti jį susikurti. „Windows“ slaptažodis reikalingas norint abonementą apsaugoti, kad jo nepasiektų nesankcionuoti asmenys ir norint pasinaudoti „HP Client Security“ funkcijomis.

4. „HP SpareKey“ puslapyje pasirinkite tris saugos klausimus. Įveskite atsakymą kiekvienam klausimui ir tada spustelėkite **Toliau**. Taip pat leidžiama naudoti savo klausimus. Daugiau informacijos rasite skyriuje „„HP SpareKey“ – slaptažodžio atkūrimas“ 14 puslapyje.

5. Pirštų atspaudų puslapyje įtraukite bent mažiausią reikiamą skaičių pirštų atspaudų ir tada spustelėkite arba bakstelėkite **Toliau**. Daugiau informacijos rasite skyriuje „Pirštų atspaudai“ 12 puslapyje.

6. „Drive Encryption“ puslapyje suaktyvinkite šifravimą, sukurti atsarginę šifravimo rakto kopiją ir tada spustelėkite arba bakstelėkite **Toliau**. Norėdami gauti daugiau informacijos, žr. „HP Drive Encryption“ programinės įrangos žinyną.

PASTABA: tai taikoma, kai vartotojas yra administratorius ir „HP Client Security“ sąrankos vedlys nebuvo anksčiau administratoriaus konfigūruotas.

7. Paskutiniame vedlio puslapyje spustelėkite arba bakstelėkite **Baigti**.

   Šiame puslapyje pateikiamos funkcijų ir kredencialų būsenos.

8. „HP Client Security“ sąrankos vedlys užtikrina, kad būtų suaktyvintos „Just In Time Authentication“ ir „File Sanitizer“ funkcijos. Norėdami gauti daugiau informacijos, žr. „HP Device Access Manager“ ir „HP File Sanitizer“ programinių įrangų žinynus.

PASTABA: tai taikoma, kai vartotojas yra administratorius ir „HP Client Security“ sąrankos vedlys nebuvo anksčiau administratoriaus konfigūruotas.

„HP Client Security“ atidarymas

„HP Client Security“ programą atidaryti galite vienu iš toliau pateiktų būdų:

PASTABA: prieš paleidžiant „HP Client Security“ programą, „HP Client Security“ sąrakos vedlys turi būti užbaigtas.

- Pradžios arba programėlių ekrane spustelėkite arba bakstelėkite **„HP Client Security“** programėlę.

  – arba –

  „Windows“ darbalaukyje spustelėkite arba bakstelėkite **„HP Client Security“** įtaisą („Windows 7“).

  – arba –

  „Windows“ darbalaukyje, pranešimų srityje, esančioje užduočių juostos dešinėje pusėje, dukart spustelėkite arba dukart bakstelėkite **„HP Client Security“** piktogramą.

  – arba –

  „Windows“ darbalaukyje, pranešimų srityje spustelėkite arba bakstelėkite **„HP Client Security“** piktogramą ir tada pasirinkite **„Open HP Client Security“** (atidaryti „HP Client Security“).

3 Supaprastintas sąrankos vadovas smulkiam verslui

Šis skyrius sukurtas siekiant pademonstruoti, kaip „HP Client Security“ priemonėje smulkiam verslui paprastais veiksmais suaktyvinti paprasčiausias ir naudingiausias parinktis. Gausybės įrankių ir parinkčių dėka galėsite pakoreguoti savo nustatymus ir nustatyti prieigos kontrolę. Šio supaprastinto sąrankos vadovo tikslas yra kiekvieną modulį paleisti mažiausiai pastangų ir laiko reikalaujančiu būdu. Norėdami gauti papildomos informacijos, pasirinkite jus dominantį modulį ir spustelėkite **?** arba žinyno mygtuką, esantį viršutiniame dešinajame kampe. Šis mygtukas automatiškai parodys informaciją, kuri jums suteiks pagalbą, susijusią su šiuo metu ekrane rodomu langu.

Darbo pradžia

1. „HP Client Security“ atidarykite „Windows“ darbalaukyje, pranešimų srityje, esančioje užduočių juostos dešinėje pusėje, dukart spustelėdami **„HP Client Security“** piktogramą.
2. Įveskite savo „Windows“ slaptažodį arba sukurkite „Windows“ slaptažodį.
3. Užbaikite „HP Client Security“ sąranką.

Kad galėtumėte naudotis „HP Client Security“ priemone, autentifikuoti turėsite tik vieną kartą – prisijungiant prie „Windows“; žr. „Saugos priemonės“ 27 puslapyje.

„Password Manager“

Kiekvienas iš mūsų naudojasi nemažu skaičiumi slaptažodžių, ypač, jei reguliariai lankosi žiniatinklio svetainėse arba naudoja programas, prie kurių reikia prisijungti. Įprastinis vartotojas naudoja tą patį slaptažodį visoms programoms arba parodo savo kūrybiškumą ir greitai užmiršta, kuris slaptažodis priklauso kuriai programai.

„Password Manager“ gali automatiškai įsiminti jūsų slaptažodžius arba suteikti galimybę išskirti, kurias svetaines įsiminti ir kurias užmiršti. Jums prisijungus prie kompiuterio, „Password Manager“ pateiks jūsų slaptažodžius arba kredencialus reikalingoms programoms arba žiniatinklio svetainėms.

Kai atidarysite programą arba apsilankysite žiniatinklio svetainėje, kurioms reikia įvesti kredencialus, „Password Manager“ automatiškai atpažins svetainę ir jūsų paklaus, ar norite, kad programa įsimintų jūsų informaciją. Jei nenorite įtraukti tam tikrų svetainių, užklausą galite atmesti.

Norėdami pradėti išsaugoti žiniatinklio vietas, vartotojo vardus ir slaptažodžius:

1. Pavyzdžiui, nueikite į norimą žiniatinklio svetainę arba programą ir tuomet spustelėkite „Password Manager“ piktogramą, esančią tinklalapio viršutiniame kairiajame kampe ir įtraukite žiniatinklio autentifikavimą.
2. Pavadinkite saitą (pasirinktina) ir „Password Manager“ priemonėje įveskite vartotojo vardą bei slaptažodį.
3. Užbaigę spustelėkite mygtuką **Gerai**.
4. „Password Manager“ taip pat gali išsaugoti jūsų vartotojo vardą ir slaptažodžius, naudojamus tinklo objektams arba priskirtiems tinklo diskų įrenginiams.

„Password Manager“ priemonėje išsaugotų autentifikavimų peržiūra ir valdymas

„Password Manager“ iš centrinės vietos jums leidžia peržiūrėti autentifikavimus, juos valdyti, paleisti ir sukurti atsarginę jų kopiją. „Password Manager“ taip pat palaiko išsaugotų svetainių paleidimą iš „Windows“.

Norėdami atidaryti „Password Manager“, naudokite klaviatūros derinį Ctrl+„Windows“ klavišas+h, atidarykite „Password Manager“ ir tuomet spustelėkite **prisijungti**, kad paleistumėte ir autentifikuotumėte išsaugotą nuorodą.

„Password Manager“ parinktis **Redaguoti** jums leidžia peržiūrėti ir modifikuoti vardą bei prisijungimo vardą ir net atskleisti slaptažodžius.

„HP Client Security“ smulkiam verslui leidžia sukurti visų kredencialų ir nustatymų atsarginę kopiją ir (arba) leidžia juos nukopijuoti į kitą kompiuterį.

„HP Device Access Manager“

Naudojant „Device Access Manager“ priemonę galima apriboti įvairių vidinių ir išorinių laikmenų įrenginių naudojimą ir taip užtikrinti, kad jūsų duomenys būtų apsaugoti standžiajame diske, o ne svetimose rankose. Pavyzdžiu galėtų būti situacija, kai vartotojui leidžiama prieiga prie jūsų duomenų, tačiau kopijavimas į kompaktinį diską, asmeninį muzikos grotuvą ar USB atminties įrenginį yra blokuojamas.

1. Atidarykite **„Device Access Manager“** (žr. „„Device Access Manager“ atidarymas“ 44 puslapyje).

   Parodoma dabartiniui vartotojui taikoma prieiga.

2. Norėdami vartotojams, grupėmsar įrenginiams pakeisti prieigą, spustelėkite arba bakstelėkite **Keisti**. Daugiau informacijos rasite skyriuje „Sistemos rodinys“ 45 puslapyje.

„HP Drive Encryption“

„HP Drive Encryption“ priemonė naudojama siekiant apsaugoti jūsų duomenis užšifruojant visą standųjį diską. Jūsų duomenys, esantys standžiajame diske, bus apsaugoti, jei jūsų kompiuteris būtų pavogtas ir (arba) standusis diskas išimtas iš originalaus kompiuterio ir įdėtas į kitą.

Papildomas saugos privalumas yra tas, kad „Drive Encryption“ priemonė reikalauja tinkamai autentifikuoti naudojant vartotojo vardą ir slaptažodį prieš paleidžiant operacinę sistemą. Šis procesas vadinamas autentifikavimu prieš įkraunant sistemą.

Siekiant palengvinti naudojimą, keletas programinės įrangos modulių automatiškai sinchronizuoja slaptažodžius, įskaitant „Windows“ vartotojo abonementus, autentifikavimo domenus, „HP Drive Encryption“, „Password Manager“ ir „HP Client Security“.

Jei norite pradinės sąrankos metu naudojant „HP Client Security“ sąrankos vedlį nustatyti „HP Drive Encryption“ priemonę, žr. „Darbo pradžia“ 8 puslapyje.

4 „HP Client Security“

Pagrindinis „HP Client Security“ puslapis yra pagrindinė greitos prieigos prie „HP Client Security“ funkcijų, programų ir nustatymų vieta. Pagrindinis puslapis yra suskirstytas į tris dalis:

- **DUOMENYS** – suteikia prieigą prie programų, kuriomis valdoma duomenų sauga.
- **ĮRENGINYS** – suteikia prieigą prie programų, kuriomis valdoma įrenginio sauga.
- **TAPATYBĖ** – suteikia autentifikavimo kredencialų įtraukimą ir valdymą.

Perkelkite žymeklį virš programos plytelės, kad būtų parodytas programos aprašymas.

„HP Client Security“ gali pateikti saitus į vartotojo ir administracinius nustatymus, esančius puslapio apačioje. „HP Client Security“ suteikia prieigą prie papildomų nustatymų ir funkcijų – spustelėkite arba bakstelėkite **„Gear“** (nustatymų) piktogramą.

Tapatybės funkcijos, programos ir nustatymai

„HP Client Security“ programos suteikiamos tapatybės funkcijos, programos ir nustatymai padės jums valdyti įvairius skaitmeninės tapatybės aspektus. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite vieną iš toliau pateikiamų plytelių ir tada įveskite savo „Windows“ slaptažodį:

- **Piršto atspaudai** – įtraukia ir valdo jūsų piršto atspaudo kredencialus.
- **„SpareKey“** – nustato ir valdo jūsų „HP SpareKey“ kredencialus, kurie gali būti naudojami prisijungiant prie kompiuterio, jei pametėte ar nežinote, kur padėjote, savo kitus kredencialus. Ši priemonė taip pat leidžia pakeisti užmirštą slaptažodį.
- **„Windows“ slaptažodis** – suteikia lengvą prieigą pakeisti „Windows“ slaptažodį.
- **„Bluetooth“ įrenginiai** – leidžia įtraukti ir valdyti savo „Bluetooth“ įrenginius.
- **Kortelės** – leidžia įtraukti ir valdyti lustines korteles, bekontaktes korteles ir judesio korteles.
- **PIN** – leidžia įtraukti ir valdyti PIN kredencialus.
- **„RSA SecurID“** – leidžia įtraukti ir valdyti „RSA SecurID“ kredencialus (jei nustatyti atitinkami nustatymai).
- **„Password Manager“** – leidžia valdyti internetinio abonemento ir programų slaptažodžius.

Pirštų atspaudai

„HP Client Security“ sąrankos vedlys jums padės atlikti pirštų atspaudų nustatymo arba „registravimo“ procesus.

Pirštų atspaudus taip pat galite užregistruoti arba ištrinti pirštų atspaudų puslapyje, kurį pasieksite spustelėdami arba bakstelėdami **pirštų atspaudų** piktogramą, esančią „HP Client Security“ pagrindiniame puslapyje.

1. Pirštų atspaudų puslapyje pabraukite pirštu, kol jis bus sėkmingai užregistruotas.

   Kiek reikia užregistruoti pirštų nurodyta puslapyje. Pageidautina, kad naudotumėte smilių arba didįjį pirštą.

2. Norėdami ištrinti anksčiau įtrauktus pirštų atspaudus, spustelėkite arba bakstelėkite **Trinti**.

3. Norėdami įtraukti papildomus pirštų atspaudus, spustelėkite arba bakstelėkite **„Enroll an additional fingerprint“** (įtraukti papildomą piršto atspaudą).

4. Prieš išeidami iš puslapio spustelėkite arba bakstelėkite **Įrašyti**.

⚠ **ĮSPĖJIMAS:** jei pirštų atspaudai įtraukiami naudojantis vedliu, pirštų atspaudų informacija nėra išsaugojama tol, kol nepaspaudžiama **Toliau**. Jei kompiuteris stovi tam tikrą laiką neaktyvus arba jūs uždarote programą, jūsų atlikti pakeitimai **nebus** išsaugojami.

- Norėdami pasiekti pirštų atspaudų administracinius nustatymus, kur administratoriai gali nurodyti įtraukimo, tikslumo ir kitus nustatymus, spustelėkite arba bakstelėkite **„Administrative Settings“** (administraciniai nustatymai, reikalingos administratoriaus teisės).
- Norėdami pasiekti pirštų atspaudų vartotojo nustatymus, kur galite nurodyti piršto atspaudo atpažinimo išvaizdą ir veikimą valdančius nustatymus, spustelėkite arba bakstelėkite **„Vartotojo nustatymai“**.

Pirštų atspaudų administraciniai nustatymai

Administratoriai gali nurodyti įtraukimo, tikslumo ir kitus nustatymus pirštų atspaudų skaitytuvui. Reikalingos administratoriaus teisės.

- Norėdami pasiekti piršto atspaudo kredencialų administracinius nustatymus, pirštų atspaudų puslapyje spustelėkite arba bakstelėkite **„Administrative Settings“** (administraciniai nustatymai).

- **Vartotojo įtraukimas** – pasirinkite mažiausią ir didžiausią pirštų atspaudų skaičių, kurį vartotojui leidžiama įtraukti.
- **Atpažinimas** – perkelkite slankiklį ir sureguliuokite pirštų atspaudų skaitytuvo jautrumą nuskaitant jūsų piršto pabraukimus.

  Jei jūsų piršto atspaudas nėra nuosekliai atpažįstamas, gali prireikti pasirinkti mažesnį atpažinimo nustatymą. Didesnis nustatymas padidina piršto atspaudo braukimo variacijų jautrumą ir todėl yra mažesnė galimybė, kad bus patvirtintas klaidingas atspaudas. **Vidutiniškai aukštas** nustatymas suteikia puikų saugos ir patogumo derinį.

Pirštų atspaudų vartotojo nustatymai

Pirštų atspaudų vartotojo nustatymų puslapyje galite nurodyti piršto atspaudo atpažinimo išvaizdą ir veikimą valdančius nustatymus.

▲ Norėdami pasiekti piršto atspaudo kredencialų vartotojo nustatymus, pirštų atspaudų puslapyje spustelėkite arba bakstelėkite **„Vartotojo nustatymai“**.

- **Įgalinti garsinį foną** – pagal numatytuosius nustatymus „HP Client Security“ programa pabraukus pirštu pateikia garsinį atsiliepimą konkretiems programos įvykiams pagrodama skirtingus garsus. Šiems įvykiams galite priskirti naujus garsus iš Garso skirtuko, esančio „Windows“ valdymo skydo garso nustatyme arba jei garsinį atsiliepimą norite išjungti, išvalykite žymės langelį.
- **Rodyti nuskaitymo kokybės atsiliepimą** – jei norite, kad būtų parodyti visi braukimai nepriklausomai nuo jų kokybės, pasirinkite žymės langelį. Jei norite, kad būtų rodomi tik geri braukimai, išvalykite žymės langelį.

„HP SpareKey“ – slaptažodžio atkūrimas

„HP SpareKey“ leidžia naudotis kompiuteriu (palaikomose platformose) atsakius į tris saugos klausimus.

„HP Client Security“ jus paragins pradinės sąrankos metu „HP Client Security“ sąrankos vedlyje nusistatyti asmeninį „HP SpareKey“.

Norėdami nusistatyti „HP SpareKey“:

1. Vedlio „HP SpareKey“ puslapyje pasirinkite tris saugos klausimus ir tada įveskite atsakymą kiekvienam klausimui.

   Galite pasirinkti klausimą iš numatytųjų klausimų sąrašo arba galite užrašyti savo klausimą.

2. Spustelėkite arba bakstelėkite **Įtraukti**.

Norėdami ištrinti „HP SpareKey“:

▲ Spustelėkite arba bakstelėkite **„Delete your SpareKey“** (trinti „SpareKey“).

Nustatę „SpareKey“, savo kompiuterį galite pasiekti naudodami „SpareKey“ autentifikavimo įjungus prisijungimo ekrane arba „Windows“ pasveikinimo ekrane.

Pasirinkti skirtingus klausimus arba pakeisti savo atsakymus galite „SpareKey“ puslapyje, kurį pasieksite pasinaudoję slaptažodžio atkūrimo plytele, esančia „HP Client Security“ pagrindiniame puslapyje.

Norėdami pasiekti „HP SpareKey“ nustatymus, kur administratoriai gali nurodyti nustatymus, susijusius su „HP SpareKey“ kredencialais, spustelėkite **Nuostatos** (reikalingos administratoriaus teisės).

„HP SpareKey Settings“ nustatymai

„HP SpareKey“ nustatymų puslapyje galite nurodyti veikimą ir „HP SpareKey“ kredencialų naudojimą valdančius nustatymus.

▲ Norėdami paleisti „HP SpareKey“ nustatymų puslapį, „HP SpareKey“ puslapyje spustelėkite arba bakstelėkite **Nuostatos** (reikalingos administratoriaus teisės).

Administratoriai gali pasirinkti šiuos nustatymus:

- „HP SpareKey“ programos sąrankos metu nurodyti, kurie klausimai bus pateikti kiekvienam vartotojui.
- Pridėti iki trijų saugos klausimų, kurie bus įtraukti į vartotojams pateikiamą klausimų sąrašą.
- Pasirinkti, ar leisti vartotojams įrašyti savo pačių saugos klausimus.
- Nurodyti, kurioms autentifikavimo aplinkoms („Windows“ ar autentifikavimui įjungus) leisti naudoti „HP SpareKey“ atkuriant slaptažodį.

„Windows“ slaptažodis

„HP Client Security“ programos dėka „Windows“ slaptažodį pakeisite lengviau ir greičiau nei tai padarytumėte naudodami „Windows“ valdymo skydą.

Norėdami pakeisti savo „Windows“ slaptažodį:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Windows“ slaptažodis.**
2. Įveskite savo dabartinį slaptažodį į **Dabartinio „Windows“ slaptažodžio** teksto langelį.
3. Įveskite naują slaptažodį į **Naujo „Windows“ slaptažodžio** teksto langelį ir tada dar kartą jį įveskite į teksto langelį **Patvirtinkite naują slaptažodį**.
4. Spustelėkite arba bakstelėkite **Keisti**, kad dabartinis slaptažodis būtų tuojau pat pakeistas jūsų įvestu nauju slaptažodžiu.

„Bluetooth“ įrenginiai

Jei administratorius „Bluetooth“ įgalino kaip autentifikavimo kredencialą, papildomai saugai kartu su kitais kredencialais galite nustatyti savo telefoną.

PASTABA: palaikomi tik „Bluetooth“ telefono įrenginiai

1. Patikrinkite, ar kompiuteryje įgalinta „Bluetooth" funkcija, ir kad „Bluetooth“ telefonas yra nustatytas veikti aptikimo režimu. Norint prijungti telefoną, gali prireikti įvesti automatiškai sukurtą kodą į „Bluetooth“ įrenginį. Priklausomai nuo „Bluetooth“ įrenginio konfigūravimo nustatymų, gali prireikti palyginti kompiuterio ir telefono susiejimo kodus.
2. Norėdami įtraukti telefoną, jį pasirinkite ir tada spustelėkite arba bakstelėkite **Įtraukti**.

Norėdami pasiekti „„Bluetooth“ įrenginių nustatymai“ 15 puslapyje“ puslapį, kur administratoriai gali nurodyti „Bluetooth“ įrenginių nustatymus, spustelėkite **Nuostatos** (reikalingos administratoriaus teisės).

„Bluetooth“ įrenginių nustatymai

Administratoriai gali nurodyti šiuos „Bluetooth“ įrenginių kredencialių veikimą ir naudojimą valdančius nustatymus:

Automatinis autentifikavimas

- **Automatiškai naudoti prijungtą ir įtrauktą „Bluetooth“ įrenginį tapatybės patvirtinimo metu** – pasirinkite žymės langelį ir leiskite vartotojams autentifikuojant naudoti „Bluetooth“ kredencialus neatliekant jokių veiksmų arba išvalykite žymės langelį, jei norite šią parinktį išjungti.

„Bluetooth“ artumas

- **Užrakinti komputerį, kai įtrauktas „Bluetooth“ įrenginys patenka už kompiuterio veikimo diapazono** – pasirinkite žymės langelį ir užrakinkite kompiuterį, kai „Bluetooth“ įrenginys, kuris buvo prijungtas prisijungimo metu, patenka už diapazono arba išvalykite žymės langelį, jei norite šią parinktį išjungti.

PASTABA: jūsų kompiuterio „Bluetooth“ modulis turi palaikyti šią galimybę, kad galėtumėte pilnai išnaudoti šią funkciją.

Kortelės

„HP Client Security“ gali palaikyti keletą skirtingų tipų identifikavimo kortelių, kurios yra mažos plastmasinės kortelės su kompiuterio lustu. Jos apima lustines korteles, bekontaktes korteles ir judesio korteles. Jei viena iš šių kortelių ir atitinkamas skaitytuvas yra prijungti prie kompiuterio, jei administratorius yra iš gamintojo įdiegęs atitinkamą tvarkyklę ir jei administratorius yra kortelę įgalinęs kaip autentifikavimo kredencialus, kortelę galite naudoti kaip autentifikavimo kredencialus.

Lustinėms kortelėms gamintojas turėtų suteikti įrankius, kuriais diegiamas saugos sertifikatas ir valdomas PIN – juos „HP Client Security“ naudoja savo saugos algoritme. PIN naudojamų simbolių skaičius ir jų tipas gali varijuoti. Prieš kortelę naudojant, ją turi inicijuoti administratorius.

„HP Client Security“ programa palaiko šiuos lustinių kortelių formatus:

- CSP
- PKCS11

„HP Client Security“ programa palaiko šiuos bekontakčių kortelių formatus:

- Bekontaktes „HID iCLASS“ atminties korteles
- Bekontaktes „MiFare Classic“ 1 k, 4 k ir mini atminties korteles

„HP Client Security“ programa palaiko šiuos judesio kortelių formatus:

- HID judesio korteles

Norėdami įtraukti lustinę kortelę:

1. Įdėkite kortelę į prijungtą lustinių kortelių skaitytuvą.
2. Kai kortelė bus atpažinta, įveskite kortelės PIN kodą ir tada spustelėkite arba bakstelėkite **Įtraukti**.

Norėdami pakeisti lustinės kortelės PIN:

1. Įdėkite kortelę į prijungtą lustinių kortelių skaitytuvą.
2. Kai kortelė bus atpažinta, įveskite kortelės PIN kodą ir tada spustelėkite arba bakstelėkite **„Authenticate“** (autentifikuoti).
3. Spustelėkite arba bakstelėkite **„Change PIN“** (keisti PIN) ir tada įveskite naują PIN.

Norėdami įtraukti bekontaktę arba judesio kortelę:

1. Kortelę uždėkite ant atitinkamo skaitytuvo arba padėkite labai arti.
2. Kai kortelė bus atpažinta, spustelėkite arba bakstelėkite **Įtraukti**.

Norėdami ištrinti įtrauktą kortelę:

1. Įdėkite arba uždėkite (atitinkamai) kortelę ant skaitytuvo.
2. Tik lustinėms kortelėms: įveskite priskirtą kortelės PIN kodą ir tada spustelėkite arba bakstelėkite **„Authenticate“** (autentifikuoti).
3. Spustelėkite arba bakstelėkite **Trinti**.

Kai kortelė yra įtraukiama, informacija apie kortelę yra pateikiama parinktyje **„Enrolled Cards“** (įtrauktos kortelės). Kai kortelė yra ištrinama, ji iš sąrašo pašalinama.

Norėdami pasiekti judesio, bekontaktės ir lustinės kortelių nustatymus, kur administratoriai gali nurodyti nustatymus, susijusius su kortelių kredencialais, spustelėkite arba bakstelėkite **Nuostatos** (reikalingos administratoriaus teisės).

Judesio, bekontaktės ir lustinės kortelių nustatymai

Norėdami pasiekti kortelės nustatymus, sąraše spustelėkite arba bakstelėkite kortelė ir tada spustelėkite arba bakstelėkite pasirodžiusią rodyklę.

Norėdami pakeisti lustinės kortelės PIN:

1. Įdėkite arba uždėkite (atitinkamai) kortelę ant skaitytuvo
2. Įveskite priskirtą kortelės PIN kodą ir tada spustelėkite arba bakstelėkite **Tęsti**.
3. Įveskite ir patvirtinkite naują PIN ir tada spustelėkite arba bakstelėkite **Tęsti**.

Norėdami inicijuoti lustinės kortelės PIN:

1. Įdėkite arba uždėkite (atitinkamai) kortelę ant skaitytuvo
2. Įveskite priskirtą kortelės PIN kodą ir tada spustelėkite arba bakstelėkite **Tęsti**.
3. Įveskite ir patvirtinkite naują PIN ir tada spustelėkite arba bakstelėkite **Tęsti**.
4. Spustelėdami arba bakstelėdami **Taip** patvirtinkite inicijavimą.

Norėdami išvalyti kortelės duomenis:

1. Įdėkite arba uždėkite (atitinkamai) kortelę ant skaitytuvo
2. Įveskite priskirtą kortelės PIN kodą (tik lustinėms kortelėms) ir tada spustelėkite arba bakstelėkite **Tęsti**.
3. Spustelėdami arba bakstelėdami **Taip** patvirtinkite trynimą.

PIN

Jei administratorius PIN įgalino kaip autentifikavimo kredencialą, papildomai saugai kartu su kitais kredencialais galite nustatyti PIN.

Norėdami nustatyti naują PIN:

▲ Įveskite PIN, dar kartą įvesdami jį patvirtinkite ir tada spustelėkite arba bakstelėkite **Taikyti**.

Norėdami ištrinti PIN:

▲ Spustelėkite arba bakstelėkite **Trinti** ir tada patvirtinkite spustelėdami arba bakstelėdami **Taip**.

Norėdami pasiekti PIN nustatymus, kur administratoriai gali nurodyti nustatymus, susijusius su PIN kredencialais, spustelėkite arba bakstelėkite **Nuostatos** (reikalingos administratoriaus teisės).

PIN nustatymai

PIN nustatymų puslapyje galite nurodyti mažiausią ir didžiausią leistiną PIN kredencialo ilgį.

„RSA SecurID“

Jei administratorius RSA įgalino kaip autentifikavimo kredencialą ir yra patenkintos toliau nurodytos sąlygos, galite įtraukti arba ištrinti „RSA SecurID“ kredencialus.

PASTABA: reikalinga atitinkama sąranka.

- Vartotojas turi būti sukurtas RSA serveryje.
- Vartotojui ir kompiuteriui priskirtas „RSA SecurID“ atpažinimo ženklas turi būti prijungtas prie RSA serverio domeno.
- Kompiuteryje įdiegta „SecurID“ pograminė įranga.
- Yra ryšys su tinkamai konfigūruotu RSA serveriu.

Norėdami įtraukti „RSA SecurID“ kredencialą:

▲ Įveskite savo „RSA SecurID“ vartotojo vardą ir slaptąjį kodą („RSA SecurID“ atpažinimo ženklo kodą arba PIN ir atpažinimo ženklo kodą priklausomai nuo jūsų naudojamos aplinkos) ir tada spustelėkite arba bakstelėkite **Taikyti**.

Sėkmingai įtraukus bus parodytas pranešimas „Your RSA SecurID creential has been successfully enrolled“ (jūsų „RSA SecurID“ kredencialai buvo sėkmingai įtraukti) ir įgalintas trynimo mygtukas.

Norėdami ištrinti „RSA SecurID“ kredencialą:

▲ Spustelėkite **Trinti** ir tada iššokančiame dialogo lange, kuriame pateiktas klausimas „Are you sure you want to delete your RSA SecurID credential?“ (ar tikrai norit eištrinti savo „RSA SecurID“ kredencialus) pasirinkite **Taip**.

„Password Manager“

Naudodami „Password Manager“ prie tinklapių ir programų prisijungsite lengviau ir daug saugiau. Galite sukurti sudėtingesnius slaptažodžius, kurių nereikėtų užsirašyti arba įsiminti, ir po to greitai r lengvai prisijungti naudojant piršto atspaudą, lustinę kortelę, bekontaktę kortelę, judesio kortelę, „Bluetooth“ telefoną, PIN, RSA kredencialus arba savo „Windows“ slaptažodį.

PASTABA: kadangi žiniatinklio prisijungimo ekranų struktūra nuolatos kinta, „Password Manager“ nevisuomet gali palaikyti visus žiniatinklius.

„Password Manager“ programos parinktys yra šios:

„Password Manager“ puslapis

- Norėdami automatiškai paleisti tinklalapį ar programą ir prisijungti, spustelėkite arba bakstelėkite abonementą.
- Abonementus sutvarkykite ir suskirstykite į kategorijas.

Slaptažodžio stiprumas

- Vienu žvilgtelėjimu pamatykite, ar bent kuris iš jūsų slaptažodžių kelia pavojų saugumui.
- Įtraukdami prisijungimo duomenis patikrinkite atskirų tinklalapių ir programų slaptažodžių stiprumą.
- Slaptažodžio stiprumą parodo raudonos, geltonos ar žalios spalvos būsenos indikatorius.

„Password Manager“ piktograma rodoma tinklalapio arba programos prisijungimo lango viršutiniame kairiajame kampe. Jei tam tinklalapiui ar programai prisijungimas dar nėra sukurtas, ant piktogramos rodomas pliuso ženklas.

▲ Spustelėkite arba bakstelėkite **„Password Manager“** piktogramą, jei norite, kad būtų parodytas kontekstinis meniu, kuriame galite pasirinkti iš toliau pateiktų parinkčių:

- Įtraukti [koksnorsdomenas.com] į „Password Manager“
- Atidaryti „Password Manager“
- Piktogramos nustatymai
- Žinynas

Tinklalapiams ir programoms, kurioms prisijungimas dar nebuvo sukurtas

Kontekstiniame meniu rodomos šios parinktys:

- **Įtraukti [koksnorsdomenas.com] į „Password Manager“** – leidžia įtraukti prisijungimą dabartiniam prisijungimo ekranui.
- **Atidaryti „Password Manager“** – paleidžia „Password Manager“.
- **Piktogramos nustatymai** – leidžia nurodyti sąlygas, kurioms esant rodoma **„Password Manager“**.
- **Žinynas** – rodo „HP Client Security“ žinyną.

Tinklalapiams ir programoms, kurioms prisijungimas yra sukurtas

Kontekstiniame meniu rodomos šios parinktys:

- **Užpildyti prisijungimo duomenis** – parodo **„Verify your identity“** (patvirtinti savo tapatybę) puslapį. Sėkmingai autentifikavus jūsų prisijungimo duomenys patalpinami prisijungimo laukeliuose ir tada puslapis yra pateikiamas (jei kuriant prisijungimą arba paskutinį kartą redaguojant buvo nurodyta jį pateikti).
- **Redaguoti prisijungimą** – leidžia redaguoti savo prisijungimo prie šio tinklalapio duomenis.
- **Įtraukti prisijungimą** – leidžia į „Password Manager“ įtraukti abonementą.
- **Atidaryti „Password Manager“** – paleidžia „Password Manager“.
- **Žinynas** – rodo „HP Client Security“ žinyną.

PASTABA: šio kompiuterio administratorius „HP Client Security“ programą galėjo sukonfigūruoti taip, kad patvirtinant jūsų tapatybę reikėtų nurodyti daugiau nei vieną kredencialą.

Prisijungimų įtraukimas

Tinklalapio ar programos prisijungimą galite lengvai įtraukti prisijungimo informaciją įvesdami tik vieną kartą. Po to „Password Manager“ informaciją automatiškai įves už jus. Šiuos prisijungimus galite naudoti nuėję į tinklalapį arba programą.

Norėdami įtraukti prisijungimą:

1. Atidarykite tinklalapio arba programos prisijungimo ekraną.
2. Spustelėkite arba bakstelėkite **„Password Manager“** piktogramą ir tada, priklausomi nuo to, ar atidarytas tinklalapio ar programos prisijungimo ekranas, spustelėkite arba bakstelėkite vieną iš toliau pateiktų parinkčių:
   - Tinkalalpiui spustelėkite arba bakstelėkite **„Add [domain name] to Password Manager“** (įtraukti [domeopavadinimas] į „Password Manager“).
   - Programai spustelėkite arba bakstelėkite **„Add this logon screen to Password Manager“** (įtraukti šį prisijungimo ekraną į „Password Manager“).
3. Įveskite savo prisijungimo duomenis. Prisijungimo laukeliai ekrane ir atitinkami laukeliai dialogo lange identifikuojami pagal paryškintas oranžines kraštines.
   a. Norėdami į prisijungimo laukelį automatiškai įvesti vieną iš suformuotų pasirinkimų, spustelėkite arba bakstelėkite dešinėje laukelio pusėje esančias rodykles.
   b. Norėdami pamatyti šio prisijungimo slaptažodį, spustelėkite arba bakstelėkite **Rodyti slaptažodį**.
   c. Jei norite, kad prisijungimo laukeliai būtų užpildyti, tačiau nepateikti, išvalykite **„Automatically submit logon data“** (automatiškai pateikti prisijungimo duomenis) žymės langelį.
   d. Spustelėkite arba bakstelėkite **Gerai**, kad pasirinktumėte autentifikavimo būdą, kurį norite naudoti (pirštų atspaudų, lustinės kortelės, judesio kortelės, bekontaktės kortelės, „Bluetooth“ telefono, PIN ar slaptažodžio) ir tada prisijunkite naudodami pasirinktą autentifikavimo būdą.

      Pliuso ženklas pašalinamas nuo **„Password Manager“** piktogramos - tai įspėjimas, kad buvo sukurtas prisijungimas.
   e. Jei „Password Manager“ programa prisijungimo laukelių neaptinka, spustelėkite arba bakstelėkite **„More fields“** (daugiau laukelių).
      - Pasirinkite kiekvieno prisijungimui reikalingo laukelio žymės langelį arba išvalykite kiekvieno prisijungimui nereikalingo laukelio žymės langelį.
      - Spustelėkite arba bakstelėkite **Uždaryti**.

Kiekvieną kartą jums apsilankius tinklalapyje arba atidarius programą, tinklalapio arba programos prisijungimo lango viršutiniame kairiajame kampe rodoma **„Password Manager“** piktograma rodanti, kad prisijungdami galite naudoti užregistruotus kredencialus.

Prisijungimų redagavimas

Norėdami redaguoti prisijungimą:

1. Atidarykite tinklalapio arba programos prisijungimo ekraną.
2. Norėdami atidaryti dialogo langą, kuriame galėsite redaguoti savo prisijungimo informaciją, spustelėkite arba bakstelėkite **„Password Manager“** piktogramą ir tada spustelėkite arba bakstelėkite **„Edit Logon“** (redaguoti prisijungimą).

   Prisijungimo laukeliai ekrane ir atitinkami laukeliai dialogo lange identifikuojami pagal paryškintas oranžines kraštines.

   Taip pat „Password Manager“ puslapyje galite redaguoti abonemento informaciją. Spustelėkite arba bakstelėkite prisijungimą, kad būtų parodytos redagavimo parinktys ir tada pasirinkite **Redaguoti**.
3. Redaguokite savo prisijungimo informaciją.
   - Norėdami redaguoti **Paskyros pavadinimą**, į laukelį įveskite naują pavadinimą.
   - Norėdami įtraukti arba redaguoti **Kategorijos** pavadinimą, įveskite arba modifikuokite pavadinimą **Kategorijos** laukelyje.
   - Norėdami pasirinkti **Vartotojo vardo** prisijungimo laukelį su vienu iš suformuotų pasirinkimų, spustelėkite arba bakstelėkite dešinėje laukelio pusėje esančią rodyklę žemyn.

     Suformuoti pasirinkimai galimi tik tuomet, jei prisijungimas redaguojamas naudojant „Password Manager“ kontekstinio meniu komandą „Redaguoti“.
   - Norėdami pasirinkti **Slaptažodžio** prisijungimo laukelį su vienu iš suformuotų pasirinkimų, spustelėkite arba bakstelėkite dešinėje laukelio pusėje esančią rodyklę žemyn.

     Suformuoti pasirinkimai galimi tik tuomet, jei prisijungimas redaguojamas naudojant „Password Manager“ kontekstinio meniu komandą „Redaguoti“.
   - Norėdami iš ekrano į savo prisijungimą įtraukti papildomus laukelius, spustelėkite arba bakstelėkite **„More fields“** (daugiau laukelių).
   - Norėdami pamatyti šio prisijungimo slaptažodį, spustelėkite arba bakstelėkite **Rodyti slaptažodį** piktogramą.
   - Jei norite, kad prisijungimo laukeliai būtų užpildyti, tačiau nepateikti, išvalykite **„Automatically submit logon data“** (automatiškai pateikti prisijungimo duomenis) žymės langelį.
   - Jei norite pažymėti, kad šio prisijungimo slaptažodis yra pažeistas, pasirinkite **„This password is compromised“** (šis slaptažodis yra pažeistas) žymės langelį.

     Pakeitimus išsaugojus, visi kiti tą patį slaptažodį naudojantys prisijungimai bus taip pat pažymėti, kad jų slaptažodis yra pažeistas. Po to galite atidaryti kiekvieną paveiktą abonementą ir pakeisti jo slaptažodį.
4. Spustelėkite arba bakstelėkite **Gerai**.

„Password Manager Quick Links“ meniu naudojimas

„Password Manager“ leidžia greitai ir lengvai paleisti tinklalapius ir programas, kurioms jūs sukūrėte prisijungimus. **„Password Manager Quick Links“** meniu arba „HP Client Security“ programos „Password Manager“ puslapyje dukart spustelėkite arba dukart bakstelėkite programos arba tinklalapio prisijungimą, kad būtų atidarytas prisijungimo ekranas ir tada įveskite savo prisijungimo duomenis.

Sukūrus prisijungimą, jis automatškai įtraukiamas į jūsų „Password Manager“ programos **„ Quick Links“** meniu.

Kad būtų parodytas **„Quick Links“** meniu:

- ▲ Paspauskite **„Password Manager“** sparčiųjų klavišų kombinaciją (Ctrl + „Windows“ klavišas + h – gamyklinė konfigūracija). Norėdami pakeisti sparčiųjų klavišų kombinaciją, „HP Client Security“ pagrindiniame puslapyje spustelėkite **„Password Manager“** ir tada spustelėkite arba bakstelėkite **Nuostatos**.

Prisijungimų skirstymas į kategorijas

Sukurkite vieną ar daugiau kategorijų ir užtikrinkite, kad jūsų prisijungimai būtų tvarkingai surūšiuoti.

Norėdami prisijungimą priskirti kategorijai:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Password Manager“.**
2. Spustelėkite arba bakstelėkite abonemento įrašą ir tada spustelėkite arba bakstelėkite **Redaguoti**.
3. **Kategorijos** laukelyje įveskite kategorijos pavadinimą.
4. Spustelėkite arba bakstelėkite **Įrašyti**.

Norėdami prisijungimą iš kategorijos pašalinti:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Password Manager“.**
2. Spustelėkite arba bakstelėkite abonemento įrašą ir tada spustelėkite arba bakstelėkite **Redaguoti**.
3. **Kategorijos** laukelyje ištrinkite kategorijos pavadinimą.
4. Spustelėkite arba bakstelėkite **Įrašyti**.

Norėdami kategoriją pervardyti:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Password Manager“.**
2. Spustelėkite arba bakstelėkite abonemento įrašą ir tada spustelėkite arba bakstelėkite **Redaguoti**.
3. **Kategorijos** laukelyje pakeiskite kategorijos pavadinimą.
4. Spustelėkite arba bakstelėkite **Įrašyti**.

Prisijungimų valdymas

„Password Manager“ dėka vienoje vietoje galite lengvai valdyti prisijungimo informaciją vartotojų vardams, slaptažodžius ir kelių prisijungimų abonementus.

Jūsų prisijungimai pateikti „Password Manager“ puslapyje.

Norėdami valdyti prisijungimus:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Password Manager“.**
2. Spustelėkite arba bakstelėkite esamą prisijungimą ir tada pasirinkite vieną iš toliau pateiktų parinkčių ir vykdykite ekrane pateikiamus nurodymus:
   - **Redaguoti** – redaguokite prisijungimą. Daugiau informacijos rasite skyriuje „Prisijungimų redagavimas“ 21 puslapyje.
   - **Prisijungti** – prisijunkite prie pasirinkto abonemento.
   - **Trinti** – ištrinkite pasirinkto abonemento prisijungimą.

Norėdami įtraukti papildomą tinklalapio arba programos prisijungimą:

1. Atidarykite tinklalapio arba programos prisijungimo ekraną.
2. Spustelėkite arba bakstelėkite **„Password Manager“** piktogramą, kad būtų parodytas jos kontekstinis meniu.
3. Spustelėkite arba bakstelėkite **„Add Logon“** (įtraukti prisijungimą) ir tada vykdykite ekrane pateikiamus nurodymus.

Jūsų slaptažodžio stiprumo įvertinimas

Norint apsaugoti savo tapatybę, nepaprastai svarbu prisijungimui prie tinklalapių ir programų naudoti sudėtingesnius slaptažodžius.

„Password Manager“ dėka saugą lengva stebėti ir tobulinti, kadangi kiekvieno slaptažodžio, kurį naudojate prisijungdami prie savo tinklalapių ar programų, stiprumas akimirksniu automatiškai analizuojamas.

Kuriant „Password Manager“ aboemento prisijungimą ir vedant slaptažodį, po slaptažodžiu rodoma spalvota juosta, kuri nurodo slaptažodžio stiprumą. Spalvų reikšmės:

- **Raudona** – silpnas
- **Geltona** – neblogas
- **Žalia** – stiprus

„Password Manager“ piktogramos nustatymai

„Password Manager“ bando nustatyti tinklalapių ir programų prisijungimo ekranus. Kai programa aptinks prisijungimo ekraną, kuriam dar nesate susikūrę prisijungimo, „Password Manager“ jus

paragins įtraukti šio ekrano prisijungimą ir parodys **„Password Manager“** piktogramą su pliuso ženklu.

1. Norėdami individualizuoti, kaip „Password Manager“ programa turėtų elgtis aptikusi galimas prisijungimo svetaines, spustelėkite arba bakstelėkite piktogramą ir tada spustelėkite arba bakstelėkite **„Icon Settings“** (piktogramos nustatymai).

   - **„Prompt to add logons for logon screens“** (paraginti įtraukti prisijungimų ekranų prisijungimus)– spustelėkite arba bakstelėkite šią parinktį, jei norite, kad „Password Manager“ jus paragintų įtraukti prisijungimą, kai bus parodytas prisijungimo ekranas, kuriam dar nėra nustatytas prisijungimas.
   - **„Exclude this screen“** (neįtraukti šio ekrano) – pasirinkite žymos langelį, jei norite, kad „Password Manager“ programa daugiau neberagintų įtraukti prisijungimo šiam prisijungimo ekranui.
   - **„Do not prompt to add logons for logon screens“** (neraginti įtraukti prisijungimus prisijungimų ekranams) – pasirinkite sukamąjį mygtuką.

2. Norėdami įtraukti prisijungimą ekranams, kurie buvo anksčiau neįtraukti:

   a. Prisijunkite prie anksčiau neįtraukto tinklalapio.

   b. Kad „Password Manager“ programa įsimintų šios svetainės slaptažodį, iššokančiame dialogo lange spustelėkite arba bakstelėkite **Įsiminti**, kad būtų išsaugotas slaptažodis ir sukurtas šio ekrano prisijungimas.

3. Norėdami pasiekti papildomus „Password Manager“ nustatymus, „Password Manager“ puslapyje spustelėkite arba bakstelėkite „Password Manager“ piktogramą, spustelėkite arba bakstelėkite **„Open Password Manager“** (atidaryti „Password Manager“) ir tada spustelėkite arba bakstelėkite **Nuostatos**.

Prisijungimų importavimas ir eksportavimas

„HP Password Manager“ programos importavimo ir eksportavimo puslapyje galite importuoti žiniatinklio naršyklių jūsų kompiuteryje išsaugotus prisijungimus. Taip pat galite importuoti duomenis iš „HP Client Security“ atsarginės kopijos saugojimo failo ir eksportuoti duomenis į „HP Client Security“ atsarginės kopijos saugojimo failą.

▲ Norėdami paleisti importavimo ir eksportavimo puslapį, „Password Manager“ puslapyje spustelėkite **„Import and export“** (importuoti ir eksportuoti).

Norėdami importuoti slaptažodžius iš naršyklės:

1. Spustelėkite arba bakstelėkite naršyklę, iš kurios norite importuoti slaptažodžius (rodomos tik įdiegtos naršyklės).
2. Išvalykite abonementų, kurių slaptažodžių importuoti nenorite, žymės langelius.
3. Spustelėkite arba bakstelėkite **Importuoti**.

Duomenų importavimas iš „HP Client Security“ atsarginės kopijos saugojimo failo arba eksportavimas į šį failą gali būti vykdomas importavimo ir eksportavimo puslapyje naudojant atitinkamus saitus (parinktyje **„Other options“** (kitos parinktys).

PASTABA: Ši funkcija importuoja ir eksportuoja tik „Password Manager“ duomenis. Norėdami gauti daugiau informacijos apie atsarginių kopijų kūrimą ir papildomų „HP Client Security“ duomenų atkūrimą, žr. „Atsarginės duomenų kopijos kūrimas ir duomenų atkūrimas“ 29 puslapyje“.

Norėdami importuoti duomenis iš „HP Client Security“ atsarginės kopijos saugojimo failo:

1. „HP Password Manager“ importavimo ir eksportavimo puskapyje spustelėkite arba bakstelėkite **„Import data from an HP Client Security backup file“** (importuoti duomenis iš „HP Client Security“ atsarginės kopijos saugojimo failo).
2. Patvirtinkite savo tapatybę.
3. Pasirinkite anksčiau sukurtą atsarginės kopijos saugojimo failą arba į pateiktą laukelį įveskite jo kelią ir tada spustelėkite arba bakstelėkite **Naršyti**.
4. Įveskite slaptažodį, kuriuo apsaugojamas failas, ir tada spustelėkite arba bakstelėkite **Toliau**.
5. Spustelėkite arba bakstelėkite **Atkurti**.

Norėdami eksportuoti duomenis į „HP Client Security“ atsarginės kopijos saugojimo failą:

1. „HP Password Manager“ importavimo ir eksportavimo puskapyje spustelėkite arba bakstelėkite **„Export data from an HP Client Security backup file“** (eksportuoti duomenis iš „HP Client Security“ atsarginės kopijos saugojimo failo).
2. Patvirtinkite savo tapatybę ir tada spustelėkite arba bakstelėkite **Toliau**.
3. Įveskite atsarginės kopijos saugojimo failo pavadinimą. Pagal numatytuosius nustatymus failas išsaugojamas aplanke „Dokumentai“. Norėdami nurodyti kitą vietą, spustelėkite arba bakstelėkite **Naršyti**.
4. Įveskite ir patvirtinkite slaptažodį, kuriuo bus apsaugojamas failas, ir tada spustelėkite arba bakstelėkite **Įrašyti**.

Nustatymai

Galite nurodyti nustatymus ir taip „Password Manager“ pritaikyti savo reikmėms:

- **„Prompt to add logons for logon screens“** (raginti įtraukti prisijungimus prisijungimų ekranams) – **„Password Manager“** piktograma su pliuso ženklu rodoma visada, kai aptinkamas tinklalapio arba programos prisijungimo ekranas. Ši piktograma reiškia, kad šio ekrano prisijungimą galite įtraukti į **„Logons“** (prisijungimai) meniu.

  Jei šią funkciją norite išjungti, išvalykite žymės langelį, esantį šalia **„Prompt to add logons for logon screens“** (raginti įtraukti prisijungimus prisijungimų ekranams).

- **„Open Password Manager with Ctrl+Win+h“** (atidaryti „Password Manager“ naudojant Ctrl + Win + h) – numatytasis spartusis klavišas, kuris atidaro **„Password Manager Quick Links“**, yra: Ctrl + „Windows“ klavišas + h.

  Norėdami pakeisti spartųjį klavišą, spustelėkite arba bakstelėkite šią parinktį ir tada įveskite naują klavišų kombinaciją. Kombinaciją gali sudaryti vienas ar daugiau iš šių klavišų: ctrl, alt arba shift ir bet kuris raidinis arba skaitmenų klavišas.

  Kombinacijų, kurias naudojama „Windows“ arba „Windows“ programos, naudoti negalima.

- Norėdami nustatymus atstatyti į numatytąsias gamintojo reikšmes, spustelėkite arba bakstelėkite **„Restore defaults“** (atkurti numatytąsias reikšmes).

Papildomi nustatymai

Administratoriai gali pasiekti toliau pateiktas parinktis pasirinkdami **„Gear“** (nustatymų) piktogramą, esančią pagrindiniame „HP Client Security“ ekrane.

- **„Administrator policies“** (administratoriaus strategijos) – leidžia sukonfigūruoti administratorių prisijungimo ir sesijų naudojimo taisykles.
- **„Standard User policies“** (paprastojo vartotojo strategijos) – leidžia sukonfigūruoti paprastųjų vartotojų prisijungimo ir sesijų naudojimo taisykles.
- **„Security Features“** (saugos priemonės) – leidžia pagerinti kompiuterio saugą: „Windows“ abonementas apsaugojamas naudojant griežtą autentifikavimą ir (arba) įgalinant autetifikavimą prieš paleidžiant „Windows“.
- **Vartotojai** – leidžia valdyti vartotojus ir jų kredencialus.
- **„My policies“** (mano strategijos) – leidžia peržiūrėti savo autentifikavimo taisykles ir įtraukimo būklę.
- **„Backup and Restore“** (atsarginis kopijavimas ir atkūrimas) – leidžia sukurti atsarginę „HP Client Security“ duomenų kopiją arba tuos duomenis atkurti.
- **„About HP Client Security“** (apie „HP Client Security“) – rodo „HP Client Security“ versijos informaciją.

Administratoriaus strategijos

Galite sukonfigūruoti šio kompiuterio administratorių prisijungimo ir sesijų naudojimo taisykles. Čia nustatytos prisijungimo strategijos valdo privalomus vietinio administratoriaus prisijungimo prie „Windows“ kredencialus. Čia nustatytos seansų strategijos valdo privalomus vietinio administratoriaus tapatybės patvirtinimo kredencialus „Windows“ operacinėje sistemoje.

Paspaudus **Taikyti**, pagal numatytuosius nustatymus visos naujos arba pakeistos strategijos pradedamos taikyti tuojau pat.

Norėdami įtraukti naują strategiją:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Gear“** piktogramą.
2. Papildomų nustatymų puslapyje spustelėkite arba bakstelėkite **„Administrator Policies“** (administratoriaus strategijos).
3. Spustelėkite arba bakstelėkite **„Add new policy“** (įtraukti naują strategiją).
4. Spustelėkite rodykles žemyn, kad pasirinktumėte pirminius (pasirinktinis) ir papildomus naujos startegijos kredencialus ir tada spustelėkite arba bakstelėkite **Įtraukti**.
5. Spustelėkite **Taikyti**.

Norėdami naujos ar pakeistos strategijos taikymą atidėti:

1. Spustelėkite arba bakstelėkite **„Enforce this policy immediately“** (Šią strategiją taikyti tuojau pat).
2. Pasirinkite **„Enforce this policy on the specific date“** (šią strategiją taikyti konkrečią datą).
3. Įveskite datą arba naudodamiesi iššokančiu kalendoriumi pasirinkite datą, kada ši strategija turėtų būti pradėta taikyti.
4. Jei pageidaujate, pasirinkite, kada apie naują strategiją priminti vartotojams.
5. Spustelėkite **Taikyti**.

Paprastojo vartotojo strategijos

Galite sukonfigūruoti šio kompiuterio paprastųjų vartotojų prisijungimo ir sesijų naudojimo taisykles. Čia nustatytos prisijungimo strategijos valdo privalomus paprastojo vartotojo prisijungimo prie „Windows“ kredencialus. Čia nustatytos seansų strategijos valdo privalomus paprastojo vartotojo tapatybės patvirtinimo kredencialus „Windows“ operacinėje sistemoje.

Paspaudus **Taikyti**, pagal numatytuosius nustatymus visos naujos arba pakeistos strategijos pradedamos taikyti tuojau pat.

Norėdami įtraukti naują strategiją:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Gear“** piktogramą.
2. Papildomų nustatymų puslapyje spustelėkite arba bakstelėkite **„Standard User Policies“** (paprastojo vartotojo strategijos).
3. Spustelėkite arba bakstelėkite **„Add new policy“** (įtraukti naują strategiją).
4. Spustelėkite rodykles žemyn, kad pasirinktumėte pirminius (pasirinktinis) ir papildomus naujos startegijos kredencialus ir tada spustelėkite arba bakstelėkite **Įtraukti**.
5. Spustelėkite **Taikyti**.

Norėdami naujos ar pakeistos strategijos taikymą atidėti:

1. Spustelėkite arba bakstelėkite **„Enforce this policy immediately“** (Šią strategiją taikyti tuojau pat).
2. Pasirinkite **„Enforce this policy on the specific date“** (šią strategiją taikyti konkrečią datą).
3. Įveskite datą arba naudodamiesi iššokančiu kalendoriumi pasirinkite datą, kada ši strategija turėtų būti pradėta taikyti.
4. Jei pageidaujate, pasirinkite, kada apie naują strategiją priminti vartotojams.
5. Spustelėkite **Taikyti**.

Saugos priemonės

Galite įgalinti „HP Client Security“ saugos priemones, kurios apsaugo nuo nesankcionuotos prieigos prie kompiuterio.

Norėdami nustatyti saugos priemones:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Gear“** piktogramą.
2. Papildomų nustatymų puslapyje spustelėkite arba bakstelėkite **Saugos priemonės**.

3. Įgalinkite saugos priemones pasirinkdami jų žymės langelius ir tada spustelėkite arba bakstelėkite **Taikyti**. Kuo daugiau priemonių pasirinksite, tuo geriau bus apsaugotas jūsų kompiuteris.

   Šie nustatymai taikomi visiems vartotojams.

   - **„Windows Logon Security“** („Windows“ prisijungimo sauga) – apsaugo jūsų „Windows“ abonementus, kadangi prieiga suteikiama tik pateikus „HP Client Security“ kredencialus.
   - **Sauga prieš įkraunant sistemą (autentifikavimas įjungus)** – apsaugo jūsų kompiuterį prieš paleidžiant „Windows“. Šis pasirinkimas negalimas, jei BIOS jo nepalaiko.
   - **„Allow One Step logon“** – (leisti vieno veiksmo prisijungimą) – šis nustatymas leidžia praleisti „Windows“ prisijungimą, jei prieš tai autentifikavimas buvo atliktas „Power–on authentication“ (autentifikavimas įjungus) arba „Drive Encryption“ lygmenyje.

4. Spustelėkite arba bakstelėkite **Vartotojai** ir tada spustelėkite arba bakstelėkite vartotojų plytelę.

Vartotojai

Galite stebėti ir valdyti šio kompiuterio „HP Client Security“ vartotojus.

Norėdami į „HP Client Security“ įtraukti kitą „Windows“ vartotoją:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Gear“** piktogramą.
2. Papildomų nustatymų puslapyje spustelėkite arba bakstelėkite **Vartotojai**.
3. Spustelėkite arba bakstelėkite **„Add another Windows user to HP Client Security“** (įtraukti kitą „Windows“ vartotoją į „HP Client Security“).
4. Įveskite vartotojo, kurį norite įtraukti, vardą ir tada spustelėkite arba bakstelėkite **Gerai**.
5. Įveskite vartotojo „Windows“ slaptažodį.

   Vartotojo puslapyje rodoma įtraukto vartotojo plytelė.

Norėdami „Windows“ vartotoją ištrinti iš „HP Client Security“:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Gear“** piktogramą.
2. Papildomų nustatymų puslapyje spustelėkite arba bakstelėkite **Vartotojai**.
3. Spustelėkite arba bakstelėkite vartotojo, kurį norite ištrinti, vardą.
4. Spustelėkite arba bakstelėkite **„Delete User“** (trinti vartotoją) ir tada patvirtinkite spustelėdami arba bakstelėdami **Taip**.

Jei norite, kad būtų parodyta vartotojui taikomų prisijungimo ir seanso strategijų suvestinė:

▲ Spustelėkite arba bakstelėkite **Vartotojai** ir tada spustelėkite arba bakstelėkite vartotojų plytelę.

Mano strategijos

Galite įjungti savo autentifikavimo taisykles ir įtraukimo būklę. Mano strategijų puslapis taip pat pateikia saitus į administratoriaus strategijų ir paprastojo vartotojo strategijų puslapius.

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Gear“** piktogramą.
2. Papildomų nustatymų puslapyje spustelėkite arba bakstelėkite **„My Policies“** (mano strategijos).

   Parodomos šiuo metu prisijungusiam vartotojui taikomos prisijungimo ir seanso naudojimo taisyklės.

Mano strategijų puslapis taip pat pateikia saitus į „„Administratoriaus strategijos“ 26 puslapyje“ ir „„Paprastojo vartotojo strategijos“ 27 puslapyje“.

Atsarginės duomenų kopijos kūrimas ir duomenų atkūrimas

Rekomenduojama, kad reguliariai suskurtumėte atsarginę savo „HP Client Security“ duomenų kopiją. Kaip dažnai turėtumėte sukurti atsarginę duomenų kopiją priklauso nuo to, kaip dažnai duomenys keičiami. Pavyzdžiui, jei kasdien įtraukiate naujus prisijungimus, atsarginę duomenų kopiją turėtumėte sukurti kasdien.

Atsargines kopijas taip pat galima naudoti perkeliant duomenis iš vieno kompiuterio į kitą, t. y. importuojant ir eksportuojant.

PASTABA: Šia funkcija sukuriama tik „Password Manager“ atsarginė kopija. „Drive Encryption“ naudoja atskirą atsarginės kopijos kūrimo metodą. „Device Access Manager“ ir autentifikavimo piršto atspaudu atsarginės kopijos nekuriamos.

Norint atkurti duomenis iš atsarginės kopijos saugojimo failo, kompiuteryje, kuriame bus atkuriami šie duomenys, turi būti įdiegta „HP Client Security“ programa.

Norėdami sukurti atsarginę duomenų kopiją:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Gear“** piktogramą.
2. Papildomų nustatymų puslapyje spustelėkite arba bakstelėkite **„Administrator Policies“** (administratoriaus strategijos).
3. Spustelėkite arba bakstelėkite **„Backup and Restore“** (atsarginis kopijavimas ir atkūrimas).
4. Spustelėkite arba bakstelėkite **Atsarginė kopija** ir tada patvirtinkite savo tapatybę.
5. Pasirinkite modulį, kurį norite įtraukti į atsarginę kopiją, ir tada spustelėkite arba bakstelėkite **Toliau**.
6. Įveskite saugojimo failo pavadinimą. Pagal numatytuosius nustatymus failas išsaugojamas aplanke „Dokumentai“. Norėdami nurodyti kitą vietą, spustelėkite arba bakstelėkite **Naršyti**.
7. Įveskite ir patvirtinkite slaptažodį, kuriuo bus apsaugojamas failas.
8. Spustelėkite arba bakstelėkite **Įrašyti**.

Norėdami atkurti duomenis:

1. „HP Client Security“ pagrindiniame puslapyje spustelėkite arba bakstelėkite **„Gear“** piktogramą.
2. Papildomų nustatymų puslapyje spustelėkite arba bakstelėkite **„Administrator Policies“** (administratoriaus strategijos).
3. Spustelėkite arba bakstelėkite **„Backup and Restore“** (atsarginis kopijavimas ir atkūrimas).
4. Pasirinkite **Atkurti** ir tada patvirtinkite savo tapatybę.

5. Pasirkite anksčiau sukurtą saugojimo failą. Į pateiktą laukelį įveskite jo kelią. Norėdami nurodyti kitą vietą, spustelėkite arba bakstelėkite **Naršyti**.
6. Įveskite slaptažodį, kuriuo apsaugojamas failas, ir tada spustelėkite arba bakstelėkite **Toliau**.
7. Pasirinkite modulius, kurių duomenis norite atkurti.
8. Spustelėkite arba bakstelėkite **Atkurti**.

5 „HP Drive Encryption“ (tik tam tikruose modeliuose)

„HP Drive Encryption“ priemonė visapusiškai apsaugo jūsų kompiuterio duomenis juos užšifruodama. Kai „Drive Encryption“ yra suaktyvinama, turite prisijungti „Drive Encryption“ prisijungimo ekrane, kuris rodomas prieš paleidžiant „Windows®“ operacinę sistemą.

„HP Client Security“ pagrindinis ekranas „Windows“ administratoriams leidžia aktyvinti „Drive Encryption“ priemonę, sukurti atsarginę šifravimo rakto kopiją ir pasirinkti užšifruoti diskų įrenginį (-ius) ar skaidinius arba panaikinti jų žymėjimą. Norėdami gauti daugiau informacijos, žr. „HP Client Security“ programinės įrangos žinyną.

Naudojant „Drive Encryption“ galima atlikti šias užduotis:

- Pasirinkti „Drive Encryption“ nuostatas:
  - užšifruoti ir iškoduoti atskirus diskų įrenginius ar skaidinius naudojant programinės įrangos šifravimą;
  - užšifruoti ir iškoduoti atskirus užsišifruojančius diskų įrenginius naudojant aparatūros šifravimą;
  - papildomai apsaugoti išjungiant energijos taupymą arba pristabdymą ir taip užtikrinti, kad visuomet prieš įkraunant sistemą ją reikėtų autentifikuoti.

PASTABA: šifruoti galima tik vidinius SATA ir išorinius eSATA standžiuosius diskus.

- Sukurti atsarginę rakto kopiją
- Atkurti prieigą prie užšifruoto kompiuterio naudojant atsarginę rakto kopiją ir „HP SpareKey“ priemonę
- Įgalinti „Drive Encryption“ autentifikavimą prieš įkraunant sistemą naudojant slaptažodį, registruotą pirštо atspaudą arba PIN lustinėms kortelėms

„Drive Encryption“ atidarymas

Administratoriai „Drive Encryption“ gali pasiekti atidarydami „HP Client Security“:

1. Pradžios ekrane spustelėkite arba bakstelėkite **„HP Client Security“** programėlę („Windows 8“).

   – arba –

   „Windows“ darbalaukyje, pranešimų srityje, esančioje užduočių juostos dešinėje pusėje, dukart spustelėkite arba dukart bakstelėkite **„HP Client Security“** piktogramą.

2. Spustelėkite arba bakstelėkite **„Drive Encryption“** piktogramą.

Bendrosios užduotys

„Drive Encryption“ aktyvinimas standartiniams standiesiems diskams

Standartiniai standieji diskai yra užšifruojami naudojant programinės įrangos šifravimą. Norėdami užšifruoti diskų įrenginį arba disko skaidinį, vykdykite tokius veiksmus:

1. Paleiskite **„Drive Encryption“**. Daugiau informacijos rasite skyriuje „„Drive Encryption“ atidarymas“ 31 puslapyje.
2. Pasirinkite diskų įrenginio arba skaidinio, kurį norite užšifruoti, žymės langelį ir tada spustelėkite arba bakstelėkite **„Backup Key“** (atsarginės kopijos raktas).

PASTABA: Kad užtikrintumėte geresnį saugumą, pasirinkite **„Disable sleep mode for increased security“** (išjungti energijos taupymo režimą geresniam saugumui) žymės langelį. Išjungus energijos taupymo režimą, nėra absoliučiai jokio pavojaus, kad kredencialai, naudojami atrakinant diskų įrenginį, būtų saugomi standžiajame diske.

3. Pasirinkite vieną ar daugiau atsarginės kopijos parinkčių ir tada spustelėkite arba bakstelėkite **„Backup“** (atsarginė kopija). Daugiau informacijos rasite skyriuje „Atsarginės šifravimo raktų kopijos kūrimas“ 35 puslapyje.
4. Galite tęsti savo darbą, kol yra kuriama atsarginė šifravimo rakto kopija. Kompiuterio neperkraukite.

PASTABA: jūs raginami kompiuterį palesti iš naujo. Paleidus iš naujo rodomas disko šifravimo ekranas prieš įkraunant sistemą – reikalingas autentifikavimas prieš paleidžiant „Windows“.

„Drive Encryption“ priemonė suaktyvinta. Pasirinkto disko skaidinio (-ių) šifravimas gali užtrukti keletą valandų, priklausomai nuo skaidinių kiekio ir dydžio.

Norėdami gauti daugiau informacijos, žr. „HP Client Security“ programinės įrangos žinyną.

„Drive Encryption“ aktyvinimas užsišifruojantiems diskų įrenginiams

Užsišifruojančius diskų įrenginius, atitinkančius „Trusted Computing Group“ grupės OPAL specifikacijas, keliamas užsišifruojančių diskų įrenginių valdymui, galima užšifruoti naudojant programinės įrangos šifravimą arba aparatūros šifravimą. Aparatūros šifravimas yra daug greitesnis nei programinės įrangos. Tačiau negalite pasirinkti, kuriuos disko skaidinius užšifruoti. Užšifruojamas ištisas diskų įrenginys, įskaitant visus skaidinius.

Jei norite užšifruoti atskirus skaidinius, turite naudoti programinės įrangos šifravimą. Nepamirškite išvalyti **„Only allow hardware encryption for Self-Encrypting Drives (SEDs)“** (užsišifruojantiems diskų įrenginiams (SED) leisti tik aparatūros šifravimą) žymos langelio.

Norėdami suaktyvinti „Drive Encryption“ užsišifruojantiems diskų įrenginiams, vykdykite tokius veiksmus:

1. Paleiskite **„Drive Encryption“**. Daugiau informacijos rasite skyriuje „„Drive Encryption“ atidarymas“ 31 puslapyje.
2. Pasirinkite diskų įrenginio, kurį norite užšifruoti, žymės langelį ir tada spustelėkite arba bakstelėkite **„Backup Key“** (atsarginės kopijos raktas).

PASTABA: Kad užtikrintumėte geresnį saugumą, pasirinkite **„Disable Sleep Mode for added security“** (išjungti energijos taupymo režimą papildomam saugumui) žymės langelį. Išjungus energijos taupymo režimą, nėra absoliučiai jokio pavojaus, kad kredencialai, naudojami atrakinant diskų įrenginį, būtų saugomi standžiajame diske.

3. Pasirinkite vieną ar daugiau atsarginės kopijos parinkčių ir tada spustelėkite arba bakstelėkite **„Backup“** (atsarginė kopija). Daugiau informacijos rasite skyriuje „Atsarginės šifravimo raktų kopijos kūrimas“ 35 puslapyje.

4. Galite tęsti savo darbą, kol yra kuriama atsarginė šifravimo rakto kopija. Kompiuterio neperkraukite.

PASTABA: užsišifruojančių diskų įrenginių atveju jūs raginami išjungti kompiuterį.

Norėdami gauti daugiau informacijos, žr. „HP Client Security“ programinės įrangos žinyną.

„Drive Encryption“ išjungimas

1. Paleiskite **„Drive Encryption“**. Daugiau informacijos rasite skyriuje „„Drive Encryption“ atidarymas“ 31 puslapyje.

2. Išvalykite visų užšifruotų diskų įrenginių žymės langelius ir tada spustelėkite arba bakstelėkite **Taikyti**.

   Pradedamas „Drive Encryption“ išjungimas.

PASTABA: Jei buvo naudojamas programinės įrangos šifravimas, pradedamas iškodavimas. Tai gali užtrukti keletą valandų, priklausomai nuo skaidinių kiekio ir dydžio. Kai iškodavimas baigtas, „Drive Encryption“ priemonė išjungiama.

Jei buvo naudojamas aparatūros šifravimas, diskų įrenginys akimirksniu iškoduojamas ir po poros minučių „Drive Encryption“ priemonė išjungiama.

Išjungus „Drive Encryption“ jūs busite paraginti išjungti kompiuterį, jei buvo naudojamas aparatūros šifravimas, arba paleisti kompiuterį iš naujo, jei buvo naudojamas programinės įrangos šifravimas.

Prisijungimas po to, kai „Drive Encryption“ priemonė suaktyvinta

Kai įjungiate kompiuterį po to, kai „Drive Encryption“ buvo suaktyvinta ir jūsų vartotojo abonementas įtrauktas, turite prisijungti „Drive Encryption“ prisijungimo ekrane.

PASTABA: kai kompiuteris aktyvinamas iš energijos taupymo ar pristabdymo, „Drive Encryption“ autentifikavimas prieš įkraunant sistemą nerodomas, jei buvo naudojamas programinės įrangos šifravimas arba aparatūros šifravimas. Aparatūros šifravimas pateikia **„Disable sleep mode for increased security“** (išjungti energijos taupymo režimą geresniam saugumui) parinktį, kurią įgalinus neleidžiama įsijungti energijos taupymo ar pristabdymo režimams.

Kai kompiuteris aktyvinamas iš sulaikytosios veiksenos, „Drive Encryption“ autentifikavimas prieš įkraunant sistemą rodomas abiem atvejais – jei buvo naudojamas programinės įrangos šifravimas arba aparatūros šifravimas.

PASTABA: jei „Windows“ administratorius „HP Client Security“ priemonėje įgalino BIOS saugą prieš įkraunant sistemą ir jei yra įgalintas (pagal numatytuosius nustatymus) prisijungimas vienu veiksmu, prie kompiuterio prisijungti galite iškart po BIOS prieš įkraunant sistemą autentifikavimo, nes dar kartą autentifikuoti „Drive Encryption“ prisijungimo ekrane nebereikia.

Vieno vartotojo prisijungimas:

- Puslapyje **Registracija** įveskite savo „Windows“ slaptažodį, lustinės kortelės PIN, „SpareKey“ arba perbraukite registruotu pirštu.

Kelių vartotojų prisijungimas:

1. Puslapyje **„Select user to logon“** (pasirinkti vartotoją, kuris prisijungs), iš išskleidžiamojo sąrašo pasirinkite vartotoją, kuris prisijungs ir tada spustelėkite arba bakstelėkite **Toliau**.
2. Puslapyje **Registracija** įveskite savo „Windows“ slaptažodį arba lustinės kortelės PIN, arba perbraukite registruotu pirštu.

PASTABA: palaikomos šios lustinės kortelės:

Palaikomos lustinės kortelės

- „Gemalto Cyberflex Access 64k V2c“

PASTABA: jei prisijungiant „Drive Encryption“ prisijungimo ekrane naudojamas atkūrimo raktas, norint gauti prieigą prie vartotojų abonementų, „Windows“ registracijoje reikia įvesti papildomus kredencialus.

Papildomų standžiųjų diskų šifravimas

Ypač rekomenduojama naudoti „HP Drive Encryption“ ir taip užšifruojant standųjį diską apsaugoti savo duomenis. Suaktyvinus, visi pridėti standieji diskai ar sukurti skaidiniai gali būti užšifruoti vykdant šiuos veiksmus:

1. Paleiskite **„Drive Encryption“**. Daugiau informacijos rasite skyriuje „„Drive Encryption“ atidarymas“ 31 puslapyje.
2. Programine įranga šifruotiems diskų įrenginiams pasirinkite disko skaidinius, kuriuos norite šifruoti.

   PASTABA: Tai taip pat taikoma, kai yra vienas arba keli standartiniai standieji diskai ir vienas ar keli užsišifruojantys diskų įrenginiai.

– arba –

▲ Aparatūra šifruotiems diskų įrenginiams pasirinkite papildomą (-us) diskų įrenginį (-iu), kurį (-iuos) norite šifruoti.

Išplėstinės užduotys

„Drive Encryption“ valdymas (administratoriaus užduotis)

Administratoriai naudodamiesi „Drive Encryption“ gali peržiūrėti ir pakeisti visų kompiuterio standžiųjų diskų šifravimo būseną (neužšifruoti arba užšifruoti).

- Jei būsena yra įgalinta, „Drive Encryption“ priemonė buvo suaktyvinta ir sukonfigūruota. Diskų įrenginys yra vienoje iš šių būsenų:

Programinės įrangos šifravimas

  - Neužšifruotas
  - Užšifruotas
  - Šifruojamas
  - Iškoduojamas

Aparatūros šifravimas

- Užšifruotas
- Neužšifruotas (papildomiems diskų įrenginiams)

Atskirų diskų skaidinių šifravimas arba iškodavimas (tik programinės įrangos šifravimas)

Administratoriai naudodamiesi „Drive Encryption“ gali šifruoti vieną ar kelis kompiuterio standžiojo disko skaidinius arba iškoduoti bet kurį jau užšifruotą disko skaidinį.

1. Paleiskite **„Drive Encryption“**. Daugiau informacijos rasite skyriuje „„Drive Encryption“ atidarymas“ 31 puslapyje.
2. Parinktyje **„Drive Status“** (diskų įrenginio būsena) pasirinkite arba išvalykite kiekvieno standžiojo disko skaidinio, kurį norite užšifruoti arba iškoduoti, žymės langelį ir tada spustelėkite arba bakstelėkite **Taikyti**.

PASTABA: Kai skaidinys yra šifruojamas arba iškoduojamas, eigos juostoje rodomi užšifruoto skaidinio procentai.

PASTABA: Dinaminiai skaidiniai nepalaikomi. Jei rodoma, kad skaidinys yra, tačiau pasirinkus jo šifruoti negalima, vadinasi skaidinys yra dinaminis. Dinaminis skaidinys atsiranda po to, kai Disko valdymo priemonėje kuriant naują skaidinį buvo sutrauktas skaidinys.

Jei skaidinys bus keičiamas į dinaminį skaidinį, bus parodytas įspėjimas.

Disko valdymas

- **Slapyvardis** – savo diskų įrenginius ar skaidinius galite kaip nors pavadinti, kad juos būtų galima lengvai identifikuoti.
- **Atjungti diskų įrenginiai** – „Drive Encryption“ gali susekti iš kompiuterio pašalintus diskus. Iš kompiuterio pašalintas diskas automatiškai perkeliamas į atjungtų sąrašą. Jei diskas grąžinamas į sistemą, jis vėl rodomas prijungtųjų sąraše.
- Jei daugiau nebenorite sekti ar valdyti atjungto diskų įrenginio, galite jį pašalinti iš atjungtų įrenginių sąrašo.
- „Drive Encryption“ priemonė bus suaktyvinta tol, kol nebus išvalyti visų prijungtų diskų įrenginių žymės langeliai ir atjungtų diskų sąrašas nebus tuščias.

Atsarginė kopija ir atkūrimas

Kai „Drive Encryption“ priemonė suaktyvinta, administratoriai, naudodamiesi šifravimo rakto atsarginės kopijos puslapiu, keičiamoje laikmenoje gali sukurti atsarginę šifravimo raktų kopiją ir atlikti atkūrimą.

Atsarginės šifravimo raktų kopijos kūrimas

Administratoriai keičiamųjų laikmenų įrenginyje gali sukurti atsarginę užšifruoto diskų įrenginio šifravimo rakto kopiją.

ĮSPĖJIMAS: Saugojimo įrenginį su atsargine rakto kopija būtinai laikykite saugioje vietoje, nes jei pamirštumėte slaptažodį, pamestumėte lustinę kortelę ir nebūtumėte užregistravę piršto, tik naudodamiesi šiuo įrenginiu galėsite atgauti prieigą prie kompiuterio. Laikymo vieta taip pat turėtų būti patikima, nes saugojimo įrenginys suteikia prieigą prie „Windows“.

1. Paleiskite **„Drive Encryption“**. Daugiau informacijos rasite skyriuje „„Drive Encryption“ atidarymas“ 31 puslapyje.
2. Pasirinkite diskų įrenginio žymės langelį ir tada spustelėkite arba bakstelėkite **„Backup Key“** (atsarginės kopijos raktas).
3. Parinktyje **„Create HP Drive Encryption recovery key“** (sukurti „HP Drive Encryption“ atkūrimo raktą) pasirinkite vieną ar kelias toliau nurodytas parinktis:
   - **„Removable Storage“** (keičiamoji laikmena) – pasirinkite žymės langelį ir tada pasirinkite saugojimo įrenginį, kuriame bus išsaugojamas šifravimo raktas.
   - **„SkyDrive“** – pasirinkite žymės langelį. Turite būti prisijungę prie interneto. Prisijunkite prie „Microsoft SkyDrive“ ir tada spustelėkite arba bakstelėkite **Taip**.

     PASTABA: jei norite pasinaudoti „HP Drive Encryption“ atsargine rakto kopija, kuri yra laikoma „SkyDrive“, turite ją atsisiųsti iš „SkyDrive“ į keičiamųjų laikmenų įrenginį ir tada saugojimo įrenginį įdėti į šį kompiuterį.

   - **TPM** (tik tam tikruose modeliuose) – leidžia atkurti duomenis naudojant TMP slaptažodį.

     ĮSPĖJIMAS: jei TMP yra išvalytas arba kompiuteris sugedęs, atsarginės kopijos pasiekti negalėsite. Jei pasirenkamas šis būdas, taip pat turėtų būti pasirenkamas ir kitas atsarginės kopijos kūrimo būdas.
4. Spustelėkite arba bakstelėkite **„Backup“** (atsarginė kopija).

   Šifravimo raktas išsaugojamas jūsų pasirinktame saugojimo įrenginyje.

Prieigos prie suaktyvinto kompiuterio atkūrimas naudojant atsarginę raktų kopiją

Administratoriai gali vykdyti atkūrimą naudodami „Drive Encryption“ raktą, kurio kopija aktyvinimo metu buvo išsaugota keičiamųjų laikmenų įrenginyje, arba „Drive Encryption“ priemonėje pasirinkdami **„Backup Key“** (atsarginė rakto kopija).

1. Įdėkite keičiamųjų laikmenų įrenginį,kuriame yra jūsų atsarginė rakto kopija.
2. Įjunkite kompiuterį.
3. Kai atsidarys „HP Drive Encryption“ prisijungimo dialogo langas, spustelėkite arba bakstelėkite **„Atkūrimas“**.
4. Įveskite failo, kuriame yra jūsų atsarginė rakto kopija, kelią arba pavadinimą ir tada spustelėkite arba bakstelėkite **Atkūrimas**.
5. Kai atsidarys patvirtinimo dialogo langas, spustelėkite arba bakstelėkite **Gerai**.

   Rodomas „Windows“ prisijungimo langas.

PASTABA: jei prisijungiant „Drive Encryption“ prisijungimo ekrane naudojamas atkūrimo raktas, norint gauti prieigą prie vartotojų abonementų, „Windows“ registracijoje reikia įvesti papildomus kredencialus. Ypač rekomenduojama atlikus atkūrimą pakeisti savo slaptažodį.

„HP SpareKey“ atkūrimo vykdymas

Jei priemonėje „Drive Encryption“ prieš įkraunant sistemą vykdysite „SpareKey“ atkūrimą, kad galėtumėte naudotis kompiuteriu, turėsite teisingai atsakyti į saugos klausimus. Norėdami gauti

daugiau informacijos apie „SpareKey“ atkūrimo nustatymą, žr. „HP Client Security“ programinės įrangos žinyną.

Jei pamiršote savo slaptažodį, „HP SpareKey“ atkūrimą atlikite taip:

1. Įjunkite kompiuterį.
2. Kai bus parodytas „HP Drive Encryption“ puslapis, nueikite į vartotojo prisijungimo puslapį.
3. Spustelėkite **„SpareKey“**.

   PASTABA: jei jūsų „SpareKey“ nebuvo inicijuotas „HP Client Security“ priemonėje, **„SpareKey“** mygtuko nebus.

4. Įveskite teisingus atsakymus į pateiktus klausimus ir tada spustelėkite **Registracija**.

   Rodomas „Windows“ prisijungimo langas.

PASTABA: jei prisijungiant „Drive Encryption“ prisijungimo ekrane naudojamas „SpareKey“ raktas, norint gauti prieigą prie vartotojų abonementų, „Windows“ registracijoje reikia įvesti papildomus kredencialus. Ypač rekomenduojama atlikus atkūrimą pakeisti savo slaptažodį.

6 „HP File Sanitizer“ (tik tam tikruose modeliuose)

Naudodami „File Sanitizer“ galite saugiai sunaikinti išteklius (pvz.: asmeninę informaciją arba failus, retrospektyvinius ar su tinklalapiais susijusius duomenis ar kitus duomenų komponentus) kompiuterio vidiniame standžiajame diske ir periodiškai ištuštinti kompiuterio vidinį standųjį diską.

„File Sanitizer“ priemone negalima apvalyti ar tuštinti šių tipų diskų:

- netriniųjų loginių diskų (SSD), įskaitant RAID tomus, kurie apima SSD įrenginį;
- išorinių diskų įrenginių, prijungtų naudojant USB, „Firewire“ arba eSATA sąsają.

Jei naikinimo ar apvalymo operaciją bandoma atlikti SSD diske, rodomas įspėjamasis pranešimas ir operacija neatliekama.

Naikinimas

Naikinimas skiriasi nuo įprastinio „Windows®“ trynimo veiksmo. Kai svarbius failus naikinate naudodami „File Sanitizer“ priemonę, failai yra perrašomi nereikšminga informacija ir originalių svarbių failų faktiškai neįmanoma atgauti. Paprastas „Windows“ trynimo veiksmas failą (arba išteklius) gali nepakeistą palikti standžiajame diske arba jį gali būti įmanoma atkurti pasitelkus kriminalistikos metodus.

Galite suplanuoti būsimą naikinimo laiką arba naikinimą galite suaktyvinti rankiniu būdu pasirinkdami **„File Sanitizer“** piktogramą pagrindiniame „HP Client Security“ ekrane arba naudodami **„File Sanitizer“** piktogramą, esančią „Windows“ darbalaukyje. Norėdami gauti daugiau informacijos, žr. „„Naikinimo tvarkaraščio nustatymas“ 40 puslapyje“, „„Naikinimas paspaudus dešinįjį pelės mygtuką“ 42 puslapyje“ arba „„Naikinimo operacijos pradėjimas rankiniu būdu“ 42 puslapyje“.

PASTABA: .dll failas naikinamas ir pašalinamas iš sistemos tik tuomet, jei jis buvo perkeltas į šiukšlinę.

Laisvos vietos tuštinimas

Ištrynus išteklių „Windows“ sistemoje, ištekliaus turinys nebus visiškai pašalintas iš jūsų standžiojo disko. „Windows“ ištrina tik ištekliaus nuorodą arba jo vietą standžiajame diske. Išteklių turinys ir toliau liks standžiajame diske, kol kiti ištekliai tą pačią vietą standžiajame diske perrašys nauja informacija.

Laisvos vietos tuštinimas leidžia saugiai įrašyti atsitiktinius duomenis į ištrintų išteklių vietą ir neleidžia vartotojams peržiūrėti originalaus ištrintų išteklių turinio.

PASTABA: Laisvos vietos tuštinimas papildomos apsaugos naikinamiems ištekliams nesuteikia.

Galite nustatyti būsimą laisvos vietos tuštinimo laiką arba laisvos vietos tuštinimą galite suaktyvinti rankiniu būdu pasirinkdami **„File Sanitizer“** piktogramą pagrindiniame „HP Client Security“ ekrane arba naudodami **„File Sanitizer“** piktogramą, esančią „Windows“ darbalaukyje. Norėdami gauti daugiau informacijos, žr. „„Laisvos vietos tuštinimo tvarkaraščio nustatymas“ 41 puslapyje“, „„Laisvos vietos tuštinimo pradėjimas rankiniu būdu“ 43 puslapyje“ arba „„„File Sanitizer“ piktogramos naudojimas“ 42 puslapyje“.

„File Sanitizer“ atidarymas

1. Pradžios ekrane spustelėkite arba bakstelėkite **„HP Client Security“** programėlę („Windows 8“).

   – arba –

   „Windows“ darbalaukyje, pranešimų srityje, esančioje užduočių juostos dešinėje pusėje, dukart spustelėkite arba dukart bakstelėkite **„HP Client Security“** piktogramą.

2. Parinktyje **Duomenys** spustelėkite arba bakstelėkite **„File Sanitizer“**.

– arba –

▲ Dukart spustelėkite arba dukart bakstelėkite **„File Sanitizer“** piktogramą „Windows“ darbalaukyje.

– arba –

▲ Dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite **„File Sanitizer“** piktogramą „Windows“ darbalaukyje ir tuomet pasirinkite **„Open File Sanitizer“** (Atidaryti „Open File Sanitizer“).

Sąrankos procedūros

Naikinimas – „File Sanitizer“ saugiai ištrina arba sunaikina pasirinktų kategorijų išteklius.

1. Parinktyje **„Shredding“** (naikinimas) kiekvienam naikinamo failo tipui pasirinkite žymės langelį arba išvalykite failų, kurių nenorite naikinti, žymės langelius.

   - **Šiukšlinė** – sunaikina visus šiukšlinėje esančius elementus.
   - **Laikinieji sistemos failai** – sunaikina visus sistemos laikinajame aplanke rastus failus. Toliau nurodyti aplinkos kintamieji ieškomi toliau pateikta tvarka ir pirmasis rastas kelias laikomas sistemos aplanku:
     - TMP
     - TEMP
   - **Laikinieji interneto failai** – sunaikina tinklalapių, vaizdų ir laikmenų kopijas, kurias žiniatinklio naršyklė įrašo, kad juos būtų galima greičiau peržiūrėti.
   - **Slapukai** – sunaikina visus failus, kuriuos kompiuteryje išsaugojo tinklalapiai, kad būtų įrašytos nuostatos, pvz., prisijungimo informacija.

2. Norėdami pradėti naikinti, spustelėkite arba bakstelėkite **„Shred“** (naikinti).

Tuštinimas – įrašo atsitiktinius duomenis į laisvą vietą ir neleidžia atkurti ištrintų elementų.

▲ Norėdami pradėti tuštinti, spustelėkite arba bakstelėkite **„Bleach“** (tuštinti).

„File Sanitizer“ parinktys – norėdami įgalinti atskiras, žemiau nurodytas parinktis, pasirinkite jų žymės langelį, arba jį išvalykite, jei parinktį norite išjungti:

- **„Enable Desktop icon“** (įgalinti darbalaukio elementą) – „File Sanitizer“ piktogramą rodo „Windows“ darbalaukyje.
- **„Enable right-click“** (įgalinti dešinįjį pelės klavišą) – leidžia spustelėti dešiniuoju pelės klavišu arba bakstelėti ir palaikyti vieną iš išteklių ir tuomet pasirinkti **„HP File Sanitizer – Shred“** („HP File Sanitizer“ – naikinti).

- **„Ask for Windows password before manual shredding“** (prašyti įvesti „Windows“ slaptažodį prieš naikinant rankiniu būdu) – reikia autentifikuoti prieš rankiniu būdu sunaikinant elementą.
- **„Shred Cookies and Temporary Internet Files on browser close“** (naikinti slapukus ir laikinuosius interneto failus uždarant naršyklę) – sunaikina visus pasirinktus išteklius, susijusius su žiniatinkliu, pvz., naršyklės URL retrospektyvą, kai uždarote interneto naršyklę.

Naikinimo tvarkaraščio nustatymas

Galite suplanuoti laiką, kuriuo naikinimas bus vykdomas automatiškai arba išteklius galite sunaikinti bet kuriuo metu rankiniu būdu. Norėdami gauti daugiau informacijos, žr. „Sąrankos procedūros“ 39 puslapyje.

1. Atidarykite „File Sanitizer“ ir tada spustelėkite arba bakstelėkite **Nuostatos**.
2. Norėdami suplanuoti laiką, kuriuo turėtų būti naikinami pasirinkti ištekliai, parinktyje **„Shred Schedule“** (naikinimo tvarkaraštis) pasirinkite **Niekada**, **Vieną kartą**, **Kasdien**, **Kas savaitę** arba **Kas mėnesį** ir tuomet pasirinkite dieną ir laiką:
   a. Spustelėkite arba bakstelėkite valandos, minutės arba AM/PM laukelį.
   b. Slinkite, kol pageidaujama reikšmė bus rodoma tame pačiame lygyje kaip ir kiti laukeliai.
   c. Spustelėkite arba bakstelėkite laiko nustatymo laukelį supančią baltą vietą.
   d. Tą patį veiksmą atlikite visiems laukeliams, kol bus pasirinktas teisingas tvarkaraštis.
3. Yra nurodyti šie keturi išteklių tipai:
   - **Šiukšlinė** – sunaikina visus šiukšlinėje esančius elementus.
   - **Laikinieji sistemos failai** – sunaikina visus sistemos laikinajame aplanke rastus failus. Toliau nurodyti aplinkos kintamieji ieškomi toliau pateikta tvarka ir pirmasis rastas kelias laikomas sistemos aplanku:
     - TMP
     - TEMP
   - **Laikinieji interneto failai** – sunaikina tinklalapių, vaizdų ir laikmenų kopijas, kurias žiniatinklio naršyklė įrašo, kad juos būtų galima greičiau peržiūrėti.
   - **Slapukai** – sunaikina visus failus, kuriuos kompiuteryje išsaugojo tinklalapiai, kad būtų įrašytos nuostatos, pvz., prisijungimo informacija.

   Jei ištekliai buvo pažymėti, jie bus sunaikinti numatytu laiku.
4. Norėdami pasirinkti papildomus išteklius sunaikinti:
   a. Parinktyje **„Scheduled Shred List“** (planuojamo naikinimo sąrašas) spustelėkite arba bakstelėkite **Įtraukti aplanką** ir tuomet nueikite į failą arba aplanką.
   b. Spustelėkite arba bakstelėkite **Atidaryti** ir tada spustelėkite arba bakstelėkite **Gerai**.

   Norėdami išteklių pašalinti iš planuojamo naikinimo sąrašo, išvalykite to ištekliaus žymės langelį.

Laisvos vietos tuštinimo tvarkaraščio nustatymas

Laisvos vietos tuštinimas papildomos apsaugos naikinamiems ištekliams nesuteikia.

1. Atidarykite „File Sanitizer“ ir tada spustelėkite arba bakstelėkite **Nuostatos**.
2. Norėdami suplanuoti laiką, kuriuo turėtų būti atliekamas laisvos vietos tuštinimas jūsų standžiajame diske, parinktyje **„Bleach Schedule“** (laisvos vietos tuštinimo tvarkaraštis) pasirinkite **Niekada**, **Vieną kartą**, **Kasdien**, **Kas savaitę** arba **Kas mėnesį** ir tuomet pasirinkite dieną ir laiką.
   a. Spustelėkite arba bakstelėkite valandos, minutės arba AM/PM laukelį.
   b. Slinkite, kol pageidaujamas laikas bus rodomas tame pačiame lygyje kaip ir kiti laukeliai.
   c. Spustelėkite arba bakstelėkite laiko nustatymo laukelį supančią baltą vietą.
   d. Veiksmą pakartokite, kol bus pasirinktas teisingas tvarkaraštis.

PASTABA: Laisvos vietos tuštinimo operacija gali užtrukti gana ilgai. Nepamirškite kompiuterio prijungti prie kintamosios srovės šaltinio. Nors laisvos vietos tuštinimo operacija atliekama kompiuterio fone, didesnis procesoriaus naudojimas gali turėti įtakos kompiuterio našumui. Laisvos vietos tuštinimo operaciją galima atlikti po darbo valandų arba kai kompiuteris nėra naudojamas.

Failų apsaugojimas nuo naikinimo

Norėdami apsaugoti failus arba aplankus, kad jie nebūtų sunaikinti:

1. Atidarykite „File Sanitizer“ ir tada spustelėkite arba bakstelėkite **Nuostatos**.
2. Parinktyje **„Never Shred List“** (niekada nenaikinamų elementų sąrašas) spustelėkite arba bakstelėkite **Įtraukti aplanką** ir tuomet nueikite į failą arba aplanką.
3. Spustelėkite arba bakstelėkite **Atidaryti** ir tada spustelėkite arba bakstelėkite **Gerai**.

PASTABA: Failai, esantys šiame sąraše, yra apsaugoti tol, kol jie bus įtraukti į šį sąrašą.

Norėdami išteklių pašalinti iš išimčių sąrašo, išvalykite to ištekliaus žymės langelį.

Bendrosios užduotys

„File Sanitizer“ naudokite norėdami atlikti šias užduotis:

- **Naudokite „File Sanitizer“ piktogramą norėdami paleisti naikinimą** – vilkite failus į **„File Sanitizer“** piktogramą „Windows“ darbalaukyje. Norėdami gauti išsamesnės informacijos, žr. „„File Sanitizer“ piktogramos naudojimas“ 42 puslapyje“.
- **Konkretų arba pasirinktą išteklių sunaikinkite rankiniu būdu** – failus naikinkite bet kuriuo metu nelaukdami numatyto naikinimo laiko. Norėdami gauti išsamesnės informacijos, žr. „„Naikinimas paspaudus dešinįjį pelės mygtuką“ 42 puslapyje“ arba „„Naikinimo operacijos pradėjimas rankiniu būdu“ 42 puslapyje“.
- **Laisvos vietos tuštinimą suaktyvinkite rankiniu** – laisvos vietos tuštinimą suaktyvinkite bet kuriuo metu. Norėdami gauti išsamesnės informacijos, žr. „„Laisvos vietos tuštinimo pradėjimas rankiniu būdu“ 43 puslapyje“.
- **Peržiūrėkite žurnalo failus** – peržiūrėkite naikinimo ir laisvos vietos tuštinimo žurnalų failus, kuriuose užfiksuotos paskutinės naikinimo arba laisvos vietos tuštinimo operacijos metu aptiktos klaidos ar gedimai. Norėdami gauti išsamesnės informacijos, žr. „„Žurnalo failų peržiūra“ 43 puslapyje“.

PASTABA: Naikinimo arba laisvos vietos tuštinimo operacija gali užtrukti gana ilgai. Nors naikinimo ir laisvos vietos tuštinimo operacijos atliekamos kompiuterio fone, didesnis procesoriaus naudojimas gali turėti įtakos kompiuterio našumui.

„File Sanitizer“ piktogramos naudojimas

ĮSPĖJIMAS: Susmulkintų elementų negalima atkurti. Gerai apgalvokite, kuriuos elementus pasirinksite sunaikinti rankiniu būdu.

Naikinimo operaciją pradėjus rankiniu būdu, sunaikinamas įprastinis naikinimo sąrašas „File Sanitizer“ rodinyje (žr. „„Sąrankos procedūros“ 39 puslapyje“).

Naikinimo operaciją rankiniu būdu galite pradėti vienu iš šių būdų:

1. Atidarykite „File Sanitizer“ (žr. „„File Sanitizer“ atidarymas“ 39 puslapyje“) ir tada spustelėkite arba bakstelėkite **„Shred“** (naikinti).
2. Kai atsidarys patvirtinimo dialogo langas, patikrinkite, ar pažymėtas išteklius, kurį norite sunaikinti ir tada spustelėkite arba bakstelėkite **Gerai**.

– arba –

1. Dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite **„File Sanitizer“** piktogramą „Windows“ darbalaukyje ir tuomet spustelėkite arba bakstelėkite **„Shred Now“** (naikinti dabar).
2. Kai atsidarys patvirtinimo dialogo langas, patikrinkite, ar pažymėtas išteklius, kurį norite sunaikinti ir tada spustelėkite arba bakstelėkite **„Shred“** (naikinti).

Naikinimas paspaudus dešinįjį pelės mygtuką

ĮSPĖJIMAS: Susmulkintų elementų negalima atkurti. Gerai apgalvokite, kuriuos elementus pasirinksite sunaikinti rankiniu būdu.

Jei **„Enable right-click shredding“** (įgalinti naikinimą paspaudus dešinįjį pelės klavišą), buvo pasirinkta „File Sanitizer“ rodinyje, išteklių galite sunaikinti taip:

1. Nueikite į dokumentą arba aplanką, kurį norite sunaikinti.
2. Dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite failą arba aplanką ir tada pasirinkite **„HP File Sanitizer – Shred“** („HP File Sanitizer“ – naikinti).

Naikinimo operacijos pradėjimas rankiniu būdu

ĮSPĖJIMAS: Susmulkintų elementų negalima atkurti. Gerai apgalvokite, kuriuos elementus pasirinksite sunaikinti rankiniu būdu.

Naikinimo operaciją pradėjus rankiniu būdu, sunaikinamas įprastinis naikinimo sąrašas „File Sanitizer“ rodinyje (žr. „„Sąrankos procedūros“ 39 puslapyje“).

Naikinimo operaciją rankiniu būdu galite pradėti vienu iš šių būdų:

1. Atidarykite „File Sanitizer“ (žr. „„File Sanitizer“ atidarymas“ 39 puslapyje“) ir tada spustelėkite arba bakstelėkite **„Shred“** (naikinti).
2. Kai atsidarys patvirtinimo dialogo langas, patikrinkite, ar pažymėtas išteklius, kurį norite sunaikinti ir tada spustelėkite arba bakstelėkite **Gerai**.

– arba –

1. Dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite **„File Sanitizer“** piktogramą „Windows“ darbalaukyje ir tuomet spustelėkite arba bakstelėkite **„Shred Now“** (naikinti dabar).
2. Kai atsidarys patvirtinimo dialogo langas, patikrinkite, ar pažymėtas išteklius, kurį norite sunaikinti ir tada spustelėkite arba bakstelėkite **„Shred“** (naikinti).

Laisvos vietos tuštinimo pradėjimas rankiniu būdu

Tuštinimo operaciją pradėjus rankiniu būdu, tuštinamas įprastinis naikinimo sąrašas „File Sanitizer“ rodinyje (žr. „Sąrankos procedūros“ 39 puslapyje“).

Tuštinimo operaciją rankiniu būdu galite pradėti vienu iš šių būdų:

1. Atidarykite „File Sanitizer“ (žr. „„File Sanitizer“ atidarymas“ 39 puslapyje“) ir tada spustelėkite arba bakstelėkite **„Bleach“** (tuštinti).
2. Kai atsidarys patvirtinimo dialogo langas, spustelėkite arba bakstelėkite **Gerai**.

– arba –

1. Dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite **„File Sanitizer“** piktogramą „Windows“ darbalaukyje ir tuomet spustelėkite arba bakstelėkite **„Bleach Now“** (tuštinti dabar).
2. Kai atsidarys patvirtinimo dialogo langas, spustelėkite arba bakstelėkite **„Bleach“** (tuštinti).

Žurnalo failų peržiūra

Po kiekvienos naikinimo ar laisvos vietos tuštinimo operacijos sukuriami aptiktų klaidų ir gedimų žurnalo failai. Žurnalo failai visuomet atnaujinami pagal paskutinę naikinimo arba laisvos vietos tuštinimo operaciją.

PASTABA: Failai, kurie sunaikinti arba ištuštinti sėkmingai, žurnalo faile nerodomi.

Vienas žurnalo failas sukuriamas naikinimo operacijai ir kitas failas sukuriamas laisvos vietos tuštinimo operacijai. Abu žurnalo failai yra šiuose standžiojo disko aplankuose:

- C:\Programų failai\„Hewlett-Packard“\„File Sanitizer“*[Vartotojovardas]*_ShredderLog.txt
- C:\Programų failai\„Hewlett-Packard“\„File Sanitizer“*[Vartotojovardas]*_DiskBleachLog.txt

64 bitų sistemoje šie žurnalo failai yra šiuose standžiojo disko aplankuose:

- C:\Programų failai (x86)\„Hewlett-Packard“\„File Sanitizer“*[Vartotojovardas]*_ShredderLog.txt
- C:\Programų failai (x86)\„Hewlett-Packard“\„File Sanitizer“*[Vartotojovardas]*_DiskBleachLog.txt

7 „HP Device Access Manager“ (tik tam tikruose modeliuose)

„HP Device Access Manager“ priemonė išjungdama duomenų perdavimo įrenginius valdo prieigą prie duomenų.

PASTABA: kai kurių vartotojo sąsajos / įvesties prietaisų, pvz., pelės, klaviatūros, jutiklinės planšetės ar pirštų atspaudų skaitytuvo, „Device Access Manager“ nevaldo. Daugiau informacijos rasite skyriuje „Nevaldomųjų įrenginių klasės“ 47 puslapyje.

„Windows®“ operacinės sistemos administratoriai naudodami „HP Device Access Manager“ valdo prieigą prie sistemos įrenginių ir apsaugo nuo nesankcionuotos prieigos:

- Įrenginių profiliai yra suskurti kiekvienam vartotojui ir nustato įrenginius, kuriuos jie gali naudoti arba prie kurių prieiga jiems nesuteikta.
- „Just In Time Authentication“ (JITA) leidžia iš anksto nurodytiems vartotojams save autentifikuoti, kad po to jie galėtų naudotis įrenginiais, kurie paprastai yra nepasiekiami.
- Administratoriai ir patikimi vartotojai gali būti neįtraukti į įrenginio prieigos apribojimus, kuriuos nustato „Device Access Manager“ priemonė juos įtraukdama į įrenginio administratorių grupę. Šios grupės narystė valdoma naudojant papildomus nustatymus.
- Prieiga prie įrenginio gali būti suteikta arba draudžiama priklausomai nuo grupės narystės ar atskiro vartotojo statuso.
- Naudojant kai kurias įrenginių klases, pvz., kompaktinių diskų ir DVD diskų įrenginius, prieiga skaityti ir prieiga rašyti gali būti suteikta arba draudžiama atskirai.

Užbaigus darbą su „HP Client Security“ sąrankos vedliu, priemonė „HP Device Access Manager“ automatiškai konfigūruojama tokiais nustatymais:

- „Just In Time Authentication“ (JITA) keičiamoji laikmena yra įgalinta administratoriams ir vartotojams.
- Įrenginio naudojimo taisyklės suteikia visišką prieigą prie kitų įrenginių.

„Device Access Manager“ atidarymas

1. Pradžios ekrane spustelėkite arba bakstelėkite **„HP Client Security“** programėlę („Windows 8“).

   – arba –

   „Windows“ darbalaukyje, pranešimų srityje, esančioje užduočių juostos dešinėje pusėje, dukart spustelėkite arba dukart bakstelėkite **„HP Client Security“** piktogramą.

2. Parinktyje **Įrenginys** spustelėkite arba bakstelėkite **„Device Permissions“** (įrenginio leidimai).

   - Paprasti vartotojai gali peržiūrėti savo dabartinę prieigą prie įrenginio žr. „Vartotojo rodinys“ 45 puslapyje“).
   - Administratoriai gali peržiūrėti ir keisti šiuo metu kompiuteriui sukonfigūruotą prieigą prie įrenginio. Tai padaryti gali spustelėdami arba bakstelėdami **Keisti** ir tada įvesdami administratoriaus slaptažodį (žr. „Sistemos rodinys“ 45 puslapyje“).

Vartotojo rodinys

Kai **„Device Permissions“** (įrenginio leidimai) parinktis yra pasirinkta, rodomas vartotojo rodinys. Priklausomai nuo naudojimo taisyklių, paprastieji vartotojai ir administratoriai gali peržiūrėti savo prieigą šiame kompiuteryje prie įrenginių klasių ar atskirų įrenginių.

- **Dabartinis vartotojas** – rodomas vartotojo, kuris šiuo metu yra prisijungęs, vardas.
- **Įrenginio klasė** – rodomi įrenginių tipai.
- **Prieiga** – rodoma jūsų šiuo metu sukonfigūruota prieiga prie įrenginių tipų ar atskirų įrenginių.
- **Trukmė** – rodomas laiko limitas prieigai prie CD / DVD-ROM diskų įrenginių arba keičiamų diskų įrenginių.
- **Nustatymai** – administratoriai gali pakeisti, kuriems diskų įrenginiams suteikiama „Device Access Manager“ priemonės valdoma prieiga.

Sistemos rodinys

Sistemos rodinyje administratoriai vartotojų arba administratorių grupėms gali suteikti arba uždrausti prieigą prie šio kompiuterio įrenginių.

▲ Administratoriai sistemos rodinį gali pasiekti spustelėdami arba bakstelėdami **Keisti**, įvesdami administratoriaus slaptažodį ir tada pasirinkdami iš šių parinkčių:

- **„Device Access Manager“** – norėdami įjungti arba išjungti „HP Device Access Manager“ priemonę su „Just In Time Authentication“, spustelėkite arba bakstelėkite **Įjungti** arba **Išjungti**.
- **Šio kompiuterio vartotojai ir grupės** – rodo vartotojų arba administratorių grupę, kuriai yra suteikta arba draudžiama prieiga prie tam tikrų įrenginių klasių.
- **Įrenginio klasė** – rodo įrenginių klases ir įrenginius, kurie yra įdiegti šioje sistemoje arba galėjo būti įdiegti anksčiau. Norėdami sąrašą išplėsti, spustelėkite **+** piktogramą. Rodomi visi prie šio kompiuterio prijungti įrenginiai ir taip pat išplečiamos administratorių ir vartotojų grupės, kad matytųsi jų narystė. Norėdami įrenginių sąrašą atnaujinti, spustelėkite apvalios strėlės (atnaujinimo) piktogramą.
  - Apsauga dažniausiai taikoma įrenginio klasei. Jei prieiga nustatyta į **Leisti**, pasirinktas vartotojas ar grupė turės prieigą prie bet kurio įrenginio, esančio įrenginio klasėje.
  - Apsauga taip pat gali būti taikoma ir konkretiems įrenginiams.
  - Sukonfigūruokite „Just In Time authentication“ (JITA), kad pasirinkti vartotojai save autentifikuodami galėtų naudotis CD / DVD-ROM diskų įrenginiais arba keičiamaisiais diskų įrenginiais. Daugiau informacijos rasite skyriuje „JITA konfigūracija“ 46 puslapyje.
  - Suteikite arba uždrauskite prieigą prie kitų įrenginių klasių, pvz., keičiamosios laikmenos (pvz., USB „flash“ disko), nuosekliojo ir lygiagrečiojo prievadų, „Bluetooth®“ įrenginio, modemo, PCMCIA / „ExpressCard“ įrenginių, 1394 įrenginių, pirštų atspaudų skaitytuvo ir lustinių kortelių skaitytuvo. Jei pirštų atspaudų skaitytuvas ir lustinių kortelių skaitytuvas yra uždrausti, jais galima naudotis kaip autentifikavimo kredencialais, tačiau jais negalima naudotis seanso naudojimo taisyklių lygmenyje.

    PASTABA: jei „Bluetooth“ įrenginiai naudojami kaip autentifikavimo kredencialai, „Bluetooth“ įrenginio prieiga neturėtų būti ribojama „Device Access Manager“ naudojimo taisyklių.

  - Kai pasirenkate nustatymą grupės arba įrenginio klasės lygmenyje ir jūsų klausiama, ar šį nustatymą taikyti antriniams objektams:

Taip – nustatymas bus išplatintas.

Ne – nustatymas nebus išplatintas.

- Kai kurias įrenginių klases, pvz., DVD ir CD-ROM, galima papildomai valdyti atskirai suteikiant arba uždraudžiant prieigą skaitymo ir rašymo veiksmams.

PASTABA: Administratorių grupės į vartotojų sąrašą įtraukti negalima.

- **Prieiga** – spustelėkite arba bakstelėkite rodyklę žemyn ir pasirinkite vieną iš toliau nurodytų prieigos tipų, kad suteiktumėte arba uždraustumėte prieigą:
  - **Leisti – visa prieiga**
  - **Leisti – tik skaitomas**
  - **Leisti – reikalinga JITA** – norėdami gauti daugiau informacijos, žr. „JITA konfigūracija“ 46 puslapyje“f

    Jei pasirinktas šis prieigos tipas, parinktyje **Trukmė** spustelėkite arba bakstelėkite rodyklę žemyn, kad pasirinktumėte laiko limitą.
  - **Drausti**
- **Trukmė** – spustelėkite arba bakstelėkite rodyklę žemyn, kad pasirinktumėte laiko limitą prieigai prie CD / DVD-ROM diskų įrenginių arba keičiamų diskų įrenginių (žr. „JITA konfigūracija“ 46 puslapyje“).

JITA konfigūracija

JITA konfigūracija leidžia administratoriui peržiūrėti ir modifikuoti vartotojų ir grupių, kurių vartotojams leidžiama prieiga prie įrenginių naudojant „Just In Time Authentication“ (JITA), sąrašus.

JITA įgalinti vartotojai galės naudotis kai kuriais įrenginiais, kurių naudojimo taisyklės sukurtos **„Device Class Configuration“** priemonės rodinyje buvo apribotos.

JITA laikotarpį galima autorizuoti nurodytoms minutėms arba neribotam laikui. Neribojamas vartotojas įrenginiu naudotis galės nuo to laiko, kai autentikuos iki tada, kai išsiregistruos iš sistemos.

Jei vartotojui suteiktas ribojamas JITA laikotarpis, minutę prieš tai, kai baigsis JITA laikas, vartotojo bus klausiama, ar reikia pratęsti prieigos laiką. Kai vartotojas išsiregistruos iš sistemos arba prie sistemos prisijungs kitas vartotojas, JITA laikotarpis pasibaigs. Vartotojui prisijungus kitą kartą ir bandant pasiekti JITA įgalintą įrenginį, jis bus paragintas įvesti kredencialus.

JITA galima šioms įrenginių klasėms:

- DVD / CD-ROM diskų įrenginių
- Keičiamųjų diskų įrenginių

JITA naudojimo taisyklių kūrimas vartotojui arba grupei

Administratoriai, naudodami „Just In Time Authentication“ (JITA), gali vartotojui arba grupei suteikti prieigą prie įrenginio.

1. Paleiskite **„Device Access Manager“** ir tada spustelėkite arba bakstelėkite **Keisti**.
2. Pasirinkite vartotoją arba grupę ir tada parinktyje **Prieiga** parinkčiai **„Removable Disk drives“** (keičiamojo disko įrenginiai) arba parinkčiai **„DVD/CD-ROM drives“** (DVD / CD-ROM diskų įrenginiai) spustelėkite arba bakstelėkite rodyklę žemyn ir pasirinkite **„Allow – JITA Required“** (leisti - reikalinga JITA).
3. Parinktyje **Trukmė** spustelėkite arba bakstelėkite rodyklę žemyn, kad pasirinktumėte laikotarpį JITA prieigai.

Vartotojas turi išsiregistruoti ir iš naujo prisijungti, kad būtų pritaikyti nauji JITA nustatymai.

JITA naudojimo taisyklių išjungimas vartotojui arba grupei

Administratoriai, naudodami „Just In Time Authentication“, gali vartotojui arba grupei išjungti prieigą prie įrenginio.

1. Paleiskite **„Device Access Manager“** ir tada spustelėkite arba bakstelėkite **Keisti**.
2. Pasirinkite vartotoją arba grupę ir tada parinktyje **Prieiga** parinkčiai **„Removable Disk drives“** (keičiamojo disko įrenginiai) arba parinkčiai **„DVD/CD-ROM drives“** (DVD / CD-ROM diskų įrenginiai) spustelėkite arba bakstelėkite rodyklę žemyn ir pasirinkite **„Deny“** (drausti).

Kai vartotojas prisijungs ir bandys pasinaudoti įrenginiu, prieiga bus uždrausta.

Nustatymai

Nustatymų rodinys administratoriui leidžia peržiūrėti ir pakeisti diskų įrenginius, kurių prieiga yra valdoma „Device Access Manager“.

PASTABA: „Device Access Manager“ priemonė turi būti įgalinta, kai konfigūruojamas diskų įrenginio raidžių sąrašas (žr. „Sistemos rodinys“ 45 puslapyje“).

Nevaldomųjų įrenginių klasės

„HP Device Access Manager“ priemonė nevaldo šių įrenginių klasių:

- Įvesties / išvesties įrenginių
  - CD-ROM
  - Diskų įrenginio
  - Diskelio valdiklio (FDC)
  - Standžiojo disko valdiklio (HDC)
  - Vartotojo sąsajos prietaiso (HID) klasės
  - Infraraudonųjų spindulių vartotojo sąsajos prietaisų
  - Pelę
  - Kelių prievadų nuosekliųjų
  - Klaviatūra

- „Plug and Play“ (PnP) spausdintuvų
- Spausdintuvų
- Spausdintuvo plėtotės

- Maitinimas
  - Patobulinto energijos vartojimo valdymo (APM) palaikymo
  - Akumuliatorius
- Kitų
  - Kompiuteris
  - Dekoderio
  - Ekranas
  - „Intel®“ suvienodinto monitoriaus tvarkyklės
  - „Legacard“
  - Laikmenų tvarkyklės
  - Laikmenų keitimo įrenginio
  - Atminties technologijos
  - Monitorius
  - Daugiafunkcinių
  - Tinklo kliento
  - Tinklo tarnybos
  - Tinklo perdavimo
  - Procesorius
  - SCSI adapterio
  - Saugos spartintuvo
  - Apsaugos įrenginių
  - Sistemos
  - Nežinomas
  - Tomo
  - Tomo momentinės kopijos

8 „HP Trust Circles“

„HP Trust Circles“ yra failų ir dokumentų saugos programa, kuri aplankų failų šifravimą derina su patogia patikimo rato dokumentus bendrinančia galimybe. Programa užšifruoja failus, esančius vartotojo nurodytuose aplankuose ir juos apsaugo patikimame rate. Apsaugotuosius failus naudoti ir bendrinti gali tik patikimo rato nariai. Jei apsaugotą failą gauną ne rato narys, failas lieka užšifruotas ir ne narys negali pasiekti jo turinio.

„Trust Circles“ atidarymas

1. Pradžios ekrane spustelėkite arba bakstelėkite **„HP Client Security“** programėlę.

   – arba –

   „Windows“ darbalaukyje, pranešimų srityje, esančioje užduočių juostos dešinėje pusėje, dukart spustelėkite **„HP Client Security“** piktogramą.

2. Parinktyje **Duomenys** spustelėkite arba bakstelėkite **„Trust Circles“**.

Darbo pradžia

El. pašto pakvietimus išsiųsti ir į juos atsakyti galite dviem būdais:

- **Naudojant „Microsoft® Outlook“** – „Trust Circles“ programą naudojant su „Microsoft Outlook“ visų pakvietimų ir atsakymų iš kitų „Trust Circle“ vartotojų apdorojimas vykdomas automatiškai.
- **Naudojant „Gmail“, „Yahoo“, „Outlook.com“ ar kitas el. pašto paslaugas (SMTP)** – kai įvedate savo vardą, el. pašto adresą ir slaptažodį, „Trust Circle“ jūsų el. pašto paslaugos pagalba išsiunčia el. pašto pakvietimus nariams, parinktiems prisijungti prie jūsų patikimo rato.

Pagrindinio profilio nustatymas

1. Įveskite savo vardą ir el. pašto adresą, o tada spustelėkite arba bakstelėkite **Toliau**.

   Vardas matomas visiems nariams, kurie yra pakviesti prisijungti prie jūsų patikimo rato. El. paštas naudojamas siųsti, gauti arba atsakyti į pakvietimus.

2. Įveskite el. pašto abonemento slaptažodį ir tada spustelėkite arba bakstelėkite **Toliau**.

   Išsiunčiamas bandomasis el. laiškas siekiant užtikrinti, kad el. paštas yra tinkamai nustatytas.

PASTABA: kompiuteris turi būti prijungtas prie tinklo.

3. **„Trust Circles Name“** („Trust Circles“ pavadinimo) laukelyje įveskite patikimo rato pavadinimą ir tada spustelėkite arba bakstelėkite **Toliau**.

4. Įtraukite narius ir aplankus ir tada spustelėkite arba bakstelėkite **Toliau**. Patikimas ratas sukuriamas su visais pasirinktais aplankais ir el. pašto pakvietimai išsiunčiami visiems pasirinktiems nariams. Jei dėl kokios nors priežasties pakvietimo neitų išsiųsti, bus parodytas pranešimas. Narius galite bet kuriuo metu pakviesti iš naujo – „Trust Circle“ rodinyje spustelėkite **„Your Trust Circles“** (jūsų patikimi ratai) ir tada dukart spustelėkite arba dukart bakstelėkite patikimą ratą. Daugiau informacijos rasite skyriuje „„Trust Circles““ 50 puslapyje.

„Trust Circles“

Patikimą ratą galite sukurti pradinės sąrankos metu, po to, kai įvesite el. pašto adresą arba „Trust Circle“ rodinyje:

▲ „Trust Circles“ rodinyje spustelėkite arba bakstelėkite **„Create Trust Circle“** (sukurti „Trust Circle“) ir tada įveskite patikimo rato pavadinimą.

- Norėdami į patikimą ratą įtraukti narius, spustelėkite arba bakstelėkite **M+** piktogramą, esančią šalia **„Members“** (nariai), ir tada vykdykite ekrane pateikiamus nurodymus.
- Norėdami į patikimą ratą įtraukti aplankus, spustelėkite arba bakstelėkite **+** piktogramą, esančią šalia **„Aplankai“**, ir tada vykdykite ekrane pateikiamus nurodymus.

Aplankų įtraukimas į patikimą ratą

Aplankų įtraukimas į naują patikimą ratą:

- Kurdami patikimą ratą galite įtraukti aplankus spustelėdami arba bakstelėdami **+** piktogramą, esančią šalia **Aplankai** ir vykdydami ekrane pateikiamus nurodymus.

  – arba –

- „Windows“ naršyklėje dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite aplanką, kuris šiuo metu nėra įtrauktas į jokį patikimą ratą, pasirinkite **„Trust Circle“** ir tada pasirinkite **„Create Trust Circle from Folder“** (sukurti „Trust Circle“ iš aplanko).

PATARIMAS: galite pasirinkti vieną ar kelis aplankus.

Aplankų įtraukimas į esamą patikimą ratą:

- „Trust Circle“ rodinyje spustelėkite **„Your Trust Circles“** (jūsų patikimi ratai), dukart spustelėkite arba dukart bakstelėkite esamą ratą, kad būtų parodyti dabartiniai aplankai, spustelėkite arba bakstelėkite **+** piktogramą, esančią šalia **Aplankai** ir tada vykdykite ekrane pateikiamus nurodymus.

  – arba –

- „Windows“ naršyklėje dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite aplanką, kuris šiuo metu nėra įtrauktas į jokį patikimą ratą, pasirinkite **„Trust Circle“** ir tada pasirinkite **„Add to existing Trust Circle from Folder“** (įtraukti į esamą „Trust Circle“ iš aplanko).

PATARIMAS: galite pasirinkti vieną ar kelis aplankus.

Kai aplankas bus įtrauktas į patikimą ratą, „Trust Circle“ programa aplanką ir jo turinį automatiškai užšifruos. Kai visi failai bus užšifruoti, bus parodytas pranešimas. Be to, ant visų užšifruotų aplankų piktogramų ir aplanko failų piktogramų rodomas žalias užrakto simbolis, kuris reiškia, kad šie elementai yra visapusiškai apsaugoti.

Narių įtraukimas į patikimą ratą

Į patikimą ratą norint įtraukti narius, reikia atlikti tris veiksmus:

1. **Pakviesti** – pirmiausia patikimo rato savininkas pakviečia narį (-ius). Kvietimo el. laiškas gali būti išsiunčiamas keletui narių arba siuntimo sąrašų / grupių.
2. **Priimti** – pakviestasis gauna pakvietimą ir nusprendžia, ar jį priimti ar atmesti. Jei pakviestasis pakvietimą priima, pakvietusiam asmeniui išsiunčiamas atsakymas el. laišku. Jei pakvietimas buvo išsiųstas grupei, kiekvienas jos narys gaus atskirą pakvietimą ir nuspręs, ar jį priimti ar atmesti.
3. **Įtraukti** – pakvietusiam asmeniui suteikiama paskutinė galimybė nuspręsti, ar įtraukti narį į patikimą ratą. Jei pakvietęs asmuo nuspręs asmenį įtraukti, pakviestajam bus išsiųstas el. laiškas patvirtinantis pakviestojo atsakymą. Pakvietęs asmuo ir pakviestasis gali pasirinktinai patikrinti pakvietimo procesą. Pakviestajam rodomas patvirtinimo kodas, kurį jis turi perskaityti pakvietusiam asmeniui telefonu. Kodą patvirtinus, pakvietęs asmuo gali išsiųsti galutinį įtraukimo el. laišką.

Narių įtraukimas į naują patikimą ratą:

▲ Kurdami patikimą ratą galite įtraukti aplankus spustelėdami arba bakstelėdami **M+** piktogramą, esančią šalia **Nariai** ir vykdydami ekrane pateikiamus nurodymus.

- Jei naudojatės „Outlook“, iš „Outlook“ adresų knygos pasirinkite adresatus ir tada spustelėkite **Gerai**.
- Jei naudojatės kita el. pašto paslauga, naujus el. pašto adresus į „Trust Circle“ įtraukite rankiniu būdu arba galite juos nuskaityti iš el. pašto adreso, užregistruoto „Trust Circle“ programoje.

Narių įtraukimas į esamą patikimą ratą:

▲ „Trust Circle“ rodinyje spustelėkite **„Your Trust Circles“** (jūsų patikimi ratai), dukart spustelėkite arba dukart bakstelėkite esamą patikimą ratą, kad būtų parodyti dabartiniai nariai, spustelėkite arba bakstelėkite **M+** piktogramą, esančią šalia **„Members“** (nariai) ir tada vykdykite ekrane pateikiamus nurodymus.

- Jei naudojatės „Outlook“, iš „Outlook“ adresų knygos pasirinkite adresatus ir tada spustelėkite **Gerai**.
- Jei naudojatės kita el. pašto paslauga, naujus el. pašto adresus į „Trust Circle“ įtraukite rankiniu būdu arba galite juos nuskaityti iš el. pašto adreso, užregistruoto „Trust Circle“ programoje.

Failų įtraukimas į patikimą ratą

Failus į patikimą ratą galite įtraukti vienu iš toliau pateiktų būdų:

- Nukopijuokite arba perkelkite failą į esamą patikimo rato aplanką.

  – arba –

- „Windows“ naršyklėje dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite failą, kuris šiuo metu nėra užšifruotas, pasirinkite **„Trust Circle“** ir tada pasirinkite **„Encrypt“** (šifruoti). Jūs būsite paraginti pasirinkti patikimą ratą, į kurį turėtų būti įtraukiamas failas.

PATARIMAS: galite pasirinkti vieną ar kelis failus.

Užšifruoti aplankai

Bet kuris patikimo rato narys gali peržiūrėti ir redaguoti tam patikimam ratui priklausančius failus.

PASTABA: „Trust Circle Manager“ / „Trust Circle Reader“ failų tarp narių nesinchronizuoja.

Failus reikia bendrinti galimais būdais, pvz., el. paštu, ftp ar debesies saugyklos paslauga. Failai, kopijuojami į patikimo rato aplanką ar jame sukurti, yra iš karto apsaugoti.

Aplankų šalinimas iš patikimo rato

Jei aplankas pašalintas iš patikimo rato, aplankas ir visas jo turinys yra iškoduojamas bei pašalinama šių elementų apsauga.

- „Trust Circle“ rodinyje spustelėkite arba bakstelėkite **„Your Trust Circles“** (jūsų patikimi ratai), dukart spustelėkite arba dukart bakstelėkite esamą patikimą ratą, kad būtų parodyti dabartiniai aplankai ir tada spustelėkite arba bakstelėkite **šiukšlinės** piktogramą, esančią šalia to aplanko.

  – arba –

- „Windows“ naršyklėje dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite aplanką, kuris šiuo metu yra įtrauktas į patikimą ratą, pasirinkite **„Trust Circle“** ir tada pasirinkite **„Remove from Trust Circle“** (šalinti iš „Trust Circle“).

PATARIMAS: galite pasirinkti vieną ar kelis aplankus.

Failo šalinimas iš patikimo rato

Norėdami iš patikimo rato pašalinti failą, „Windows“ naršyklėje dešiniuoju pelės klavišu spustelėkite arba bakstelėkite ir palaikykite failą, kuris šiuo metu nėra užšifruotas, pasirinkite **„Trust Circle“** ir tada pasirinkite **„Decrypt File“** (iškoduoti failą).

Narių šalinimas iš patikimo rato

Nario, kuris buvo galutinai įtrauktas, negalima pašalinti iš patikimo rato. Kita galimybė būtų sukurti naują patikimą ratą, kuriam priklausytų visi kiti nariai, visus failus ir aplankus perkelti į naują patikimą ratą ir tada ištrinti senąjį patikimą ratą. Taip bus užtikrinta, kad naujai gauti failai šiam nariui bus nepasiekiami, tačiau failai, kurie buvo bendrinti anksčiau, ir toliau bus pasiekiami senojo patikimo rato nariui.

Jei narys galutinai įtrauktas nėra (narys buvo pakviestas prisijungti prie patikimo rato arba pakvietimo prisijungti prie patikimo rato nepriėmė), jį iš patikimo rato pašalinti galite vienu iš toliau pateiktų būdų:

- „Trust Circle“ rodinyje spustelėkite arba bakstelėkite **„Your Trust Circles“** (jūsų patikimi ratai) ir tada dukart spustelėkite arba dukart bakstelėkite patikimą ratą, kad būtų parodytas esamų narių sąrašas. Spustelėkite arba bakstelėkite **šiukšlinės** piktogramą, esančią šalia nario, kurį norite pašalinti, vardo.
- „Trust Circle“ rodinyje spustelėkite arba bakstelėkite **„Members“** (nariai) ir tada dukart spustelėkite arba dukart bakstelėkite narį, kad būtų parodyti patikimi ratai, kuriems tas narys priklauso. Spustelėkite arba bakstelėkite **šiukšlinės** piktogramą, esančią šalia patikimo rato ir taip pašalinkite narį iš to patikimo rato.

Patikimo rato ištrynimas

Norint ištrinti patikimą ratą, reikia turėti jo nuosavybę.

▲ „Trust Circle“ rodinyje spustelėkite arba bakstelėkite **„Your Trust Circles“** (jūsų patikimi ratai) ir tada spustelėkite arba bakstelėkite **šiukšlinės** piktogramą, esančią šalia patikimo rato, kurį norite ištrinti.

Taip patikimas ratas bus pašalintas iš puslapio ir visiems patikimo rato nariams bus išsiųsti el. laiškai informuojantys, jog patikimas ratas yra ištrintas. Visi tame patikimame rate buvę failai ir aplankai yra iškoduojami.

Nuostatų nustatymas

„Trust Circle“ rodinyje spustelėkite arba bakstelėkite **Nuostatos**. Parodomi trys skirtukai

- **El. pašto nustatymai**

Parinktis	Aprašas
Vartotojo vardas	Rodomas šiuo metu naudojamas vartotojo vardas. Norėdami jį pakeisti, teksto langelyje įveskite naują vartotojo vardą. Pakeitimai išsaugojami automatiškai.
El. pašto adresas	Rodomas šiuo metu naudojamas el. pašto abonementas. Norėdami jį pakeisti, spustelėkite arba bakstelėkite **„Change Email Settings“** (keisti el. pašto nustatymus) ir tada vykdykite ekrane pateikiamus nurodymus.
Naujo nario patvirtinimas	Pasirinkite iš toliau pateiktų parinkčių: ◦ **„Confirm Automatically“** (patvirtinti automatiškai) – gavus pakviestojo (-ųjų) pakvietimo priėmimą, jų patikimame rate rankiniu būdu patvirtinti nebereikia ir pakviestajam (-iesiems) bus išsiunčiamas patvirtinantis el. laiškas. ◦ **„Confirm Manually“** (patvirtinti rankiniu būdu) – gavus pakviestojo (-ųjų) pakvietimo priėmimą, reikia rankiniu būdu naujus narius įtraukti į patikimą ratą ir tik tada pakviestajam (-iesiems) bus išsiunčiamas patvirtinantis el. laiškas. ◦ **„Require Verifiction“** (reikalingas patvirtinimas) – gavus pakviestojo (-ųjų) pakvietimo priėmimą, reikia panaudoti patvirtinimo kodą, kad pakviestasis (-ieji) būtų galutinai įtraukti. Patikimo rato savininkas turi susisiekti su pakviestuoju (-aisiais) ir iš jų sužinoti patvirtinimo kodą. Įvedus teisingą kodą bus išsiunčiami patvirtinamieji el. laiškai.
Periodiškas autentifikavimas	Periodiškas autentifikavimas, praėjus skirtajam laikui (skaičiuojamas minutėmis), o taip pat vykdant slaptą operaciją, vartotojui nurodo įvesti „Windows“ slaptažodį. Ši nuostata vartotojams suteikia galimybę autentifikavimą įjungti ir išjungti.
Skirtasis autentifikavimo laikas	Prieš pradedant autentifikavimą reikia pasirinkti konkretų skirtąjį laiką (skaičiuojamas minutėmis).
Nerodyti patvirtinimo pranešimo	Pasirinkite žymės langelį, kad išjungtumėte patvirtinimo pranešimų rodymą arba išvalykite žymės langelį, kad patvirtinimo pranešimai būtų rodomi.
Norėčiau padėti tobulinti „HP Trust Circle“ naudojant anonimiško naudojimo stebėjimą	Pasirinkite žymės langelį, kad dalyvautumėte programoje arba išvalykite žymės langelį, jei programoje dalyvauti nepageidaujate.

- **Atsarginis kopijavimas / atkūrimas**

Parinktis	Aprašas
Atsarginė kopija	Nukopijuoja jūsų „Trust Circle Manager“ / „Trust Circle Reader“ programų duomenis (nustatymus ir patikimus ratus) į atsarginės kopijos saugojimo failą. Strigties atveju ar sugedus sistemai, galite pasinaudoti šiuo failu ir atkurti savo naują „Trust Circle“ įdiegimą į faile išsaugotą būseną. **PASTABA:** Išsaugomi tik jūsų „Trust Circle“ programos duomenys (patikimi ratai, nustatymai ir nariai). Patčių failų, esančių patikimų ratų aplankuose, atsarginės kopijos nesukuriamos. Šių failų atsarginės kopijos turėtų būti sukurtos atskirai. Norėdami sukurti atsarginę nustatymų ir vartotojo duomenų kopiją: **1.** Spustelėkite arba bakstelėkite **„Backup“** (atsarginė kopija). **2.** Pasirinkite atsarginės kopijos saugojimo failo pavadinimą ir katalogą ir tada spustelėkite arba bakstelėkite **Įrašyti**. **3.** Įveskite slaptažodį, jį patvirtinkite ir tada spustelėkite arba bakstelėkite **Gerai**. Šis slaptažodis bus reikalingas norint šį failą atkurti.
Atkūrimas	Iš atsarginės kopijos saugojimo failo atkuria nustatymus ir patikimus ratus, dažniausiai po įvykusios sistemos strigties ar perkėlimo į kitą kompiuterį. Norėdami atkurti „Trust Circle Manager“ nustatymus ir vartotojo duomenis: **1.** Spustelėkite arba bakstelėkite **Atkurti**. **2.** Nueikite į atsarginės kopijos saugojimo failo katalogą ir failo pavadinimą ir tada spustelėkite arba bakstelėkite **Atidaryti**. **3.** Įveskite slaptažodį, kuris buvo naudojamas kuriant atsarginę kopiją.

- **Apie** – rodoma „Trust Circle Manager“ / „Trust Circle Reader“ programinės įrangos versija. Pateikiami saitai leidžiantys „Trust Circle Manager“ programą atnaujinti į „Pro“ versiją arba parodantys HP privatumo deklaraciją.

9 „Theft Recovery“ (tik tam tikruose modeliuose)

Naudodami „Computrace“ (įsigyjama atskirai) nuotoliniu būdu galite stebėti, valdyti ir sekti savo kompiuterį.

Suaktyvinus, „Computrace“ priemonė sukonfigūruojama „Absolute Software“ klientų aptarnavimo centre. Klientų aptarnavimo centre administratoriai gali sukonfigūruoti „Computrace“ priemonę, kad ši stebėtų arba valdytų kompiuterį. Jei sistema būtų pamesta arba pavogta, klientų aptarnavimo centras gali vietos valdžios organams padėti nustatyti kompiuterio buvimo vietą ir jį grąžinti jums. Sukonfigūravus „Computrace“, ši priemonė veiks net ir tada, kai standusis diskas bus ištrintas arba išimtas.

Norėdami suaktyvinti „Computrace“:

1. Prisijungkite prie interneto.
2. Atidarykite „HP Client Security“. Daugiau informacijos rasite skyriuje „„HP Client Security“ atidarymas“ 9 puslapyje.
3. Spustelėkite **„Theft Recovery“**.
4. Norėdami paleisti „Computrace“ aktyvinimo vedlį, spustelėkite **Darbo pradžia**.
5. Įveskite savo kontaktinius duomenis ir kreditinės kortelės mokėjimo informaciją arba įveskite iš anksto įsigytą produkto kodą.

Aktyvinimo vedlys saugiai apdoros pirkimo operaciją ir nustatys jūsų vartotojo abonementą „Absolute Software“ klientų aptarnavimo centro žiniatinklio svetainėje. Kai procesą užbaigsite, gausite patvirtinamąjį el. laišką, kuriame nurodyta klientų aptarnavimo centro abonemento informacija.

Jei esate anksčiau paleidę „Computrace“ aktyvinimo vedlį ir jums jau yra sukurtas klientų aptarnavimo centro abonementas, susisiekdami su HP abonemento atstovu galėsite įsigyti papildomas licencijas.

Norėdami prisijungti prie klientų aptarnavimo centro:

1. Eikite į https://cc.absolute.com/.
2. Į **prisijungimo ID** ir **slaptažodžio** laukelius įveskite jums el. laišku atsiųstus kredencialus ir spustelėkite **Prisijungti**.

Naudodamiesi klientų aptarnavimo centru galėsite:

- Stebėti savo kompiuterius.
- Apsaugoti savo tolimuosius duomenis.
- Pranešti apie bet kurį pavogtą ir „Computrace“ apsaugotą kompiuterį.

▲ Spustelėkite **Sužinokite daugiau**, jei norite gauti daugiau informacijos apie „Computrace“.

10 Lokalizuoto slaptažodžio išimtys

Slaptažodžio lokalizavimo palaikymas „Power–on authentication“ (autentifikavimas įjungus) ir „HP Drive Encryption“ lygmenyje yra ribotas. Daugiau informacijos rasite skyriuje „„Windows“ IME nepalaikoma „Power–on authentication“ (autentifikavimas įjungus) ir „Drive Encryption“ lygmenyje.“ 56 puslapyje.

Ką daryti, jei slaptažodis atmestas

Slaptažodis gali būti atmetamas dėl šių priežasčių:

- Vartotojas naudoja nepalaikomą IME. Tai dažnai atsitinka su dviejų baitų kalbomis (korėjiečių, japonų, kinų). Kad išspręstumėte šią problemą:
  1. Naudodami **Valdymo skydą** įtraukite palaikomą klaviatūros išdėstymą (įtraukite JAV / angliška klaviatūra kinų kalbos įvesties parinktyje).
  2. Palaikomą klaviatūrą nustatykite numatytajai įvesčiai.
  3. Paleiskite „HP Client Security“ ir tada įveskite „Windows“ slaptažodį.
- Vartotojas naudoja nepalaikomus simbolius. Kad išspręstumėte šią problemą:
  1. Pakeiskite „Windows“ slaptažodį, kad jame būtų tik palaikomi simboliai. Norėdami gauti daugiau informacijos apie nepalaikomus simbolius, žr. „Specialių klavišų tvarkymas“ 57 puslapyje“.
  2. Paleiskite „HP Client Security“ ir tada įveskite „Windows“ slaptažodį.

„Windows“ IME nepalaikoma „Power–on authentication“ (autentifikavimas įjungus) ir „Drive Encryption“ lygmenyje.

„Windows“ sistemoje vartotojas gali pasirinkti IME (įvesties būdo rengyklę) įvesti sudėtingiems ženklams ir simboliams, pvz., japonų ar kinų kalbos simboliams, naudojant standartinę vakarietišką klaviatūrą.

IME nepalaikoma „Power–on authentication“ (autentifikavimas įjungus) ir „Drive Encryption“ lygmenyje. „Windows“ slaptažodžio negalima įvesti IME naudojant „Power–on authentication“ (autentifikavimas įjungus) ir „HP Drive Encryption“ prisijungimo ekraną, o tai vis tiek padarius gali būti užblokuojama. Kai kuriais atvejais „Microsoft® Windows“ vartotojui įvedant slaptažodį IME neparodo.

Tuomet reikėtų įjungti vieną iš toliau pateiktų palaikomų klaviatūros išdėstymų, kurį galima konvertuoti į 00000411 klaviatūros išdėstymą:

- „Microsoft“ IME japonų kalbai.
- Japonų kalbos klaviatūros išdėstymas.
- „Office 2007“ IME japonų kalbai – jei „Microsoft“ arba trečioji šalis naudoja terminą „IME“ arba „įvesties būdo rengyklė“, įvesties būdas iš tikrųjų gali būti ne IME. Gali kilti painiava, tačiau programinė įranga nuskaito šešioliktainį kodo simbolį. Todėl, jei IME nurodo palaikomos klaviatūros išdėstymą, tuomet „HP Client Security“ konfigūraciją gali palaikyti.

PERSPĖJIMAS! kai „HP Client Security“ programa yra diegiama, slaptažodžiai, įvesti naudojant „Windows“ IME, bus atmesti.

Slaptažodžio keitimas naudojant klaviatūros išdėstymą, kuris taip pat palaikomas

Jei slaptažodis iš pradžių nustatytas naudojant vienokį klaviatūros išdėstymą, pvz., JAV anglų k. (409), o po to vartotojas slaptažodį pakeičia naudodamas kitokį klaviatūros išdėstymą, kuris yra taip pat palaikomas, pvz., Lotynų Amerikos (080A), slaptažodis veiks „HP Drive Encryption“ programoje, tačiau neveiks BIOS, jei vartotojas naudos simbolius, kurie egzistuoja antrosios klaviatūros išdėstyme, tačiau neegzistuoja pirmosios (pvz., ē).

PASTABA: administratoriai šią problemą gali išspręsti „HP Client Security“ vartotojų puslapyje (pasiekiamas per **„Gear“** piktogramą, esančią pagrindiniame puslapyje) pašalindami vartotoją iš „HP Client Security“, operacinėje sistemoje pasirinkdami pageidaujamą klaviatūros išdėstymą ir tam pačiam vartotojui iš naujo paleisdami „HP Client Security“ sąrankos vedlį. BIOS pageidaujamą klaviatūros išdėstymą įsimena ir slaptažodžiai, kuriuos galima įvesti šiuo klaviatūros išdėstymu, bus tinkamai nustatyti BIOS.

Kita galima problema yra ta, kad naudojami skirtingi klaviatūros išdėstymai ir jais galima surinkti tuos pačius simbolius. Pavyzdžiui, JAV tarptautinis klaviatūros išdėstymas (20409) ir Lotynų Amerikos klaviatūros išdėstymas (080A) turi simbolį „é“, nors gali reikėti naudoti skirtingą klavišų seką. Jei slaptažodis iš pradžių nustatytas naudojant Lotynų Amerikos klaviatūros išdėstymą, o po to Lotynų Amerikos klaviatūros išdėstymas yra nustatomas BIOS, net ir tada, kai slaptažodis vėliau buvo pakeistas naudojant JAV tarptautinį klaviatūros išdėstymą.

Specialių klavišų tvarkymas

- Kinų, slovakų, Kanados prancūzų ir čekų kalbos

  Kai vartotojas pasirenka vieną iš anksčiau nurodytų klaviatūros išdėstymų ir tada įveda slaptažodį (pvz., abcdef), tas pats slaptažodis turi būti įvedamas nuspaudus shift klavišą, jei įvedamos mažosios raidės ir shift klavišą kartu su caps lock klavišu, jei įvedamos didžiosios raidės „Power–on authentication“ (autentifikavimas įjungus) ir „HP Drive Encryption“ programoje. Skaitinis slaptažodis turi būti įvedamas naudojant skaitmenų klaviatūrą.

- Korėjiečių kalba

  Kai vartotojas pasirenka palaikomą korėjiečių kalbos klaviatūros išdėstymą ir tada įveda slaptažodį, tas pats slaptažodis turi būti įvedamas nuspaudus dešinįjį alt klavišą, jei įvedamos mažosios raidės ir dešinįjį alt klavišą kartu su caps lock klavišu, jei įvedamos didžiosios raidės „Power–on authentication“ (autentifikavimas įjungus) ir „HP Drive Encryption“ programoje

- Nepalaikomi simboliai yra nurodyti šioje lentelėje:

Language (Kalba)	„Windows“	BIOS	„Drive Encryption“
Arabų kalba	ﻻ ,ﻷ ir ﻹ klavišai sukuria du simbolius.	ﻻ ,ﻷ ir ﻹ klavišai sukuria vieną simbolį.	ﻻ ,ﻷ ir ﻹ klavišai sukuria vieną simbolį.
Kanados prancūzų kalba	ç, è, à ir é kartu su caps lock yra Ç, È, À ir É „Windows“ operacinėje sistemoje.	ç, è, à ir é kartu su caps lock yra ç, è, à ir é naudojant autentifikavimą įjungus.	ç, è, à ir é kartu su caps lock yra ç, è, à ir é „HP Drive Encryption“ priemonėje.

Language (Kalba)	„Windows“	BIOS	„Drive Encryption“
Ispanų kalba	40a nepalaikoma. Tačiau vis tiek veikia, kadangi programinė įranga konvertuoja į c0a. Tačiau dėl vos pastebimo skirtumo tarp klaviatūros išdėstymų, ispaniškai kalbantiems vartotojams rekomenduojama savo „Windows“ klaviatūros išdėstymą pasikeisti į 1040a (ispanų kalbos variantas) arba 080a (Lotynų Amerikos variantas).	netaikoma	netaikoma
JAV tarptautinis	◦ ¡, ¤, ‘, ’, ¥ ir × klavišai viršutinėje eilėje atmetami. ◦ å, ® ir Þ klavišai antroje eilėje atmetami. ◦ á, ð ir ø klavišai trečioje eilėje atmetami. ◦ æ klavišas apatinėje eilėje atmetamas.	netaikoma	netaikoma
Čekų kalba	◦ ğ klavišas atmetamas. ◦ į klavišas atmetamas. ◦ ų klavišas atmetamas. ◦ ė, ı ir ż klavišai atmetami. ◦ ġ, ķ, ļ, ņ ir ţ klavišai atmetami.	netaikoma	netaikoma
Slovakų kalba	ż klavišas atmetamas.	◦ š, ś ir ş klavišai juos spaudžiant atmetami, tačiau priimami, kai renkami programine klaviatūra. ◦ ţ kombinacinis klavišas sukuria du simbolius.	netaikoma
Vengrų kalba	ż klavišas atmetamas.	ţ klavišas sukuria du simbolius.	netaikoma
Slovėnų kalba	żŻ klavišas atmetamas „Windows“ sistemoje, o alt klavišas sukuria kombinacinį klavišą BIOS.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š ir Š klavišai atmetami BIOS.	netaikoma
Japonų kalba	Jei įmanoma, geriau naudoti „Microsoft Office 2007“ IME. Nepaisant IME pavadinimo, iš tikrųjų tai yra 411 klaviatūros išdėstymas, kuris yra palaikomas.	netaikoma	netaikoma

Žodynėlis

administratorius
Žr. *„Windows“ administratorius*.

aktyvinimas
Užduotis, kurią reikia atlikti, kad būtų galimos „Drive Encryption“ funkcijos. Administratoriai „Drive Encryption“ suaktyvinti gali naudodamiesi „HP Client Security“ sąrankos vedliu arba „HP Client Security“ priemone. Į aktyvinimą įeina programinės įrangos aktyvinimas, disko įrenginio šifravimas ir pirminio šifravimo rakto atsarginės kopijos kūrimas keičiamųjų laikmenų įrenginyje.

aparatūros šifravimas
Užsišifruojančių diskų įrenginių, atitinkančių „Trusted Computing Group“ grupės OPAL specifikacijas, keliamas užsišifruojančių diskų įrenginių valdymui, naudojimas atliekant momentinį šifravimą. Aparatūros šifravimas atliekamas akimirksniu ir gali užtrukti tik keletą minučių, tačiau programinės įrangos šifravimas gali užtrukti keletą valandų.

atkūrimas
Programos informacijos kopijavimas iš anksčiau išsaugoto atsarginės kopijos saugojimo failo į šią programą.

atsarginė kopija
Atsarginio kopijavimo funkcijos naudojimas išsaugojant svarbią programos informaciją į vietą, kuri nėra toje pačioje programoje. Vėliau ši funkcija gali būti naudojama atkuriant šią informaciją tame pačiame arba kitame kompiuteryje.

autentifikavimas
Procesas, kurio metu naudojant kredencialus, įskaitant jūsų „Windows“ slaptažodį, jūsų piršto atspaudą, lustinę kortelę, bekontaktę kortelę ar judesio kortelę, patvirtinama, jog esate nurodytas asmuo.

autentifikavimas įjungus
Saugos priemonė, kuri reikalauja autentifikavimo kokiu nors būdu, pvz., lustine kortele, apsaugos lustu arba slaptažodžiu, kai kompiuteris yra įjungiamas.

automatinis naikinimas
Naikinimas,kurį jūs suplanuojate „File Sanitizer“ priemone.

avarinio atkūrimo archyvas
Apsaugotoji saugojimo vieta leidžianti atlikti pakartotinį bazinio vartotojo raktų šifravimą iš vieno platformos savininko rakto į kitą.

bekontaktė kortelė
Plastmasinė kortelė su kompiuterio lustu, kurią galima naudoti autentifikuojant.

domenas
Grupė kompiuterių, kurie priklauso tinklui ir naudoja bendrą katalogo duomenų bazę. Domenams priskirti unikalūs pavadinimai ir kiekvienam iš jų taikomos įprastinės taisyklės ir procedūros.

grupė
Vartotojų grupė, kurios vartotojams suteikta arba uždrausta tokio pačio lygio prieiga prie įrenginių klasės arba konkretaus įrenginio.

ID kortelė
„Windows“ darbalaukio įtaisas, kuris vizualiai identifikuoja jūsų darbalaukį su jūsų vartotojo vardu ir pasirinktu paveikslėliu.

iškodavimas

Procedūra, naudojama kriptografijoje užšifruotus duomenis konvertuojant į grynąjį tekstą.

išteklius
Duomenų komponentas susidedantis iš asmeninės informacijos arba failų, retrospektyvinių ar su tinklalapiais susijusių duomenų ir t.t., ir kuris randamas standžiajame diske.

įrenginio klasė
Visi tam tikro tipo įrenginiai, tokie kaip diskų įrenginiai.

įrenginio prieigos kontrolės politika
Įrenginių sąrašas, kurio prieiga vartotojui suteikta arba uždrausta.

judesio kortelė
Plastmasinė kortelė su kompiuterio lustu, kurią kartu su kitais kredencialais galima naudoti autentifikuojant ir taip pagerinti saugą.

kredencialas
Konkreti informacija arba aparatūros įrenginys, kuris naudojamas autentifikuoti atskirą vartotoją.

laisvos vietos tuštinimas
Atsitiktinių duomenų įrašymas į ištrintų išteklių vietą ir nepanaudotą vietą. Šis procesas mažina ištrintus išteklius ir dėl to originalių išteklių yra sunkiau atkurti.

lustinė kortelė
Aparatūros įrenginys, kurį galima naudoti kartu su PIN autentifikuojant.

naikinimas
Algoritmo, kuris ištekliaus duomenis perrašo nereikšmingais duomenimis, vykdymas.

naikinimas rankiniu būdu
Tiesioginis ištekliaus ar pasirinktų išteklių naikinimas apeinantis suplanuotą naikinimą.

Pagrindinis puslapis
Centrinė vieta, kurioje galite pasiekti ir valdyti „HP Client Security“ programos funkcijas ir nustatymus.

perkrovimas
Procesas, kurio metu kompiuteris paleidžiamas iš naujo.

PIN
Asmeninis identifikacijos numeris suteikiamas įtrauktam vartotojui ir naudojamas autentifikuojant.

piršto atspaudas
Skaitmeninis jūsų piršto atspaudo vaizdo išgavimas. Jūsų tikrasis piršto atspaudas „HP Client Security“ programoje niekada neišsaugojamas.

PKI
Viešojo rakto infrastruktūros standartas, kuris apibūdina sertifikatų ir kriptografijos raktų kūrimo, naudojimo ir administravimo sąsajas.

prijungti įrenginiai
Aparatūros įrenginys, kuris yra prijungtas prie kompiuterio prievado.

prisijungimas
„HP Client Security“ programos objektas, susidedantis iš vartotojo vardo ir slaptažodžio (galimas daiktas ir kitos tam tikros informacijos) ir kuris gali būti naudojamas prisijungiant prie tinklalapių ar kitų programų.

programinės įrangos šifravimas
Programinės įrangos naudojimas užšifruoti standžiųjų diskų sektoriams. Šis procesas yra lėtesnis nei aparatūros šifravimas

saugaus prisijungimo būdas
Būdas, kuriuo prisijungiama prie kompiuterio.

šifravimas
Procedūra, pvz., algoritmo, taikomo kriptografijoje grynąjį tekstą konvertuojant į šifruotą tekstą, kad tų užšifruotų duomenų negalėtų nuskaityti nesankcionuoti gavėjai, naudojimas. Yra daug duomenų šifravimo tipų ir jie sudaro tinklo saugos pagrindą. Dažniausiai naudojami tipai apima standartinį duomenų šifravimą ir viešo rakto šifravimą.

tapatybė
„HP Client Security“ priemonėje – kredencialų ir nustatymų, kurie apdorojami kaip konkretaus vartotojo abonementas arba profilis, grupė.

tinklo abonementas
„Windows“ vartotojo arba administratoriaus abonementas vietiniame kompiuteryje, darbo grupėje arba domene.

vartotojas
Bet kuris asmuo, įtrauktas į „Drive Encryption“. Vartotojų ne administratorių teisės naudojantis „Drive Encryption“ yra ribotos. Jie gali tik užsiregistruoti (patvirtinus administratoriui) ir prisijungti.

Vienintelė registracija
Funkcija, kuri saugo autentifikavimo informaciją ir leidžia naudotis „HP Client Security“ priemone norint prisijungti prie interneto ir „Windows“ programų, kurios reikalauja slaptažodžio autentifikavimo.

„Bluetooth“
Technologija, kuri naudoja radijo ryšio perdavimus ir „Bluetooth" funkciją palaikančius kompiuterius, spausdintuvus, peles, mobiliuosius telefonus ir kitus įrenginius įgalina mažu atstumu naudoti belaidį ryšį.

„Drive Encryption“
Apsaugo jūsų duomenis užšifruojant standųjį diską (-us) ir informaciją paverčiant nenuskaitoma asmenims, kuriems nesuteikta tinkama prieiga.

„Drive Encryption“ autentifikavimas prieš įkraunant sistemą
Prisijungimo ekranas, kuris rodomas prieš paleidžiant „Windows“. Vartotojai turi įvesti arba „Windows“ vartotojo vardą, arba savo slaptažodį, arba lustinės kortelės PIN, arba perbraukti registruotas pirštu. Jei pasirinktas prisijungimas vienu veiksmu, tuomet „Drive Encryption“ prisijungimo ekrane įvedus teisingą informaciją galima iš karto paleisti „Windows“ sistemą, nes dar kartą prisijungti „Windows“ prisijungimo ekrane nebereikia.

„Drive Encryption“ prisijungimo ekranas
Žr. „Drive Encryption“ autentifikavimas prieš įkraunant sistemą.

„DriveLock“
Saugos priemonė, kuri standųjį diską susieja su vartotoju ir reikalauja, kad vartotojas teisingai įvestų „DriveLock“ slaptažodį, kai kompiuteris yra įjungiamas.

„Encryption File System“ (EFS)
Sistema, kuri užšifruoja visus failus ir poaplankius pasirinktame aplanke.

„HP SpareKey“ atkūrimas
Galimybė naudotis kompiuteriu teisingai atsakius saugos klausimus.

„Just In Time Authentification“
Žr. „HP Device Access Manager“ programinės įrangos žinyną.

„Trust Circle“
Pateikia sudėtinių elementų duomenis siejant duomenis su nurodyta patikimų vartotojų grupe. Tai apsaugo duomenis, kad jie atsitiktinai ar tyčia nepatektų į netinkamas rankas. Apsaugoti „CryptoMill’s Zero Overhead Key Management“ technologijų, duomenys yra kriptografiškai susieti su patikimu ratu. Tai apsaugo nuo galimo dokumentų ar kitos slaptos informacijos iškodavimo už patikimo rato ribų

„Trust Circle“ aplankas
Bet kuris patikimo rato apsaugotas aplankas.

„Trust Circle Manager“ / „Trust Circle Reader“

„Trust Circle Reader“ programa gali priimti pakvietimus išsiųstus tik iš „Trust Circle Manager“ vartotojų. Tačiau „Trust Circle Manager“ leidžia patikimų ratų kūrimą. Viena iš funkcijų yra asmens pakvietimas prisijungti prie patikimo rato ir pakvietimų iš kitų asmenų priėmimas naudojantis el. paštu. Kai tarp lygiaverčių vartotojų sukuriamas patikimą ratas, failus, kurie to patikimo rato yra apsaugoti, galima saugiai bendrinti.

„Trusted Platform Module“ (TPM) integruotos saugos lustas
TPM priemonė, saugodama pagrindiniam kompiuteriui būdingą informaciją, pvz., šifravimo raktą, skaitmeninius sertifikatus ir slaptažodžius, autentifikuoja kompiuterį, o ne vartotoją. TPM priemonės dėka mažėja rizika, kad kompiuteryje esanti informacija bus pažeista, ją fiziškai pavogus ar programišiui įsilaužus į kompiuterį.

„Windows“ administratorius
Vartotojas turintis visas teises modifikuoti leidimus ir valdyti kitus vartotojus.

„Windows“ vartotojo abonementas
Vartotojas, kuris yra įgaliotas prisijungti prie tinklo ar atskiro kompiuterio.

„Windows Logon Security“ („Windows“ prisijungimo sauga)
Apsaugo jūsų „Windows“ abonementą (- us), kadangi prieiga suteikiama tik pateikus konkrečius kredencialus.

Rodyklė