# HP Client Security

## Darba sākšana

Pirmais izdevums: 2013. gada augustā

Dokumenta daļas numurs: 735339-E11

# Saturs

# 1 Par programmatūru HP Client Security Manager

HP Client Security ļauj aizsargāt datus, ierīci un identitāti, tādējādi palielinot datora drošību.

Datoram pieejamie programmatūras moduļi var atšķirties atkarībā no datora modeļa.

HP Client Security programmatūras moduļi var būt iepriekš instalēti, iepriekš ielādēti vai lejupielādējami no HP vietnes. Papildinformāciju skatiet sadaļā http://www.hp.com

**PIEZĪME.** Norādījumi šajā rokasgrāmatā ir doti, pieņemot, ka jau ir instalēti atbilstošie HP Client Security programmatūras moduļi.

## HP Client Security līdzekļi

Šajā tabulā ir uzskaitītas HP Client Security moduļu galvenās funkcijas.

| Modulis | Galvenās funkcijas |
|---|---|
| HP Client Security Manager | Administratori var veikt tālāk minētās funkcijas:<br>• Aizsargāt datoru pirms Windows® palaišanas<br>• Aizsargāt Windows kontu, izmantojot stipru autentifikāciju<br>• Pārvaldīt pieteikšanos un paroles tīmekļa vietnēm un lietojumprogrammām<br>• Vienkārši mainīt Windows operētājsistēmas paroli<br>• Lietot pirkstu nospiedumus papildu drošībai un ērtībām<br>• Iestatīt viedkarti, bezkontakta karti vai karti ar mikroshēmu autentifikācijas veikšanai<br>• Lietot Bluetooth tālruni kā identifikācijas metodi<br>• Iestatīt PIN kodu autentifikācijas izvēles iespēju paplašināšanai<br>• Konfigurēt pieteikšanās un sesijas politikas<br>• Dublēt un atjaunot programmas datus<br>• Pievienot vēl citas lietojumprogrammas, tādas kā HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager un HP Computrace<br>Parasti lietotāji var veikt tālāk minētās funkcijas:<br>• Skatīt šifrēšanas statusa un Device Access Manager iestatījumus.<br>• Aktivizēt CompuTrace.<br>• Konfigurēt preferenču un dublēšanas un atjaunošanas opcijas. |

| Modulis | Galvenās funkcijas |
|---|---|
| Password Manager | Parasti lietotāji var veikt tālāk minētās funkcijas:<br>• Organizēt un iestatīt lietotājvārdus un paroles.<br>• Izveidot spēcīgas paroles uzlabotai konta drošībai e-pasta un tīmekļa kontiem. Password Manager ieraksta un nosūta informāciju automātiski.<br>• Racionalizēt pieteikšanās procesu ar vienotās pierakstīšanās funkciju, kura automātiski atceras un lieto lietotāja akreditācijas datus.<br>• Atzīmēt kontu kā apdraudētu, lai saņemtu brīdinājumu par citu(-iem) kontu(-iem) ar līdzīgiem akreditācijas datiem.<br>• Importēt pieteikšanās datus no atbalstīta pārlūka. |
| HP Drive Encryption (tikai atsevišķiem modeļiem) | • Nodrošina pilnīgu, pilna apjoma cietā diska šifrēšanu.<br>• Liek izmantot pirmsāknēšanas autentifikāciju datu atšifrēšanai un piekļuvei datiem.<br>• Piedāvā iespēju aktivizēt paššifrējošos diskus (tikai atsevišķiem modeļiem). |
| HP Device Access Manager | • Ļauj IT sistēmu pārvaldniekiem kontrolēt piekļuvi ierīcēm, pamatojoties uz lietotāju profiliem.<br>• Neļauj nesankcionētiem lietotājiem iegūt datus, ierakstot tos ārējās atmiņas ierīcēs, un inficēt sistēmu ar vīrusiem no ārējiem datu nesējiem.<br>• Ļauj administratoriem atspējot konkrētu personu vai lietotāju grupu piekļuvi sakaru ierīcēm. |
| HP Trust Circles | • Garantē failu un dokumentu drošību.<br>• Šifrē failus, kuri ievietoti lietotāja norādītajās mapēs, un aizsargā tos uzticamajā lietotāju lokā.<br>• Ļauj failus lietot un kopīgot tikai uzticamā lietotāju loka dalībniekiem. |
| Atgūšana zādzības gadījumā (CompuTrace, iegādājama atsevišķi) | • Lai aktivizētu, nepieciešami atsevišķi iegādāti izsekošanas un trasēšanas abonementi.<br>• Garantē drošu resursu izsekošanu.<br>• Uzrauga lietotāja aktivitāti, kā arī programmaparatūras un programmatūras izmaiņas.<br>• Paliek aktīva pat pēc cietā diska atkārtotas formatēšanas vai nomaiņas. |

# HP Client Security produkta apraksts un parastas lietošanas piemēri

Gandrīz visiem HP Client Security produktiem tiek izmantota gan lietotāja autentifikācija (parasti — parole), gan administratīvais dublējums, lai nodrošinātu piekļuvi pazaudētu, nepieejamu vai aizmirstu paroļu gadījumā vai tad, kad to pieprasa korporatīvās drošības speciālisti.

**PIEZĪME.** Daži no HP Client Security produktiem ir paredzēti tam, lai ierobežotu piekļuvi datiem. Ja dati ir tik svarīgi, ka lietotājs vēlas tos drīzāk zaudēt, nekā pakļaut apdraudējumam, tad dati ir jāšifrē. Ieteicams visus datus dublēt kādā drošā vietā.

## Password Manager

Password Manager saglabā lietotājvārdus un paroles un var tikt izmantots šādiem nolūkiem:

- Saglabāt lietotājvārdus un paroles, lai varētu piekļūt internetam vai e-pastam.
- Nodrošināt automātisku lietotāja pieteikšanos vietnē vai e-pastā.
- Pārvaldīt un organizēt autentifikāciju.
- Atlasīt tīmekļa vai tīkla resursu un tieši piekļūt saitei.
- Kad nepieciešams, apskatīt vārdus un paroles.
- Atzīmēt kontu kā apdraudētu, lai saņemtu brīdinājumu par citu(-iem) kontu(-iem) ar līdzīgiem akreditācijas datiem.
- Importēt pieteikšanās datus no atbalstīta pārlūka.

**1. piemērs.** Kāda liela ražotāja iepirkumu aģente lielāko daļu no korporatīvajiem darījumiem veic interneta tīklā. Viņa arī bieži apmeklē vairākas populāras vietnes, kuras pieprasa pieteikšanās informāciju. Aģentei ir labi zināmi ar drošību saistītie apsvērumi, tādēļ viņa katram no kontiem izmanto citu paroli. Iepirkumu aģente ir nolēmusi izmantot Password Manager, lai tīmekļa saites atbilstoši sakārtotu ar dažādiem lietotājvārdiem un parolēm. Kad viņa atver vietni, lai pieteiktos, Password Manager automātiski ievada akreditācijas datus. Ja viņa vēlas apskatīt lietotājvārdus un paroles, moduli Password Manager var konfigurēt to parādīšanai.

Password Manager var izmantot arī autentifikācijas pārvaldīšanai un organizēšanai. Šis rīks ļaus lietotājam atlasīt vietni vai tīkla resursu un tieši piekļūt saitei. Ja nepieciešams, lietotājs var apskatīt arī lietotājvārdus un paroles.

**2. piemērs.** Kāds centīgs darbinieks ir saņēmis paaugstinājumu un tagad pārvalda visu grāmatvedības nodaļu. Viņa darba grupai ir jāpiesakās ļoti daudzos klientu tīmekļa kontos, un šiem visiem kontiem ir atšķirīgi pieteikšanās dati. Šie pieteikšanās dati ir jākoplieto ar citiem darbiniekiem, tādēļ problēma ir konfidencialitātes saglabāšana. Darbinieks nolemj organizēt visas tīmekļa saites, uzņēmuma lietotājvārdus un paroles modulī Password Manager. Pēc tam viņš nodrošina Password Manager visiem citiem darbiniekiem, lai viņi varētu strādāt ar tīmekļa kontiem un nezinātu lietotos pieteikšanās akreditācijas datus.

## HP Drive Encryption (tikai atsevišķiem modeļiem)

HP Drive Encryption tiek lietots, lai ierobežotu piekļuvi datiem visā datora cietajā diskā vai sekundārajā diskā. Drive Encryption var pārvaldīt arī paššifrējošos diskus.

**1. piemērs.** Ārsts vēlas nodrošināt, lai tikai viņš pats varētu piekļūt datiem sava datora cietajā diskā. Ārsts aktivizē Drive Encryption, kas pirms pieteikšanās Windows pieprasa pirmsāknēšanas autentifikāciju. Pēc iestatīšanas cietajam diskam nevar piekļūt bez paroles, kas ievadāma pirms operētājsistēmas palaišanas. Ārsts var vēl vairāk palielināt diska drošību, šifrējot datus, izmantojot paššifrējošā diska opciju.

**2. piemērs.** Slimnīcas administrators vēlas nodrošināt, lai vietējos datoros saglabātajiem datiem var piekļūt tikai ārsti un atbilstoši pilnvarotie darbinieki un lai viņi varētu to izdarīt bez savas personīgās paroles kopīgošanas. IT nodaļas darbinieks pievieno administratoru, ārstus un visus atbilstoši pilnvarotos darbiniekus kā Drive Encryption lietotājus. Tagad tikai pilnvarotie darbinieki var sāknēt datoru vai domēnu, izmantojot savu personīgo lietotājvārdu un paroli.

## HP Device Access Manager (tikai atsevišķiem modeļiem)

HP Device Access Manager ļauj administratoriem ierobežot un pārvaldīt piekļuvi aparatūrai. Device Access Manager var izmantot, lai bloķētu nesankcionētu piekļuvi USB zibatmiņas diskiem, kur var

nokopēt datus. Tas var ierobežot piekļuvi arī CD/DVD diskiem, USB ierīču pārvaldīšanai, tīkla savienojumiem un tamlīdzīgi. Kā piemēru var minēt situāciju, kad ārējiem pakalpojumu sniedzējiem ir nepieciešama piekļuve uzņēmuma datoriem, tomēr jānodrošina, lai viņi nevar nokopēt datus USB diskā.

**1. piemērs.** Medicīnisko materiālu piegādes uzņēmuma vadītājs bieži strādā ar sava uzņēmuma datiem apvienojumā ar dažādiem personīgajiem medicīniskajiem ierakstiem. Darbiniekiem ir nepieciešama piekļuve šiem datiem, tomēr ir ārkārtīgi svarīgi, lai šie dati netiktu izņemti no datora, izmantojot USB disku vai kādu citu ārējo atmiņas ierīci. Tīkls ir drošs, bet datoriem ir CD rakstītāji un USB porti, kuri var ļaut šos datus nokopēt vai nozagt. Vadītājs lieto Device Access Manager USB portu un CD rakstītāju atspējošanai, lai tos nevarētu izmantot. Kaut arī USB porti ir bloķēti, pele un tastatūras turpina darboties.

**2. piemērs.** Apdrošināšanas uzņēmums nevēlas, lai darbinieki instalētu vai ielādētu personīgo programmatūru vai datus, kas atnesti no mājām. Dažiem darbiniekiem ir nepieciešama piekļuve visiem datoru USB portiem. IT sistēmas pārvaldnieks lieto Device Access Manager, lai dažiem darbiniekiem iespējotu piekļuvi un vienlaikus citiem darbiniekiem bloķētu ārējo piekļuvi.

## CompuTrace (iegādājams atsevišķi)

CompuTrace (iegādājams atsevišķi) ir pakalpojums, kas var izsekot nozagtu datoru vienmēr, kad tā lietotājs piekļūst internetam. CompuTrace ļauj arī attāli pārvaldīt un atrast datorus, kā arī uzraudzīt datora lietošanu un lietojumprogrammas.

**1. piemērs.** Skolas direktors ir devis norādījumu IT daļai uzraudzīt visus skolas datorus. Pēc datoru inventarizācijas IT administrators ir reģistrējis visus datorus CompuTrace, lai gadījumā, ka tie kādreiz tiktu nozagti, varētu tos izsekot. Nesen skola konstatēja, ka vairāki datori ir pazuduši, tādēļ IT administrators paziņoja to atbilstošajām varas iestādēm un CompuTrace darbiniekiem. Varas iestādes atrada datorus un nogādāja atpakaļ skolā.

**2. piemērs.** Nekustamā īpašuma uzņēmumam ir jāpārvalda un jāatjaunina datori visā pasaulē. Viņi lieto CompuTrace, lai uzraudzītu un atjauninātu datorus bez nepieciešamības nosūtīt IT darbinieku uz katra datora konkrēto atrašanās vietu.

# Galveno drošības mērķu sasniegšana

HP Client Security moduļus var izmantot vienlaikus, tā nodrošinot risinājumus dažādām drošības problēmām, tostarp šādiem galvenajiem drošības mērķiem:

- Aizsardzība pret mērķtiecīgu zādzību
- Piekļuves ierobežošana sensitīviem datiem
- Ārējas un iekšējas nesankcionētas piekļuves novēršana
- Stipru paroļu politikas izveidošana

## Aizsardzība pret mērķtiecīgu zādzību

Mērķtiecīgas zādzības piemērs varētu būt datora zādzība lidostas drošības kontrolpunktā, kur datorā ir konfidenciāli dati un klientu informācija. Tālāk minētās funkcijas palīdz nodrošināt aizsardzību pret mērķtiecīgu zādzību.

- Ja iespējota pirmssāknēšanas autentifikācija, tā palīdz novērst piekļuvi operētājsistēmai.
  - HP Client Security — skat. HP Client Security 12. lpp..
  - HP Drive Encryption — skat. HP Drive Encryption (tikai atsevišķiem modeļiem) 30. lpp..
- Šifrēšana palīdz nodrošināt to, ka datiem nevar piekļūt pat pēc cietā diska izņemšanas un ievietošanas neaizsargātā sistēmā.
- CompuTrace var izsekot datora atrašanās vietu pēc nozagšanas.
  - CompuTrace — skat. Atgūšana zādzības gadījumā (tikai atsevišķiem modeļiem) 53. lpp..

## Piekļuves ierobežošana sensitīviem datiem

Iedomājieties, ka uzņēmumā strādā kāds nolīgts ārējais auditors, kuram ir nodrošināta piekļuve datorā saglabātajiem sensitīvajiem finanšu datiem. Jūs nevēlaties, lai auditors var izdrukāt vai saglabāt kādā rakstāmā ierīcē (piemēram, CD) šos datus. Šī funkcija palīdz ierobežot piekļuvi datiem:

- HP Device Access Manager ļauj IT sistēmas pārvaldniekiem ierobežot piekļuvi saziņas ierīcēm tā, lai sensitīvos datus nevarētu nokopēt no cietā diska. Skatiet sadaļu Sistēmas skats 43. lpp..

## Ārējas un iekšējas nesankcionētas piekļuves novēršana

Nesankcionēta piekļuve neaizsargātam uzņēmējdarbības vajadzībām izmantojamam datoram rada ļoti lielu risku korporatīvā tīkla resursiem, piemēram, no finanšu dienestiem, vadības, izpētes vai attīstības plāna grupas saņemtajai informācijai un privātajai informācijai, piemēram, pacientu ierakstiem vai personīgajiem finanšu datiem. Šīs funkcijas palīdz novērst nesankcionētu piekļuvi:

- Ja iespējota pirmssāknēšanas autentifikācija, tā palīdz novērst piekļuvi operētājsistēmai. (skatiet HP Drive Encryption (tikai atsevišķiem modeļiem) 30. lpp..
- HP Client Security palīdz nodrošināt to, ka nepilnvarots lietotājs nevar iegūt paroles vai piekļuvi ar paroli aizsargātām lietojumprogrammām. Skatiet sadaļu HP Client Security 12. lpp..
- HP Device Access Manager ļauj IT sistēmas pārvaldniekiem ierobežot piekļuvi rakstāmām ierīcēm tā, lai sensitīvos datus nevarētu nokopēt no cietā diska. Skatiet sadaļu HP Device Access Manager (tikai atsevišķiem modeļiem) 42. lpp..

## Stipru paroļu politikas izveidošana

Ja stājas spēkā uzņēmuma noteikumi, kuri pieprasa stipru paroļu politiku vairākiem dučiem tīmekļa lietojumprogrammu un datubāžu, Password Manager nodrošina aizsargātu paroļu repozitoriju un vienotas pierakstīšanās nodrošinātās ērtības. Skatiet sadaļu Password Manager 18. lpp..

# Papildu drošības elementi

## Drošības lomu piešķiršana

Pārvaldot datora drošību (it īpaši lielās organizācijās) viena no pašām svarīgākajām praksēm ir pienākumu un tiesību sadalīšana starp dažādiem administratoru un lietotāju veidiem.

**PIEZĪME.** Mazā organizācijā vai lietojot datoru personīgajām vajadzībām, visas šīs lomas var pildīt viena un tā pati persona.

Lietojumprogrammai HP Client Security ar drošību saistītos pienākumus un privilēģijas var sadalīt starp šādu lomu pildītājiem:

- Drošības speciālists — nosaka uzņēmuma vai tīkla drošības līmeni un izmantojamos drošības līdzekļus, piemēram, Drive Encryption.

  **PIEZĪME.** Drošības speciālists sadarbībā ar HP var pielāgot daudzas no HP Client Security funkcijām. Papildinformāciju skatiet sadaļā http://www.hp.com

- IT administrators — lieto un pārvalda drošības speciālista noteiktās drošības funkcijas. Var arī iespējot un atspējot dažas funkcijas. Piemēram, ja drošības speciālists ir nolēmis izmantot viedkartes, IT administrators var iespējot gan paroles, gan viedkartes režīmu.
- Lietotājs — lieto drošības funkcijas. Piemēram, ja drošības speciālists un IT administrators ir iespējojuši viedkaršu lietošanu sistēmai, lietotājs var iestatīt viedkartes PIN un lietot šo karti autentifikācijai.

**UZMANĪBU!** Administratori tiek mudināti ievērot „vislabāko darba praksi”, ierobežojot lietotāju privilēģijas un piekļuvi.

Nepilnvarotiem lietotājiem nevajadzētu piešķirt administratora privilēģijas.

## HP Client Security paroļu pārvaldīšana

Gandrīz visas HP Client Security funkcijas ir aizsargātas ar parolēm. Šajā tabulā ir norādītas parasti lietotās paroles, programmatūras modulis, kurā parole tiek iestatīta, un paroles funkcija.

Tajā ir norādītas arī tās paroles, kuras var iestatīt un izmantot tikai IT administratori. Visas citas paroles var iestatīt parastie lietotāji vai administratori.

| HP Client Security parole | Iestatīšanas modulis | Funkcija |
|---|---|---|
| Windows pieteikšanās parole | Windows vadības panelis vai HP Client Security | Var izmantot, lai manuāli pieteiktos un lai veiktu autentifikāciju piekļuvei dažādām HP Client Security funkcijām. |
| HP Client Security dublēšana un paroles atkopšana | HP Client Security, atsevišķiem lietotājiem | Aizsargā piekļuvi HP Client Security dublēšanas un atkopšanas failam. |
| Viedkartes PIN | Credential Manager | Var izmantot kā daudzveidīgu autentifikāciju.<br>Var izmantot kā Windows autentifikāciju.<br>Ja izvēlēta viedkarte, veic Drive Encryption lietotāju autentifikāciju. |

### Drošas paroles izveidošana

Izveidojot paroles, vispirms jāievēro programmas noteiktās specifikācijas. Tomēr, kopumā, lai izveidotu stipras paroles un samazinātu to apdraudējuma iespēju, ievērojiet šādas vadlīnijas:

- Lietojiet paroles, kurās ir vairāk nekā 6 rakstzīmes, vēlams — vairāk nekā 8 rakstzīmes.
- Izmantojiet parolē pārmaiņus gan lielos, gan mazos burtus.
- Ja iespējams, izmantojiet pārmaiņus gan burtus, gan ciparus un iekļaujiet arī īpašās rakstzīmes un pieturzīmes.

- Aizstājiet atslēgvārda burtus ar īpašām rakstzīmēm vai cipariem. Piemēram, varat izmantot ciparu 1 burta I vai L vietā.
- Apvienojiet 2 vai vairāk valodu vārdus.
- Sadaliet vārdu vai frāzi, pa vidu ievietojot ciparus vai īpašās rakstzīmes, piemēram, „Mary2-2Cat45.”
- Neizmantojiet paroli, kuru var atrast vārdnīcā.
- Neizmantojiet parolē savu vārdu vai citu personīgo informāciju, piemēram, dzimšanas datumu, mājdzīvnieku vārdus vai mātes meitas uzvārdu, pat tad, ja to rakstāt ačgārni.
- Regulāri mainiet paroles. Varat mainīt paroli, tai pievienojot tikai vēl dažas rakstzīmes.
- Ja paroli pierakstāt, neglabājiet to redzamā vietā un ļoti tuvu datoram.
- Nesaglabājiet paroli failā, piemēram, e-pastā vai datorā.
- Nekoplietojiet kontus un nevienam nesakiet savu paroli.

## Akreditācijas datu un iestatījumu dublēšana

Jūs varat izmantot dublēšanas un atkopšanas rīku HP Client Security kā centrālo atrašanās vietu, no kuras varat dublēt un atjaunot drošības akreditācijas datus no kāda instalētā HP Client Security moduļa.

# 2 Darba sākšana

Lai konfigurētu HP Client Security lietošanai ar jūsu autentificēšanas datiem, palaidiet HP Client Security vienā no tālāk norādītajiem veidiem. Kad lietotājs ir pabeidzis visas darbības ar vedni, viņš vairs nevar vedni vēlreiz palaist.

1. Sākuma ekrānā vai lietojumprogrammas ekrānā noklikšķiniet uz lietotnes vai pieskarieties lietotnei **HP Client Security** (Windows 8).

   — vai —

   Uz Windows darbvirsmas noklikšķiniet uz vai pieskarieties pie **HP Client Security Gadget** (Windows 7).

   — vai —

   Windows darbvirsmas paziņojumu apgabalā veiciet dubultklikšķi uz vai dubultskārienu pie ikonas **HP Client Security**, kas atrodas uzdevumjoslas labajā pusē.

   — vai —

   Uz Windows darbvirsmas noklikšķiniet uz vai pieskarieties pie ikonas **HP Client Security**, kas atrodas paziņojumu apgabalā, un pēc tam atlasiet **Open HP Client Security** (Atvērt HP Client Security).

2. Tiek palaists HP Client Security iestatīšanas vednis un redzama sveiciena lapa.

3. Izlasiet sveiciena ekrānā redzamo informāciju, aplieciniet savu identitāti, ierakstot savu Windows paroli, un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).

   Ja vēl neesat izveidojis Windows paroli, tiks prasīts tādu izveidot. Windows parole ir nepieciešama tādēļ, lai Windows kontam nevarētu piekļūt personas, kurām tā lietošana nav atļauta, un lai varētu lietot HP Security drošības līdzekļus.

4. HP SpareKey lapā atlasiet trīs drošības jautājumus. Ievadiet atbildi uz katru no šiem jautājumiem un pēc tam noklikšķiniet uz **Next** (Tālāk). Atļauta arī šo jautājumu pielāgošana. Papildinformāciju skatiet sadaļā HP SpareKey — paroles atkopšana 14. lpp.

5. Pirkstu nospiedumu lapā reģistrējiet vismaz minimālo nepieciešamo pirkstu nospiedumu skaitu un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk). Papildinformāciju skatiet sadaļā Pirkstu nospiedumi 12. lpp.

6. Diska šifrēšanas lapā aktivizējiet šifrēšanu, dublējiet šifrēšanas atslēgu un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk). Papildinformāciju skatiet HP Drive Encryption programmatūras sadaļā Palīdzība.

**PIEZĪME.** Tas attiecas uz scenāriju, kad lietotājs ir administrators un kad administrators nav iepriekš konfigurējis HP Client Security iestatīšanas vedni.

7. Vedņa pēdējā lapā noklikšķiniet uz vai pieskarieties pie **Finish** (Pabeigt).

   Šajā lapā ir redzams funkciju statuss un autentificēšanas dati.

8. HP Client Security iestatīšanas vednis nodrošina Just In Time Authentication un File Sanitizer funkciju aktivizēšanu. Papildinformāciju skatiet HP Device Access Manager programmatūras sadaļā Palīdzība un HP File Sanitizer programmatūras sadaļā Palīdzība.

**PIEZĪME.** Tas attiecas uz scenāriju, kad lietotājs ir administrators un kad administrators nav iepriekš konfigurējis HP Client Security iestatīšanas vedni.

# HP Client Security atvēršana

Varat atvērt lietojumprogrammu HP Client Security vienā no tālāk norādītajiem veidiem.

**PIEZĪME.** HP Client Security iestatīšanas vedņa darbības ir jāpabeidz, un tikai pēc tam būs iespējams palaist lietojumprogrammu HP Client Security.

- Sākuma ekrānā vai lietojumprogrammas ekrānā noklikšķiniet uz vai pieskarieties pie lietotnes **HP Client Security**,

  — vai —

  Uz Windows darbvirsmas noklikšķiniet uz vai pieskarieties pie **HP Client Security** Gadget (Windows 7).

  — vai —

  Windows darbvirsmas paziņojumu apgabalā veiciet dubultklikšķi uz vai dubultskārienu pie ikonas **HP Client Security**, kas atrodas uzdevumjoslas labajā pusē.

  — vai —

  Uz Windows darbvirsmas noklikšķiniet uz vai pieskarieties pie ikonas **HP Client Security**, kas atrodas paziņojumu apgabalā, un pēc tam atlasiet **Open HP Client Security** (Atvērt HP Client Security).

# 3 Vienkāršās iestatīšanas rokasgrāmata mazajiem uzņēmumiem

Šīs nodaļas mērķis ir nodemonstrēt galvenās darbības, kas jāveic, lai aktivizētu visparastākās un visnoderīgākās HP Client Security opcijas mazajiem uzņēmumiem. Šīs programmatūras neskaitāmie rīki un opcijas ļauj precīzi pieskaņot preferences un iestatīt piekļuves kontroli. Šī Vienkāršās iestatīšanas rokasgrāmata mēģina palīdzēt palaist katru no moduļiem, iestatīšanai veltot vismazāk pūļu un laika. Lai iegūtu papildu informāciju, atlasiet moduli, kurš jūs interesē, un pēc tam noklikšķiniet uz simbola **?** vai pogas Palīdzība augšējā labajā stūrī. Pēc noklikšķināšanas uz šīs pogas automātiski parādīsies informācija, lai palīdzētu ar dotajā brīdī atvērto logu.

## Darba sākšana

1. Windows darbvirsmas paziņojumu apgabalā atveriet HP Client Security, veicot dubultklikšķi uz ikonas **HP Client Security**, kas atrodas uzdevumjoslas labajā pusē.
2. Ievadiet vai izveidojiet Windows paroli.
3. Veiciet HP Client Security iestatīšanu.

Lai iestatītu HP Client Security pieprasīt autentifikāciju tikai vienreiz, kamēr notiek pieteikšanās Windows operētājsistēmā, skatiet Drošības līdzekļi 27. lpp..

## Password Manager

Ikvienam ir visai daudz paroļu — it īpaši, regulāri piekļūstot vietnēm un izmantojot lietojumprogrammas, kuras pieprasa pieteikšanos. Parasts lietotājs vai nu izmanto vienu un to pašu paroli visām lietojumprogrammām un vietnēm, vai arī kļūst radošs un drīz vien aizmirst, kura parole ir kurai lietojumprogrammai.

Password Manager var automātiski atcerēties paroles vai nodrošināt iespēju izvēlēties, kuru vietņu paroles atcerēties un kuru vietņu paroles neatcerēties. Pēc pieteikšanās datorā Password Manager iesniegs jūsu paroles vai akreditācijas datus atbilstošajām lietojumprogrammām vai tīmekļa vietnēm.

Kad atvērsiet lietojumprogrammu vai vietni, kas pieprasa akreditācijas datus, Password Manager automātiski atpazīs šo vietni un jautās, vai vēlaties, lai programmatūra atceras jūsu informāciju. Ja nevēlaties iekļaut zināmas vietnes, varat noraidīt šo pieprasījumu.

Lai sāktu saglabāt tīmekļa vietas, lietotājvārdu un paroles, rīkojieties šādi.

1. Piemēram, atveriet atbilstošo vietni vai lietojumprogrammu un pēc tam pievienojiet tīmekļa autentifikāciju, noklikšķinot uz ikonas Password Manager, kura atrodas tīmekļa lapas augšējā kreisajā stūrī.
2. Piešķiriet šai saitei nosaukumu (izvēles iespēja) un ievadiet lietotājvārdu un paroli modulī Password Manager.
3. Pēc pabeigšanas noklikšķiniet uz pogas **OK** (Labi).
4. Password Manager var saglabāt arī jūsu lietotājvārdu un paroles tīkla koplietojumam vai kartētiem tīkla diskiem.

## Password Manager saglabāto autentifikācijas datu apskatīšana un pārvaldīšana

Password Manager ļauj apskatīt, pārvaldīt, dublēt un palaist autentifikācijas datus no centrālās atrašanās vietas. Password Manager atbalsta saglabāto vietņu palaišanu arī no Windows operētājsistēmas.

Lai atvērtu Password Manager, izmantojiet tastatūras taustiņu kombināciju Ctrl+Windows taustiņš+h un pēc tam noklikšķiniet uz **Log in** (Pieteikties), lai palaistu un autentificētu saglabāto saīsni.

Password Manager opcija **Edit** (Rediģēt) ļauj apskatīt un mainīt nosaukumu, lietotājvārdu un pat atklāj paroles.

HP Client Security mazajiem uzņēmumiem ļauj visus akreditācijas datus un iestatījumus dublēt un/vai nokopēt citā datorā.

# HP Device Access Manager

Device Access Manager var izmantot, lai ierobežotu dažādu iekšēju un ārēju atmiņas ierīču izmantošanu, lai dati būtu droši cietajā diskā un netiktu iznesti pa jūsu uzņēmuma durvīm. Piemēram, varat atļaut lietotāja piekļuvi datiem, bet bloķēt datu kopēšanu CD, personīgajā mūzikas atskaņotājā vai USB atmiņas ierīcē.

1. Atveriet **Device Access Manager** (skatiet HP Device Access Manager atvēršana 42. lpp.).

   Redzama pašreizējā lietotāja piekļuve.

2. Lai mainītu lietotāju, grupu vai ierīču piekļuvi, noklikšķiniet uz vai pieskarieties pie **Change** (Mainīt). Papildinformāciju skatiet sadaļā Sistēmas skats 43. lpp.

# HP Drive Encryption

Modulis HP Drive Encryption tiek izmantots datu aizsardzībai, šifrējot visu cieto disku. Cietajā diskā esošie dati būs aizsargāti pat tad, ja dators kādreiz tiks nozagts un/vai cietais disks tiks izņemts no sākotnējā datora un ievietots citā datorā.

Papildu drošības priekšrocība ir tāda, ka Drive Encryption pieprasa veikt pareizu autentifikāciju, izmantojot lietotājvārdu un paroli pirms operētājsistēmas palaišanas. Šis process tiek saukts par pirmsāknēšanas autentifikāciju.

Lai atvieglotu šo procesu, daudzie programmatūras moduļi automātiski sinhronizē paroles, tostarp Windows lietotāju kontu, autentificēšanas domēnu, HP Drive Encryption, Password Manager un HP Client Security paroles.

Lai sākotnējās iestatīšanas laikā iestatītu HP Drive Encryption, izmantojot HP Client Security iestatīšanas vedni, skatiet Darba sākšana 8. lpp..

# 4 HP Client Security

HP Client Security sākuma lapa ir centrālā vieta, no kuras var vienkārši piekļūt HP Client Security funkcijām, lietojumprogrammām un iestatījumiem. Sākuma lapa ir sadalīta trīs daļās.

- **DATA** (DATI) — nodrošina piekļuvi lietojumprogrammām, kuras tiek lietotas datu drošības pārvaldīšanai.
- **DEVICE** (IERĪCE) — nodrošina piekļuvi lietojumprogrammām, kuras tiek lietotas ierīces drošības pārvaldīšanai.
- **IDENTITY** (IDENTITĀTE) — nodrošina autentificēšanas datu reģistrēšanu un pārvaldīšanu.

Novietojiet kursoru virs lietojumprogrammas elementa, lai skatītu lietojumprogrammas aprakstu.

HP Client Security var lapas apakšā nodrošināt saites uz lietotāja un administratora iestatījumiem. HP Client Security nodrošina piekļuvi opcijai Uzlabotie iestatījumi un funkcijām, noklikšķinot uz vai pieskaroties pie (iestatījumu) ikonas **Gear** (Zobrats).

## Identitātes funkcijas, lietojumprogrammas un iestatījumus

HP Client Security nodrošinātās identitātes funkcijas, lietojumprogrammas un iestatījumi palīdz jums pārvaldīt dažādus jūsu digitālās identitātes aspektus. Noklikšķiniet uz vai pieskarieties pie viena no šiem elementiem HP Client Security sākuma lapā un pēc tam ievadiet savu Windows paroli.

- **Fingerprints** (Pirkstu nospiedumi) — reģistrē un pārvalda pirkstu nospiedumu autentificēšanas datus.
- **SpareKey** — iestata un pārvalda HP SpareKey autentificēšanas datus, kurus var lietot, lai pieteiktos datorā, ja citi autentificēšanas dati ir pazaudēti vai novietoti kādā nepareizā vietā. Šī funkcija ļauj arī atiestatīt pazudušu paroli.
- **Windows Password** (Windows parole) — nodrošina vienkāršu piekļuvi, lai varētu mainīt Windows paroli.
- **Bluetooth Devices** (Bluetooth ierīces) — ļauj reģistrēt un pārvaldīt Bluetooth ierīces.
- **Cards** (Kartes) — ļauj reģistrēt un pārvaldīt viedkartes, bezkontakta kartes un kartes ar mikroshēmu.
- **PIN** — ļauj reģistrēt un pārvaldīt PIN kodu.
- **RSA SecurID** — ļauj reģistrēt un pārvaldīt RSA SecurID akreditācijas datus (ja notikusi atbilstoša iestatīšana).
- **Password Manager** — ļauj pārvaldīt jūsu tiešsaistes kontu un lietojumprogrammu paroles.

### Pirkstu nospiedumi

HP Client Security iestatīšanas vednis vada jūs cauri pirkstu nospiedumu iestatīšanas jeb „reģistrēšanas” procesam.

Jūs varat reģistrēt vai dzēst savus pirkstu nospiedumus arī pirkstu nospiedumu lapā, kurai varat piekļūt HP Client Security sākuma lapā noklikšķinot uz vai pieskaroties pie ikonas **Fingerprints** (Pirkstu nospiedumi).

1. Pirkstu nospiedumu lapā pārvelciet ar pirkstu, līdz tas ir veiksmīgi reģistrēts.

   Nepieciešamais reģistrējamo pirkstu skaits ir norādīts šajā lapā. Ieteicams reģistrēt rādītājpirkstus vai vidējos pirkstus.

2. Lai izdzēstu iepriekš reģistrētos pirkstu nospiedumus, noklikšķiniet uz vai pieskarieties pie **Delete** (Dzēst).

3. Lai reģistrētu papildu pirkstus, noklikšķiniet uz vai pieskarieties pie **Enroll an additional fingerprint** (Reģistrēt papildu pirkstu nospiedumu).

4. Pirms iziešanas no lapas noklikšķiniet uz vai pieskarieties pie **Save** (Saglabāt).

⚠ **UZMANĪBU!** Reģistrējot pirkstu nospiedumus, izmantojot vedni, pirkstu nospiedumu dati netiek saglabāti, kamēr nav noklikšķināts uz **Next** (Tālāk). Ja ļausiet datoram uz brīdi kļūt neaktīvam vai aizvērsiet programmu, veiktās izmaiņas **netiks** saglabātas.

- Lai piekļūtu opcijai Pirkstu nospiedumu administratora iestatījumi, kurā administratori var norādīt reģistrēšanas, precizitātes un citus iestatījumus, noklikšķiniet uz vai pieskarieties pie **Administrative Settings** (Administratora iestatījumi) (tam nepieciešamas administratora privilēģijas).
- Lai piekļūtu opcijai Pirkstu nospiedumu lietotāja iestatījumi, kurā varat norādīt iestatījumus, kas nosaka pirkstu nospiedumu pazīšanas sistēmas izskatu un darbību, noklikšķiniet uz vai pieskarieties pie **User Settings** (Lietotāja iestatījumi).

## Pirkstu nospiedumu administratora iestatījumi

Administratori var norādīt pirkstu nospiedumu lasītāja reģistrēšanas, precizitātes un citus iestatījumus. Tam nepieciešamas administratora privilēģijas.

- Lai piekļūtu pirkstu nospiedumu autentificēšanas datu administratora iestatījumiem, pirkstu nospiedumu lapā noklikšķiniet uz vai pieskarieties pie **Administrative Settings** (Administratora iestatījumi).

- **User enrollment** (Lietotāja reģistrēšana) — izvēlieties minimālo un maksimālo lietotāja reģistrējamo pirkstu nospiedumu skaitu.
- **Recognition** (Atpazīšana) — pārvietojiet slīdni, lai noregulētu pirkstu nospiedumu lasītāja jutīgumu brīdī, kad pārvelkat ar pirkstu.

  Ja pirkstu nospiedums atkārtoti netiek atpazīts, iespējams, jāatlasa zemāks atpazīšanas iestatījums. Augstāks iestatījums palielina jutību pret dažāda veida pārvilkšanu ar pirkstu un tādēļ samazina kļūdainas pirkstu nospiedumu apstiprināšanas iespēju. Iestatījums **Medium-High** (Vidējs-Augsts) nodrošina labu drošības un ērtību apvienojumu.

### Pirkstu nospiedumu lietotāja iestatījumi

Pirkstu nospiedumu lietotāja iestatījumu lapā varat norādīt iestatījumus, kas nosaka pirkstu nospiedumu pazīšanas sistēmas izskatu un darbību.

▲ Lai piekļūtu pirkstu nospiedumu autentificēšanas datu lietotāja iestatījumiem, pirkstu nospiedumu lapā noklikšķiniet uz vai pieskarieties pie **User Settings** (Lietotāja iestatījumi).

- **Enable sound feedback** (Iespējot skaņas signālus) — pēc noklusējuma pirksta pārvilkšanas laikā HP Client Security atskaņo skaņas signālu, kas ir atšķirīgs dažādiem programmas notikumiem. Jūs varat piešķirt jaunus skaņas signālus šiem notikumiem Windows vadības paneļa iestatījuma Skaņa cilnē Skaņas signāli vai atspējot skaņas signālus, notīrot izvēles rūtiņu.
- **Show scan quality feedback** (Rādīt skenēšanas kvalitāti) — lai būtu redzami visi skenētie pirkstu nospiedumi neatkarīgi no kvalitātes, atlasiet izvēles rūtiņu. Lai būtu redzami, tikai skenētie labas kvalitātes pirkstu nospiedumi, notīriet šo izvēles rūtiņu.

## HP SpareKey — paroles atkopšana

HP SpareKey ļauj iegūt piekļuvi (atbalstītās platformas) datoram, atbildot uz trim drošības jautājumiem.

Veicot sākotnējo iestatīšanu HP Client Security iestatīšanas vednī, HP Client Security prasa iestatīt personīgo HP SpareKey.

Lai iestatītu HP SpareKey, rīkojieties šādi.

1. Vedņa HP SpareKey lapā atlasiet trīs drošības jautājumus un pēc tam ievadiet atbildi uz katru no šiem jautājumiem.

   Varat atlasīt jautājumu no iepriekš definēto jautājumu saraksta vai ierakstīt pats savu jautājumu.

2. Noklikšķiniet uz vai pieskarieties pie **Enrolll** (Reģistrēt).

Lai izdzēstu HP SpareKey, rīkojieties šādi.

▲ Noklikšķiniet uz vai pieskarieties pie **Delete your SpareKey** (Dzēst SpareKey).

Pēc SpareKey iestatīšanas varat piekļūt datoram, lietojot SpareKey ieslēgšanas autentifikācijas pieteikšanās ekrānā vai Windows sveiciena ekrānā.

SpareKey lapā, kurai var piekļūt no paroles atkopšanas elementa HP Client Security sākuma lapā, varat atlasīt dažādus jautājumus vai mainīt atbildes.

Lai piekļūtu HP SpareKey iestatījumiem, kur administrators var norādīt iestatījumus HP SpareKey autentificēšanas datiem, noklikšķiniet uz **Settings** (Iestatījumi) (tam nepieciešamas administratora privilēģijas).

### HP SpareKey Settings

HP SpareKey iestatījumu lapā varat norādīt iestatījumus, kuri nosaka HP SpareKey autentificēšanas datu darbību un lietošanu.

▲ Lai palaistu HP SpareKey iestatījumu lapu, HP SpareKey lapā noklikšķiniet uz vai pieskarieties pie **Settings** (Iestatījumi) (tam nepieciešamas administratora privilēģijas).

Administratori var atlasīt tālāk minētos iestatījumus.

- Norādīt jautājumus, kuri jāuzdod katram lietotājam HP SpareKey iestatīšanas laikā.
- Pievienot līdz trim pielāgotiem drošības jautājumiem lietotājiem parādāmajā sarakstā.

- Izvēlēties, vai atļaut vai neatļaut lietotājiem sastādīt pašiem savus drošības jautājumus.
- Norādīt, kuras autentifikācijas vides (Windows vai ieslēgšanas autentifikāciju) atļauj lietot HP SpareKey paroles atkopšanai.

## Windows parole

HP Client Security ļauj nomainīt Windows paroli vienkāršāk un ātrāk nekā Windows vadības panelī.

Lai nomainītu Windows paroli, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie **Windows Password** (Windows parole).
2. Ievadiet savu pašreizējo paroli tekstlodziņā **Current Windows password** (Pašreizējā Windows parole).
3. Ierakstiet jauno paroli tekstlodziņā **New Windows password** (Jaunā Windows parole) un pēc tam to vēlreiz ierakstiet tekstlodziņā **Confirm new password** (Apstipriniet jauno paroli).
4. Noklikšķiniet uz vai pieskarieties pie **Change** (Mainīt), lai nekavējoties mainītu savu pašreizējo paroli pret ievadīto jauno paroli.

## Bluetooth ierīces

Ja administrators ir iespējojis Bluetooth kā autentificēšanas datus, varat iestatīt Bluetooth tālruni kopā ar citiem datiem papildu drošībai.

**PIEZĪME.** Tiek atbalstītas tikai Bluetooth tālruņa tipa ierīces.

1. Pārliecinieties, vai datorā ir iespējota Bluetooth funkcionalitāte un Bluetooth tālrunis ir iestatīts noteikšanas režīmā. Lai pievienotu tālruni, var būt nepieciešams ierakstīt Bluetooth ierīcē automātiski ģenerētu kodu. Atkarībā no Bluetooth ierīces konfigurācijas iestatījumiem, var būt nepieciešama datora un tālruņa kodu savienošanas pārī salīdzināšana.
2. Lai reģistrētu tālruni, atlasiet to un pēc tam noklikšķiniet uz vai pieskarieties pie **Enroll** (Reģistrēt).

Lai piekļūtu lapai Bluetooth ierīču iestatījumi 15. lpp., kurā administrators var norādīt Bluetooth ierīču iestatījumus, noklikšķiniet uz **Settings** (Iestatījumi) (tam nepieciešamas administratora privilēģijas).

### Bluetooth ierīču iestatījumi

Administratori var norādīt tālāk minētos iestatījumus, kas nosaka Bluetooth ierīces uzvedību un autentificēšanas datu lietošanu.

#### Klusā autentifikācija

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Identitātes pārbaudes laikā automātiski lietot pievienoto reģistrēto Bluetooth ierīci) — atlasiet šo izvēles rūtiņu, lai ļautu lietotājiem lietot Bluetooth autentificēšanas datus, neprasot lietotāja darbību, vai notīriet šo izvēles rūtiņu, lai atspējotu šo opciju.

#### Bluetooth tuvums

- **Lock computer when your enrolled Bluetooth device moves out of range of your computer** (Slēgt datoru, kad reģistrētā Bluetooth ierīce pārvietojas ārpus datora uztveršanas diapazona) — atlasiet šo izvēles rūtiņu, lai slēgtu datoru, kad pieteikšanās laikā pievienotā

Bluetooth ierīce pārvietojas ārpus uztveršanas diapazona, vai notīriet šo izvēles rūtiņu, lai atspējotu šo opciju.

**PIEZĪME.** Lai varētu izmantot šīs funkcijas piedāvātās priekšrocības, datora Bluetooth modulim ir jāatbalsta šī iespēja.

## Kartes

HP Client Security var atbalstīt vairākus atšķirīgus identifikācijas karšu veidus, t.i. mazas plastmasas kartes ar datora mikroshēmām. To skaitā ietilpst viedkartes, bezkontakta kartes un kartes ar mikroshēmu. Ja viena no šīm kartēm un atbilstošais kartes lasītājs ir pievienoti datoram, ja administrators ir instalējis ražotāja nodrošināto atbilstošo draiveri un ja administrators ir iespējojis šo karti kā autentificēšanas datus, varat lietot šo karti kā autentificēšanas datus.

Viedkartēm ražotājam ir jānodrošina rīki drošības sertifikāta instalēšanai un PIN pārvaldīšanai, ko HP Client Security lieto savā drošības algoritmā. PIN lietotais rakstzīmju skaits un veids var atšķirties. Pirms viedkaršu lietošanas administratoriem ir tās jāinicializē.

HP Client Security atbalsta šādas viedkartes:

- CSP
- PKCS11

HP Client Security atbalsta šādas bezkontakta kartes:

- Bezkontakta HID iCLASS atmiņas kartes
- Bezkontakta MiFare Classic 1k, 4k un mini atmiņas kartes

HP Client Security atbalsta šādas kartes ar mikroshēmām:

- HID Proximity Cards

Lai reģistrētu viedkarti, rīkojieties šādi.

1. Ievietojiet karti pievienotajā viedkaršu lasītājā.
2. Pēc kartes atpazīšanas ievadiet kartes PIN un pēc tam noklikšķiniet uz vai pieskarieties pie **Enroll** (Reģistrēt).

Lai mainītu viedkartes PIN, rīkojieties šādi.

1. Ievietojiet karti pievienotajā viedkaršu lasītājā.
2. Pēc kartes atpazīšanas ievadiet kartes PIN un pēc tam noklikšķiniet uz vai pieskarieties pie **Authenticate** (Autentificēt).
3. Noklikšķiniet uz vai pieskarieties pie **Change PIN** (Mainīt PIN) un pēc tam ievadiet jauno PIN.

Lai reģistrētu bezkontakta karti vai karti ar mikroshēmu, rīkojieties šādi.

1. Novietojiet karti uz atbilstošā lasītāja vai ļoti tuvu atbilstošajam lasītājam.
2. Pēc kartes atpazīšanas noklikšķiniet uz vai pieskarieties pie **Enroll** (Reģistrēt).

Lai dzēstu reģistrēto karti, rīkojieties šādi.

1. Ļaujiet lasītajam karti nolasīt.
2. Lietojot viedkartes, ievadiet kartes piešķirto PIN un pēc tam noklikšķiniet uz vai pieskarieties pie **Authenticate** (Autentificēt).
3. Noklikšķiniet uz vai pieskarieties pie **Delete** (Dzēst).

Pēc kartes reģistrēšanas kartes dati ir redzami sadaļā **Enrolled Cards** (Reģistrētās kartes). Pēc kartes dzēšanas karte tiek izņemta no šī saraksta.

Lai piekļūtu opcijai Karšu ar mikroshēmām, bezkontakta karšu un viedkaršu iestatījumi, kur administratori var norādīt iestatījumus karšu autentificēšanas datiem, noklikšķiniet uz vai pieskarieties pie **Settings** (Iestatījumi) (tam nepieciešamas administratora privilēģijas).

### Karšu ar mikroshēmām, bezkontakta karšu un viedkaršu iestatījumi

Lai piekļūtu kartes iestatījumiem, noklikšķiniet uz vai pieskarieties pie kartes šajā sarakstā un pēc tam noklikšķiniet uz vai pieskarieties pie redzamās bultiņas.

Lai mainītu viedkartes PIN, rīkojieties šādi.

1. Ļaujiet lasītajam karti nolasīt.
2. Ievadiet kartes piešķirto PIN un pēc tam noklikšķiniet uz vai pieskarieties pie **Continue** (Turpināt).
3. Ievadiet un apstipriniet jauno PIN un pēc tam noklikšķiniet uz vai pieskarieties pie **Continue** (Turpināt).

Lai inicializētu viedkartes PIN, rīkojieties šādi.

1. Ļaujiet lasītajam karti nolasīt.
2. Ievadiet kartes piešķirto PIN un pēc tam noklikšķiniet uz vai pieskarieties pie **Continue** (Turpināt).
3. Ievadiet un apstipriniet jauno PIN un pēc tam noklikšķiniet uz vai pieskarieties pie **Continue** (Turpināt).
4. Noklikšķiniet uz vai pieskarieties pie **Yes** (Jā), lai apstiprinātu inicializēšanu.

Lai notīrītu kartes datus, rīkojieties šādi.

1. Ļaujiet lasītajam karti nolasīt.
2. Ievadiet kartes piešķirto PIN (tikai veidkartēm) un pēc tam noklikšķiniet uz vai pieskarieties pie **Continue** (Turpināt).
3. Noklikšķiniet uz vai pieskarieties pie **Yes** (Jā), lai apstiprinātu dzēšanu.

## PIN

Ja administrators ir iespējojis PIN kā autentificēšanas datus, varat iestatīt PIN kopā ar citiem datiem papildu drošībai.

Lai iestatītu jaunu PIN, rīkojieties šādi.

- Ievadiet PIN, ievadiet to vēlreiz, lai apstiprinātu, un pēc tam noklikšķiniet uz vai pieskarieties pie **Apply** (Lietot).

Lai dzēstu PIN, rīkojieties šādi.

- Noklikšķiniet uz vai pieskarieties pie **Delete** (Dzēst) un pēc tam noklikšķiniet uz vai pieskarieties pie **Yes** (Jā), lai apstiprinātu.

Lai piekļūtu opcijai PIN iestatījumi, kur administratori var norādīt iestatījumus PIN autentificēšanas datiem, noklikšķiniet uz vai pieskarieties pie **Settings** (Iestatījumi) (tam nepieciešamas administratora privilēģijas).

### PIN Settings

PIN iestatījumu lapā varat norādīt minimālo un maksimālo pieļaujamo PIN autentificēšanas datu garumu.

## RSA SecurID

Ja administrators ir iespējojis RSA kā autentificēšanas datus un tālāk minētie nosacījumi ir izpildīti, varat reģistrēt vai dzēst RSA SecurID autentificēšanas datus.

**PIEZĪME.** Nepieciešama atbilstoša iestatīšana.

- Lietotājam ir jābūt izveidotam serverī RSA Server.
- Lietotājam un datoram piešķirtajai RSA SecurID pilnvarai ir jābūt savienotai ar RSA Server domēnu.
- Datorā ir instalēta SecurID programmatūra.
- Pieejams savienojums ar pareizi konfigurētu RSA Server.

Lai reģistrētu RSA SecurID autentificēšanas datus, rīkojieties šādi.

▲ Ievadiet RSA SecurID lietotājvārdu un ieejas kodu (RSA SecurID pilnvaras kodu vai PIN + pilnvaras kodu atkarībā no vides) un pēc tam noklikšķiniet uz vai pieskarieties pie **Apply** (Lietot).

Pēc veiksmīgas reģistrēšanas parādās ziņojums „Your RSA SecurID credential has been successfully enrolled” („RSA SecurID autentificēšanas dati ir veiksmīgi reģistrēti”) un ir iespējota poga Delete (Dzēst).

Lai dzēstu RSA SecurID autentificēšanas datus, rīkojieties šādi.

▲ Noklikšķiniet uz **Delete** (Dzēst) un pēc tam uznirstošajā dialoglodziņā atlasiet **Yes** (Jā), atbildot uz jautājumu „Are you sure you want to delete your RSA SecurID credential?” („Vai tiešām vēlaties dzēst savus RSA SecurID autentificēšanas datus?”).

## Password Manager

Lietojot Password Manager, pieteikšanās tīmekļa vietnēs un lietojumprogrammās ir daudz vienkāršāka un drošāka. Jūs varat izveidot stiprākas paroles, kuras jums nav jāpieraksta vai jāatceras, un pēc tam vienkārši un ātri pieteikties, izmantojot pirksta nospiedumu, viedkarti, karti ar mikroshēmu, bezkontakta karti, Bluetooth tālruni, PIN, RSA autentificēšanas datus vai Windows paroli.

**PIEZĪME.** Tā kā tīmekļa pieteikšanās ekrānu struktūra nepārtraukti mainās, Password Manager var vienmēr nespēt atbalstīt visas tīmekļa vietnes.

Password Manager piedāvā tālāk norādītās opcijas.

### Password Manager lapa

- Noklikšķināt uz vai pieskarties pie konta, lai automātiski palaistu tīmekļa lapu un lietojumprogrammu un pieteiktos.
- Lietot kategorijas kontu organizēšanai.

### Paroles drošums

- Uzreiz redzēt, vai pastāv kādas jūsu paroles drošības risks.
- Pievienojot pieteikšanās datus, pārbaudīt atsevišķu tīmekļa vietnēm un lietojumprogrammām lietoto paroļu stiprumu.
- Paroles drošums ir norādīts ar sarkaniem, dzelteniem vai zaļiem statusa indikatoriem.

Tīmekļa lapas vai lietojumprogrammas pieteikšanās ekrāna augšējā kreisajā stūrī ir redzama ikona **Password Manager**. Ja šai tīmekļa lapai vai lietojumprogrammai vēl nav izveidoti pieteikšanās dati, uz ikonas ir redzama plus zīme.

▲ Noklikšķiniet uz vai pieskarieties pie ikonas **Password Manager**, lai atvērtu kontekstizvēlni, kurā var izvēlēties kādu no tālāk norādītajām opcijām.

- Pievienot [kadudomenu.com] lietotnei Password Manager
- Atvērt Password Manager
- Ikonas iestatījumi
- Palīdzība

## Tīmekļa lapām vai programmām, kurām vēl nav izveidoti pieteikšanās dati

Tālāk minētās opcijas ir redzamas kontekstizvēlnē.

- **Add [somedomain.com] to the Password Manager** (Pievienot [kadudomenu.com] lietotnei Password Manager) — ļauj pievienot pieteikšanās datus, ar kuriem pieteikties redzamajā pieteikšanās ekrānā.
- **Open Password Manager** (Atvērt Password Manager) — palaiž Password Manager.
- **Icon Settings** (Ikonas iestatījumi) — ļauj norādīt apstākļus, kuros ir redzama ikona **Password Manager**.
- **Help** (Palīdzība) — atver HP Client Security sadaļu Palīdzība.

## Tīmekļa lapām vai programmām, kurām jau ir izveidoti pieteikšanās dati

Tālāk minētās opcijas ir redzamas kontekstizvēlnē.

- **Fill in logon data** (Ierakstīt pieteikšanās datus) — atver lapu **Verify your identity** (Apstipriniet savu identitāti). Ja autentificēšana ir veiksmīga, jūsu pieteikšanās dati tiek ievadīti pieteikšanās laukos un pēc tam lapa tiek iesniegta (ja pieteikšanās izveidošanas vai pēdējās rediģēšanas laikā norādīta iesniegšana).
- **Edit Logon** (Rediģēt pieteikšanās datus) — ļauj rediģēt pieteikšanās datus konkrētajai tīmekļa vietnei.
- **Add Logon** (Pievienot pieteikšanās datus) — ļauj pievienot kontu lietotnei Password Manager.
- **Open Password Manager** (Atvērt Password Manager) — palaiž Password Manager.
- **Help** (Palīdzība) — atver HP Client Security sadaļu Palīdzība.

**PIEZĪME.** Šī datora administrators var būt konfigurējis HP Client Security tā, lai identitātes apstiprināšanai tiktu pieprasīti nevis viena, bet vairāku veidu autentificēšanas dati.

## Pieteikšanās datu pievienošana

Jūs varat vienkārši pievienot pieteikšanās datus kādai tīmekļa vietnei vai programmai, vienreiz ievadot pieteikšanās informāciju. Pēc tam Password Manager automātiski ievada šo informāciju jūsu vietā. Jūs varat lietot šos pieteikšanās datus pēc tīmekļa vietnes vai programmas pārlūkošanas.

Lai pievienotu pieteikšanās datus, rīkojieties šādi.

1. Atveriet tīmekļa lapas vai programmas pieteikšanās ekrānu.
2. Noklikšķiniet uz vai pieskarieties pie ikonas **Password Manager** un pēc tam noklikšķiniet uz vai pieskarieties pie viena no tālāk norādītajiem elementiem, atkarībā no tā, vai tas ir tīmekļa vietnes vai programmas pieteikšanās ekrāns.
   - Tīmekļa vietnes gadījumā noklikšķiniet uz vai pieskarieties pie **Add [domain name] to Password Manager** (Pievienot [domēna nosaukums] Password Manager).
   - Programmas gadījumā noklikšķiniet uz vai pieskarieties pie **Add this logon screen to Password Manager** (Pievienot šo pieteikšanās ekrānu Password Manager).
3. Ievadiet savus pieteikšanās datus. Pieteikšanās lauki ekrānā un atbilstošie lauki dialoglodziņā ir norādīti ar trekninātu oranžu apmali.
   a. Lai aizpildītu pieteikšanās lauku ar vienu no iepriekš formatētajām iespējām, noklikšķiniet uz vai pieskarieties pie bultiņām lauka labajā pusē.
   b. Lai skatītu šīs pieteikšanās paroli, noklikšķiniet uz vai pieskarieties pie **Show password** (Rādīt paroli).
   c. Lai pieteikšanās lauki tiktu aizpildīti, bet netiktu iesniegti, notīriet izvēles rūtiņu **Automatically submit logon data** (Automātiski iesniegt pieteikšanās datus).
   d. Noklikšķiniet uz vai pieskarieties pie **OK** (Labi), lai atlasītu vēlamo autentifikācijas metodi (pirkstu nospiedumus, viedkarti, karti ar mikroshēmu, bezkontakta karti, Bluetooth tālruni, PIN vai paroli) un pēc tam piesakieties ar atlasīto autentifikācijas metodi.

      Tagad no ikonas **Password Manager** ir noņemta plus zīme, lai norādītu, ka pieteikšanās dati ir izveidoti.
   e. Ja Password Manager nekonstatē pieteikšanās laukus, noklikšķiniet uz vai pieskarieties pie **More fields** (Citi lauki).
      - Atlasiet katra pieteikšanās laikā nepieciešamā lauka izvēles rūtiņu vai notīriet izvēles rūtiņu tiem laukiem, kuri pieteikšanās laikā nav nepieciešami.
      - Noklikšķiniet uz vai pieskarieties pie **Close** (Aizvērt).

Katru reizi piekļūstot šai tīmekļa vietnei vai atverot šo programmu, tīmekļa vietnes vai lietojumprogrammas pieteikšanās ekrāna augšējā kreisajā stūrī parādīsies ikona **Password Manager**, norādot, ka varat lietot reģistrētos autentificēšanas datus tam, lai pieteiktos.

## Pieteikšanās datu reģistrēšana

Lai rediģētu pieteikšanās datus, rīkojieties šādi.

1. Atveriet tīmekļa lapas vai programmas pieteikšanās ekrānu.
2. Lai atvērtu dialoglodziņu, kurā var rediģēt pieteikšanās informāciju, noklikšķiniet uz vai pieskarieties pie ikonas **Password Manager** un pēc tam noklikšķiniet uz vai pieskarieties pie **Edit Logon** (Rediģēt pieteikšanās datus).

   Pieteikšanās lauki ekrānā un atbilstošie lauki dialoglodziņā ir norādīti ar trekninātu oranžu apmali.

   Varat rediģēt konta informāciju arī no Password Manager lapas, noklikšķinot uz vai pieskaroties pie pieteikšanās datiem, lai atvērtu rediģēšanas opcijas, un pēc tam atlasot **Edit** (Rediģēt).
3. Rediģējiet pieteikšanās informāciju.
   - Lai rediģētu lauku **Account name** (Konta nosaukums), ievadiet jauno nosaukumu šajā laukā.
   - Lai pievienotu vai rediģētu nosaukumu laukā **Category** (Kategorija), ievadiet vai mainiet šo nosaukumu laukā **Category** (Kategorija).
   - Lai atlasītu pieteikšanās lauku **Username** (Lietotājvārds) ar vienu no iepriekš formatētajām iespējām, noklikšķiniet uz vai pieskarieties pie lejupvērstās bultiņas lauka labajā pusē.

     Iepriekš formatētas iespējas ir pieejamas tikai rediģējot pieteikšanās datus, izmantojot komandu Edit (Rediģēt) Password Manager ikonas kontekstizvēlnē.
   - Lai atlasītu pieteikšanās lauku **Password** (Parole) ar vienu no iepriekš formatētajām iespējām, noklikšķiniet uz vai pieskarieties pie lejupvērstās bultiņas lauka labajā pusē.

     Iepriekš formatētas iespējas ir pieejamas tikai rediģējot pieteikšanās datus, izmantojot komandu Edit (Rediģēt) Password Manager ikonas kontekstizvēlnē.
   - Lai pievienotu ekrānā redzamos papildu laukus pieteikšanās datiem, noklikšķiniet uz vai pieskarieties pie **More fields** (Citi lauki).
   - Lai skatītu šīs pieteikšanās paroli, noklikšķiniet uz vai pieskarieties pie ikonas **Show password** (Rādīt paroli).
   - Lai pieteikšanās lauki tiktu aizpildīti, bet netiktu iesniegti, notīriet izvēles rūtiņu **Automatically submit logon data** (Automātiski iesniegt pieteikšanās datus).
   - Lai atzīmētu, ka šie pieteikšanās dati ietver apdraudētu paroli, atlasiet izvēles rūtiņu **This password is compromised** (Šī parole ir apdraudēta).

     Pēc izmaiņu saglabāšanas kā apdraudēti tiks atzīmēti arī visi citi pieteikšanās dati, kuri ietver šo pašu paroli. Pēc tam varat atvērt katru ietekmēto kontu un pēc nepieciešamības nomainīt paroles.
4. Noklikšķiniet uz vai pieskarieties pie **OK** (Labi).

## Password Manager izvēlnes Quick Links (Ātras saites) lietošana

Password Manager nodrošina ātru un vienkāršu veidu, kā palaist tīmekļa vietnes un programmas, kurām ir izveidoti pieteikšanās dati. Veiciet dubultklikšķi vai dubultskārienu uz programmas vai tīmekļa vietnes pieteikšanās lauka Password Manager izvēlnē **Quick Links** (Ātrās saites) vai Password Manager lapā ar HP Client Security, lai atvērtu pieteikšanās ekrānu un pēc tam ierakstītu pieteikšanās datus.

Izveidojot pieteikšanās datus, tie tiks automātiski pievienoti jūsu Password Manager izvēlnei **Quick Links** (Ātrās saites).

Lai atvērtu izvēlni **Quick Links** (Ātrās saites), rīkojieties šādi.

- Nospiediet **Password Manager** karsto taustiņu kombināciju (Ctrl+Windows taustiņš+h ir rūpnīcas iestatījums). Lai mainītu karstā taustiņa kombināciju, HP Client Security sākuma lapā noklikšķiniet uz **Password Manager** un pēc tam noklikšķiniet uz vai pieskarieties pie **Settings** (Iestatījumi).

## Pieteikšanās datu organizēšana kategorijās

Izveidojiet vienu vai vairākas kategorijas, lai pieteikšanās dati būtu labi organizēti.

Lai piešķirtu pieteikšanās datus kādai kategorijai, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie **Password Manager**.
2. Noklikšķiniet uz vai pieskarieties pie konta ieraksta un pēc tam noklikšķiniet uz vai pieskarieties pie **Edit** (Rediģēt).
3. Laukā **Category** (Kategorija) ievadiet kategorijas nosaukumu.
4. Noklikšķiniet uz vai pieskarieties pie **Save** (Saglabāt).

Lai izņemtu kontu no kādas kategorijas, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie **Password Manager**.
2. Noklikšķiniet uz vai pieskarieties pie konta ieraksta un pēc tam noklikšķiniet uz vai pieskarieties pie **Edit** (Rediģēt).
3. Laukā **Category** (Kategorija) izdzēsiet kategorijas nosaukumu.
4. Noklikšķiniet uz vai pieskarieties pie **Save** (Saglabāt).

Lai pārdēvētu kategoriju, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie **Password Manager**.
2. Noklikšķiniet uz vai pieskarieties pie konta ieraksta un pēc tam noklikšķiniet uz vai pieskarieties pie **Edit** (Rediģēt).
3. Laukā **Category** (Kategorija) mainiet kategorijas nosaukumu.
4. Noklikšķiniet uz vai pieskarieties pie **Save** (Saglabāt).

## Pieteikšanās datu pārvaldīšana

Password Manager ļauj no vienas centralizētas vietas viegli pārvaldīt tādu pieteikšanās informāciju kā lietotājvārdi, paroles un daudzi pieteikšanās konti.

Šie pieteikšanās dati ir uzskaitīti Password Manager lapā.

Lai pārvaldītu pieteikšanās datus, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie **Password Manager**.
2. Noklikšķiniet uz vai pieskarieties pie esošajiem pieteikšanās datiem un pēc tam atlasiet vienu no tālāk norādītajām opcijām un izpildiet ekrānā redzamās instrukcijas.
   - **Edit** (Rediģēt) — rediģēt pieteikšanās datus. Papildinformāciju skatiet sadaļā Pieteikšanās datu reģistrēšana 21. lpp.
   - **Log in** (Pieteikties) — pieteikties atlasītajā kontā.
   - **Delete** (Dzēst) — dzēst atlasītā konta pieteikšanās datus.

Lai pievienotu papildu pieteikšanās datus, ar kuriem var pieteikties kādā tīmekļa vietnē vai programmā, rīkojieties šādi.

1. Atveriet tīmekļa lapas vai programmas pieteikšanās ekrānu.
2. Noklikšķiniet uz vai pieskarieties pie ikonas **Password Manager**, lai atvērtu tās kontekstizvēlni.
3. Noklikšķiniet uz vai pieskarieties pie **Add Logon** (Pievienot pieteikšanās datus) un pēc tam izpildiet ekrānā redzamās instrukcijas.

## Paroles drošuma novērtēšana

Stipras paroles lietošana, piesakoties tīmekļa vietnēs un programmās, ir identitātes aizsargāšanas svarīgs aspekts.

Password Manager atvieglo drošības uzraudzīšanu un uzlabošanu, nodrošinot katras, piesakoties tīmekļa vietnēs un lietojumprogrammās lietotās, paroles stipruma tūlītēju un automātisku analīzi.

Ja ievadāt paroli, izveidojot Password Manager pieteikšanās datus kontam, zem paroles ir redzama krāsaina josla, kas norāda paroles stiprumu. Krāsas norāda šādas vērtības:

- **sarkana** — vāja
- **dzeltena** — viduvēja
- **zaļa** — stipra

## Password Manager ikonas iestatījumi

Password Manager mēģina identificēt tīmekļa vietņu un programmu pieteikšanās ekrānus. Kad Password Manager nosaka pieteikšanās ekrānu, kuram neesat izveidojis pieteikšanās datus, šī

lietotne prasa pievienot pieteikšanās datus šim ekrānam, atverot ikonu **Password Manager** ar plus zīmi.

1. Noklikšķiniet uz vai pieskarieties pie ikonas un pēc tam noklikšķiniet uz vai pieskarieties pie **Icon Settings** (Ikonas iestatījumi), lai pielāgotu Password Manager darbību iespējamo pieteikšanās vietņu gadījumā.

   - **Prompt to add logons for logon screens** (Prasīt pievienot pieteikšanās datus pieteikšanās ekrāniem) — noklikšķiniet uz vai pieskarieties pie šīs opcijas, lai Password Manager prasītu pievienot pieteikšanās datus pieteikšanās ekrānam tad, ja tam tādi vēl nav iestatīti.
   - **Exclude this screen** (Neiekļaut šo ekrānu) — atlasiet šo izvēles rūtiņu, lai Password Manager vairs atkārtoti neprasītu ievadīt pieteikšanās datus šim ekrānam.
   - **Do not prompt to add logons for logon screens** (Neprasīt pievienot pieteikšanās datus pieteikšanās ekrānam) — atlasiet radio pogu.

2. Lai pievienotu pieteikšanās datus ekrānam, kas iepriekš nav bijis iekļauts, rīkojieties šādi.

   **a.** Piesakieties tīmekļa vietnē, kura iepriekš nav bijusi iekļauta.

   **b.** Lai Password Manager atcerētos šīs vietnes paroli, uznirstošajā dialoglodziņā noklikšķiniet uz vai pieskarieties pie **Remember** (Atcerēties), lai saglabātu paroli un izveidotu pieteikšanās datus šim ekrānam.

3. Lai piekļūtu Password Manager papildu iestatījumiem, noklikšķiniet uz vai pieskarieties pie ikonas Password Manager, noklikšķiniet uz vai pieskarieties pie **Open Password Manager** (Atvērt Password Manager) un pēc tam Password Manager lapā noklikšķiniet uz vai pieskarieties pie **Settings** (Iestatījumi).

## Pieteikšanās datu importēšana un eksportēšana

HP Password Manager importa un eksporta lapā varat importēt pieteikšanās datus, kurus tīmekļa pārlūkprogrammas ir saglabājušas datorā. Varat importēt arī HP Client Security dublējuma failu un eksportēt datus uz HP Client Security dublējuma failu.

▲ Lai palaistu importa un eksporta lapu, Password Manager lapā noklikšķiniet uz vai pieskarieties pie **Import and export** (Imports un eksports).

Lai importētu paroles no pārlūkprogrammas, rīkojieties šādi.

1. Noklikšķiniet uz vai pieskarieties pie pārlūkprogrammas, no kuras vēlaties importēt paroles (redzamas ir tikai instalētās pārlūkprogrammas).
2. Notīriet izvēles rūtiņas visiem tiem kontiem, kuru paroles nevēlaties importēt.
3. Noklikšķiniet uz vai pieskarieties pie **Import** (Importēt).

Datu importēšanu no HP Client Security dublējuma faila vai datu eksportēšanu uz HP Client Security failu var veikt, izmantojot saistītās saites importa un eksporta lapā (**Other Options** (Citas opcijas)).

**PIEZĪME.** Šī funkcija importē un eksportē tikai Password Manager datus. Informāciju par papildu HP Client Security datu dublēšanu un atjaunošanu skatiet Datu dublēšana un atjaunošana 28. lpp..

Lai importētu datus no HP Client Security dublējuma faila, rīkojieties šādi.

1. HP Password Manager importa un eksporta lapā noklikšķiniet uz vai pieskarieties pie **Import data from an HP Client Security backup file** (Importēt datus no HP Client Security dublējuma faila).
2. Aplieciniet savu identitāti.

3. Atlasiet iepriekš izveidoto dublējuma failu vai ievadiet ceļu nodrošinātajā laukā un pēc tam noklikšķiniet uz vai pieskarieties pie **Browse** (Pārlūkot).
4. Ievadiet faila aizsardzībai lietoto paroli un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).
5. Noklikšķiniet uz vai pieskarieties pie **Restore** (Atjaunot).

Lai eksportētu datus HP Client Security dublējuma failā, rīkojieties šādi.

1. HP Password Manager importa un eksporta lapā noklikšķiniet uz vai pieskarieties pie **Eksport data from an HP Client Security backup file** (Eksportēt datus no HP Client Security dublējuma faila).
2. Aplieciniet savu identitāti un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).
3. Ievadiet dublējuma faila nosaukumu. Pēc noklusējuma šis fails tiks saglabāts jūsu mapē Documents (Dokumenti). Lai norādītu atšķirīgu atrašanās vietu, noklikšķiniet uz vai pieskarieties pie **Browse** (Pārlūkot).
4. Ievadiet un apstipriniet faila aizsardzībai lietoto paroli un pēc tam noklikšķiniet uz vai pieskarieties pie **Save** (Saglabāt).

### Iestatījumi

Varat norādīt iestatījumus Password Manager personalizēšanai.

- **Prompt to add logons for logon screens** (Prasīt pievienot pieteikšanās datus pieteikšanās ekrāniem) — ikona **Password Manager** ar plus zīmi ir redzama vienmēr, kad noteikts tīmekļa vietnes vai programmas pieteikšanās ekrāns, tā norādot, ka var pievienot pieteikšanās datus šim ekrānam izvēlnē **Logons** (Pieteikšanās dati).

  Lai atspējotu šo funkciju, notīriet izvēles rūtiņu līdzās opcijai **Prompt to add logons for logon screens** (Prasīt pievienot pieteikšanās datus pieteikšanās ekrāniem).

- **Open Password Manager with Ctrl+Win+h** (Atvērt Password Manager ar Ctrl+Win+h) — noklusējuma karstais taustiņš, kas atver izvēlni **Password Manager Quick Links** (Password Manager Ātrās saites) ir Ctrl+Windows taustiņš+h.

  Lai mainīto šo karsto taustiņu, noklikšķiniet uz vai pieskarieties pie šīs opcijas un pēc tam ievadiet jauno taustiņu kombināciju. Kombinācijas var ietvert vienu vai vairākus no šiem taustiņiem: ctrl, alt vai shift un jebkuru burtu vai ciparu taustiņu.

  Windows vai Windows lietojumprogrammu rezervētās kombinācijas nevar izmantot.

- Lai atgrieztos pie iestatījumiem ar rūpnīcas noklusējuma vērtībām, noklikšķiniet uz vai pieskarieties pie **Restore defaults** (Atjaunot noklusējuma iestatījumus).

# Uzlabotie iestatījumi

Administratori var piekļūt tālāk norādītajām opcijām, HP Client Security sākuma ekrānā atlasot **Gear** (Zobrats) (iestatījumu) ikonu.

- **Administrator Policies** (Administratoru politikas) — ļauj konfigurēt pieteikšanās un sesijas politikas administratoriem.
- **Standard User Policies** (Standarta lietotāju politikas) — ļauj konfigurēt pieteikšanās un sesijas politikas standarta lietotājiem.
- **Security Features** (Drošības līdzekļi) — ļauj palielināt datora drošību, aizsargājot Windows kontu ar stipru autentifikāciju un/vai iespējojot autentificēšanu pirms Windows palaišanas.

- **Users** (Lietotāji) — ļauj pārvaldīt lietotājus un viņu akreditācijas datus.
- **My Policies** (Manas politikas) — ļauj jums pārskatīt savas autentificēšanas politikas un reģistrēšanās statusu.
- **Backup and Restore** (Dublēšana un atjaunošana) — ļauj dublēt un atjaunot HP Client Security datus.
- **About HP Client Security** (Par HP Client Security) — parāda HP Client Security versijas informāciju.

## Administratoru politikas

Jūs varat konfigurēt šajā datorā pieteikšanās un sesijas politikas administratoriem. Šeit iestatītā pieteikšanās politika nosaka autentificēšanas datus, kuri vietējiem administratoriem ir nepieciešami, lai pieteiktos Windows. Šeit iestatītā sesijas politika nosaka autentificēšanas datus, kuri vietējiem administratoriem ir nepieciešami, lai pārbaudītu identitāti Windows sesijas laikā.

Pēc noklusējuma visas jaunās vai mainītās politikas stājas spēkā uzreiz pēc noklikšķināšanas uz vai pieskaršanās pie **Apply** (Lietot).

Lai pievienotu jaunu politiku, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie ikonas **Gear** (Zobrats).
2. Uzlaboto iestatījumu lapā noklikšķiniet uz vai pieskarieties pie **Administrator Policies** (Administratoru politikas).
3. Noklikšķiniet uz vai pieskarieties pie **Add new policy** (Pievienot jaunu politiku).
4. Noklikšķiniet uz lejupvērstajām bultiņām, lai atlasītu jaunās politikas primāros un (papildu) sekundāros autentificēšanas datus un pēc tam noklikšķiniet uz vai pieskarieties pie **Add** (Pievienot).
5. Noklikšķiniet uz **Lietot**.

Lai aizkavētu jaunās vai mainītās politikas stāšanos spēkā, rīkojieties šādi.

1. Noklikšķiniet uz vai pieskarieties pie **Enforce this policy immediately** (Ieviest šo politiku nekavējoties).
2. Atlasiet **Enforce this policy on the specific date** (Ieviest šo politiku no noteikta datuma).
3. Ievadiet datumu vai uznirstošajā kalendārā atlasiet datumu, kurā šo politiku vajadzētu ieviest.
4. Ja vajadzīgs, atlasiet, kad lietotājiem atgādināt par šo jauno politiku.
5. Noklikšķiniet uz **Lietot**.

## Standarta lietotāju politikas

Jūs varat konfigurēt šajā datorā pieteikšanās un sesijas politikas standarta lietotājiem. Šeit iestatītā pieteikšanās politika nosaka autentificēšanas datus, kuri standarta lietotājiem ir nepieciešami, lai pieteiktos Windows. Šeit iestatītā sesijas politika nosaka autentificēšanas datus, kuri standarta lietotājiem ir nepieciešami, lai pārbaudītu identitāti Windows sesijas laikā.

Pēc noklusējuma visas jaunās vai mainītās politikas stājas spēkā uzreiz pēc noklikšķināšanas uz vai pieskaršanās pie **Apply** (Lietot).

Lai pievienotu jaunu politiku, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie ikonas **Gear** (Zobrats).
2. Uzlaboto iestatījumu lapā noklikšķiniet uz vai pieskarieties pie **Standard User Policies** (Standarta lietotāju politikas).
3. Noklikšķiniet uz vai pieskarieties pie **Add new policy** (Pievienot jaunu politiku).
4. Noklikšķiniet uz lejupvērstajām bultiņām, lai atlasītu jaunās politikas primāros un (papildu) sekundāros autentificēšanas datus un pēc tam noklikšķiniet uz vai pieskarieties pie **Add** (Pievienot).
5. Noklikšķiniet uz **Lietot**.

Lai aizkavētu jaunās vai mainītās politikas stāšanos spēkā, rīkojieties šādi.

1. Noklikšķiniet uz vai pieskarieties pie **Enforce this policy immediately** (Ieviest šo politiku nekavējoties).
2. Atlasiet **Enforce this policy on the specific date** (Ieviest šo politiku no noteikta datuma).
3. Ievadiet datumu vai uznirstošajā kalendārā atlasiet datumu, kurā šo politiku vajadzētu ieviest.
4. Ja vajadzīgs, atlasiet, kad lietotājiem atgādināt par šo jauno politiku.
5. Noklikšķiniet uz **Lietot**.

# Drošības līdzekļi

Jūs varat iespējot HP Client Security drošības līdzekļus, kuri palīdz aizsargāt no nepilnvarotas piekļuves datoram.

Lai iestatītu drošības līdzekļus, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie ikonas **Gear** (Zobrats).
2. Uzlaboto iestatījumu lapā noklikšķiniet uz vai pieskarieties pie **Security Features** (Drošības līdzekļi).
3. Iespējojiet drošības līdzekļus, atlasot izvēles rūtiņas un pēc tam noklikšķiniet uz vai pieskarieties pie **Apply** (Lietot). Jo vairāk līdzekļu ir atlasīts, jo drošāks ir dators.

   Šie iestatījumi attiecas uz visiem lietotājiem.

   - **Windows Logon Security** (Windows pieteikšanās drošība) — aizsargā Windows, pieprasot lietot HP Client Security autentificēšanas datus piekļuvei.
   - **Pre-Boot Security (Power-on authentication)** (Pirmsāknēšanas drošība (Ieslēgšanas autentifikācija)) — aizsargā datoru pirms Windows palaišanas. Šī atlase nav iespējama, ja BIOS to neatbalsta.
   - **Allow One Step logon** (Atļaut pieteikšanos ar vienu soli) — šis iestatījums ļauj izlaist Windows pieteikšanos, ja iepriekš veikta autentificēšana ieslēgšanas autentifikācijas vai Drive Encryption līmenī.
4. Noklikšķiniet uz vai pieskarieties pie **Users** (Lietotāji) un pēc tam noklikšķiniet uz vai pieskarieties pie lietotāja elementa.

# Lietotāji

Varat uzraudzīt un pārvaldīt šī datora HP Client Security lietotājus.

Lai pievienotu vēl vienu Windows lietotāju lietotnei HP Client Security, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie ikonas **Gear** (Zobrats).
2. Uzlaboto iestatījumu lapā noklikšķiniet uz vai pieskarieties pie **Users** (Lietotāji).
3. Noklikšķiniet uz vai pieskarieties pie **Add another Windows user to HP Client Security** (Pievienot vēl vienu lietotāju lietotnei HP Client Security).
4. Ievadiet pievienojamā lietotāja vārdu un pēc tam noklikšķiniet uz vai pieskarieties pie **OK** (Labi).
5. Ievadiet šī lietotāja Windows paroli.

   Pievienotā lietotāja elements ir redzams lietotāju lapā.

Lai izdzēstu Windows lietotāju no HP Client Security, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie ikonas **Gear** (Zobrats).
2. Uzlaboto iestatījumu lapā noklikšķiniet uz vai pieskarieties pie **Users** (Lietotāji).
3. Noklikšķiniet uz vai pieskarieties pie izdzēšamā lietotāja vārda.
4. Noklikšķiniet uz vai pieskarieties pie **Delete User** (Dzēst lietotāju) un pēc tam noklikšķiniet uz vai pieskarieties pie **Yes** (Jā), lai apstiprinātu.

Lai atvērtu lietotājam noteikto pieteikšanās un sesiju politiku kopsavilkumu, rīkojieties šādi.

- ▲ Noklikšķiniet uz vai pieskarieties pie **Users** (Lietotāji) un pēc tam noklikšķiniet uz vai pieskarieties pie lietotāja elementa.

# Manas politikas

Varat atvērt savas autentificēšanas politikas un reģistrēšanās statusu. Lapā Manas politikas dotas arī saites uz lapām Administratoru politikas un Standarta lietotāju politikas.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie ikonas **Gear** (Zobrats).
2. Uzlaboto iestatījumu lapā noklikšķiniet uz vai pieskarieties pie **My policies** (Manas politikas).

   Tiks parādītas tam lietotājam, kurš šajā brīdī ir pieteicies, noteiktās pieteikšanās un sesiju politikas.

Lapā Manas politikas ir dotas arī saites uz Administratoru politikas 26. lpp. un Standarta lietotāju politikas 26. lpp..

# Datu dublēšana un atjaunošana

Ieteicama regulāra HP Client Security datu dublēšana. Dublēšanas biežums ir atkarīgs no datu izmaiņu biežuma. Piemēram, ja jauni pieteikšanās dati tiek pievienoti katru dienu, tad datu dublēšana ir jāveic katru dienu.

Dublējumus var izmantot arī migrācijai starp datoriem. Šo procesu sauc arī par importēšanu un eksportēšanu.

**PIEZĪME.** Ar šīs funkcijas palīdzību tiek dublēts tikai Password Manager. Drive Encryption ir neatkarīga dublēšanas metode. Device Access Manager un autentifikācijas izmantojot pirksta nospiedumu dati netiek dublēti.

Pirms datu atjaunošanas no dublējuma faila HP Client Security ir jābūt instalētai jebkurā datorā, kas saņem dublētus datus.

Lai dublētu datus, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie ikonas **Gear** (Zobrats).
2. Uzlaboto iestatījumu lapā noklikšķiniet uz vai pieskarieties pie **Administrator Policies** (Administratoru politikas).
3. Noklikšķiniet uz vai pieskarieties pie **Backup and Restore** (Dublēt un atjaunot).
4. Noklikšķiniet uz vai pieskarieties pie **Backup** (Dublēt) un pēc tam aplieciniet savu identitāti.
5. Atlasiet moduli, kuru vēlaties iekļaut dublējumā, un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).
6. Ievadiet atmiņas faila nosaukumu. Pēc noklusējuma šis fails tiks saglabāts jūsu mapē Documents (Dokumenti). Lai norādītu atšķirīgu atrašanās vietu, noklikšķiniet uz vai pieskarieties pie **Browse** (Pārlūkot).
7. Ievadiet un apstipriniet paroli, lai aizsargātu failu.
8. Noklikšķiniet uz vai pieskarieties pie **Save** (Saglabāt).

Lai atjaunotu datus, rīkojieties šādi.

1. HP Client Security sākuma lapā noklikšķiniet uz vai pieskarieties pie ikonas **Gear** (Zobrats).
2. Uzlaboto iestatījumu lapā noklikšķiniet uz vai pieskarieties pie **Administrator Policies** (Administratoru politikas).
3. Noklikšķiniet uz vai pieskarieties pie **Backup and Restore** (Dublēt un atjaunot).
4. Atlasiet **Restore** (Atjaunot) un pēc tam aplieciniet savu identitāti.
5. Atlasiet iepriekš izveidoto atmiņas failu. Ievadiet ceļu tam nodrošinātajā laukā. Lai norādītu atšķirīgu atrašanās vietu, noklikšķiniet uz vai pieskarieties pie **Browse** (Pārlūkot).
6. Ievadiet faila aizsardzībai lietoto paroli un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).
7. Atlasiet moduļus, kuru datus vēlaties atjaunot.
8. Noklikšķiniet uz vai pieskarieties pie **Restore** (Atjaunot).

# 5 HP Drive Encryption (tikai atsevišķiem modeļiem)

HP Drive Encryption nodrošina pilnīgu datu aizsardzību, šifrējot datorā ierakstītos datus. Kad aktivizēts modulis Drive Encryption, jāpiesakās Drive Encryption pieteikšanās ekrānā, kurš ir redzams pirms Windows® operētājsistēmas palaišanas.

HP Client Security sākuma ekrāns ļauj Windows administratoriem aktivizēt Drive Encryption, dublēt šifrēšanas atslēgu un atlasīt vai atatlasīt šifrējamo(-os) disku(-us) vai nodalījumu(-us). Papildinformāciju skatiet HP Client Security programmatūras sadaļā Palīdzība.

Izmantojot Drive Encryption, var veikt tālāk norādītos uzdevumus.

- Drive Encryption iestatījumu atlasīšana
  - Atsevišķu disku vai nodalījumu šifrēšana vai atšifrēšana, izmantojot programmatūras šifrēšanu
  - Atsevišķu paššifrējošo disku šifrēšana vai atšifrēšana, izmantojot aparatūras šifrēšanu
  - Papildu drošības pievienošana, atspējojot miega vai gaidstāves režīmu, lai vienmēr tiktu pieprasīta Drive Encryption pirmsāknēšanas autentifikācija

**PIEZĪME.** Var šifrēt tikai iekšējos SATA un ārējos eSATA cietos diskus.

- Dublēšanas atslēgu izveidošana
- Piekļuves atkopšana šifrētam datoram, izmantojot dublēšanas atslēgas un HP SpareKey
- Drive Encryption pirmsāknēšanas autentifikācijas ar paroli, reģistrēto pirksta nospiedumu vai atlasīto viedkaršu PIN iespējošana

## Drive Encryption atvēršana

Administratori var piekļūt Drive Encryption, atverot HP Client Security.

1. Sākuma ekrānā noklikšķiniet uz lietotnes vai pieskarieties lietotnei **HP Client Security** (Windows 8).

   — vai —

   Windows darbvirsmas paziņojumu apgabalā veiciet dubultklikšķi uz vai dubultskārienu pie ikonas **HP Client Security**, kas atrodas uzdevumjoslas labajā pusē.

2. Noklikšķiniet uz vai pieskarieties pie ikonas **Drive Encryption**.

# Vispārējie uzdevumi

## Drive Encryption aktivizēšana standarta cietajiem diskiem

Standarta cietie diski ir šifrēti, izmantojot programmatūras šifrēšanu. Veiciet tālāk norādītās darbības, lai šifrētu disku vai diska nodalījumu.

1. Palaidiet **Drive Encryption**. Papildinformāciju skatiet sadaļā Drive Encryption atvēršana 30. lpp..
2. Atlasiet šifrējamā diska vai nodalījuma izvēles rūtiņu un pēc tam noklikšķiniet uz vai pieskarieties pie **Backup Key** (Dublēšanas atslēga).

**PIEZĪME.** Lai palielinātu drošību, atlasiet izvēles rūtiņu **Disable sleep mode for increased security** (Atspējot miega režīmu drošības palielināšanai). Kad miega režīms ir atspējots, nepastāv itin nekāds risks, ka diska atslēgšanai izmantotie akreditācijas dati ir saglabāti atmiņā.

3. Atlasiet vienu vai vairākas dublēšanas opcijas un pēc tam noklikšķiniet uz vai pieskarieties pie **Backup** (Dublēt). Papildinformāciju skatiet sadaļā Šifrēšanas atslēgu dublēšana 34. lpp.
4. Šifrēšanas atslēgas dublēšanas laikā varat turpināt darbu. Neatsāknējiet datoru.

**PIEZĪME.** Parādīsies uzvedne ar aicinājumu restartēt datoru. Pēc restartēšanas būs redzams diska šifrēšanas pirmsāknēšanas ekrāns, pieprasot autentifikāciju pirms Windows palaišanas.

Drive Encryption ir aktivizēta. Atkarībā no nodalījuma(-u) skaita un lieluma, atlasītā(-o) diska nodalījuma(-u) šifrēšana var notikt vairākas stundas.

Papildinformāciju skatiet HP Client Security programmatūras sadaļā Palīdzība.

## Drive Encryption aktivizēšana paššifrējošajiem cietajiem diskiem

Paššifrējošos diskus, kuri atbilst Trusted Computing Group paššifrējošo disku pārvaldības OPAL specifikācijai, var šifrēt, izmantojot vai nu programmatūras šifrēšanu, vai aparatūras šifrēšanu. Aparatūras šifrēšana ir daudz ātrāka nekā programmatūras šifrēšana. Tomēr nav iespējams izvēlēties, kuri diska nodalījumi tiks šifrēti. Šifrēts tiek viss disks, tostarp visi diska nodalījumi.

Lai šifrētu konkrētus nodalījumus, jāizmanto programmatūras šifrēšana. Neaizmirstiet notīrīt izvēles lodziņu **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Atļaut tikai paššifrējošo disku (SED) aparatūras šifrēšanu).

Veiciet tālāk norādītās darbības, lai aktivizētu Drive Encryption paššifrējošajiem diskiem.

1. Palaidiet **Drive Encryption**. Papildinformāciju skatiet sadaļā Drive Encryption atvēršana 30. lpp..
2. Atlasiet šifrējamā diska izvēles rūtiņu un pēc tam noklikšķiniet uz vai pieskarieties pie **Backup Key** (Dublēšanas atslēga).

**PIEZĪME.** Lai palielinātu drošību, atlasiet izvēles rūtiņu **Disable Sleep mode for added security** (Atspējot miega režīmu drošības palielināšanai). Kad miega režīms ir atspējots, nepastāv itin nekāds risks, ka diska atslēgšanai izmantotie akreditācijas dati ir saglabāti atmiņā.

3. Atlasiet vienu vai vairākas dublēšanas opcijas un pēc tam noklikšķiniet uz vai pieskarieties pie **Backup** (Dublēt). Papildinformāciju skatiet sadaļā Šifrēšanas atslēgu dublēšana 34. lpp..
4. Šifrēšanas atslēgas dublēšanas laikā varat turpināt darbu. Neatsāknējiet datoru.

**PIEZĪME.** Strādājot ar paššifrējošajiem diskiem parādīsies uzvedne ar aicinājumu izslēgt datoru.

Papildinformāciju skatiet HP Client Security programmatūras sadaļā Palīdzība.

## Drive Encryption deaktivizēšana

1. Palaidiet **Drive Encryption**. Papildinformāciju skatiet sadaļā Drive Encryption atvēršana 30. lpp..
2. Notīriet visu šifrēto disku izvēles rūtiņu un pēc tam noklikšķiniet uz vai pieskarieties pie **Apply** (Lietot).

   Sākas Drive Encryption deaktivizēšana.

**PIEZĪME.** Ja lietota programmatūras šifrēšana, sākas atšifrēšana. Atkarībā no šifrētā cietā diska nodalījuma(-u) lieluma, šifrēšana var notikt vairākas stundas. Kad atšifrēšana ir pabeigta, Drive Encryption ir deaktivizēta.

Ja lietota aparatūras šifrēšana, disks tiek automātiski atšifrēts un pēc dažām minūtēm Drive Encryption ir deaktivizēta.

Pēc Drive Encryption deaktivizēšanas parādās uzvedne ar aicinājumu izslēgt datoru, ja šifrēta aparatūra, vai restartēt datoru, ja šifrēta programmatūra.

## Reģistrācija pēc Drive Encryption aktivizēšanas

Pēc Drive Encryption aktivizēšanas un lietotāja konta reģistrēšanas ieslēdzot datoru, jāpiesakās Drive Encryption pieteikšanās ekrānā.

**PIEZĪME.** Kad notikusi aktivizēšana, kamēr dators atrodas miega vai gaidstāves režīmā, nav redzama Drive Encryption pirmsāknēšanas autentifikācija programmatūras šifrēšanai vai aparatūras šifrēšanai. Aparatūras šifrēšana nodrošina opciju **Disable sleep mode for increased security** (Atspējot miega režīmu drošības palielināšanai), kuras lietošanas laikā nenotiek datora pārslēgšanās miega vai gaidstāves režīmā.

Kad notikusi aktivizēšana, kamēr dators atrodas hibernācijas režīmā, nav redzama Drive Encryption pirmsāknēšanas autentifikācija ne programmatūras, ne aparatūras šifrēšanai.

**PIEZĪME.** Ja Windows administrators ir iespējojis BIOS pirmsāknēšanas drošību programmatūrā HP Client Security un ja ir iespējota pieteikšanās ar vienu soli (pēc noklusējuma), varat pieteikties datorā uzreiz pēc tā autentifikācijas BIOS pirmssāknēšanas laikā bez nepieciešamības veikt atkārtotu autentifikāciju Drive Encryption pieteikšanās ekrānā.

### Viena lietotāja pieteikšanās

- Lapā **Logon** (Pieteikšanās) ievadiet Windows paroli, viedkartes PIN, SpareKey vai novelciet ar reģistrēto pirkstu.

### Vairāku lietotāju pieteikšanās

1. Lapā **Select user to logon** (Tā lietotāja, kurš pieteiksies, atlasīšana) nolaižamajā sarakstā atlasiet lietotāju, kurš pieteiksies un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).
2. Lapā **Logon** (Pieteikšanās) ievadiet Windows paroli vai viedkartes PIN vai novelciet ar reģistrēto pirkstu.

**PIEZĪME.** Atbalstītas tiek šādas viedkartes:

### Atbalstītās viedkartes

- Gemalto Cyberflex Access 64k V2c

**PIEZĪME.** Ja atkopšanas atslēga ir lietota, lai pieteiktos Drive Encryption pieteikšanās ekrānā, piesakoties Windows ir nepieciešami papildu akreditācijas dati, lai piekļūtu lietotāju kontiem.

## Papildu cieto disku šifrēšana

Tiek ļoti ieteikts izmantot HP Drive Encryption datu aizsardzībai ar cietā diska šifrēšanas palīdzību. Pēc aktivizēšanas jebkurus pievienotos cietos diskus vai izveidotos nodalījumus var šifrēt, veicot tālāk norādītās darbības.

1. Palaidiet **Drive Encryption**. Papildinformāciju skatiet sadaļā Drive Encryption atvēršana 30. lpp..
2. Diskiem ar šifrētu programmatūru atlasiet šifrējamos diska nodalījumus.

**PIEZĪME.** Tas attiecas arī uz jauktu disku scenāriju, kur ir viens vai vairāki standarta cietie diski un viens vai vairāki paššifrējošie diski.

— vai —

- Diskiem ar šifrētu aparatūru atlasiet šifrējamo(-os) papildu disku(-us).

# Papildu uzdevumi

## Drive Encryption pārvaldīšana (administratora uzdevums)

Administratori var lietot Drive Encryption datora visu cieto disku šifrēšanas statusa (Nav šifrēts vai Šifrēts) apskatīšanai un mainīšanai.

- Ja statuss ir Iespējots, Drive Encryption ir aktivizēta un konfigurēta. Disks ir vienā no tālāk norādītajiem stāvokļiem.

### Programmatūras šifrēšana

- Nav šifrēts
- Šifrēts
- Notiek šifrēšana
- Notiek atšifrēšana

### Aparatūras šifrēšana

- Šifrēts
- Nav šifrēts (papildu diskiem)

## Atsevišķu diska nodalījumu šifrēšana vai atšifrēšana (tikai programmatūras šifrēšanai)

Administratori var lietot Drive Encryption datora cietā diska viena nodalījuma vai vairāku nodalījumu šifrēšanai vai jau šifrēta(-u) diska nodalījuma(-u) atšifrēšanai.

1. Palaidiet **Drive Encryption**. Papildinformāciju skatiet sadaļā Drive Encryption atvēršana 30. lpp..
2. Opcijā **Drive Status** (Diska statuss) atlasiet vai notīriet izvēles rūtiņu līdzās katram cietā diska nodalījumam, kuru vēlaties šifrēt vai atšifrēt, un pēc tam noklikšķiniet uz vai pieskarieties pie **Apply** (Lietot).

**PIEZĪME.** Pēc nodalījuma šifrēšanas vai atšifrēšanas tiek parādīta norises josla, kurā redzama nodalījuma atšifrētās daļas procentuālā vērtība.

**PIEZĪME.** Dinamiskie nodalījumi netiek atbalstīti. Ja nodalījums ir redzams kā pieejams, bet pēc atlasīšanas nevar tikt šifrēts, šis nodalījums ir dinamisks. Dinamisks nodalījums rodas, samazinot nodalījumu, lai izveidotu jaunu nodalījumu ar diska pārvaldības palīdzību.

Ja nodalījums tiks pārvērsts par dinamisko nodalījumu, parādās brīdinājums.

## Diska pārvaldība

- **Nickname** (Segvārds) — varat piešķirt diskiem un nodalījumiem vārdus to identificēšanas atvieglošanai.
- **Disconnected drives** (Atvienoti diski) — Drive Encryption var izsekot diskus, kas ir izņemti no datora. Disks, kas ir izņemts no datora, tiek automātiski pārvietots uz Atvienoto disku sarakstu. Ja disks ir pievienots atpakaļ sistēmai, tas atkal parādās Pievienoto disku sarakstā.
- Ja vairs nevajag izsekot vai pārvaldīt atvienoto disku, varat izņemt atvienoto disku no Atvienoto disku saraksta.
- Drive Encryption paliek aktīva, līdz notīrītas visu pievienoto disku izvēles rūtiņas un Atvienoto disku saraksts ir tukšs.

## Dublējums un atkopšana (administratora uzdevums)

Kad aktivizēta Drive Encryption, administratori var izmantot šifrēšanas atslēgas dublēšanas lapu, lai dublētu šifrēšanas atslēgas noņemamajiem datu nesējiem un veiktu atkopšanu.

### Šifrēšanas atslēgu dublēšana

Administratori var dublēt šifrētā diska šifrēšanas atslēgu noņemamajā atmiņas ierīcē.

**UZMANĪBU!** Saglabājiet drošā vietā atmiņas ierīci, kurā ir dublēšanas atslēga, jo ja aizmirsīsiet paroli, pazaudēsiet viedkarti vai jums nebūs reģistrēta pirksta nospieduma, šī ierīce nodrošinās vienīgo piekļuvi datoram. Šai glabāšanas vietai ir jābūt arī drošai, jo atmiņas ierīce atļauj piekļūt Windows.

1. Palaidiet **Drive Encryption**. Papildinformāciju skatiet sadaļā Drive Encryption atvēršana 30. lpp..
2. Atlasiet diska izvēles rūtiņu un pēc tam noklikšķiniet uz vai pieskarieties pie **Backup Key** (Dublēšanas atslēga).
3. Opcijā **Create HP Drive Encryption recovery key** (Izveidot HP Drive Encryption atkopšanas atslēgu) atlasiet vienu vai vairākas no tālāk norādītajām opcijām.
   - **Removable Storage** (Noņemama krātuve) — atlasiet izvēles rūtiņu un pēc tam atlasiet atmiņas krātuvi, kurā jāsaglabā šifrēšanas atslēga.
   - **SkyDrive** — atlasiet izvēles rūtiņu. Jābūt izveidotam savienojumam ar internetu. Piesakieties Microsoft SkyDrive un pēc tam noklikšķiniet uz vai pieskarieties pie **Yes** (Jā).

     **PIEZĪME.** Lai lietotu HP Drive Encryption dublēšanas atslēgu, kura ir saglabāta SkyDrive, to nepieciešams lejupielādēt no SkyDrive noņemamā atmiņas ierīcē un pēc tam ievietot atmiņas ierīcē šajā datorā.
   - **TPM** (tikai atlasītiem modeļiem) — ļauj atkopt datus, izmantojot TPM paroli.

**UZMANĪBU!** Ja TPM ir notīrīts vai dators ir bojāts, tiek zaudēta piekļuve dublējumam. Ja atlasīta šī metode, jābūt atlasītai arī citai dublēšanas metodei.

4. Noklikšķiniet uz vai pieskarieties pie **Backup** (Dublējums).

   Šifrēšanas atslēga ir saglabāta atlasītajā atmiņas ierīcē.

### Piekļuves atkopšana aktivizētam datoram izmantojot dublēšanas atslēgas

Administratori var veikt atkopšanu, izmantojot Drive Encryption atslēgu, kas, aktivizējot atlasot opciju **Backup Key** (Dublēšanas atslēga) programmatūrā Drive Encryption, ir dublēta noņemamā atmiņas ierīcē.

1. Ievietojiet noņemamo atmiņas ierīci, kurā ir jūsu dublēšanas atslēga.
2. Ieslēdziet datoru.
3. Kad tiek atvērts HP Drive Encryption pieteikšanās dialoglodziņš, noklikšķiniet uz vai pieskarieties pie **Recovery** (Atkopšana).
4. Ievadiet faila ceļu vai nosaukumu, kas ietver dublēšanas atslēgu, un pēc tam noklikšķiniet uz vai pieskarieties pie **Recovery** (Atkopšana).
5. Kad tiek atvērts apstiprinājuma dialoglodziņš, noklikšķiniet uz vai pieskarieties pie **OK** (Labi).

   Tiek atvērts Windows pieteikšanās ekrāns.

**PIEZĪME.** Ja atkopšanas atslēga ir lietota, lai pieteiktos Drive Encryption pieteikšanās ekrānā, piesakoties Windows, piekļuvei lietotāju kontiem ir nepieciešami papildu akreditācijas dati. Tiek ļoti ieteikts pēc atkopšanas atiestatīt paroli.

## HP SpareKey atkopšanas veikšana

Veicot SpareKey atkopšanu diska šifrēšanas pirmsāknēšanas laikā, pareizi jāatbild uz drošības jautājumiem un tikai pēc tam var piekļūt datoram. Papildinformāciju par HP SpareKey atkopšanas iestatīšanu skatiet HP Client Security programmatūras sadaļā Palīdzība.

Lai veiktu HP SpareKey atkopšanu, ja esat aizmirsis paroli, rīkojieties šādi.

1. Ieslēdziet datoru.
2. Kad redzama HP Drive Encryption lapa, navigējiet uz lietotāja pieteikšanās lapu.
3. Noklikšķiniet uz **SpareKey**.

**PIEZĪME.** Ja SpareKey nav inicializēta programmatūrā HP Client Security, poga **SpareKey** nav pieejama.

4. Ierakstiet pareizās atbildes uz redzamajiem jautājumiem un pēc tam noklikšķiniet uz **Logon** (Pieteikties).

   Tiek atvērts Windows pieteikšanās ekrāns.

**PIEZĪME.** Ja SpareKey ir lietota, lai pieteiktos Drive Encryption pieteikšanās ekrānā, piesakoties Windows, piekļuvei lietotāju kontiem ir nepieciešami papildu akreditācijas dati. Tiek ļoti ieteikts pēc atkopšanas atiestatīt paroli.

# 6 HP File Sanitizer (tikai atsevišķiem modeļiem)

File Sanitizer ļauj droši saplēst resursus (piemēram, personas informāciju vai failus, vēsturiskos vai ar tīmekli saistītos datus vai citus datu komponentus), kas atrodas datora iekšējā cietajā diskā, un periodiski notīrīt datora iekšējo cietu disku.

File Sanitizer nevar lietot tālāk norādīto veidu disku sanitizācijai vai notīrīšanai.

- Cietvielu diski (SSD), tostarp RAID sējumi, kas izvērš SSD ierīci
- Ārējie diski, kas pievienoti, izmantojot USB, Firewire vai eSATA interfeisu

Mēģinot veikt SSD esošo resursu saplēšanas vai notīrīšanas operāciju, tiek parādīts brīdinājuma ziņojums un šī operācija netiek veikta.

## Sasmalcināšana

Saplēšana atšķiras no Windows® standarta dzēšanas. Saplēšot kādu resursu ar File Sanitizer, faili tiek pārrakstīti ar bezjēdzīgiem datiem, padarot sākotnējā resursa izgūšanu virtuāli neiespējamu. Windows vienkāršā izdzēšana var atstāt failu (vai resursu) cietajā diskā neskartu vai tādā stāvoklī, kad to iespējams atkopt ar kriminālistikas metodēm.

Varat ieplānot saplēšanas izpildes laiku vai manuāli aktivizēt saplēšanu, HP Client Security sākuma ekrānā atlasot ikonu **File Sanitizer** vai uz Windows darbvirsmas lietojot ikonu **File Sanitizer**. Plašāku informāciju skatiet Saplēšanas grafika iestatīšana 38. lpp., Saplēšana ar labās pogas klikšķi 40. lpp. vai Saplēšanas operācijas manuāla sākšana 40. lpp..

**PIEZĪME.** .dll fails tiek saplēsts un sistēmā likvidēts tikai tad, ja tas ir pārvietots atkritnē.

## Brīvās vietas notīrīšana

Resursa izdzēšana operētājsistēmā Windows pilnīgi neizņem šī resursa saturu no cietā diska. Windows izdzēš tikai atsauci uz resursu vai tā atrašanās vietu cietajā diskā. Resursa saturs paliek cietajā diskā, līdz kāds cits resurss pārraksta to pašu cietā diska apgabalu ar jaunu informāciju.

Brīvās vietas notīrīšana ļauj droši ierakstīt nejauši izvēlētus datus virs izdzēstajiem resursiem, novēršot iespēju, ka lietotāji var skatīt dzēstā resursa sākotnējo saturu.

**PIEZĪME.** Brīvās vietas notīrīšana nodrošina saplēsto resursu papildu drošību.

Varat iestatīt saplēšanas izpildes laiku vai manuāli aktivizēt iepriekš saplēsto resursu brīvās vietas notīrīšanu, HP Client Security sākuma ekrānā atlasot ikonu **File Sanitizer** vai uz Windows darbvirsmas lietojot ikonu **File Sanitizer**. Plašāku informāciju skatiet Brīvās vietas notīrīšanas grafika iestatīšana 39. lpp., Brīvās vietas notīrīšanas manuāla sākšana 41. lpp. vai Ikonas File Sanitizer lietošana 40. lpp..

# HP File Sanitizer atvēršana

1. Sākuma ekrānā noklikšķiniet uz lietotnes vai pieskarieties lietotnei **HP Client Security** (Windows 8).

   — vai —

   Windows darbvirsmas paziņojumu apgabalā veiciet dubultklikšķi uz vai dubultskārienu pie ikonas **HP Client Security**, kas atrodas uzdevumjoslas labajā pusē.

2. Opcijā **Data** (Dati), noklikšķiniet uz vai pieskarieties pie **File Sanitizer**.

— vai —

▲ Uz Windows darbvirsmas veiciet dubultklikšķi vai dubultskārienu uz ikonas **File Sanitizer**.

— vai —

▲ Uz Windows darbvirsmas noklikšķiniet ar peles labo pogu uz ikonas vai pieskarieties un turiet ikonu **File Sanitizer** un pēc tam atlasiet **Open File Sanitizer** (Atvērt File Sanitizer).

# Iestatīšanas procedūras

**Shredding** (Saplēšana) — File Sanitizer droši izdzēš vai saplēš atlasītās resursu kategorijas.

1. Opcijā **Shredding** (Saplēšana) atlasiet izvēles rūtiņu katram saplēšamo failu veidam vai notīriet izvēles rūtiņu, ja nevēlaties, lai šie faili tiek saplēsti.

   - **Recycle Bin** (Atkritne) — saplēš visus atkritnē esošos failus.
   - **Temporary system files** (Pagaidu sistēmas faili) — saplēš visus failus, kas atrodas sistēmas pagaidu failu mapē. Tālāk redzamie vides mainīgie tiek meklēti norādītajā secībā, un pirmais atrastais ceļš tiek uzskatīts par sistēmas mapi.
     - TMP
     - TEMP
   - **Temporary Internet files** (Pagaidu interneta faili) — saplēš tīmekļa lapu, attēlu un datu nesēju kopijas, kas saglabātas tīmekļa pārlūkprogrammās ātrākai to skatīšanai.
   - **Cookies** (Sīkfaili) — saplēš visus failus, kurus datorā saglabājušas tīmekļa vietnes, lai saglabātu preferences, piemēram, pieteikšanās informāciju.

2. Lai sāktu saplēšanu, noklikšķiniet uz vai pieskarieties pie **Shred** (Saplēst).

**Bleaching** (Notīrīšana) — ieraksta nejauši izvēlētus datus brīvajā vietā un novērš izdzēsto objektu atkopšanu.

▲ Lai sāktu notīrīšanu, noklikšķiniet uz vai pieskarieties pie **Bleach** (Notīrīt).

**File Sanitizer Options** (File Sanitizer opcijas) — atlasiet izvēles rūtiņu, lai iespējotu katru no tālāk redzamajām opcijām, vai notīriet izvēles rūtiņu, lai atspējotu šo opciju.

- **Enable Desktop icon** (Darbvirsmas ikonas iespējošana) — parāda File Sanitizer ikonu uz darbvirsmas.
- **Enable right-click** (Labās pogas klikšķa iespējošana) — ļauj noklikšķināt ar peles labo pogu uz resursa vai pieskarties un turēt resursu un pēc tam atlasīt **HP File Sanitizer – Shred** (HP File Sanitizer — saplēšana).

- **Ask for Windows password before manual shredding** (Pirms manuālās saplēšanas prasīt Windows paroli) — pirms objekta manuālas saplēšanas pieprasa autentificēšanu, norādot Windows paroli.
- **Shred Cookies and Temporary Internet Files on browser close** (Sīkfailu un pagaidu interneta failu saplēšana pārlūkprogrammas aizvēršanas laikā) — saplēš visus atlasītos ar tīmekli saistītos resursus, piemēram, pārlūkprogrammas URL vēsturi, aizverot tīmekļa pārlūkprogrammu.

## Saplēšanas grafika iestatīšana

Varat iestatīt laiku, kad saplēšana notiek automātiski, vai arī resursus laiku pa laikam saplēst manuāli. Papildinformāciju skatiet sadaļā Iestatīšanas procedūras 37. lpp..

1. Atveriet File Sanitizer un pēc tam noklikšķiniet uz vai pieskarieties pie **Settings** (Iestatījumi).
2. Lai ieplānotu atlasīto resursu saplēšanu, opcijā **Shred Schedule** (Saplēšanas grafiks) atlasiet biežumu **Never** (Nekad), **Once** (Vienreiz), **Daily** (Katru dienu), **Weekly** (Katru nedēļu) vai **Monthly** (Katru mēnesi) un pēc tam atlasiet dienu un laiku.
   a. Noklikšķiniet uz vai pieskarieties pie stundu, minūšu vai AM/PM lauka.
   b. Ritiniet, līdz vēlamā vērtība ir redzama vienā līmenī ar citiem laukiem.
   c. Noklikšķiniet uz vai pieskarieties pie baltstarpas, kas ir laika iestatījumu lauku abās pusēs.
   d. Atkārtojiet šo darbību ar visiem laukiem, līdz atlasīts pareizs grafiks.
3. Norādīti šādi četri resursu tipi.
   - **Recycle Bin** (Atkritne) — saplēš visus atkritnē esošos failus.
   - **Temporary system files** (Pagaidu sistēmas faili) — saplēš visus failus, kas atrodas sistēmas pagaidu failu mapē. Tālāk redzamie vides mainīgie tiek meklēti norādītajā secībā, un pirmais atrastais ceļš tiek uzskatīts par sistēmas mapi.
     - TMP
     - TEMP
   - **Temporary Internet files** (Pagaidu interneta faili) — saplēš tīmekļa lapu, attēlu un datu nesēju kopijas, kas saglabātas tīmekļa pārlūkprogrammās ātrākai to skatīšanai.
   - **Cookies** (Sīkfaili) — saplēš visus failus, kurus datorā saglabājušas tīmekļa vietnes, lai saglabātu preferences, piemēram, pieteikšanās informāciju.

   Ja šie resursi ir atzīmēti, tie tiks saplēsti ieplānotajā laikā.
4. Lai saplēšanai atlasītu pielāgotus papildu resursus, rīkojieties šādi.
   a. Opcijā **Scheduled Shred List** (Saplēšamo resursu saraksts) noklikšķiniet uz vai pieskarieties pie **Add folder** (Pievienot mapi) un pēc tam navigējiet līdz šim failam vai mapei.
   b. Noklikšķiniet uz vai pieskarieties pie **Open** (Atvērt) un pēc tam noklikšķiniet uz vai pieskarieties pie **OK** (Labi).

   Lai izņemtu resursu no Saplēšamo resursu saraksta, notīriet šī resursa izvēles rūtiņu.

## Brīvās vietas notīrīšanas grafika iestatīšana

Brīvās vietas notīrīšana nodrošina saplēsto resursu papildu drošību.

1. Atveriet File Sanitizer un pēc tam noklikšķiniet uz vai pieskarieties pie **Settings** (Iestatījumi).
2. Lai ieplānotu cietā diska notīrīšanu, opcijā **Bleach Schedule** (Notīrīšanas grafiks) atlasiet biežumu **Never** (Nekad), **Once** (Vienreiz), **Daily** (Katru dienu), **Weekly** (Katru nedēļu) vai **Monthly** (Katru mēnesi) un pēc tam atlasiet dienu un laiku.
   a. Noklikšķiniet uz vai pieskarieties pie stundu, minūšu vai AM/PM lauka.
   b. Ritiniet, līdz vēlamais laiks ir redzams vienā līmenī ar citiem laukiem.
   c. Noklikšķiniet uz vai pieskarieties pie baltstarpas, kas ir laika iestatījumu lauku abās pusēs.
   d. Atkārtojiet, līdz atlasīts pareizs grafiks.

**PIEZĪME.** Brīvās vietas notīrīšanas operācija var prasīt ilgu laiku. Pārliecinieties, vai dators ir pievienots maiņstrāvas avotam. Kaut arī brīvās vietas notīrīšana notiek fonā, paaugstinātā procesora lietošana var ietekmēt datora veiktspēju. Brīvās vietas notīrīšanu var veikt pēc parastā darbalaika beigām vai tad, kad dators netiek lietots.

## Failu aizsargāšana no saplēšanas

Lai aizsargātu failus un mapes no saplēšanas, rīkojieties šādi.

1. Atveriet File Sanitizer un pēc tam noklikšķiniet uz vai pieskarieties pie **Settings** (Iestatījumi).
2. Opcijā **Never Shred List** (Nekad nesaplēšamo resursu saraksts) noklikšķiniet uz vai pieskarieties pie **Add folder** (Pievienot mapi) un pēc tam navigējiet līdz šim failam vai mapei.
3. Noklikšķiniet uz vai pieskarieties pie **Open** (Atvērt) un pēc tam noklikšķiniet uz vai pieskarieties pie **OK** (Labi).

**PIEZĪME.** Šajā sarakstā iekļautie faili būs aizsargāti tik ilgi, kamēr tie atradīsies šajā sarakstā.

Lai izņemtu resursu no izņēmumu saraksta, notīriet šī resursa izvēles rūtiņu.

# Vispārējie uzdevumi

Lietojiet File Sanitizer tālāk norādīto uzdevumu veikšanai.

- **Lietojiet File Sanitizer ikonu saplēšanas iniciēšanai** — aizvelciet failus uz ikonu **File Sanitizer** uz Windows darbvirsmas. Papildinformāciju skatiet Ikonas File Sanitizer lietošana 40. lpp..
- **Manuāli saplēsiet kādu konkrētu resursu vai visus atlasītos resursus** — jebkurā brīdī saplēsiet objektus, negaidot ieplānoto saplēšanas laiku. Papildinformāciju skatiet Saplēšanas operācijas manuāla sākšana 40. lpp. vai Saplēšana ar labās pogas klikšķi 40. lpp..
- **Manuāli aktivizējiet brīvās vietas notīrīšanu** — jebkurā brīdī aktivizējiet brīvās vietas notīrīšanu. Papildinformāciju skatiet Brīvās vietas notīrīšanas manuāla sākšana 41. lpp..
- **Skatiet žurnālfailus** — skatiet saplēšanas un brīvās vietas notīrīšanas žurnālfailus, kuros norādītas pēdējās saplēšanas vai brīvās vietas notīrīšanas laikā radušās kļūdas vai kļūmes. Papildinformāciju skatiet Žurnālfailu skatīšana 41. lpp..

**PIEZĪME.** Saplēšana vai brīvās vietas notīrīšana var prasīt ilgu laiku. Kaut arī saplēšana un brīvās vietas notīrīšana notiek fonā, paaugstinātā procesora lietošana var ietekmēt datora veiktspēju.

## Ikonas File Sanitizer lietošana

⚠ **UZMANĪBU!** Sasmalcinātie līdzekļi nav atkopjami. Uzmanīgi apsveriet, kurus objektus atlasīt manuālai saplēšanai.

Sākot saplēšanas operāciju manuāli, tiek saplēsti standarta saplēšamo resursu sarakstā iekļautie resursi File Sanitizer skatā (skat. Iestatīšanas procedūras 37. lpp.).

Varat sākt saplēšanas operāciju manuāli vienā no šiem veidiem.

1. Atveriet File Sanitizer (skat. HP File Sanitizer atvēršana 37. lpp.) un pēc tam noklikšķiniet uz vai pieskarieties pie **Shred** (Saplēst).
2. Kad tiek atvērts apstiprinājuma dialoglodziņš, pārliecinieties, vai ir atzīmēti saplēšamie resursi un pēc tam noklikšķiniet uz vai pieskarieties pie **OK** (Labi).

— vai —

1. Uz Windows darbvirsmas noklikšķiniet ar peles labo pogu uz ikonas vai pieskarieties un turiet ikonu **File Sanitizer** un pēc tam noklikšķiniet uz vai pieskarieties pie **Shred Now** (Saplēst tūlīt).
2. Kad tiek atvērts apstiprinājuma dialoglodziņš, pārliecinieties, vai ir atzīmēti saplēšamie resursi un pēc tam noklikšķiniet uz vai pieskarieties pie **Shred** (Saplēst).

## Saplēšana ar labās pogas klikšķi

⚠ **UZMANĪBU!** Sasmalcinātie līdzekļi nav atkopjami. Uzmanīgi apsveriet, kurus objektus atlasīt manuālai saplēšanai.

Ja File Sanitizer skatā ir atlasīta opcija **Enable right-click shredding** (Iespējot saplēšanu ar labās pogas klikšķi), varat saplēst resursu, rīkojieties šādi.

1. Navigējiet līdz saplēšamajam dokumentam vai mapei.
2. Noklikšķiniet ar peles labo pogu uz faila vai mapes vai pieskarieties un pieturiet failu vai mapi un pēc tam atlasiet **HP File Sanitizer – Shred** (HP File Sanitizer — saplēšana).

## Saplēšanas operācijas manuāla sākšana

⚠ **UZMANĪBU!** Sasmalcinātie līdzekļi nav atkopjami. Uzmanīgi apsveriet, kurus objektus atlasīt manuālai saplēšanai.

Sākot saplēšanas operāciju manuāli, tiek saplēsti standarta saplēšamo resursu sarakstā iekļautie resursi File Sanitizer skatā (skat. Iestatīšanas procedūras 37. lpp.).

Varat sākt saplēšanas operāciju manuāli vienā no šiem veidiem.

1. Atveriet File Sanitizer (skat. HP File Sanitizer atvēršana 37. lpp.) un pēc tam noklikšķiniet uz vai pieskarieties pie **Shred** (Saplēst).
2. Kad tiek atvērts apstiprinājuma dialoglodziņš, pārliecinieties, vai ir atzīmēti saplēšamie resursi un pēc tam noklikšķiniet uz vai pieskarieties pie **OK** (Labi).

— vai —

1. Uz Windows darbvirsmas noklikšķiniet ar peles labo pogu uz ikonas vai pieskarieties un turiet ikonu **File Sanitizer** un pēc tam noklikšķiniet uz vai pieskarieties pie **Shred Now** (Saplēst tūlīt).
2. Kad tiek atvērts apstiprinājuma dialoglodziņš, pārliecinieties, vai ir atzīmēti saplēšamie resursi un pēc tam noklikšķiniet uz vai pieskarieties pie **Shred** (Saplēst).

## Brīvās vietas notīrīšanas manuāla sākšana

Sākot notīrīšanas operāciju manuāli, tiek notīrīti standarta saplēšamo resursu sarakstā iekļautie resursi File Sanitizer skatā (skat. Iestatīšanas procedūras 37. lpp.).

Varat sākt notīrīšanas operāciju manuāli vienā no šiem veidiem.

1. Atveriet File Sanitizer (skat. HP File Sanitizer atvēršana 37. lpp.) un pēc tam noklikšķiniet uz vai pieskarieties pie **Bleach** (Notīrīt).
2. Kad tiek atvērts apstiprinājuma dialoglodziņš, noklikšķiniet uz vai pieskarieties pie **OK** (Labi).

— vai —

1. Uz Windows darbvirsmas noklikšķiniet ar peles labo pogu uz ikonas vai pieskarieties un turiet ikonu **File Sanitizer** un pēc tam noklikšķiniet uz vai pieskarieties pie **Bleach Now** (Notīrīt tūlīt).
2. Kad tiek atvērts apstiprinājuma dialoglodziņš, noklikšķiniet uz vai pieskarieties pie **Bleach** (Notīrīt).

## Žurnālfailu skatīšana

Katru reizi, kad tiek veikta saplēšanas vai brīvās vietas notīrīšanas operācija, tiek ģenerēti jebkuru kļūdu vai kļūmju žurnālfaili. Žurnālfaili tiek vienmēr atjaunināti atbilstoši pēdējai saplēšanas vai brīvās vietas notīrīšanas operācijai.

**PIEZĪME.** Faili, kuri ir veiksmīgi saplēsti vai notīrīti, neparādās žurnālfailos.

Viens žurnālfails tiek izveidots saplēšanas operācijām un otrs žurnālfails — brīvās vietas notīrīšanas operācijām. Abi faili atrodas cietajā diskā šādas mapēs:

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

64 bitu sistēmās abi faili atrodas cietajā diskā šādas mapēs:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Lietotājvārds]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Lietotājvārds]*_DiskBleachLog.txt

# 7 HP Device Access Manager (tikai atsevišķiem modeļiem)

HP Device Access Manager kontrolē piekļuvi datiem, atspējojot datu pārsūtīšanas ierīces.

**PIEZĪME.** Device Acess Manager nekontrolē zināmas lietotāja interfeisa ierīces / ievades ierīces, piemēram, peli, tastatūru, skārienpaneli un pirkstu nospiedumu lasītāju. Papildinformāciju skatiet sadaļā Nepārvaldītas ierīces klases 45. lpp..

Windows® operētājsistēmas administratori lieto HP Device Access Manager, lai kontrolētu ierīču piekļuvi sistēmai un aizsargātu sistēmu no nesankcionētas piekļuves.

- Visiem lietotājiem ir izveidoti ierīču profili, lai definētu ierīces, kurām viņiem ir vai nav atļauts piekļūt.
- Just In Time Authentication (JITA) ļauj iepriekš definētiem lietotājiem veikt pašiem savu autentificēšanu, lai piekļūtu ierīcēm, kuriem bez tās piekļuve ir liegta.
- Administratoriem un uzticamajiem lietotājiem var nepiemērot Device Access Manager noteiktos ierīces piekļuves ierobežojumus, šīs personas pievienojiet ierīces administratoru grupai. Šīs grupas dalībnieki tiek pārvaldīti, izmantojot opciju Advanced Settings (Uzlabotie iestatījumi).
- Piekļuvi ierīcei var piešķirt vai aizliegt pēc lietotāju grupas vai atsevišķu lietotāju principa.
- Tādām ierīces klasēm kā CD-ROM diskdziņi un DVD diskdziņi var atsevišķi atļaut vai aizliegt lasīšanas piekļuvi un rakstīšanas piekļuvi.

HP Client Security iestatīšanas vednis automātiski konfigurē HP Device Access Manager ar šādiem iestatījumiem:

- Just In Time Authentication (JITA) noņemamais datu nesējs ir iespējots administratoriem un lietotājiem;
- ierīces politika atļauj pilnu piekļuvi citām ierīcēm.

## HP Device Access Manager atvēršana

1. Sākuma ekrānā noklikšķiniet uz lietotnes vai pieskarieties lietotnei **HP Client Security** (Windows 8).

   — vai —

   Windows darbvirsmas paziņojumu apgabalā veiciet dubultklikšķi uz vai dubultskārienu pie ikonas **HP Client Security**, kas atrodas uzdevumjoslas labajā pusē.

2. Vienumā **Device** (Ierīce), noklikšķiniet uz vai pieskarieties pie **Device Permissions** (Ierīces atļaujas).

   - Standarta lietotāji var redzēt savu pašreizējo piekļuvi ierīcēm (skat. Lietotāja skats 43. lpp.).
   - Administratori var skatīt un mainīt datorā konfigurēto piekļuvi ierīcēm noklikšķinot uz vai pieskaroties pie **Change** (Mainīt) un pēc tam ievadot administratora paroli (skat. Sistēmas skats 43. lpp.).

## Lietotāja skats

Kad atlasīta opcija **Device Permission** (Ierīces atļauja), redzams lietotāja skats. Atkarībā no politikas, standarta lietotāji un administratori var redzēt paši savu piekļuvi ierīču klasēm vai atsevišķām ierīcēm šajā datorā.

- **Current user** (Pašreizējais lietotājs) — redzams tā lietotāja vārds, kurš attiecīgajā brīdī ir pieteicies.
- **Device Class** (Ierīces klase) — redzami ierīču veidi.
- **Access** (Piekļuve) — redzama attiecīgajā brīdī konfigurētā piekļuve ierīču veidiem un norādītajām ierīcēm.
- **Duration** (Ilgums) — redzams laika limits piekļuvei CD/DVD-ROM diskdziņiem vai noņemamā diska diskdziņiem.
- **Settings** (Iestatījumi) — administratori var mainīt, kuru diskdziņu piekļuvi kontrolē Device Access Manager.

## Sistēmas skats

Sistēmas skatā administratori var atļaut vai aizliegt lietotāju grupai vai administratoru grupai piekļuvi ierīcēm šajā datorā.

▲ Administratori var piekļūt sistēmas skatam, noklikšķinot uz vai pieskaroties pie **Change** (Mainīt), ievadot administratora paroli un pēc tam atlasot vienu no tālāk norādītajām opcijām.

- **Device Access Manager** — lai ieslēgtu HP Device Access Manager ar ieslēgtu vai izslēgtu Just In Time Authentication, noklikšķiniet uz vai pieskarieties pie **On** (Ieslēgts) vai **Off** (Izslēgts).
- **Users and groups on this PC** (Lietotāji un grupas šajā datorā) — parāda lietotāju grupu vai administratoru grupu, kurai ir atļauta vai aizliegta piekļuve atlasītajām ierīces klasēm.
- **Device Class** (Ierīces klase) — parāda ierīces klases un ierīces, kuras ir tagad instalētas vai var būt bijušas iepriekš instalētas sistēmā. Lai izvērstu sarakstu, noklikšķiniet uz ikonas **+**. Redzamas visas datoram pievienotās ierīces, un administratoru un lietotāju grupas ir izvērstas, lai parādītu viņu dalību. Lai atsvaidzinātu ierīču sarakstu, noklikšķiniet uz apaļās bultiņas (atsvaidzināšanas) ikonas.
  - Aizsardzība parasti tiek piemērota pa ierīces klasēm. Ja piekļuve ir iestatīta kā **Allow** (Atļaut), atlasītais lietotājs vai grupa var piekļūt jebkurai ierīces klases ierīcei.
  - Aizsardzību var piemērot arī konkrētām ierīcēm.
  - Konfigurējiet Just In Time authentication (JITA), atļaujot atlasītajiem lietotājiem piekļūt DVD/CD-ROM diskdziņiem vai noņemamo disku diskdziņiem, pašiem sevi autentificējot. Papildinformāciju skatiet sadaļā JITA konfigurācija 44. lpp..
  - Atļaujiet vai aizliedziet piekļuvi citām ierīces klasēm, tādām kā noņemamie datu nesēji (piem., USB zibatmiņas diski), seriālie un paralēlie porti, Bluetooth® ierīces, modema ierīces, PCMCIA/ExpressCard ierīces, 1394 ierīces, pirkstu nospiedumu lasītājs un viedkaršu lasītājs. Ja pirkstu nospiedumu lasītājs un viedkaršu lasītājs ir aizliegti, tos var lietot kā autentificēšanas datus, bet nevar lietot sesijas politikas līmenī.

    **PIEZĪME.** Ja Bluetooth ierīces tiek lietotas kā autentificēšanas dati, Bluetooth ierīces piekļuvei nevajadzētu būt ierobežotai Device Access Manager politikā.
  - Kad, atlasot iestatījumu grupas vai ierīces klases līmenī, tiek prasīts, vai lietot šo iestatījumu bērnobjektiem:

**Yes** (Jā) — iestatījums tiek ģenerēts;

**No** (Nē) — iestatījums netiek ģenerēts.

- Zināmas ierīces klases, tādas kā DVD un CD-ROM, var vēl tālāk kontrolēt, atsevišķi atļaujot vai aizliedzot piekļuvi lasīšanas un rakstīšanas operācijām.

**PIEZĪME.** Administratoru grupu nevar pievienot lietotāju sarakstam.

- **Access** (Piekļuve) — noklikšķiniet uz vai pieskarieties pie lejupvērstās bultiņas un pēc tam atlasiet vienu no tālāk norādītajiem piekļuves veidiem, lai atļautu vai aizliegtu piekļuvi.
  - **Atļaut — pilna piekļuve**
  - **Atļaut — tikai lasīt**
  - **Allow – JITA Required** (Atļaut — nepieciešams JITA), papildinformāciju skatiet JITA konfigurācija 44. lpp..

    Ja atlasīts šis piekļuves veids, opcijā **Duration** (Ilgums) noklikšķiniet uz vai pieskarieties pie lejupvērstās bultiņas, lai atlasītu laika limitu.
  - **Aizliegt**
- **Duration** (Ilgums) —noklikšķiniet uz vai pieskarieties pie lejupvērstās bultiņas, lai atlasītu piekļuvi CD/DVD-ROM diskdziņiem vai noņemamā diska diskdziņiem (skatiet JITA konfigurācija 44. lpp.).

## JITA konfigurācija

JITA Configuration ļauj administratoriem skatīt un mainīt tos lietotāju un grupu sarakstus, kuriem atļauts piekļūt ierīcēm, lietojot Just In Time Authentication (JITA).

JITA iespējoti lietotāji var piekļūt zināmām ierīcēm, kuru **Device Class Configuration** (Ierīces klases konfigurācija) skatā izveidotā politika ir tikusi ierobežota.

JITA periodu var autorizēt noteiktam minūšu skaitam vai kā neierobežotu. Neierobežoti lietotāji var piekļūt ierīcei, sākot no sava autentificēšanās brīža līdz iziešanai no sistēmas.

Ja lietotājam ir piešķirts ierobežots JITA periods, vienu minūti pirms JITA perioda beigām lietotājam tiek jautāts, vai pagarināt piekļuvi. Tiklīdz lietotājs iziet no sistēmas vai cits lietotājs tajā piesakās, JITA periods beidzas. Kad lietotājs nākamajā reizē piesakās un mēģina piekļūt JITA iespējotai ierīcei, parādās uzvedne ar aicinājumu ievadīt akreditācijas datus.

JITA ir pieejams tālāk norādītajām ierīces klasēm.

- DVD/CD-ROM diskdziņi
- Noņemamo disku diskdziņi

### JITA politikas izveidošana lietotājam vai grupai

Administratori var ļaut lietotājiem vai grupām piekļūt ierīcēm, lietojot Just In Time Authentication (JITA).

1. Palaidiet **Device Access Manager** un pēc tam noklikšķiniet uz vai pieskarieties pie **Change** (Mainīt).
2. Atlasiet lietotāju vai grupu un pēc tam vienumā **Access** (Piekļuve) opcijai **Removable Disk drives** (Noņemamā diska diskdziņi) vai **DVD/CD-ROM drives** (DVD/CD-ROM diskdziņi) noklikšķiniet uz vai pieskarieties pie lejupvērstās bultiņas un pēc tam atlasiet **Allow – JITA Required** (Atļaut — nepieciešams JITA).
3. Opcijā **Duration** (Ilgums) noklikšķiniet uz vai pieskarieties pie lejupvērstās bultiņas, lai atlasītu JITA piekļuves laika periodu.

Lai tiktu lietots jaunais JITA iestatījums, lietotājam ir jāiziet un pēc tam vēlreiz jāpiesakās.

### JITA politikas atspējošana lietotājam vai grupai

Administratori var atspējot lietotāja vai grupas piekļuvi ierīcēm, lietojot Just In Time Authentication (JITA).

1. Palaidiet **Device Access Manager** un pēc tam noklikšķiniet uz vai pieskarieties pie **Change** (Mainīt).
2. Atlasiet lietotāju vai grupu un pēc tam vienumā **Access** (Piekļuve) opcijai **Removable Disk drives** (Noņemamā diska diskdziņi) vai **DVD/CD-ROM drives** (DVD/CD-ROM diskdziņi) noklikšķiniet uz vai pieskarieties pie lejupvērstās bultiņas un pēc tam atlasiet **Deny** (Aizliegt).

Kad lietotājs piesakās un mēģina piekļūt ierīcei, piekļuve ir aizliegta.

# Iestatījumi

Skats **Settings** (Iestatījumi) ļauj administratoriem skatīt un mainīt diskdziņus, kuru piekļuvi kontrolē Device Access Manager.

**PIEZĪME.** Device Access Manager jābūt iespējotam, kad ir konfigurēts disku burtu saraksts (skatiet Sistēmas skats 43. lpp.).

## Nepārvaldītas ierīces klases

HP Device Access Manager nepārvalda tālāk norādītās ierīces klases.

- Ievades/izvades ierīces
  - CD-ROM
  - Diska diskdzinis
  - Disketes kontrolleris (FDC)
  - Cietā diska kontrolleris (HDC)
  - Lietotāja interfeisa ierīces (HID) klase
  - Infrasarkanās lietotāja interfeisa ierīces
  - Peli
  - Vairākportu seriāla

- Tastatūra
- Plug and play (PnP) printeri
- Printeris
- Printera jauninājums

- strāva
  - Uzlabotas barošanas pārvaldības atbalsts
  - Akumulators
- Dažādi
  - Dators
  - Dekodētājs
  - Displejs
  - Intel® vienotais displeja draiveris
  - Legacard
  - Datu nesēja disks
  - Vides maiņa
  - Atmiņas tehnoloģija
  - Monitors
  - Daudzfunkciju
  - Tīkla klients
  - Tīkla pakalpojums
  - Tīkla pārv.
  - Procesors
  - SCSI adapteris
  - Drošības paātrinātājs
  - Drošības ierīces
  - Sistēma
  - Nezināms
  - Apjoms
  - Apjoma momentuzņēmums

# 8 HP Trust Circles

HP Trust Circles ir failu un dokumentu drošības lietojumprogramma, kurā apvienota mapju failu šifrēšana ar ērtu iespēju kopīgot dokumentus uzticamā lietotāju lokā. Šī lietojumprogramma šifrē failus, kuri ievietoti lietotāja norādītajās mapēs, un aizsargā tos uzticamajā lietotāju lokā. Pēc aizsardzības piemērošanas šos failus var lietot un koplietot tikai uzticamā lietotāju loka dalībnieki. Ja aizsargātu failu saņem kāds, kas nav šī loka dalībnieks, fails paliek šifrēts un nav iespējams piekļūt tā saturam.

## Trust Circles atvēršana

1. Sākuma ekrānā noklikšķiniet uz lietotnes vai pieskarieties lietotnei **HP Client Security**.

   — vai —

   Windows darbvirsmas paziņojumu apgabalā veiciet dubultklikšķi uz ikonas **HP Client Security**, kas atrodas uzdevumjoslas labajā pusē.

2. Vienumā **Data** (Dati), noklikšķiniet uz vai pieskarieties pie **Trust Circles**.

## Darba sākšana

E-pasta uzaicinājumu nosūtīšana un atbildēšana un šiem uzaicinājumiem ir iespējama divos veidos.

- **Using Microsoft® Outlook** (Microsoft® Outlook lietošana) — Trust Circles lietošana kopā ar Microsoft Outlook automatizē Trust Circle uzaicinājumu un citu Trust Circle lietotāju atbilžu apstrādi.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)** (Gmail, Yahoo, Outlook.com vai citu e-pasta pakalpojumu (SMTP) lietošana) — kad esat ievadījis savu vārdu, e-pasta adresi un paroli, Trust Circles izmanto jūsu e-pasta pakalpojumu, lai nosūtītu e-pasta ielūgumus dalībniekiem, kuri atlasīti tam, lai pievienotos jūsu uzticamajam lietotāju lokam.

Lai izveidotu savu pamatprofilu, rīkojieties, kā norādīts tālāk.

1. Ievadiet savu vārdu un e-pasta adresi un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).

   Jūsu vārds būs redzams visiem dalībniekiem, kurus esat uzaicinājis pievienoties savam uzticamo lietotāju lokam. E-pasta adrese tiek lietota, lai nosūtītu un saņemtu ielūgumus, kā arī atbildētu uz ielūgumiem.

2. Ievadiet e-pasta konta adresi un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).

   Tiek nosūtīts e-pasta pārbaudes ziņojums, lai pārliecinātos, ka e-pasta iestatījumi ir precīzi.

   **PIEZĪME.** Datoram ir jābūt savienotam ar tīklu.

3. Laukā **Trust Circle Name** (Trust Circle nosaukums), ievadiet uzticamo lietotāju loka nosaukumu un noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk).

4. Pievienojiet dalībniekus un mapes un pēc tam noklikšķiniet uz vai pieskarieties pie **Next** (Tālāk). Uzticamo dalībnieku loks ir izveidots ar visām atlasītajām mapēm un nosūta e-pasta uzaicinājumus visiem atlasītajiem dalībniekiem. Ja kaut kāda iemesla dēļ uzaicinājumu nevar

nosūtīt, tiek parādīts paziņojums. Dalībniekus var jebkurā laikā uzaicināt vēlreiz, skatā Trust Circle noklikšķinot uz **Your Trust Circles** (Jūsu Trust Circles) un pēc tam veicot dubultklikšķi uz vai dubultskārienu pie uzticamo lietotāju loka. Papildinformāciju skatiet sadaļā HP Trust Circles 48. lpp..

# HP Trust Circles

Varat izveidot uzticamo lietotāju loku sākotnējās iestatīšanas laikā pēc e-pasta adreses ievadīšanas vai arī skatā Trust Circle.

▲ Skatā Trust Circle noklikšķiniet uz vai pieskarieties pie **Create Trust Circle** (Izveidot Trust Circle) un pēc tam ievadiet šī uzticamo lietotāju loka nosaukumu.

- Lai pievienotu uzticamā lietotāju loka dalībniekus, noklikšķiniet uz ikonas vai pieskarieties ikonai **M+**, kas atrodas līdzās opcijai **Members** (Dalībnieki), un pēc tam izpildiet ekrānā redzamās instrukcijas.
- Lai pievienotu uzticamā lietotāju loka mapes, noklikšķiniet uz ikonas vai pieskarieties ikonai **+**, kas atrodas līdzās opcijai **Folders** (Mapes), un pēc tam izpildiet ekrānā redzamās instrukcijas.

## Mapju pievienošana uzticamo lietotāju lokam

### Mapju pievienošana jaunam uzticamo lietotāju lokam

- Uzticamo lietotāju loka izveidošanas laikā varat pievienot mapes, noklikšķinot uz ikonas vai pieskaroties ikonai **+**, kas atrodas līdzās opcijai **Folders** (Mapes), un pēc tam izpildot ekrānā redzamās instrukcijas.

  — vai —

- Windows Explorer noklikšķiniet ar peles labo pogu uz mapes vai pieskarieties un turiet mapi, kura attiecīgajā brīdī nav daļa no uzticamo lietotāju loka, atlasiet **Trust Circle** un pēc tam atlasiet **Create Trust Circle from Folder** (Izveidot Trust Circle no mapes).

**PADOMS.** Varat atlasīt vienu vai vairākas mapes.

### Mapju pievienošana jau esošam Trust Circle

- Skatā Trust Circle noklikšķiniet uz **Your Trust Circles** (Jūsu Trust Circles). veiciet dubultklikšķi uz vai dubultskārienu pie jau esošā uzticamo lietotāju loka, lai skatītu tam jau pievienotās mapes, noklikšķiniet uz ikonas vai pieskarieties ikonai **+**, kas atrodas līdzās opcijai **Folders** (Mapes) un pēc tam izpildiet ekrānā redzamās instrukcijas.

  — vai —

- Windows Explorer noklikšķiniet ar peles labo pogu uz mapes vai pieskarieties un turiet mapi, kura attiecīgajā brīdī nav daļa no uzticamo lietotāju loka, atlasiet **Trust Circle** un pēc tam atlasiet **Add to existing Trust Circle from Folder** (Pievienot esošajam Trust Circle no mapes).

**PADOMS.** Varat atlasīt vienu vai vairākas mapes.

Pēc mapes pievienošanas uzticamo lietotāju lokam Trust Circles automātiski šifrē mapi un tās saturu. Pēc visu failu šifrēšanas tiek parādīts paziņojums. Turklāt uz visu šifrēto mapju ikonām ir redzams arī zaļas slēdzenes simbols un mapēs esošo failu ikonas norāda, ka tie ir pilnīgi aizsargāti.

## Dalībnieku pievienošana uzticamo lietotāju lokam

Lai pievienotu dalībniekus uzticamo lietotāju lokam, jāveic trīs darbības.

1. **Uzaicināšana** — vispirms uzticamo lietotāju loka īpašnieks uzaicina dalībniekus. Uzaicinājuma e-pastu var nosūtīt vairākiem lietotājiem vai izplatīšanas sarakstiem/grupām.
2. **Apstiprināšana** — uzaicinātās personas saņem uzaicinājumu un nolemj, vai to apstiprināt vai noraidīt. Ja uzaicinātā persona pieņem uzaicinājumu, tiek nosūtīta e-pasta atbilde uzaicinātājam. Ja uzaicinājums ir nosūtīts grupai, katrs tās dalībnieks saņemt uzaicinājumu un nolemj, vai to apstiprināt vai noraidīt.
3. **Reģistrēšana** — noslēgumā, uzaicinātājam ir iespēja nolemt, vai pievienot dalībnieku uzticamo lietotāju lokam. Ja uzaicinātājs nolemj reģistrēt dalībnieku, uzaicinājuma saņēmējam tiek nosūtīts e-pasts ar atbildes apstiprinājumu. Uzaicinātājam un uzaicinājuma saņēmējam ir izvēles iespēja pārbaudīt uzaicināšanas procesa drošību. Uzaicinājuma saņēmējam ir redzams pārbaudes kods, kas viņam ir jānolasa pa tālruni uzaicinātājam. Pēc šī koda apstiprināšanas uzaicinātājs var nosūtīt pēdējo reģistrēšanas e-pastu.

**Dalībnieku pievienošana jaunam uzticamo lietotāju lokam**

▲ Uzticamo lietotāju loka izveidošanas laikā varat pievienot dalībniekus, noklikšķinot uz ikonas vai pieskaroties ikonai **M+**, kas atrodas līdzās opcijai **Members** (Dalībnieki), un pēc tam izpildot ekrānā redzamās instrukcijas.

- Ja lietojat Outlook, atlasiet kontaktpersonas no Outlook adrešu grāmatas un pēc tam noklikšķiniet uz **OK** (Labi).
- Ja lietojat citu e-pasta pakalpojumu, vai nu manuāli pievienojiet jaunas e-pasta adreses Trust Circle, vai arī izgūstiet tās no Trust Circle reģistrētās e-pasta adreses.

**Dalībnieku pievienošana jau esošam uzticamo lietotāju lokam**

▲ Skatā Trust Circle noklikšķiniet uz **Your Trust Circles** (Jūsu Trust Circles), veiciet dubultklikšķi uz vai dubultskārienu pie jau esošā uzticamo lietotāju loka, lai skatītu tā dalībniekus, noklikšķiniet uz ikonas vai pieskarieties ikonai **M+**, kas atrodas līdzās opcijai **Members** (Dalībnieki), un pēc tam izpildiet ekrānā redzamās instrukcijas.

- Ja lietojat Outlook, atlasiet kontaktpersonas no Outlook adrešu grāmatas un pēc tam noklikšķiniet uz **OK** (Labi).
- Ja lietojat citu e-pasta pakalpojumu, vai nu manuāli pievienojiet jaunas e-pasta adreses Trust Circle, vai arī izgūstiet tās no Trust Circle reģistrētās e-pasta adreses.

## Failu pievienošana uzticamo lietotāju lokam

Jūs varat pievienot failus uzticamo lietotāju lokam vienā no tālāk norādītajiem veidiem.

- Nokopējiet vai pārvietojiet failu esošā uzticamo lietotāju loka mapē.

  — vai —

- Windows Explorer noklikšķiniet ar peles labo pogu uz faila vai pieskarieties un turiet failu, kurš attiecīgajā brīdī nav šifrēts, atlasiet **Trust Circle** un pēc tam atlasiet **Encrypt** (Šifrēt). Tiks parādīta uzvedne ar aicinājumu atlasīt uzticamo lietotāju loku, kuram šis fails ir jāpievieno.

**PADOMS.** Varat atlasīt vienu vai vairākus failus.

## Šifrētas mapes

Ikviens uzticamo lietotāju loka dalībnieks var skatīt un rediģēt sava uzticamo lietotāja loka failus.

**PIEZĪME.** Trust Circle pārvaldnieks/lasītājs nesinhronizē dažādu lietotāju failus.

Failu kopīgošanai jāizmanto pieejamie līdzekļi, tādi kā e-pasts, ftp vai mākoņkrātuves pakalpojumu sniedzēji. Uzticamo lietotāju loka mapē iekopētie, pārvietotie vai izveidotie faili ir nekavējoties aizsargāti.

## Mapju izņemšana no uzticamo lietotāju loka

Mapes izņemšana no uzticamo lietotāju loka atšifrē mapi un visu tās saturu un noņem to aizsardzību.

- Skatā Trust Circle noklikšķiniet uz **Your Trust Circles** (Jūsu Trust Circles), veiciet dubultklikšķi uz vai dubultskārienu pie jau esošā lietotāju loka, lai skatītu tā mapes, un pēc tam noklikšķiniet uz ikonas vai pieskarieties ikonai **trash can** (atkritne).

  — vai —

- Windows Explorer noklikšķiniet ar peles labo pogu uz mapes vai pieskarieties un turiet mapi, kura attiecīgajā brīdī ir daļa no uzticamo lietotāju loka, atlasiet **Trust Circle** un pēc tam atlasiet **Remove from Trust Circle** (Izņemt no Trust Circle).

**PADOMS.** Varat atlasīt vienu vai vairākas mapes.

## Faila izņemšana no uzticamo lietotāju loka

Lai izņemtu failu no uzticamo lietotāju loka, Windows Explorer noklikšķiniet ar peles labo pogu uz faila vai pieskarieties un turiet failu, kas attiecīgajā brīdī nav šifrēts, atlasiet **Trust Circle** un atlasiet **Decrypt File** (Atšifrēt failu).

## Dalībnieku izņemšana no uzticamo lietotāju loka

Pilnīgi reģistrētu dalībnieku nevar izņemt no uzticamo lietotāju loka. Alternatīvs risinājums ir izveidot citu uzticamo lietotāju loku ar visiem pārējiem dalībniekiem, pārvietot visus failus un mapes uz jauno uzticamo lietotāju loku un izdzēst veco lietotāju loku. Tādējādi šis dalībnieks nevarēs piekļūt jauniem failiem, tomēr šim vecā uzticamo lietotāju loka dalībniekam vēl arvien būs pieejami visi iepriekš kopīgotie materiāli.

Ja dalībnieks nav pilnīgi reģistrēts (šis dalībnieks ir vai nu tikai uzaicināts pievienoties, vai arī nav pieņēmis uzaicinājumu pievienoties uzticamo lietotāju lokam), varat izņemt šo dalībnieku no uzticamo lietotāju loka vienā no tālāk norādītajiem veidiem.

- Skatā Trust Circle noklikšķiniet uz vai pieskarieties pie **Your Trust Circles** (Jūsu Trust Circles) un pēc tam veiciet dubultklikšķi uz vai dubultskārienu pie uzticamo lietotāju loka, lai tiktu rādīts pašreizējais dalībnieku saraksts. Noklikšķiniet uz ikonas vai pieskarieties pie ikonas **trash can**, kas atrodas līdzās izņemamā dalībnieka vārdam.
- Skatā Trust Circle noklikšķiniet uz vai pieskarieties pie **Members** (Dalībnieki) un pēc tam veiciet dubultklikšķi uz vai dubultskārienu pie dalībnieka, lai parādītu uzticamo lietotāju lokus, kuros viņš ietilpst. Noklikšķiniet uz ikonas vai pieskarieties pie ikonas **trash can** (atkritne), kas atrodas līdzās uzticamo lietotāju lokam, lai izņemtu dalībnieku no šī uzticamo lietotāju loka.

## Uzticamo lietotāju loka dzēšana

Lai izdzēstu uzticamo lietotāju loku, vajadzīgas īpašumtiesības.

▲ Skatā Trust Circle noklikšķiniet uz vai pieskarieties pie **Your Trust Circles** (Jūsu Trust Circles), noklikšķiniet uz ikonas vai pieskarieties ikonai **trash can** (atkritne), kas atrodas līdzās izdzēšamajam uzticamo lietotāju lokam.

Tas izdzēš uzticamo lietotāju loku no lapas un nosūta e-pastu visiem šī uzticamo lietotāju loka dalībniekiem, informējot par uzticamo lietotāju loka dzēšanu. Visi šajā uzticamo lietotāju lokā ietvertie faili un mapes tiek atšifrēti.

# Preferenču iestatīšana

Skatā Trust Circle noklikšķiniet uz vai pieskarieties pie **Preferences** (Preferences). Būs redzamas trīs cilnes.

- **E-pasta iestatījumi**

| Opcija | Apraksts |
|---|---|
| **Lietotājvārds** | Redzams dotajā brīdī izmantotais lietotājvārds. Lai to mainītu, ievadiet jaunu lietotājvārdu tekstlodziņā. Izmaiņas tiek automātiski saglabātas, |
| **E-pasta adrese** | Redzams dotajā brīdī izmantotais e-pasta konts. Lai to mainītu, noklikšķiniet uz vai pieskarieties pie **Change Email Settings** (Mainīt e-pasta iestatījumus) un izpildiet ekrānā redzamās instrukcijas. |
| **Jauna dalībnieka apstiprinājums** | Atlasiet kādu no tālāk minētajām opcijām.<br>◦ **Confirm Automatically** (Apstiprināt automātiski) — pēc katras uzaicinātās personas piekrišanas saņemšanas šī persona bez jebkādas manuālas ievades palīdzības tiek apstiprināta kā pievienota uzticamo lietotāju lokam un uzaicinātajai personai tiek nosūtīts apstiprinājuma e-pasts.<br>◦ **Confirm Manually** (Apstiprināt manuāli) — pēc katras uzaicinātās personas piekrišanas saņemšanas nepieciešama manuāla ievade, lai reģistrētu šo jauno dalībnieku uzticamo lietotāju lokā un pēc tam šai uzaicinātajai personai tiek nosūtīts apstiprinājuma e-pasts.<br>◦ **Require Verification** (Pieprasīt apstiprinājumu) — pēc katras uzaicinātās personas piekrišanas saņemšanas pirms pilnīgas šīs personas reģistrēšanas tiek pieprasīts apstiprinājuma kods. Uzticamo lietotāju loka īpašniekam ir jāsazinās ar uzaicinātajām personām un jāsaņem no viņām pārbaudes kods. Pēc pareizā koda ievadīšanas tiek nosūtīti apstiprinājuma e-pasti. |
| **Periodiska autentificēšana** | Periodiska autentificēšana pieprasa, lai lietotājs pēc noteiktā (minūtēs reģistrētā) taimauta paiešanas un sensitīvu operāciju veikšanas laikā ievada Windows paroli. Šis iestatījums ļauj lietotājiem ieslēgt un izslēgt autentificēšanu. |
| **Autentificēšanas taimauts** | Pirms nepieciešamās autentificēšanas atlasiet norādīto (minūtēs reģistrēto) taimauta periodu. |
| **Nerādīt apstiprinājuma ziņojumu.** | Atlasiet izvēles rūtiņu, lai atspējotu apstiprinājuma ziņojumu rādīšanu, vai notīriet izvēles rūtiņu, lai rādītu apstiprinājuma ziņojumus. |
| **Es vēlētos palīdzēt uzlabot HP Trust Circle, izmantojot anonīmu lietojuma izsekošanu** | Atlasiet izvēles rūtiņu, lai piedalītos programmā, vai notīriet izvēles rūtiņu, ja nevēlaties piedalīties. |

- **Dublēšana/atjaunošana**

| Opcija | Apraksts |
| --- | --- |
| **Dublēšana** | Kopē Trust Circle pārvaldnieka/lasītāja lietojumprogrammas datus (iestatījumus un uzticamo lietotāju lokus) dublējuma failā. Avārijas vai sistēmas kļūmes gadījumā varat lietot šo failu, lai atjaunotu jauno Trust Circles instalāciju šajā failā saglabātajā stāvoklī.<br><br>**PIEZĪME.** Tiek saglabāti tikai jūsu Trust Circle lietojumprogrammas dati (uzticamo lietotāju loki, iestatījumi un dalībnieki). Uzticamo lietotāju loka reālās mapes netiek dublētas. Šie faili ir jādublē atsevišķi.<br><br>Lai dublētu Trust Circle iestatījumus un lietotāja datus, rīkojieties, kā norādīts tālāk.<br><br>**1.** Noklikšķiniet uz vai pieskarieties pie **Backup** (Dublējums).<br><br>**2.** Izvēlieties dublējuma faila nosaukumu un direktoriju un pēc tam noklikšķiniet uz vai pieskarieties pie **Save** (Saglabāt).<br><br>**3.** Ievadiet paroli, apstipriniet to un pēc tam noklikšķiniet uz vai pieskarieties pie **OK** (Labi). Šī parole būs vajadzīga faila atjaunošanai. |
| **Atjaunošana** | Atjauno iestatījumus un uzticamo lietotāju lokus no dublējuma faila. Parasti šī opcija tiek lietota pēc sistēmas kļūdas vai migrācijas uz citu datoru.<br><br>Lai atjaunotu Trust Circle pārvaldnieka iestatījumus un lietotāja datus, rīkojieties, kā norādīts tālāk.<br><br>**1.** Noklikšķiniet uz vai pieskarieties pie **Restore** (Atjaunot).<br><br>**2.** Navigējiet uz dublējuma faila direktoriju un faila nosaukumu un pēc tam noklikšķiniet uz vai pieskarieties pie **Open** (Atvērt).<br><br>**3.** Ievadiet dublējuma izveidošanas laikā iestatīto paroli. |

- **About** (Par) — norāda Trust Circle pārvaldnieka/lasītāja programmatūras versiju. Šeit norādītas saites, lai varētu veikt Trust Circle Manager jauninašanu uz Pro versiju vai skatīt HP paziņojumu par konfidencialitāti.

# 9 Atgūšana zādzības gadījumā (tikai atsevišķiem modeļiem)

CompuTrace (iegādājams atsevišķi) ļauj attāli uzraudzīt, pārvaldīt un izsekot datoru.

Pēc aktivizēšanas lietojumprogramma CompuTrace tiek konfigurēta no Absolute Software klientu centra. Klientu centrā administrators var konfigurēt CompuTrace uzraudzīt vai pārvaldīt datoru. Ja sistēma ir pazaudēta vai nozagta, klientu centrs var palīdzēt vietējām varas iestādēm atrast un atgūt datoru. Ja lietojumprogramma CompuTrace ir konfigurēta, tā var turpināt darboties pat pēc cietā diska izdzēšanas vai nomaiņas.

Lai aktivizētu CompuTrace, rīkojieties šādi.

1. Izveidojiet savienojumu ar internetu.
2. Atveriet HP Client Security. Papildinformāciju skatiet sadaļā HP Client Security atvēršana 9. lpp..
3. Noklikšķiniet uz **Theft Recovery** (Atgūšana zādzības gadījumā).
4. Lai palaistu CompuTrace aktivizācijas vedni, noklikšķiniet uz **Get Started** (Darba sākšana).
5. Ievadiet savu kontaktinformāciju un kredītkartes maksājuma datus vai ievadiet iepriekš nopirkto produkta atslēgu.

Aktivizācijas vednis droši apstrādās transakciju un izveidos jūsu lietotāja kontu Absolute Software klientu centra vietnē. Pēc tā pabeigšanas jūs saņemsiet apstiprinājuma e-pastu ar saviem klientu centra konta datiem.

Ja esat palaidis CompuTrace aktivizācijas vedni jau agrāk un jūsu klientu centra lietotāja konts ir jau izveidots, varat iegādāties papildu licences, sazinoties ar HP konta pārstāvi.

Lai pieteiktos klientu centrā, rīkojieties šādi.

1. Dodieties uz vietni https://cc.absolute.com/.
2. Laukos **Login ID** (Pieteikšanās ID) un **Password** (Parole) ievadiet apstiprinājuma e-pastā saņemtos autentificēšanās datus un pēc tam noklikšķiniet uz **Log in** (Pieteikties).

Izmantojot klientu centru, jūs varat:

- Uzraudzīt savus datorus.
- Aizsargāt savus attālos datus.
- Ziņot par jebkura ar CompuTrace aizsargāta datora zādzību.

▲ Noklikšķināt uz **Learn More** (Uzzināt vairāk), lai iegūtu papildinformāciju par CompuTrace.

# 10 Lokalizēto paroļu izņēmumi

Ieslēgšanas autentifikācijas līmenī un HP Drive Encryption līmenī paroļu lokalizācijas atbalsts ir ierobežots. Papildinformāciju skatiet sadaļā Windows IME nav atbalstīti ieslēgšanas autentifikācijas līmenī vai Drive Encryption līmenī 54. lpp..

## Rīcība gadījumā, ja noraidīta parole

Paroles var tikt noraidītas tālāk norādīto iemeslu dēļ.

- Lietotājs lieto neatbalstītu IME. Tā ir parasta problēma valodās, kurās tiek lietoti dubultbaiti (t.i. korejiešu, japāņu, ķīniešu valodā). Lai novērstu šo problēmu, rīkojieties šādi.
  1. Lietojot **Control Panel** (Vadības panelis), pievienojiet atbalstītu tastatūras izkārtojumu (pievienojiet ASV/angļu tastatūras zem ķīniešu ievades valodas opcijas).
  2. Iestatiet atbalstīto tastatūru noklusējuma ievadei.
  3. Palaidiet HP Client Security un pēc tam ievadiet Windows paroli.
- Lietotājs lieto neatbalstītu rakstzīmi. Lai novērstu šo problēmu, rīkojieties šādi.
  1. Mainiet Windows paroli tā, lai tajā būtu lietotas tikai atbalstītas rakstzīmes. Papildinformāciju par neatbalstītām rakstzīmēm skatiet Īpašo taustiņu lietošana 55. lpp..
  2. Palaidiet HP Client Security un pēc tam ievadiet Windows paroli.

## Windows IME nav atbalstīti ieslēgšanas autentifikācijas līmenī vai Drive Encryption līmenī

Windows operētājsistēmā lietotājs var izvēlēties IME (ievades metodes redaktoru), lai ievadītu sarežģītas rakstzīmes un simbolus, piemēram, japāņu un ķīniešu rakstzīmes, lietojot rietumu standarta tastatūru.

IME nav atbalstīti ieslēgšanas autentifikācijas vai Drive Encryption līmenī Windows paroli nevar ievadīt ar IME ieslēgšanas autentifikācijas vai HP Drive Encryption pieteikšanās ekrānā, un šāda rīcība var izraisīt lokautu. Dažos gadījumos Microsoft® Windows neparāda IME, kad lietotājs ievada paroli.

Risinājums ir ieslēgt vienu no tālāk norādītajiem atbalstītajiem tastatūras izkārtojumiem, kas pārvēršas par tastatūras izkārtojumu 00000411.

- Microsoft IME japāņu valodai
- Japāņu valodas tastatūras izkārtojums
- Office 2007 IME japāņu valodai — ja Microsoft vai kāda trešā puse lieto terminu IME vai ievades metodes redaktoru, reālā ievades metode var nebūt IME. Tas var radīt apjukumu, tomēr programmatūra nolasa heksadecimāla koda atveidojumu. Tādējādi, ja IME veic kartēšanu uz atbalstītu tastatūras izkārtojumu, HP Client Security var atbalstīt šo konfigurāciju.

⚠ **BRĪDINĀJUMS!** Kad izvietota lietotne HP Client Security, ar Windows IME ievadītās paroles tiek noraidītas.

# Paroles maiņa ar citu, bet arī atbalstītu tastatūras izkārtojumu

Ja parole ir sākotnēji iestatīta ar vienu tastatūras izkārtojumi, piemēram, ASV angļu valodas izkārtojumu (409) un pēc tam lietotājs nomaina paroli, lietojot citu, bet arī atbalstītu tastatūras izkārtojumu, piemēram, Latīņamerikas izkārtojumu (080A), paroles maiņa izdosies lietotnē HP Drive Encryption, bet neizdosies BIOS gadījumā, ja lietotājs izmanto rakstzīmes, kuras ir otrajā izkārtojumā, bet nav pirmajā izkārtojumā (piemēram, ē).

**PIEZĪME.** Administratori var atrisināt šo problēmu, izmantojot HP Client Security lietotāju lapu (kurai var piekļūt no ikonas **Gear** (Zobrats) sākumā lapā), lai izņemtu šo lietotāju no lietotnes HP Client Security, atlasot vēlamo tastatūras izkārtojumu operētājsistēmā un pēc tam vēlreiz palaižot HP Client Security iestatīšanas vedni tam pašam lietotājam. BIOS saglabā vēlamo tastatūras izkārtojumu un paroles, kuras var ierakstīt ar šo tastatūras izkārtojumu, tiks pareizi iestatītas BIOS.

Cita iespējamā problēma ir tādu dažādu tastatūras izkārtojumu lietošana, kas var radīt vienādas rakstzīmes. Piemēram, gan ar ASV starptautisko tastatūras izkārtojumu (20409), gan ar Latīņamerikas tastatūras izkārtojumu (080A) var uzrakstīt burtu é, tomēr tam var būt vajadzīga dažāda taustiņsitienu secība. Ja parole ir sākotnēji iestatīta ar Latīņamerikas tastatūras izkārtojumu, Latīņamerikas tastatūras izkārtojums ir iestatīts BIOS pat tad, ja parole ir vēlāk mainīta, lietojot ASV starptautisko tastatūras izkārtojumu.

# Īpašo taustiņu lietošana

- Ķīniešu, slovāku, Kanādas franču un čehu valoda

  Kad lietotājs atlasa vienu no iepriekšējiem tastatūras izkārtojumiem un pēc tam ievada paroli (piemēram, abcdef), tā pati parole ir jāievada, kamēr nospiests shift taustiņš mazajiem burtiem un shift taustiņš un caps lock taustiņš lielajiem burtiem ieslēgšanas autentifikācijas un HP Drive Encryption lietošanas laikā. No cipariem sastāvošas paroles ir jāievada ar ciparu papildtastatūru.

- Korejiešu valoda

  Kad lietotājs atlasa kādu atbalstītu korejiešu tastatūras izkārtojumu un pēc tam ievada paroli, tā pati parole ir jāievada, kamēr nospiests labais alt taustiņš mazajiem burtiem un labais alt taustiņš un caps lock taustiņš lielajiem burtiem ieslēgšanas autentifikācijas un HP Drive Encryption lietošanas laikā.

- Tālāk redzamajā tabulā ir norādītas neatbalstītās rakstzīmes.

| Language (Valoda) | Windows | BIOS | Drive Encryption |
|---|---|---|---|
| Arābu valoda | ﻻ, ﻷ un ﻹ taustiņi ģenerē divas rakstzīmes. | ﻻ, ﻷ un ﻹ taustiņi ģenerē vienu rakstzīmi. | ﻻ, ﻷ un ﻹ taustiņi ģenerē vienu rakstzīmi. |
| Kanādas franču valoda | ç, è, à un é, nospiežot caps lock, ir Ç, È, À, un É operētājsistēmā Windows. | ç, è, à un é, nospiežot caps lock, ir ç, è, à un é ieslēgšanas autentifikācijas laikā. | ç, è, à un é, nospiežot caps lock, ir ç, è, à un é HP Drive Encryption lietošanas laikā. |

| Language (Valoda) | Windows | BIOS | Drive Encryption |
|---|---|---|---|
| Spāņu valoda | 40a nav atbalstīts. Tomēr tas darbojas, jo programmatūra to konvertē par c0a. Taču, tā kā pastāv nelielas atšķirības starp tastatūras izkārtojumiem, spāņu valodā runājošajiem lietotājiem būtu ieteicams mainīt savu Windows tastatūras izkārtojumu uz 1040a (Spānijas variāciju) vai 080a (Latiņamerikas variāciju). | n/a | n/a |
| ASV starptautiskais izkārtojums | ◦ ¡, ¤, ‘, ’, ¥ un × taustiņi augšējā rindā ir noraidīti.<br>◦ å, ® un Þ taustiņi otrajā rindā ir noraidīti.<br>◦ á, ð un ø taustiņi trešajā rindā ir noraidīti.<br>◦ æ taustiņš apakšējā rindā ir noraidīts. | n/a | n/a |
| Čehu valoda | ◦ ğ taustiņš ir noraidīts.<br>◦ į taustiņš ir noraidīts.<br>◦ ų taustiņš ir noraidīts.<br>◦ ė, ı un ż taustiņi ir noraidīti.<br>◦ ģ, ķ, ļ, ņ un ţ taustiņi ir noraidīti. | n/a | n/a |
| Slovāku valoda | ż taustiņš ir noraidīts. | ◦ š, ś un ş taustiņi ir noraidīti, kad tiek rakstīti, bet tiek pieņemti, kad tie tiek ievadīti ar ekrāntastatūru.<br>◦ ţ diakritiskās zīmes taustiņš ģenerē divas rakstzīmes. | n/a |
| Ungāru valoda | ż taustiņš ir noraidīts. | ţ taustiņš ģenerē divas rakstzīmes. | n/a |
| Slovēņu valoda | žŽ taustiņš ir noraidīts operētājsistēmā Windows, un alt taustiņš ģenerē diakritiskās zīmes taustiņu BIOS. | ú, Ú, ů, Ů, ş, Ş, ś, Ś, š un Š taustiņi ir noraidīti BIOS. | n/a |
| Japāņu valoda | Kad pieejams Microsoft Office 2007 IME, tā ir labāka izvēle. Par spīti IME nosaukumam, īstenībā tiek atbalstīts tastatūras izkārtojums 411. | n/a | n/a |

# Vārdnīca

**administrators**
Skat. *Windows administrators*.

**akreditācijas dati**
īpaša informācija vai aparatūras ierīce, kas lietota atsevišķa lietotāja autenficēšanai.

**aktivizēšana**
Drive Encryption funkcijas būs pieejamas tikai pēc šī uzdevuma pabeigšanas. Administratori var aktivizēt Drive Encryption, lietojot HP Client Security iestatīšanas vedni vai HP Client Security. Aktivizācijas procesā ietilpst programmatūras aktivizācija, diska šifrēšana un sākotnējās dublējuma šifrēšanas atslēgas izveidošana noņemamajā atmiņas ierīcē.

**aparatūras šifrēšana**
Trusted Computing Group paššifrējošo disku pārvaldības OPAL specifikācijai atbilstošo paššifrējošo disku lietošana paššifrējošo disku pārvaldīšanai, lai varētu veikt tūlītēju šifrēšanu. Aparatūras šifrēšana ir tūlītēja, un tai var būt nepieciešamas tikai dažas minūtes, bet programmatūras šifrēšana var notikt vairākas stundas.

**atjaunošana**
Process, kas nokopē programmas informāciju no iepriekš saglabātā dublējuma faila šajā programmā.

**atsāknēšana**
Datora restartēšanas process.

**atšifrēšana**
Procedūra, kas tiek izmantota kriptogrāfijā, lai pārvērstu šifrētos datus par vienkāršu tekstu.

**autentifikācija**
verifikācijas process, kas tiek lietots, lai pārbaudītu, vai persona ir tā, par kuru uzdodas. Šī procesa laikā tiek lietoti akreditācijas dati, tostarp Windows parole, pirkstu nospiedums, viedkarte, bezkontakta karte un karte ar mikroshēmu.

**automātiska saplēšana**
programmatūrā File Sanitizer ieplānotā resursu saplēšana.

**ārkārtas atkopšanas arhīvs**
Aizsargāta krātuve, kas ļauj atkārtoti šifrēt vienkāršas lietotāja atslēgas no vienas platformas īpašnieka atslēgas uz citu.

**bezkontakta karte**
plastmasas karte ar datora mikroshēmu, kuru var lietot autentifikācijai.

**Bluetooth**
tehnoloģija, kura izmanto radiopārraidi, lai iespējotu datorus, printerus, peles, mobilos tālruņus un citas ierīces ar Bluetooth tehnoloģiju bezvadu sakariem nelielā attālumā.

**brīvās vietas notīrīšana**
nejauši izvēlētu datu uzrakstīšana virsū izdzēstajiem resursiem un neizmantotajai vietai. Šis process samazina iespēju, ka izdzēstais resurss var vēl arvien pastāvēt, padarot sākotnējā resursa atkopšanu daudz grūtāku.

**domēns**
Datoru grupa, kas ir daļa no tīkla un koplieto kopīgu direktorija datubāzi. Domēniem ir piešķirti unikāli nosaukumi, un katram no tiem ir kopēju noteikumu un procedūru kopa.

**Drive Encryption**

Aizsargā datus, šifrējot cieto(-os) disku(-us), padarot informāciju neizlasāmu tiem, kuri nav atbilstoši pilnvaroti.

**Drive Encryption pieteikšanās ekrāns**
skat. Drive Encryption pirmsāknēšanas autentifikācija.

**Drive Encryption pirmsāknēšanas autentifikācija**
pieteikšanās ekrāns, kas ir redzams pirms Windows palaišanas. Lietotājiem ir jāievada Windows lietotājvārds un parole vai viedkartes PIN vai jānovelk ar reģistrēto pirkstu. Ja atlasīta pieteikšanās ar vienu soli, pareizās informācijas ievadīšana Drive Encryption pieteikšanās ekrānā ļauj tieši piekļūt Windows bez nepieciešamības atkārtoti pieteikties Windows pieteikšanās ekrānā.

**DriveLock**
Drošības funkcija, kas sasaista cieto disku ar lietotāju un pieprasa, lai datora palaišanas laikā lietotājs ieraksta pareizu paroli.

**drošas pieteikšanās metode**
Metode, kas lietota, lai pieteiktos datorā.

**dublēšana**
dublēšanas līdzekļa lietošana programmas svarīgas informācijas kopijas saglabāšanai kādā vietā ārpus šīs programmas. Vēlāk to var izmantot šīs informācijas atjaunošanai tajā pašā vai citā datorā.

**Encryption File System (EFS)**
Sistēma, kas šifrē visus failus un apakšmapes atlasītajā mapē.

**grupa**
lietotāju grupa, uz kuras visiem dalībniekiem attiecas vienāds atļaujas vai aizlieguma līmenis lietot kādu ierīces klasi vai konkrētu ierīci.

**HP SpareKey atkopšana**
Iespēja piekļūt datoram, pareizi atbildot uz drošības jautājumiem.

**ID karte**
Windows darbvirsmas sīkrīks, kas palīdz vizuāli identificēt jūsu darbvirsmu ar jūsu lietotājvārdu un izvēlēto attēlu.

**Identitāte**
Modulī HP Client Security tā ir akreditācijas datu un iestatījumu grupa, kas izmantošanas laikā tiek pielīdzināta konkrētā lietotāja kontam vai profilam.

**ierīces klase**
visas īpaša tipa ierīces, piemēram, diskdziņi.

**ierīces piekļuves vadības politika**
to ierīču saraksts, kuram lietotājam ir atļauta vai aizliegta piekļuve.

**ieslēgšanas autentifikācija**
Drošības līdzeklis, kas, ieslēdzot datoru, pieprasa kaut kāda veida autentifikāciju, piemēram, viedkarti, drošības mikroshēmu vai paroli.

**Just In Time Authentication**
skat. HP Device Access Manager programmatūras palīdzības failu.

**karte ar mikroshēmu**
plastmasas karte, kurā ir datora mikroshēma un kuru var lietot autentifikācijai kopā ar citiem akreditācijas datiem papildu drošībai.

**lietotājs**
ikviens, kas ir reģistrējies Drive Encryption. Lietotājiem, kuri nav administratori, ir ierobežotas tiesības lietot Drive Encryption. Viņi var tikai reģistrēties (ar administratora apstiprinājumu) un pieteikties.

**manuāla saplēšana**

kāda resursa vai atlasīto resursu tūlītēja saplēšana, apejot plānoto saplēšanu.

**pieteikšanās**
HP Client Security objekts, kas sastāv no lietotājvārda un paroles (un iespējams arī citas atlasītas informācijas). ko var lietot, lai pieteiktos vietnēs un citās programmās.

**pievienotā ierīce**
aparatūras ierīce, kura ir pievienota datora portam.

**PIN**
reģistrētā lietotāja personīgais identifikācijas numurs, kas lietojams autentifikācijai.

**pirksta nospiedums**
pirksta nospieduma attēla digitāls izvilkums. Reālo pirkstu nospiedumu attēls nekad netiek saglabāts programmā HP Client Security.

**PKI**
Publiskās atslēgas infrastruktūras standarts, kas definē interfeisu sertifikātu un kriptogrāfisko atslēgu izveidošanu, lietošanu un administrēšanu.

**programmatūras šifrēšana**
programmatūras lietošana cietā diska šifrēšanai sektoru pa sektoram. Šis process ir lēnāks nekā aparatūras šifrēšana.

**resurss**
datu komponents, kas atrodas cietajā diskā un sastāv no personas informācijas vai failiem, vēsturiskiem vai ar tīmekli saistītiem un līdzīgiem datiem.

**saplēšana**
tāda algoritma izpilde, kas pa virsu resursa datiem uzraksta bezjēdzīgus datus.

**Sākumlapa**
centrālā atrašanās vieta, no kuras iespējama piekļuve HP Client Security funkcijām un iestatījumiem, kā arī to pārvaldīšana.

**šifrēšana**
Procedūra, piemēram, tāda kā algoritma lietošana, kas tiek izmantota kriptogrāfijā, lai pārveidotu vienkāršu tekstu par šifrētu tekstu un neļautu nesankcionētiem saņēmējiem nolasīt šos datus. Ir dažādi datu šifrēšanas veidi, un tie ir tīkla drošības pamats. Parasti veidi ir datu šifrēšanas standarts un publiskā atslēgšifrēšana.

**tīkla konts**
Windows lietotāja vai administratora konts, vai nu vietējā datorā, vai darba grupā, vai domēnā.

**Trust Circle**
nodrošina datu ietvērumu, piesaistot datus noteiktai uzticamu lietotāju grupai. Tas novērš datu netīšu vai tīšu nonākšanu nepareizās rokās. Šie ar CryptoMill tehnoloģiju Zero Overhead Key Management aizsargātie dati ir kriptogrāfiski piesaistīti uzticamo lietotāju lokam. Tas novērš dokumentu un citas sensitīvas informācijas atšifrēšanu ārpus uzticamo lietotāju loka.

**Trust Circle mape**
jebkura mape, kuru aizsargā uzticamo lietotāju loks.

**Trust Circle pārvaldnieks/lasītājs**
Trust Circle lasītājs var pieņemt tikai Trust Circle pārvaldnieka lietotāju nosūtītus uzaicinājumus. Tomēr Trust Circle pārvaldnieks ļauj izveidot uzticamo lietotāju lokus. Funkciju skaitā ietilpst uzaicināšana, nosūtot e-pastu, un uzaicinājumu pievienoties uzticamo lietotāju lokam pieņemšana no citiem. Pēc vienranga lietotāju uzticamo lietotāju loka izveidošanas var droši koplietot šī uzticamo lietotāju loka aizsargātos failus.

**Uzticama platformas moduļa (TPM, Trusted Platform Module) iegultās drošības mikroshēma**

TPM autentificē drīzāk datoru nekā lietotāju, saglabājot resurssistēmai specifisko informāciju, piemēram, šifrēšanas atslēgas, digitālos sertifikātus un paroles. TPM līdz minimumam samazina risku, ka datorā esošo informāciju var apdraudēt fiziska zādzība vai kāda ārēja urķa veikts uzbrukums.

**viedkarte**
aparatūras ierīce, ko var izmantot kopā ar PIN autentifikācijas nolūkā.

**Vienota pierakstīšanās**
Funkcija, kas saglabā autentificēšanās informāciju un ļauj izmantot HP Client Security, lai piekļūtu interneta tīklam un Windows lietojumprogrammām, kuras pieprasa paroles autentificēšanu.

**Windows administrators**
lietotājs ar pilnām tiesībām mainīt atļaujas un pārvaldīt citus lietotājus.

**Windows lietotāja konts**
lietotājs, kas ir autorizēts pieteikties tīklā vai individuālā datorā.

**Windows pieteikšanās drošība**
Aizsargā Windows kontu(-us), pieprasot īpašu akreditācijas datu izmantošanu piekļuvei.

# Alfabētiskais rādītājs