HP Client Security

Začetek dela

Prva izdaja: avgust 2013

Številka dela dokumenta: 735339-BA1

Kazalo

1 Uvod v program HP Client Security Manager

HP Client Security vam omogoča, da zaščitite svoje podatke, napravo in identiteto, s tem pa povečate varnost računalnika.

Od modela vašega računalnika je odvisno, kateri moduli programske opreme so na voljo zanj.

Moduli programske opreme HP Client Security so lahko prednameščeni, prednaloženi ali na voljo za prenos iz spletnega mesta HP. Za več informacij, glejte http://www.hp.com.

OPOMBA: Navodila v tem priročniku predvidevajo, da ste že namestili upoštevne module programske opreme HP Client Security.

Funkcije programske opreme HP Client Security

V naslednji tabeli so predstavljene ključne funkcije modulov HP Client Security.

Modul	Ključne funkcije
HP Client Security Manager	Skrbniki lahko izvajate naslednje funkcije: • Zaščitite računalnik, preden se zažene sistem Windows®. • Zaščitite račun Windows z močnim preverjanjem pristnosti. • Upravljate prijavne podatke in gesla za spletna mesta in programe. • Preprosto spreminjate gesla za operacijski sistem Windows®. • Uporabljate prstne odtise, ki so še bolj varni in priročni. • Nastavite pametno kartico, brezstično kartico ali brezkontaktno kartico za preverjanje pristnosti. • Za identifikacijo uporabljate telefon s tehnologijo Bluetooth. • Nastavite kodo PIN in razširite možnosti preverjanja pristnosti. • Konfigurirate pravilnike za prijavo in seje. • Varnostno kopirate in obnovite podatke programov. • Dodajate programe, na primer HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager in HP Computrace. Splošni uporabniki lahko izvajate naslednje funkcije: • Oglejte si nastavitve za stanje šifriranja in Device Access Manager. • Aktivirate Computrace. • Konfigurirate prednostne nastavitve ter možnosti varnostnega kopiranja in obnovitev.

Modul	Ključne funkcije
Password Manager	Splošni uporabniki lahko izvajate naslednje funkcije: • Organizirate in nastavitve uporabniška imena in gesla. • Ustvarite močnejša gesla za izboljšano varnost računa za elektronsko pošto in spletnih računov. Password Manager samodejno izpolni in pošlje podatke. • Postopek prijave lahko poenostavite s funkcijo enotne prijave, ki samodejno pomni in uporablja uporabniške poverilnice. • Račun lahko označite kot zlorabljen in prejmete opozorilo za druge račune s podobnimi poverilnicami. • Uvozite lahko podatke za prijavo iz podprtega brskalnika.
HP Drive Encryption (samo nekateri modeli)	• Ponuja popolno šifriranje celotnega trdega diska. • Vsili preverjanje pristnosti pred zagonom, da omogoči dešifriranje in dostop do podatkov. • Ponuja možnost aktiviranja samo-šifrirnih pogonov (samo nekateri modeli).
HP Device Access Manager	• Vodjem IT omogoča nadzor dostopa do naprav na podlagi uporabniških profilov. • Nepooblaščenim uporabnikom preprečuje odstranitev podatkov s pomočjo zunanjega medija za shranjevanje in vnos virusov v sistem iz zunanjih medijev. • Skrbnikom omogoča onemogočanje dostopa do komunikacijskih naprav za posamezne uporabnike ali skupine uporabnikov.
HP Trust Circles	• Ponuja varnost datotek in dokumentov. • Šifrira datoteke v mapah, ki jih določijo uporabniki, in jih varuje znotraj kroga zaupanja. • Uporabo in skupno rabo datotek omogoča samo članom v krogu zaupanja.
Theft Recovery (Computrace, kupljeno posebej)	• Za aktiviranje je potreben ločen nakup naročniškega razmerja na sledenje in spremljanje. • Ponuja varno sledenje sredstvom. • Nadzoruje dejavnost uporabnikov ter spremembe strojne in programske opreme. • Ostane aktiven, tudi če se trdi disk ponovno formatira ali zamenja.

Opis izdelkov HP Client Security in primeri najpogostejše uporabe

Večina izdelkov HP Client Security uporablja tako preverjanje pristnosti uporabnika (običajno z geslom) kot skrbniško varovalko, ki omogoča dostop do gesel, če so le-ta izgubljena, niso na voljo ali pa so pozabljena, in vedno, ko varnost podjetja zahteva dostop.

OPOMBA: Nekateri izdelki HP Client Security so zasnovani za omejevanje dostopa do podatkov. Podatke je treba šifrirati, kadar so tako pomembni, da uporabniku manj škoduje njihova izguba kot njihova zloraba. Priporočeno je, da se vsi podatki varnostno kopirajo na varno lokacijo.

Password Manager

Password Manager shranjuje uporabniška imena in gesla in omogoča naslednje funkcije:

- Shranite lahko imena za prijavo in gesla za spletni dostop ali elektronski naslov.
- Možna je samodejna prijava uporabnika v spletno mesto ali e-pošto.
- Upravljate in organizirate lahko preverjanje pristnosti.
- Izberete lahko spletno ali omrežno sredstvo in neposredno dostopate do povezave.
- Po potrebi si lahko ogledate imena in gesla.
- Račun lahko označite kot zlorabljen in prejmete opozorilo za druge račune s podobnimi poverilnicami.
- Uvozite lahko podatke za prijavo iz podprtega brskalnika.

Primer 1: Nabavna posrednica za večjega proizvajalca opravi večino poslovnih transakcij prek spleta. Prav tako redno obiskuje več priljubljenih spletnih mest, ki zahtevajo podatke za prijavo. Močno se zaveda varnosti, zato ne uporablja enakega gesla za vse račune. Posrednica se je odločila uporabiti Password Manager, da bi spletne povezave povezala z različnimi uporabniškimi imeni in gesli. Ko se želi prijaviti v spletno mesto, Password Manager samodejno vnese poverilnice. Če želi, da sta uporabniško ime in geslo vidna, lahko Password Manager konfigurira tako, da se prikažeta.

Password Manager je mogoče uporabiti tudi za upravljanje in organiziranje preverjanja pristnosti. To orodje bo uporabniku omogočilo, da izbere spletno ali omrežno sredstvo in neposredno dostopi do povezave. Uporabnik si lahko po potrebi ogleda uporabniška imena in gesla.

Primer 2: Prizadevni delavec je napredoval in bo zdaj upravljal celoten računovodski oddelek. Skupina se mora prijavljati v številne spletne račune strank, in za vsakega potrebujejo druge podatke za prijavo. Te podatke za prijavo morajo souporabljati z drugimi delavci, zato je zaupnost težavna. Delavec se odloči, da bo organiziral vse spletne povezave, uporabniška imena podjetja in gesla v programu Password Manager. Ko to pripravi, uvede program Password Manager, da lahko delavci delajo v spletnih računih, ne da bi poznali podatke za prijavo, ki jih uporabljajo.

HP Drive Encryption (samo nekateri modeli)

HP Drive Encryption se uporablja za omejevanje dostopa do podatkov na celotnem trdem disku računalnika ali sekundarnem pogonu. Drive Encryption lahko upravlja tudi samo-šifrirne pogone.

Primer 1: Zdravnik želi zagotoviti, da ima le on dostop do podatkov na trdem disku svojega računalnika. Zdravnik aktivira Drive Encryption, ki zahteva preverjanje pristnosti pred zagonom, pred prijavo v sistem Windows. Ko je ta možnost nastavljena, do trdega diska ni mogoče dostopati, če se pred zagonom sistema ne vnese geslo. Zdravnik lahko dodatno izboljša varnost pogona tako, da uporabi šifriranje podatkov s samo-šifrirnim pogonom.

Primer 2: Administrator v bolnišnici želi zagotoviti, da lahko samo zdravniki in pooblaščeno osebje dostopajo do podatkov na njihovih lokalnih računalnikih, ne da bi razkrili svoja osebna gesla. Oddelek IT doda administratorja, zdravnike in pooblaščeno osebje med uporabnike orodja Drive Encryption. Nato lahko samo pooblaščeno osebje zažene računalnik ali domeno z uporabo svojega osebnega uporabniškega imena in gesla.

HP Device Access Manager (samo nekateri modeli)

HP Device Access Manager skrbniku omogoča omejevanje in upravljanje dostopa do strojne opreme. Device Access Manager se lahko uporabi za blokiranje nedovoljenega dostopa do pomnilniškega pogona USB, na katerega bi bilo mogoče kopirati podatke. Prav tako omeji dostop do pogonov CD/

DVD, upravljanje naprav USB, omrežne povezave ipd. Primer je situacija, v kateri potrebujejo zunanji dobavitelji dostop do računalnikov podjetja, vendar podatkov ne smejo kopirati na pogon USB.

Primer 1: Direktor podjetja za oskrbo z medicinsko opremo pogosto dela z osebnimi medicinskimi kartotekami poleg podatkov svojega podjetja. Zaposleni potrebujejo dostop do teh podatkov, toda izjemno pomembno je, da se podatki ne odtujijo z računalnika prek pogona USB ali katerega koli drugega medija za zunanje shranjevanje. Omrežje je varno, toda računalniki imajo zapisovalnike CD-jev in vrata USB, prek katerih bi bilo mogoče kopirati ali ukrasti podatke. Direktor uporabi Device Access Manager, da onemogoči uporabo vrat USB in zapisovalnikov CD-jev. Čeprav so vrata USB blokirana, miška in tipkovnice nemoteno delujejo.

Primer 2: Zavarovalniško podjetje ne želi, da bi zaposleni nameščali ali nalagali osebno programsko opremo ali podatke od doma. Nekateri zaposleni potrebujejo dostop do vrat USB na vseh računalnikih. Vodja oddelka IT uporabi Device Access Manager, da omogoči dostop nekaterim zaposlenim, medtem ko blokira zunanji dostop drugim.

Computrace (nakup posebej)

Computrace (nakup posebej) je storitev, ki omogoča sledenje lokaciji ukradenega računalnika povsod tam, kjer uporabnik dostopa do interneta. Computrace omogoča tudi oddaljeno upravljanje in iskanje računalnikov ter nadzor uporabe računalnika in programov.

Primer 1: Ravnatelj šole je oddelku IT naročil, naj zagotovi sledenje vsem računalnikov na šoli. Po opravljeni inventuri računalnikov je skrbnik IT registriral vse računalnike v storitvi Computrace, da bi omogočil sledenje računalnikom, če bi bili ukradeni. Šola je nedavno ugotovila, da nekaj računalnikov manjka, zato je skrbnik IT obvestil organe pregona in skrbnike storitve Computrace. Organi pregona so našli računalnike in jih vrnili šoli.

Primer 2: Nepremičninsko podjetje potrebuje upravljanje in posodobitev računalnikov po vsem svetu. S pomočjo storitve Computrace računalnike nadzorujejo in jih posodabljajo, ne da bi morali strokovnjaki IT »obiskati« vsak računalnik posebej.

Doseganje ključnih varnostnih ciljev

Moduli HP Client Security lahko sodelujejo v zagotavljanju rešitev za različna varnostna vprašanja, vključno z naslednjimi ključnimi varnostnimi cilji:

- Zaščita pred namensko krajo
- Omejevanje dostopa do občutljivih podatkov
- Preprečevanje nepooblaščenega dostopa z notranjih ali zunanjih lokacij
- Ustvarjanje pravilnikov za močna gesla

Zaščita pred namensko krajo

Primer namenske kraje je, na primer, kraja računalnika, ki vsebuje zaupne podatke in podatke o strankah na kontrolnih točkah na letališču. K zaščiti pred namensko krajo prispevajo naslednje funkcije:

- Funkcija preverjanja pristnosti pred zagonom, če je omogočena, pomaga preprečiti dostop do operacijskega sistema.
  - HP Client Security – Glejte HP Client Security na strani 12.
  - HP Drive Encryption – Glejte HP Drive Encryption (samo nekateri modeli) na strani 30.
- Šifriranje pomaga zagotoviti, da do podatkov ne bo mogoče dostopati, tudi če je trdi disk odstranjen in nameščen v nezavarovan sistem.
- Computrace lahko izsledi lokacijo računalnika po kraji.
  - Computrace – Glejte Iskanje v primeru kraje (samo nekateri modeli) na strani 54.

Omejevanje dostopa do občutljivih podatkov

Predpostavimo da, na primer, pogodbeni revizor dela na lokaciji in dobi dostop do občutljivih podatkov na računalniku. Ne želite, da bi revizor lahko natisnil datoteke ali jih shranil na zapisljivo napravo, na primer CD. Dostop do podatkov pomaga omejiti naslednja funkcija:

- HP Device Access Manager omogoča vodjem IT, da omejijo dostop do komunikacijskih naprav, kar onemogoči kopiranje občutljivih podatkov s trdega diska. Glejte Sistemski pogled na strani 44.

Preprečevanje nepooblaščenega dostopa z notranjih ali zunanjih lokacij

Nedovoljen dostop do nezavarovanega poslovnega računalnika predstavlja zelo stvarno tveganje za sredstva poslovnega omrežja, na primer informacije finančnih storitev, izvršnih oseb ali skupine za raziskave in razvoj, ter za zasebne informacije, kot so kartoteke bolnikov ali osebni finančni izpiski. Nedovoljen dostop pomagajo preprečiti naslednje funkcije:

- Funkcija preverjanja pristnosti pred zagonom, če je omogočena, pomaga preprečiti dostop do operacijskega sistema. Glejte HP Drive Encryption (samo nekateri modeli) na strani 30.
- HP Client Security pomaga zagotoviti, da nepooblaščen uporabnik ne more dobiti gesla ali dostopa do programov, zaščitenih z geslom. Glejte HP Client Security na strani 12.
- HP Device Access Manager omogoča vodjem IT, da omejijo dostop do zapisljivih naprav, kar onemogoči kopiranje občutljivih podatkov s trdega diska. Glejte HP Device Access Manager (samo nekateri modeli) na strani 43.

Ustvarjanje pravilnikov za močna gesla

Če se uveljavi pravilnik podjetja, ki zahteva uporabo pravilnik za močna gesla za številne spletne programe in zbirke podatkov, ponuja Password Manager zaščiteno skladišče za gesla in priročno enotno prijavo. Glejte Password Manager na strani 18.

Dodatni elementi varnosti

Dodelitev varnostnih vlog

Pri upravljanju računalniške varnosti (zlasti za velike organizacije) je ena od pomembnih praks razdelitev odgovornosti in pravic med različne vrste skrbnikov in uporabnikov.

OPOMBA: V majhni organizaciji ali pri individualni rabi ima lahko ena oseba vse te vloge.

Za program HP Client Security je varnostne obveznosti in pravice mogoče razdeliti na naslednje vloge:

- Strokovnjak za varnost – Opredeli raven varnosti za podjetje ali omrežje in določi, katere varnostne funkcije se uvedejo, na primer Drive Encryption.

  OPOMBA: Številne funkcije v programu HP Client Security lahko strokovnjak za varnost prilagodi v sodelovanju s HP-jem. Za več informacij, glejte http://www.hp.com.

- Skrbnik IT – Uporablja in upravlja varnostne funkcije, ki jih določi strokovnjak za varnost. Nekatere funkcije lahko tudi omogoči ali onemogoči. Če je strokovnjak za varnost, na primer, določil uvedbo pametnih kartic, lahko skrbnik IT omogoči geslo in način pametnih kartic.
- Uporabnik – Uporablja varnostne funkcije. Če strokovnjak za varnost in skrbnik IT, na primer, omogočita pametne kartice v sistemu, lahko uporabnik nastavi PIN-številko pametne kartice in za preverjanje pristnosti uporablja kartico.

POZOR: Priporočeno je, da skrbniki upoštevajo »najboljše prakse« pri omejevanju pravic končnega uporabnika in omejevanju dostopa uporabnika.

Nepooblaščeni uporabniki ne bi smeli imeti skrbniških privilegijev.

Upravljanje gesel za HP Client Security

Večina funkcij programa HP Client Security je zavarovana z geslom. V naslednji tabeli so navedena običajno uporabljana gesla, modul programske opreme, v katerem se geslo nastavi, in funkcija gesla.

V tej tabeli so prav tako navedena gesla, ki jih nastavijo in uporabljajo samo skrbniki IT. Vsa druga gesla lahko nastavijo običajni uporabniki ali skrbniki.

Geslo za HP Client Security	Modul, v katerem se nastavi	Funkcija
Geslo za prijavo v Windows	Windows Control Panel ali HP Client Security	Uporablja se lahko za ročno prijavo in za preverjanje pristnosti za dostop do različnih funkcij orodja HP Client Security.
Geslo za varnostno kopijo in obnovitev programa HP Client Security	HP Client Security, posamezni uporabniki	Ščiti dostop do datoteke za varnostno kopiranje in obnovitev v orodju HP Client Security.
PIN-številka pametne kartice	Upravitelj poverilnic	Uporablja se lahko kot večplastno preverjanje pristnosti. Uporablja se lahko kot preverjanje pristnosti za sistem Windows. Če je izbrana pametna kartica, preveri pristnost uporabnikov orodja Drive Encryption.

Ustvarjanje varnega gesla

Pri ustvarjanju gesla morate upoštevati določila programa. Načeloma pa vedno upoštevaje naslednje smernice, ki vam bodo pomagale ustvariti močno geslo in zmanjšati možnosti zlorabe vašega gesla.

- Gesla naj imajo več kot 6 znakov, najbolje več kot 8.
- V geslu uporabite kombinacijo malih in velikih črk.
- Če je le mogoče, vključite tudi alfanumerične znake ter posebne znake in ločila.
- V ključni besedi zamenjajte črke s posebnimi znaki ali številkami. Uporabite lahko, na primer, številko 1 za črko I ali črko L.
- Kombinirajte besede iz 2 ali več jezikov.
- Besedo ali besedno zvezo prekinite s številkami ali posebnimi znaki, na primer »Mojca2-2Muc45«.
- Ne uporabljajte gesla, ki je v slovarju.
- Za geslo ne uporabljajte svojega imena ali drugih osebnih podatkov, kot so rojstni datum, imena ljubljenčkov ali materino dekliško ime, pa čeprav bi jih črkovali z desne proti levi.
- Gesla redno spreminjajte. Spremenite lahko le nekaj znakov z naraščajočimi nasledniki.
- Če geslo zapišete, ga nikoli ne shranjujte na vsem vidnem mestu neposredno ob računalniku.
- Gesla ne shranjujte v datoteke, na primer elektronsko sporočilo, ali v računalniku.
- Ne omogočajte uporabe svojega računa drugim in nikomur ne povejte svojega gesla.

Varnostno kopiranje poverilnic in nastavitev

Orodje za varnostno kopiranje in obnovitev v programu HP Client Security lahko uporabite kot osrednjo lokacijo, s katere lahko varnostno kopirate in obnovite varnostne poverilnice nekaterih nameščenih modulov HP Client Security.

2 Začetek dela

Če želite konfigurirati program HP Client Security za uporabo z vašimi poverilnicami, zaženite HP Client Security na enega od spodaj opisanih načinov. Ko uporabnik zaključi delo s čarovnikom, ga ta uporabnik ne more več zagnati.

1. Na začetnem zaslonu ali zaslonu Programi kliknite oziroma tapnite program **HP Client Security** (Windows 8).

   – ali –

   Na namizju Windows kliknite oziroma tapnite pripomoček **HP Client Security** (Windows 7).

   – ali –

   Na namizju Windows dvokliknite ali dvotapnite ikono **HP Client Security** v območju za obvestila, ki ga najdete na skrajni desni strani opravilne vrstice.

   – ali –

   Na namizju Windows kliknite oziroma tapnite ikono **HP Client Security** v območju za obvestila, nato izberite **Open HP Client Security** (Odpri HP Client Security).

2. Čarovnik za nastavitev HP Client Security zaženete, ko je prikazana pozdravna stran.

3. Preberite pozdravni zaslon, preverite svojo identiteto, tako da vnesete geslo za Windows, nato kliknite oziroma tapnite **Next** (Naprej).

   Če gesla za Windows še niste ustvarili, boste pozvani, da ga ustvarite. Geslo za Windows je potrebno, če želite zaščititi račun Windows pred dostopom nepooblaščenih oseb ter če želite uporabljati funkcije HP Client Security.

4. Na strani HP SpareKey izberite tri varnostna vprašanja. Vnesite odgovor za vsako od vprašanj, nato kliknite **Next** (Naprej). Dovoljena so tudi vprašanja po meri. Za več informacij, glejte HP SpareKey – Obnovitev gesla na strani 14.

5. Na strani Fingerprints (Prstni odtisi) vpišite vsaj najmanjše število zahtevanih prstnih odtisov, nato kliknite oziroma tapnite **Next** (Naprej). Za več informacij, glejte Prstni odtisi na strani 12.

6. Na strani Drive Encryption (Šifriranje pogona) aktivirajte šifriranje, varnostno kopirajte ključ šifriranja, nato kliknite oziroma tapnite **Next** (Naprej). Za več informacij glejte pomoč za programsko opremo HP Drive Encryption.

   OPOMBA: To velja v primeru, ko je uporabnik skrbnik, čarovnika za nastavitev HP Client Security pa skrbnik pred tem ni konfiguriral.

7. Na zadnji strani čarovnika kliknite oziroma tapnite **Finish** (Dokončaj).

   Na tej strani je stanje funkcij in poverilnic.

8. Čarovnik za nastavitev HP Client Security omogoča aktivacijo ravno pravočasnega preverjanja pristnosti ter funkcije File Sanitizer. Za več informacij glejte pomoč za programsko opremo HP Device Access Manager ter pomoč za programsko opremo HP File Sanitizer.

   OPOMBA: To velja v primeru, ko je uporabnik skrbnik, čarovnika za nastavitev HP Client Security pa skrbnik pred tem ni konfiguriral.

Odpiranje programa HP Client Security

Program HP Client Security odprete na enega od spodaj opisanih načinov:

OPOMBA: Najprej morate zaključiti čarovnika za nastavitev HP Client Security, šele nato lahko zaženete program HP Client Security.

- Na začetnem zaslonu ali zaslonu Programi kliknite oziroma tapnite program **HP Client Security**.

  – ali –

  Na namizju Windows kliknite oziroma tapnite pripomoček **HP Client Security** (Windows 7).

  – ali –

  Na namizju Windows dvokliknite ali dvotapnite ikono **HP Client Security** v območju za obvestila, ki ga najdete na skrajni desni strani opravilne vrstice.

  – ali –

  Na namizju Windows kliknite oziroma tapnite ikono **HP Client Security** v območju za obvestila, nato izberite **Open HP Client Security** (Odpri HP Client Security).

3 Priročnik za hitro nastavitev za mala podjetja

To poglavje je namenjeno predstavitvi osnovnih korakov za aktiviranje najpogostejših in najbolj uporabnih možnosti v programu HP Client Security za mala podjetja. Številna orodja in možnosti te programske opreme omogočajo podrobno prilagajanje vaših prednostnih nastavitev in nastavitev nadzora dostopa. Ta priročnik za hitro nastavitev se osredotoča na zagon vsakega posameznega modula s kar najmanj truda in v kar najkrajšem času. Za dodatne informacije izberite modul, ki vas zanima, in nato kliknite **?** ali gumb za pomoč v zgornjem desnem kotu. Ta gumb samodejno prikaže informacije, ki vam bodo pomagale pri delu s trenutno prikazanim oknom.

Začetek dela

1. Na namizju Windows dvokliknite ikono **HP Client Security** v območju za obvestila, ki ga najdete na skrajni desni strani opravilne vrstice, da se odpre program HP Client Security.
2. Vnesite svoje geslo za sistem Windows ali ustvarite geslo za sistem Windows.
3. Dokončajte nastavitev programa HP Client Security.

Če želite, da HP Client Security samo enkrat zahteva preverjanje pristnosti med prijavo v sistem Windows, glejte Varnostne funkcije na strani 26.

Password Manager

Vsakdo ima veliko gesel – zlasti če redno dostopate do spletnih mest ali uporabljate programe, ki zahtevajo prijavo. Uporabniki običajno uporabljajo enako geslo za vse programe in spletna mesta ali pa so sprva ustvarjalni in takoj zatem pozabijo, katero geslo pripada kateremu programu.

Password Manager si lahko samodejno zapomni vaša gesla ali pa vam omogoči razlikovanje med spletnimi mesti, ki jih je treba pomniti, in tistimi, ki jih je treba prezreti. Ko se prijavite v računalnik, Password Manager zagotavlja gesla ali poverilnice za zabeležene programe ali spletna mesta.

Ko dostopite do katerega koli programa ali spletnega mesta, ki zahteva poverilnice, Password Manager samodejno prepozna spletno mesto in vas vpraša, ali želite, da programska oprema pomni vaše podatke. Če želite posamezna mesta izločiti, lahko to zahtevo zavrnete.

Kako shranjujete spletna mesta, uporabniška imena in gesla:

1. Odprite, na primer, spletno mesto ali program, in nato kliknite ikono programa Password Manager v zgornjem levem kotu spletnega mesta, da dodate spletno preverjanje pristnosti.
2. Poimenujte povezavo (izbiroma) in vnesite uporabniško ime in geslo v Password Manager.
3. Ko končate, kliknite gumb **V redu**.
4. Password Manager lahko tudi shrani vaše uporabniško ime in gesla za skupno rabo v omrežju ali povezane omrežne pogone.

Ogled in upravljanje shranjenih podatkov za preverjanje pristnosti v programu Password Manager

Password Manager omogoča ogled, upravljanje, varnostno kopiranje in zagon podatkov za preverjanje pristnosti z osrednjega mesta. Password Manager podpira tudi zagon shranjenih spletnih mest iz sistema Windows.

Če želite odpreti Password Manager, uporabite kombinacijo Ctrl+tipka Windows+h na tipkovnici, in nato kliknite **Prijava**, da se shranjena bližnjica odpre in se izvede preverjanje pristnosti.

Možnost **Edit** programa Password Manager omogoča ogled in spreminjanje imena in imena za prijavo ter tudi gesel.

HP Client Security za mala podjetja omogoča varnostno kopiranje in/ali kopiranje vseh poverilnic in nastavitev na drug računalnik.

HP Device Access Manager

Device Access Manager je mogoče uporabiti za omejevanje različnih notranjih in zunanjih pomnilniških naprav, da bi vaši podatki ostali zavarovani na trdem disku, ne pa odtujeni. Tako lahko, na primer, omogočite dostop uporabnikov do vaših podatkov, vendar jim preprečite kopiranje podatkov na CD, osebni glasbeni predvajalnik ali pomnilniško napravo USB.

1. Odprite program **Device Access Manager** (glejte Odpiranje programa Device Access Manager na strani 44).

   Prikazan je dostop za trenutnega uporabnika.

2. Če želite spremeniti dostop za uporabnike, skupine ali naprave, kliknite ali tapnite **Spremeni**. Za več informacij, glejte Sistemski pogled na strani 44.

HP Drive Encryption

HP Drive Encryption se uporablja za zaščito vaših podatkov s šifriranjem podatkov na celotnem trdem disku. Podatki na vašem trdem disku bodo zaščiteni, če bi bil vaš računalnik kadar koli ukraden in/ali če se trdi disk odstrani iz prvotnega računalnika in namesti v drug računalnik.

Dodatna prednost za varnost je zahteva programa Drive Encryption po uspešnem preverjanju pristnosti z vašim uporabniškim imenom in geslom pred zagonom operacijskega sistema. Postopek se imenuje preverjanje pristnosti pred zagonom.

Za preprostejše delo več modulov programske opreme samodejno sinhronizira gesla, med drugim uporabniškimi računi programa Windows, HP Drive Encryption, Password Manager in HP Client Security.

Če želite pri začetni nastavitvi nastaviti orodje HP Drive Encryption s pomočjo čarovnika HP Client Security, glejte Začetek dela na strani 8.

4 HP Client Security

Začetna stran HP Client Security je osrednje mesto, kjer preprosto dostopate do funkcij, programov in nastavitev programske opreme HP Client Security. Začetna stran je razdeljena na tri dele.

- **DATA** (PODATKI) – Nudi dostop do programov za upravljanje varnosti podatkov.
- **DEVICE** (NAPRAVA) – Nudi dostop do programov za upravljanje varnosti naprav.
- **IDENTITY** (IDENTITETA) – Omogoča vpis in upravljanje poverilnic za preverjanje pristnosti.

Pomaknite kazalec nad ploščico programa in pokazal se bo njegov opis.

HP Client Security ima lahko na dnu strani povezave do uporabniških in skrbniških nastavitev. HP Client Security nudi dostop do dodatnih nastavitev in funkcij, če tapnete oziroma kliknete ikono **zobnika** (nastavitve).

Funkcije, programi in nastavitve identitete

Funkcije, programi in nastavitve identitete, ki jih nudi HP Client Security, vam pomagajo pri upravljanju različnih vidikov vaše digitalne identitete. Kliknite oziroma tapnite eno od naslednjih ploščic na začetni strani HP Client Security, nato vnesite geslo za Windows:

- **Fingerprints** (Prstni odtisi) – Vpiše in upravlja vašo poverilnico prstnih odtisov.
- **SpareKey** – Nastavi in upravlja vašo poverilnico HP SpareKey, s katero se lahko prijavite v računalnik, če izgubite ali založite druge poverilnice. Omogoča tudi, da ponastavite pozabljeno geslo.
- **Windows Password** (Geslo za Windows) – Nudi preprost dostop za spreminjanje gesla za Windows.
- **Bluetooth Devices** (Naprave Bluetooth) – Omogoča vpis in upravljanje naprav Bluetooth.
- **Cards** (Kartice) – Omogoča vpis in upravljanje pametnih kartic, brezstičnih in brezkontaktnih kartic.
- **PIN** – Omogoča vpis in upravljanje vaše poverilnice PIN.
- **RSA SecurID** – Omogoča vpis in upravljanje vaše poverilnice RSA SecurID (če je na voljo ustrezna nastavitev).
- **Password Manager** (Upravitelj gesel) – Omogoča upravljanje gesel za internetne račune in programe.

Prstni odtisi

Čarovnik za nastavitev HP Client Security vas vodi skozi postopek nastavljanja oz. »vpisa« prstnih odtisov.

Prstne odtise lahko vpišete ali izbrišete tudi na strani za prstne odtise, do katere pridete tako, da kliknete oziroma tapnete ikono **Fingerprints** (Prstni odtisi) na začetni strani HP Client Security.

1. Na strani za prstne odtise podrsajte s prstom, da ga uspešno vpišete.

   Na strani je prikazano, koliko prstov mora biti vpisanih. Prednost imajo kazalci in sredinci.

2. Če želite izbrisati prej vpisane prstne odtise, kliknite oziroma tapnite **Delete** (Izbriši).

3. Če želite vpisati več prstov, kliknite oziroma tapnite **Enroll an additional fingerprint** (Vpiši dodaten prstni odtis).

4. Preden zapustite stran, kliknite oziroma tapnite **Save** (Shrani).

⚠ **POZOR:** Ko prstne odtise vpisujete s čarovnikom, se podatki o njih ne shranijo, dokler ne kliknete **Next** (Naprej). Če računalnik nekaj časa pustite nedejaven ali zaprete program, se spremembe, ki ste jih naredili, **ne** shranijo.

- ▲ Če želite odpreti skrbniške nastavitve za prstne odtise, kjer skrbniki lahko določijo vpis, natančnost in druge nastavitve, kliknite oziroma tapnite **Administrative Settings** (Skrbniške nastavitve) (potrebne so skrbniške pravice).
- ▲ Če želite odpreti uporabniške nastavitve za prstne odtise, kjer lahko navedete nastavitve, ki upravljajo videz in vedenje prepoznavanja prstnih odtisov, kliknite oziroma tapnite **User Settings** (Uporabniške nastavitve).

Skrbniške nastavitve za prstne odtise

Skrbniki lahko navedejo vpis, natančnost ter druge nastavitve za bralnik prstnih odtisov. Potrebne so skrbniške pravice.

- ▲ Če želite odpreti skrbniške nastavitve za poverilnico prstnih odtisov, kliknite oziroma tapnite **Administrative Settings** (Skrbniške nastavitve) na strani prstnih odtisov.

- **User enrollment** (Vpis uporabnika) – Izberite najmanjše in največje število prstnih odtisov, ki jih je uporabniku dovoljeno vpisati.
- **Recognition** (Prepoznavanje) – Pomaknite drsnik in prilagodite občutljivost bralnika prstnih odtisov od drsljaju s prstom.

  Če se prstni odtis slabo prepoznava, bi bilo morda dobro izbrati nižjo nastavitev prepoznavanja. Višja nastavitev pomeni večjo občutljivost na odstopanja pri podrsanju prsta, zato je tudi možnost lažne prepoznave manjša. Nastavitev **Medium-High** (Srednje visoko) je dobra kombinacija varnosti in preprostosti.

Uporabniške nastavitve za prstne odtise

Na strani z uporabniškimi nastavitvami prstnih odtisov lahko določite nastavitve, ki upravljajo videz in vedenje prepoznavanja prstnih odtisov.

▲ Če želite odpreti uporabniške nastavitve za poverilnico prstnih odtisov, kliknite oziroma tapnite **User Settings** (Uporabniške nastavitve) na strani prstnih odtisov.

- **Enable sound feedback** (Omogoči povratno informacijo z zvokom) – HP Client Security privzeto nudi zvočne povratne informacije, ko podrsate s prstom. Za posamezne dogodke programa predvaja različne zvoke. Tem dogodkom lahko dodelite nove zvoke na kartici Zvoki v nastavitvi zvoka na nadzorni plošči Windows. Če želite zvoke onemogočiti, počistite potrditveno polje.
- **Show scan quality feedback** (Pokaži povratno informacijo o kakovosti optičnega branja) – Če želite prikazati vse drsljaje, ne glede na kakovost, potrdite to polje. Če želite prikazati samo kakovostne drsljaje, počistite to polje.

HP SpareKey – Obnovitev gesla

HP SpareKey omogoča, da (na podprtih platformah) pridobite dostop do računalnika tako, da odgovorite na tri varnostna vprašanja.

HP Client Security vas pozove, da nastavite osebni HP SpareKey med začetno nastavitvijo v čarovniku za nastavitev HP Client Security.

Nastavitev HP SpareKey:

1. Na strani HP SpareKey v čarovniku izberite tri varnostna vprašanja, nato vnesite odgovor na vsako vprašanje.

   Vprašanje lahko izberete s seznama ali napišete svoje.

2. Kliknite oziroma tapnite **Enroll** (Vpiši).

Če želite izbrisati HP SpareKey:

▲ Kliknite oziroma tapnite **Delete your SpareKey** (Izbriši SpareKey).

Ko nastavite SpareKey, lahko dostopate do računalnika s ključem SpareKey na zaslonu za preverjanje pristnosti pri vklopu ali na pozdravnem zaslonu za Windows.

Na strani SpareKey lahko izberete različna vprašanja ali spremenite odgovore nanje. Do te strani lahko dostopate s ploščice Password Recovery (Obnovitev gesla) na začetni strani HP Client Security.

Če želite dostopati do nastavitev za HP SpareKey, kjer lahko skrbnik določi nastavitve v zvezi s poverilnico HP SpareKey, kliknite **Settings** (Nastavitve) (potrebne so skrbniške pravice).

HP SpareKey Settings

Na strani z nastavitvami HP SpareKey lahko določite nastavitve, ki upravljajo vedenje in uporabo poverilnice HP SpareKey.

▲ Če želite odpreti stran z nastavitvami HP SpareKey, kliknite oziroma tapnite **Settings** (Nastavitve) na strani HP SpareKey (potrebne so skrbniške pravice).

Skrbniki lahko izberejo naslednje nastavitve:

- Določite vprašanja, ki bodo uporabnikom ponujena med nastavitvijo orodja HP SpareKey.
- Dodajte do tri varnostna vprašanja po meri, ki bodo dodana na seznam, ponujen uporabnikom.

- Izberite, ali boste uporabnikom dovolili, da sami napišejo varnostna vprašanja.
- Določite, katera okolja za preverjanje pristnosti (Windows ali preverjanje pristnosti pri vklopu) dovoljujejo uporabo orodja HP SpareKey za obnovitev gesel.

Geslo za Windows

HP Client Security skrbi, da je spreminjanje gesla za Windows preprostejše in hitrejše kot prek nadzorne plošče za Windows.

Geslo za Windows spremenite tako:

1. Na začetni strani HP Client Security kliknite oziroma tapnite **Windows Password** (Geslo za Windows).
2. V besedilno polje **Current Windows password** (Trenutno geslo za Windows) vnesite svoje trenutno geslo.
3. V besedilno polje **New Windows password** (Novo geslo za Windows) vnesite novo geslo, nato ga znova vnesite v besedilno polje **Confirm new password** (Potrditev novega gesla).
4. Kliknite oziroma tapnite **Change** (Spremeni), da takoj spremenite trenutno geslo v novo geslo, ki ste ga vnesli.

Naprave Bluetooth

Če je skrbnik omogočil Bluetooth kot poverilnico za preverjanje pristnosti, lahko za večjo varnost nastavite telefon Bluetooth v kombinaciji z drugimi poverilnicami.

OPOMBA: Podprte so samo telefonske naprave Bluetooth.

1. Prepričajte se, da je v računalniku omogočena funkcija Bluetooth in da je telefon Bluetooth v načinu za odkrivanje. Če želite povezati telefon, boste morda morali vnesti samodejno ustvarjeno kodo na napravi Bluetooth. Glede na nastavitve konfiguracije naprave Bluetooth bo morda potrebna primerjava kod za seznanjanje med računalnikom in telefonom.
2. Če želite vpisati telefon, ga izberite, nato pa kliknite oziroma tapnite **Enroll** (Vpiši).

Za dostop do strani Nastavitve naprav Bluetooth na strani 15, kjer skrbnik lahko določi nastavitve za naprave Bluetooth, kliknite **Settings** (Nastavitve) (potrebne so skrbniške pravice).

Nastavitve naprav Bluetooth

Skrbniki lahko določijo naslednje nastavitve, ki usmerjajo vedenje in uporabo poverilnic naprave Bluetooth:

Tiho preverjanje pristnosti

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Samodejno uporabi povezano vpisano napravo Bluetooth med preverjanjem vaše identitete) – Potrdite to polje, da bodo uporabniki lahko poverilnico Bluetooth uporabljali za preverjanje pristnosti, ne da bi moral uporabnik karkoli narediti. Počistite polje, če želite to možnost onemogočiti.

Bližina Bluetooth

- **Lock computer when your enrolled Bluetooth device moves out of range of your computer** (Zakleni računalnik, ko vpisana naprava Bluetooth izstopi iz dosega računalnika) –

Potrdite to polje, da zaklenete računalnik, ko se naprava Bluetooth, ki je bila povezana med prijavo, premakne izven dosega. Počistite polje, če želite to možnost onemogočiti.

OPOMBA: Če hočete izkoristiti to funkcijo, mora modul Bluetooth v računalniku podpirati to zmogljivost.

Kartice

HP Client Security lahko podpira vrsto različnih izkaznic; to so plastične kartice z računalniškim čipom. Med njimi so pametne, brezstične in brezkontaktne kartice. Če tovrstno kartico in ustrezni bralnik kartic povežete z računalnikom, če je skrbnik namestil ustrezni gonilnik izdelovalca in če je skrbnik omogočil kartico kot poverilnico za preverjanje pristnosti, potem lahko kartico uporabljate kot poverilnico za preverjanje pristnosti.

Za pametne kartice mora izdelovalec preskrbeti orodja za namestitev varnostnega potrdila in upravljanje kode PIN, ki jih uporablja HP Client Security v svojem varnostnem algoritmu. Število in vrsta znakov, ki se uporabljajo kot koda PIN, se lahko razlikuje. Preden pametno kartico lahko uporabite, jo mora skrbnik inicializirati.

HP Client Security podpira te oblike pametnih kartic:

- CSP
- PKCS11

HP Client Security podpira te vrste brezstičnih kartic:

- Brezstične pomnilniške kartice HID iCLASS
- Brezstične kartice MiFare Classic 1k, 4k, in mini pomnilniške kartice

HP Client Security podpira te brezkontaktne kartice:

- Brezkontaktne kartice HID

Če želite vpisati pametno kartico:

1. Vstavite kartico v povezan bralnik pametnih kartic.
2. Ko računalnik prepozna kartico, vnesite njeno kodo PIN, nato kliknite oziroma tapnite **Enroll** (Vpiši).

Če želite spremeniti kodo PIN pametne kartice:

1. Vstavite kartico v povezan bralnik pametnih kartic.
2. Ko računalnik prepozna kartico, vnesite njeno kodo PIN, nato kliknite oziroma tapnite **Authenticate** (Preveri pristnost).
3. Kliknite oziroma tapnite **Change PIN** (Spremeni kodo PIN) in vnesite novo kodo PIN.

Če želite vpisati brezstično ali brezkontaktno kartico:

1. Položite kartico v neposredno bližino ustreznega bralnika.
2. Ko računalnik prepozna kartico, kliknite oziroma tapnite **Enroll** (Vpiši).

Če želite izbrisati vpisano kartico:

1. Ponudite kartico bralniku.
2. Samo za pametne kartice vnesite dodeljeno kodo PIN kartice, nato kliknite oziroma tapnite **Authenticate** (Preveri pristnost).
3. Kliknite oziroma tapnite **Delete** (Izbriši).

Ko je kartica vpisana, so njene podrobnosti prikazane v možnosti **Enrolled Cards** (Vpisane kartice). Ko kartico izbrišete, se odstrani s seznama.

Za dostop do nastavitev brezkontaktnih, brezstičnih in pametnih kartic, kjer lahko skrbniki določijo nastavitve, povezane s poverilnicami kartic, kliknite oziroma tapnite **Settings** (Nastavitve) (potrebne so skrbniške pravice).

Nastavitve brezkontaktnih, brezstičnih in pametnih kartic

Za dostop do nastavitev za kartico kliknite oziroma tapnite kartico na seznamu, nato kliknite oziroma tapnite puščico, ki je prikazana.

Če želite spremeniti kodo PIN pametne kartice:

1. Ponudite kartico bralniku
2. Vnesite dodeljeno kodo PIN kartice, nato kliknite oziroma tapnite **Continue** (Nadaljuj).
3. Vnesite in potrdite novo kodo PIN, nato kliknite oziroma tapnite **Continue** (Nadaljuj).

Če želite inicializirati kodo PIN pametne kartice:

1. Ponudite kartico bralniku
2. Vnesite dodeljeno kodo PIN kartice, nato kliknite oziroma tapnite **Continue** (Nadaljuj).
3. Vnesite in potrdite novo kodo PIN, nato kliknite oziroma tapnite **Continue** (Nadaljuj).
4. Kliknite oziroma tapnite **Yes** (Da), da potrdite inicializacijo.

Če želite počistiti podatke kartice:

1. Ponudite kartico bralniku
2. Vnesite dodeljeno kodo PIN kartice (samo za pametne kartice), nato kliknite oziroma tapnite **Continue** (Nadaljuj).
3. Kliknite oziroma tapnite **Yes** (Da), da potrdite brisanje.

PIN

Če je skrbnik omogočil kodo PIN kot poverilnico za preverjanje pristnosti, lahko za večjo varnost nastavite kodo PIN v kombinaciji z drugimi poverilnicami.

Če želite nastaviti novo kodo PIN:

- Vnesite kodo PIN, vnesite jo znova, da jo potrdite, nato kliknite oziroma tapnite **Apply** (Uporabi).

Če želite izbrisati kodo PIN:

- Kliknite oziroma tapnite **Delete** (Izbriši), nato kliknite oziroma tapnite **Yes** (Da), da potrdite.

Za dostop do nastavitev kode PIN, kjer lahko skrbniki določijo nastavitve, povezane s poverilnicami kode PIN, kliknite oziroma tapnite **Settings** (Nastavitve) (potrebne so skrbniške pravice).

PIN Settings

Na strani z nastavitvami kode PIN lahko navedete najmanjšo in največjo sprejemljivo dolžino za poverilnico PIN.

RSA SecurID

Če je skrbnik omogočil RSA kot poverilnico za preverjanje pristnosti in če so naslednji pogoji resnični, lahko vpišete ali izbrišete poverilnico RSA SecurID.

OPOMBA: Potrebna je ustrezna nastavitev.

- Uporabnik je moral biti ustvarjen na strežniku RSA.
- Žeton RSA SecurID, ki je dodeljen uporabniku in računalniku, je moral biti priključen domeni strežnika RSA.
- V računalniku je nameščena programska oprema SecurID.
- Na voljo je povezava s pravilno konfiguriranim strežnikom RSA.

Če želite vpisati poverilnico RSA SecurID:

▲ Vnesite svoje uporabniško ime in geslo RSA SecurID (RSA SecurID koda žetona ali PIN + koda žetona, glede na okolje, v katerem ste), nato kliknite oziroma tapnite **Apply** (Uporabi).

Ob uspešnem vpisu bo prikazano sporočilo »Your RSA SecurID credential has been successfully enrolled« (Vaša poverilnica RSA SecurID je bila uspešno vpisana) in gumb Delete (Izbriši) bo omogočen.

Če želite izbrisati poverilnico RSA SecurID:

▲ Kliknite **Delete** (Izbriši), nato izberite **Yes** (Da) v pojavnem oknu, ki sprašuje »Are you sure you want to delete your RSA SecurID credential?« (Ali res želite izbrisati svojo poverilnico RSA SecurID?)

Password Manager

Prijavljanje na spletna mesta in v programe je lažje in varnejše, če uporabljate Password Manager. Ustvarite lahko močnejša gesla, ki si jih ni treba zapisati ali zapomniti, nato pa se preprosto in hitro prijavite s prstnim odtisom, pametno kartico, brezkontaktno kartico, brezstično kartico, telefonom Bluetooth, kodo PIN, poverilnico RSA ali z geslom za Windows.

OPOMBA: Ker spletni zasloni za prijavo ves čas spreminjajo strukturo, Password Manager morda ne bo vselej podpiral vseh spletnih mest.

Password Manager nudi te možnosti:

Stran Password Manager

- Kliknite oziroma tapnite račun, da samodejno zaženete spletno stran ali program in se prijavite.
- Račune organizirajte po kategorijah.

Moč gesla

- Na prvi pogled vidite, ali je katero izmed vaših gesel varnostno tveganje.
- Ko dodajate prijavne podatke, preverite moč posameznih gesel za spletna mesta in programe.
- Moč gesel je prikazana z rdečo, rumeno ali zeleno oznako stanja.

Ikona **Password Manager** je prikazana v zgornjem levem kotu spletne strani ali zaslona za prijavo programa. Če za posamezno spletno mesto ali program še ni bila ustvarjena prijava, je na ikoni prikazan znak plus.

▲ Kliknite oziroma tapnite ikono **Password Manager**, da se pokaže kontekstni meni, kjer lahko izbirate med temi možnostmi:

- Add [somedomain.com] to Password Manager (Dodaj [nekadomena.com] v Password Manager)
- Open Password Manager (Odpri Password Manager)
- Icon Settings (Nastavitve ikon)
- Pomoč

Za spletne strani ali programe, za katere še ni bila ustvarjena prijava

V kontekstnem meniju so prikazane te možnosti:

- **Add [somedomain.com] to the Password Manager** (Dodaj [nekadomena.com] v Password Manager) – Omogoča dodajanje prijave iz trenutnega zaslona za prijavo.
- **Open Password Manager** (Odpri Password Manager) – Zažene Password Manager.
- **Icon Settings** (Nastavitve ikon) – Omogoča, da določite pogoje, v katerih bo prikazana ikona **Password Manager**.
- **Help** (Pomoč) – Prikaže pomoč za HP Client Security.

Za spletne strani ali programe, za katere je bila že ustvarjena prijava

V kontekstnem meniju so prikazane te možnosti:

- **Fill in logon data** (Vnesite podatke za prijavo) – Prikaže stran **Verify your identity** (Preverite svojo identiteto). Če uspešno preverite pristnost, se bodo vaši prijavni podatki pokazali v prijavnih poljih, nato pa bo stran poslana (če ste določili pošiljanje, ko ste prijavo ustvarili oziroma nazadnje uredili).
- **Edit Logon** (Urejanje prijave) – Omogoča urejanje prijavnih podatkov za to spletno mesto.
- **Add Logon** (Dodajanje prijave) – Omogoča dodajanje računa v Password Manager.
- **Open Password Manager** (Odpri Password Manager) – Zažene Password Manager.
- **Help** (Pomoč) – Prikaže pomoč za HP Client Security.

OPOMBA: Skrbnik računalnika je morda konfiguriral HP Client Security tako, da pri preverjanju vaše identitete zahteva več kot eno poverilnico.

Dodajanje prijav

Če enkrat vnesete prijavne podatke, z lahkoto dodate prijavo za spletno mesto ali program. Po tem bo Password Manager samodejno vnašal te podatke namesto vas. Te prijave lahko uporabljate tudi po tem, ko ste že na spletnem mestu ali v programu.

Če želite dodati prijavo:

1. Odprite zaslon za prijavo spletnega mesta ali programa.
2. Kliknite oziroma tapnite ikono **Password Manager**, nato kliknite ali tapnite nekaj od naslednjega, glede na to, ali je zaslon za prijavo za spletno mesto ali za program:
   - Za spletno mesto kliknite oziroma tapnite **Add [domain name] to Password Manager** (Dodaj [nekadomena.com] v Password Manager).
   - Za program kliknite oziroma tapnite **Add this logon screen to Password Manager** (Dodaj ta zaslon za prijavo v Password Manager).
3. Vnesite svoje prijavne podatke. Polja za prijavo na zaslonu ter ustrezna polja v pogovornem oknu prepoznate po krepki oranžni obrobi.
   a. Če želite polje za prijavo izpolniti z eno od vnaprej pripravljenih izbir, kliknite oziroma tapnite puščice desno od polja.
   b. Če si želite ogledati geslo za to prijavo, kliknite oziroma tapnite **Show password** (Pokaži geslo).
   c. Če želite izpolniti polja za prijavo, vendar jih ne poslati, počistite polje **Automatically submit logon data** (Samodejno pošlji podatke za prijavo).
   d. Kliknite oziroma tapnite **OK** (V redu), da izberete način preverjanja pristnosti, ki ga želite uporabiti (prstni odtisi, pametna, brezkontaktna, brezstična kartica, telefon Bluetooth, koda PIN ali geslo), nato se prijavite z izbranim načinom preverjanja pristnosti.

      Z ikone **Password Manager** izgine znak plus, kar pomeni, da je bila prijava ustvarjena.
   e. Če Password Manager ne zazna polj za prijavo, kliknite oziroma tapnite **More fields** (Več polj).
      - Izberite potrditveno polje za vsako polje, ki je zahtevano za prijavo, ali pa počistite potrditveno polje za katero koli polje, ki ni zahtevano za prijavo.
      - Kliknite oziroma tapnite **Close** (Zapri).

Vsakič ko boste dostopali do tega spletnega mesta ali odprli ta program, bo prikazana ikona **Password Manager** v zgornjem levem kotu zaslona za prijavo v spletno mesto oziroma program, kar pomeni, da za prijavo lahko uporabite vpisane poverilnice.

Urejanje prijave

Če želite urediti prijavo:

1. Odprite zaslon za prijavo spletnega mesta ali programa.
2. Kliknite oziroma tapnite ikono **Password Manager**, da se pokaže pogovorno okno, v katerem lahko urejate podatke za prijavo, nato kliknite oziroma tapnite **Edit Logon** (Urejanje prijave).

   Polja za prijavo na zaslonu ter ustrezna polja v pogovornem oknu prepoznate po krepki oranžni obrobi.

   Podatke računa lahko urejate tudi na strani Password Manager, tako da kliknete oziroma tapnete prijavo, da se pokažejo možnosti urejanja, ter izberete **Edit** (Urejanje).
3. Uredite svoje podatke za prijavo.
   - Če želite urediti **Account name** (Ime računa), vnesite v polje novo ime.
   - Če želite dodati ali urediti ime kategorije, vnesite ali spremenite ime v polju **Category** (Kategorija).

- Če želite izbrati polje za prijavo **Username** (Uporabniško ime) z eno od vnaprej pripravljenih izbir, kliknite oziroma tapnite puščico navzdol desno od polja.

  Vnaprej pripravljene izbire so na voljo le, če prijavo urejate iz ukaza Edit (Urejanje) kontekstnega menija ikone Password Manager.

- Če želite izbrati polje **Password** (Geslo) za prijavo z eno od vnaprej pripravljenih izbir, kliknite oziroma tapnite puščico navzdol desno od polja.

  Vnaprej pripravljene izbire so na voljo le, če prijavo urejate iz ukaza Edit (Urejanje) kontekstnega menija ikone Password Manager.

- Če želite prijavi dodati več polj z zaslona, kliknite oziroma tapnite **More fields** (Več polj).
- Če si želite ogledati geslo za to prijavo, kliknite oziroma tapnite ikono **Show password** (Pokaži geslo).
- Če želite izpolniti polja za prijavo, vendar jih ne poslati, počistite polje **Automatically submit logon data** (Samodejno pošlji podatke za prijavo).
- Če želite to prijavo označiti, da ima zlorabljeno geslo, potrdite polje **This password is compromised** (To geslo je zlorabljeno).

  Ko spremembe shranite, bodo tudi druge prijave s tem geslom označene kot zlorabljene. Nato lahko obiščete vsak račun, na katerega to vpliva, in po potrebi spremenite gesla.

4. Kliknite oziroma tapnite **OK** (V redu).

Uporaba menija hitrih povezav za Password Manager

S programom Password Manager lahko hitro in preprosto zaženete spletna mesta in programe, za katere ste ustvarili prijave. V meniju **Password Manager Quick Links** (Hitre povezave za Password Manager) ali na strani Password Manager v programu HP Client Security dvokliknite oziroma dvotapnite prijavo v program ali spletno mesto, da se odpre zaslon za prijavo, in vnesite svoje podatke za prijavo.

Ko ustvarite prijavo, se ta samodejno doda v meni **Quick Links** (Hitre povezave) programa Password Manager.

Če želite prikazati meni **Quick Links** (Hitre povezave):

▲ Pritisnite kombinacijo bližnjičnih tipk za **Password Manager** (tovarniško nastavljena kombinacija je (Ctrl+tipka Windows+h). Če želite spremeniti kombinacijo bližnjičnih tipk, na začetni strani HP Client Security kliknite **Password Manager**, nato kliknite oziroma tapnite **Settings** (Nastavitve).

Razvrščanje prijav v kategorije

Skrbite, da bodo prijave urejene, tako da zanje ustvarite vsaj eno kategorijo.

Če želite prijavo dodeliti kategoriji:

1. Na začetni strani HP Client Security kliknite oziroma tapnite **Password Manager**.
2. Kliknite oziroma tapnite vnos računa, nato kliknite oziroma tapnite **Edit** (Urejanje).
3. V polju **Category** (Kategorija) vnesite ime kategorije.
4. Kliknite oziroma tapnite **Save** (Shrani).

Če želite račun odstraniti iz kategorije:

1. Na začetni strani HP Client Security kliknite oziroma tapnite **Password Manager**.
2. Kliknite oziroma tapnite vnos računa, nato kliknite oziroma tapnite **Edit** (Urejanje).
3. V polju **Category** (Kategorija) izbrišite ime kategorije.
4. Kliknite oziroma tapnite **Save** (Shrani).

Če želite preimenovati kategorijo:

1. Na začetni strani HP Client Security kliknite oziroma tapnite **Password Manager**.
2. Kliknite oziroma tapnite vnos računa, nato kliknite oziroma tapnite **Edit** (Urejanje).
3. V polju **Category** (Kategorija) spremenite ime kategorije.
4. Kliknite oziroma tapnite **Save** (Shrani).

Upravljanje prijav

Password Manager vam olajša upravljanje podatkov za prijavo, kot so uporabniška imena, gesla, več računov za prijavo, in sicer na enem osrednjem mestu.

Vaše prijave so navedene na strani Password Manager.

Če želite upravljati svoje prijave:

1. Na začetni strani HP Client Security kliknite oziroma tapnite **Password Manager**.
2. Kliknite oziroma tapnite obstoječo prijavo, nato izberite eno od spodnjih možnosti ter sledite navodilom na zaslonu:
   - **Edit** (Urejanje) – Uredite prijavo. Za več informacij, glejte Urejanje prijave na strani 20.
   - **Log in** (Prijava) – Prijavite se v izbrani račun.
   - **Delete** (Brisanje) – Izbrišite prijavo za izbrani račun.

Če želite dodati še eno prijavo za spletno mesto ali program:

1. Odprite zaslon za prijavo spletnega mesta ali programa.
2. Kliknite oziroma tapnite ikono **Password Manager**, da se pokaže njen kontekstni meni.
3. Kliknite oziroma tapnite **Add Logon** (Dodaj prijavo), nato sledite navodilom na zaslonu.

Ocenjevanje moči gesel

Pri varovanju identitete je pomembno, da za prijavo v spletna mesta in programe uporabljate močna gesla.

Password Manager vam olajša nadziranje in izboljšave varnosti, saj v hipu samodejno analizira moč vsakega posameznega gesla, s katerim se prijavljate v spletna mesta in programe.

Ko med ustvarjanjem prijave za Password Manager za račun vnašate geslo, je pod geslom prikazana barvna vrstica, ki ponazarja moč gesla. Barve imajo naslednje vrednosti:

- **Rdeča** – šibko
- **Rumena** – zadovoljivo
- **Zelena** – močno

Nastavitve ikone programa Password Manager

Password Manager na spletnih mestih in v programih poskuša prepoznati zaslone za prijavo. Ko Password Manager zazna zaslon za prijavo, za katerega še niste ustvarili prijave, vas pozove, da dodajte prijavo za ta zaslon, tako da prikaže ikono **Password Manager** z znakom plus.

1. Kliknite oziroma tapnite ikono, nato kliknite oziroma tapnite **Icon Settings** (Nastavitve ikone), da prilagodite postopek, kako naj Password Manager obravnava morebitna mesta za prijavo.
   - **Prompt to add logons for logon screens** (Poziv za dodajanje prijav za prijavne zaslone) – Kliknite oziroma tapnite to možnost, če želite, da vas Password Manager pozove, da dodajte prijavo, kadar je prikazan zaslon za prijavo, ki še nima ustvarjene prijave.
   - **Exclude this screen** (Izključi ta zaslon) – To polje potrdite, če ne želite, da vas Password Manager poziva, da dodajte prijavo za ta zaslon za prijavo.
   - **Do not prompt to add logons for logon screens** (Brez poziva za dodajanje prijav za prijavne zaslone) – Izberite izbirni gumb.
2. Če želite dodati prijavo za zaslon, ki je bil pred tem izključen:
   a. Prijavite se na spletno mesto, ki je bilo pred tem izključeno.
   b. Če želite, da si Password Manager zapomni geslo za to spletno mesto, kliknite oziroma tapnite **Remember** (Zapomni si) v pojavnem oknu, da shranite geslo in ustvarite prijavo za ta zaslon.
3. Če želite dostopati do dodatnih nastavitev programa Password Manager, kliknite oziroma tapnite ikono Password Manager, kliknite oziroma tapnite **Open Password Manager** (Odpri Password Manager) in nato kliknite oziroma tapnite **Settings** (Nastavitve) na strani Password Manager.

Uvoz in izvoz prijav

Na strani HP Password Manager za uvoz in izvoz lahko uvozite prijave, ki so jih v računalniku shranili spletni brskalniki. Prav tako lahko uvozite podatke iz datoteke varnostne kopije za HP Client Security in izvozite podatke v datoteko varnostne kopije za HP Client Security.

▲ Če želite odpreti stran za uvoz in izvoz, kliknite oziroma tapnite **Import and export** (Uvoz in izvoz) na strani Password Manager.

Če želite gesla uvoziti iz brskalnika:

1. Kliknite oziroma tapnite brskalnik, iz katerega želite uvoziti gesla (prikazani so samo nameščeni brskalniki).
2. Počistite potrditveno polje za račune, za katere ne želite uvoziti gesel.
3. Kliknite oziroma tapnite **Import** (Uvoz).

Podatke iz datoteke varnostne kopije HP Client Security uvozite oziroma jih vanjo izvozite s pomočjo ustreznih povezav (**Other Options**) (Druge možnosti) na strani za uvoz in izvoz.

OPOMBA: Ta funkcija uvaža in izvaža samo podatke za Password Manager. Če vas zanima, kako lahko varnostno kopirate in obnovite dodatne podatke HP Client Security, glejte Varnostno kopiranje in obnavljanje podatkov na strani 28.

Če želite uvoziti podatke iz datoteke varnostne kopije HP Client Security:

1. Na strani za uvoz in izvoz v programu HP Password Manager kliknite oziroma tapnite **Import data from an HP Client Security backup file** (Uvozite podatke iz datoteke varnostne kopije HP Client Security).
2. Preverite svojo identiteto.
3. Izberite prej ustvarjeno datoteko varnostne kopije ali v ponujeno polje vnesite pot, nato kliknite oziroma tapnite **Browse** (Prebrskaj).
4. Vnesite geslo, ki ste ga uporabili za zaščito datoteke, nato kliknite oziroma tapnite **Next** (Naprej).
5. Kliknite oziroma tapnite **Restore** (Obnovi).

Če želite izvoziti podatke v datoteko varnostne kopije HP Client Security:

1. Na strani za uvoz in izvoz v programu HP Password Manager kliknite oziroma tapnite **Export data from an HP Client Security backup file** (Izvozite podatke iz datoteke varnostne kopije HP Client Security).
2. Preverite svojo identiteto, nato kliknite oziroma tapnite **Next** (Naprej).
3. Vnesite ime za datoteko varnostne kopije. Privzeto se datoteka shrani v mapo Dokumenti. Če želite izbrati drugo lokacijo, kliknite oziroma tapnite **Browse** (Prebrskaj).
4. Vnesite in potrdite geslo, ki ste ga uporabili za zaščito datoteke, nato kliknite oziroma tapnite **Save** (Shrani).

Nastavitve

Password Manager lahko prilagodite po meri z nastavitvami:

- **Prompt to add logons for logon screens** (Poziv za dodajanje prijav za prijavne zaslone) – Ikona **Password Manager** z znakom plus je prikazana, kadar je zaznano spletno mesto ali program, kar pomeni, da za ta zaslon lahko dodate prijavo v meni **Logons** (Prijave).

  Če želite to možnost onemogočiti, počistite polje poleg **Prompt to add logons for logon screens** (Poziv za dodajanje prijav za prijavne zaslone).

- **Open Password Manager with Ctrl+Win+h** (Odpri Password Manager s Ctrl+Win+h) – Privzeta bližnjica, ki odpre meni **Password Manager Quick Links** (Hitre povezave za Password Manager), je Ctrl+tipka Windows +h.

  Če želite bližnjico spremeniti, kliknite oziroma tapnite to možnost, nato vnesite novo kombinacijo tipk. Kombinacije lahko vsebujejo eno ali več spodnjih možnosti: ctrl, alt ali shift, in katero koli črkovno ali številsko tipko.

  Kombinacij, ki so rezervirane za Windows ali programe Windows, ne morete uporabiti.

- Če želite obnoviti tovarniške vrednosti za nastavitve, kliknite oziroma tapnite **Restore defaults** (Obnovi privzeto).

Dodatne nastavitve

Skrbniki lahko dostopajo do spodnjih možnosti, tako da izberejo ikono **zobnika** (nastavitve) na začetni strani HP Client Security.

- **Administrator Policies** (Pravilniki za skrbnike) – Omogoča konfiguriranje pravilnikov za prijavo in seje za skrbnike.
- **Standard User Policies** (Pravilniki za standardne uporabnike) – Omogoča konfiguriranje pravilnikov za prijavo in seje za standardne uporabnike.
- **Security Features** (Varnostne funkcije) – Omogoča povečanje varnosti računalnika, tako da zaščiti vaš račun Windows z močnim preverjanjem pristnosti, oziroma tako, da omogoči preverjanje pristnosti pred zagonom sistema Windows.
- **Users** (Uporabniki) – Omogoča upravljanje uporabnikov in njihovih poverilnic.
- **My Policies** (Moji pravilniki) – Omogoča, da pregledate svoje pravilnike preverjanja pristnosti in stanje vpisa.
- **Backup and Restore** (Varnostno kopiranje in obnavljanje) – Omogoča, da varnostno kopirate ali obnovite podatke HP Client Security.
- **About HP Client Security** (Vizitka programa HP Client Security) – Prikaže podatke o različici programa HP Client Security.

Pravilniki za skrbnike

Za skrbnike v tem računalniku lahko konfigurirate pravilnike za prijavo in seje. Pravilniki za prijavo upravljajo poverilnice, ki so potrebne, da se lokalni skrbnik prijavi v Windows. Pravilniki za seje upravljajo poverilnice, ki so potrebne, da lokalni skrbnik preveri identiteto znotraj seje Windows.

Privzeto začnejo vsi novi ali spremenjeni pravilniki veljati takoj, ko tapnete oziroma kliknete **Apply** (Uporabi).

Če želite dodati nov pravilnik:

1. Na začetni strani HP Client Security kliknite oziroma tapnite ikono **zobnika**.
2. Na strani Advanced Settings (Dodatne nastavitve) kliknite oziroma tapnite **Administrator Policies** (Pravilniki za skrbnike).
3. Kliknite oziroma tapnite **Add new policy** (Dodaj nov pravilnik).
4. Kliknite puščice navzdol, da izberete primarne in (neobvezno) sekundarne poverilnice za novi pravilnik, nato kliknite oziroma tapnite **Add** (Dodaj).
5. Kliknite **Uporabi**.

Če želite, da nov ali spremenjen pravilnik stopi v veljavo pozneje:

1. Kliknite oziroma tapnite **Enforce this policy immediately** (Ta pravilnik uveljavi takoj).
2. Izberite **Enforce this policy on the specific date** (Ta pravilnik uveljavi na določen datum).
3. Vnesite datum oziroma na pojavnem koledarju izberite datum, ko naj ta pravilnik stopi v veljavo.
4. Če želite, določite tudi, kdaj naj bodo uporabniki opomnjeni na novi pravilnik.
5. Kliknite **Uporabi**.

Pravilniki za standardne uporabnike

Za standardne uporabnike v tem računalniku lahko konfigurirate pravilnike za prijavo in seje. Pravilniki za prijavo upravljajo poverilnice, ki so potrebne, da se standardni uporabnik prijavi v Windows. Pravilniki za seje upravljajo poverilnice, ki so potrebne, da standardni uporabnik preveri identiteto znotraj seje Windows.

Privzeto začnejo vsi novi ali spremenjeni pravilniki veljati takoj, ko tapnete oziroma kliknete **Apply** (Uporabi).

Če želite dodati nov pravilnik:

1. Na začetni strani HP Client Security kliknite oziroma tapnite ikono **zobnika**.
2. Na strani Advanced Settings (Dodatne nastavitve) kliknite oziroma tapnite **Standard User Policies** (Pravilniki za standardne uporabnike).
3. Kliknite oziroma tapnite **Add new policy** (Dodaj nov pravilnik).
4. Kliknite puščice navzdol, da izberete primarne in (neobvezno) sekundarne poverilnice za novi pravilnik, nato kliknite oziroma tapnite **Add** (Dodaj).
5. Kliknite **Uporabi**.

Če želite, da nov ali spremenjen pravilnik stopi v veljavo pozneje:

1. Kliknite oziroma tapnite **Enforce this policy immediately** (Ta pravilnik uveljavi takoj).
2. Izberite **Enforce this policy on the specific date** (Ta pravilnik uveljavi na določen datum).
3. Vnesite datum oziroma na pojavnem koledarju izberite datum, ko naj ta pravilnik stopi v veljavo.
4. Če želite, določite tudi, kdaj naj bodo uporabniki opomnjeni na novi pravilnik.
5. Kliknite **Uporabi**.

Varnostne funkcije

Omogočite lahko varnostne funkcije za HP Client Security, ki pomagajo računalnik ščititi pred nepooblaščenim dostopom.

Če želite nastaviti varnostne funkcije:

1. Na začetni strani HP Client Security kliknite oziroma tapnite ikono **zobnika**.
2. Na strani Advanced Settings (Dodatne nastavitve) kliknite oziroma tapnite **Security Features** (Varnostne funkcije).

3. Omogočite varnostne funkcije, tako da izberete potrditvena polja, nato kliknite oziroma tapnite **Apply** (Uporabi). Več funkcij kot izberete, bolj varen bo vaš računalnik.

   Nastavitve veljajo za vse uporabnike.

   - **Windows Logon Security** (Varnost ob prijavi v Windows) – Zaščitite račune Windows, tako da za dostop zahtevate uporabo poverilnic HP Client Security.
   - **Pre-Boot Security (Power-on authentication)** (Varnost pred zagonom (Preverjanje pristnosti pri vklopu)) – Zaščiti računalnik pred zagonom sistema Windows. Ta izbira ni na voljo, če je BIOS ne podpira.
   - **Allow One Step logon** (Dovoli prijavo v enem koraku) – Ta nastavitev omogoča, da preskočite prijavo v Windows, če je bilo preverjanje pristnosti pred tem opravljeno na ravni ob vklopu ali na ravni Drive Encryption.

4. Kliknite oziroma tapnite **Users** (Uporabniki), nato kliknite oziroma tapnite uporabnikovo ploščico.

Uporabniki

Uporabnike HP Client Security v tem računalniku lahko nadzirate in upravljate.

Če želite dodati novega uporabnika sistema Windows v HP Client Security:

1. Na začetni strani HP Client Security kliknite oziroma tapnite ikono **zobnika**.
2. Na strani Advanced Settings (Dodatne nastavitve) kliknite oziroma tapnite **Users** (Uporabniki).
3. Kliknite oziroma tapnite **Add another Windows user to HP Client Security** (Dodajanje novega uporabnika sistema Windows v HP Client Security).
4. Vnesite ime uporabnika, ki ga želite dodati, nato kliknite oziroma tapnite **OK** (V redu).
5. Vnesite geslo za Windows tega uporabnika.

   Na strani uporabnika bo prikazana ploščica za dodanega uporabnika.

Če želite izbrisati uporabnika sistema Windows iz HP Client Security:

1. Na začetni strani HP Client Security kliknite oziroma tapnite ikono **zobnika**.
2. Na strani Advanced Settings (Dodatne nastavitve) kliknite oziroma tapnite **Users** (Uporabniki).
3. Kliknite oziroma tapnite ime uporabnika, ki ga želite izbrisati.
4. Kliknite oziroma tapnite **Delete user** (Izbriši uporabnika), nato kliknite oziroma tapnite **Yes** (Da), da potrdite.

Če želite prikazati povzetek pravilnikov za prijavo in seje, ki so v veljavi za uporabnika:

▲ Kliknite oziroma tapnite **Users** (Uporabniki), nato kliknite oziroma tapnite uporabnikovo ploščico.

Moji pravilniki

Prikažete lahko svoje pravilnike preverjanja pristnosti ter stanje vpisa. Na strani My Policies (Moji pravilniki) so tudi povezave na stran s pravilniki za skrbnike ter na stran s pravilniki za standardne uporabnike.

1. Na začetni strani HP Client Security kliknite oziroma tapnite ikono **zobnika**.
2. Na strani Advanced Settings (Dodatne nastavitve) kliknite oziroma tapnite **My Policies** (Moji pravilniki).

   Prikazani so pravilniki za prijavo in seje, ki so v veljavi za trenutno prijavljenega uporabnika.

Na strani My Policies (Moji pravilniki) so tudi povezave na Pravilniki za skrbnike na strani 25 in Pravilniki za standardne uporabnike na strani 26.

Varnostno kopiranje in obnavljanje podatkov

Priporočamo, da svoje podatke HP Client Security redno varnostno kopirate. Kako pogosto varnostno kopirate, je odvisno od tega, kako pogosto se podatki spreminjajo. Če na primer vsak dan dodajate nove prijave, tudi varnostno kopirajte vsak dan.

Varnostne kopije lahko uporabljate za selitev z enega računalnika na drugega. To se imenuje tudi uvoz in izvoz.

OPOMBA: Ta funkcija varnostno kopira samo Password Manager. Funkcija Drive Encryption ima ločen postopek varnostnega kopiranja. Device Access Manager in preverjanje pristnosti s prstnimi odtisi se ne bosta varnostno kopirala.

Preden je podatke mogoče obnoviti iz datoteke varnostne kopije, mora biti HP Client Security nameščen v vsakem računalniku, ki bo sprejel varnostno kopirane podatke.

Če želite varnostno kopirati podatke:

1. Na začetni strani HP Client Security kliknite oziroma tapnite ikono **zobnika**.
2. Na strani Advanced Settings (Dodatne nastavitve) kliknite oziroma tapnite **Administrator Policies** (Pravilniki za skrbnike).
3. Kliknite oziroma tapnite **Backup and Restore** (Varnostno kopiranje in obnovitev).
4. Kliknite oziroma tapnite **Backup** (Varnostno kopiranje), nato preverite svojo identiteto.
5. Izberite modul, ki ga želite vključiti v varnostno kopijo, nato kliknite oziroma tapnite **Next** (Naprej).
6. Vnesite ime za datoteko, ki bo shranjena. Privzeto se datoteka shrani v mapo Dokumenti. Če želite izbrati drugo lokacijo, kliknite oziroma tapnite **Browse** (Prebrskaj).
7. Vnesite in potrdite geslo, da zaščitite datoteko.
8. Kliknite oziroma tapnite **Save** (Shrani).

Če želite obnoviti podatke:

1. Na začetni strani HP Client Security kliknite oziroma tapnite ikono **zobnika**.
2. Na strani Advanced Settings (Dodatne nastavitve) kliknite oziroma tapnite **Administrator Policies** (Pravilniki za skrbnike).
3. Kliknite oziroma tapnite **Backup and Restore** (Varnostno kopiranje in obnovitev).
4. Izberite **Restore** (Obnovi), nato preverite svojo identiteto.
5. Izberite pred tem ustvarjeno datoteko za shranjevanje. Vnesite pot v ponujeno polje. Če želite izbrati drugo lokacijo, kliknite oziroma tapnite **Browse** (Prebrskaj).
6. Vnesite geslo, ki ste ga uporabili za zaščito datoteke, nato kliknite oziroma tapnite **Next** (Naprej).

7. Izberite module, za katere želite obnoviti podatke.
8. Kliknite oziroma tapnite **Restore** (Obnovi).

5 HP Drive Encryption (samo nekateri modeli)

HP Drive Encryption nudi celostno zaščito podatkov, tako da šifrira podatke v vašem računalniku. Ko je šifriranje pogonov aktivirano, se morate prijaviti na prijavnem zaslonu modula Drive Encryption, ki se odpre pred zagonom operacijskega sistema Windows®.

Začetni zaslon HP Client Security omogoča skrbnikom sistema Windows, da aktivirajo Drive Encryption, varnostno kopirajo ključ šifriranja ter izberejo oziroma prekličejo izbiro pogonov ali particij za šifriranje. Za več informacij glejte pomoč za programsko opremo HP Client Security.

Z Drive Encryption lahko izvedete naslednja opravila:

- Izbira nastavitev za Drive Encryption:
  - Šifriranje ali dešifriranje posameznih pogonov ali particij s programskim šifriranjem
  - Šifriranje ali dešifriranje posameznih samo-šifrirnih pogonov s strojnim šifriranjem
  - Dodajanje dodatne varnosti, tako da onemogočite stanje spanja ali pripravljenosti in zagotovite, da bo vedno zahtevano preverjanje pristnosti pred zagonom s programom Drive Encryption

OPOMBA: Šifrirati je mogoče le notranje trde diske SATA in zunanje diske eSATA.

- Ustvarjanje varnostnih ključev
- Obnavljanje dostopa do šifriranega računalnika z varnostnimi ključi in programom HP SpareKey
- Omogočanje preverjanja pristnosti pred zagonom s programom Drive Encryption z geslom, vpisanim prstnim odtisom ali kodo PIN za nekatere pametne kartice

Odpiranje programa Drive Encryption

Skrbniki imajo dostop do programa Drive Encryption znotraj programa HP Client Security:

1. Na začetnem zaslonu kliknite oziroma tapnite program **HP Client Security** (Windows 8).

   – ali –

   Na namizju Windows dvokliknite ali dvotapnite ikono **HP Client Security** v območju za obvestila, ki ga najdete na skrajni desni strani opravilne vrstice.

2. Kliknite oziroma tapnite ikono **Drive Encryption**.

Splošna opravila

Aktiviranje programa Drive Encryption za standardni trdi disk

Standardni trdi diski so šifrirani s programskim šifriranjem. Za šifriranje pogona ali particije diska sledite tem korakom:

1. Zaženite **Drive Encryption**. Za več informacij, glejte Odpiranje programa Drive Encryption na strani 30.
2. Izberite potrditveno polje za pogon ali particijo, ki ju želite šifrirati, nato kliknite oziroma tapnite **Backup Key** (Ključ za varnostno kopiranje).

OPOMBA: Za boljšo varnost potrdite polje **Disable sleep mode for increased security** (Za večjo varnost onemogoči način spanja). Ko onemogočite način spanja, izgine vsako tveganje, da bi se poverilnice za odklepanje pogona shranile v pomnilnik.

3. Izberite vsaj eno možnost varnostnega kopiranja, nato kliknite oziroma tapnite **Backup** (Varnostno kopiraj). Za več informacij, glejte Varnostno kopiranje ključev šifriranja na strani 34.
4. Medtem ko se ključ šifriranja varnostno kopira, lahko delate dalje. Računalnika ne zaganjajte ponovno.

OPOMBA: Računalnik vas pozove, da ga ponovno zaženite. Po ponovnem zagonu bo prikazan zaslon šifriranega pogona pred zagonom, ki zahteva preverjanje pristnosti, preden se zažene Windows.

Drive Encryption je aktiviran. Šifriranje izbranih pogonskih particij lahko traja več ur, glede na število in velikost particij.

Za več informacij glejte pomoč za programsko opremo HP Client Security.

Aktiviranje programa Drive Encryption za samo-šifrirni pogon

Samo-šifrirne pogone, ki ustrezajo specifikaciji Trusted Computing Group OPAL za upravljanje samo-šifrirnih pogonov, je mogoče šifrirati ali s programskim ali s strojnim šifriranjem. Strojno šifriranje je veliko hitrejše od programskega šifriranja. Ne morete pa izbrati, katere particije na disku želite šifrirati. Šifrira se celotni disk, vključno s particijami.

Če želite šifrirati posamezne particije, morate uporabiti programsko šifriranje. Obvezno počistite polje **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Dovoli samo strojno šifriranje za samo-šifrirne pogone (SED)).

Če želite aktivirati Drive Encryption za samo-šifrirne pogone, sledite tem korakom:

1. Zaženite **Drive Encryption**. Za več informacij, glejte Odpiranje programa Drive Encryption na strani 30.
2. Izberite potrditveno polje za pogon, ki ga želite šifrirati, nato kliknite oziroma tapnite **Backup Key** (Ključ za varnostno kopiranje).

OPOMBA: Za boljšo varnost potrdite polje **Disable Sleep Mode for added security** (Za večjo varnost onemogoči način spanja). Ko onemogočite način spanja, izgine vsako tveganje, da bi se poverilnice za odklepanje pogona shranile v pomnilnik.

3. Izberite vsaj eno možnost varnostnega kopiranja, nato kliknite oziroma tapnite **Backup** (Varnostno kopiraj). Za več informacij, glejte Varnostno kopiranje ključev šifriranja na strani 34.
4. Medtem ko se ključ šifriranja varnostno kopira, lahko delate dalje. Računalnika ne zaganjajte ponovno.

OPOMBA: Pri samo-šifrirnih pogonih vas računalnik pozove, da ga zaustavite.

Za več informacij glejte pomoč za programsko opremo HP Client Security.

Deaktiviranje programa Drive Encryption

1. Zaženite **Drive Encryption**. Za več informacij, glejte Odpiranje programa Drive Encryption na strani 30.
2. Počistite potrditveno polje za vse šifrirane pogone, nato kliknite oziroma tapnite **Apply** (Uporabi).

   Deaktiviranje programa Drive Encryption se začne.

OPOMBA: Če je bilo uporabljeno programsko šifriranje, se začne dešifriranje. To lahko traja več ur, glede na velikost šifriranih particij trdega diska. Ko je dešifriranje končano, se Drive Encryption deaktivira.

Če je bilo uporabljeno strojno šifriranje, se pogon takoj dešifrira, po nekaj minutah pa se tudi Drive Encryption deaktivira.

Ko bo program Drive Encryption deaktiviran, boste pozvani, da zaustavite računalnik, če je bilo uporabljeno strojno šifriranje, oziroma da ga ponovno zaženete, če je bilo uporabljeno programsko šifriranje.

Prijava po aktiviranju programa Drive Encryption

Ko vklopite računalnik, potem ko je bil aktiviran program Drive Encryption, in je vaš uporabniški račun vpisan, se morate prijaviti na prijavnem zaslonu za Drive Encryption:

OPOMBA: Pri prehodu iz spanja ali stanja pripravljenosti za programsko šifriranje ali strojno šifriranje ni prikazano preverjanje pristnosti Drive Encryption pred zagonom. Strojno šifriranje vsebuje možnost **Disable sleep mode for increased security** (Za večjo varnost onemogoči način spanja), ki preprečuje prehod v spanje ali stanje pripravljenosti, ko je omogočena.

Pri prehodu iz stanja mirovanja je tako za programsko šifriranje kot za strojno šifriranje prikazano preverjanje pristnosti Drive Encryption pred zagonom.

OPOMBA: Če je skrbnik sistema Windows v programu HP Client Security omogočil predzagonsko varnost v BIOS-u in če je omogočena prijava v enem koraku (privzeto), se lahko v računalnik prijavite takoj po preverjanju pristnosti pred zagonom v BIOS-u, ne da bi morali znova preveriti pristnost na prijavnem zaslonu programa Drive Encryption.

Prijava enega uporabnika:

- Na strani **Logon** (Prijava) vpišite svoje geslo za Windows, kodo PIN pametne kartice, SpareKey, oziroma podrsajte vpisan prst.

Prijava več uporabnikov:

1. Na strani **Select user to logon** (Izbira uporabnika za prijavo) na spustnem seznamu izberite uporabnika, ki se prijavlja, nato kliknite oziroma tapnite **Next** (Naprej).
2. Na strani **Logon** (Prijava) vpišite svoje geslo za Windows ali kodo PIN pametne kartice oziroma podrsajte vpisan prst.

OPOMBA: Podprte so te pametne kartice:

Podprte pametne kartice

- Gemalto Cyberflex Access 64k V2c

OPOMBA: Če se na zaslonu Drive Encryption za prijavo prijavljate z obnovitvenim ključem, bodo pri prijavi v Windows za dostop do uporabniških računov potrebne dodatne poverilnice.

Šifriranje dodatnih trdih diskov

Močno priporočamo, da za zaščito svojih podatkov uporabite HP Drive Encryption in šifrirate trdi disk. Po aktiviranju lahko šifrirate tudi dodatne trde diske ali particije, ki ste jih ustvarili, in sicer:

1. Zaženite **Drive Encryption**. Za več informacij, glejte Odpiranje programa Drive Encryption na strani 30.
2. Pri programsko šifriranih pogonih izberite particije pogona, ki jih želite šifrirati.

OPOMBA: To velja tudi v primerih mešanih pogonov, kjer je prisoten vsaj en standardni trdi disk in vsaj en samo-šifrirni pogon.

– ali –

▲ Pri strojno šifriranih pogonih izberite dodatne pogone, ki jih želite šifrirati.

Napredna opravila

Upravljanje programa Drive Encryption (skrbniško opravilo)

Skrbniki lahko s programom Drive Encryption pregledujejo in spreminjajo stanje šifriranja (Ni šifrirano ali Šifrirano) vseh trdih diskov v računalniku.

- Če je stanje Omogočeno, je Drive Encryption aktiviran in konfiguriran. Pogon je v enem od teh stanj:

Programsko šifriranje

- Ni šifrirano
- Šifrirano
- Šifriranje
- Dešifriranje

Strojno šifriranje

- Šifrirano
- Ni šifrirano (za dodatne pogone)

Šifriranje in dešifriranje posameznih particij pogona (samo programsko šifriranje)

Skrbniki lahko s programom Drive Encryption šifrirajo eno ali več particij trdega diska v računalniku oziroma dešifrirajo particije trdega diska, ki so bile že šifrirane.

1. Zaženite **Drive Encryption**. Za več informacij, glejte Odpiranje programa Drive Encryption na strani 30.
2. V možnosti **Drive Status** (Stanje pogona) izberite oziroma počistite potrditveno polje ob vsaki particiji trdega diska, ki jo želite šifrirati ali dešifrirati, nato kliknite oziroma tapnite **Apply** (Uporabi).

OPOMBA: Medtem ko se particija šifrira ali dešifrira, vrstica napredovanja prikazuje odstotek šifriranosti particije.

OPOMBA: Dinamične particije niso podprte. Če je prikazano, da je particija na voljo, toda ko jo izberete, je ne morete šifrirati, je to dinamična particija. Dinamična particija nastane, ko z Upravljanjem diskov skrčite particijo, da bi ustvarili novo particijo.

Če bo particija pretvorjena v dinamično particijo, se prikaže opozorilo.

Upravljanje diskov

- **Vzdevek** – Svojim pogonom in particijam lahko daste imena, da jih boste lažje prepoznali.
- **Nepovezani pogoni** – Drive Encryption lahko sledi diskom, ki jih odstranite iz računalnika. Disk, ki ga odstranite iz računalnika, se samodejno premakne na seznam Nepovezanih. Če disk vrnete v sistem, se spet pojavi na seznamu Povezanih.
- Če določenega nepovezanega pogona ni treba več spremljati, ga lahko odstranite s seznama nepovezanih.
- Drive Encryption ostane aktiviran, dokler niso počiščena vsa polja za povezane pogone in dokler ni seznam nepovezanih prazen.

Varnostno kopiranje in obnovitev (skrbniško opravilo)

Ko je Drive Encryption aktiviran, skrbniki lahko na strani Varnostno kopiranje ključa šifriranja varnostno kopirajo ključe šifriranja na izmenljive medije ter izvedejo obnovitev.

Varnostno kopiranje ključev šifriranja

Skrbniki lahko varnostno kopirajo ključ šifriranja za šifriran pogon na izmenljivo napravo za shranjevanje.

POZOR: Pazite, da bo naprava za shranjevanje z varnostno kopiranim ključem na varnem. Če pozabite geslo, izgubite pametno kartico ali nimate vpisanega prsta, bo ta naprava vaš edini dostop do računalnika. Kraj za shranjevanje mora biti tudi zavarovan, ker naprava za shranjevanje omogoča dostop do sistema Windows.

1. Zaženite **Drive Encryption**. Za več informacij, glejte Odpiranje programa Drive Encryption na strani 30.
2. Potrdite polje za želeni pogon, nato kliknite oziroma tapnite **Backup Key** (Ključ za varnostno shranjevanje).

3. V možnosti **Ustvari obnovitveni ključ HP Drive Encryption** izberite vsaj eno od teh možnosti:

   - **Removable Storage** (Izmenljiva shramba) – Potrdite polje, nato izberite napravo za shranjevanje, na kateri bo shranjen ključ šifriranja.
   - **SkyDrive** – Izberite potrditveno polje. Povezani morate biti v internet. Prijavite se v Microsoft SkyDrive, nato kliknite oziroma tapnite **Yes** (Da).

   OPOMBA: Če želite uporabiti varnostno kopirani ključ HP Drive Encryption, ki je shranjen v storitvi SkyDrive, ga morate prenesti iz storitve SkyDrive v izmenljivo napravo za shranjevanje, nato pa to napravo vstaviti v računalnik.

   - **TPM** (samo nekateri modeli) – Omogoča obnovitev podatkov z geslom TPM.

   POZOR: Če počistite TPM ali se računalnik poškoduje, boste izgubili dostop do varnostne kopije. Če izberete ta način, izberite tudi dodaten način varnostnega kopiranja.

4. Kliknite oziroma tapnite **Backup** (Varnostno kopiranje).

   Ključ šifriranja se shrani na napravi za shranjevanje, ki ste jo izbrali.

Obnavljanje dostopa do aktiviranega računalnika z varnostno kopiranimi ključi

Skrbniki lahko izvedejo obnovitev s ključem Drive Encryption, ki je bil varnostno kopiran na izmenljivo napravo za shranjevanje ob aktivaciji, ali pa tako, da izberejo možnost **Backup Key** (Ključ za varnostno kopiranje) v programu Drive Encryption.

1. Vstavite izmenljivo napravo za shranjevanje, ki vsebuje vaš varnostno kopirani ključ.
2. Vklopite računalnik.
3. Ko se pojavi prijavno pogovorno okno HP Drive Encryption, kliknite oziroma tapnite **Recovery** (Obnovitev).
4. Vnesite pot do datoteke ali ime datoteke, ki vsebuje vaš varnostno kopirani ključ, nato kliknite oziroma tapnite **Recovery** (Obnovitev).
5. Ko se odpre pogovorno okno za potrditev, kliknite oziroma tapnite **OK** (V redu).

   Pokaže se prijavni zaslon za Windows.

OPOMBA: Če se na zaslonu Drive Encryption za prijavo prijavljate z obnovitvenim ključem, bodo pri prijavi v Windows za dostop do uporabniških računov potrebne dodatne poverilnice. Močno priporočamo, da po končani obnovitvi ponastavite geslo.

Izvajanje obnovitve HP SpareKey

Obnovitev SpareKey s predzagonskim šifriranjem pogona zahteva, da pravilno odgovorite na vprašanja, preden lahko dostopate do računalnika. Za več informacij o nastavljanju obnovitve SpareKey glejte pomoč za programsko opremo HP Client Security.

Izvajanje obnovitve HP SpareKey, če pozabite geslo:

1. Vklopite računalnik.
2. Ko se prikaže stran HP Drive Encryption, poiščite stran za prijavo uporabnika.

3. Kliknite **SpareKey**.

OPOMBA: Če vaš SpareKey še ni bil inicializiran v programu HP Client Security, gumb **SpareKey** ni na voljo.

4. Vnesite pravilne odgovore na prikazana vprašanja in nato kliknite **Logon** (Prijava).

   Pokaže se prijavni zaslon za Windows.

OPOMBA: Če se na zaslonu Drive Encryption za prijavo prijavljate z orodjem SpareKey, bodo pri prijavi v Windows za dostop do uporabniških računov potrebne dodatne poverilnice. Močno priporočamo, da po končani obnovitvi ponastavite geslo.

6 HP File Sanitizer (samo nekateri modeli)

File Sanitizer omogoča, da varno izbrišete sredstva (na primer: osebne podatke ali datoteke, zgodovinske ali s spletom povezane podatke ter druge podatkovne komponente) na notranjem trdem disku računalnika, ter da redno prepisujete notranji trdi disk računalnika.

Programa File Sanitizer ne morete uporabiti za čiščenje ali prepisovanje teh vrst pogonov:

- fiksni pogoni (SSD), vključno z nosilci RAID, ki obsegajo napravo SSD
- zunanji pogoni, priključeni prek vmesnikov USB, Firewire ali eSATA

Če na disku SSD poskušate izvesti operacijo varnega brisanja ali prepisovanja, bo prikazano opozorilno sporočilo, operacija pa se ne bo izvedla.

Varno brisanje

Varno brisanje se razlikuje od običajnega postopka brisanja v sistemu Windows®. Ko sredstvo varno izbrišete s programom File Sanitizer, se datoteke prepišejo z nesmiselnimi podatki, tako da je praktično nemogoče znova pridobiti prvotno sredstvo. Preprosto dejanje brisanja v sistemu Windows lahko pusti datoteko (ali sredstvo) nedotaknjeno na trdem disku ali v stanju, v katerem jo je mogoče s forenzičnimi postopki obnoviti.

Čas varnega brisanja lahko določite vnaprej, lahko pa tudi ročno aktivirate varno brisanje, tako da izberete ikono **File Sanitizer** na domačem zaslonu HP Client Security oziroma z ikono **File Sanitizer** na namizju Windows. Za več informacij glejte Določanje urnika varnega brisanja na strani 39, Varno brisanje z desnim klikom na strani 41 ali Ročni zagon operacije varnega brisanja na strani 41.

OPOMBA: Datoteka .dll se varno izbriše in odstrani iz sistema le, če je bila premaknjena v koš.

Prepisovanje praznega prostora

Če v sistemu Windows izbrišete sredstvo, se njegova vsebina ne odstrani popolnoma s trdega diska. Windows izbriše samo sklic na sredstvo oziroma njegovo lokacijo na trdem disku. Vsebina sredstva pa ostane na trdem disku, dokler tega istega mesta na trdem disku ne prepiše drugo sredstvo z novimi podatki.

Prepisovanje praznega prostora omogoča, da varno zapisujete naključne podatke čez izbrisana sredstva, kar uporabnikom preprečuje, da bi videli prvotno vsebino izbrisanega sredstva.

OPOMBA: Prepisovanje praznega prostora ne nudi dodatne varnosti za varno izbrisana sredstva.

Čas prepisovanja praznega prostora lahko določite vnaprej, lahko pa tudi ročno aktivirate prepisovanje praznega prostora, tako da izberete ikono **File Sanitizer** na domačem zaslonu HP Client Security oziroma z ikono **File Sanitizer** na namizju Windows. Za več informacij glejte Določanje urnika prepisovanja praznega prostora na strani 40, Ročni zagon prepisovanja praznega prostora na strani 42 ali Uporaba ikone File Sanitizer na strani 41.

Odpiranje programa File Sanitizer

1. Na začetnem zaslonu kliknite oziroma tapnite program **HP Client Security** (Windows 8).

   – ali –

   Na namizju Windows dvokliknite ali dvotapnite ikono **HP Client Security** v območju za obvestila, ki ga najdete na skrajni desni strani opravilne vrstice.

2. V možnosti **Data** (Podatki) kliknite oziroma tapnite **File Sanitizer**.

– ali –

▲ Dvokliknite oziroma dvotapnite ikono **File Sanitizer** na namizju sistema Windows.

– ali –

▲ Z desno miškino tipko kliknite oziroma tapnite in pridržite ikono **File Sanitizer** na namizju Windows, nato izberite **Open File Sanitizer** (Odpri File Sanitizer).

Postopki nastavitve

Shredding (Varno brisanje) – File Sanitizer varno izbriše izbrane kategorije sredstev.

1. V možnosti **Shredding** (Varno brisanje) potrdite polje za vsako od vrst datotek, ki jih želite izbrisati, oziroma počistite polje, če teh datotek nočete izbrisati.
   - **Recycle Bin** (Koš) – Elementi v košu bodo varno izbrisani.
   - **Temporary system files** (Začasne sistemske datoteke) – Varno izbriše vse datoteke, najdene v začasni mapi sistema. Naslednje okoljske spremenljivke bodo preiskane po tem vrstnem redu, in prva najdena pot velja za mapo sistema:
     - TMP
     - TEMP
   - **Temporary Internet files** (Začasne internetne datoteke) – Varno izbriše kopije spletnih strani, slik in predstavnosti, ki jih spletni brskalniki shranijo za hitrejši ogled.
   - **Cookies** (Piškotki) – Varno izbriše vse datoteke, ki jih spletna mesta shranjujejo v računalniku zaradi shranjevanja nastavitev, na primer prijavnih podatkov.
2. Za začetek varnega brisanja kliknite oziroma tapnite **Shred** (Varno izbriši).

Bleaching (Prepisovanje) – Zapiše naključne podatke v prazen prostor in preprečuje obnavljanje izbrisanih elementov.

▲ Za začetek prepisovanja kliknite oziroma tapnite **Bleach** (Prepiši).

File Sanitizer Options (Možnosti programa File Sanitizer) – Izberite potrditveno polje, da omogočite posamezne možnosti, oziroma počistite polje, da jih onemogočite:

- **Enable Desktop icon** (Omogoči ikono na namizju) – Prikaže ikono programa File Sanitizer na namizju sistema Windows.
- **Enable right-click** (Omogoči klik z desno tipko) – Omogoča, da z desno tipko miške kliknete oziroma tapnete in pridržite sredstvo, nato pa izberete **HP File Sanitizer – Shred** (HP File Sanitizer – Varno izbriši).

- **Ask for Windows password before manual shredding** (Pred ročnim varnim brisanjem zahtevaj geslo sistema Windows) – Zahteva preverjanje pristnosti z geslom za Windows, preden ročno varno izbrišete element.
- **Shred Cookies and Temporary Internet Files on browser close** (Varno izbriši piškotke in začasne internetne datoteke ob izhodu iz brskalnika) – Varno izbriše vsa izbrana sredstva, povezana s spletom, na primer zgodovino URL-jev v brskalniku, ko zaprete spletni brskalnik.

Določanje urnika varnega brisanja

Za samodejno varno brisanje lahko vnaprej določite čas, lahko pa sredstva kadar koli izbrišete tudi ročno. Za več informacij glejte Postopki nastavitve na strani 38.

1. Odprite File Sanitizer ter kliknite oziroma tapnite **Settings** (Nastavitve).
2. Če želite določiti čas v prihodnosti za varno brisanje izbranih sredstev, v možnosti **Shred Schedule** (Urnik varnega brisanja) izberite **Never** (Nikoli), **Once** (Enkrat), **Daily** (Vsak dan), **Weekly** (Vsak teden) ali **Monthly** (Vsak mesec), nato izberite datum in čas:
   a. Kliknite oziroma tapnite uro, minuto ali polje za dopoldne/popoldne.
   b. Pomikajte se do želene vrednosti, ki naj bo prikazana na isti ravni kot druga polja.
   c. Kliknite oziroma tapnite v beli prostor okoli polj za nastavitev časa.
   d. Ponovite za vsako polje, dokler ni določen pravilni urnik.
3. Navedene so te štiri vrste sredstev:
   - **Recycle Bin** (Koš) – Elementi v košu bodo varno izbrisani.
   - **Temporary system files** (Začasne sistemske datoteke) – Varno izbriše vse datoteke, najdene v začasni mapi sistema. Naslednje okoljske spremenljivke bodo preiskane po tem vrstnem redu, in prva najdena pot velja za mapo sistema:
     - TMP
     - TEMP
   - **Temporary Internet files** (Začasne internetne datoteke) – Varno izbriše kopije spletnih strani, slik in predstavnosti, ki jih spletni brskalniki shranijo za hitrejši ogled.
   - **Cookies** (Piškotki) – Varno izbriše vse datoteke, ki jih spletna mesta shranjujejo v računalniku zaradi shranjevanja nastavitev, na primer prijavnih podatkov.

   Če je polje teh sredstev potrjeno, bodo ob predvidenem času izbrisana.
4. Če želite izbrati dodatna sredstva po meri za varno brisanje:
   a. V možnosti **Scheduled Shred List** (Seznam Urnik varnega brisanja) kliknite oziroma tapnite **Add folder** (Dodaj mapo), nato poiščite datoteko oziroma mapo.
   b. Kliknite oziroma tapnite **Open** (Odpri), nato kliknite oziroma tapnite **OK** (V redu).

   Če želite s seznama urnika varnega brisanja odstraniti sredstvo, počistite njegovo potrditveno polje.

Določanje urnika prepisovanja praznega prostora

Prepisovanje praznega prostora ne nudi dodatne varnosti za varno izbrisana sredstva.

1. Odprite File Sanitizer ter kliknite oziroma tapnite **Settings** (Nastavitve).
2. Če želite, da se prepisovanje trdega diska izvede ob načrtovanem času v prihodnosti, pri možnosti **Bleach Schedule** (Urnik prepisovanja) izberite **Never** (Nikoli), **Once** (Enkrat), **Daily** (Dnevno), **Weekly** (Tedensko) ali **Monthly** (Mesečno), in nato izberite dan in uro.
   a. Kliknite oziroma tapnite uro, minuto ali polje za dopoldne/popoldne.
   b. Pomikajte se do želenega časa, ki naj bo prikazan na isti ravni kot druga polja.
   c. Kliknite oziroma tapnite v beli prostor okoli polj za nastavitev časa.
   d. Ponavljajte, dokler ni nastavljen pravilni urnik.

OPOMBA: Operacija prepisovanja praznega prostora lahko vzame precej časa. Poskrbite, da bo računalnik priključen na omrežno napajanje. Čeprav prepisovanje praznega prostora teče v ozadju, lahko povečana uporaba procesorja vpliva na učinkovitost računalnika. Prepisovanje praznega prostora lahko izvedete po koncu delovnega časa ali ko računalnika ne uporabljate.

Zaščita datotek pred varnim brisanjem

Če želite zaščititi datoteke ali mape pred varnim brisanjem:

1. Odprite File Sanitizer ter kliknite oziroma tapnite **Settings** (Nastavitve).
2. V možnosti **Never Shred List** (Seznam Nikoli ne izvedi varnega brisanja) kliknite oziroma tapnite **Add folder** (Dodaj mapo), nato poiščite datoteko oziroma mapo.
3. Kliknite oziroma tapnite **Open** (Odpri), nato kliknite oziroma tapnite **OK** (V redu).

OPOMBA: Datoteke na tem seznamu so zaščitene, dokler so na seznamu.

Če želite s seznama izjem odstraniti sredstvo, počistite njegovo potrditveno polje.

Splošna opravila

File Sanitizer uporabite za naslednja opravila:

- **Use the File Sanitizer icon to initiate shredding** (Z ikono programa File Sanitizer zaženi varno brisanje) – Povlecite datoteke na ikono programa **File Sanitizer** na namizju sistema Windows. Za podrobnosti glejte Uporaba ikone File Sanitizer na strani 41.
- **Manually shred a specific asset or all selected assets** (Ročno varno izbriši določeno sredstvo ali vsa izbrana sredstva) – Kadar koli varno izbrišite elemente, brez čakanja na urnik za varno brisanje. Za podrobnosti glejte Varno brisanje z desnim klikom na strani 41 ali Ročni zagon operacije varnega brisanja na strani 41.
- **Manually activate free space bleaching** (Ročno aktiviraj prepisovanje praznega prostora) – Kadar koli aktivirajte prepisovanje praznega prostora. Za podrobnosti glejte Ročni zagon prepisovanja praznega prostora na strani 42.
- **View the log files** (Ogled dnevniških datotek) – Oglejte si dnevniške datoteke o varnem brisanju in prepisovanju praznega prostora, ki vsebujejo morebitne napake ali neuspehe zadnje operacije varnega brisanja oziroma prepisovanja praznega prostora. Za podrobnosti glejte Ogled dnevniških datotek na strani 42.

OPOMBA: Operacija varnega brisanja ali prepisovanja praznega prostora lahko vzame precej časa. Čeprav varno brisanje in prepisovanje praznega prostora tečeta v ozadju, lahko povečana uporaba procesorja vpliva na učinkovitost računalnika.

Uporaba ikone File Sanitizer

POZOR: Sredstev, ki so bila varno izbrisana, ni mogoče obnoviti. Dobro premislite, katere elemente boste izbrali za ročno varno brisanje.

Ko operacijo varnega brisanja zaženete ročno, se varno izbriše vsebina standardnega seznama varnostnega brisanja v pogledu File Sanitizer (glejte Postopki nastavitve na strani 38).

Operacijo varnega brisanja lahko zaženete ročno tako:

1. Odprite File Sanitizer (glejte Odpiranje programa File Sanitizer na strani 38), nato kliknite oziroma tapnite **Shred** (Varno izbriši).
2. Ko se odpre pogovorno okno za potrditev, se prepričajte, da so sredstva, ki jih želite varno izbrisati, obkljukana, nato kliknite oziroma tapnite **OK** (V redu).

– ali –

1. Z desno miškino tipko kliknite oziroma tapnite in pridržite ikono **File Sanitizer** na namizju Windows, nato kliknite oziroma tapnite **Shred Now** (Varno izbriši zdaj).
2. Ko se odpre pogovorno okno za potrditev, se prepričajte, da so sredstva, ki jih želite varno izbrisati, obkljukana, nato kliknite oziroma tapnite **Shred** (Varno izbriši).

Varno brisanje z desnim klikom

POZOR: Sredstev, ki so bila varno izbrisana, ni mogoče obnoviti. Dobro premislite, katere elemente boste izbrali za ročno varno brisanje.

Če je bila izbrana možnost **Enable right-click shredding** (Omogoči varno brisanje z desno tipko miške) v pogledu File Sanitizer, sredstvo lahko izbrišete tako:

1. Poiščite dokument ali mapo, ki jo želite varno izbrisati.
2. Z desno tipko miške kliknite oziroma tapnite in pridržite datoteko oziroma mapo, nato izberite **HP File Sanitizer – Shred** (HP File Sanitizer – Varno izbriši).

Ročni zagon operacije varnega brisanja

POZOR: Sredstev, ki so bila varno izbrisana, ni mogoče obnoviti. Dobro premislite, katere elemente boste izbrali za ročno varno brisanje.

Ko operacijo varnega brisanja zaženete ročno, se varno izbriše vsebina standardnega seznama varnostnega brisanja v pogledu File Sanitizer (glejte Postopki nastavitve na strani 38).

Operacijo varnega brisanja lahko zaženete ročno tako:

1. Odprite File Sanitizer (glejte Odpiranje programa File Sanitizer na strani 38), nato kliknite oziroma tapnite **Shred** (Varno izbriši).
2. Ko se odpre pogovorno okno za potrditev, se prepričajte, da so sredstva, ki jih želite varno izbrisati, obkljukana, nato kliknite oziroma tapnite **OK** (V redu).

– ali –

1. Z desno miškino tipko kliknite oziroma tapnite in pridržite ikono **File Sanitizer** na namizju Windows, nato kliknite oziroma tapnite **Shred Now** (Varno izbriši zdaj).
2. Ko se odpre pogovorno okno za potrditev, se prepričajte, da so sredstva, ki jih želite varno izbrisati, obkljukana, nato kliknite oziroma tapnite **Shred** (Varno izbriši).

Ročni zagon prepisovanja praznega prostora

Ko operacijo prepisovanja zaženete ročno, se prepiše vsebina standardnega seznama varnostnega brisanja v pogledu File Sanitizer (glejte Postopki nastavitve na strani 38).

Operacijo prepisovanja lahko zaženete ročno tako:

1. Odprite File Sanitizer (glejte Odpiranje programa File Sanitizer na strani 38), nato kliknite oziroma tapnite **Bleach** (Prepiši).
2. Ko se odpre pogovorno okno za potrditev, kliknite oziroma tapnite **OK** (V redu).

– ali –

1. Z desno miškino tipko kliknite oziroma tapnite in pridržite ikono **File Sanitizer** na namizju Windows, nato kliknite oziroma tapnite **Bleach Now** (Prepiši zdaj).
2. Ko se odpre pogovorno okno za potrditev, kliknite oziroma tapnite **Bleach** (Prepiši).

Ogled dnevniških datotek

Ob vsaki operaciji varnega brisanja ali prepisovanja praznega prostora se ustvarita dnevniški datoteki z zapisi morebitnih napak ali neuspehov. Dnevniški datoteki sta vedno posodobljeni na najnovejšo operacijo varnega brisanja oziroma prepisovanja praznega prostora.

OPOMBA: Datoteke, ki so bile uspešno varno izbrisane ali prepisane, niso prikazane v dnevniških datotekah.

Ena dnevniška datoteka se ustvari za operacije varnega brisanja, druga pa za operacije prepisovanja praznega prostora. Obe dnevniški datoteki najdete na trdem disku v naslednjih mapah:

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

V 64-bitnih sistemih obe dnevniški datoteki najdete na trdem disku v naslednjih mapah:

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

7 HP Device Access Manager (samo nekateri modeli)

HP Device Access Manager nadzira dostop do podatkov, tako da onemogoča naprave za prenos podatkov.

OPOMBA: Nekaterih naprav za človeški vnos/vmesnikov, kot so na primer miška, tipkovnica, sledilna ploščica in bralnik prstnih odtisov, program Device Access Manager ne nadzira. Za več informacij, glejte Neupravljani razredi naprav na strani 46.

Skrbniki sistema Windows® uporabljajo HP Device Access Manager za nadzor dostopa do naprav v sistemu in za zaščito pred nepooblaščenim dostopom:

- Vsakemu uporabniku so dodeljeni profili naprav, s katerimi so določene naprave, ki jim je dovoljen ali zavrnjen dostop.
- Ravno pravočasno preverjanje pristnosti (JITA) omogoča, da vnaprej določeni uporabniki preverijo svojo pristnost, da jim je omogočen dostop do naprav, do katerih je dostop sicer zavrnjen.
- Skrbnike in zaupanja vredne uporabnike je mogoče izključiti iz omejitev dostopa do naprav, ki jih vsiljuje Device Access Manager, tako, da se dodajo v skupino skrbnikov naprav. Članstvo v tej skupini se upravlja prek naprednih nastavitev.
- Dostop do naprav je mogoče podeliti ali zavrniti na osnovi članstva v skupini ali za posamezne uporabnike.
- Za razrede naprav, kot so pogoni CD-ROM ali DVD, je dostop za branje in dostop za pisanje mogoče dovoliti ali zavrniti ločeno.

HP Device Access Manager se ob zaključku čarovnika za namestitev HP Client Security samodejno konfigurira z naslednjimi nastavitvami:

- Izmenljivi mediji z ravno pravočasnim preverjanjem pristnosti (JITA) so omogočeni za skrbnike in uporabnike.
- Pravilnik naprav dovoljuje poln dostop do drugih naprav.

Odpiranje programa Device Access Manager

1. Na začetnem zaslonu kliknite oziroma tapnite program **HP Client Security** (Windows 8).

   – ali –

   Na namizju Windows dvokliknite ali dvotapnite ikono **HP Client Security** v območju za obvestila, ki ga najdete na skrajni desni strani opravilne vrstice.

2. V možnosti **Device** (Naprava) kliknite oziroma tapnite **Device Permissions** (Dovoljenja za naprave).

   - Standardni uporabniki si lahko ogledajo svoj trenutni dostop do naprav (gl. Uporabniški pogled na strani 44).
   - Skrbniki si lahko ogledajo in spremenijo dostop do naprav, ki je trenutno konfiguriran za računalnik, tako, da kliknejo ali tapnejo **Change** (Spremeni), nato pa vnesejo skrbniško geslo (glejte Sistemski pogled na strani 44).

Uporabniški pogled

Ko izberete **Device Permission** (Dovoljenja za naprave), je prikazan uporabniški pogled. Glede na pravilnik si lahko standardni uporabniki in skrbniki ogledajo lastni dostop za razrede naprav ali za posamezne naprave v računalniku.

- **Current user** (Trenutni uporabnik) – Prikazano je ime uporabnika, ki je trenutno prijavljen.
- **Device Class** (Razred naprav) – Prikazane so vrste naprav.
- **Access** (Dostop) – Prikazan je trenutno konfigurirani dostop do vrst naprav ali posameznih naprav.
- **Duration** (Trajanje) – Prikazana je časovna omejitev vašega dostopa do pogonov CD/DVD-ROM ali izmenljivih diskov.
- **Settings** (Nastavitve) – Skrbniki lahko spremenijo, za katere pogone dostop nadzira Device Access Manager.

Sistemski pogled

V sistemskem pogledu skrbniki lahko dovolijo ali zavrnejo dostop do naprav v računalniku za skupino uporabnikov ali za skupino skrbnikov.

▲ Skrbniki lahko dostopajo do sistemskega pogleda, tako da kliknejo oziroma tapnejo **Change** (Spremeni), vnesejo skrbniško geslo in izberejo izmed naslednjih možnosti:

- **Device Access Manager** – Če želite vklopiti ali izklopiti HP Device Access Manager z ravno pravočasnim preverjanjem, kliknite oziroma tapnite **On** (Vklop) ali **Off** (Izklop).
- **Users and groups on this PC** (Uporabniki in skupine v tem računalniku) – Prikaže skupino uporabnikov ali skupino skrbnikov, ki jim je dovoljen ali zavrnjen dostop do izbranih razredov naprav.
- **Device Class** (Razred naprav) – Prikaže razrede naprav in naprave, ki so nameščene v sistemu ali ki so bile morda prej nameščene v sistemu. Če želite razširiti seznam, kliknite ikono **+**. Prikazane so vse naprave, ki so povezane z računalnikom, skupini skrbnikov in uporabnikov pa

sta razširjeni in prikazujeta člane. Če želite osvežiti seznam naprav, kliknite ikono z okroglo puščico (osvežitev).

- Zaščita se navadno uveljavi za razred naprav. Če dostop nastavite na **Allow** (Dovoli), bosta izbrani uporabnik ali skupina lahko dostopala do vsake naprave v tem razredu naprav.
- Zaščito lahko uveljavite tudi za posamezne naprave.
- Konfigurirajte ravno pravočasno preverjanje pristnosti (JITA), ki omogoča izbranim uporabnikom dostop do pogonov DVD/CD-ROM ali izmenljivih pogonov, ko preverijo svojo pristnost. Za več informacij, glejte Konfiguracija JITA na strani 45.
- Dovolite ali zavrnite dostop do drugih razredov naprav, na primer izmenljivih medijev (kot so bliskovni pogoni USB), serijskih in paralelnih vrat, naprav Bluetooth®, modemov, naprav PCMCIA/ExpressCard, naprav 1394, bralnika prstnih odtisov in bralnika pametnih kartic. Če sta bralnik prstnih odtisov in bralnik pametnih kartic zavrnjena, ju je mogoče uporabiti kot poverilnici za preverjanje pristnosti, ni pa ju mogoče uporabiti na ravni pravilnika seje.

OPOMBA: Če kot poverilnice za preverjanje pristnosti uporabljate naprave Bluetooth, dostop do naprav Bluetooth v pravilniku programa Device Access Manager ne sme biti omejen.

- Ko izberete nastavitev na ravni skupine ali razreda naprav in vas program vpraša, ali želite nastavitev uporabiti tudi za podrejene predmete:

  Yes (Da) – Nastavitev se bo razširila.

  No (Ne) – Nastavitev se ne bo razširila.
- Nekatere razrede naprav, na primer DVD in CD-ROM, je mogoče še bolj nadzirati, tako da dostop dovolite ali zavrnete ločeno za operaciji branja in pisanja.

OPOMBA: Skupine skrbnikov ne morete dodati na seznam uporabnikov.

- **Access** (Dostop) – Kliknite oziroma tapnite puščico navzdol, nato izberite eno od naslednjih vrst dostopa, da dovolite oziroma zavrnete dostop:
  - **Allow – Full Access** (Omogoči – Poln dostop)
  - **Allow – Read Only** (Omogoči – Samo branje)
  - **Allow – JITA Required** (Omogoči – potreben je način JITA) – Za več informacij glejte Konfiguracija JITA na strani 45.

    Če je izbrana ta vrsta dostopa, v možnosti **Duration** (Trajanje) kliknite oziroma tapnite puščico navzdol, da določite časovno omejitev.
  - **Deny** (Zavrni)
- **Duration** (Trajanje) – Kliknite oziroma tapnite puščico navzdol, da izberete časovno omejitev za dostop do pogonov CD/DVD-ROM ali izmenljivih pogonov (glejte Konfiguracija JITA na strani 45).

Konfiguracija JITA

Konfiguracija JITA omogoča skrbniku, da pregleduje in spreminja sezname uporabnikov in skupin, ki jim je dovoljeno dostopati do naprav z ravno pravočasnim preverjanjem pristnosti (JITA).

Uporabniki, za katere je omogočeno JITA, bodo imeli dostop do nekaterih naprav, za katere so bili omejeni pravilniki, ustvarjeni v pogledu **Device Class Configuration** (Konfiguracija razreda naprav).

Čas preverjanja JITA je mogoče nastaviti na določeno število minut ali Neomejeno. Neomejeni uporabniki bodo imeli dostop do naprave od trenutka, ko preverijo svojo pristnost, pa dokler se ne odjavijo iz sistema.

Če je uporabniku dodeljen omejen čas JITA, bo eno minuto pred potekom časa JITA vprašan, ali želi podaljšati dostop. Takoj ko se uporabnik odjavi iz sistema ali se prijavi drug uporabnik, čas JITA poteče. Ko se bo uporabnik naslednjič prijavil in poskusil dostopati do naprave, za katero je omogočeno JITA, bo prikazan poziv, naj vnese poverilnice.

JITA je na voljo za naslednje razrede naprav:

- Pogoni DVD/CD-ROM
- Izmenljivi pogoni

Ustvarjanje pravilnika JITA za uporabnika ali skupino

Skrbniki lahko dovolijo uporabnikom ali skupinam dostop do naprav z ravno pravočasnim preverjanjem pristnosti (JITA).

1. Zaženite **Device Access Manager**, nato kliknite oziroma tapnite **Change** (Spremeni).
2. Izberite uporabnika ali skupino, nato v možnosti **Access** (Dostop) za **Removable Disk drives** (Izmenljivi pogoni) ali **DVD/CD-ROM drives** (Pogoni DVD/CD-ROM) kliknite oziroma tapnite puščico navzdol, nato izberite **Allow – JITA Required** (Omogoči – potreben je način JITA).
3. V možnosti **Duration** (Trajanje) kliknite oziroma tapnite puščico navzdol, da izberete časovno omejitev za dostop JITA.

Uporabnik se mora odjaviti in znova prijaviti, da se nova nastavitev JITA uveljavi.

Onemogočanje pravilnika JITA za uporabnika ali skupino

Skrbniki lahko onemogočijo uporabnikom ali skupinam dostop do naprav z ravno pravočasnim preverjanjem pristnosti (JITA).

1. Zaženite **Device Access Manager**, nato kliknite oziroma tapnite **Change** (Spremeni).
2. Izberite uporabnika ali skupino, nato v možnosti **Access** (Dostop) za **Removable Disk drives** (Izmenljivi pogoni) ali **DVD/CD-ROM drives** (Pogoni DVD/CD-ROM) kliknite oziroma tapnite puščico navzdol, nato izberite **Deny** (Zavrni).

Ko se bo uporabnik prijavil in poskušal dostopati do naprave, bo dostop zavrnjen.

Nastavitve

Pogled **Settings** (Nastavitve) omogoča skrbnikom pogled in spremembo pogonov, za katere dostop nadzira Device Access Manager.

OPOMBA: Device Access Manager mora biti omogočen, ko konfigurirate seznam črk pogonov (glejte Sistemski pogled na strani 44).

Neupravljani razredi naprav

HP Device Access Manager ne upravlja naslednjih razredov naprav:

- Vhodne/izhodne naprave
  - CD-ROM
  - Diskovni pogon

- Krmilnik disketnega pogona (FDC)
- Krmilnik trdega diska (HDC)
- Razred naprav za človeški vnos (HID)
- Naprave za človeški vnos z infrardečim sprejemnikom
- miška
- Serijska kartica z več vrati
- tipkovnica
- Tiskalniki plug-and-play (PnP)
- Tiskalnik
- Nadgradnja tiskalnika

- Stikalo za
  - Podpora za zahtevnejše upravljanje porabe (APM)
  - Akumulator
- Razno
  - Računalnik
  - Dekodirnik
  - Zaslon
  - Enotni gonilnik za zaslone Intel®
  - Legacard
  - Gonilnik za medij
  - Menjalnik medijev
  - Pomnilniška tehnologija
  - Monitor
  - Več funkcij
  - Net odjemalec
  - Net storitev
  - Net trans
  - Procesor
  - Kartica SCSI
  - Varnostni pospeševalnik
  - Varnostne naprave
  - Sistem
  - Neznano
  - Glasnost
  - Posnetek nosilca

8 HP Trust Circles

HP Trust Circles je program za varnost datotek in dokumentov, ki šifriranje map z datotekami združuje s priročno zmogljivostjo skupne rabe dokumentov s krogom oseb, ki jim zaupate. Program šifrira datoteke, ki so spravljene v mapah, ki jih navede uporabnik, in jih zaščiti znotraj kroga zaupanja. Ko so datoteke zaščitene, jih lahko uporabljajo in imajo v skupni rabi samo člani kroga zaupanja. Če zaščiteno datoteko prejme ne-član, datoteka ostane šifrirana, ne-član pa nima dostopa do vsebine.

Odpiranje programa Trust Circles

1. Na začetnem zaslonu kliknite oziroma tapnite program **HP Client Security**.

   – ali –

   Na namizju Windows dvokliknite ikono **HP Client Security** v območju za obvestila, ki ga najdete na skrajni desni strani opravilne vrstice.

2. V možnosti **Data** (Podatki) kliknite oziroma tapnite **Trust Circles**.

Začetek dela

E-poštna povabila lahko prejmete in nanje odgovarjate na dva načina:

- **S programom Microsoft® Outlook** – Če uporabljate program Trust Circles s programom Microsoft Outlook, se obdelava povabil v kroge zaupanja Trust Circle in odgovorov drugih uporabnikov programa Trust Circle izvede samodejno.
- **S storitvami Gmail, Yahoo, Outlook.com ali drugimi e-poštnimi storitvami (SMTP)** – Ko vnesete svoje ime, e-naslov in geslo, program Trust Circle prek vaše e-poštne storitve pošlje e-poštna povabila članom, ki jih želite vključiti v svoj krog zaupanja.

Če želite nastaviti osnovni profil:

1. Vnesite svoje ime in e-naslov, nato kliknite oziroma tapnite **Next** (Naprej).

   Ime bo vidno vsem članom, ki so povabljeni, da se pridružijo vašemu krogu zaupanja. E-naslov bo uporabljen za pošiljanje, prejemanje in odgovore na povabila.

2. Vnesite geslo za e-poštni račun, nato kliknite ali tapnite **Next** (Naprej).

   Poslano bo testno e-sporočilo, ki preverja, da so nastavitve e-pošte pravilne.

   OPOMBA: Računalnik mora biti povezan v omrežje.

3. V polju **Trust Circle Name** (Ime kroga zaupanja) vnesite ime za krog zaupanja, nato kliknite oziroma tapnite **Next** (Naprej).

4. Dodajte člane in mape, nato kliknite oziroma tapnite **Next** (Naprej). Krog zaupanja se ustvari z vsemi mapami, ki so bile izbrane, in pošlje e-poštna povabila vsem članom, ki so bili izbrani. Če iz kakršnega koli razloga povabila ne morete poslati, bo prikazano obvestilo. Člane lahko iz programa Trust Circle kadar koli znova povabite, tako da kliknete **Your Trust Circles** (Vaši krogi zaupanja), nato pa dvokliknete oziroma dvotapnete krog zaupanja. Za več informacij, glejte Trust Circles na strani 49.

Trust Circles

Krog zaupanja lahko ustvarite med prvotno nastavitvijo, potem ko vnesete svoj e-naslov, ali v pogledu Trust Circle (Krog zaupanja):

▲ V pogledu Trust Circle (Krog zaupanja) kliknite oziroma tapnite **Create Trust Circle** (Ustvari krog zaupanja), nato vnesite ime za krog zaupanja.

- Če želite dodati člane v krog zaupanja, kliknite oziroma tapnite ikono **M+** poleg možnosti **Members** (Člani), nato sledite navodilom na zaslonu.
- Če želite dodati mape v krog zaupanja, kliknite oziroma tapnite ikono **+** poleg možnosti **Folders** (Mape), nato sledite navodilom na zaslonu.

Dodajanje map v krog zaupanja

Dodajanje map v nov krog zaupanja:

- Medtem ko ustvarjate krog zaupanja, mu lahko dodajate mape, tako da kliknete oziroma tapnete ikono **+** poleg možnosti **Folders** (Mape), nato pa sledite navodilom na zaslonu.

  – ali –

- V Raziskovalcu z desno tipko miške kliknite oziroma tapnite in pridržite mapo, ki trenutno ni del kroga zaupanja, izberite **Trust Circle** (Krog zaupanja), nato izberite **Create Trust Circle from Folder** (Ustvari krog zaupanja iz mape).

NASVET: Izberete lahko eno ali več map.

Dodajanje map obstoječemu krogu zaupanja:

- V pogledu Trust Circle (Krog zaupanja) kliknite **Your Trust Circles** (Vaši krogi zaupanja), dvokliknite oziroma dvotapnite obstoječi krog zaupanja, da prikažete trenutne mape, kliknite oziroma tapnite ikono **+** poleg možnosti **Folders** (Mape), nato sledite navodilom na zaslonu.

  – ali –

- V Raziskovalcu z desno tipko miške kliknite oziroma tapnite in pridržite mapo, ki trenutno ni del kroga zaupanja, izberite **Trust Circle** (Krog zaupanja), nato izberite **Add to Existing Trust Circle from Folder** (Dodaj obstoječemu krogu zaupanja iz mape).

NASVET: Izberete lahko eno ali več map.

Ko je mapa enkrat dodana v krog zaupanja, program Trust Circles samodejno šifrira mapo in njeno vsebino. Ko so vse datoteke šifrirane, se pokaže obvestilo. Poleg tega je na vseh ikonah šifriranih map ter na ikonah datotek znotraj teh map prikazan zelen simbol ključavnice, kar pomeni, da so popolnoma zaščitene.

Dodajanje članov v krog zaupanja

Če želite dodati člane v krog zaupanja, so potrebni trije koraki:

1. **Povabilo** – Najprej lastnik kroga zaupanja povabi člane. E-pošto s povabilom lahko pošlje več uporabnikom ali seznamom prejemnikov/skupinam.
2. **Sprejem** – Povabljenec prejme povabilo in se odloči, ali ga bo sprejel ali zavrnil. Če povabljenec sprejme povabilo, je vabitelju poslan e-poštni odgovor. Če je bilo povabilo poslano skupini, ga prejme vsak član posebej in se lahko odloči, ali ga bo sprejel ali zavrnil.
3. **Vpis** – Vabitelj ima končno priložnost, da se odloči, ali bo člana dodal v krog zaupanja. Če se vabitelj odloči, da bo člana vpisal, je povabljencu poslana e-pošta, ki potrjuje odziv. Vabitelj in povabljenec lahko neobvezno tudi preverita varnost postopka povabila. Za povabljenca je prikazana koda za preverjanje, ki jo mora vabitelju prebrati po telefonu. Ko je koda preverjena, lahko vabitelj pošlje končno e-pošto za vpis.

Dodajanje članov v nov krog zaupanja:

▲ Medtem ko ustvarjate krog zaupanja, mu lahko dodajate člane, tako da kliknete oziroma tapnete ikono **M+** poleg možnosti **Members** (Člani), nato pa sledite navodilom na zaslonu.

- Če uporabljate Outlook, izberite stike iz adresarja v Outlooku in kliknite **OK** (V redu).
- Če uporabljate drugo e-poštno storitev, lahko nove e-naslove v krog zaupanja dodate ročno ali pa jih pridobite iz e-naslova, ki je registriran v krogu zaupanja.

Dodajanje članov obstoječemu krogu zaupanja:

▲ V pogledu Trust Circle (Krog zaupanja) kliknite **Your Trust Circles** (Vaši krogi zaupanja), dvokliknite oziroma dvotapnite obstoječi krog zaupanja, da prikažete trenutne člane, kliknite oziroma tapnite ikono **M+** poleg možnosti **Members** (Člani), nato sledite navodilom na zaslonu.

- Če uporabljate Outlook, izberite stike iz adresarja v Outlooku in kliknite **OK** (V redu).
- Če uporabljate drugo e-poštno storitev, lahko nove e-naslove v krog zaupanja dodate ročno ali pa jih pridobite iz e-naslova, ki je registriran v krogu zaupanja.

Dodajanje datotek v krog zaupanja

Datoteke lahko dodate v krog zaupanja na enega od teh načinov:

- Kopirajte ali premaknite datoteko v mapo, ki je že v krogu zaupanja.

  – ali –

- V Raziskovalcu z desno tipko miške kliknite oziroma tapnite in pridržite datoteko, ki trenutno ni šifrirana, izberite **Trust Circle** (Krog zaupanja), nato izberite **Encrypt** (Šifriraj). Pozvani boste, da izberite krog zaupanja, ki naj mu bo datoteka dodana.

NASVET: Izberete lahko eno ali več datotek.

Šifrirane mape

Vsak član kroga zaupanja si lahko ogleda in ureja datoteke, ki pripadajo temu krogu zaupanja.

OPOMBA: Trust Circle Manager/Reader ne sinhronizira datotek med člani.

Datoteke je treba dati v skupno rabo na obstoječe načine, na primer po e-pošti, prek FTP-ja ali ponudnikov shranjevanja v oblaku. Datoteke, ki so kopirane, premaknjene ali ustvarjene znotraj kroga zaupanja, so nemudoma zaščitene.

Odstranjevanje map iz kroga zaupanja

Če odstranite mapo iz kroga zaupanja, se skupaj z vso vsebino dešifrira in zaščita je odstranjena.

- V pogledu Trust Circle (Krog zaupanja) kliknite oziroma tapnite **Your Trust Circles** (Vaši krogi zaupanja), dvokliknite oziroma dvotapnite obstoječi krog zaupanja, da prikažete trenutne mape, nato kliknite oziroma tapnite ikono **koša** poleg te mape.

  – ali –

- V Raziskovalcu z desno tipko miške kliknite oziroma tapnite in pridržite mapo, ki je trenutno del kroga zaupanja, izberite **Trust Circle** (Krog zaupanja), nato izberite **Remove from Trust Circle** (Odstrani iz kroga zaupanja).

NASVET: Izberete lahko eno ali več map.

Odstranjevanje datoteke iz kroga zaupanja

Če želite datoteko odstraniti iz kroga zaupanja, v Raziskovalcu z desno tipko kliknite oziroma tapnite in pridržite datoteko, ki je trenutno šifrirana, izberite **Trust Circle** (Krog zaupanja), izberite **Decrypt File** (Dešifriraj datoteko).

Odstranjevanje članov iz kroga zaupanja

Člana, ki je bil popolnoma vpisan, ni mogoče odstraniti iz kroga zaupanja. Druga možnost je, da ustvarite nov krog zaupanja z vsemi drugi člani, premaknete vse datoteke in mape v novi krog zaupanja, nato pa izbrišete stari krog zaupanja. Tako zagotovite, da nove datoteke, ki jih član prejme, ne bodo dostopne, vse, kar je bilo prej dano v skupno rabo, pa bo ostalo dostopno članu starega kroga zaupanja.

Če član ni popolnoma vpisan (če je bil ali povabljen, da se pridruži krogu zaupanja ali pa ni sprejel povabila, da se pridruži krogu zaupanja), ga lahko odstranite iz kroga zaupanja na enega od teh načinov:

- V pogledu Trust Circle (Krog zaupanja) kliknite oziroma tapnite **Your Trust Circles** (Vaši krogi zaupanja), nato dvokliknite oziroma dvotapnite krog zaupanja, da se pokaže seznam trenutnih članov. Kliknite oziroma tapnite ikono **koša** poleg imena člana, ki ga želite odstraniti.
- V pogledu Trust Circle (Krog zaupanja) kliknite oziroma tapnite **Members** (Člani), nato dvokliknite oziroma dvotapnite krog zaupanja, da se pokaže seznam krogov zaupanja, katerih član je. Kliknite oziroma tapnite ikono **koša** poleg kroga zaupanja, da odstranite člana iz tega kroga zaupanja.

Brisanje kroga zaupanja

Če želite izbrisati krog zaupanja, potrebujete lastništvo.

- V pogledu Trust Circle (Krog zaupanja) kliknite oziroma tapnite **Your Trust Circles** (Vaši krogi zaupanja), kliknite oziroma tapnite ikono **koša** poleg kroga zaupanja, ki naj bo izbrisan.

  S tem se krog zaupanja odstrani s strani in pošlje e-pošto vsem članom kroga zaupanja ter jih obvesti, da je bil krog zaupanja izbrisan. Vse datoteke in mape, ki so bile del tega kroga zaupanja, se dešifrirajo.

Prednostne nastavitve

V pogledu Trust Circle (Krog zaupanja) kliknite oziroma tapnite **Preferences** (Prednostne nastavitve). Prikazane so tri kartice.

- **Email Settings** (Nastavitve e-pošte)

Možnost	Opis
Username (Uporabniško ime)	Prikazano je uporabniško ime, ki je trenutno v uporabi. Če ga želite spremeniti, v besedilno polje vnesite novo uporabniško ime. Spremembe se samodejno shranijo.
Email Address (E-naslov)	Prikazan je trenutno uporabljeni e-naslov. Če ga želite spremeniti, kliknite oziroma tapnite **Change Email Settings** (Spremeni nastavitve e-pošte), nato sledite navodilom na zaslonu.
New Member Confirmation (Potrditev novega člana)	Izberite med naslednjimi možnostmi: ◦ **Confirm Automatically** (Potrdi samodejno) – Ko od povabljencev prejmete potrditve, se v krogu zaupanja potrdijo brez ročnih posegov in dobijo potrditveno e-pošto. ◦ **Confirm Manually** (Potrdi ročno) – Ko od povabljencev prejmete potrditve, je potreben ročni vnos, da nove člane vpišete v krog zaupanja, nato pa povabljenci dobijo potrditveno e-pošto. ◦ **Require Verification** (Zahtevaj preverjanje) – Ko od povabljencev prejmete potrditve, je potrebna koda za preverjanje, preden so popolnoma vpisani. Lastnik kroga zaupanja mora stopiti v stik s povabljenci in od njih pridobiti kodo za preverjanje. Ko je vnesena pravilna koda, se pošlje potrditvena e-pošta.
Periodic Authentication (Redno preverjanje pristnosti)	Z rednim preverjanjem pristnosti mora uporabnik vnesti geslo za Windows, potem ko poteče določen čas (ki se šteje v minutah), ter pri izvajanju občutljivih operacij. Nastavitev omogoča uporabnikom, da preverjanje pristnosti vklopijo ali izklopijo.
Authentication Timeout (Časovna omejitev preverjanja pristnosti)	Določite časovno omejitev (ki se šteje v minutah), preden program zahteva preverjanje pristnosti.
Don't show confirmation message (Ne kaži potrditvenega sporočila)	Potrdite to polje, da onemogočite prikaz potrditvenih sporočil, oziroma ga počistite, če želite videti potrditvena sporočila.
I'd like to help improve the HP Trust Circle through anonymous usage tracking (Želim izboljšati HP Trust Circle z anonimnim sledenjem uporabe)	Potrdite to polje, če želite sodelovati v tem programu, oziroma ga počistite, če ne želite sodelovati.

- **Backup/Restore** (Varnostna kopija/obnovitev)

Možnost	Opis
Varnostno kopiranje	Kopira podatke programa Trust Circle Manager/Reader (nastavitve in kroge zaupanja) v datoteko varnostne kopije. Če pride do zrušitve ali odpovedi sistema, iz te datoteke lahko obnovite novo namestitev krogov zaupanja na stanje, shranjeno v datoteki. **OPOMBA:** Shranijo se samo podatki programa Trust Circle (krogi zaupanja, nastavitve in člani). Same datoteke v mapah v krogu zaupanja niso varnostno kopirane. Te datoteke morate ločeno varnostno kopirati. Če želite varnostno kopirati nastavitve in uporabniške podatke za Trust Circle: **1.** Kliknite oziroma tapnite **Backup** (Varnostno kopiranje). **2.** Izberite ime datoteke in imenik za datoteko varnostne kopije, nato kliknite oziroma tapnite **Save** (Shrani). **3.** Vnesite geslo, ga potrdite, nato kliknite oziroma tapnite **OK** (V redu). Za obnovitev te datoteke bo potrebno to geslo.
Obnovitev	Obnovi nastavitve in kroge zaupanja iz datoteke varnostne kopije, navadno po zrušitvi sistema ali selitvi v drug računalnik. Če želite obnoviti nastavitve in uporabniške podatke programa Trust Circle Manager: **1.** Kliknite oziroma tapnite **Restore** (Obnovi). **2.** Poiščite imenik in ime datoteke varnostne kopije, nato kliknite oziroma tapnite **Open** (Odpri). **3.** Vnesite geslo, ki je bilo nastavljeno med varnostnim kopiranjem.

- **About** (Vizitka) – Prikazana je različica programske opreme Trust Circle Manager/Reader. Prikazane so povezave, da lahko nadgradite Trust Circle Manager na različico Pro, in da lahko prikažete HP-jevo izjavo o zasebnosti.

9 Iskanje v primeru kraje (samo nekateri modeli)

Computrace (nakup posebej) omogoča oddaljeni nadzor in upravljanje ter sledenje računalniku.

Ko je storitev Computrace aktivirana, jo lahko konfigurirate iz središča za stranke Absolute Software Customer Center. Iz središča za stranke lahko skrbnik konfigurira Computrace za nadzor ali upravljanje računalnika. Če je sistem založen ali ukraden, lahko središče za stranke pomaga lokalnim organom pregona pri iskanju in povrnitvi računalnika. Če je storitev konfigurirana, se delovanje storitve Computrace lahko nadaljuje, tudi če je trdi disk izbrisan ali zamenjan.

Aktiviranje storitve Computrace:

1. Vzpostavite povezavo z internetom.
2. Odprite HP Client Security. Za več informacij, glejte Odpiranje programa HP Client Security na strani 9.
3. Kliknite **Theft Recovery**.
4. Če želite zagnati čarovnik za aktiviranje storitve Computrace, kliknite **Get Started** (Začetek dela).
5. Vnesite svoje podatke za stik in podatke za plačilo s kreditno kartico ali pa vnesite vnaprej kupljen ključ izdelka.

Čarovnik za aktiviranje varno izvede transakcijo in vam odpre uporabniški račun v spletnem mestu Absolute Software Customer Center. Ko se postopek zaključi, prejmete potrditveno elektronsko sporočilo, ki vsebuje podatke vašega računa v središču za stranke.

Če ste že izvedli postopek čarovnika za aktiviranje storitve Computrace in že imate uporabniški račun v središču za stranke, lahko dokupite dodatne licence prek svojega predstavnika HP.

Prijava v središče za stranke:

1. Obiščite spletno mesto https://cc.absolute.com/.
2. V polji **Login ID** in **Password** vnesite poverilnice, ki ste jih prejeli v potrditvenem elektronskem sporočilu, in nato kliknite **Log in**.

Središče za stranke vam omogoča naslednje:

- Nadzorujete lahko svoje računalnike.
- Svoje oddaljene podatke lahko zaščitite.
- Prijavite lahko krajo računalnika, zaščitenega s storitvijo Computrace.

▲ Za več informacij o storitvi Computrace kliknite **Learn More** (Več informacij).

10 Izjeme za lokalizirana gesla

Na ravni preverjanja pristnosti ob vklopu in ravni HP Drive Encryption obstaja omejena podpora za lokalizacijo gesel. Za več informacij, glejte Urejevalniki vnosne metode, ki jih Windows ne podpira na ravni preverjanja pristnosti ob vklopu ali na ravni Drive Encryption na strani 55.

Kaj storiti, ko je geslo zavrnjeno

Geslo je lahko zavrnjeno iz teh razlogov:

- Uporabnik uporablja urejevalnik vnosne metode, ki ni podprt. To je pogosta težava pri dvobajtnih jezikih (korejščina, japonščina, kitajščina). Če želite to težavo razrešiti:
  1. Na **nadzorni plošči** dodajte podprto razporeditev tipkovnice (za vnosni jezik kitajščina npr. dodajte ameriško tipkovnico).
  2. Nastavite podprto tipkovnico kot privzeto vnosno metodo.
  3. Zaženite HP Client Security, nato vnesite geslo za Windows.
- Uporabnik uporablja znak, ki ni podprt. Če želite to težavo razrešiti:
  1. Spremenite geslo za Windows, tako da uporablja samo podprte znake. Za več informacij o nepodprtih znakih glejte Obravnava posebnih tipk na strani 56.
  2. Zaženite HP Client Security, nato vnesite geslo za Windows.

Urejevalniki vnosne metode, ki jih Windows ne podpira na ravni preverjanja pristnosti ob vklopu ali na ravni Drive Encryption

V sistemu Windows lahko uporabnik izbere urejevalnik vnosne metode za vnos kompleksnih znakov in simbolov, na primer japonskih ali kitajskih pismenk, z uporabo standardne zahodne tipkovnice.

Urejevalniki vnosne metode niso podprti na ravni preverjanja pristnosti ob vklopu in na ravni Drive Encryption. Gesla za Windows ni mogoče vnesti z urejevalnikom vnosne metode na zaslonu za prijavo pri preverjanju pristnosti ob vklopu ali pri HP Drive Encryption. Če to storite, se lahko zaklenete iz sistema. V nekaterih primerih Microsoft® Windows ne prikaže urejevalnika vnosne metode, ko uporabnik vnese geslo.

Rešitev je, da preklopite na eno od naslednjih podprtih razporeditev tipkovnice, ki prevaja v razporeditev tipkovnice 00000411:

- Microsoft IME za japonščino
- Japonska razporeditev tipkovnice
- Office 2007 IME za japonščino – Če Microsoft ali drug proizvajalec uporablja izraz IME ali urejevalnik vnosne metode, vnosna metoda v resnici morda ni IME. To lahko vodi do zmede, toda program bere šestnajstiški zapis kode. Če torej IME prevaja v podprto razporeditev tipkovnice, lahko HP Client Security podpira to konfiguracijo.

⚠ **OPOZORILO!** Ko je v uporabi HP Client Security, bodo zavrnjena gesla, vnesena z urejevalnikom vnosne metode za Windows.

Spremembe gesla z razporeditvijo tipkovnice, ki je prav tako podprta

Če ste geslo prvotno nastavili z eno razporeditvijo tipkovnice, npr. ameriška angleščina (409), nato pa uporabnik geslo spremeni z drugo razporeditvijo tipkovnice, ki je prav tako podprta, npr. latinsko ameriška (080A), bo sprememba gesla delovala v programu HP Drive Encryption, vendar ne bo uspela v BIOS-u, če uporabnik vključi znake, ki obstajajo v njegovi razporeditvi tipkovnice, ne pa v vaši (na primer ē).

OPOMBA: Skrbniki to težavo lahko rešijo na strani Users (Uporabniki) programa HP Client Security (odprete jo s pomočjo ikone **zobnika** na začetni strani), tako da odstranijo uporabnika iz programa HP Client Security, izberejo želeno razporeditev tipkovnice v operacijskem sistemu, nato pa znova zaženejo čarovnika za nastavitev HP Client Security za istega uporabnika. V BIOS-u se shrani želena razporeditev tipkovnice. Gesla, ki jih je mogoče vnesti s to tipkovnico, bodo v BIOS-u ustrezno nastavljena.

Še ena možna težava nastane ob uporabi različnih razporeditev tipkovnice, ki vse lahko ustvarijo isti znak. Tako mednarodna ameriška razporeditev tipkovnice (20409) kot latinsko ameriška razporeditev tipkovnice (080A) lahko ustvarita znak é, toda zanj je potrebno različno zaporedje pritiskov tipk. Če geslo prvotno nastavite z latinsko ameriško razporeditvijo tipkovnice, bo latinsko ameriška razporeditev tipkovnice nastavljena v BIOS-u, tudi če geslo naknadno spremenite z mednarodno ameriško razporeditvijo tipkovnice.

Obravnava posebnih tipk

- Kitajščina, slovaščina, kanadska francoščina in češčina

  Če uporabnik izbere eno od predhodnih razporeditev tipkovnice in nato vnese geslo (npr. abcdef), je treba enako geslo vnesti med pritiskanjem tipke shift za male črke ter tipke shift ter tipke Caps Lock za velike črke pri preverjanju pristnosti pri vklopu in v orodju HP Drive Encryption. Gesla iz številk je treba vnesti s številsko tipkovnico.

- korejščina

  Če uporabnik izbere podprto korejsko razporeditev tipkovnice in nato vnese geslo, je treba enako geslo vnesti med pritiskanjem desne tipke alt za male črke ter desne tipke alt in tipke Caps Lock za velike črke pri preverjanju pristnosti pri vklopu in v orodju HP Drive Encryption.

- V spodnji tabeli so navedeni nepodprti znaki:

Language (Jezik)	Windows	BIOS	Drive Encryption
arabščina	Tipke ﻯ ,ﻱ in ﻯ ustvarijo dva znaka.	Tipke ﻯ ,ﻱ in ﻯ ustvarijo en znak.	Tipke ﻯ ,ﻱ in ﻯ ustvarijo en znak.
kanadska francoščina	ç, è, à in é so skupaj s tipko Caps Lock Ç, È, À in É v sistemu Windows.	ç, è, à in é so skupaj s tipko Caps Lock ç, è, à in é pri preverjanju pristnosti pri vklopu.	ç, è, à in é so skupaj s tipko Caps Lock ç, è, à in é v programu HP Drive Encryption.

Language (Jezik)	Windows	BIOS	Drive Encryption
španščina	40a ni podprta. Vseeno pa deluje, ker jo program pretvori v c0a. Toda zaradi neznatnih razlik med razporeditvama tipkovnice priporočamo, da špansko govoreči uporabniki spremenijo svojo razporeditev tipkovnice v sistemu Windows v 1040a (španska različica) ali 080a (latinsko ameriška).	/	/
mednarodna ameriška	◦ Tipke ¡, ¤, ‘, ’, ¥ in × v zgornji vrstici so zavrnjene. ◦ Tipke å, ® in Þ v drugi vrstici so zavrnjene. ◦ Tipke á, ð in ø v tretji vrstici so zavrnjene. ◦ Tipka æ v spodnji vrstici je zavrnjena.	/	/
češčina	◦ Tipka ğ je zavrnjena. ◦ Tipka į je zavrnjena. ◦ Tipka ų je zavrnjena. ◦ Tipke ė, ı in ż so zavrnjene. ◦ Tipke ģ, ķ, ļ, ņ in ţ so zavrnjene.	/	/
slovaščina	Tipka ż je zavrnjena.	◦ Tipke š, ś in ş so zavrnjene, ko jih pritisnete, sprejete pa so, če jih vnesete s programsko tipkovnico. ◦ Mrtva tipka ţ ustvari dva znaka.	/
madžarščina	Tipka ż je zavrnjena.	Tipka ţ ustvari dva znaka.	/
slovenščina	Tipka żŻ je zavrnjena v sistemu Windows, tipka alt pa ustvari mrtvo tipko v BIOS-u.	Tipke ú, Ú, ů, Ů, ş, Ş, ś, Ś, š in Š so zavrnjene v BIOS-u.	/
japonščina	Microsoft Office 2007 IME je boljša izbira, če je na voljo. Kljub imenu IME gre dejansko za razporeditev tipkovnice 411, ki je podprta.	/	/

Pojmovnik

aktiviranje
Opravilo, ki ga je treba dokončati, preden postanejo dostopne funkcije programa Drive Encryption. Skrbniki lahko aktivirajo Drive Encryption z nastavitvenim čarovnikom HP Client Security ali s programom HP Client Security. Postopek aktiviranja tvorijo aktivacija programske opreme, šifriranje pogona ter ustvarjanje začetnega ključa šifriranja za varnostno kopiranje na izmenljivi napravi za shranjevanje.

arhiv za obnovitev v sili
Je zaščiteno pomnilniško območje, ki omogoča ponovno šifriranje osnovnih ključev uporabnika iz enega ključa lastnika platforme v drugega.

Bluetooth
Je tehnologija, ki uporablja radijsko oddajanje, s katerim omogoča računalnikom, tiskalnikom, miškam, mobilnim telefonom in drugim napravam, ki imajo omogočen Bluetooth, da brezžično komunicirajo na kratke razdalje.

brezkontaktne kartice
Plastična kartica, ki vsebuje računalniški čip, ki ga je za dodatno varnost mogoče uporabiti za preverjanje pristnosti v kombinaciji z drugimi poverilnicami.

brezstična kartica
Je plastična kartica, ki vsebuje računalniški čip, ki ga je mogoče uporabiti za preverjanje pristnosti.

dešifriranje
Je postopek, ki se v uporablja v kriptografiji za pretvorbo šifriranih podatkov v navadno besedilo.

Domača stran
Osrednje mesto, s katerega lahko dostopate do funkcij in nastavitev programa HP Client Security ter jih upravljate.

domena
Je skupina računalnikov, ki so del omrežja in imajo skupno imeniško zbirko podatkov. Domene so enolično poimenovane in vsaka ima nabor običajnih pravil in postopkov.

Drive Encryption
Zaščiti podatke tako, da šifrira trde diske, in tako tisti, ki nimajo pooblastil, ne morejo prebirati informacij.

enotna prijava
Je funkcija, ki shrani podatke za preverjanje pristnosti in vam omogoča uporabo programa HP Client Security za dostop do interneta in programov sistema Windows, ki zahtevajo preverjanje pristnosti z geslom.

funkcija DriveLock
Je varnostna funkcija, ki povezuje trdi disk z uporabnikom in ob zagonu računalnika od uporabnika zahteva pravilen vnos gesla DriveLock.

identiteta
V programu HP Client Security je to skupina poverilnic in nastavitev, ki se obravnavajo kot račun ali profil posameznega uporabnika.

infrastruktura javnih ključev (PKI)
Je standard infrastrukture javnih ključev, ki določa vmesnike za ustvarjanje, uporabo in upravljanje digitalnih potrdil in kriptografskih ključev.

Mapa Trust Circle
Mapa, ki jo ščiti krog zaupanja.

način varne prijave
Je način, ki se uporablja za prijavo v računalnik.

obnovitev
Je postopek, ki kopira podatke programa iz predhodno shranjene datoteke varnostne kopije v program.

Obnovitev HP SpareKey
Je možnost dostopa do vašega računalnika s pravilnimi odgovori na varnostno vprašanje.

omrežni račun
Uporabniški ali skrbniški račun sistema Windows na lokalnem računalniku, v delovni skupini ali v domeni.

osebna izkaznica
Je namizni pripomoček v sistemu Windows, ki omogoča vizualno identifikacijo vašega namizja z vašim uporabniškim imenom in izbrano sliko.

pametna kartica
Strojna naprava, ki jo lahko v kombinaciji s kodo PIN uporabljate za preverjanje pristnosti.

PIN
Osebna identifikacijska številka za vpisanega uporabnika, ki se uporablja za preverjanje pristnosti.

poverilnica
Je določena informacija ali strojna naprava, s katero posamezni uporabnik potrdi svojo pristnost.

povezana naprava
Je strojna naprava, je povezana z vrati v računalniku.

pravilnik za nadzor dostopa do naprave
Je seznam naprav, za katere ima uporabnik omogočen ali zavrnjen dostop.

prepisovanje praznega prostora
Zapisovanje naključnih podatkov prek izbrisanih sredstev in neuporabljenega prostora. S tem postopkom postane izbrisano sredstvo manj obstoječe, tako da je prvotno sredstvo težje obnoviti.

preverjanje pristnosti
Je postopek preverjanja, ali ste res oseba, za katero se predstavljate, z uporabo poverilnic, ki lahko vključujejo vaše geslo za Windows, prstne odtise, pametno kartico, brezstično kartico ali brezkontaktno kartico.

preverjanje pristnosti pred zagonom z modulom Drive Encryption
Je prijavni zaslon, ki je prikazan, preden se zažene sistem Windows. Uporabniki morajo vnesti svoje uporabniško ime in geslo za Windows oziroma kodo PIN pametne kartice, ali pa podrsati vpisan prst. Če je izbrana prijava v enem koraku, boste ob vnosu pravilnih podatkov na zaslonu Drive Encryption za prijavo neposredno prijavljeni v Windows, ne da bi se morali znova prijaviti na prijavnem zaslonu za Windows.

preverjanje pristnosti pri vklopu
Varnostna funkcija, ki ob vklopu računalnika zahteva določeno obliko preverjanja pristnosti, kot je pametna kartica, varnostni čip ali geslo.

prijava
Predmet znotraj programa HP Client Security, ki ga tvorita uporabniško ime in geslo (ter morda še drugi izbrani podatki), in s katerim se lahko prijavljate v spletna mesta ali v druge programe.

programski zagon
Je postopek ponovnega zagona računalnika.

programsko šifriranje
Uporaba programske opreme za šifriranje trdega diska, sektor za sektorjem. Ta postopek je počasnejši od strojnega šifriranja.

prstni odtis

Digitalni izvleček slike vašega prstnega odtisa. HP Client Security ne shrani dejanske slike vašega prstnega odtisa.

Ravno pravočasno preverjanje pristnosti
Glejte pomoč za programsko opremo HP Device Access Manager.

razred naprav
Vse naprave določene vrste, na primer pogoni.

ročno varno brisanje
Takojšnje varno brisanje sredstva ali izbranih sredstev, ki zaobide varno brisanje po urniku.

samodejno varno brisanje
Je brisanje, ki ga vnaprej načrtujete v programu File Sanitizer.

skrbnik
Glejte *Skrbnik sistema Windows*.

Skrbnik sistema Windows
Uporabnik s polnimi pravicami, da spreminja dovoljenja in upravlja druge uporabnike.

skupina
Je skupina uporabnikov z enako ravnjo dostopa ali zavrnjenega dostopa do razreda naprav ali do posamezne naprave.

sredstvo
Je podatkovna komponenta, ki jo tvorijo osebni podatki ali datoteke, zgodovinski ter s spletom povezani podatki in tako dalje, ki jih najdemo na trdem disku.

strojno šifriranje
Uporabljajo se samo-šifrirni pogoni, ki ustrezajo specifikaciji Trusted Computing Group OPAL za upravljanje samo-šifrirnih pogonov, za izvedbo takojšnjega šifriranja. Strojno šifriranje se izvede takoj in lahko traja le nekaj minut, medtem ko programsko šifriranje lahko traja več ur.

šifriranje
Je postopek, kot je uporaba algoritma, ki se uporablja v kriptografiji za pretvorbo navadnega besedila v šifrirano besedilo, kar nepooblaščenim prejemnikom preprečuje branje teh podatkov. Obstajajo različne vrste šifriranja podatkov, ki so osnova za varnost omrežja. Med najpogostejšimi vrstami sta šifrirni algoritem DES in šifriranje z javnim ključem.

Šifrirni datotečni sistem (EFS)
Je sistem, ki šifrira vse datoteke in podmape v izbrani mapi.

Trust Circle
Omejuje podatke in jih veže na določeno skupino zaupanja vrednih uporabnikov. To preprečuje, da bi podatki namerno ali nenamerno zašli v napačne roke. Podatki so zavarovani s tehnologijo CryptoMill Zero Overhead Key Management. Kriptografsko so vezani na krog zaupanja. To preprečuje, da bi bili dokumenti ali drugi občutljivi podatki dešifrirani zunaj kroga zaupanja.

Trust Circle Manager/Reader
Program Trust Circle Reader lahko sprejema samo povabila, ki jih pošljejo uporabniki programa Trust Circle Manager. Toda Trust Circle Manager dovoljuje ustvarjanje krogov zaupanja. Funkcije so med drugim: povabilo osebe v krog zaupanja po e-pošti in sprejem povabil v krog zaupanja od drugih. Ko se med enakimi vzpostavi krog zaupanja, si lahko osebe v njem varno izmenjujejo datoteke, ki jih krog zaupanja ščiti.

uporabniška
Katera koli oseba, ki je uveljavljena v možnosti Drive Encryption (Šifriranje pogonov). Uporabniki, ki niso skrbniki, imajo v možnosti Drive Encryption (Šifriranje pogonov) omejene pravice. Lahko se samo uveljavijo (z odobritvijo skrbnika) in vpišejo.

Uporabniški račun programa Windows

Uporabnik, ki je pooblaščen za prijavo v omrežje ali v posamezni računalnik.

varno brisanje
Izvedba algoritma, ki prepiše podatke, ki jih sredstvo vsebuje, z nesmiselnimi podatki.

Varnost s prijavo v Windows
Ščiti vaš(-e) račun(-e) Windows tako, da za dostop zahteva posebne poverilnice.

varnostna kopija
Z uporabo funkcije varnostnega kopiranja lahko shranite kopijo pomembnih podatkov o programu na lokacijo zunaj programa. Kasneje jo lahko uporabite za obnovitev podatkov v isti računalnik ali drug računalnik.

vdelan varnostni čip za Trusted Platform Module (TPM)
TPM preverja pristnost računalnika, ne uporabnika, in sicer tako, da shranjuje podatke, značilne za gostiteljski sistem, kot so šifrirni ključi, digitalna potrdila in gesla. TPM zmanjšuje tveganje zlorabe podatkov v računalniku zaradi fizične kraje ali napada zunanjega hekerja.

zaslon Drive Encryption za prijavo
Glejte preverjanje pristnosti Drive Encryption pred zagonom.

Stvarno kazalo