HP Client Security

Početak rada

Prvo izdanje: kolovoz 2013.

Kataloški broj dokumenta: 735339-BC1

Sadržaj

1 Uvod u softver HP Client Security Manager

Aplikacija HP sigurnost klijenta omogućuje vam zaštiti podatke, uređaj i identitet i na taj način povećati sigurnost vašeg računala.

Moduli softvera dostupni za vaše računalo mogu se razlikovati ovisno o modelu.

Moduli softvera HP Client Security mogu biti unaprijed instalirani, unaprijed učitani ili dostupni za preuzimanje s web-mjesta tvrtke HP. Dodatne informacije potražite u odjeljku http://www.hp.com.

NAPOMENA: Upute u ovom vodiču napisane su uz pretpostavku da ste već instalirali odgovarajuće module softvera HP Client Security.

Značajke softvera HP Client Security

U sljedećoj tablici detaljno su razrađene glavne značajke modula HP Client Security.

Modul	Glavne značajke
HP Client Security Manager	Administratori mogu obavljati sljedeće funkcije: • Zaštitu računala prije pokretanja sustava Windows® • Zaštitu vašeg Windows računa pomoću jake provjere autentičnosti • Upravljanje prijavom i lozinkama za web-mjesta i aplikacije • Jednostavnu promjenu vaše lozinke za operacijski sustav Windows • Upotrebu otisaka prstiju za dodatnu sigurnost i praktičnost • Postavljanje pametne kartice, beskontaktne kartice ili blizinske kartice za provjeru autentičnosti • Upotrebu vašeg Bluetooth telefona kao načina identifikacije • Postavljanje PIN broja kako bi se proširile vaše mogućnosti provjere autentičnosti • Konfiguriranje pravila prijave i sesije • Sigurnosno kopiranje i vraćanje podataka programa • Dodavanje više aplikacija kao što su HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager i HP Computrace Korisnici mogu obavljati sljedeće funkcije: • Pregled postavki značajki Encryption Status i Device Access Manager. • Pokrenuti Computrace. • Konfigurirati opcije Postavki i Sigurnosnog kopiranja i vraćanja.

Modul	Glavne značajke
Password Manager	Korisnici mogu obavljati sljedeće funkcije: • Organizirati i postaviti korisnička imena i lozinke. • Stvoriti jače lozinke za veću sigurnost računa za elektroničku poštu i web računa. Password Manager automatski popunjava i šalje informacije. • Pojednostavnite postupak prijave pomoću značajke Jedinstvena prijava koja automatski pamti i primjenjuje vjerodajnice korisnika. • Označite račun kao ugrožen te ćete tako dobiti upozorenje za drugi račun(e) sa sličnim vjerodajnicama. • Uvezite podatke za prijavu s podržanog preglednika.
HP Drive Encryption (samo odabrani modeli)	• Pruža potpuno šifriranje cijelog tvrdog diska. • Prinudno provodi provjeru autentičnosti kod predpokretanja kako bi dešifrirao podatke i pristupio im. • Pruža mogućnost aktivacije samošifranja pogona (samo odabrani modeli).
HP Device Access Manager	• Omogućuje upraviteljima IT sustava upravljanje pristupom uređajima na temelju korisničkih profila. • Sprječava da neovlašteni korisnicu uklanjaju podatke pomoću vanjskih medija za pohranjivanje te uvođenje virusa u sustav s vanjskog medija. • Omogućuje administratorima onemogućavanje pristupa komunikacijskim uređajima za određene pojedince ili grupe korisnika.
HP Trust Circles	• Daje sigurnost datotekama i dokumentima. • Šifrira datoteke koje se nalaze u korisnički definiranima mapama štiteći ih unutar kruga povjerenja. • Omogućuje da datoteke upotrebljavaju i dijele isključivo članovi kruga povjerenja.
Oporavak nakon krađe (Computrace, kupuje se odvojeno)	• Potrebno je posebno kupiti praćenje i aktivirati pretplatu za praćenje. • Omogućuje sigurno praćenje zapisa. • Nadzire aktivnost korisnika kao i promjene hardvera i softvera. • Ostaje aktivan čak i ako se tvrdi disk ponovno formatira ili zamijeni.

Opis proizvoda HP Client Security i primjeri najčešćih načina primjene

Većina proizvoda HP Client Security ima provjeru autentičnosti korisnika (obično lozinku) i sigurnosno kopiranje administratora kako bi se omogućio pristup u slučaju da se lozinka izgubi, ne bude dostupna ili se zaboravi i u svakom trenutku kada je pristup potreban zbog korporativne sigurnosti.

NAPOMENA: Neki od proizvoda HP Client Security izrađeni su kako bi se ograničio pristup podacima. Podaci se moraju šifrirati kada su tako važni da bi korisnik radije izgubio informacije nego li ih ugrozio. Preporučuje se sigurnosno kopirati sve podatke na sigurno mjesto.

Password Manager

Password Manager pohranjuje korisnička imena i lozinke i može se upotrebljavati za:

- Spremanje imena za prijavu i lozinki za pristup internetu ili e-pošti.
- Automatsku prijavu korisnika na web-mjesto ili e-poštu.
- Upravljanje i organiziranje provjera autentičnosti.
- Odabir zapisa na webu ili mreži i izravno pristupanje vezi.
- Prikaz imena i lozinki kada je to potrebno.
- Označite račun kao ugrožen te ćete tako dobiti upozorenje za drugi račun(e) sa sličnim vjerodajnicama.
- Uvezite podatke za prijavu s podržanog preglednika.

Primjer 1: Osoba zadužena za kupovinu velikog proizvođača obavlja većinu korporacijskih transakcija putem interneta. Ona često posjećuje nekoliko popularnih web-mjesta za koja trebaju podaci za prijavu. Budući da se brine za sigurnost ne upotrebljava istu lozinku na svakom računu. Osoba zadužena za kupovinu odlučila je upotrebljavati značajku Password Manager za usklađivanje web-veza s različitim korisničkim imenima i lozinkama. Kada odlazi na određeno web-mjesto kako bi se prijavila, Password Manager automatski daje vjerodajnice. Ako želi vidjeti korisnička imena i lozinke može konfigurirati značajku Password Manager da ih prikazuje.

Password Manager može se upotrebljavati i za upravljanje i organiziranje provjere autentičnosti. Taj će alat omogućiti korisniku odabir zapisa na webu ili mreži i izravno pristupiti vezi. Korisnik, kada je to potrebno, može i vidjeti korisnička imena i lozinke.

Primjer 2: Zaposlenik koji vrijedno radi unaprijeđen je i sada će upravljati cijelim odjelom računovodstva. Tim se mora prijavljivati na veliki broj web-računa stranki, a svaki od njih upotrebljava drugačije podatke za prijavu. Ti podaci moraju se dijeliti s drugim zaposlenicima tako da je povjerljivost vrlo važna. Zaposlenik odluči organizirati sve web-veze, korisnička imena tvrtke i lozinke unutar značajke Password Manager. Kada se to završi, zaposlenik uvodi značajku Password Manager ostalim zaposlenicima tako da mogu raditi na web-računima, a da nikada ne saznaju vjerodajnice za prijavu koje upotrebljavaju.

HP Drive Encryption (samo odabrani modeli)

HP Drive Encryption se upotrebljava za ograničavanje pristupa podacima na cijelom tvrdom disku računala ili na sekundarnom disku. Drive Encryption može upravljati i samošifrirajućim diskovima.

Primjer 1: Liječnik želi biti siguran da samo on ima pristup svim podacima na tvrdom disku računala. Liječnik aktivira softver Drive Encryption za koji je potrebna provjera autentičnosti prije prijave u sustav Windows. Kada se postavi, tvrdom se disku ne može pristupiti bez unosa lozinke prije pokretanja operacijskog sustava. Liječnik može dodatno povećati sigurnost diska odabirom šifriranja podataka u opciji samošifrirajućeg diska.

Primjer 2: Administrator bolnice želi osigurati da samo liječnici i ovlašteno osoblje mogu pristupati svim podacima na njihovom lokalnom računalu, a da ne moraju dijeliti svoje osobne lozinke. Informatički odjel dodaje administratora, liječnike i sve ovlaštene osobe kao korisnike softvera Drive Encryption. Sada se samo ovlaštene osobe mogu prijaviti na računalo ili domenu pomoću svojih osobnih korisničkih imena i lozinki.

HP Device Access Manager (samo odabrani modeli)

HP Device Access Manager omogućuje administratoru ograničavanje i upravljanje pristupom hardveru. Softver Device Access Manager može se upotrebljavati za blokiranje neovlaštenog pristupa

USB izbrisivom memorijskom pogonu gdje se podaci mogu kopirati. On također može ograničiti pristup CD/DVD pogonima, upravljanje USB uređajima, mrežnim vezama i tako dalje. Kao primjer može poslužiti slučaj kada vanjski prodavači trebaju pristupiti računalima tvrtke, ali ne smiju imati mogućnost kopiranja podataka na USB disk.

Primjer 1: Upravitelj tvrtke za opskrbu medicinskim materijalima često radi s osobnim liječničkim podacima kao i s njegovim podacima tvrtke. Zaposlenici trebaju imati pristup tim podacima, međutim, iznimno je važno da se ti podaci ne mogu ukloniti s računala pomoću USB diska ili vanjskog medija za pohranjivanje. Mreža je sigurna, no računala imaju CD snimače i USB priključke koji omogućuju kopiranje ili krađu podataka. Upravitelj upotrebljava softver Device Access Manager kako bi onemogućio upotrebu USB priključaka i CD snimača. Čak i kada se blokiraju USB priključci, miš i tipkovnice nastavljaju raditi.

Primjer 2: Osiguravajuća tvrtka ne želi da zaposlenici instaliraju ili učitaju osobne softvere ili podatke od kuće. Neki zaposlenici trebaju pristup USB priključcima na svim računalima. Voditelj informatičkog odjela može upotrijebiti softver Device Access Manager kako bi omogućio pristup nekim zaposlenicima istovremeno blokirajući vanjski pristup ostalima.

Computrace (kupuje se odvojeno)

Computrace (kupuje se odvojeno) je usluga koja može pratiti lokaciju ukradenog računala svaki put kada korisnik pristupi internetu. Computrace također može daljinski upravljati i odrediti položaj računala te nadzirati upotrebu računala i aplikacija.

Primjer 1: Ravnatelj škole dao je upute informatičkom odjelu da prati sva računala u školi. Nakon što je obavljena inventura računala, administrator informatičkog odjela registrirao je sva računala opremljena značajkom Computrace te se ona, u slučaju krađe, mogu pratiti. Nedavno su u školi primijetili da neka računa nedostaju te je administrator informatičkog odjela o tome obavijestio policiju i službenike Computrace. Računalima je određen položaj i policija ih je vratila u školu.

Primjer 2: Tvrtka koja se bavi nekretninama treba upravljati i ažurirati računala diljem svijeta. Oni upotrebljavaju uslugu Computrace za nadzor i ažuriranje računala, a da ne moraju slati informatičara do svakog pojedinog računala.

Ostvarivanje glavnih sigurnosnih ciljeva

Moduli HP Client Security mogu zajedno djelovati kako bi pružili rješenja za cijeli niz sigurnosnih pitanja uključujući i sljedeće glavne sigurnosne ciljeve:

- zaštitu od ciljane krađe
- ograničavanje pristupa osjetljivim podacima
- sprječavanje neovlaštenog pristupa s internih ili vanjskih lokacija
- strategija stvaranja snažne lozinke

Zaštita od ciljane krađe

Primjer ciljane krađe bila bi krađa računala koje sadrži povjerljive podatke i podatke o korisniku na sigurnosnoj kontrolnoj točci aerodroma. Sljedeće značajke pomažu u sprječavanju od ciljane krađe:

- značajka provjere autentičnosti kod pokretanja, ako je omogućena, pomaže u sprječavanju pristupa operacijskom sustavu.
  - HP Client Security—Pogledajte HP Client Security na stranici 12.
  - HP Drive Encryption—Pogledajte HP Drive Encryption (samo odabrani modeli) na stranici 29.
- Šifriranjem se osigurava da se podacima ne može pristupiti čak i ako se tvrdi disk ukloni i instalira ne sustav koji nije osiguran.
- Computrace može pratiti lokaciju računala nakon krađe.
  - Computrace—Pogledajte Oporavak nakon krađe (samo odabrani modeli) na stranici 53.

Ograničavanje pristupa osjetljivim podacima

Pretpostavimo da ovlašteni revizor radi u tvrtci i da mu je odobren pristup računalu za pregled osjetljivih financijskih podataka. Ne želite da revizor može ispisati datoteke ili ih pohraniti na uređaju na koji se može upisivati kao što je CD. Sljedeće značajke pomažu u ograničavanju pristupa podacima:

- HP Device Access Manager omogućuje voditeljima informatičkog odjela ograničavanje pristupa komunikacijskim uređajima tako da se osjetljive informacije ne mogu kopirati s tvrdog diska. Pogledajte odjeljak Prikaz sustava na stranici 43.

Sprječavanje neovlaštenog pristupa s internih ili vanjskih lokacija

Neovlašteni pristup neosiguranom poslovnom računalu predstavlja iznimno veliku stvarnu opasnost za mrežne resurse poduzeća kao što su informacije iz financijskih službi, izvršnog odjela ili odjela za istraživanje i razvoj te privatnih informacija kao što su podaci o bolesnicima ili osobni financijski podaci. Sljedeće značajke pomažu u sprječavanju neovlaštenog pristupa:

- Značajka provjere autentičnosti kod pokretanja, ako je omogućena, pomaže u sprječavanju pristupa operacijskom sustavu. (pogledajte HP Drive Encryption (samo odabrani modeli) na stranici 29.
- HP Client Security osigurava da neovlašteni korisnik ne može dobiti lozinku ili pristupiti aplikacijama zaštićenima lozinkom. Pogledajte odjeljak HP Client Security na stranici 12.
- HP Device Access Manager omogućuje voditeljima informatičkog odjela ograničavanje pristupa uređajima za upisivanje tako da se osjetljive informacije ne mogu kopirati s tvrdog diska. Pogledajte odjeljak HP Device Access Manager (samo odabrani modeli) na stranici 42.

Pravila stvaranja jake lozinke

Ako je pravilo tvrtke da je potrebno stvoriti jake lozinke za desetke aplikacija koje se temelje na webu i baze podataka, značajka Password Manager pruža zaštićeno sigurno spremište za lozinke i mogućnost jedinstvene prijave. Pogledajte odjeljak Password Manager na stranici 18.

Dodatni sigurnosni elementi

Dodjeljivanje sigurnosnih uloga

U upravljanju računalnom sigurnosti (posebice za velike organizacije), važno je podijeliti odgovornosti i prava različitim vrstama administratora i korisnika.

NAPOMENA: U malim organizacijama ili za pojedinačnu upotrebu te uloge može imati ista osoba.

Za softver HP Client Security sigurnosne dužnosti i ovlasti mogu se podijeliti na sljedeće uloge:

- Voditelj sigurnosti—Određuje razinu sigurnosti za tvrtku ili mrežu i određuje koje se sigurnosne značajke trebaju primijeniti kao što je Drive Encryption.

  NAPOMENA: Brojne značajke softvera HP Client Security voditelj sigurnosti može prilagoditi u suradnji s tvrtkom HP. Dodatne informacije potražite u odjeljku http://www.hp.com.

- Administrator informatičkog odjela—Primjenjuje i upravlja sigurnosnim značajkama koje je odredio voditelj sigurnosti. Neke značajke može i omogućiti ili onemogućiti. Na primjer, ako je voditelj sigurnosti odlučio primijeniti pametne kartice, administrator informatičkog odjela može omogućiti i način rada pomoću lozinke i način rada pametne kartice.
- Korisnik—Upotrebljava sigurnosne značajke. Na primjer, ako su voditelj sigurnosti i administrator informatičkog odjela omogućili pametne kartice za sustav, korisnik može postaviti PIN pametne kartice i upotrebljavati karticu za provjeru autentičnosti.

OPREZ: Administratori se potiču na primjenu “dobrih rješenja” za ograničavanje ovlasti krajnjih korisnika i ograničavanje pristupa korisnicima.

Neovlaštenim korisnicima ne smiju se dodijeliti ovlasti administratora.

Upravljanje lozinkama softvera HP Client Security

Većina značajki softvera HP Client Security zaštićena je lozinkama. U sljedećoj tablici navedene su često korištene lozinke, moduli softvera gdje je lozinka postavljena i funkcije lozinke.

Lozinke koje postavljaju i upotrebljavaju samo administratori informatičkog odjela također su navedeni u ovoj tablici. Sve ostale lozinke mogu postaviti redoviti korisnici ili administratori.

Lozinka softvera HP Client Security	Postavljeni u sljedećem modulu	Funkcija
Lozinka za prijavu u sustav Windows	Upravljačka ploča sustava Windows ili HP Client Security	Služi za ručnu prijavu i za provjeru autentičnosti prilikom pristupanja raznim značajkama softvera HP Client Security.
Lozinka značajke sigurnosnog kopiranja i oporavka softvera HP Client Security	HP Client Security, od strane pojedinačnog korisnika	Štiti pristup datoteci sigurnosne kopije i oporavka softvera HP Client Security.
PIN pametne kartice	Credential Manager (Upravitelj vjerodajnica)	Može se upotrebljavati kao provjera autentičnosti za više faktora. Može se upotrebljavati kao provjera autentičnosti za sustav Windows. Provjerava autentičnost korisnika aplikacije Drive Encryption, ako se odabere pametna kartica.

Stvaranje sigurne lozinke

Prilikom stvaranja lozinki morate najprije slijediti sve specifikacije koje postavlja program. Ipak, u pravilu, sljedeće smjernice smatrajte pomoći za stvaranje snažnih lozinki i smanjenje mogućnosti ugrožavanja lozinki:

- Upotrebljavajte lozinke s više od 6, a po mogućnosti s više od 8 znakova.
- U lozinkama pomiješajte mala i velika slova.
- Gdje je god moguće pomiješajte alfanumeričke znakove te dodajte posebne znakove i punktuacije.
- Posebnim znakovima ili brojkama zamijenite slova u glavnoj riječi. Na primjer brojkom 1 možete zamijeniti slova I ili L.
- Kombinirajte riječi iz 2 ili više jezika.
- Razdvojite riječ ili rečenicu brojkama ili posebnim znakovima u sredini, na primjer “Mary2-2Cat45.”
- Ne upotrebljavajte kao lozinku riječ koja se javlja u rječniku.
- Za lozinku ne upotrebljavajte svoje ime ili bilo koji drugi osobni podatak kao što je datum rođenja, ime kućnog ljubimca, djevojačko prezime majke pa čak niti napisano obrnutim redoslijedom.
- Redovito mijenjajte lozinku. Možete promijeniti samo nekoliko slova kao dodatak.
- Ako lozinku zapisujete, ne pohranjujte je na vidljivom mjestu blizu računala.
- Ne spremajte lozinku u datoteku računala kao što je poruka e-pošte.
- Ne dijelite račune i nikome ne povjeravajte svoju lozinku.

Stvaranje sigurnosne kopije vjerodajnica i postavki

Alat za stvaranje sigurnosne kopije i vraćanje softvera HP Client Security možete upotrijebiti kao središnje mjesto s kojeg možete stvarati sigurnosne kopije i vraćati sigurnosne vjerodajnice za neke od instaliranih modula softvera HP Client Security.

2 Početak rada

Za konfiguriranje aplikacije HP Client Security za upotrebu s vašim vjerodajnicama pokrenite aplikaciju HP Client Security na jedan od sljedećih načina: Kada je korisnik dovršio čarobnjaka, isti ga korisnik više ne može pokrenuti.

1. Na početnom zaslonu ili zaslonu Aplikacije kliknite ili dodirnite **HP Client Security** (Windows 8).

   – ili –

   S radne površine sustava Windows kliknite ili dodirnite **programčić HP Client Security** (Windows 7).

   – ili –

   Na radnoj površini sustava Windows dva puta kliknite ikonu **HP Client Security** u području obavijesti na krajnjem desnom dijelu programske trake.

   – ili –

   S radne površine Windows kliknite ili dodirnite ikonu **HP Client Security** u području obavijesti i zatim odaberite **Otvori HP Client Security**.

2. Čarobnjak za postavljanje aplikacije HP Client Security pokreće se s prikazanom stranicom dobrodošlice.

3. Pročitajte zaslon dobrodošlice, potvrdite svoj identitet upisujući lozinku sustava Windows i zatim kliknite ili dodirnite **Sljedeće**.

   Ako još niste stvorili lozinku za sustav Windows, od vas će se tražiti da je stvorite. Lozinka za sustav Windows potrebna je kako biste zaštitili svoj Windows račun od pristupa neovlaštenih osoba i kako biste mogli upotrebljavati značajke aplikacije HP Client Security.

4. Na stranici HP SpareKey odaberite tri sigurnosna pitanja. Unesite odgovor na svako od pitanja i zatim kliknite **Sljedeće**. Dozvoljena su i prilagođena pitanja. Dodatne informacije potražite u odjeljku HP SpareKey—Oporavak lozinke na stranici 14.

5. Na stranici otisci prstiju unesite barem najmanje traženi broj otisaka prstiju i zatim kliknite ili dodirnite **Sljedeće**. Dodatne informacije potražite u odjeljku Otisci prstiju na stranici 12.

6. Na stranici Drive Encryption aktivirajte šifriranje, sigurnosno kopirajte ključ za šifriranje i zatim kliknite ili dodirnite **Sljedeće**. Više informacija potražite u Pomoći za softver HP Drive Encryption.

   NAPOMENA: Ovo se odnosi na slučaj kada je korisnik administrator i kada administrator ranije nije konfigurirao čarobnjaka za postavljanje aplikacije HP Client Security.

7. Na zadnjoj stranici čarobnjaka kliknite ili dodirnite **Završi**.

   Na ovoj se stranici donosi status značajki u vjerodajnica.

8. Čarobnjak za postavljanje aplikacije HP Client Security osigurava aktivaciju značajki Just In Time Authentication i File Sanitizer. Više informacija potražite u Pomoći za softver HP Device Access Manager i Pomoći za softver HP File Sanitizer.

   NAPOMENA: Ovo se odnosi na slučaj kada je korisnik administrator i kada administrator ranije nije konfigurirao čarobnjaka za postavljanje aplikacije HP Client Security.

Otvaranje aplikacije HP Client Security

Aplikaciju HP Client Security možete otvoriti na jedan od sljedećih načina:

NAPOMENA: Čarobnjak za postavljanje aplikacije HP Client Security mora biti dovršen prije nego što se može pokrenuti aplikacija HP Client Security.

- Na početnom zaslonu ili zaslonu Aplikacije kliknite ili dodirnite aplikaciju **HP Client Security**.

  – ili –

  S radne površine sustava Windows kliknite ili dodirnite **programčić HP Client Security** (Windows 7).

  – ili –

  Na radnoj površini sustava Windows dva puta kliknite ikonu **HP Client Security** u području obavijesti na krajnjem desnom dijelu programske trake.

  – ili –

  S radne površine Windows kliknite ili dodirnite ikonu **HP Client Security** u području obavijesti i zatim odaberite **Otvori HP Client Security**.

3 Vodič za lako postavljanje za male tvrtke

Ovo je poglavlje sastavljeno kako bi vam se pokazali osnovni koraci za uključivanje najčešći i najkorisnijih opcija softvera HP Client Security za male tvrtke. Brojni alati i opcije omogućuju vam fino podešavanje postavki i postavljanje kontroli za pristup. Ovaj vodič za lako postavljanje usmjeren je na što najlakše i najkraće postavljanje i pokretanje svakog modula. Za dodatne informacije odaberite modul koji vas zanima i kliknite **?** ili gumb Pomoć u gornjem desnom kutu. Ovaj će gumb automatski prikazati informacije za pomoć s trenutačno prikazanim prozorom.

Početak rada

1. S radne površine Windows otvorite HP Client Security taji dva puta kliknite ikonu **HP Client Security** u području obavijesti koje se nalazi na krajnjem desnom dijelu programske trake.
2. Unesite svoju lozinku za sustav Windows ili stvorite lozinku za sustav Windows.
3. Dovršite postavljanje softvera HP Client Security.

Kako bi softver HP sigurnosni klijent samo jednom trebao provjeru autentičnosti prilikom prijave u sustav Windows, pogledajte Značajke sigurnosti na stranici 26.

Password Manager

Svi imaju priličan broj lozinki – posebice ako često pristupaju web-mjestima ili upotrebljavaju aplikacije za koje je potrebna prijava. Obični korisnici upotrebljavaju iste lozinke za sve aplikacije i web-mjesta ili postanu kreativni i brzo zaborave koja lozinka ide uz koju aplikaciju.

Password Manager može automatski zapamtiti vaše lozinke ili vam pružiti mogućnost razlikovanja koja mjesta treba upamtiti, a koja izostaviti. Kada se prijavite na računalo, aplikacija Password Manager dat će vam lozinke ili vjerodajnice za pristupanje aplikacijama ili web-mjestima.

Kada pristupite aplikaciji ili web-mjestu za koje trebaju vjerodajnice, Password Manager automatski će prepoznati mjesto i upitati vas želite li da softver pamti tu informaciju. Ako neka mjesta želite izuzeti možete odbiti zahtjev.

Za pokretanje spremanja web-lokacija. korisničkih imena i lozinki:

1. Na primjer, otiđite na web-mjesto ili aplikaciju i zatim kliknite na ikonu softvera Password Manager u gornjem lijevom kutu web-mjesta kako biste dodali provjeru autentičnosti web mjesta.
2. Dodijelite ime vezi (opcija) i unesite korisničko ime i lozinku u Password Manager.
3. Kada završite kliknite gumb **U redu**.
4. Password Manager može spremiti i korisničko ime i lozinke za zajedničke mrežne resurse ili preslikane mrežne pogone.

Prikaz i upravljanje spremljenih provjera autentičnosti u softveru Password Manager

Password Manager omogućuje vam prikazivanje, upravljanje, sigurnosno kopiranje i pokretanje provjere autentifikacije s jedne središnje lokacije. Password Manager također podržava i pokretanje spremljenih mjesta iz sustava Windows.

Za otvaranje softvera Password Manager na tipkovnici pritisnite kombinaciju tipki Ctrl+Windows+h kako biste otvorili Password Manager, a zatim kliknite **Prijavi** za pokretanje spremljene kratice provjere autentičnosti.

Opcija **Uredi** softvera Password Manager omogućuje vam izmjenu imena, imena za prijavu pa čak i otkrivanje lozinke.

HP sigurnosni klijent za male tvrtke omogućuje vam da sigurnosno kopiranje i/ili kopiranje svih vjerodajnica i postavki na drugo računalo.

HP Device Access Manager

Device Access Manager može se upotrijebiti za ograničavanje upotrebe različitih internih i vanjskih uređaja za pohranjivanje tako da su podaci sigurni na tvrdom disku i ne mogu se odšetati iz vaše tvrtke. Primjer bi bio slučaj kada se korisniku omogući pristup vašim podacima, ali mu se blokira kopiranje na CD, uređaj za reprodukciju glazbe ili memorijski USB uređaj.

1. Otvorite **Device Access Manager** (pogledajte Otvaranje softvera Device Access Manager na stranici 42).

   Prikazuje se pristup za trenutačnog korisnika.

2. Za promjenu pristupa za korisnike, grupe ili uređaje, kliknite ili dodirnite **Promijeni**. Dodatne informacije potražite u odjeljku Prikaz sustava na stranici 43.

HP Drive Encryption

HP Drive Encryption upotrebljava se za zaštitu podataka šifriranjem cijelog tvrdog diska. Podaci na tvrdom disku ostaju zaštićeni čak i ako dođe do krađe računala i/ili ako se tvrdi disk skine s originalnog računala i postavi na drugo računalo.

Dodatna sigurnosna pogodnost je da softver Drive Encryption traži da se pravilno provjeri autentičnost pomoću korisničkog imena i lozinke prije pokretanja operacijskog sustava. Ovaj se postupak naziva provjera autentičnosti prije pokretanja.

Kako bi vam se ovo olakšalo, brojni moduli softvera automatski sinkroniziraju lozinke uključujući i korisničke račune sustava Windows, provjeru autentičnosti domene, softvera HP Drive Encryption, Password Manager i HP Client Security.

Za postavljanje softvera HP Drive Encryption tijekom početnog postavljanja pomoću čarobnjaka za postavljanje softvera HP Client Security, pogledajte Početak rada na stranici 8.

4 HP Client Security

Početna stranica aplikacije HP Client Security središnje je mjesto jednostavnog pristupa značajkama, aplikacijama i postavkama HP Client Security. Početna stranica podijeljena je na tri dijela:

- **PODACI**—Omogućuje pristup aplikacijama koje se upotrebljavaju za upravljanje sigurnošću podataka.
- **UREĐAJI**—Omogućuje pristup aplikacijama koje se upotrebljavaju za upravljanje sigurnošću uređaja.
- **IDENTITET**—Omogućuje unošenje i upravljanje vjerodajnicama autentičnosti.

Pomaknite klizač preko pločice aplikacije kako bi se prikazao opis aplikacije.

Aplikacija HP Client Security može pružiti veze za korisničke i administrativne postavke na dnu stranice. Aplikacija HP Client Security omogućuje pristup naprednim postavkama i značajkama tako da se dodirne ikona (postavki) **Zupčanik**.

Značajke, aplikacije i postavke identiteta

Značajke, aplikacije i postavke identiteta koje daje HP Client Security pomažu vam u upravljanju različitim aspektima digitalnog identiteta. Kliknite ili dodirnite sljedeće pločice na početnoj stranici HP sigurnosnog klijenta i unesite svoju lozinku za sustav Windows:

- **Otisak prsta**—Unosi i upravlja vašim vjerodajnicama otiska prsta.
- **SpareKey**—Postavlja i upravlja vašim vjerodajnicama za HP SpareKey koje se mogu upotrijebiti za prijavu na vašem računalu ako su ostale vjerodajnice izgubljene ili zametnute. Također vam omogućuje ponovno postavljanje zaboravljene lozinke.
- **Lozinka za sustav Windows**—Daje jednostavan pristup za promjenu vaše lozinke za sustav Windows.
- **Bluetooth uređaji**—Omogućuje vam unošenje i upravljanje vašim Bluetooth uređajima.
- **Kartice**—Omogućuje vam unošenje i upravljanje pametnim karticama, beskontaktnim karticama i blizinskim karticama.
- **PIN**—Omogućuje vam unošenje i upravljanje vašom vjerodajnicom PIN.
- **RSA SecurID**—Omogućuje vam unošenje i upravljanje vjerodajnicama RSASecurID (ako je odgovarajuća instalacija postavljena).
- **Password Manager**—Omogućuje vam upravljanje lozinkama za vaše račune i aplikacije na mreži.

Otisci prstiju

Čarobnjak za postavljanje aplikacije HP Client Security vodi vas kroz postupak postavljanja ili “unosa” vaših otisaka prstiju.

Otiske prstiju možete unijeti ili izbrisati na stranici otisaka prstiju kojoj možete pristupiti tako da kliknete ili dodirnete ikonu **Otisci prstiju** na početnoj stranici HP Client Security.

1. Na stranici otisaka prstiju prelazite prstom sve dok se uspješno ne unese.

   Broj prstiju koje je potrebno unijeti naveden je na stranici. Najbolje bi bilo unijeti kažiprst ili srednji prst.

2. Za brisanje ranije unesenih otisaka prstiju kliknite ili dodirnite **Izbriši**.

3. Za unos dodatnih prstiju kliknite ili dodirnite **Unesi dodatni otisak prsta**.

4. Kliknite ili dodirnite **Spremi** prije napuštanja stranice.

⚠ **OPREZ:** Kada unosite otiske prstiju kroz čarobnjak podaci o otisku prsta ne spremaju se sve dok ne kliknete **Sljedeće**. Ako na neko vrijeme ostavite računalo neaktivnim ili zatvorite program, promjene koje ste napravili **nisu** spremljene.

- ▲ Za pristup administrativnim postavkama otiska prsta u kojima administratori mogu odrediti unos, preciznost i druge postavke kliknite ili dodirnite **Administrativne postavke** (za ovo su potrebne administrativne ovlasti).
- ▲ Za pristup korisničkim postavkama otisaka prstiju u kojima možete odrediti postavke koje upravljanju izgledom i ponašanjem za prepoznavanje otiska prsta kliknite ili dodirnite **Korisničke postavke**.

Administrativne postavke otisaka prstiju

Administratori mogu odrediti unos, preciznost i druge postavke za čitač otiska prsta. Potrebne su administratorske ovlasti.

- ▲ Za pristup administrativnim postavkama za vjerodajnice otiska prsta kliknite ili dodirnite **Administrativne postavke** na stranici otisaka prsta.

- **Unos korisnika**—Odaberite najmanji i najveći broj otisaka prstiju koje korisnik može unijeti.
- **Prepoznavanje**—Pomaknite klizač kako biste podesili osjetljivost čitača otiska prsta kada prijeđete prstom.

  Ako se otisak prsta stalno ne prepoznaje možda ćete trebati odabrati nižu postavku prepoznavanja. Viša postavka povećava osjetljivost na varijacije prelaska otiska prsta i zbog toga se umanjuje mogućnost lažnog prihvaćanja. **Srednje visoka** postavka predstavlja dobru kombinaciju sigurnosti i praktičnosti.

Korisničke postavke otisaka prstiju

Na stranici korisničkih postavki otiska prsta možete odrediti postavke koje upravljanju izgledom i ponašanjem za prepoznavanje otiska prsta .

- ▲ Za pristup korisničkim postavkama za vjerodajnice otiska prsta kliknite ili dodirnite **Korisničke postavke** na stranici otisaka prsta.

- **Omogući zvučnu povratnu informaciju**—Po zadanim postavkama, HP Client Security daje zvučnu povratnu informaciju kada se prijeđe prstom reproducirajući različite zvukove za određene događaje programa. Nove zvukove tim događajima možete dodijeliti kroz karticu Zvukovi u postavkama zvuka na upravljačkoj ploči sustava Windows ili za onemogućavanje zvučne povratne informacije očistite potvrdni okvir.
- **Prikaži povratnu informaciju kvalitete skeniranja**—Za prikaz svih prelazaka prstiju, neovisno o kvaliteti, odaberite potvrdni okvir. Za prikaz samo prelazaka prstiju dobre kvalitete očistite potvrdni okvir.

HP SpareKey—Oporavak lozinke

HP SpareKey omogućuje vam da dobijete pristup svom računalu (na platformama koje se podržavaju) odgovarajući na tri sigurnosna pitanja.

HP Client Security traži od vas da postavite vlastiti HP SpareKey tijekom početnog postavljanja u čarobnjaku za postavljanje aplikacije HP Client Security.

Za postavljanje vlastitog HP SpareKey:

1. Na stranici HP SpareKey čarobnjaka odaberite tri sigurnosna pitanja i zatim unesite odgovor na svako pitanje.

   Možete odabrati pitanje s unaprijed određenog popisa pitanja ili napisati vlastito pitanje.

2. Kliknite ili dodirnite **Unesi**.

Za brisanje vlastitog HP SpareKey:

▲ Kliknite ili dodirnite **Obriši svoj SpareKey**.

Nakon što postavite vlastiti SpareKey svojem računalu možete pristupiti pomoću značajke SpareKey iz zaslona za prijavu za provjeru autentičnosti pri uključivanju ili iz zaslona dobrodošlice sustava Windows.

Možete odabrati različita pitanja ili promijeniti svoje odgovore na stranici Sparekey kojoj se pristupa iz pločice Oporavak lozinke na početnoj stranici aplikaciji HP Client Security.

Za pristup postavkama uslužnog programa HP SpareKey gdje administrator može odrediti postavke koje se odnose na vjerodajnice HP SpareKey kliknite **Postavke** (za ovo su potrebne administrativne ovlasti).

Postavke HP SpareKey

Na stranici postavki uslužnog programa HP SpareKey možete odrediti postavke koje upravljaju ponašanjem i upotrebom vjerodajnice za HP SpareKey.

▲ Za pokretanje stranice postavki uslužnog programa HP SpareKey kliknite ili dodirnite **Postavke** na stranici HP SpareKey (za ovo su potrebne administrativne ovlasti).

Administratori mogu odabrati sljedeće postavke:

- Odredite pitanja koja se predstavljaju svakom korisniku tijekom postavljanja uslužnog programa HP SpareKey.
- Dodajte najviše tri prilagođena sigurnosna pitanja koja se dodaju popisu koji se predstavlja korisnicima.
- Odaberite želite li ili ne dozvoliti korisnicima upisivanje vlastitih sigurnosnih pitanja.
- Odredite koje okruženje provjere autentičnosti (Windows ili provjera autentičnosti kod uključenja) omogućuje upotrebu uslužnog programa HP SpareKey za oporavak lozinke.

Lozinka za sustav Windows

Aplikacija HP Client Security omogućuje jednostavniju i bržu promjenu vaše lozinke za sustav Windows nego što je to moguće kroz upravljačku ploču sustava Windows.

Za promjenu lozinke za sustav Windows:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite **Lozinka za sustav Windows**.
2. Unesite svoju trenutačnu lozinku u tekstualni okvir **Trenutačna lozinka za sustav Windows**.
3. Upišite novu lozinku u tekstualni okvir **Nova lozinka za sustav Windows** i zatim je ponovno upišite u tekstualni okvir **Potvrdi novu lozinku**.
4. Kliknite ili dodirnite **Promijeni** kako biste odmah promijenili svoju trenutačnu lozinku u novu koju ste unijeli.

Bluetooth uređaji

Ako je administrator omogućio Bluetooth kao vjerodajnicu za provjeru možete postaviti Bluetooth telefon u vezi s drugim vjerodajnicama za dodatnu sigurnost.

NAPOMENA: Podržavaju se samo Bluetooth telefonski uređaji.

1. Provjerite je li na računalu omogućena funkcija Bluetooth i je li Bluetooth telefon postavljen u načinu rada za otkrivanje. Za spajanje telefona možda ćete trebati u Bluetooth uređaj upisati kod koji se automatski generira. Ovisno o postavkama konfiguracije Bluetooth uređaja možda ćete trebati obaviti usporedbu kodova uparivanja između računala i telefona.
2. Za unos telefona, odaberite ga i zatim kliknite ili dodirnite **Unesi**.

Za pristup Postavke Bluetooth uređaja na stranici 15stranici gdje administrator može odrediti postavke za Bluetooth uređaje kliknite **Postavke** (za ovo su potrebne administrativne ovlasti).

Postavke Bluetooth uređaja

Administratori mogu odrediti sljedeće postavke koje upravljaju ponašanjem i upotrebom vjerodajnica Bluetooth uređaja:

Tiha provjera

- **Automatski upotrijebi spojeni uneseni Bluetooth uređaj tijekom provjere identiteta**—Odaberite potvrdni okvir kako bi se korisnicima omogućila upotreba vjerodajnica za Bluetooth za provjeru, a da nije potrebno djelovanje korisnika ili očistite potvrdni okvir kako biste onemogućili tu opciju.

Blizina Bluetooth

- **Zaključajte računalo kada se uneseni Bluetooth uređaj pomakne izvan dosega vašeg računala**—Odaberite potvrdni okvir kako biste zaključali računalo kada se Bluetooth uređaj koji je spojen tijekom prijave pomakne izvan dosega ili očistite potvrdni okvir kako biste onemogućili tu opciju.

NAPOMENA: Bluetooth modul na računalu mora podržavati ovu mogućnost kako bi se iskoristila ova značajka.

Kartice

Aplikacija HP Client Security može podržati više različitih vrsta identifikacijskih kartica koje su male plastične kartice koje sadrže računalni čip. To uključuje male kartice, beskontaktne kartice i blizinske kartice. Ako su neka od tih kartica i odgovarajući čitač kartice spojen na računalo, ako administrator ima instaliran povezani upravljački program proizvođača i ako je administrator omogućio karticu kao vjerodajnice za provjeru, vi možete upotrijebiti karticu kao vjerodajnicu za provjeru.

Za pametne kartice proizvođač treba omogućiti alate za instaliranje sigurnosnog certifikata i upravljanje PIN-om kojeg aplikacija HP Client Security upotrebljava u svojem sigurnosnom algoritmu. Broj i vrsta znakova koji se upotrebljavaju kao PIN mogu se mijenjati. Administrator mora inicijalizirati pametnu karticu prije nego što se može upotrijebiti.

Sljedeće formate pametnih kartica podržava aplikacija HP Client Security:

- CSP
- PKCS11

Sljedeće vrste beskontaktnih kartica podržava aplikacija HP Client Security:

- Beskontaktne memorijske kartice HID iCLASS
- Beskontaktne MiFare Classic 1k, 4k i mini memorijske kartice

Sljedeće formate blizinskih kartica podržava aplikacija HP Client Security:

- Blizinske kartice HID

Za unos pametne kartice:

1. Umetnite karticu u priloženi čitač pametne kartice.
2. Kada se kartica prepozna unesite PIN kartice i zatim kliknite ili dodirnite **Unesi**.

Za promjenu PIN-a pametne kartice:

1. Umetnite karticu u priloženi čitač pametne kartice.
2. Kada se kartica prepozna unesite PIN kartice i zatim kliknite ili dodirnite **Provjeri autentičnost**.
3. Kliknite ili dodirnite **Promijeni PIN** i zatim unesite novi PIN.

Za unos beskontaktne ili blizinske kartice:

1. Postavite karticu na odgovarajući čitač ili vrlo blizu njega.
2. Kada se kartica prepozna kliknite ili dodirnite **Unesi**.

Za brisanje unesene kartice:

1. Pokažite karticu čitaču.
2. Samo za pametne kartice unesite dodijeljeni PIN kartice i zatim kliknite ili dodirnite **Provjeri autentičnost**.
3. Kliknite ili dodirnite **Izbriši**.

Kada je kartica unesena pojedinosti o kartici prikazuju se u okviru **Unesene kartice**. Kada se kartica izbriše ona se uklanja s popisa.

Za pristup postavkama blizinske, beskontaktne i pametne kartice gdje administratori mogu odrediti postavke koje se odnose na vjerodajnice kartica kliknite ili dodirnite **Postavke** (za ovo su potrebne administrativne ovlasti).

Postavke blizinske, beskontaktne i pametne kartice

Za pristup postavkama kartice kliknite ili dodirnite karticu na popisu i zatim kliknite ili dodirnite strelicu koja se prikazuje.

Za promjenu PIN-a pametne kartice:

1. Pokažite karticu čitaču
2. Unesite dodijeljeni PIN kartice i zatim kliknite ili dodirnite **Nastavi**.
3. Unesite i potvrdite novi PIN i zatim kliknite ili dodirnite **Nastavi**.

Za inicijalizaciju PIN-a pametne kartice:

1. Pokažite karticu čitaču
2. Unesite dodijeljeni PIN kartice i zatim kliknite ili dodirnite **Nastavi**.
3. Unesite i potvrdite novi PIN i zatim kliknite ili dodirnite **Nastavi**.
4. Kliknite ili dodirnite **Da** za potvrdu inicijalizacije.

Za brisanje podataka kartice:

1. Pokažite karticu čitaču
2. Unesite dodijeljeni PIN kartice (samo za pametne kartice, a zatim kliknite ili dodirnite **Nastavi**.
3. Kliknite ili dodirnite **Da** za potvrdu brisanja.

PIN

Ako je administrator omogućio PIN kao vjerodajnicu za provjeru možete postaviti PIN u vezi s drugim vjerodajnicama za dodatnu sigurnost.

Za postavljanje novog PIN-a:

▲ Unesite PIN, ponovno ga unesite kako biste ga potvrdili , a zatim kliknite ili dodirnite **Primijeni**.

Za brisanje PIN-a:

▲ Kliknite ili dodirnite **Izbriši**, a zatim kliknite ili dodirnite **Da** za potvrdu.

Za pristup postavkama PIN-a gdje administratori mogu odrediti postavke koje se odnose na vjerodajnice PIN-a kliknite ili dodirnite **Postavke** (za ovo su potrebne administrativne ovlasti).

PIN postavke

Na stranici postavki za PIN možete odrediti najmanju i najveću prihvatljivu dužinu PIN vjerodajnice.

RSA SecurID

Ako je administrator omogućio RSA kao vjerodajnicu za provjeru i ako su sljedeći uvjeti točni možete unijeti ili izbrisati vjerodajnicu RSA SecurID.

NAPOMENA: Potrebne je odgovarajuća instalacija.

- Korisnik je morao biti stvoren na RSA poslužitelju.
- RSA SecurID token koji je dodijeljen korisniku i računalu morao se pridružiti domeni RSA poslužitelja.
- Softver SecurID instaliran je na računalo.
- Spajanje je omogućeno za pravilno konfiguriran RSA poslužitelj.

Za unos RSA SecurID vjerodajnica:

▲ Unesite svoje RSA SecurID korisničko ime i pristupni kod (RSA SecurID Token kod ili PIN +Token kod ovisno o vašem okruženju), a zatim kliknite ili dodirnite **Primijeni**.

Nakon uspješnog unosa prikazuje se poruka “Vaša RSA SecurID vjerodajnica uspješno je unesena” i omogućen je gumb Izbriši.

Za brisanje RSA SecurID vjerodajnica:

▲ Kliknite **Izbriši** i zatim odaberite **Da** u skočnom dijaloškom okviru koji postavlja pitanje “Jeste li sigurni da želite izbrisati svoju RSA SecurID vjerodajnicu?”

Password Manager

Prijavljivanje na web-mjesta i aplikacije jednostavnije je i sigurnije kada upotrebljavate Password Manager. Možete stvarati snažnije lozinke koje ne morate zapisivati ili pamtiti, a zatim se lako i brzo prijaviti pomoću otiska prsta, pametne, blizinske ili beskontaktne kartice, Bluetooth telefona, PIN-a, RSA vjerodajnice ili lozinke za sustav Windows.

NAPOMENA: Zbog zaslona za prijavu na web s neprestano promjenjivom strukturom, Password Manager možda neće moći uvijek podržavati sva web-mjesta.

Password Manager pruža sljedeće opcije:

Stranica Password Manager

- Kliknite ili dodirnite račun za automatsko pokretanje web-stranice ili aplikacije i prijavu.
- Za organiziranje računa upotrebljavajte kategorije.

Jačina lozinke

- U tren oka pogledajte je li neka od vaših lozinki u opasnosti.
- Prilikom dodavanja podataka za prijavu provjerite jačinu pojedinih lozinki koje upotrebljavajte za web-mjesta i aplikacije.
- Jačinu lozinke prikazuju crveni, žuti ili zeleni indikatori stanja.

Ikona **Password Manager** prikazuje se u gornjem lijevom kutu zaslon za prijavu web-stranice ili aplikacije. Kada prijava još nije stvorena za web-mjesto ili aplikaciju na ikoni se prikazuje znak plus.

▲ Kliknite ili dodirnite ikonu **Password Manager** za prikaz kontekstnog izbornika gdje možete birati između sljedećih opcija:

- Dodajte [somedomain.com] u Password Manager
- Otvorite Password Manager
- Postavke ikone
- Pomoć

Za web-stranice ili programe gdje prijava još nije stvorena

Sljedeće se opcije prikazuju u kontekstnom izborniku:

- **Dodaj [somedomain.com] u Password Manager**—Omogućuje vam dodavanje prijave u trenutačni zaslon za prijavu.
- **Otvori Password Manager**—Pokreće Password Manager.

- **Postavke ikone**—Omogućuje vam određivanje uvjeta u kojima se prikazuje ikona **Password Manager**.
- **Pomoć**—Prikazuje Pomoć aplikacije HP Client Security.

Za web-stranice ili programe gdje je prijava već stvorena

Sljedeće se opcije prikazuju u kontekstnom izborniku:

- **Upiši podatke za prijavu**—Prikazuje stranicu **Provjeri svoj identitet**. Ako se uspješno provjeri autentičnost vaši se podaci za prijavu postavljaju u polja za prijavu i tada se stranica šalje (ako je slanje navedeno kada je prijava stvorena ili posljednji put uređena).
- **Uredi prijavu**—Omogućuje vam uređivanje podataka za prijavu za to web-mjesto.
- **Dodaj prijavu**—Omogućuje vam dodavanje računa u Password Manager.
- **Otvori Password Manager**—Pokreće Password Manager.
- **Pomoć**—Prikazuje Pomoć aplikacije HP Client Security.

NAPOMENA: Administrator ovog računala možda je konfigurirao aplikaciju HP Client Security tako da traži više od jedne vjerodajnice prilikom provjere vašeg identiteta.

Dodavanje prijava

Jednostavno možete dodati prijavu za web-mjesto ili program tako da jednom unesete informacije za prijavu. Od tog trenutka pa na dalje Password Manager automatski unosi informacije za vas. Te prijave možete upotrijebiti nakon pretraživanja web-mjesta ili programa.

Za dodavanje prijave:

1. Otvorite zaslon za prijavu web-mjesta ili programa.
2. Kliknite ili dodirnite ikonu **Password Manager** i zatim kliknite ili dodirnite jedno od sljedećeg ovisno o tome je li zaslon za prijavu za web-mjesto ili program:
   - Za web-mjesto, kliknite ili dodirnite **Dodaj [naziv domene] u Password Manager**.
   - Za program, kliknite ili dodirnite **Dodaj ovaj zaslon za prijavu u Password Manager**.
3. Unesite podatke za prijavu. Polja za prijavu na zaslonu i odgovarajuća polja u dijaloškom okviru prepoznaju se prema deblje označenom narančastom okviru.
   a. Za popunjavanje polja za prijavu jednim od unaprijed oblikovanih odabira kliknite ili dodirnite strelice desno od polja.
   b. Za prikaz lozinke za ovu prijavu kliknite ili dodirnite **Prikaži lozinku**.
   c. Za dobivanje popunjenih polja prijave, ali ne i poslanih, očistite potvrdni okvir **Automatsko upisivanje podataka za prijavu**.
   d. Kliknite ili dodirnite **U redu** za odabir načina za provjeru autentičnosti koji želite upotrijebiti (otisak prsta, pametna kartica, blizinska kartica, beskontaktna kartica, Bluetooth telefon, PIN ili lozinka) i prijavite se koristeći odabrani način provjere.

      Znak plus uklanja se iz ikone **Password Manager** kako bi označio da je prijava stvorena.
   e. Ako Password Manager ne otkrije polja za prijavu kliknite ili dodirnite **Više polja**.
      - Potvrdite okvir za svako polje koje je potrebno za prijavu, odnosno poništite potvrdni okvir za ona koja nisu potrebna.
      - Kliknite ili dodirnite **Zatvori**.

Svaki put kada pristupite tom web-mjestu ili otvorite program ikona **Password Manager** prikazuje se u gornjem lijevom kutu zaslona za prijavu web-mjesta ili aplikacije označavajući da možete upotrijebiti registrirane vjerodajnice za prijavu.

Uređivanje prijava

Za uređivanje prijave:

1. Otvorite zaslon za prijavu web-mjesta ili programa.
2. Za prikaz dijaloškog okvira u kojem možete urediti svoje podatke za prijavu kliknite ili dodirnite ikonu **Password Manager** i zatim kliknite ili dodirnite **Uredi prijavu**.

   Polja za prijavu na zaslonu i odgovarajuća polja u dijaloškom okviru prepoznaju se prema deblje označenom narančastom okviru.

   Svoje podatke o računu možete urediti i sa stranice Password Manager tako da kliknite ili dodirnete prijavu za prikaz opcija za uređivanje i zatim odaberete **Uredi**.
3. Uredi svoje podatke za prijavu.
   - Za uređivanje **Naziva računa** unesite novi naziv u polje.
   - Za dodavanje ili uređivanje naziva **Kategorije** uredite ili izmijenite naziv u polju **Kategorija**.
   - Za odabir polja za prijavu **Korisničko ime** jednim od unaprijed oblikovanih odabira kliknite ili dodirnite strelice desno od polja.

     Unaprijed oblikovani odabiri dostupni su samo kada uređujete prijavu iz naredbe Uredi u ikoni kontekstnog izbornika Password Manager.
   - Za odabir polja za prijavu **Lozinka** jednim od unaprijed oblikovanih odabira kliknite ili dodirnite strelice desno od polja.

     Unaprijed oblikovani odabiri dostupni su samo kada uređujete prijavu iz naredbe Uredi u ikoni kontekstnog izbornika Password Manager.
   - Za dodavanje dodatnih polja sa zaslona svoje prijave kliknite ili dodirnite **Više polja**.
   - Za prikaz lozinke za ovu prijavu kliknite ili dodirnite **Prikaži lozinku**.
   - Za dobivanje popunjenih polja prijave, ali ne i poslanih, očistite potvrdni okvir **Automatsko upisivanje podataka za prijavu**.
   - Za označavanje ove prijave kao da imate ugroženu lozinku odaberite potvrdni okvir **Ova lozinka je ugrožena**.

     Nakon spremanja promjena sve ostale prijave koje dijele istu lozinku također će se označiti kao ugrožene. Tada ćete moći posjetit sve pogođene račune i po potrebi promijeniti lozinku.
4. Kliknite ili dodirnite **U redu**.

Upotreba izbornika brze veze za Password Manager

Password Manager daje brz i jednostavan način za pokretanje web-mjesta i programa za koje ste stvorili prijave. Dva puta kliknite ili dva puta dodirnite prijavu za program ili web-mjesto iz izbornika **Brze veze Password Manager** ili sa stranice Password Manager u aplikaciji HP Client Security za otvaranje zaslona za prijavu i zatim unesite svoje podatke za prijavu.

Kada stvorite prijavu ona se automatski dodaje u vaš izbornik **Brze veze** za Password Manager.

Za prikaz izbornika **Brze veze**:

▲ Pritisnite kombinaciju tipkovničkog prečaca za **Password Manager** (Ctrl+tipka Windows+h predstavljaju tvorničku postavku). Za promjenu kombinacije tipkovničkog prečaca s početne stranice HP Client Security kliknite **Password Manager**, a zatim kliknite ili dodirnite **Postavke**.

Organiziranje prijava u kategorije

Stvorite jednu ili više kategorija kako biste držali svoje prijave urednima.

Za dodjeljivanje prijave u kategoriju:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite **Password Manager**.
2. Kliknite ili dodirnite unos računa, a zatim kliknite ili dodirnite **Uredi**.
3. U polju **Kategorija** unesite naziv kategorije.
4. Kliknite ili dodirnite **Spremi**.

Za uklanjanje računa iz kategorije:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite **Password Manager**.
2. Kliknite ili dodirnite unos računa, a zatim kliknite ili dodirnite **Uredi**.
3. U polju **Kategorija** izbrišite naziv kategorije.
4. Kliknite ili dodirnite **Spremi**.

Za preimenovanje kategorije:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite **Password Manager**.
2. Kliknite ili dodirnite unos računa, a zatim kliknite ili dodirnite **Uredi**.
3. U polju **Kategorija** promijenite naziv kategorije.
4. Kliknite ili dodirnite **Spremi**.

Upravljanje prijavama

Password Manager olakšava upravljanje podacima za prijavu za korisnička imena. lozinke i višestruke račune za prijavu sa jednog središnjeg mjesta.

Vaše su prijave popisane na stranici Password Manager.

Za upravljanje prijavama:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite **Password Manager**.
2. Kliknite ili dodirnite postojeću prijavu i zatim odaberite jednu od sljedećih opcija i pratite upute na zaslonu:
   - **Uredi**—Uredite prijavu. Dodatne informacije potražite u odjeljku Uređivanje prijava na stranici 20.
   - **Prijavi**—Prijavite se na odabrani račun.
   - **Izbriši**—Izbrišite prijavu za odabrani račun.

Za dodavanje dodatne prijave za web-mjesto ili program:

1. Otvorite zaslon za prijavu web-mjesta ili programa.
2. Kliknite ili dodirnite ikonu **Password Manager** za prikaz njegovog kontekstualnog izbornika.
3. Kliknite ili dodirnite **Dodaj prijavu** i zatim slijedite upute na zaslonu.

Odredite jačinu lozinke

Upotreba jakih lozinki za prijavu na svoja web-mjesta ili programe važna je aspekt zaštite identiteta.

Password Manager olakšava nadzor i poboljšavanje sigurnosti uz trenutačnu i automatsku analizu jačine svake od lozinki koja se upotrebljava za prijavu na web-mjesta i programe.

Dok unosite lozinku tijekom stvaranje Password Manager prijave za jedan od računa ispod lozinke se prikazuje traka u boji koja označava jačinu lozinke. Boje označavaju sljedeće vrijednosti:

- **Crvena**—Slabo
- **Žuta**—Dobro
- **Zelena**—Jako

Postavke ikone Password Manager

Password Manager pokušava prepoznati zaslone za prijavu za web-mjesta i programe. Kada otkrije zaslon za prijavu za koje niste stvorili prijavu, Password Manager od vas traži da dodate prijavu za zaslon tako da prikazuje ikonu **Password Manager** sa znakom plus.

1. Kliknite ili dodirnite ikonu, a zatim kliknite ili dodirnite **Postavke ikone** kako biste prilagodili način na koji Password Manager rukuje mogućim mjestima za prijavu.
   - **Upitaj za dodavanje prijava za zaslon za prijavu**—Kliknite ili dodirnite ovu opciju kako bi Password Manager od vas zatražio da dodate prijavu kada se prikazuje zaslon za prijavu koji još nema postavljenu prijavu.
   - **Izostavi ovaj zaslon**—Odaberite potvrdni okvir tako da Password Manager od vas ponovno ne traži dodavanje prijave za ovaj zaslon za prijavu.
   - **Ne traži dodavanje prijava za zaslone za prijavu**—Odaberite gumb radio.
2. Za dodavanje prijave za zaslon koji je ranije bio izostavljen:
   a. Prijavite se na ranije isključeno web-mjesto.
   b. Kako bi Password Manager upamtio lozinku za ovo mjesto kliknite ili dodirnite **Zapamti** u skočnom dijaloškom okviru kako biste spremili lozinku i stvorili prijavu za zaslon.
3. Za pristupanje dodatnim postavkama za Password Manager kliknite ili dodirnite ikonu Password Manager, kliknite ili dodirnite **Otvori Password Manager** i zatim kliknite ili dodirnite **Postavke** na stranici Password Manager.

Uvoz i izvoz prijava

Na stranici uvoza i izvoza za HP Password Manager možete uvesti prijave koje su spremili web-preglednici na vašem računalu. Također možete i uvesti podatke iz datoteke sigurnosne kopije aplikacije HP Client Security i uvesti podatke u datoteku sigurnosne kopije aplikacije HP Client Security.

▲ Za pokretanje stranice Uvoz i izvoz kliknite ili dodirnite **Uvoz i izvoz** na stranici Password Manager.

Za uvoz lozinki iz preglednika:

1. Kliknite ili dodirnite preglednik iz kojeg želite uvesti lozinke (prikazuju se samo instalirani preglednici).
2. Očistite potvrdni okvir svih računa za koje ne želite uvesti lozinke.
3. Kliknite ili dodirnite **Uvezi**.

Uvoz podataka s datoteke sigurnosne kopije aplikacije HP Client Security ili izvoz podataka u nju može se obaviti preko pripadajućih veza (u kartici **Ostale opcije)** na stranici Uvoz i izvoz.

NAPOMENA: Ova značajka uvozi i izvozi samo podatke za Password Manager. Više podataka o stvaranju sigurnosne kopije i obnavljanju dodatnih podataka za aplikaciju HP Client Security potražite u Sigurnosno kopiranje i vraćanje podataka na stranici 27.

Za uvoz podataka iz datoteke sigurnosne kopije aplikacije HP Client Security:

1. Sa stranice uvoz i izvoz značajke HP Password Manager kliknite ili dodirnite **Uvezi podatke iz datoteke sigurnosne kopije aplikacije HP Client Security**.
2. Provjerite svoj identitet.
3. Odaberite ranije stvorenu datoteku sigurnosne kopije ili unesite putanju u navedeno polje i zatim kliknite ili dodirnite **Pregledaj**.
4. Unesite lozinku koja se upotrebljava za zaštitu datoteke, a zatim kliknite ili dodirnite **Sljedeći**.
5. Kliknite ili dodirnite **Vrati**.

Za izvoz podataka iz datoteke sigurnosne kopije aplikacije HP Client Security:

1. Sa stranice uvoz i izvoz značajke HP Password Manager kliknite ili dodirnite **Izvezi podatke iz datoteke sigurnosne kopije aplikacije HP Client Security**.
2. Provjerite svoj identitet, a zatim kliknite ili dodirnite **Sljedeće**.
3. Unesite naziv za datoteku sigurnosne kopije. Po zadanim postavkama datoteka se sprema u mapu Dokumenti. Za određivanje druge lokacije kliknite ili dodirnite **Pregledaj**.
4. Unesite i potvrdite lozinku koja se upotrebljava za zaštitu datoteke, a zatim kliknite ili dodirnite **Spremi**.

Postavke

Možete odrediti postavke za personalizaciju značajke Password Manager:

- **Upitaj za dodavanje prijava za zaslon za prijavu**—Ikona **Password Manager** sa znakom plus prikazuje se svaki put kada se otkrije zaslon za prijavu za web-mjesto ili program navodeći da možete dodati prijavu za ovaj zaslon u izborniku **Prijave**.

  Za onemogućavanje ove značajke očistite potvrdni okvir pored **Upitaj za dodavanje prijava za zaslon za prijavu**.

- **Otvori Password Manager pomoću Ctrl+Win+h**—Zadani tipkovnički prečac koji otvara izbornik **Brze veze za Password Manager** je Ctrl+tipka Windows+h.

  Za promjenu tipkovničkog prečaca kliknite ili dodirnite ovu opciju i zatim unesite novu kombinaciju tipki. Kombinacija može uključivati jednu ili više sljedećih mogućnosti: ctrl, alt ili shift i bilo koja tipka slova ili brojke.

  Kombinacije koje su rezervirane za sustav Windows ili aplikacije sustava Windows ne mogu se upotrebljavati.

- Za povratak na postavke tvornički zadanih vrijednosti kliknite ili dodirnite **Vrati zadano**.

Napredne postavke

Administratori mogu pristupiti sljedećom opcijama tako da odaberu ikonu **Zupčanik** (postavke) na početnom zaslonu aplikacije HP Client Security.

- **Pravila administratora**—Omogućuju vam konfiguriranje pravila za prijavu i sesiju za administratore.
- **Pravila standardnog korisnika**—Omogućuju vam konfiguriranje pravila za prijavu i sesiju za standardne korisnike.
- **Sigurnosne značajke**—Omogućuju vam povećanje sigurnosti računala tako da zaštitite svoj račun sustava Windows jakim provjerama autentičnosti i/ili omogućavanjem provjere autentičnosti prije pokretanja sustava Windows.
- **Korisnici**—Omogućuje vam upravljanje korisnicima i njihovim vjerodajnicama.
- **Moja pravila**—Omogućuje vam pregled vaših pravila provjere autentičnosti i statusa unosa.
- **Sigurnosno kopiranje i vraćanje**—Omogućuje vam sigurnosno kopiranje i vraćanje podataka aplikacije HP Client Security.
- **O aplikaciji HP Client Security**—Prikazuje informacije o inačici aplikacije HP Client Security.

Pravila administratora

Možete konfigurirati pravila prijave i sesije za administratore ovog računala. Ovdje postavljena pravila prijave upravljaju vjerodajnicama potrebnima za lokalne administratore za prijavu u sustav Windows. Ovdje postavljena pravila sesije upravljaju vjerodajnicama potrebnima za lokalne administratore za provjeru identiteta tijekom sesije u sustavu Windows.

Po zadanim postavkama sva nova ili izmijenjena pravila postaju važeća odmah nakon što kliknete ili dodirnete **Primijeni**.

Za dodavanje novog pravila:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite ikonu **Zupčanik**.
2. Na stranici Napredne postavke kliknite ili dodirnite **Pravila administratora**.
3. Kliknite ili dodirnite **Dodaj novo pravilo**.
4. Kliknite strelicu prema dolje kako biste odabrali primarnu i (opcionalno) sekundarnu vjerodajnicu za nova pravila i zatim kliknite ili dodirnite **Dodaj**.
5. Kliknite **Apply** (Primijeni).

Za odgađanje nametanja novih ili izmijenjenih pravila:

1. Kliknite ili dodirnite **Odmah nametni ova pravila**.
2. Odaberite **Ova pravila nametni od određenog datuma**.
3. Unesite datum ili upotrijebite skočni kalendar kako biste odabrali datum od kojeg ova pravila vrijede.
4. Po želji odaberite kada želite podsjetiti korisnik na nova pravila.
5. Kliknite **Apply** (Primijeni).

Pravila standardnog korisnika

Možete konfigurirati pravila prijave i sesije za standardne korisnike ovog računala. Ovdje postavljena pravila prijave upravljaju vjerodajnicama potrebnima za standardne korisnike za prijavu u sustav Windows. Ovdje postavljena pravila sesije upravljaju vjerodajnicama potrebnima za standardne korisnike za provjeru identiteta tijekom sesije u sustavu Windows.

Po zadanim postavkama sva nova ili izmijenjena pravila postaju važeća odmah nakon što kliknete ili dodirnete **Primijeni**.

Za dodavanje novog pravila:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite ikonu **Zupčanik**.
2. Na stranici Napredne postavke kliknite ili dodirnite **Pravila standardnog korisnika**.
3. Kliknite ili dodirnite **Dodaj novo pravilo**.
4. Kliknite strelicu prema dolje kako biste odabrali primarnu i (opcionalno) sekundarnu vjerodajnicu za nova pravila i zatim kliknite ili dodirnite **Dodaj**.
5. Kliknite **Apply** (Primijeni).

Za odgađanje nametanja novih ili izmijenjenih pravila:

1. Kliknite ili dodirnite **Odmah nametni ova pravila**.
2. Odaberite **Ova pravila nametni od određenog datuma**.
3. Unesite datum ili upotrijebite skočni kalendar kako biste odabrali datum od kojeg ova pravila vrijede.
4. Po želji odaberite kada želite podsjetiti korisnik na nova pravila.
5. Kliknite **Apply** (Primijeni).

Značajke sigurnosti

Možete omogućiti Značajke sigurnosti HP klijenta koje pomažu u zaštiti od neovlaštenog pristupa računalu.

Za postavljanje značajke sigurnosti:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite ikonu **Zupčanik**.
2. Na stranici Napredne postavke kliknite ili dodirnite **Značajke sigurnosti**.
3. Omogućite značajke sigurnosti tako da odaberete potvrdne okvire i tada kliknite ili dodirnite **Primijeni**. Što više značajki odaberete to je vaše računalo sigurnije.

   Ove se postavke primjenjuju na sve korisnike.

   - **Sigurnost prijave u sustav Windows**—Štiti vaše račune za sustav Windows tražeći upotrebu vjerodajnica aplikacije HP Client Security za pristup.
   - **Zaštita prije pokretanje sustava (Provjera autentičnosti kod uključenja)**—Štiti vaše računalo prije pokretanja sustava Windows. Ovaj odabir nije dostupan ako ga BIOS ne podržava.
   - **Omogući Prijavu u jednom koraku**—ova postavka omogućuje preskakanje prijave u sustav Windows ako je provjera autentičnosti već obavljena na razini Provjera autentičnosti kod uključenja ili Drive Encryption.
4. Kliknite ili dodirnite **Korisnici**, a zatim kliknite ili dodirnite pločicu korisnika.

Korisnici

Možete nadzirati i upravljati korisnicima aplikacije HP Client Security ovog računala.

Za dodavanje drugog korisnika sustava Windows aplikaciji HP Client Security:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite ikonu **Zupčanik**.
2. Na stranici Napredne postavke kliknite ili dodirnite **Korisnici**.
3. Kliknite ili dodirnite **Dodaj drugog korisnika sustava Windows aplikaciji HP Client Security**.
4. Unesite ime korisnika kojeg želite dodati i zatim kliknite ili dodirnite **U redu**.
5. Unesite korisnikovu lozinku za sustav Windows.

   Pločica dodanog korisnika prikazuje se na stranici Korisnik.

Za brisanje korisnika sustava Windows aplikaciji HP Client Security:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite ikonu **Zupčanik**.
2. Na stranici Napredne postavke kliknite ili dodirnite **Korisnici**.
3. Kliknite ili dodirnite ime korisnika kojeg želite izbrisati.
4. Kliknite ili dodirnite **Izbriši korisnika**, a zatim kliknite ili dodirnite **Da** za potvrdu.

Za prikaz sažetka pravila prijave i sesija koja vrijede za korisnika:

▲ Kliknite ili dodirnite **Korisnici**, a zatim kliknite ili dodirnite pločicu korisnika.

Moja pravila

Možete prikazati svoja pravila za provjeru autentičnosti i status unosa. Stranica Moja pravila daje i veze za stranice Pravila administratora i Pravila standardnog korisnika.

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite ikonu **Zupčanik**.
2. Na stranici Napredne postavke kliknite ili dodirnite **Moja pravila**.

   Prikazuju se pravila prijave i sesije koja vrijede za trenutačno prijavljene korisnike.

Stranica Moja pravila daje i veze za Pravila administratora na stranici 24i Pravila standardnog korisnika na stranici 25.

Sigurnosno kopiranje i vraćanje podataka

Preporučuje se da redovito sigurnosno kopirate podatke aplikacije HP Client Security. Učestalost sigurnosnog kopiranja ovisi o učestalosti promjene podataka. Na primjer, ako svakodnevno dodajete nove prijave, svakodnevno biste trebali sigurnosno kopirati svoje podatke.

Sigurnosne kopije mogu se upotrebljavati i za migriranje s jednog računala na drugo koje se još naziva i uvozom i izvozom.

NAPOMENA: Ova značajka sigurnosno kopira samo Password Manager. Drive Encryption ima neovisan način sigurnosnog kopiranja. Za podatke Device Access Manager i provjeru autentičnosti otiskom prsta ne izrađuje se sigurnosna kopija.

HP Client Security mora se instalirati na svako računalo koje će primiti sigurnosnu kopiju podataka prije nego što se ti podaci mogu vratiti iz datoteke sigurnosne kopije.

Za stvaranje sigurnosne kopije vaših podataka:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite ikonu **Zupčanik**.
2. Na stranici Napredne postavke kliknite ili dodirnite **Pravila administratora**.
3. Kliknite ili dodirnite **Sigurnosno kopiraj i vrati**.
4. Kliknite ili dodirnite **Sigurnosno kopiraj** i zatim provjerite svoj identitet.
5. Odaberite modul koji želite uključiti u sigurnosnu kopiju i zatim kliknite ili dodirnite **Sljedeće**.
6. Unesite naziv za datoteke za pohranu. Po zadanim postavkama datoteka se sprema u mapu Dokumenti. Za određivanje druge lokacije kliknite ili dodirnite **Pregledaj**.
7. Unesite i potvrdite lozinku za zaštitu datoteke.
8. Kliknite ili dodirnite **Spremi**.

Za vraćanje podataka:

1. S početne stranice aplikacije HP Client Security kliknite ili dodirnite ikonu **Zupčanik**.
2. Na stranici Napredne postavke kliknite ili dodirnite **Pravila administratora**.
3. Kliknite ili dodirnite **Sigurnosno kopiraj i vrati**.
4. Odaberite **Vrati** i zatim provjerite svoj identitet.
5. Odaberite prethodno stvorenu datoteku za pohranu. Unesite putanju u navedeno polje. Za određivanje druge lokacije kliknite ili dodirnite **Pregledaj**.
6. Unesite lozinku koja se upotrebljava za zaštitu datoteke, a zatim kliknite ili dodirnite **Sljedeći**.

7. Odaberite module za koje želite vratiti podatke.
8. Kliknite ili dodirnite **Vrati**.

5 HP Drive Encryption (samo odabrani modeli)

Softver HP Drive Encryption pruža zaštitu svih podataka šifriranjem podataka vašeg računala. Kada se uključi softver Drive Encryption morate se prijaviti na zaslon za prijavu koji se prikazuje prije nego što se pokrene operacijski sustav Windows®.

Početni zaslon HP sigurnosnog klijenta omogućuje administratorima sustava Windows uključivanje softvera Drive Encryption, sigurnosno kopiranje ključa za šifriranje i odabir ili poništavanje odabira jednog ili više pogona ili particije koje treba šifrirati. Više informacija potražite u Pomoći za softver HP sigurnosnog klijenta.

Sljedeći se zadaci mogu obaviti pomoću softvera Drive Encryption:

- Odabir postavki softvera Drive Encryption:
  - šifriranje ili dešifriranje pojedinačnih pogona ili particija pomoću softvera za šifriranje
  - šifriranje ili dešifriranje pojedinačnih samošifrirajućih pogona pomoću hardvera za šifriranje
  - dodavanje dodatne sigurnosni onemogućavanjem stanja mirovanja ili čekanja kako bi se osiguralo da se uvijek traži provjera autentičnosti prije pokretanja softvera Drive Encryption

NAPOMENA: samo se interni SATA i vanjski eSATA tvrdi diskovi mogu šifrirati.

- Stvaranje ključeva sigurnosne kopije
- Oporavak pristupa šifriranom računalu pomoću ključeva sigurnosne kopije i uslužnog programa HP SpareKey
- Omogućavanje provjere autentičnosti prije pokretanja softvera Drive Encryption pomoću lozinke, registriranog otiska prsta ili PIN-a za odabir pametne kartice

Otvaranje softvera Drive Encryption

Administratori mogu pristupiti softveru Drive Encryption tako da otvore HP sigurnosnog klijenta:

1. Na početnom zaslonu kliknite ili dodirnite aplikaciju **HP Client Security** (Windows 8).

   – ili –

   Na radnoj površini sustava Windows dva puta kliknite ikonu **HP Client Security** u području obavijesti na krajnjem desnom dijelu programske trake.

2. Kliknite ili dodirnite ikonu **Drive Encryption**.

Opći zadaci

Aktiviranje softvera Drive Encryption za standardne tvrde diskove

Standardni tvrdi diskovi šifriraju se pomoću softvera za šifriranje. Pratite ove korake za šifriranje pogona ili particije diska:

1. Pokrenite **Drive Encryption**. Dodatne informacije potražite u odjeljku Otvaranje softvera Drive Encryption na stranici 29.
2. Odaberite potvrdni okvir pogona ili particiju koju želite šifrirati i zatim kliknite ili dodirnite **Ključ sigurnosne kopije**.

NAPOMENA: Za još više sigurnosti odaberite potvrdni okvir **Onemogući stanje mirovanja za veću sigurnost**. Kada onemogućite stanje mirovanja više uopće ne postoji opasnost da će se vjerodajnice upotrijebljene za otključavanje pogona pohraniti u memoriji.

3. Odaberite jednu ili više opcija sigurnosnog kopiranja i zatim kliknite ili dodirnite **Izradi sigurnosnu kopiju**. Dodatne informacije potražite u odjeljku Sigurnosno kopiranje ključeva za šifriranje na stranici 33.
4. Možete nastaviti s radom dok se ključ za šifriranje sigurnosno kopira. Računalo ne pokrećite ponovno.

NAPOMENA: Od vas se traži da ponovno pokrenete računalo. Nakon ponovnog pokretanja prikazuje se zaslon prije pokretanja šifriranja pogona u kojem se traži potvrda autentičnosti prije nego što se pokrene sustav Windows.

Aktiviran je softver Drive Encryption. Šifriranje jedne ili više odabranih particija pogona može potrajati nekoliko sati ovisno o broju i veličini particije(a).

Više informacija potražite u Pomoći za softver HP sigurnosnog klijenta.

Aktiviranje softvera Drive Encryption za samošifrirajuće pogone

Samošifrirajući pogoni koji ispunjavaju specifikacije OPAL organizacije Trusted Computing Group mogu se šifrirati šifriranjem softvera ili šifriranjem hardvera. Šifriranje hardvera je puno brže od šifriranja softvera. Međutim, ne možete odabrati koja će se particija diska šifrirati. Šifrira se cijeli disk uključujući i sve particije diska.

Za šifriranje određenih particija morate upotrijebiti šifriranje softvera. Obavezno očistite potvrdni okvir **Dopusti samo šifriranje hardvera za samošifrirajuće pogone(SEDs)**.

Slijedite ove korake za pokretanje softvera Drive Encryption za samošifrirajuće pogone:

1. Pokrenite **Drive Encryption**. Dodatne informacije potražite u odjeljku Otvaranje softvera Drive Encryption na stranici 29.
2. Odaberite potvrdni okvir pogona kojeg želite šifrirati i zatim kliknite ili dodirnite **Ključ sigurnosne kopije**.

NAPOMENA: Za još više sigurnosti odaberite potvrdni okvir **Onemogući stanje mirovanja za veću sigurnost**. Kada onemogućite stanje mirovanja više uopće ne postoji opasnost da će se vjerodajnice upotrijebljene za otključavanje pogona pohraniti u memoriji.

3. Odaberite jednu ili više opcija sigurnosnog kopiranja i zatim kliknite ili dodirnite **Izradi sigurnosnu kopiju**. Dodatne informacije potražite u odjeljku Sigurnosno kopiranje ključeva za šifriranje na stranici 33.

4. Možete nastaviti s radom dok se ključ za šifriranje sigurnosno kopira. Računalo ne pokrećite ponovno.

NAPOMENA: Za samošifrirajuće pogone od vas će se zatražiti da isključite računalo.

Više informacija potražite u Pomoći za softver HP sigurnosnog klijenta.

Isključivanje softvera Drive Encryption

1. Pokrenite **Drive Encryption**. Dodatne informacije potražite u odjeljku Otvaranje softvera Drive Encryption na stranici 29.

2. Očistite potvrdni okvir svih šifriranih pogona pa zatim kliknite ili dodirnite **Primijeni**.

   Isključivanje softvera Drive Encryption započinje.

NAPOMENA: Ako se upotrebljavalo šifriranje softvera započinje dešifriranje. Ovo može potrajati nekoliko sati ovisno o veličini šifrirane(ih) particije(a) tvrdog diska. Kada se dešifriranje dovrši, isključuje se softver Drive Encryption.

Ako se upotrebljavalo šifriranje hardvera, pogon se trenutačno dešifrira i za nekoliko minuta isključuje se softver Drive Encryption.

Kada se isključi softver Drive Encryption od vas će se zatražiti da isključite računalo ako se radilo o šifriranju hardvera ili da ponovno pokrenete računalo ako se radilo o šifriranju softvera.

Prijavljivanje nakon pokretanja softvera Drive Encryption

Kada uključite računalo nakon pokretanja softvera Drive Encryption i kada je unesen vaš korisnički račun, morate se prijaviti na zaslonu za prijavu softvera Drive Encryption:

NAPOMENA: Kada se izlazi iz stanja mirovanja ili čekanja za šifriranje softvera ili šifriranje hardvera ne prikazuje se provjera autentičnosti prije pokretanja softvera Drive Encryption. Šifriranje hardvera omogućuje opciju **Onemogući stanje mirovanja za veću sigurnost** koja sprječava uključivanje stanja mirovanja ili čekanja kada su omogućeni.

Kada se izlazi iz stanja hibernacije za šifriranje softvera ili hardvera prikazuje se provjera autentičnosti prije pokretanja softvera Drive Encryption.

NAPOMENA: Ako je administrator sustava Windows omogućio BIOS zaštitu prije pokretanja sustava u aplikaciji HP sigurnosnog klijenta i ako je omogućen One-Step Logon (po zadanim postavkama) možete se prijaviti na računalo odmah nakon provjere autentičnosti u BIOS zaštiti prije pokretanja, a da nije potrebna ponovno provjera autentičnosti na zaslonu za prijavu softvera Drive Encryption.

Prijava jednog korisnika:

- Na stranici **Prijava** unesite lozinku sustava Windows, PIN pametne kartice, SpareKey ili prijeđite registriranim prstom.

Prijava više korisnika:

1. Na stranici **Odaberi korisnika za prijavu** odaberite s padajućeg popisa korisnika kojeg treba prijaviti, a zatim kliknite ili dodirnite **Sljedeće**.
2. Na stranici **Prijava** unesite lozinku sustava Windows, PIN pametne kartice ili prijeđite registriranim prstom.

NAPOMENA: Podržavaju se sljedeće pametne kartice:

Podržane pametne kartice

- Gemalto Cyberflex Access 64k V2c

NAPOMENA: Ako se ključ za oporavak upotrebljava za prijavu na zaslonu za prijavu softvera Drive Encryption, potrebne su dodatne vjerodajnice prilikom prijave u sustavu Windows za pristup korisničkim računima.

Šifriranje dodatnih tvrdih pogona

Preporučujemo vam da upotrebljavate softver HP Drive Encryption za zaštitu vaših podataka prilikom šifriranja vašeg tvrdog pogona. Nakon uključivanja svi stvoreni dodani tvrdi pogoni ili particije mogu se šifrirati tako da se prate ovi koraci:

1. Pokrenite **Drive Encryption**. Dodatne informacije potražite u odjeljku Otvaranje softvera Drive Encryption na stranici 29.
2. Za pogone sa šifriranim softverom odaberite particije pogona koje treba šifrirati.

NAPOMENA: Ovo se primjenjuje i na scenarij s mješovitim pogonom u kojem se nalaze jedan ili više standardnih tvrdih diskova i jedan ili više samošifrirajućih pogona

– ili –

▲ Za pogone sa šifriranim hardverom odaberite dodatnu(e) particiju(e) pogona koje treba šifrirati.

Napredni zadaci

Upravljanje softverom Data Encryption (zadatak administratora)

Administratori mogu upotrebljavati softver Data Encryption za prikaz i promjenu statusa (Nešifrirano ili Šifrirano) svih tvrdih pogona na računalu.

- Ako je status Omogućen, softver Drive Encryption je uključen i konfiguriran. Pogon je u jednom od sljedećih stanja:

Šifriranje softvera

- Nije šifrirano
- Šifrirano
- Šifriranje
- Dešifriranje

Šifriranje hardvera

- Šifrirano
- Nije šifrirano (za dodatne pogone)

Šifriranje ili dešifriranje pojedinačnih particija pogona (samo šifriranje softvera)

Administratori mogu upotrebljavati softver Drive Encryption za šifriranje jedne ili više particija tvrdog diska na računalu ili za dešifriranje bilo koje particije(a) pogona koja je već šifrirana.

1. Pokrenite **Drive Encryption**. Dodatne informacije potražite u odjeljku Otvaranje softvera Drive Encryption na stranici 29.
2. U kartici **Status pogona**, odaberite ili očistite potvrdni okvir pored svake particije tvrdog pogona koju želite šifrirati ili dešifrirati i zatim kliknite ili dodirnite **Primijeni**.

NAPOMENA: Kada se particija šifrira ili dešifrira na traci prikaza tijeka prikazuje se postotak šifrirane particije.

NAPOMENA: Ne podržavaju se dinamičke particije. Ako se particija prikazuje kao dostupna, ali se ne može šifrirati kada se odabere, ta je particija dinamička. Dinamička particija nastaje smanjivanjem particije kako bi se stvorila nova particija u opciji Upravljanje diskom.

Upozorenje se prikazuje ako će se particija pretvoriti u dinamičku particiju.

Upravljanje diskom

- **Nadimak**—Možete imenovati svoje pogone ili particije radi lakše identifikacije.
- **Odspojeni pogoni**—Softver Drive Encryption može pratiti diskove koji su uklonjeni s računala. Disk uklonjen s računala automatski se premješta na Popis odspajanja. Ako se disk vrati u sustav ponovno će se pojaviti na Popisu spajanja.
- Ako više ne trebate pratiti ili upravljati odspojenim pogonom možete ga ukloniti s Popisa odspajanja.
- Softver Drive Encryption ostaje uključen sve dok se ne očiste potvrdni okviri svih spojenih pogona i dok se ne isprazni Popis odspajanja.

Sigurnosno kopiranje i oporavak (zadatak administratora)

Kada je softver Drive Encryption uključen administratori mogu upotrijebiti stranicu Sigurnosno kopiranje ključa za šifriranje za stvaranje sigurnosne kopije ključa za šifriranje za uklonjive medije i za provođenje oporavka.

Sigurnosno kopiranje ključeva za šifriranje

Administratori mogu sigurnosno kopirati ključ za šifriranje za šifrirani pogon na uklonjivom uređaju za pohranu.

OPREZ: Provjerite je li uređaj za pohranu koji sadrži ključ sigurnosne kopije na sigurnom mjestu jer ako zaboravite lozinku, izgubite pametnu karticu ili nemate registrirani prst, ovaj uređaj vam omogućuje jedini pristup računalu. Mjesto za pohranu također mora biti sigurno jer uređaj za pohranu omogućuje pristup sustavu Windows.

1. Pokrenite **Drive Encryption**. Dodatne informacije potražite u odjeljku Otvaranje softvera Drive Encryption na stranici 29.
2. Odaberite potvrdni okvir pogona, a zatim kliknite ili dodirnite **Ključ sigurnosne kopije**.

3. U kartici **Stvaranje ključa za oporavak softvera HP Drive Encryption**, odaberite jednu ili više od sljedećih opcija:

   - **Uklonjiva pohrana**—Odaberite potvrdni okvir i zatim odaberite uređaj za pohranu gdje se može spremiti ključ za šifriranje.
   - **SkyDrive**—Odaberite potvrdni okvir. Morate biti spojeni na internet. Prijavite se za aplikaciju Microsoft SkyDrive pa zatim kliknite ili dodirnite **Da**.

   NAPOMENA: Za upotrebu ključa sigurnosne kopije softvera HP Drive Encryption koji je spremljen u aplikaciji SkyDrive, morate ga preuzeti iz aplikacije SkyDrive na uklonjivi disk za pohranu i zatim umetnuti uređaj za pohranu u ovo računalo.

   - **TPM** (samo odabrani modeli)—Omogućuje vam oporavak podataka pomoću vaše TPM lozinke.

   OPREZ: Ako je TPM očišćen ili je računalo oštećeno izgubit ćete pristup sigurnosnoj kopiji. Ako se odabere ovaj način rada mora se odabrati i drugi način stvaranja sigurnosne kopije.

4. Kliknite ili dodirnite **Stvori sigurnosnu kopiju**.

   Ključ za šifriranje spremljen je u uređaj za pohranu koji ste odabrali.

Oporavak pristupa uključenom računalu pomoću ključeva sigurnosne kopije

Administratori mogu obaviti oporavak pomoću ključa za šifriranje pogona koji je sigurnosno kopiran na uklonjivom uređaju za pohranu prilikom uključivanja ili odabirom opcije **Ključ sigurnosne kopije** u softveru Drive Encryption.

1. Umetnite uklonjivi uređaj za pohranu koji sadrži vaš ključ sigurnosne kopije.
2. Uključite računalo.
3. Kada se otvori dijaloški okvir potvrde prijave za softver HP Drive Encryption kliknite ili dodirnite **Oporavak**.
4. Unesite put do datoteke ili naziv koji sadrži ključ sigurnosne kopije i zatim kliknite ili dodirnite **Oporavak**.
5. Kada se otvori dijaloški okvir potvrde kliknite ili dodirnite **U redu**.

   Prikazuje se zaslon prijave sustava Windows.

NAPOMENA: Ako se ključ za oporavak upotrebljava za prijavu na zaslonu za prijavu softvera Drive Encryption, potrebne su dodatne vjerodajnice prilikom prijave u sustavu Windows za pristup korisničkim računima. Preporučujemo vam da ponovno postavite svoju lozinku nakon obavljanja oporavka.

Obavljanje oporavka uslužnog programa HP SpareKey

Za oporavak uslužnog programa HP SpareKey kod ponovnog pokretanja softvera Drive encryption trebate ispravno odgovoriti na sigurnosna pitanja prije nego što možete pristupiti računalu. Više informacija o postavljanju Oporavka uslužnog programa SpareKey potražite u Pomoći za softver HP sigurnosnog klijenta.

Za obavljanje Oporavka uslužnog programa SpareKey ako zaboravite lozinku:

1. Uključite računalo.
2. Kada se prikazuje zaslon softvera HP Drive encryption pomaknite se na zaslon za prijavu korisnika.

3. Kliknite **SpareKey**.

NAPOMENA: Ako vaš SpareKey još nije inicijaliziran u aplikaciji HP sigurnosnog klijenta, gumb **SpareKey** nije dostupan.

4. Upišite točan odgovor na prikazana pitanja, a zatim kliknite **Prijava**.

   Prikazuje se zaslon prijave sustava Windows.

NAPOMENA: Ako se SpareKey upotrebljava za prijavu na zaslonu za prijavu softvera Drive Encryption, potrebne su dodatne vjerodajnice prilikom prijave u sustavu Windows za pristup korisničkim računima. Preporučujemo vam da ponovno postavite svoju lozinku nakon obavljanja oporavka.

6 HP File Sanitizer (samo odabrani modeli)

Program File Sanitizer omogućuje vam sigurno trajno brisanje imovine (na primjer: osobnih podataka ili datoteka, podataka o povijesti ili onih vezanih uz web ili druge komponente podataka) na internom tvrdom disku računala i povremeno čišćenje internog tvrdog diska računala.

Program File Sanitizer ne može se upotrebljavati za trajno brisanje ili čišćenje sljedećih vrsta diskova:

- diskova Solid-state drives (SSD), uključujući RAID jedinice koje obuhvaćaju SSD uređaj
- vanjskih diskova spojenih putem USB, Firewire ili eSATA sučelja

Ako se na SSD disku pokuša obaviti trajno brisanje ili čišćenje pojavljuje se poruka upozorenja i radnja se ne može obaviti.

Trajno brisanje

Trajno se brisanje razlikuje od uobičajene akcije brisanja sustava Windows®. Kada pomoću programa File Sanitizer trajno izbrišete neku imovinu, datoteke se prepisuju besmislenim podacima čineći tako virtualno nemogućim dohvaćanje originalne imovine. Jednostavna akcija brisanja sustava Windows može ostaviti datoteku (ili imovinu) nedirnutom na tvrdom disku ili je pak ostaviti u stanja da se forenzičkim metodama može oporaviti.

Možete zakazati vrijeme trajnog brisanja u budućnosti ili možete ručno pokrenuti trajno brisanje birajući ikonu **File Sanitizer** na početnom zaslonu HP sigurnosnog klijenta ili pomoću ikone **File Sanitizer** na radnoj površini sustava Windows. Više informacije potražite u Postavljanje rasporeda trajnog brisanja na stranici 38, Trajno brisanje desnim klikom na stranici 40 ili Ručno pokretanje postupka trajnog brisanja na stranici 40.

NAPOMENA: Neka .dll datoteka trajno je izbrisana ili uklonjena iz sustava samo ako se premjesti u koš za smeće.

Čišćenje praznog prostora

Brisanje zapisa u sustavu Windows ne uklanja u potpunosti sadržaj zapisa s vašeg tvrdog diska. Sustav Windows briše samo adresu zapisa ili njegovu lokaciju na tvrdom disku. Sadržaj zapisa i dalje ostaje na tvrdom disku sve dok neki drugi zapis ne prepiše isto područje na tvrdom disku novim informacijama.

Čišćenje praznog prostora omogućuje vam sigurno upisivanje nasumičnih podataka preko izbrisanog zapisa sprječavajući da korisnik vidi originalne sadržaje izbrisanog zapisa.

NAPOMENA: Čišćenje praznog prostora ne daje dodatnu sigurnost trajno izbrisanom zapisu.

Možete postaviti vrijeme čišćenja praznog prostora u budućnosti ili možete ručno pokrenuti čišćenje praznog prostora birajući ikonu **File Sanitizer** na početnom zaslonu HP sigurnosnog klijenta ili pomoću ikone **File Sanitizer** na radnoj površini sustava Windows. Više informacije potražite u Postavljanje rasporeda za čišćenje praznog prostora na stranici 39, Ručno pokretanje čišćenja praznog prostora na stranici 41 ili Upotreba ikone programa File Sanitizer na stranici 40.

Otvaranje programa File Sanitizer

1. Na početnom zaslonu kliknite ili dodirnite aplikaciju **HP Client Security** (Windows 8).

   – ili –

   Na radnoj površini sustava Windows dva puta kliknite ikonu **HP Client Security** u području obavijesti na krajnjem desnom dijelu programske trake.

2. U **Podacima** kliknite ili dodirnite **File Sanitizer**.

– ili –

▲ Dva puta kliknite ili dva puta dodirnite ikonu **File Sanitizer** na radnoj površini sustava Windows.

– ili –

▲ Kliknite desnom tipkom miša ili dodirnite i držite ikonu **File Sanitizer** na radnoj površini sustava Windows pa zatim odaberite **Otvori File Sanitizer**.

Postupci postavljanja

Trajno brisanje—File Sanitizer na siguran način briše ili trajno briše odabrane kategorije zapisa.

1. U kartici **Trajno brisanje** odaberite potvrdni okvir za svaku vrstu datoteke koja se treba trajno izbrisati ili očistite potvrdni okvir ako ne želite trajno izbrisati te datoteke.

   - **Koš za smeće**—Trajno briše sve stavke u košu za smeće.
   - **Privremene sistemske datoteke**—Trajno briše sve datoteke koje se nalaze u privremenoj mapi sustava. Sljedeće varijable okruženja pretražuju se sljedećim redom i prva pronađena putanja smatra se mapom sustava:
     - TMP
     - TEMP
   - **Privremene internetske datoteke**—Trajno briše kopije web stranica, slika i medija koje su web-preglednici pohranili za brže pregledavanje.
   - **Kolačići**—Trajno briše sve datoteke koje su web-mjesta pohranila na računalu kako bi se spremile postavke kao što su podaci za prijavu.

2. Za pokretanje trajnog brisanja kliknite ili dodirnite **Trajno izbriši**.

Čišćenje—Upisuje nasumične podatke u prazan prostor i sprječava oporavak izbrisanih stavki.

▲ Za pokretanje čišćenja kliknite ili dodirnite **Čisti**.

Opcije programa File Sanitizer—Odaberite potvrdni okvir kako biste omogućili svaku od sljedećih opcija ili očistite potvrdni okvir kako biste onemogućili jednu od opcija:

- **Omogući ikonu radne površine**—Prikazuje ikonu programa File Sanitizer na radnoj površini sustava Windows.
- **Omogući desni klik**—Omogućuje vam da kliknete desnom tipkom miša ili dodirnete i zadržite zapis i da zatim odaberete **HP File Sanitizer – Trajno izbriši**.

- **Zatraži lozinku za sustav Windows prije obavljanja ručnog trajnog brisanja**—Traži provjeru autentičnosti pomoću lozinke za sustav Windows prije obavljanja ručnog trajnog brisanja neke stavke.
- **Trajno izbriši kolačiće i privremene internetske datoteke kod zatvaranja preglednika**—Trajno briše odabrane zapise koji se odnosi na web kao što je URL povijest preglednika kada zatvorite web-preglednik.

Postavljanje rasporeda trajnog brisanja

Možete zakazati vrijeme automatskog obavljanja trajnog brisanja ili možete u bilo koje vrijeme i ručno trajno izbrisati zapise. Dodatne informacije potražite u Postupci postavljanja na stranici 37.

1. Otvorite File Sanitizer, a zatim kliknite ili dodirnite **Postavke**.
2. Za zakazivanje vremena za trajno brisanje imovine u budućnosti u kartici **Raspored trajnog brisanja** odaberite **Nikada**, **Jednom**, **Svakodnevno**, **Tjedno** ili **Mjesečno**, pa zatim odaberite dan i vrijeme:
   a. Kliknite ili dodirnite sat, minutu ili polje ujutro/poslije podne.
   b. Pomaknite se do željene vrijednosti koja je prikazana na istoj razini kao i ostala polja.
   c. Kliknite ili dodirnite bijeli prostor oko polja postavki.
   d. Ponovite za svako polje dok se ne odabere ispravan raspored.
3. Ispisuju se sljedeće četiri vrste zapisa:
   - **Koš za smeće**—Trajno briše sve stavke u košu za smeće.
   - **Privremene sistemske datoteke**—Trajno briše sve datoteke koje se nalaze u privremenoj mapi sustava. Sljedeće varijable okruženja pretražuju se sljedećim redom i prva pronađena putanja smatra se mapom sustava:
     - TMP
     - TEMP
   - **Privremene internetske datoteke**—Trajno briše kopije web stranica, slika i medija koje su web-preglednici pohranili za brže pregledavanje.
   - **Kolačići**—Trajno briše sve datoteke koje su web-mjesta pohranila na računalu kako bi se spremile postavke kao što su podaci za prijavu.

   Ti zapisi, ako su označeni, trajno se briše u zakazano vrijeme.
4. Za odabir dodatnih prilagođenih zapisa koji se trebaju trajno izbrisati:
   a. U kartici **Popis zakazanog trajnog brisanja** kliknite ili dodirnite **Dodaj mapu** pa se zatim pomaknite do datoteke ili mape.
   b. Kliknite ili dodirnite **Otvori**, a zatim kliknite ili dodirnite **U redu**.

   Za uklanjanje zapisa s popisa zakazanog trajnog brisanja očistite potvrdni okvir zapisa.

Postavljanje rasporeda za čišćenje praznog prostora

Čišćenje praznog prostora ne daje dodatnu sigurnost trajno izbrisanom zapisu.

1. Otvorite File Sanitizer, a zatim kliknite ili dodirnite **Postavke**.
2. Za zakazivanje vremena čišćenja tvrdog diska u budućnosti u kartici **Raspored čišćenja** odaberite **Nikada**, **Jednom**, **Svakodnevno**, **Tjedno** ili **Mjesečno**, a zatim odaberite dan i vrijeme.
   a. Kliknite ili dodirnite sat, minutu ili polje ujutro/poslije podne.
   b. Pomaknite se do željenog vremena koje je prikazano na istoj razini kao i ostala polja.
   c. Kliknite ili dodirnite bijeli prostor oko polja postavki.
   d. Ponavljajte dok se ne odabere ispravan raspored.

NAPOMENA: Postupak čišćenja praznog prostora može dulje trajati. Provjerite je li računalo priključeno na izvor izmjenične struje. Iako se postupak čišćenja praznog prostora obavlja u pozadini povećano korištenje procesora može utjecati na performanse računala. Čišćenje praznog prostora može se obaviti nakon radnog vremena ili kada se računalo ne upotrebljava.

Zaštita datoteka od trajnog brisanja

Kako biste zaštitili datoteke ili mape od trajnog brisanja:

1. Otvorite File Sanitizer, a zatim kliknite ili dodirnite **Postavke**.
2. U kartici **Popis trajnog brisanja koje se nikada ne obavlja** kliknite ili dodirnite **Dodaj mapu** pa se zatim pomaknite do datoteke ili mape.
3. Kliknite ili dodirnite **Otvori**, a zatim kliknite ili dodirnite **U redu**.

NAPOMENA: Datoteke na tom popisu zaštićene su sve dok se nalaze na popisu.

Za uklanjanje zapisa s popisa izuzeća očistite potvrdni okvir zapisa.

Opći zadaci

Program File Sanitizer upotrebljavajte za obavljanje sljedećih zadataka:

- **Ikonu programa File Sanitizer upotrijebite za pokretanje trajnog brisanja**—Povucite datoteke do ikone **File Sanitizer** na radnoj površini sustava Windows. Više pojedinosti potražite u Upotreba ikone programa File Sanitizer na stranici 40.
- **Ručno trajno brisanje određenog zapisa ili svih zapisa**—Stavke trajno izbrišite u bilo koje vrijeme, a da ne čekate zakazano vrijeme trajnog brisanja. Više pojedinosti potražite u Trajno brisanje desnim klikom na stranici 40 ili Ručno pokretanje postupka trajnog brisanja na stranici 40.
- **Ručno pokrenite čišćenje praznog prostora**—Čišćenje praznog prostora pokrenite u bilo koje vrijeme. Više pojedinosti potražite u Ručno pokretanje čišćenja praznog prostora na stranici 41.
- **Prikažite datoteke zapisnika**—Prikažite datoteke zapisnika za trajno brisanje i čišćenje praznog prostora koje sadrže sve pogreške ili neispravnosti iz zadnjeg postupka trajnog brisanja ili čišćenja praznog prostora. Više pojedinosti potražite u Prikaz datoteka zapisnika na stranici 41.

NAPOMENA: Postupak trajnog brisanja ili čišćenja praznog prostora može dulje trajati. Iako se postupak trajnog brisanja i čišćenja praznog prostora obavlja u pozadini povećano korištenje procesora može utjecati na performanse računala.

Upotreba ikone programa File Sanitizer

OPREZ: Uništeni zapisi ne mogu se oporaviti. Pažljivo razmislite o stavkama koje odabirete za ručni postupak trajnog brisanja.

Kada ručno pokrenete postupak trajnog brisanja standardni popis za trajno brisanje u prikazu File Sanitizer trajno se briše (pogledajte Postupci postavljanja na stranici 37).

Ručni postupak trajnog brisanja možete pokrenuti na jedan od sljedećih načina:

1. Otvorite File Sanitizer (pogledajte Otvaranje programa File Sanitizer na stranici 37), a zatim kliknite ili dodirnite **Trajno izbriši**.
2. Kada se otvori dijaloški okvir potvrde provjerite je li označen zapis koji želite izbrisati i zatim kliknite ili dodirnite **U redu**.

– ili –

1. Kliknite desnom tipkom miša ili dodirnite i držite ikonu **File Sanitizer** na radnoj površini sustava Windows pa zatim kliknite ili dodirnite **Sada trajno izbriši**.
2. Kada se otvori dijaloški okvir potvrde provjerite je li označen zapis koji želite izbrisati i zatim kliknite ili dodirnite **Trajno izbriši**.

Trajno brisanje desnim klikom

OPREZ: Uništeni zapisi ne mogu se oporaviti. Pažljivo razmislite o stavkama koje odabirete za ručni postupak trajnog brisanja.

Ako je u prikazu File Sanitizer odabrano **Omogući trajno brisanje desnim klikom** imovinu možete trajno izbrisati na sljedeći način:

1. Pomaknite se do dokumenta ili mape koju želite trajno izbrisati.
2. Kliknite desnom tipkom miša ili dodirnite i zadržite datoteku ili mapu i zatim odaberite **HP File Sanitizer – Trajno izbriši**.

Ručno pokretanje postupka trajnog brisanja

OPREZ: Uništeni zapisi ne mogu se oporaviti. Pažljivo razmislite o stavkama koje odabirete za ručni postupak trajnog brisanja.

Kada ručno pokrenete postupak trajnog brisanja standardni popis za trajno brisanje u prikazu File Sanitizer trajno se briše (pogledajte Postupci postavljanja na stranici 37).

Ručni postupak trajnog brisanja možete pokrenuti na jedan od sljedećih načina:

1. Otvorite File Sanitizer (pogledajte Otvaranje programa File Sanitizer na stranici 37), a zatim kliknite ili dodirnite **Trajno izbriši**.
2. Kada se otvori dijaloški okvir potvrde provjerite je li označen zapis koji želite izbrisati i zatim kliknite ili dodirnite **U redu**.

– ili –

1. Kliknite desnom tipkom miša ili dodirnite i držite ikonu **File Sanitizer** na radnoj površini sustava Windows pa zatim kliknite ili dodirnite **Sada trajno izbriši**.
2. Kada se otvori dijaloški okvir potvrde provjerite je li označen zapis koji želite izbrisati i zatim kliknite ili dodirnite **Trajno izbriši**.

Ručno pokretanje čišćenja praznog prostora

Kada ručno pokrenete postupak čišćenja praznog prostora, čisti se standardni popis za trajno brisanje u prikazu File Sanitizer (pogledajte Postupci postavljanja na stranici 37).

Ručni postupak čišćenja praznog prostora možete pokrenuti na jedan od sljedećih načina:

1. Otvorite File Sanitizer (pogledajte Otvaranje programa File Sanitizer na stranici 37), a zatim kliknite ili dodirnite **Očisti prazan prostor**.
2. Kada se otvori dijaloški okvir potvrde kliknite ili dodirnite **U redu**.

– ili –

1. Kliknite desnom tipkom miša ili dodirnite i držite ikonu **File Sanitizer** na radnoj površini sustava Windows pa zatim kliknite ili dodirnite **Sada očisti prazan prostor**.
2. Kada se otvori dijaloški okvir potvrde kliknite ili dodirnite **Očisti prazan prostor**.

Prikaz datoteka zapisnika

Prilikom svakog obavljanja postupka trajnog brisanja ili čišćenje praznog prostora stvara se datoteka zapisnika za sve pogreške ili neispravnosti. Datoteke zapisnika sustavno se ažuriraju prema zadnjem obavljenom postupku trajnog brisanja ili čišćenja praznog prostora.

NAPOMENA: Datoteke na kojima je uspješno obavljen postupak trajnog brisanja ili čišćenja praznog prostora ne pojavljuju se u datotekama zapisnika.

Jedna datoteka zapisnika stvara se za postupak trajnog brisanja, a druga za postupak čišćenja praznog prostora. Obje datoteke zapisnika nalaze se na tvrdom disku u sljedećim mapama:

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

U 64-bitnim sustavima datoteke zapisnika nalaze se na tvrdom disku u sljedećim mapama:

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

7 HP Device Access Manager (samo odabrani modeli)

Softver HP Device Access Manager upravlja pristupom podacima onemogućavajući uređaje za prijenos podataka.

NAPOMENA: Nekim sučeljima za interakciju s ljudima/ulaznim uređajima kao što su miš, tipkovnica, TouchPad i čitač otisaka prstiju ne upravlja softver Device Access Manager. Dodatne informacije potražite u odjeljku Neupravljane klase uređaja na stranici 45.

Administratori operacijskog sustava Windows® upotrebljavaju softver HP Device Access Manager za upravljanjem pristupom uređajima na sustavu i za zaštitu od neovlaštenog pristupa:

- Profili uređaja stvoreni su za svakog korisnika kako bi se odredili uređaji za koje im je dozvoljena ili uskraćena dozvola pristupa.
- Opcija Just In Time Authentication (JITA) omogućuje unaprijed definiranim korisnicima provjeru autentičnosti kako bi se omogućio pristup uređajima koji im je inače uskraćen.
- Administratori i pouzdani korisnici mogu se isključiti iz ograničenja pristupa uređaju koje uvjetuje softver Device Acces Manager tako da ih se doda u grupu administratora uređaja. Članstvom u ovoj grupi upravlja se pomoću naprednih postavki.
- Uređaji se mogu dozvoliti ili uskratiti na temelju članstva u grupi korisnika ili za pojedinačne korisnike.
- Za klase uređaja kao što su CD-ROM i DVD pogoni, pristup za pisanje i pristup za čitanje mogu se odvojeno dozvoliti ili uskratiti.

Softver HP Device Access Manager automatski se konfigurira sa sljedećim postavkama tijekom dovršenja čarobnjaka za postavljanje HP sigurnosnog klijenta:

- Uklonjivi medij opcije Just In Time Authentication (JITA) omogućen je za administratore i korisnike.
- Pravila uređaja omogućuju potpuni pristup ostalim uređajima.

Otvaranje softvera Device Access Manager

1. Na početnom zaslonu kliknite ili dodirnite aplikaciju **HP Client Security** (Windows 8).

   – ili –

   Na radnoj površini sustava Windows dva puta kliknite ikonu **HP Client Security** u području obavijesti na krajnjem desnom dijelu programske trake.

2. U kartici **Uređaji** kliknite ili dodirnite **Dozvole uređaja**.

   - Standardni korisnici mogu vidjeti svoje trenutačne pristupe uređaju (pogledajte Prikaz korisnika na stranici 43).
   - Administratori mogu vidjeti i unijeti izmjene u trenutačno konfiguriran pristup uređaju računala tako da kliknu ili dodirnu **Promijeni** a zatim unesu lozinku administratora (pogledajte Prikaz sustava na stranici 43).

Prikaz korisnika

Kada se odaberu **Dozvole uređaja**, prikazuje prikaz korisnika. Ovisno o pravilima standardni korisnici i administratori mogu prikazati svoj vlastiti pristup klasama uređaja ili pojedinačnim uređajima na ovom računalu.

- **Trenutačni korisnik**—Prikazuje se ime korisnika koji je trenutačno prijavljen.
- **Klasa uređaja**—Prikazuju se vrste uređaja.
- **Pristup**—Prikazuje se vaš trenutačno konfiguriran pristup vrstama uređaja ili određenim uređajima.
- **Trajanje**—Prikazuje se vremensko ograničenje vašeg pristupa CD/DVD-ROM-u ili uklonjivim diskovnim pogonima.
- **Postavke**—Administratori mogu promijeniti koje pogone kojima upravlja softver Device Access Manager.

Prikaz sustava

U prikazu sustavu administratori mogu odobriti ili uskratiti pristup uređajima na ovom računalu grupi korisnika ili grupi administratora.

▲ Administratori mogu pristupiti prikazu sustava tako da kliknu ili dodirnu **Promijeni**, unesu lozinku administratora i zatim odaberu jednu od sljedećih opcija:

- **Device Access Manager**—Za uključivanje ili isključivanje softvera HP Device Access Manager pomoću opcije Just In Time Authentication kliknite ili dodirnite **Uključi** ili **Isključi**.
- **Korisnici i grupe na ovom računalu**—Prikazuje grupu korisnika ili grupu administratora kojima je odobren ili uskraćen pristup odabranim klasama uređaja.
- **Klasa uređaja**—Prikazuje klase uređaja i uređaje koji su instalirani na sustavu ili koji su možda ranije bili instalirani na sustav. Za proširenje popisa kliknite ikonu **+**. Prikazani su svi uređaji spojeni na računalo, administratori i grupa korisnika su prošireni kako bi se prikazalo njihovo članstvo. Za osvježavanje popisa uređaja kliknite ikonu okrugle strelice (osvježi).
  - Zaštita se obično primjenjuje za klasu uređaja. Ako je pristup postavljen na **Dozvoli**, odabrani korisnik ili grupa moći će pristupiti bilo kojem uređaju u klasi uređaja.
  - Zaštita se može primijeniti i na određene uređaje.
  - Konfigurirajte opciju Just In Time authentication (JITA) omogućujući odabranim korisnicima pristup DVD/CD-ROM-u ili uklonjivim diskovnim pogonima uz provjeru njihove autentičnosti. Dodatne informacije potražite u odjeljku Konfiguracija opcije JITA na stranici 44.
  - Omogućite ili uskratite pristup ostalim klasama uređaja kao što su uklonjivi mediji (kao što je USB izbrisivi memorijski pogon), serijski i paralelni priključci, Bluetooth® uređaji, modemski uređaji, PCMCIA/ExpressCard uređaji, uređaji 1394, čitač otiska prsta i čitač pametne kartice. Ako se uskrate čitač otiska prsta i čitač pametne kartice oni se mogu upotrebljavati kao vjerodajnice za provjeru, ali se ne mogu upotrebljavati na razini pravila sesije.

    NAPOMENA: Ako se Bluetooth upotrebljava kao vjerodajnice za provjeru, pristup uređaju Bluetooth ne smije biti ograničen u pravilima softvera Device Access Manager.

  - Kada odaberete postavku na razini grupe ili klase uređaja upitat će vas se želite li primijeniti postavku na određene objekte.

    Da—Postavka će se prenijeti.

Ne—Postavka se neće prenijeti.

- Za neke klase uređaja kao što su DVD i CD-rom može se postaviti dodatno upravljanje tako da se odvojeno omoguće ili uskrate radnje čitanja i pisanja.

NAPOMENA: Grupa administratora ne može se dodati na popis korisnika.

- **Pristup**—Kliknite ili dodirnite strelicu prema dolje i zatim odaberite jednu od sljedećih vrsta pristupa kako biste omogućili ili uskratili pristup:
  - **Dozvoli – Potpuni pristup**
  - **Dozvoli – Samo za čitanje**
  - **Dozvoli – obavezan je JITA**—Više informacija potražite u Konfiguracija opcije JITA na stranici 44.

    Ako je odabrana ova vrsta pristupa u kartici **Trajanje** kliknite ili dodirnite strelicu prema dolje kako biste odabrali vremensko ograničenje.
  - **Uskrati**
- **Trajanje**—Kliknite ili dodirnite strelicu prema dolje kako biste odabrali vremensko ograničenje za CD/DVD-ROM ili uklonjive diskovne pogone (pogledajte Konfiguracija opcije JITA na stranici 44).

Konfiguracija opcije JITA

Konfiguracija opcije JITA administratorima omogućuje izmjenu popisa korisnika i grupa kojima je odobren pristup uređajima upotrebom opcije Just In Time Authentication (JITA).

Korisnici za koje je omogućena opcije JITA moći će pristupiti nekim uređajima za koje su ograničena pravila stvorena u prikazu **Konfiguracija klase uređaja**.

Razdoblje opcije JITA može se odobriti za postavljen broj minuta ili na neograničeno. Korisnici s neograničenim pristupom, imat će pristup uređaju od trenutka provjere autentičnosti do trenutka kada se odjave iz sustava.

Ako je korisniku dozvoljeno ograničeni razdoblje opcije JITA, jednu minutu prije nego što istekne razdoblje JITA od korisnika će se zatražiti proširenje pristupa. Čim se korisnik odjavi iz sustava ili se drugi korisnik prijavi, razdoblje JITA ističe. Kada se korisnik sljedeći put prijavi i pokuša pristupiti uređaju za koji je omogućena opcija JITA prikazat će se upit za unos vjerodajnica.

JITA je dostupna za sljedeće klase uređaja:

- DVD/CD-rom-ove
- uklonjive diskovne pogone

Stvaranje JITA pravila za korisnika ili grupu

Administratori mogu omogućiti korisnicima ili grupama pristup uređajima uz upotrebu opcije Just In Time Authentication (JITA).

1. Pokrenite softver **Device Access Manager**, a zatim kliknite ili dodirnite **Promijeni**.
2. Odaberite korisnika ili grupu i zatim u kartici **Pristup** za **Izmjenjive diskovne pogone** ili **DVD/CD-ROM-ove** kliknite ili dodirnite strelicu prema dolje i zatim odaberite **Dozvoli – potreban JITA**.
3. U kartici **Trajanje** kliknite ili dodirnite strelicu prema dolje kako biste odabrali vremenski rok za JITA pristup.

Korisnik se mora odjaviti i zatim ponovno prijaviti kako bi se primijenila nova postavka opcije JITA.

Onemogućavanje JITA pravila za korisnika ili grupu

Administratori mogu onemogućiti korisnicima ili grupama pristup uređajima uz upotrebu opcije Just In Time Authentication.

1. Pokrenite softver **Device Access Manager**, a zatim kliknite ili dodirnite **Promijeni**.
2. Odaberite korisnika ili grupu i zatim u kartici **Pristup** za **Izmjenjive diskovne pogone** ili **DVD/CD-ROM-ove** kliknite ili dodirnite strelicu prema dolje i zatim odaberite **Uskrati**.

Kada se korisnik prijavi i pokuša pristupiti uređaju, pristup je uskraćen.

Postavke

Prikaz **Postavke** administratorima omogućuje prikazivanje i promjenu pogona čijim pristupom upravlja softver Device Access Manager.

NAPOMENA: Softver Device Access Manager mora biti omogućen kada se konfigurira popis slova pogona (pogledajte Prikaz sustava na stranici 43).

Neupravljane klase uređaja

Softver HP Device Access Manager ne upravlja sljedećim klasama uređaja:

- Ulazni/izlazni uređaji
  - CD-ROM
  - Diskovni pogon
  - Kontrolor diskete (FDC)
  - Kontrolor tvrdog diska (HDC)
  - Klasa Human interface device (HID)
  - Infracrveni uređaji sučelja za interakciju s ljudima
  - Miš
  - Serijski s više priključaka
  - Tipkovnica
  - Pisači "uključi i radi" (PnP)
  - Pisač
  - Nadogradnja pisača
- Gumb
  - Podrška za napredno upravljanje napajanjem (APM)
  - Baterija
- Razno
  - Računalo
  - Dekoder

- Zaslon
- Ujednačeni upravljački program za zaslon Intel®
- Legacard
- Upravljački program za medije
- Uređaji za izmjenu medija
- Memorijska tehnologija
- Monitor
- Višefunkcijski
- Mrežni klijent
- Mrežna usluga
- Mrežni prijenos
- Procesor
- Prilagodnik za SCSI
- Akcelerator sigurnosti
- Sigurnosni uređaji
- Sustav
- Nepoznato
- Jedinica
- Snimka stanja jedinice

8 HP Trust Circles

HP Trust Circles je datoteka i aplikacija za sigurnost dokumenta koja predstavlja kombinaciju šifriranja mape i datoteke s praktičnom mogućnošću dijeljenja dokumenta u pouzdanom krugu. Aplikacija šifrira datoteke koje se nalaze u korisnički definiranima mapama štiteći ih unutar pouzdanog kruga. Jednom kada se zaštite datoteke mogu upotrebljavati i dijeliti samo članovi u krugu povjerenja. Ako zaštićenu datoteku primi netko tko nije član ona ostaje šifrirana i osoba koja nije član ne može joj pristupiti.

Otvaranje aplikacije Trust Circles

1. Na početnom zaslonu kliknite ili dodirnite aplikaciju **HP Client Security**.

   – ili –

   S radne površine Windows dva puta kliknite ikonu **HP Client Security** u području obavijesti koje se nalazi na krajnjem desnom dijelu programske trake.

2. U **Podacima** kliknite ili dodirnite **Trust Circles**.

Početak rada

Dva su načina za slanje pozivnica putem e-pošte i odgovaranja na njih:

- **Pomoću programa Microsoft® Outlook**—Upotreba aplikacije Trust Circles s programom Microsoft Outlook automatizira obradu svih pozivnica iz aplikacije Trust Circle i odgovora drugih korisnika aplikacije Trust Circle.
- **Pomoću usluga Gmail, Yahoo, Outlook.com ili drugih usluge e-pošte (SMTP)**—Kada unesete svoje ime, adresu e.pošte i lozinku aplikacija Trust Circles upotrebljava vašu uslugu e-pošte za slanje pozivnica putem e-pošte članovima koji su odabrani za pridruživanje vašem krugu povjerenja.

Za postavljanje osnovnog profila:

1. Unesite svoje ime i adresu e-pošte, a zatim kliknite ili dodirnite **Sljedeće**.

   Ime je vidljivo svim članima pozvanima u vaš krug povjerenja. Adresa e-pošte upotrebljava se za slanje, primanje ili odgovaranje na pozivnice.

2. Unesite lozinku koja se upotrebljava za račun e-pošte, a zatim kliknite ili dodirnite **Sljedeći**.

   Šalje se probna poruka e-pošte kako bi se povjerilo jesu li postavke e-pošte točne.

   NAPOMENA: Računalo mora biti spojeno na mrežu.

3. U polju **Naziv kruga povjerenja** unesite naziv kruga povjerenja i zatim kliknite ili dodirnite **Sljedeći**.

4. Dodajte članove i mape, a zatim kliknite ili dodirnite **Sljedeće**. Krug povjerenja stvara se sa svim odabranim mapama i šalje pozivnice e-pošte svim odabranim članovima. Ako se, iz bilo kojeg razloga, neka pozivnica ne može poslat, prikazuje se obavijest. Članovi se mogu uvijek ponovno pozvati iz prikaza kruga povjerenja tako da kliknete **Vaši krugovi povjerenja** i zatim dva puta

kliknete ili dva puta dodirnete krug povjerenja. Dodatne informacije potražite u odjeljku Trust Circles na stranici 48.

Trust Circles

Krug povjerenja možete stvoriti tijekom početnog postavljanja nakon što unesete svoju adresu e-pošte ili u prikazu kruga povjerenja:

▲ Iz prikaza kruga povjerenja kliknite ili dodirnite **Stvori krug povjerenja** i zatim unesite naziv kruga povjerenja.

- Za dodavanje članova u krug povjerenja kliknite ili dodirnite ikonu **M+** pored **Članova** i zatim slijedite upute na zaslonu.
- Za dodavanje mapa u krug povjerenja kliknite ili dodirnite ikonu **+** pored **Mapa** i zatim slijedite upute na zaslonu.

Dodavanje mapa u krug povjerenja

Dodavanje mapa u novi krug povjerenja:

- Tijekom stvaranja kruga povjerenja mape možete dodati tako da kliknite ili dodirnete ikonu **+** pored **Mapa** i zatim slijedite upute na zaslonu.

  – ili –

- U pregledniku Windows Explorer, kliknite desnom tipkom miša ili dodirnite i držite mapu koja trenutačno nije dio kruga povjerenja, odaberite **Krug povjerenja** i zatim odaberite **Stvori krug povjerenja iz mape**.

SAVJET: Možete odabrati jednu ili više mapa.

Dodavanje mapa u postojeći krug povjerenja:

- Iz prikaza kruga povjerenja kliknite **Vaši krugovi povjerenja**, dva puta kliknite ili dva puta dodirnite postojeći krug povjerenja kako biste prikazali trenutačne mape, kliknite ili dodirnite ikonu **+** pored **Mapa**, a zatim pratite upute na zaslonu.

  – ili –

- U pregledniku Windows Explorer, kliknite desnom tipkom miša ili dodirnite i držite mapu koja trenutačno nije dio kruga povjerenja, odaberite **Krug povjerenja** i zatim odaberite **Dodaj u postojeći krug povjerenja iz mape**.

SAVJET: Možete odabrati jednu ili više mapa.

Kada se mapa doda u krug povjerenja, aplikacija Trust Circles automatski šifrira mapu i njezine sadržaje. Kada su sve datoteke šifrirane prikazuje se obavijest. Osim toga prikazuje se zeleni simbol brave na svim ikonama šifriranih mapa i ikonama datoteka unutar mapa označavajući tako da su u potpunosti zaštićene.

Dodavanje članova u krug povjerenja

Za dodavanje članova u krug povjerenja treba obaviti tri koraka:

1. **Pozovi**—Najprije vlasnik kruga povjerenja poziva člana(ove). E-poruka s pozivnicom može se poslati za više korisnika ili popisima primatelja/grupama.
2. **Prihvati**—Pozvani korisnik prima pozivnicu i bira hoće li je prihvatiti ili odbiti. Ako pozvani korisnik prihvatu pozivnicu šalje se e-poruka s odgovorom pozivatelju. Ako se pozivnica pošalje grupi svaki korisnik prima pozivnicu i odabire hoće li je prihvatiti ili odbiti.
3. **Unesi**—Pozivatelj ima završnu mogućnost odlučiti želi li dodati člana u krug povjerenja. Ako pozivatelj odluči unijeti člana pozvanom korisniku šalje se e-poruka s potvrdom odgovora. Pozivatelj i pozvani korisnik mogu, ako žele, provjeriti sigurnost postupka pozivanja. Kod za provjeru prikazuje se pozvanom korisniku i on ga pozivatelju mora pročitati preko telefona. Kada je kod provjeren pozivatelj može poslati finalnu e-poruku za unos.

Dodavanje članova u novi krug povjerenja:

▲ Tijekom stvaranja kruga povjerenja članove možete dodati tako da kliknite ili dodirnete ikonu **M+** pored **Članovi** i zatim slijedite upute na zaslonu.

- Ako upotrebljavate Outlook, odaberite kontakte iz adresara programa Outlook i zatim kliknite **U redu**
- Ako upotrebljavate neku drugu uslugu e-pošte ili ručno dodajte nove adrese e-pošte u Trust Circle ili ih možete dohvatiti iz adresa e-pošte registriranih u aplikaciji Trust Circle.

Dodavanje članova u postojeći krug povjerenja:

▲ Iz prikaza kruga povjerenja kliknite **Vaši krugovi povjerenja**, dva puta kliknite ili dva puta dodirnite postojeći krug povjerenja kako biste prikazali trenutačne članove, kliknite ili dodirnite ikonu **M+** pored **Članova**, a zatim pratite upute na zaslonu.

- Ako upotrebljavate Outlook, odaberite kontakte iz adresara programa Outlook i zatim kliknite **U redu**.
- Ako upotrebljavate neku drugu uslugu e-pošte ili ručno dodajte nove adrese e-pošte u Trust Circle ili ih možete dohvatiti iz adresa e-pošte registriranih u aplikaciji Trust Circle.

Dodavanje datoteka u krug povjerenja

Datoteke možete dodati u krug povjerenja na jedan od sljedećih načina:

- Kopirajte ili premjestite datoteke u postojeću mapu kruga povjerenja.

  – ili –

- U pregledniku Windows Explorer, kliknite desnom tipkom miša ili dodirnite i držite datoteku koja trenutačno nije šifrirana, odaberite **Trust Circle** i zatim odaberite **Šifriraj**. Od vas će se zatražiti da odaberete krug povjerenja u koji se datoteka treba dodati.

SAVJET: Možete odabrati jednu ili više datoteka

Šifrirane mape

Svaki član kruga povjerenja može pregledavati i uređivati datoteke koje pripadaju tom krugu povjerenja.

NAPOMENA: Upravitelj/čitač aplikacije Trust Circle ne sinkronizira datoteke između članova.

Datoteke se moraju dijeliti putem postojećih načina kao što su e-pošta, ftp ili davatelji usluge pohrane u oblaku. Datoteke koje su kopirane ili premještene u mapu kruga povjerenja ili stvorene u njoj odmah su zaštićene.

Uklanjanje mapa iz kruga povjerenja

Uklanjanjem mapa iz kruga povjerenja dešifrira se mapa i njezini sadržaji i uklanja se njihova zaštita.

- Iz prikaza kruga povjerenja kliknite **Vaši krugovi povjerenja**, dva puta kliknite ili dva puta dodirnite postojeći krug povjerenja kako biste prikazali trenutačne mape, kliknite ili dodirnite ikonu **koš za smeće** pored te mape.

  – ili –

- U pregledniku Windows Explorer, kliknite desnom tipkom miša ili dodirnite i držite mapu koja je trenutačno dio kruga povjerenja, odaberite **Trust Circle** i zatim odaberite **Ukloni iz kruga povjerenja**.

SAVJET: Možete odabrati jednu ili više mapa.

Uklanjanje datoteke iz kruga povjerenja

Za uklanjanje datoteke iz kruga povjerenja u pregledniku Windows Explorer, kliknite desnom tipkom miša ili dodirnite i držite datoteku koja trenutačno nije šifrirana, odaberite **Trust Circle**, odaberite **Dešifriraj datoteku**.

Uklanjanje članova iz kruga povjerenja

Član koji je bio u potpunosti unesen ne može se ukloniti iz kruga povjerenja. Alternativa bi bila stvaranje novog kruga povjerenja sa svim ostalim članovima, premještanje svih datoteka i mapa u novi krug povjerenja te zatim brisanje starog kruga povjerenja. Na taj će se način osigurati da sve nove datoteke koje član primi neće biti dostupne, ali sve što je ranije podijeljeno ostat će dostupno članu starog kruga povjerenja.

Ako član nije u potpunosti unesen (ili član nije pozvan u krug povjerenja ili nije prihvatio pozivnicu za krug povjerenja) možete ga ukloniti iz kruga povjerenja na jedan od sljedećih načina:

- Iz prikaza Trust Circle kliknite ili dodirnite **vaši krugovi povjerenja** i zatim dva puta kliknite ili dva puta dodirnite krug povjerenja kako bi se prikazao trenutačni popis članova. Kliknite ili dodirnite ikonu **koša za smeće** pored imena člana kojeg treba ukloniti.
- Iz prikaza Trust Circle kliknite ili dodirnite **Članovi** i zatim dva puta kliknite ili dva puta dodirnite člana kako bi se prikazali krugovi povjerenja u kojima je član. Kliknite ili dodirnite ikonu **koša za smeće** pored kruga povjerenja kako biste uklonili člana iz tog kruga povjerenja.

Brisanje kruga povjerenja

Za brisanje kruga povjerenja morate biti njegov vlasnik.

- ▲ Iz prikaza Trust Circle kliknite ili dodirnite **Vaši krugovi povjerenja**, kliknite ili dodirnite ikonu **koša za smeće** pored kruga povjerenja kojeg treba izbrisati.

  Na ovaj se način uklanja krug povjerenja sa stranice i svim se članovima kruga povjerenja šalje poruka e-pošte kojom ih se obavještava da je krug izbrisan. Sve datoteke ili mape koje su se nalazile u krugu povjerenja dešifrirane su.

Osobne postavke

Iz prikaza Trust Circle kliknite ili dodirnite **Postavke**. Prikazuju se tri kartice

- **Postavke e-pošte**

Opcija	Opis
Korisničko ime	Prikazuje se korisničko ime koje se trenutačno upotrebljava. Kako biste to promijenili unesite novo korisničko ime u tekstualni okvir. Promjene se automatski spremaju.
Adresa e-pošte	Prikazuje se adresa e-pošte koja se trenutačno upotrebljava. Za njezinu promjenu kliknite ili dodirnite **Promijeni postavke e-pošte** i zatim slijedite upute na zaslonu.
Potvrda novog člana	Odaberite među sljedećim opcijama: ◦ **Automatski potvrdi**—Nakon primanja prihvaćanja pozvanog(ih) korisnika oni se potvrđuju u krugu povjerenja bez ikakvog ručnog unosa i e-poruka potvrde šalje se pozvanom(im) korisniku(ima) ◦ **Ručno potvrdi**—Nakon primanja prihvaćanja pozvanog(ih) korisnika, obavezan je ručni unos za unošenje novih članova u krug povjerenja, a zatim se šalje e-poruka potvrde. ◦ **Potrebna je provjera**—Nakon primanja prihvaćanja pozvanog(ih) korisnika, potreban je kod za provjeru za potpuno unošenje pozvanog(ih) korisnika. Vlasnik kruga povjerenja mora kontaktirati pozvanog(e) korisnika(e) i od njih zatražiti kod za provjeru. Nakon unošenja ispravnog koda šalje se e-poruka potvrde.
Periodična provjera autentičnosti	Kod periodične provjere autentičnosti korisnik mora unijeti lozinku za sustav Windows nakon isteka određenog vremenskog razdoblja (snimljenog u minutama) i kada provodi osjetljive radnje. Ova postavka omogućuje korisnicima da uključe ili isključe provjeru autentičnosti.
Vremensko ograničenje za provjeru autentičnosti	Odaberite navedeno vremensko razdoblje (snimljeno u minutama) prije obavezne provjere autentičnosti.
Ne prikazuj poruku potvrde.	Odaberite potvrdni okvir kako biste onemogućili prikazivanje poruka potvrde ili očistite potvrdi okvir za prikazivanje poruka potvrde.
Želio/željela bih pomoći u poboljšavanju aplikacije HP Trust Circle kroz anonimno praćenje upotrebe	Odaberite potvrdni okvir za sudjelovanje u programu ili očistite potvrdni okvir ako ne želite sudjelovati.

- **Sigurnosna kopija/Vraćanje**

Opcija	Opis
Sigurnosno kopiranje	Kopira podatke aplikacije Upravitelj/čitač za Trust Circle (postavke i krugove povjerenja) u datoteku sigurnosne kopije. U slučaju pada ili kvara sustava ovu datoteku možete upotrijebiti za vraćanje svoje nove instalacije aplikacije Trust Circle na stanje spremljeno u datoteci. **NAPOMENA:** Spremaju se samo vaši podaci aplikacije Trust Circle (krugovi povjerenja, postavke i članovi). Trenutačne datoteke u mapama kruga povjerenja nisu sigurnosno kopirane. Ove se mape trebaju odvojeno sigurnosno kopirati. Za sigurnosno kopiranje postavi aplikacije Trust Circle i podataka korisnika: **1.** Kliknite ili dodirnite **Stvori sigurnosnu kopiju**. **2.** Odaberite naziv datoteke i direktorij datoteke sigurnosne kopije i zatim kliknite ili dodirnite **Spremi**. **3.** Unesite lozinku, potvrdite je i zatim kliknite ili dodirnite **U redu**. Ova će vam lozinka trebati za vraćanje ove datoteke.
Vraćanje	Vraća postavke i krugove povjerenja iz datoteke sigurnosne kopije obično nakon pada sustava ili migracije na drugo računalo. Za obnavljanje postavki aplikacije Upravitelja Trust Circle i podataka korisnika: **1.** Kliknite ili dodirnite **Vrati**. **2.** Odaberite direktorij i naziv datoteke sigurnosne kopije i zatim kliknite ili dodirnite **Otvori**. **3.** Unesite lozinku koja je postavljena prilikom izrade sigurnosne kopije.

- **O aplikaciji**—Prikazuje se verzija softvera Upravitelj/čitač za Trust Circle. Veze se prikazuju kako bi omogućile nadogradnju Upravitelja za Trust Circle na Pro verziju ili za prikaz Izjave o zaštiti privatnosti za HP.

9 Oporavak nakon krađe (samo odabrani modeli)

Computrace (kupuje se odvojeno) omogućuje vam daljinski nadzor, upravljanje i praćenje računala.

Nakon što se aktivira aplikacija Computrace konfigurira se s centra za korisnike Absolute Software. Iz centra za korisnike Absolute Software administrator može konfigurirati Computrace tako da nazire ili upravlja računalom. Ako se sustav zametne ili izgubi, centar za korisnike može pomoći lokalnoj policiji u pronalaženju i oporavku računala. Ako je konfigurirana, aplikacija Computrace može nastaviti s radom čak i ako se tvrdi disk izbriše ili zamjeni.

Za aktiviranje aplikacije Computrace:

1. Spojite se na internet.
2. Otvorite softver HP Client Security. Dodatne informacije potražite u odjeljku Otvaranje aplikacije HP Client Security na stranici 9.
3. Kliknite **Oporavak nakon krađe**.
4. Za pokretanje čarobnjaka za aktivaciju aplikacije Computrace, kliknite **Započni s radom**.
5. Unesite kontaktne podatke i podatke o plaćanju kreditnom karticom ili unesite unaprijed kupljeni Ključ proizvoda.

Čarobnjak za aktivaciju sigurno će obraditi transakciju i postaviti vaš korisnički račun na web-mjesto centra za korisnike Absolute Software. Kada se dovrši dobit ćete e-poruku potvrde koja sadrži podatke o vašem računu centra za korisnike.

Ako ste ranije pokrenuli čarobnjaka za aktivaciju Computrace i već imate postojeći račun centra za korisnike, dodatne licence možete kupiti tako da kontaktirate svojeg predstavnika za HP račun.

Za prijavu u centar za korisnike:

1. Idite na https://cc.absolute.com/.
2. U polja **ID prijave** i **Lozinka** unesite vjerodajnice koje ste dobili u e-poruci potvrde i zatim kliknite **Prijavi**.

Pomoću centra za korisnike možete:

- Nadzirati svoja računala.
- Zaštiti svoje udaljene podatke.
- Prijaviti krađu svakog računala zaštićenog aplikacijom Computrace.

▲ Kliknite **Saznaj više** za dodatne informacije o aplikaciji Computrace.

10 Iznimke lokalizirane lozinke

Na razini Provjera autentičnosti kod uključenja i na razini HP Drive Encryption ograničena je podrška za lokalizaciju lozinke. Dodatne informacije potražite u odjeljku IME alati za sustav Windows nemaju podršku na razini Provjera autentičnosti kod uključenja ili razini Drive Encryption na stranici 54.

Što napraviti kada se lozinka odbije

Lozinke se mogu odbiti iz nekog od sljedećih razloga:

- Korisnik upotrebljava IME za koji nema podršku. To je čest problem kod dvobajtnih jezika (korejski, japanski, kineski). Za rješavanje ovog problema:

  1. Upotrebom **Upravljačke ploče** dodajte podržani izgled tipkovnice (dodajte tipkovnice za SAD/Engleski za kineski kao ulazni jezik).
  2. Postavite podržane tipkovnice za unos po zadanim postavkama.
  3. Pokrenite HP Client Security i zatim unesite lozinku za sustav Windows.

- Korisnik upotrebljava znak za koji nema podršku. Za rješavanje ovog problema:

  1. Promijenite lozinku za sustav Windows tako da sadrži samo podržane znakove. Za više informacija o nepodržanim znakovima pogledajte Rukovanje posebnim tipkama na stranici 55.
  2. Pokrenite HP Client Security i zatim unesite lozinku za sustav Windows.

IME alati za sustav Windows nemaju podršku na razini Provjera autentičnosti kod uključenja ili razini Drive Encryption

U sustavu Windows korisnik može odabrati IME (urednika načina unosa) za unos složenih znakova i simbola kao što su japanski ili kineski znakovi upotrebnom standardne zapadnjačke tipkovnice.

IME alati nemaju podršku na razini Provjera autentičnosti kod uključenja ili razini Drive Encryption Lozinka za sustav Windows ne može se unijeti pomoću alata IME na kod povjere autentičnosti kod uključenja i na zaslonu za prijavu aplikacije HP Drive Encryption, a ako se to pokuša to može dovesti do prekida rada. U nekim slučajevima, Microsoft® Windows ne prikazuje IME kada korisnici unose lozinku.

Rješenje je prebaciti se na jedan od sljedećih podržanih rasporeda tipkovnice koji prevodi raspored tipkovnice 00000411:

- Microsoft IME za japanski
- Raspored tipkovnice za japanski
- Office 2007 IME za japanski—Ako tvrtka Microsoft ili treća strana upotrebljava naziv IME ili urednika za način unosa, urednik za način unosa možda zapravo neće biti IME. Ovo može dovesti do konfuzije, no softver čita predstavljanje heksadecimalnog koda. Zbog toga ako se IME prikazuje na podržanom rasporedu tipkovnice, tada HP Client Security može podržati konfiguraciju.

UPOZORENJE! Kada se uvede HP Client Security lozinke unesene pomoću alata IME sustava Windows bit će odbijene.

Promjene lozinke pomoću rasporeda tipkovnice koji je također podržan

Ako se lozinka početno postavi pomoću jednog rasporeda tipkovnice kao što je SAD engleski (409) i zatim korisnik promijeni lozinku koristeći tipkovnicu s drugačijim rasporedom koji se također podržava kao što je latinskoamerička (080A), promjena lozinke djelovat će u aplikaciji HP Drive Encryption, ali ne i u BIOS-u ako korisnik upotrijebi znakove koji postoje na potonjoj tipkovnici, ali ne i na prvotnoj tipkovnici (npr., ē).

NAPOMENA: Administratori mogu ovaj problem riješiti upotrebom stranice Korisnici aplikacije HP Client Security (kojoj se pristupa s ikone **Zupčanik** na početnoj stranici) za uklanjanje korisnika iz aplikacije HP Client Security odabirući željeni raspored tipkovnice u operacijskom sustavu i zatim ponovnim pokretanjem čarobnjaka za postavljanje aplikacije HP Client Security za istog korisnika. BIOS pohranjuje željeni raspored tipkovnice i lozinke koje se mogu upisivati na ovom rasporedu tipkovnice bit će ispravno postavljeni u BIOS-u.

Drugi mogući problem je upotreba drugačijih rasporeda tipkovnice koji svi mogu stvoriti iste znakove. Na primjer i SAD međunarodni raspored tipkovnice (20409) i latinskoamerički raspored tipkovnice (080A) mogu proizvesti znak é, iako će možda trebati primijeniti drugačiji slijed tipki. Ako je lozinka početno postavljena pomoću latinskoameričkog rasporeda tipkovnice, tada se latinskoamerički raspored tipkovnice postavlja u BIOS, čak i ako se lozinka naknadno promijeni upotrebom SAD međunarodnog rasporeda tipkovnice.

Rukovanje posebnim tipkama

- Kineski, slovački, kanadski francuski i češki

  Kada korisnik odabere jedan od prethodnih rasporeda tipkovnice i zatim unese lozinku (na primjer, abcdef), ista se lozinka mora unijeti dok pritišće tipku shift za mala slova i tipku shift i tipku caps lock za velika slova u Provjeri autentičnosti kod uključenja i HP Drive Encryption. Brojčane lozinke moraju se unijeti pomoću numeričke tipkovnice.

- Korejski

  Kada korisnik odabere jedan od podržanih rasporeda korejske tipkovnice i zatim unese lozinku, ista se lozinka mora unijeti dok pritišće desnu tipku alt za mala slova i desnu tipku alt i tipku caps lock za velika slova u Provjeri autentičnosti kod uključenja i HP Drive Encryption.

- Nepodržani znakovi popisani su u sljedećoj tablici:

Jezik	Windows	BIOS	Drive Encryption
Arapski	Tipke ﻷ ,ﻹ i ﻵ stvaraju dva znaka.	Tipke ﻷ ,ﻹ i ﻵ stvaraju jedan znak.	Tipke ﻷ ,ﻹ i ﻵ stvaraju jedan znak.
Kanadski francuski	ç, è, à, i é s tipkom caps lock su Ç, È, À, i É u sustavu Windows.	ç, è, à, i é s tipkom caps lock su ç, è, à, i é u aplikaciji Provjera autentičnosti kod uključenja.	ç, è, à, i é s tipkom caps lock su ç, è, à, i é u aplikaciji HP Drive Encryption.

Jezik	Windows	BIOS	Drive Encryption
Španjolski	40a se ne podržava. Pa ipak radi jer ga softver pretvara u c0a. Međutim zbog suptilne razlike između rasporeda tipkovnica preporučuje se da korisnici sa španjolskog govornog područja promijene raspored svoje tipkovnice za sustav Windows u 1040a (španjolska varijanta) ili 080a (latinskoamerička).	nije dostupno	nije dostupno
SAD međunarodna	◦ Ne prihvaćaju se tipke ¡, ¤, ‘, ’, ¥ i × iz gornjeg reda. ◦ Ne prihvaćaju se tipke å, ® i Þ iz drugog reda. ◦ Ne prihvaćaju se tipke á, ð i ø iz trećeg reda. ◦ Ne prihvaća se tipka æ iz donjeg reda.	nije dostupno	nije dostupno
Češki	◦ Ne prihvaća se tipka ğ ◦ Ne prihvaća se tipka į. ◦ Ne prihvaća se tipka ų. ◦ Ne prihvaćaju se tipke ė, ı i ż ◦ Ne prihvaćaju se tipke ģ, ķ, ļ, ņ i ţ.	nije dostupno	nije dostupno
Slovački	Ne prihvaća se tipka ż.	◦ Tipke š, ś i ş ne prihvaćaju se dok se upisuju, ali se prihvaćaju kada se unesu pomoću softverske tipkovnice. ◦ Mrtva tipka ţ stvara dva znaka.	nije dostupno
Mađarski	Ne prihvaća se tipka ż.	Tipka ţ stvara dva znaka.	nije dostupno
Slovenski	Tipka żŻ ne prihvaća se u sustavu Windows, a tipka alt stvara mrtvu tipku u BIOS-u.	Tipke ú, Ú, ů, Ů, ş, Ş, ś, Ś, š i Š ne prihvaćaju se u BIOS-u.	nije dostupno
Japanski	Kada je dostupan, alat Microsoft Office 2007 IME predstavlja bolji izbor. Unatoč nazivu IME radi se zapravo o rasporedu tipkovnice 411 koja je podržana.	nije dostupno	nije dostupno

Pojmovnik

administrator
Pogledajte *Administrator sustava Windows*.

administrator sustava Windows
Korisnik sa svim pravima za mijenjanje dozvola i upravljanje ostalim korisnicima.

aktivacija
Zadatak se mora dovršiti prije nego što postanu dostupne značajke softvera Drive Encryption. Administratori mogu aktivirati softver Drive Encryption pomoću čarobnjaka za postavljanje HP sigurnosnog klijenta ili aplikacije HP Client Security. Postupak aktivacije sastoji se od aktiviranja softvera, šifriranja pogona i stvaranje početne sigurnosne kopije ključa za šifriranje na uklonjivom uređaju za pohranu.

arhiva za hitni oporavak
Zaštićeno područje pohranjivanja koje omogućuje ponovno šifriranje osnovnih korisničkih ključeva s jedne platforme vlasnika ključa na drugu.

automatsko trajno brisanje
Trajno brisanje koje zakazujete u programu File Sanitizer.

beskontaktna kartica
Plastična kartica koja sadrži računalni čip koji se može upotrijebiti za provjeru autentičnosti.

blizinska kartica
Plastična kartica koja sadrži računalni čip koji se može upotrijebiti za provjeru autentičnosti zajedno s ostalim vjerodajnicama za dodatnu sigurnost.

Bluetooth
Tehnologija koja upotrebljava radio prijenos za omogućavanje računala, pisača, miševa, mobilnih telefona koji podržavaju Bluetooth i za druge uređaje za bežičnu komunikaciju na malim udaljenostima.

čišćenje praznog prostora
Upisivanje nasumičnih podataka preko izbrisane imovine i nekorištenog prostora. Ovaj postupak umanjuje postojanje izbrisane imovine tako da je originalnu imovinu teže oporaviti.

dešifriranje
Postupak koji se upotrebljava u kriptografiji za pretvaranje šifriranih podataka u običan tekst.

domena
Grupa računala koja su dio mreže i dijele zajedničku bazu podataka direktorija. Domene imaju jedinstvene nazive i svaka ima svoj set pravila i postupaka.

Drive Encryption
Štiti podatke šifriranjem tvrdog diska i na taj ih način čini nečitljivima osobama koje nemaju odgovarajuće ovlasti.

DriveLock
Sigurnosna značajka koja povezuje tvrdi disk s korisnikom u traži od korisnika točan unos lozinke za DriveLock kada se računalo pokrene.

grupa
Grupa korisnika koja ima istu razinu pristupa ili mu je uskraćena klasa uređaja ili određeni uređaj.

identitet

U softveru HP sigurnost klijenta grupa vjerodajnica i postavki kojima se rukuje kao računom ili profilom za određenog korisnika.

ID kartica
Programčić radne površine sustava Windows koji služi za vizualno prepoznavanje radne površine s vašim korisničkim imenom i odabranom slikom.

jedinstvena prijava
Značajka koja sprema podatke o autentičnosti i omogućuje vam upotrebu softvera HP Client Security za pristup internetu i aplikacijama sustava Windows za koje je potrebna provjera autentičnosti lozinkom.

klasa uređaja
Svi uređaji određene vrste kao što su pogoni.

korisnički račun u sustavu Windows
Korisnik kojem je dozvoljeno prijavljivanje na mrežu ili na pojedino računalo.

korisnik
Osobe unesene u Drive Encryption (šifriranje pogona). Korisnici koji nisu administratori imaju ograničena prava u značajki Drive Encryption (šifriranje pogona). Mogu samo unijeti svoje podatke (uz odobrenje administratora) i prijaviti se.

Mapa Trust Circle
Sve mape zaštićene u krugu povjerenja.

metoda zaštićene prijave
Način prijave na računalo.

mrežni račun
Račun korisnika ili administratora sustava Windows bilo na lokalnom računalu, radnoj grupi ili na domeni.

Opcija Just In Time Authentication
Pogledajte Pomoć za softver HP Device Access Manager.

Oporavak uslužnog programa HP SpareKey
Mogućnost pristupa računalu točnim odgovorima na sigurnosna pitanja.

otisak prsta
Digitalno izdvajanje slike otiska prsta. Slika stvarnog otiska prsta nikada se ne pohranjuje u aplikaciji HP Client Security.

pametna kartica
Hardverski uređaj koji se s PIN-om može upotrijebiti za provjeru autentičnosti.

PIN
Osobni identifikacijski broj za unesenog korisnika koje se upotrebljava za provjeru autentičnosti.

PKI
Standard Public Key Infrastructure, koji definira sučelja za stvaranje, korištenje i administriranje ključeva za certifikate i šifriranje.

Početna stranica
Središnje mjesto gdje možete pristupiti i upravljati značajkama i postavkama u aplikaciji HP Client Security.

ponovno pokretanje
Postupak ponovnog pokretanja računala.

pravila upravljanja pristupom uređajima
Popis uređaja za koje je korisniku dozvoljen ili uskraćen pristup.

prijava

Objekt unutar aplikacije HP Client Security koji se sastoji od korisničkog imena i lozinke (i uz moguće druge odabrane informacije) koje se mogu upotrijebiti za prijavu na web-mjesta ili druge programe.

provjera autentičnosti
Postupak provjere da ste vi upravo osoba za koju se predstavljate kroz upotrebu vjerodajnica uključujući lozinku za sustav Windows, otisak prsta, pametnu karticu, beskontaktnu karticu ili blizinsku karticu.

Provjera autentičnosti prije pokretanja softvera Drive Encryption
Zaslon za prijavu koji se prikazuje prije pokretanja sustava Windows. Korisnici moraju unijeti svoje korisničko ime i lozinku za sustav Windows ili PIN pametne kartice ili prijeći registriranim prstom. Ako se odabere prijava u jednom koraku, unosom točnih informacija na početnom zaslonu softvera Drive Encryption omogućuje se izravan pristup sustavu Windows, a da se ne mora ponovno prijaviti na zaslonu za prijavu sustava Windows.

provjera pri uključivanju
Sigurnosna značajka koja, kada je računalo uključeno, traži neki oblik provjere autentičnosti kao što su pametna kartica, sigurnosni čip ili lozinka.

ručno trajno brisanje
Trenutačno trajno brisanje imovine ili odabrane imovine kojim se premošćuje zakazano trajno brisanje.

sigurnosna kopija
Upotreba značajke sigurnosnog kopiranja za spremanje kopije podataka o važnom programu na mjesto izvan programa. Ona se zatim može upotrijebiti za naknadno vraćanje podataka na isto ili drugo računalo.

Sigurnosna prijava u sustav Windows
Štiti vaše račune u sustavu Windows pomoću određenih vjerodajnica za pristup.

spojeni uređaj
Hardverski uređaj koji je spojen na priključak na računalu.

Sustav za šifriranje datoteka (EFS)
Sustav koji šifrira sve datoteke i podmape u odabranoj mapi.

šifriranje
Postupak, kao što je upotreba algoritma, koji se promjenjuje u kriptografiji za pretvaranje običnog teksta u šifrirani tekst kako bi se spriječilo da neovlašteni primatelji čitaju te podatke. Postoji puno načina šifriranja podataka i oni su temelj mrežne sigurnosti. Česte vrste šifriranja uključuju standardne načine šifriranja podataka i šifriranje javnim ključem.

šifriranje hardvera
Upotreba samošifrirajućih pogona koji ispunjavaju zahtjeve OPAL organizacije Trusted Computing Group za upravljanje samošifrirajućim pogonom za dovršavanje trenutačnog šifriranja. Šifriranje hardvera je trenutačno i može potrajati svega nekoliko minuta, no šifriranje softvera može potrajati nekoliko sati.

šifriranje softvera
Upotreba softvera kako bi se šifrirao sektor po sektor tvrdog pogona. Postupak je sporiji od šifriranja hardvera

trajno brisanje
Provođenje algoritma kojim se podaci koji se nalaze u zapisima prepisuju besmislenim podacima.

Trust Circle
Omogućuju zaustavljanje podataka povezujući podatke u definiranu grupu povjerljivih korisnika. Na ovaj se način sprječava da podaci dospiju u krive ruke bilo slučajno bilo namjerno. Zaštićeni tehnologijom CryptoMill's Zero Overhead Key Management podaci se kriptografski povezuju u krug povjerenja. Ovime se sprječava dešifriranje dokumenata ili drugih osjetljivih podataka izvan kruga povjerenja

Uloženi sigurnosni čip modula Trusted Platform (TPM)
TPM provjerava autentičnost računala radije nego korisnika spremajući posebne podatke koji se odnose na glavno računalo kao to su tipke za šifriranje, digitalni podaci i lozinke TPM umanjuje opasnost da će se informacije na računalu ugroziti fizičkom krađom ili napadom vanjskog hakera.

Upravitelj/čitač za Trust Circle
Čitač aplikacije Trust Circle može prihvaćati samo pozivnice koje šalju korisnicu Upravitelja za Trust Circle. Međutim, Upravitelj za Trust Circle omogućuje stvaranje krugova povjerenja. Značajka uključuje pozivanja osobe puten e-pošte u krug povjerenja i prihvaćanja pozivnica za krug povjerenja drugih osoba. Kada se među ravnopravnim članovima uspostavi krug povjerenja, datoteke zaštićene krugom povjerenja mogu se sigurno dijeliti.

vjerodajnice
Poseban dio podataka ili hardverski uređaj koji se upotrebljava za provjeru autentičnosti pojedinačnog korisnika.

vraćanje
Postupak koji kopira podatke programa iz u tom programu prethodno spremljene datoteke sigurnosne kopije.

zapis
Komponenta podataka koja se sastoji od osobnih podataka ili datoteka, podatka o povijesti ili podataka vezanih uz web, itd. koji se nalaze na tvrdom disku.

zaslon za prijavu za šifriranje pogona
Pogledajte provjeru autentičnosti prije pokretanja softvera Drive Encryption.

Kazalo