HP Client Security

Prvi koraci

Prvo izdanje: avgust 2013.

Broj dela dokumenta: 735339-E31

Sadržaj

1 Uvod u program HP Client Security Manager

HP Client Security omogućava vam da zaštitite svoje podatke, uređaj i identitet i tako povećate bezbednost vašeg računara.

Softverski moduli dostupni za vaš računar mogu se razlikovati u zavisnosti od vašeg modela.

HP Client Security softverski moduli mogu da budu unapred instalirani, učitani ili mogu da se preuzmu sa HP veb-sajta. Više informacija potražite u odeljku http://www.hp.com.

NAPOMENA: Uputstva u ovom vodiču su napisana pod pretpostavkom da ste već instalirali primenljive softverske module za HP Client Security.

Funkcije softvera HP Client Security

U tabeli koja sledi navedeni su detalji o ključnim funkcijama HP Client Security modula.

Modul	Ključne funkcije
HP Client Security Manager	Administratori mogu da koriste sledeće funkcije da bi: • Zaštitili računar pre nego što se Windows® pokrene • Zaštitili Windows nalog pomoću bezbedne provere identiteta • Upravljali korisničkim imenima i lozinkama za prijavljivanje na veb-sajtove i aplikacije • Lako promenili lozinke za operativni sistem Windows® • Koristili otiske prstiju radi veće bezbednosti i praktičnosti • Podesili pametne kartice, beskontaktne kartice ili proximity kartice za korišćenje prilikom provere identiteta • Koristili Bluetooth telefon kao metod identifikacije • Podesili PIN da biste proširili opcije provere identiteta • Konfigurisali smernice prijavljivanja i sesija • Pravili rezervne kopije podataka iz programa i obnovili ih • Dodali još aplikacija, kao što su HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager i HP Computrace Opšti korisnici mogu da koriste sledeće funkcije da bi: • Prikazali postavke za Encryption Status i Device Access Manager • Aktivirali Computrace • Konfigurisali Preferences (Željene postavke) i Backup and Restore (Rezervne kopije i vraćanje)

Modul	Ključne funkcije
Password Manager	Opšti korisnici mogu da koriste sledeće funkcije da bi: • Organizovali i konfigurisali korisnička imena i lozinke • Kreirali jače lozinke za poboljšanu bezbednost naloga za e-poštu i veb naloge; Password Manager automatski popunjava i šalje podatke • Organizovali proces prijavljivanja sa funkcijom Single Sign On, koja automatski pamti i primenjuje akreditive korisnika • Označili nalog kao ugrožen tako da se i za drugi nalog(e) sa sličnim akreditivma šalje upozorenje • Uvozili podatke za prijavljivanje iz podržanog pretraživača
HP Drive Encryption (samo na odabranim modelima)	• Pruža potpuno šifrovanje čitavog kapaciteta čvrstog diska. • Nameće autorizaciju pre dizanja sistema zbog dešifrovanja i pristupa podacima. • Nudi opciju aktiviranja disk jedinica sa sopstvenim šifrovanjem (samo na odabranim modelima)
HP Device Access Manager	• Omogućuje IT menadžerima da kontrolišu pristup uređajima na osnovu korisničkih profila. • Sprečava da neovlašćeni korisnici uklanjaju podatke pomoću spoljašnjih medija za skladištenje i uvođenje virusa u sistem sa spoljašnjih medija. • Omogućuje administratorima da onemoguće pristup uređajima za komunikaciju za određene pojedince ili grupe korisnika.
HP Trust Circles	• Pruža bezbednost datoteka i dokumenata. • Šifruje datoteke smeštene u fascikle koje je izabrao korisnik i štiti ih u okviru kruga poverenja. • Omogućuje da članovi u krugu poverenja koriste i razmenjuju datoteke.
Vraćanje u slučaju krađe (Computrace, kupuje se posebno)	• Zahteva posebnu kupovinu pretplata za praćenje i lociranje da bi se aktivirao. • Obezbeđuje bezbedno praćenje imovine. • Prati aktivnost korisnika, kao i izmene u hardveru i softveru. • Ostaje aktivan čak i ako se čvrsti disk ponovo formatira ili zameni.

Opis proizvoda HP Client Security i primeri uobičajene upotrebe

Većina HP Client Security proizvoda ima i potvrdu identiteta korisnika (obično lozinku) i administrativnu rezervnu kopiju za dobijanje pristupa ako se lozinke izgube, ako su nedostupne, zaboravljene ili kad god je korporativnom obezbeđenju potreban pristup.

NAPOMENA: Neki od HP Client Security proizvoda napravljeni su da ograničavaju pristup podacima. Podatke bi trebalo šifrovati kada su toliko važni da bi korisnik radije izgubio informacije nego dozvolio da budu ugroženi. Preporučljivo je da se na bezbednoj lokaciji napravi rezervna kopija svih podataka.

Password Manager

Password Manager čuva korisnička imena i lozinke i može se koristiti za:

- čuvanje korisničkih imena i lozinki za pristup internetu ili e-pošti
- automatsko prijavljivanje korisnika na veb-sajt ili e-poštu
- upravljanje i organizovanje podataka za potvrdu identiteta
- biranje veb ili mrežnog sredstva i direktan pristup vezi
- prikaz imena i lozinki kada je neophodno
- označavanje naloga kao ugroženog tako da se i za drugi nalog(e) sa sličnim akreditivma šalje upozorenje
- uvoz podataka za prijavljivanje iz podržanog pretraživača

Primer 1: Agent za nabavke za velikog proizvođača najveći broj korporativnih transakcija obavlja preko interneta. Takođe često posećuje nekoliko popularnih veb-sajtova koji zahtevaju informacije za prijavu. Ona veoma vodi računa o bezbednosti i zato ne koristi istu lozinku za svaki nalog. Agent za nabavke odlučuje da koristi Password Manager da poveže veze na vebu sa različitim korisničkim imenima i lozinkama. Kada ode na veb-sajt da se prijavi, Password Manager automatski unese akreditive. Ako želi da pregleda korisnička imena i lozinke, Password Manager može da se konfiguriše tako da ih prikazuje.

Password Manager takođe može da se koristi za upravljanje i organizovanje podataka za potvrdu identiteta. Ova alatka će omogućiti korisniku da izabere veb ili mrežno sredstvo i da direktno pristupi vezi. Korisnik takođe može po potrebi da pregleda korisnička imena i lozinke.

Primer 2: Vredan zaposleni je unapređen i sada upravlja čitavim odeljenjem knjigovodstva. Tim mora da se prijavljuje na veliki broj veb naloga klijenata, a svaki od naloga koristi drugačije informacije za prijavljivanje. Ove informacije za prijavljivanje moraju da se dele sa drugim radnicima, pa poverljivost predstavlja problem. Zaposleni odlučuje da organizuje sve veb veze, korisnička imena i lozinke u kompaniji u okviru programa Password Manager. Kada je sve to uradio, zaposleni daje radnicima da koriste Password Manager kako bi mogli da rade na veb nalozima i nikada ne saznaju akreditive koje koriste.

HP Drive Encryption (samo na odabranim modelima)

HP Drive Encryption se koristi za ograničavanje pristupa podacima na čitavom čvrstom disku računara ili na sekundarnoj disk jedinici. Drive Encryption takođe može da upravlja disk jedinicama sa sopstvenim šifrovanjem.

Primer 1: Lekar želi da bude siguran da samo on može da pristupa podacima na čvrstom disku njegovog računara. Lekar aktivira Drive Encryption koji zahteva autorizaciju pre dizanja sistema pre prijavljivanja na Windows. Kada se podesi, čvrstom disku se više ne može pristupiti bez lozinke pre nego što se operativni sistem pokrene. Lekar bi mogao dodatno da poboljša bezbednost disk jedinice tako što će izabrati da šifruje podatke sa opcijom disk jedinice sa sopstvenim šifrovanjem.

Primer 2: Administrator u bolnici želi da bude siguran da samo lekari i ovlašćeno osoblje mogu da pristupaju podacima na lokalnom računaru i da pri tom ne dele lične lozinke. IT odeljenje dodaje administratora, lekare i svo ovlašćeno osoblje kao korisnike programa Drive Encryption. Sada samo ovlašćeno osoblje može da pokreće računar ili domen koristeći lično korisničko ime i lozinku.

HP Device Access Manager (samo na odabranim modelima)

HP Device Access Manager omogućuje administratoru da ograniči i upravlja pristupom hardveru. Device Access Manager može da se koristi da blokira neovlašćen pristup USB fleš diskovima na koje

mogu da se kopiraju podaci. Takođe može da ograniči pristup CD/DVD jedinicama, da kontroliše USB uređaje, mrežne veze, i tako dalje. Jedan od primera bila bi situacija u kojoj spoljni dobavljači moraju da pristupaju računarima u kompaniji, ali ne bi trebalo da imaju mogućnost da kopiraju podatke na USB disk jedinicu.

Primer 1: Menadžer kompanije za medicinsku opremu često pored informacija o kompaniji u radu koristi lične zdravstvene kartone. Zaposlenima je potreban pristup ovim podacima, međutim, izuzetno je važno da se ovi podaci ne uklanjaju iz računara preko USB disk jedinice ili bilo kog drugog spoljašnjeg medija za skladištenje podataka. Mreža je bezbedna, ali računari imaju CD rezače i USB portove koji bi mogli da omoguće kopiranje ili krađu podataka. Menadžer koristi Device Access Manager da onemogući USB portove i CD rezače kako ne bi mogli da se koriste. Iako su USB portovi blokirani, miš i tastature će i dalje funkcionisati.

Primer 2: Osiguravajuće društvo ne želi da njegovi zaposleni instaliraju ili učitavaju lični softver ili podatke od kuće. Nekim zaposlenima je potreban pristup USB portu na svim računarima. IT menadžer koristi Device Access Manager da omogući pristup za neke zaposlene i blokira spoljašnji pristup za druge.

Computrace (kupuje se posebno)

Computrace (kupuje se posebno) je usluga koja može da prati lokaciju ukradenog računara kad god korisnik pristupi internetu. Computrace takođe može da pomogne da daljinski upravljate i locirate računare, kao i da pratite korišćenje računara i aplikacije.

Primer 1: Direktor škole je naložio IT odeljenju da vodi evidenciju o svim računarima u školi. Nakon što je napravljen popis računara, IT administrator je registrovao sve računare sa Computrace-om kako bi mogli da se prate u slučaju krađe. Nedavno je u školi primećeno da nekoliko računara nedostaje, pa je IT administrator o tome obavestio vlasti i zvaničnike iz Computrace-a. Vlast je pronašla računare i vratila ih školi.

Primer 2: Kompanija koja se bavi nekretninama mora da organizuje i ažurira računare širom sveta. Oni koriste Computrace da bi pratili i ažurirali računare a da ne moraju da šalju IT stručnjaka do svakog računara.

Postizanje ključnih bezbednosnih ciljeva

HP Client Security moduli mogu da rade zajedno da bi obezbedili rešenja za niz bezbednosnih problema, uključujući sledeće ključne bezbednosne ciljeve:

- Zaštita od ciljane krađe
- Ograničavanje pristupa osetljivim podacima
- Sprečavanje neovlašćenog pristupa unutrašnjim ili spoljašnjim lokacijama
- Kreiranje smernica za jake lozinke

Zaštita od ciljane krađe

Primer ciljane krađe bila bi krađa računara koji sadrži poverljive podatke i informacije o klijentima na kontrolnom punktu aerodromskog obezbeđenja. Sledeće funkcije će vas zaštititi od ciljane krađe:

- Funkcija autorizacije pre dizanja sistema, ako je omogućena, pomaže da se spreči pristup operativnom sistemu.
  - HP Client Security—videti HP Client Security na stranici 12.
  - HP Drive Encryption—videti HP Drive Encryption (samo na odabranim modelima) na stranici 30.
- Šifrovanje pomaže da obezbedite da podacima ne može da se pristupi čak i ako se čvrsti disk ukloni i instalira na neobezbeđenom sistemu.
- Computrace može da locira računar nakon krađe.
  - Computrace—videti Vraćanje u slučaju krađe (samo na odabranim modelima) na stranici 54.

Ograničavanje pristupa osetljivim podacima

Pretpostavimo da revizor po ugovoru radi u prostorijama kompanije i da je dobio pristup računaru da bi pregledao osetljive finansijske podatke. Ne želite da revizor može da odštampa datoteke ili da ih sačuva na uređaju za memorisanje podataka, kao što je CD. Sledeća funkcija pomaže da se ograniči pristup podacima:

- HP Device Access Manager omogućuje IT menadžerima da ograniče pristup uređajima za komunikaciju kako osetljive informacije ne bi mogle da se kopiraju sa čvrstog diska. Pogledajte odeljak Sistemski prikaz na stranici 44.

Sprečavanje neovlašćenog pristupa unutrašnjim ili spoljašnjim lokacijama

Neovlašćen pristup neobezbeđenom poslovnom računaru predstavlja veoma stvaran rizik za korporativne mrežne resurse, kao što su informacije iz finansijskih službi, izvršnog, istraživačkog i razvojnog tima, i za privatne informacije, kao što su kartoni pacijenata ili lični finansijski podaci. Sledeće funkcije pomažu da se spreči neovlašćen pristup:

- Funkcija autorizacije pre dizanja sistema, ako je omogućena, pomaže da se spreči pristup operativnom sistemu. (pogledajte odeljak HP Drive Encryption (samo na odabranim modelima) na stranici 30.
- HP Client Security pomaže da obezbedite da neovlašćeni korisnik ne može da dobije lozinke ili pristup aplikacijama zaštićenim lozinkama. Pogledajte odeljak HP Client Security na stranici 12.
- HP Device Access Manager omogućuje IT menadžerima da ograniče pristup uređajima za skladištenje podataka kako osetljive informacije ne bi mogle da se kopiraju sa čvrstog diska. Pogledajte odeljak HP Device Access Manager (samo na odabranim modelima) na stranici 43.

Kreiranje smernica za jake lozinke

Ako na snagu stupi politika kompanije koja zahteva primenu smernica za jake lozinke za desetine veb aplikacija i baza podataka, Password Manager pruža zaštićeno spremište za lozinke i praktičnu funkciju Single Sign On (Jedno prijavljivanje). Pogledajte odeljak Password Manager na stranici 18.

Dodatni bezbednosni elementi

Dodela bezbednosnih uloga

Kod upravljanja bezbednošću računara (naročito kod velikih organizacija), važnu praksu predstavlja podela odgovornosti i prava na više različitih tipova administratora i korisnika.

NAPOMENA: U malim organizacijama ili kod pojedinačne upotrebe, sve ove uloge može imati ista osoba.

Kod HP Client Security bezbednosne dužnosti i privilegije mogu da se podele na sledeće uloge:

- Stručni saradnik za bezbednost—definiše nivo bezbednosti za kompaniju ili mrežu i određuje bezbednosne funkcije koje će se primenjivati, na primer Drive Encryption (Šifrovanje disk jedinice).

  NAPOMENA: Stručni saradnik za bezbednost u saradnji sa HP-om može da prilagodi mnoge od funkcija u programu HP Client Security. Više informacija potražite u odeljku http://www.hp.com.

- IT administrator—primenjuje i organizuje bezbednosne funkcije koje je definisao stručni saradnik za bezbednost. Takođe može da omogući ili onemogući neke funkcije. Na primer, ako stručni saradnik za bezbednost odluči da koristi pametne kartice, IT administrator može da omogući i režim lozinke i režim pametne kartice.

- Korisnik—koristi bezbednosne funkcije. Na primer, ako stručni saradnik za bezbednost i IT administrator omoguće na sistemu pametne kartice, korisnik može da podesi PIN za pametnu karticu i da koristi karticu za potvrdu identiteta.

OPREZ: Administratori se podstiču da se pridržavaju „najboljih praksi“ u ograničavanju privilegija krajnjeg korisnika i ograničavanju pristupa korisnicima.

Neovlašćeni korisnici ne bi trebalo da imaju administratorske privilegije.

Upravljanje HP Client Security lozinkama

Većina funkcija programa HP Client Security je obezbeđena lozinkama. U tabeli koja sledi nalaze se lozinke koje se obično koriste, softverski modul u kome se lozinka podešava i funkcija lozinke.

U tabeli su takođe označene lozinke koje podešavaju i koriste samo IT administratori. Sve ostale lozinke mogu da podešavaju obični korisnici ili administratori.

HP Client Security lozinka	Podešava se u sledećem modulu	Funkcija
Lozinka za prijavu u Windows	Windows kontrolna tabla ili HP Client Security	Može da se koristi za ručno prijavljivanje i za potvrdu identiteta za pristup različitim funkcijama programa HP Client Security.

HP Client Security lozinka	Podešava se u sledećem modulu	Funkcija
Lozinka za HP Client Security Backup and Recovery (Rezervna kopija i spasavanje)	HP Client Security, pojedinačni korisnik	Štiti od pristupa datoteci HP Client Security Backup and Recovery (Rezervna kopija i spasavanje).
PIN za pametnu karticu	Credential Manager (Upravljač akreditivima)	Može se koristiti za potvrdu identiteta sa više činilaca. Može da se koristi za potvrdu identiteta u Windows-u. Potvrđuje identitet korisnika programa Drive Encryption ako se izabere pametna kartica.

Kreiranje bezbedne lozinke

Kada kreirate lozinke, prvo se morate pridržavati svih specifikacija koje određuje program. Generalno bi trebalo da imate u vidu sledeće smernice koje vam pomažu da kreirate jake lozinke i smanjite šansu da vaša lozinka bude ugrožena:

- Koristite lozinke koje su duže od 6 karaktera, po mogućnosti duže od 8.
- Lozinka treba da bude sastavljena od pomešanih velikih i malih slova.
- Kad god je to moguće, mešajte alfanumeričke znakove i uključite specijalne znakove i znakove interpunkcije.
- Umesto slova u ključnoj reči koristite specijalne znakove ili brojeve. Na primer, umesto slova I ili L možete koristiti broj 1.
- Kombinujte reči iz 2 ili više jezika.
- Ubacite u sredinu reči ili fraze brojeve ili specijalne znakove, na primer, „Mary2-2Cat45“.
- Nemojte da koristite lozinku koja bi mogla da se nađe u rečniku.
- Nemojte da kao lozinku koristite svoje ime, ili neke druge lične informacije, kao što su rođendan, imena ljubimaca, majčino devojačko ime, čak i ako su te reči napisane unazad.
- Redovno menjajte lozinke. Možete da promenite samo nekoliko znakova koji su uzastopni.
- Ako zapisujete svoju lozinku, ne čuvajte je na lako uočljivom mestu, veoma blizu računara.
- Ne čuvajte lozinku u datoteci, kao što je e-poruka, na računaru.
- Ne delite naloge i ne otkrivajte nikome svoju lozinku.

Pravljenje rezervne kopije akreditiva i postavki

Alatku Backup and Recovery (Rezervna kopija i spasavanje) u programu HP Client Security možete da koristite kao centralnu lokaciju sa koje možete da pravite rezervne kopije i spasavate akreditive za neke od instaliranih HP Client Security modula.

2 Prvi koraci

Da biste konfigurisali program HP Client Security za korišćenje sa vašim akreditivima, pokrenite HP Client Security na neki od sledećih načina. Kada korisnik jednom završi čarobnjaka, taj korisnik više neće moći ponovo da ga pokrene.

1. Na početnom ekranu ili ekranu sa aplikacijama, kliknite ili dodirnite aplikaciju **HP Client Security** (Windows 8).

   – ili –

   Na Windows radnoj površini, kliknite ili dodirnite stavku **HP Client Security Gadget** (Gadžet za HP Client Security) (Windows 7).

   – ili –

   Na Windows radnoj površini, dvaput kliknite ili dodirnite dvaput ikonu **HP Client Security** u polju za obaveštavanje, koje se nalazi u desnom uglu trake zadataka.

   – ili –

   Na Windows radnoj površini, kliknite ili dodirnite ikonu **HP Client Security** u polju za obaveštavanje, a zatim izaberite opciju **Open HP Client Security** (Otvori HP Client Security).

2. Pokrenuće se Čarobnjak za podešavanje programa HP Client Security sa otvorenom stranicom dobrodošlice.

3. Pročitajte stranicu dobrodošlice, potvrdite svoj identitet tako što ćete uneti Windows lozinku, a zatim kliknite ili dodirnite dugme **Next** (Dalje).

   Ako još niste kreirali Windows lozinku, od vas će se tražiti da je kreirate. Windows lozinka je neophodna za zaštitu vašeg Windows naloga od pristupa neovlašćenih osoba, kao i za korišćenje funkcija programa HP Client Security.

4. Na stranici HP SpareKey izaberite tri bezbednosna pitanja. Unesite odgovor na svako od ovih pitanja, a zatim kliknite na dugme **Next** (Dalje). Moguće je kreirati i prilagođena pitanja. Više informacija potražite u odeljku HP SpareKey—Oporavak lozinke na stranici 14.

5. Na stranici Fingerprints (Otisci prsta), unesite bar minimalan broj otisaka prstiju, pa kliknite ili dodirnite dugme **Next** (Dalje). Više informacija potražite u odeljku Otisci prstiju na stranici 12.

6. Na stranici Drive Encryption, aktivirajte šifrovanje, napravite rezervnu kopiju ključa za šifrovanje, a zatim kliknite ili dodirnite dugme **Next** (Dalje). Dodatne informacije potražite u pomoći za softver HP Drive Encryption.

   NAPOMENA: Ovaj postupak važi za scenario kod kojeg je korisnik administrator, a Čarobnjak za podešavanje programa HP Client Security po prvi put konfiguriše administrator.

7. Na poslednjoj stranici čarobnjaka, kliknite ili dodirnite dugme **Finish** (Završi).

   Na ovoj stranici prikazuje se status funkcija i akreditiva.

8. Čarobnjak za podešavanje programa HP Client Security aktivira funkcije Just in Time Authentication i File Sanitizer. Dodatne informacije potražite u pomoći za softver HP Device Access Manager i pomoći za softver HP File Sanitizer.

   NAPOMENA: Ovaj postupak važi za scenario kod kojeg je korisnik administrator, a Čarobnjak za podešavanje programa HP Client Security po prvi put konfiguriše administrator.

Otvaranje programa HP Client Security

Aplikaciju HP Client Security možete otvoriti na neki od sledećih načina:

NAPOMENA: Da bi aplikacija HP Client Security mogla da se pokrene, potrebno je da dovršite Čarobnjak za podešavanje programa HP Client Security.

- Na početnom ekranu ili ekranu sa aplikacijama, kliknite ili dodirnite aplikaciju **HP Client Security**.

  – ili –

  Na Windows radnoj površini, kliknite ili dodirnite gadžet za **HP Client Security** (Windows 7).

  – ili –

  Na Windows radnoj površini, dvaput kliknite ili dodirnite dvaput ikonu **HP Client Security** u polju za obaveštavanje, koje se nalazi u desnom uglu trake zadataka.

  – ili –

  Na Windows radnoj površini, kliknite ili dodirnite ikonu **HP Client Security** u polju za obaveštavanje, a zatim izaberite opciju **Open HP Client Security** (Otvori HP Client Security).

3 Vodič za lako podešavanje za mala preduzeća

Predviđeno je da ovo poglavlje prikaže osnovne korake za aktiviranje najčešćih i najkorisnijih opcija u okviru verzije programa HP Client Security za mala preduzeća. Brojne alatke i opcije u ovom softveru omogućuju vam da precizno naštelujete svoje postavke i podesite kontrolu pristupa. U središtu pažnje ovog vodiča za lako podešavanje je kako da svaki od modula pokrenete uz minimalno ulaganje napora i vremena u podešavanje. Za dodatne informacije, izaberite modul koji vas zanima i zatim kliknite na **?** ili na dugme Pomoć u gornjem desnom uglu. Ovo dugme će automatski prikazati informacije koje vam pomažu sa trenutno prikazanim prozorom.

Prvi koraci

1. Na Windows radnoj površini otvorite HP Client Security tako što ćete dvaput kliknuti na ikonu **HP Client Security** u polju za obaveštavanje, koje se nalazi u desnom uglu trake zadataka.
2. Unesite svoju Windows lozinku ili kreirajte Windows lozinku.
3. Završite podešavanje programa HP Client Security.

Da bi HP Client Security zahtevao potvrdu identiteta samo jednom tokom prijavljivanja na Windows, pogledajte Bezbednosne funkcije na stranici 27.

Password Manager

Svi mi imamo veliki broj lozinki – naročito ako redovno pristupamo veb-sajtovima ili koristimo aplikacije koje zahtevaju prijavljivanje. Običan korisnik ili koristi istu lozinku za svaku aplikaciju i veb-sajt, ili želi da bude kreativan pa brzo zaboravi koja lozinka ide sa kojom aplikacijom.

Password Manager može automatski da pamti vaše lozinke ili da vam pruži mogućnost da odlučite koji sajtovi se pamte, a koji se izostavljaju. Kada se prijavite na računar, Password Manager će vam pružiti lozinke ili akreditive za registrovane aplikacije ili veb-sajtove.

Kada pristupite bilo kojoj aplikaciji ili veb-sajtu koji zahtevaju akreditive, Password Manager će automatski prepoznati sajt i pitaće vas da li želite da softver zapamti vaše podatke. Ako želite da isključite određene sajtove, možete da odbijete zahtev.

Da biste počeli da čuvate veb lokacije, korisnička imena i lozinke:

1. Na primer, idite do veb-sajta ili aplikacije koji učestvuju u programu i zatim kliknite na ikonu Password Manager u gornjem levom uglu veb-strane kako biste dodali veb potvrdu identiteta.
2. Dajte naziv vezi (opcionalno) i unesite korisničko ime i lozinku u Password Manager.
3. Kada završite kliknite na dugme **OK** (U redu).
4. Password Manager takođe može da sačuva korisničko ime i lozinke za deljene mrežne resurse ili mapirane mrežne diskove.

Prikazivanje i organizovanje sačuvanih podataka za potvrdu identiteta u programu Password Manager

Password Manager vam omogućuje da prikažete, organizujete, napravite rezervnu kopiju i pokrenete svoje podatke za potvrdu identiteta sa centralne lokacije. Password Manager takođe podržava pokretanje sačuvanih sajtova iz Windows-a.

Da biste otvorili Password Manager, koristite kombinaciju tastera Ctrl+Windows taster+h da otvorite Password Manager, a zatim kliknite na **Log in** (Prijavljivanje) da biste pokrenuli i autorizovali sačuvanu prečicu.

Opcija **Edit** (Uredi) u programu Password Manager omogućuje vam da prikažete i modifikujete naziv, ime za prijavljivanje i čak da otkrijete lozinke.

HP Client Security za mala preduzeća pruža mogućnost da se napravi rezervna kopija svih akreditiva i postavki i/ili da se kopira na drugi računar.

HP Device Access Manager

Device Access Manager može da se koristi za ograničavanje korišćenja različitih unutrašnjih i spoljašnjih uređaja za skladištenje kako bi vaši podaci bili bezbedni na čvrstom disku i kako ne bi napustili vaše prostorije. Primer za ovo bila bi situacija u kojoj korisniku dozvoljavate pristup vašim podacima, ali mu blokirate kopiranje podataka na CD, lični muzički plejer ili na USB memorijski uređaj.

1. Otvorite **Device Access Manager** (pogledajte Otvaranje alatke Device Access Manager na stranici 43).

   Prikazuje se pristup za trenutnog korisnika.

2. Da biste promenili pristup za korisnike, grupe ili uređaje, kliknite ili dodirnite **Change** (Promeni). Više informacija potražite u odeljku Sistemski prikaz na stranici 44.

HP Drive Encryption

HP Drive Encryption služi da zaštiti podatke tako što šifruje ceo čvrsti disk. Podaci na vašem čvrstom disku će ostati zaštićeni čak i ako vaš računar bude ukraden i/ili ako se čvrsti disk ukloni iz originalnog računara i stavi u drugi računar.

Dodatna prednost u smislu bezbednosti je to što Drive Encryption zahteva da pravilno potvrdite identitet pomoću korisničkog imena i lozinke pre nego što se operativni sistem pokrene. Ovaj postupak se zove autorizacija pre dizanja sistema.

Da bi vama bilo lakše, više softverskih modula automatski sinhronizuje lozinke, uključujući korisničke naloge za Windows, domene za autorizaciju, HP Drive Encryption, Password Manager i HP Client Security.

Da biste tokom početnog podešavanja konfigurisali HP Drive Encryption pomoću čarobnjaka za instalaciju programa HP Client Security, pogledajte Prvi koraci na stranici 8.

4 HP Client Security

Matična stranica programa HP Client Security predstavlja centralno mesto za lak pristup funkcijama, aplikacijama i postavkama programa HP Client Security. Matična stranica podeljena je na tri dela:

- **DATA** (Podaci)—Služi za pristup aplikacijama koje se koriste za upravljanje bezbednošću podataka.
- **DEVICE** (Uređaj)—Služi za pristup aplikacijama koje se koriste za upravljanje bezbednošću uređaja.
- **IDENTITY** (Identitet)—Služi za upisivanje i upravljanje akreditivima za potvrdu identiteta.

Pomerite kursor preko pločice sa aplikacijom da bi se prikazao opis te aplikacije.

U dnu stranice programa HP Client Security mogu se nalaziti veze ka postavkama za korisnike i administratore. Naprednim postavkama i funkcijama programa HP Client Security možete pristupiti ako dodirnete ili kliknete na ikonu **zupčanika** (Postavke).

Funkcije, aplikacije i postavke u vezi sa identitetom

Funkcije, aplikacije i postavke u vezi sa identitetom koje nudi program HP Client Security pomažu vam da upravljate raznim aspektima vašeg digitalnog identiteta. Kliknite ili dodirnite neku od sledećih pločica na matičnoj stranici programa HP Client Security, a zatim unesite svoju Windows lozinku.

- **Fingerprints** (Otisci prstiju)—Upisivanje otisaka prstiju i upravljanje akreditivima otisaka prstiju.
- **SpareKey**—Podešavanje i upravljanje HP SpareKey akreditivom koji možete koristiti za prijavljivanje na računar ako se ostali akreditivi izgube ili zature. Takođe, ovde možete resetovati lozinku ako ste je zaboravili.
- **Windows Password** (Windows lozinka)—Lak pristup postavkama za menjanje Windows lozinke.
- **Bluetooth Devices** (Bluetooth uređaji)—Upisivanje i upravljanje Bluetooth uređajima.
- **Cards** (Kartice)—Upisivanje i upravljanje pametnim karticama, beskontaktnim karticama ili proximity karticama.
- **PIN**—Upisivanje i upravljanje PIN kodovima koji služe kao akreditivi.
- **RSA SecurID**—Upisivanje i upravljanje RSA SecurID akreditivom (ako je prisutna odgovarajuća infrastruktura).
- **Password Manager**—Upravljanje lozinkama za naloge na mreži i aplikacije.

Otisci prstiju

Čarobnjak za podešavanje programa HP Client Security vodi vas kroz proces podešavanja ili „upisivanja“ otisaka prstiju.

Otiske prstiju takođe možete upisati ili izbrisati na stranici Fingerprints (Otisci prstiju), kojoj možete pristupiti tako što ćete kliknuti ili dodirnuti ikonu **Fingerprints** (Otisci prstiju) na matičnoj stranici programa HP Client Security.

1. Na stranici Fingerprints (Otisci prstiju), prevucite prstom preko senzora sve dok sistem uspešno ne upiše otisak.

   Koliko je otisaka prstiju potrebno upisati navedeno je na samoj stranici. Preporučuje se korišćenje kažiprsta ili srednjeg prsta.

2. Da biste izbrisali otiske prstiju koji su prethodno upisani, kliknite ili dodirnite opciju **Delete** (Izbriši).

3. Da biste upisali još otisaka prstiju, kliknite ili dodirnite opciju **Enroll an additional fingerprint** (Upisivanje još otisaka prstiju).

4. Kliknite ili dodirnite opciju **Save** (Sačuvaj) pre nego što napustite stranicu.

⚠ **OPREZ:** Kada se otisci prstiju upisuju putem čarobnjaka, informacije o otiscima prstiju neće biti sačuvane sve dok ne kliknete na dugme **Next** (Dalje). Ako neko vreme ne koristite računar ili zatvorite program, promene koje ste uneli **neće** biti sačuvane.

- ▲ Da biste pristupili administrativnim postavkama za otiske prstiju u kojima administratori mogu podesiti upisivanje, preciznost i druge postavke, kliknite ili dodirnite opciju **Administrative Settings** (Administrativne postavke) (potrebne su administrativne privilegije).
- ▲ Da biste pristupili korisničkim postavkama za otiske prstiju u kojima možete podesiti postavke koje upravljaju izgledom i ponašanjem funkcije prepoznavanja otisaka prstiju, kliknite ili dodirnite opciju **User Settings** (Korisničke postavke).

Administrativne postavke za otiske prstiju

Administratori mogu podesiti upisivanje, preciznost i druge postavke čitača otiska prsta. Potrebne su administrativne privilegije.

- ▲ Da biste pristupili administrativnim postavkama za akreditive otisaka prstiju, kliknite ili dodirnite opciju **Administrative Settings** (Administrativne postavke) na stranici Fingerprints (Otisci prstiju).
- **User enrollment** (Upis otisaka za korisnike)—Izaberite minimalan i maksimalan broj otisaka prstiju koje korisnik može da upiše.
- **Recognition** (Prepoznavanje)—Pomerite klizač da biste podesili osetljivost čitača otiska prsta kada prevučete prstom preko njega.

  Ako čitač često ne može da prepozna otisak prsta, potrebno je da izaberete nižu postavku prepoznavanja. Viša postavka povećava osetljivost na varijacije u prevlačenju prstom i tako smanjuje mogućnost lažnih pogodaka. Postavka **Medium-High** (Srednje visoka) predstavlja dobar spoj bezbednosti i praktičnosti.

Korisničke postavke za otiske prstiju

Na stranici User Settings (Korisničke postavke) za otiske prstiju, možete podesiti postavke koje upravljaju izgledom i ponašanjem funkcije prepoznavanja otisaka prstiju.

▲ Da biste pristupili korisničkim postavkama za akreditive otisaka prstiju, kliknite ili dodirnite opciju **User Settings** (Korisničke postavke) na stranici Fingerprints (Otisci prstiju).

- **Enable sound feedback** (Omogući povratni zvuk)—Program HP Client Security podrazumevano pruža zvučnu povratnu informaciju prilikom prevlačenja prstom tako što reprodukuje različite zvuke za svaki programski događaj. Ovim događajima možete dodeliti nove zvukove tako što ćete otvoriti Windows meni Kontrolna tabla, a zatim kliknuti na karticu Zvukovi u meniju Zvuk ili, ako želite da onemogućite povratni zvuk, poništite izbor polja za potvrdu.
- **Show scan quality feedback** (Prikaži povratne informacije o kvalitetu skeniranja)—Izaberite polje za potvrdu da bi se prikazivalo svako prevlačenje prstom, bez obzira na kvalitet. Da bi se prikazivala samo prevlačenja prstom dobrog kvaliteta, poništite izbor polja za potvrdu.

HP SpareKey—Oporavak lozinke

Funkcija HP SpareKey omogućava vam da pristupite računaru (na podržanim platformama) tako što ćete odgovoriti na tri bezbednosna pitanja.

HP Client Security tražiće od vas da podesite svoj HP SpareKey u toku početnog podešavanja pomoću Čarobnjaka za podešavanje programa HP Client Security.

Da biste podesili svoj HP SpareKey:

1. Na stranici čarobnjaka koja se odnosi na HP SpareKey, izaberite tri bezbednosna pitanja, a zatim unesite odgovor na svako od tih pitanja.

   Možete izabrati neko od pitanja sa unapred definisane liste ili sami upisati pitanje.

2. Kliknite ili dodirnite opciju **Enroll** (Unesi).

Da biste izbrisali svoj HP SpareKey:

▲ Kliknite ili dodirnite opciju **Delete your SpareKey** (Izbrišite svoj SpareKey).

Nakon što podesite svoj SpareKey, moći ćete da pristupate računaru tako što ćete ga uneti na ekranu za proveru identiteta pri pokretanju sistema ili na Windows ekranu dobrodošlice.

Stranicu SpareKey možete otvoriti preko pločice Password Recovery (Oporavak lozinke) na matičnoj stranici programa HP Client Security, a na njoj možete izabrati drugačija pitanja ili promeniti svoje odgovore.

Da biste pristupili postavkama za HP SpareKey, u kojima administratori mogu podesiti postavke u vezi sa HP SpareKey akreditivom, kliknite na stavku **Settings** (Postavke) (potrebne su administrativne privilegije).

HP SpareKey Settings

Na stranici sa postavkama za HP SpareKey možete podesiti postavke koje upravljaju ponašanjem i korišćenjem HP SpareKey akreditiva.

▲ Da biste otvorili stranicu sa postavkama za HP SpareKey, kliknite ili dodirnite stavku **Settings** (Postavke) na stranici funkcije HP SpareKey (potrebne su administrativne privilegije).

Administratori mogu izabrati sledeće postavke:

- Navedite pitanja koja se postavljaju svakom korisniku u toku podešavanja funkcije HP SpareKey.
- Dodajte do tri prilagođena bezbednosna pitanja na listu koja se nudi korisnicima.
- Izaberite da li želite da dozvolite korisnicima da unose sopstvena bezbednosna pitanja.
- Navedite koja će okruženja za proveru identiteta (Windows ili provera identiteta pri pokretanju sistema) podržavati korišćenje funkcije HP SpareKey za oporavak lozinke.

Windows lozinka

Pomoću programa HP Client Security možete lakše i brže promeniti Windows lozinku u odnosu na meni Kontrolna tabla u operativnom sistemu Windows.

Da biste promenili svoju Windows lozinku:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite stavku **Windows Password** (Windows lozinka).
2. Unesite svoju trenutnu lozinku u okvir za tekst **Current Windows password** (Trenutna Windows lozinka).
3. Unesite novu lozinku u okvir za tekst **New Windows password** (Nova Windows lozinka), a zatim je ponovo unesite u okvir za tekst **Confirm new password** (Potvrdi novu lozinku).
4. Kliknite ili dodirnite opciju **Change** (Promeni) da biste odmah promenili trenutnu lozinku u novounetu lozinku.

Bluetooth uređaji

Ako je administrator omogućio Bluetooth kao akreditiv za potvrdu identiteta, možete da podesite Bluetooth telefon uz ostale akreditive radi veće bezbednosti.

NAPOMENA: Podržani su samo Bluetooth uređaji sa funkcijom telefona.

1. Proverite da li je na računaru omogućena Bluetooth funkcija, kao i da li je Bluetooth telefon postavljen u režim u kojem drugi uređaji mogu da ga otkriju. Da biste povezali telefon, možda će biti potrebno da unesete automatski generisani kod na Bluetooth uređaju. U zavisnosti od postavki Bluetooth uređaja, možda će biti potrebno da uporedite kodove za uparivanje.
2. Da biste upisali telefon, izaberite ga, a zatim kliknite ili dodirnite opciju **Enroll** (Unesi).

Da biste pristupili stranici Postavke Bluetooth uređaja na stranici 15 na kojoj administratori mogu podesiti postavke za Bluetooth uređaje, kliknite na stavku **Settings** (Postavke) (potrebne su administrativne privilegije).

Postavke Bluetooth uređaja

Administratori mogu podesiti sledeće postavke koje upravljaju ponašanjem i korišćenjem akreditiva u vidu Bluetooth uređaja:

Tiha provera identiteta

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Automatski koristi povezani upisani Bluetooth uređaj prilikom verifikacije identiteta)—Izaberite ovo polje za potvrdu da biste omogućili korisnicima da koriste Bluetooth akreditiv za

proveru identiteta bez potrebe da korisnik bilo šta preduzme ili poništite izbor polja za potvrdu da biste onemogućili ovu opciju.

Blizina Bluetooth uređaja

- **Lock computer when your enrolled Bluetooth device moves out of range of your computer** (Zaključaj računar kada upisani Bluetooth uređaj izađe iz dometa računara)—Izaberite ovo polje za potvrdu ako želite da se računar zaključa kada Bluetooth uređaj koji je povezan prilikom prijavljivanja izađe iz dometa ili poništite izbor polja za potvrdu da biste onemogućili ovu opciju.

NAPOMENA: Bluetooth modul na vašem računaru mora podržavati ovu funkciju da biste mogli da je koristite.

Kartice

HP Client Security podržava više tipova identifikacionih kartica—plastičnih kartica koje sadrže računarski čip. To su pametne kartice, beskontaktne kartice i proximity kartice. Ako se neka od ovih kartica, zajedno sa odgovarajućem čitačem kartica, poveže na računar, a administrator je instalirao odgovarajući upravljački program od proizvođača i omogućio kartice kao akreditiv za potvrdu identiteta, moći ćete da koristite karticu kao akreditiv za potvrdu identiteta.

Kod pametnih kartica, proizvođač bi trebalo da obezbedi alatke za instalaciju bezbednosnog certifikata i upravljanje PIN kodom koje će HP Client Security koristiti u svom bezbednosnom algoritmu. Broj i tip znakova koji čine PIN mogu se razlikovati. Da biste mogli da koristite pametnu karticu, potrebno je da je administrator inicijalizuje.

Program HP Client Security podržava sledeće formate pametnih kartica:

- CSP
- PKCS11

Program HP Client Security podržava sledeće tipove beskontaktnih kartica:

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

Program HP Client Security podržava sledeće proximity kartice:

- HID Proximity kartice

Da biste upisali pametnu karticu:

1. Umetnite karticu u povezani čitač pametne kartice.
2. Kada kartica bude prepoznata, unesite njen PIN, a zatim kliknite ili dodirnite opciju **Enroll** (Unesi).

Da biste promenili PIN pametne kartice:

1. Umetnite karticu u povezani čitač pametne kartice.
2. Kada kartica bude prepoznata, unesite njen PIN, a zatim kliknite ili dodirnite opciju **Authenticate** (Proveri identitet).
3. Kliknite ili dodirnite opciju **Change PIN** (Promeni PIN), pa unesite novi PIN.

Da biste upisali beskontaktnu ili proximity karticu:

1. Postavite karticu na odgovarajući čitač ili blizu njega.
2. Kada kartica bude prepoznata, kliknite ili dodirnite opciju **Enroll** (Unesi).

Da biste izbrisali upisanu karticu:

1. Postavite karticu tako da je čitač pročita.
2. Ako je reč o pametnoj kartici, unesite njen PIN, a zatim kliknite ili dodirnite opciju **Authenticate** (Proveri identitet).
3. Kliknite ili dodirnite opciju **Delete** (Izbriši).

Nakon što se kartica upiše, informacije o kartici prikazuju se na listi **Enrolled Cards** (Upisane kartice). Kada se kartica izbriše, uklanja se sa liste.

Da biste pristupili postavkama za proximity, beskontaktne i pametne kartice u kojima administratori mogu podesiti postavke u vezi sa akreditivima u vidu kartica, kliknite ili dodirnite stavku **Settings** (Postavke) (potrebne su administrativne privilegije).

Postavke za proximity, beskontaktne i pametne kartice

Da biste pristupili postavkama za određenu karticu, kliknite ili dodirnite željenu karticu sa liste, pa kliknite ili dodirnite strelicu koja će se prikazati.

Da biste promenili PIN pametne kartice:

1. Postavite karticu tako da je čitač pročita.
2. Unesite PIN kartice, a zatim kliknite ili dodirnite dugme **Continue** (Nastavi).
3. Unesite i potvrdite novi PIN, a zatim kliknite ili dodirnite dugme **Continue** (Nastavi).

Da biste inicijalizovali PIN pametne kartice:

1. Postavite karticu tako da je čitač pročita.
2. Unesite PIN kartice, a zatim kliknite ili dodirnite dugme **Continue** (Nastavi).
3. Unesite i potvrdite novi PIN, a zatim kliknite ili dodirnite dugme **Continue** (Nastavi).
4. Kliknite ili dodirnite dugme **Yes** (Da) da biste potvrdili inicijalizaciju.

Da biste obrisali podatke o kartici:

1. Postavite karticu tako da je čitač pročita.
2. Unesite PIN kartice (samo za pametne kartice), a zatim kliknite ili dodirnite dugme **Continue** (Nastavi).
3. Kliknite ili dodirnite dugme **Yes** (Da) da biste potvrdili brisanje.

PIN

Ako je administrator omogućio PIN kao akreditiv za potvrdu identiteta, možete da podesite PIN uz ostale akreditive radi veće bezbednosti.

Da biste podesili novi PIN:

- Unesite željeni PIN, unesite ga ponovo da biste ga potvrdili, a zatim kliknite ili dodirnite dugme **Apply** (Primeni).

Da biste izbrisali PIN:

▲ Kliknite ili dodirnite opciju **Delete** (Izbriši), a zatim kliknite ili dodirnite **Yes** (Da) da biste potvrdili.

Da biste pristupili postavkama za PIN kodove, u kojima administratori mogu podesiti postavke u vezi sa akreditivima u vidu PIN kodova, kliknite ili dodirnite stavku **Settings** (Postavke) (potrebne su administrativne privilegije).

HP PIN Settings

Na stranici sa postavkama za PIN kodove možete navesti minimalnu i maksimalnu prihvatljivu dužinu PIN koda koji se koristi kao akreditiv.

RSA SecurID

Ako je administrator omogućio RSA kao akreditiv za potvrdu identiteta, a sledeći uslovi su ispunjeni, moći ćete da upišete ili izbrišete RSA SecurID akreditiv.

NAPOMENA: Potrebno je da bude podešena odgovarajuća infrastruktura.

- Na RSA serveru mora biti kreiran korisnik.
- RSA SecurID token koji dodeljen korisniku i računaru mora biti povezan sa domenom RSA servera.
- SecurID softver mora biti instaliran na računaru.
- Potrebna je veza sa pravilno konfigurisanim RSA serverom.

Da biste upisali RSA SecurID akreditiv:

▲ Unesite svoje korisničko ime i RSA SecurID kôd (kôd RSA SecurID tokena ili PIN+kôd tokena, u zavisnosti od okruženja), a zatim kliknite ili dodirnite dugme **Apply** (Primeni).

Nakon uspešnog upisivanja, prikazaće se poruka „Your RSA SecurID credential has been successfully enrolled“ (Vaš RSA SecurID akreditiv uspešno je upisan) i biće omogućeno dugme Delete (Izbriši).

Da biste izbrisali RSA SecurID akreditiv:

▲ Kliknite na dugme **Delete** (Delete), pa izaberite **Yes** (Da) u iskačućem dijalogu sa pitanjem „Are you sure you want to delete your RSA SecurID credential?“ (Želite li zaista da izbrišete svoj RSA SecurID akreditiv?).

Password Manager

Prijavljivanje na veb lokacije i aplikacije bezbednije je i lakše uz alatku Password Manager. Možete kreirati snažnije lozinke koje ne morate da zapisujete ili pamtite, a zatim da se lako i brzo prijavite pomoću otiska prsta, pametne kartice, proximity kartice, beskontaktne kartice, Bluetooth telefona, PIN koda, RSA akreditiva ili vaše Windows lozinke.

NAPOMENA: Pošto se struktura ekrana za prijavljivanje na veb stranicama neprekidno menja, Password Manager možda neće uvek podržavati sve veb lokacije.

Password Manager nudi sledeće opcije:

Stranica Password Manager

- Kliknite ili dodirnite neki od naloga da biste automatski pokrenuli veb stranicu ili aplikaciju i prijavili se na nju.
- Naloge možete organizovati pomoću kategorija.

Snaga lozinke

- Dovoljan je jedan pogled da biste videli da li neka od vaših lozinki predstavlja bezbednosni rizik.
- Kada dodajete podatke za prijavljivanje, proverite snagu pojedinačnih lozinki koje koristite za veb lokacije i aplikacije.
- Snaga lozinke označena je crvenim, žutim ili zelenim indikatorom statusa.

Ikona **Password Manager** prikazuje se u gornjem levom uglu stranice za prijavljivanje na veb lokaciju ili aplikaciju. Ako za otvorenu veb lokaciju ili aplikaciju još nisu kreirani podaci za prijavljivanje, na ikoni se prikazuje znak plus.

▲ Kliknite ili dodirnite ikonu **Password Manager** da bi se prikazao kontekstualni meni u kojem možete izabrati neku od sledećih opcija:

- Add [somedomain.com] to Password Manager (Dodaj [nekidomen.com] u Password Manager)
- Open Password Manager (Otvori Password Manager)
- Icon Settings (Postavke ikona)
- Pomoć

Za veb stranice ili programe za koje još nisu kreirani podaci za prijavljivanje

U kontekstualnom meniju prikazuju se sledeće opcije:

- **Add [somedomain.com] to the Password Manager** (Dodaj [nekidomen.com] u Password Manager)—Dodavanje podataka za prijavljivanje za trenutno otvoreni ekran za prijavu.
- **Open Password Manager** (Otvori Password Manager)—Pokretanje alatke Password Manager.
- **Icon Settings** (Postavke ikona)—Služi za navođenje uslova pod kojima se prikazuje ikona alatke **Password Manager**.
- **Help** (Pomoć)—Prikazivanje pomoći za program HP Client Security.

Za veb stranice ili programe za koje su već kreirani podaci za prijavljivanje

U kontekstualnom meniju prikazuju se sledeće opcije:

- **Fill in logon data** (Unesite podatke za prijavljivanje)—Prikazuje se stranica **Verify your identity** (Potvrdite svoj identitet). Ako uspešno potvrdite identitet, uneti podaci za prijavljivanje biće smešteni u polja za prijavljivanje, nakon čega će stranica biti prosleđena (ako je prosleđivanje podešeno prilikom kreiranja ili poslednjeg uređivanja podataka za prijavljivanje).
- **Edit Logon** (Uredi podatke za prijavljivanje)—Uređivanje podataka za prijavljivanje za otvorenu veb lokaciju.
- **Add Logon** (Dodaj podatke za prijavljivanje)—Dodavanje naloga u Password Manager.
- **Open Password Manager** (Otvori Password Manager)—Pokretanje alatke Password Manager.
- **Help** (Pomoć)—Prikazivanje pomoći za program HP Client Security.

NAPOMENA: Administrator računara možda je podesio program HP Client Security tako da zahteva unos više od jednog akreditiva prilikom provere identiteta.

Dodavanje podataka za prijavljivanje

Lako možete dodati podatke za prijavljivanje za željenu veb lokaciju ili program tako što ćete samo jednom uneti informacije za prijavljivanje. Nakon toga, Password Manager automatski će unositi ove informacije umesto vas. Unete podatke za prijavljivanje moći ćete da koristite nakon što otvorite odgovarajuću veb lokaciju ili program.

Da biste dodali podatke za prijavljivanje:

1. Otvorite ekran za prijavljivanje na željenu veb lokaciju ili program.
2. Kliknite ili dodirnite ikonu **Password Manager**, pa kliknite ili dodirnite neku od sledećih opcija, u zavisnosti od toga da li je otvoren ekran za prijavljivanje na veb lokaciju ili program:
   - Ako je reč o veb lokaciji, kliknite ili dodirnite opciju **Add [domain name] to Password Manager** (Dodaj [ime domena] u Password Manager).
   - Ako je reč o programu, kliknite ili dodirnite opciju **Add this logon screen to Password Manager** (Dodaj ovaj ekran za prijavljivanje u Password Manager).
3. Unesite svoje podatke za prijavljivanje. Polja za prijavljivanje na ekranu, kao i odgovarajuća polja u dijalozima, biće istaknuta podebljanim narandžastim okvirom.
   a. Da biste polje za prijavljivanje popunili nekim od već unetih izbora, kliknite ili dodirnite strelice sa desne strane polja.
   b. Da biste videli lozinku za tu veb lokaciju ili program, kliknite ili dodirnite opciju **Show password** (Prikaži lozinku).
   c. Da biste popunili polja za prijavljivanje, ali ne i prosledili, poništite izbor polja za potvrdu **Automatically submit logon data** (Automatski prosledi podatke za prijavljivanje).
   d. Kliknite ili dodirnite dugme **OK** (U redu) da biste izabrali koji metod provere identiteta želite da koristite (otisak prsta, pametnu karticu, proximity karticu, beskontaktnu karticu, Bluetooth telefon, PIN kod ili lozinku), a zatim se prijavite pomoću izabranog metode provera identiteta.

      Znak plus biće uklonjen sa ikone alatke **Password Manager** što znači da su podaci za prijavljivanje kreirani.
   e. Ako Password Manager ne otkrije polja za prijavljivanje, kliknite ili dodirnite opciju **More fields** (Još polja).
      - Izaberite polje za potvrdu za svako polje koje je potrebno za prijavljivanje ili poništite izbor polja za potvrdu koja nisu potrebna za prijavljivanje.
      - Kliknite ili dodirnite opciju **Close** (Zatvori).

Prilikom svakog pristupanja toj veb lokaciji ili svakog otvaranja tog programa, ikona **Password Manager** biće prikazana u gornjem levom uglu ekrana za prijavljivanje na veb lokaciju ili aplikaciju, što znači da možete upotrebiti registrovane akreditive za prijavljivanje.

Uređivanje podataka za prijavljivanje

Da biste uredili podatke za prijavljivanje:

1. Otvorite ekran za prijavljivanje na željenu veb lokaciju ili program.
2. Da biste otvorili dijalog za unos informacija za prijavljivanje, kliknite ili dodirnite ikonu **Password Manager**, a zatim kliknite ili dodirnite opciju **Edit Logon** (Uredi podatke za prijavljivanje).

   Polja za prijavljivanje na ekranu, kao i odgovarajuća polja u dijalozima, biće istaknuta podebljanim narandžastim okvirom.

   Takođe, ako otvorite alatku Password Manager, moći ćete da uredite informacije o nalogu tako što ćete dodirnuti željene podatke za prijavljivanje, a zatim izabrati opciju **Edit** (Uredi).
3. Uredite informacije za prijavljivanje.
   - Da biste uredili **Account name** (Ime naloga), unesite novo ime u ovo polje.
   - Da biste dodali ili uredili stavku **Category** (Kategorija), unesite ili izmenite ime kategorije u polju **Category** (Kategorija).
   - Da biste polje za prijavljivanje **Username** (Korisničko ime) popunili nekim od već unetih izbora, kliknite ili dodirnite strelicu nadole sa desne strane polja.

     Već uneti izbori dostupni su samo kada podatke za prijavljivanje uređujete pomoću komande Edit (Uredi) u okviru kontekstualnog menija za ikonu Password Manager.
   - Da biste polje za prijavljivanje **Password** (Lozinka) popunili nekim od već unetih izbora, kliknite ili dodirnite strelicu nadole sa desne strane polja.

     Već uneti izbori dostupni su samo kada podatke za prijavljivanje uređujete pomoću komande Edit (Uredi) u okviru kontekstualnog menija za ikonu Password Manager.
   - Da biste među podatke za prijavljivanje dodali još polja sa ekrana, kliknite ili dodirnite opciju **More fields** (Još polja).
   - Da biste videli lozinku za tu veb lokaciju ili program, kliknite ili dodirnite ikonu **Show password** (Prikaži lozinku).
   - Da biste popunili polja za prijavljivanje, ali ne i prosledili, poništite izbor polja za potvrdu **Automatically submit logon data** (Automatski prosledi podatke za prijavljivanje).
   - Da biste označili da određeni podaci za prijavljivanje sadrže ugroženu lozinku, izaberite polje za potvrdu **This password is compromised** (Ova lozinka je ugrožena).

     Nakon što sačuvate izmene, ova oznaka biće dodata svim podacima za prijavljivanje koji sadrže istu lozinku. Zatim možete otvoriti svaki od ugroženih naloga i promeniti lozinke po potrebi.
4. Kliknite ili dodirnite dugme **OK** (U redu).

Korišćenje menija Quick Links (Brze veze) u okviru alatke Password Manager

Password Manager nudi brz i lak način za otvaranje veb lokacija i programa za koje ste kreirali podatke za prijavljivanje. Dvaput kliknite ili dodirnite dvaput podatke za prijavljivanje za određeni program ili veb lokaciju u meniju **Password Manager Quick Links** (Brze veze) ili na stranici Password Manager u okviru programa HP Client Security da biste otvorili ekran za prijavljivanje, a zatim unesite svoje podatke za prijavljivanje.

Kada kreirate podatke za prijavljivanje, automatski će biti dodati u meni **Quick Links** (Brze veze) u okviru alatke Password Manager.

Da biste otvorili meni **Quick Links** (Brze veze):

▲ Pritisnite kombinaciju interventnih tastera za **Password Manager** (Ctrl+Windows taster+h je fabrička postavka). Da biste promenili kombinaciju interventnih tastera, na matičnoj stranici programa HP Client Security kliknite na stavku **Password Manager**, a zatim kliknite ili dodirnite stavku **Settings** (Postavke).

Organizovanje podataka za prijavljivanje u kategorije

Kreirajte jednu ili više kategorija pomoću kojih ćete organizovati svoje podatke za prijavljivanje.

Da biste rasporedili podatke za prijavljivanje po kategorijama:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite stavku **Password Manager**.
2. Kliknite ili dodirnite željeni nalog, a zatim kliknite ili dodirnite opciju **Edit** (Uredi).
3. Unesite ime kategorije u polje **Category** (Kategorija).
4. Kliknite ili dodirnite dugme **Save** (Sačuvaj).

Da biste uklonili nalog iz kategorije:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite stavku **Password Manager**.
2. Kliknite ili dodirnite željeni nalog, a zatim kliknite ili dodirnite opciju **Edit** (Uredi).
3. Izbrišite ime kategorije iz polja **Category** (Kategorija).
4. Kliknite ili dodirnite dugme **Save** (Sačuvaj).

Da biste preimenovali kategoriju:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite stavku **Password Manager**.
2. Kliknite ili dodirnite željeni nalog, a zatim kliknite ili dodirnite opciju **Edit** (Uredi).
3. Promenite ime kategorije u polju **Category** (Kategorija).
4. Kliknite ili dodirnite dugme **Save** (Sačuvaj).

Upravljanje podacima za prijavljivanje

Password Manager omogućava lako upravljanje informacijama za prijavljivanje, koje obuhvataju korisnička imena, lozinke i naloge za višestruko prijavljivanje, i to na jednom mestu.

Vaši podaci za prijavljivanje biće navedeni na stranici Password Manager.

Upravljanje podacima za prijavljivanje:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite stavku **Password Manager**.
2. Kliknite ili dodirnite postojeće podatke za prijavljivanje, izaberite neku od sledećih opcija, a zatim pratite uputstva na ekranu:
   - **Edit** (Uredi)—Uređivanje podataka za prijavljivanje. Više informacija potražite u odeljku Uređivanje podataka za prijavljivanje na stranici 21.
   - **Log in** (Prijavljivanje)—Prijavljivanje u izabrani nalog.
   - **Delete** (Izbriši)—Brisanje podataka za prijavljivanje za izabrani nalog.

Da biste dodali dodatne podatke za prijavljivanje za određenu veb lokaciju ili program:

1. Otvorite ekran za prijavljivanje na željenu veb lokaciju ili program.
2. Kliknite ili dodirnite ikonu **Password Manager** da biste otvorili kontekstualni meni.
3. Kliknite ili dodirnite opciju **Add Logon** (Dodaj podatke za prijavljivanje), a zatim pratite uputstva na ekranu.

Procenjivanje snage lozinke

Korišćenje snažnih lozinki za prijavljivanje na veb lokacije i programe predstavlja važan aspekat zaštite identiteta.

Alatka Password Manager olakšava proces nadgledanja i upravljanja bezbednošću tako što omogućava trenutnu automatizovanu analizu snage svake lozinke koja se koristi za prijavljivanje na veb lokacije i programe.

Dok u okviru alatke Password Manager unosite lozinku kao deo kreiranja podataka za prijavljivanje na određeni nalog, ispod lozinke prikazuje se traka u boji koja pokazuje snagu lozinke. Boje imaju sledeća značenja:

- **Crvena**—Slaba
- **Žuta**—Srednja
- **Zelena**—Snažna

Postavke ikone alatke Password Manager

Password Manager nastoji da prepozna ekrane za prijavljivanje na veb lokacije i programe. Kada otkrije ekran za prijavljivanje za koji još niste uneli podatke za prijavljivanje, Password Manager će tražiti od vas da unesete podatke za prijavljivanje za taj ekran tako što će se na ikoni **Password Manager** prikazati znak plus.

1. Kliknite ili dodirnite ikonu, a zatim kliknite ili dodirnite opciju **Icon Settings** (Postavke ikone) da biste prilagodili način na koji Password Manager postupa sa potencijalnim lokacijama za prijavljivanje.
   - **Prompt to add logons for logon screens** (Traži da dodam podatke za prijavljivanje na ekranima za prijavljivanje)—Kliknite ili dodirnite ovu opciju da bi Password Manager tražio od as da unesete podatke za prijavljivanje kada se prikaže ekran za prijavljivanje za koji još niste uneli podatke za prijavljivanje.
   - **Exclude this screen** (Izuzmi ovaj ekran)—Izaberite ovo polje za potvrdu da Password Manager više ne bi tražio od vas da unesete podatke za prijavljivanje za taj ekran.
   - **Do not prompt to add logons for logon screens** (Ne traži da dodam podatke za prijavljivanje na ekranima za prijavljivanje)—Izaberite radio dugme.
2. Da biste dodali podatke za prijavljivanje za ekran koji je prethodno bio izuzet:
   a. Prijavite se na veb lokaciju koja je prethodno bila izuzeta.
   b. Da bi alatka Password Manager zapamtila lozinku za ovaj veb-sajt, kliknite ili dodirnite opciju **Remember** (Zapamti) u iskačućem dijalogu da biste sačuvali lozinku i kreirali podatke za prijavljivanje za taj ekran.
3. Da biste pristupili dodatnim postavkama za Password Manager, kliknite ili dodirnite ikonu alatke Password Manager, kliknite ili dodirnite opciju **Open Password Manager** (Otvori Password Manager), a zatim kliknite ili dodirnite stavku **Settings** (Postavke) na stranici Password Manager.

Uvoz i izvoz podataka za prijavljivanje

Na stranici za uvoz i izvoz u okviru alatke HP Password Manager možete da uvezete podatke za prijavljivanje koji su sačuvani u veb pregledaču na računaru. Takođe, možete uvoziti podatke iz rezervnih datoteka programa HP Client Security i izvoziti podatke u njih.

▲ Da biste otvorili stranicu za uvoz i izvoz, kliknite ili dodirnite opciju **Import and export** na stranici Password Manager.

Da biste uvezli lozinke iz pregledača:

1. Kliknite ili dodirnite pregledač iz kojeg želite da uvezete lozinke (prikazuju se samo instalirani pregledači).
2. Poništite izbor polja za potvrdu pored naloga za koje ne želite da uvezete lozinke.
3. Kliknite ili dodirnite dugme **Import** (Uvezi).

Uvoz podataka iz rezervne datoteke programa HP Client Security i uvoz podataka u nju obavlja se pomoću odgovarajućih veza (u odeljku **Other Options** (Ostale opcije)) na stranici Import and export (Uvoz i izvoz).

NAPOMENA: Ova funkcija služi za uvoz i izvoz samo podataka iz alatke Password Manager. Dodatne informacije o pravljenju rezervnih kopija i vraćanju dodatnih podataka iz programa HP Client Security potražite u odeljku Pravljenje rezervnih kopija i vraćanje podataka u prethodno stanje na stranici 28.

Da biste uvezli podatke iz rezervne datoteke programa HP Client Security:

1. Na stranici Import and export (Uvoz i izvoz) u okviru alatke HP Password Manager, kliknite ili dodirnite opciju **Import data from an HP Client Security backup file** (Uvezi podatke iz rezervne datoteke programa HP Client Security).
2. Potvrdite svoj identitet.
3. Izaberite već kreiranu rezervnu datoteku ili unesite lozinku u za to predviđeno polje, a zatim kliknite ili dodirnite stavku **Browse** (Potraži).
4. Unesite lozinku kojom je datoteka zaštićena, a zatim kliknite ili dodirnite dugme **Next** (Dalje).
5. Kliknite ili dodirnite opciju **Restore** (Vrati).

Da biste izvezli podatke u rezervnu datoteku programa HP Client Security:

1. Na stranici Import and export (Uvoz i izvoz) u okviru alatke HP Password Manager, kliknite ili dodirnite opciju **Export data from an HP Client Security backup file** (Izvezi podatke u rezervnu datoteku programa HP Client Security).
2. Potvrdite svoj identitet, pa kliknite ili dodirnite dugme **Next** (Dalje).
3. Unesite ime rezervne datoteke. Datoteka će podrazumevano biti sačuvana u fascikli Dokumenti. Da biste izabrali drugu lokaciju, kliknite ili dodirnite stavku **Browse** (Potraži).
4. Unesite i potvrdite lozinku za zaštitu datoteke, a zatim kliknite ili dodirnite dugme **Save** (Sačuvaj).

Postavke

Možete podesiti postavke za personalizovanje alatke Password Manager:

- **Prompt to add logons for logon screens** (Traži da dodam podatke za prijavljivanje na ekranima za prijavljivanje)—Ikona alatke **Password Manager** sa znakom plus prikazivaće kad god se otkrije ekran za prijavljivanje na veb lokaciju ili program, što označava da za taj ekran možete dodati podatke za prijavljivanje u meniju **Logons** (Podaci za prijavljivanje).

  Da biste onemogućili ovu funkciju, poništite izbor polja za potvrdu pored opcije **Prompt to add logons for logon screens** (Traži da dodam podatke za prijavljivanje na ekranima za prijavljivanje).

- **Open Password Manager with Ctrl+Win+h** (Otvori Password Manager kada pritisnem Ctrl +Win+h)—Podrazumevana kombinacija interventnih tastera za otvaranje menija **Password Manager Quick Links** (Brze veze) je Ctrl+Windows taster+h.

  Da biste promenili interventne tastere, kliknite ili dodirnite ovu opciju, a zatim unesite novu kombinaciju tastera. Kombinacije mogu obuhvatati jedan ili više sledećih tastera: ctrl, alt ili shift i bilo koji slovni ili numerički taster.

  Ne mogu se izabrati kombinacije koje se već koriste u operativnom sistemu Windows ili Windows aplikacijama.

- Da biste vratili postavke na fabričke podrazumevane vrednosti, kliknite ili dodirnite opciju **Restore defaults** (Vrati podrazumevane vrednosti).

Napredne postavke

Administratori mogu pristupiti sledećim opcijama tako što će izabrati ikonu **zupčanika** (Postavke) na matičnoj stranici programa HP Client Security.

- **Administrator Policies** (Smernice za administratore)—Konfigurisanje smernica prijavljivanja i sesija za administratore.
- **Standard User Policies** (Smernice za standardne korisnike)—Konfigurisanje smernica prijavljivanja i sesija za standardne korisnike.
- **Security Features** (Bezbednosne funkcije)—Omogućava vam da povećate bezbednost računara tako što ćete zaštititi svoju Windows nalog pomoću snažne provere identiteta i/ili omogućiti proveru identiteta pre pokretanja operativnog sistema Windows.
- **Users** (Korisnici)—Upravljanje korisnicima i njihovim akreditivima.
- **My Policies** (Moje smernice)—Omogućava vam da pogledate svoje smernice za proveru identiteta i status unosa.
- **Backup and Restore** (Rezervne kopije i vraćanje)—Omogućava vam da napravite rezervnu kopiju podataka iz programa HP Client Security ili da ih vratite u prethodno stanje.
- **About HP Client Security** (Osnovne informacije o programu HP Client Security)—Informacije o verziji programa HP Client Security.

Smernice za administratore

Možete konfigurisati smernice prijavljivanja i sesija za administratore računara. Smernice prijavljivanja koje se ovde podese upravljaju akreditivima pomoću kojih se lokalni administrator prijavljuje u operativni sistem Windows. Smernice sesija koje se ovde podese upravljaju akreditivima pomoću kojih lokalni administrator potvrđuje svoj identitet u okviru Windows sesije.

Sve nove ili promenjene smernice podrazumevano stupaju na snagu odmah nakon što kliknete ili dodirnete dugme **Apply** (Primeni).

Da biste dodali nove smernice:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite ikonu **zupčanika**.
2. Na stranici Advanced Settings (Napredne postavke), kliknite ili dodirnite stavku **Administrator Policies** (Smernice za administratore).
3. Kliknite ili dodirnite opciju **Add new policy** (Dodaj nove smernice).
4. Kliknite na strelice nadole da biste izabrali primarni i (opcionalni) sekundarni akreditiv za nove smernice, pa kliknite ili dodirnite opciju **Add** (Dodaj).
5. Kliknite na dugme **Apply** (Primeni).

Da biste odložili početak stupanja na snagu novih ili promenjenih smernica:

1. Kliknite ili dodirnite opciju **Enforce this policy immediately** (Nametni ove smernice odmah).
2. Izaberite opciju **Enforce this policy on the specific date** (Nametni ove smernice od određenog datuma).
3. Unesite željeni datum ili upotrebite iskačući kalendar da biste izabrali datum kada izabrane smernice stupaju na snagu.
4. Ako želite, izaberite kada će korisnici dobiti podsetnik u vezi sa novim smernicama.
5. Kliknite na dugme **Apply** (Primeni).

Smernice za standardne korisnike

Možete konfigurisati smernice prijavljivanja i sesija za standardne korisnike ovog računara. Smernice prijavljivanja koje se ovde podese upravljaju akreditivima pomoću kojih se standardni korisnici prijavljuju u operativni sistem Windows. Smernice sesija koje se ovde podese upravljaju akreditivima pomoću kojih standardni korisnici potvrđuju svoj identitet u okviru Windows sesije.

Sve nove ili promenjene smernice podrazumevano stupaju na snagu odmah nakon što kliknete ili dodirnete dugme **Apply** (Primeni).

Da biste dodali nove smernice:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite ikonu **zupčanika**.
2. Na stranici Advanced Settings (Napredne postavke), kliknite ili dodirnite stavku **Standard User Policies** (Smernice za standardne korisnike).
3. Kliknite ili dodirnite opciju **Add new policy** (Dodaj nove smernice).
4. Kliknite na strelice nadole da biste izabrali primarni i (opcionalni) sekundarni akreditiv za nove smernice, pa kliknite ili dodirnite opciju **Add** (Dodaj).
5. Kliknite na dugme **Apply** (Primeni).

Da biste odložili početak stupanja na snagu novih ili promenjenih smernica:

1. Kliknite ili dodirnite opciju **Enforce this policy immediately** (Nametni ove smernice odmah).
2. Izaberite opciju **Enforce this policy on the specific date** (Nametni ove smernice od određenog datuma).
3. Unesite željeni datum ili upotrebite iskačući kalendar da biste izabrali datum kada izabrane smernice stupaju na snagu.

4. Ako želite, izaberite kada će korisnici dobiti podsetnik u vezi sa novim smernicama.
5. Kliknite na dugme **Apply** (Primeni).

Bezbednosne funkcije

Možete da omogućite bezbednosne funkcije u okviru programa HP Client Security kako biste zaštitili računar od neovlašćenog pristupa.

Da biste podesili bezbednosne funkcije:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite ikonu **zupčanika**.
2. Na stranici Advanced Settings (Napredne postavke), kliknite ili dodirnite stavku **Security Features** (Bezbednosne funkcije).
3. Omogućite bezbednosne funkcije tako što ćete izabrati odgovarajuća polja za potvrdu, a zatim kliknite ili dodirnite dugme **Apply** (Primeni). Što više funkcija izaberete, to će vaš računar biti bezbedniji.

   Ove postavke važe za sve korisnike.

   - **Windows Logon Security** (Bezbednost pri prijavljivanju u Windows)—Štiti vaše Windows naloge tako što zahteva korišćenje akreditiva iz programa HP Client Security za pristup sistemu.
   - **Pre-Boot Security (Power-on authentication)** (Bezbednost pre pokretanja sistema (Provera identiteta pri pokretanju sistema))—Štiti računar pre pokretanja operativnog sistema Windows. Ova opcija nije dostupna ako je BIOS ne podržava.
   - **Allow One Step logon** (Omogući prijavljivanje u jednom koraku)—Ova postavka omogućava da se prijavljivanje u operativni sistem Windows prekoči ako je provera identiteta već obavljena na nivou provere identiteta pri pokretanju sistema ili nivou alatke Drive Encryption.
4. Kliknite ili dodirnite opciju **Users** (Korisnici), a zatim kliknite ili dodirnite pločicu željenog korisnika.

Korisnici

Možete nadgledati i upravljati korisnicima programa HP Client Security na ovom računaru.

Da biste dodali novog Windows korisnika u program HP Client Security:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite ikonu **zupčanika**.
2. Na stranici Advanced Settings (Napredne postavke), kliknite ili dodirnite stavku **Users** (Korisnici).
3. Kliknite ili dodirnite opciju **Add another Windows user to HP Client Security** (Dodaj novog Windows korisnika u HP Client Security).
4. Unesite ime korisnika kojeg želite da dodate, pa kliknite ili dodirnite opciju **OK** (U redu).
5. Unesite Windows lozinku tog korisnika.

   Pločica novog korisnika prikazaće se na stranici sa korisnicima.

Da biste izbrisali Windows korisnika iz programa HP Client Security:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite ikonu **zupčanika**.
2. Na stranici Advanced Settings (Napredne postavke), kliknite ili dodirnite stavku **Users** (Korisnici).
3. Kliknite ili dodirnite ime korisnika kojeg želite da izbrišete.
4. Kliknite ili dodirnite opciju **Delete User** (Izbriši korisnika), a zatim kliknite ili dodirnite **Yes** (Da) da biste potvrdili.

Da biste prikazali rezime smernica prijavljivanja i sesija koje važe za određenog korisnika:

- ▲ Kliknite ili dodirnite opciju **Users** (Korisnici), a zatim kliknite ili dodirnite pločicu željenog korisnika.

Moje smernice

Možete da prikažete svoje smernice za proveru identiteta i status unosa. Na stranici My Policies (Moje smernice) nalaze se i veze ka stranicama Administrators Policies (Smernice za administratore) i Standard User Policies (Smernice za standardne korisnike).

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite ikonu **zupčanika**.
2. Na stranici Advanced Settings (Napredne postavke), kliknite ili dodirnite stavku **My Policies** (Moje smernice).

   Prikazaće se smernice prijavljivanja i sesija koje važe za trenutno prijavljenog korisnika.

Na stranici My Policies (Moje smernice) nalaze se i veze ka stranicama Smernice za administratore na stranici 25 i Smernice za standardne korisnike na stranici 26.

Pravljenje rezervnih kopija i vraćanje podataka u prethodno stanje

Preporučujemo da redovno pravite rezervne kopije podataka iz programa HP Client Security. Koliko često treba praviti rezervne kopije zavisi od toga koliko se često podaci menjaju. Na primer, ako svakodnevno dodajete nove podatke za prijavljivanje, trebalo bi da svakog dana pravite rezervnu kopiju podataka.

Rezervne kopije mogu se koristiti iz migraciju podataka sa jednog računara na drugi, koja se takođe naziva uvoz i izvoz.

NAPOMENA: Pomoću ove funkcije pravi se rezervna kopija samo za alatku Password Manager. Alatka Drive Encryption poseduje zaseban način pravljenja rezervnih kopija. Za Device Access Manager i potvrdu identiteta pomoću otiska prsta ne mogu se praviti rezervne kopije.

Da bi se podaci vratili iz rezervne kopije, potrebno je da program HP Client Security bude instaliran na računaru na koji se prebacuju podaci.

Da biste napravili rezervnu kopiju podataka:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite ikonu **zupčanika**.
2. Na stranici Advanced Settings (Napredne postavke), kliknite ili dodirnite stavku **Administrator Policies** (Smernice za administratore).
3. Kliknite ili dodirnite opciju **Backup and Restore** (Rezervne kopije i vraćanje).

4. Kliknite ili dodirnite opciju **Backup** (Napravi rezervnu kopiju), a zatim potvrdite svoj identitet.
5. Izaberite modul čije podatke želite da obuhvatite rezervnom kopijom, a zatim kliknite ili dodirnite dugme **Next** (Dalje).
6. Unesite ime datoteke za skladištenje. Datoteka će podrazumevano biti sačuvana u fascikli Dokumenti. Da biste izabrali drugu lokaciju, kliknite ili dodirnite stavku **Browse** (Potraži).
7. Unesite i potvrdite lozinku da biste zaštitili datoteku.
8. Kliknite ili dodirnite dugme **Save** (Sačuvaj).

Da biste vratili podatke u prethodno stanje:

1. Na matičnoj stranici programa HP Client Security, kliknite ili dodirnite ikonu **zupčanika**.
2. Na stranici Advanced Settings (Napredne postavke), kliknite ili dodirnite stavku **Administrator Policies** (Smernice za administratore).
3. Kliknite ili dodirnite opciju **Backup and Restore** (Rezervne kopije i vraćanje).
4. Izaberite opciju **Restore** (Vrati), a zatim potvrdite svoj identitet.
5. Izaberite datoteku za skladištenje koju ste prethodno kreirali. Unesite putanju do datoteke u odgovarajuće polje. Da biste izabrali drugu lokaciju, kliknite ili dodirnite stavku **Browse** (Potraži).
6. Unesite lozinku kojom je datoteka zaštićena, a zatim kliknite ili dodirnite dugme **Next** (Dalje).
7. Izaberite module čije podatke želite da vratite.
8. Kliknite ili dodirnite opciju **Restore** (Vrati).

5 HP Drive Encryption (samo na odabranim modelima)

HP Drive Encryption pruža sveobuhvatnu zaštitu podataka tako što šifruje podatke na računaru. Kada je alatka Drive Encryption aktivirana, potrebno je da se prijavite na ekranu Drive Encryption, koji se prikazuje pre pokretanja operativnog sistema Windows®.

Na početnom ekranu programa HP Client Security, administratori operativnog sistema Windows mogu da aktiviraju Drive Encryption, naprave rezervnu kopiju ključa za šifrovanje, kao i da izaberu ili ponište izbor disk jedinice ili particije za šifrovanje. Dodatne informacije potražite u pomoći za softver HP Client Security.

Pomoću alatke Drive Encryption možete obaviti sledeće zadatke:

- Izbor postavki za Drive Encryption:
  - Šifrovanje ili dešifrovanje pojedinačnih disk jedinica ili particija pomoću softverskog šifrovanja
  - Šifrovanje ili dešifrovanje pojedinačnih disk jedinica sa sopstvenim šifrovanjem pomoću hardverskog šifrovanja
  - Dodavanje dodatnog sloja bezbednosti onemogućavanjem režima spavanja ili stanja mirovanja kako bi provera identiteta pre pokretanja sistema koju sprovodi Drive Encryption uvek bila aktivirana

NAPOMENA: Mogu se šifrovati samo interni SATA i eSATA spoljašnji čvrsti diskovi.

- Kreiranje rezervne kopije ključeva
- Ponovno omogućavanje pristupa šifrovanom računaru pomoću rezervne kopije ključeva i funkcije HP SpareKey
- Omogućavanje provere identiteta pre pokretanja sistema koju sprovodi Drive Encryption pomoću lozinke, registrovanog otiska prsta ili PIN koda za određene pametne kartice

Otvaranje alatke Drive Encryption

Administratori mogu da pristupe alatki Drive Encryption tako što će otvoriti program HP Client Security:

1. Na početnom ekranu, kliknite ili dodirnite stavku **HP Client Security** (Windows 8).

   – ili –

   Na Windows radnoj površini, dvaput kliknite ili dodirnite dvaput ikonu **HP Client Security** u polju za obaveštavanje, koje se nalazi u desnom uglu trake zadataka.

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

Opšti zadaci

Aktiviranje alatke Drive Encryption na standardnim čvrstim diskovima

Standardni čvrsti diskovi šifruju se softverskim šifrovanjem. Pratite sledeće korake da biste šifrovali disk jedinicu ili particiju diska:

1. Pokrenite alatku **Drive Encryption**. Više informacija potražite u odeljku Otvaranje alatke Drive Encryption na stranici 30.
2. Izaberite polje za potvrdu za disk jedinicu ili particiju koju želite da šifrujete, pa kliknite ili dodirnite opciju **Napravi rezervnu kopiju ključa**.

NAPOMENA: Radi veće bezbednosti, izaberite polje za potvrdu **Onemogućite režim spavanja radi povećane bezbednosti**. Ako onemogućite režim spavanja, nema opasnosti da će akreditivi koji se koriste za otključavanje disk jedinice biti sačuvani u memoriji.

3. Izaberite jednu ili više opcija za pravljenje rezervne kopije, pa kliknite ili dodirnite opciju **Napravi rezervnu kopiju**. Više informacija potražite u odeljku Pravljenje rezervne kopije ključeva za šifrovanje na stranici 34.
4. Dok je u toku pravljenje rezervne kopije ključa za šifrovanje, možete nastaviti sa radom. Nemojte ponovo pokretati računar.

NAPOMENA: Od vas će se tražiti da ponovo pokrenete računar. Nakon ponovnog pokretanja, prikazaće se Drive Encryption ekran za proveru identiteta pre pokretanja sistema, a zatim će se pokrenuti operativni sistem Windows.

Alatka Drive Encryption je aktivirana. Šifrovanje izabranih particija diska mogu trajati nekoliko sati, u zavisnosti od broja i veličina particija.

Dodatne informacije potražite u pomoći za softver HP Client Security.

Aktiviranje alatke Drive Encryption na disk jedinicama sa sopstvenim šifrovanjem

Disk jedinice sa sopstvenim šifrovanjem koje ispunjavaju OPAL specifikaciju organizacije Trusted Computing Group za upravljanje disk jedinicama sa sopstvenim šifrovanjem mogu se šifrovati softverskim ili hardverskim putem. Hardversko šifrovanje je mnogo brže od softverskog šifrovanja. Međutim, nije moguće izabrati koje particije diska želite da šifrujete. Šifruje se cela disk jedinica sa svim particijama.

Ako želite da šifrujete samo određene particije, moraćete da koristite softversko šifrovanje. Poništite izbor polja za potvrdu **Dozvoli samo hardversko šifrovanje za disk jedinice sa sopstvenim šifrovanjem (Self-Encrypting Drives, SED)**.

Pratite sledeće korake da biste aktivirali funkciju Drive Encryption za disk jedinice sa sopstvenim šifrovanjem.

1. Pokrenite alatku **Drive Encryption**. Više informacija potražite u odeljku Otvaranje alatke Drive Encryption na stranici 30.
2. Izaberite polje za potvrdu za disk jedinicu koju želite da šifrujete, pa kliknite ili dodirnite opciju **Napravi rezervnu kopiju ključa**.

NAPOMENA: Radi veće bezbednosti, izaberite polje za potvrdu **Onemogućite režim spavanja radi povećane bezbednosti**. Ako onemogućite režim spavanja, nema opasnosti da će akreditivi koji se koriste za otključavanje disk jedinice biti sačuvani u memoriji.

3. Izaberite jednu ili više opcija za pravljenje rezervne kopije, pa kliknite ili dodirnite opciju **Napravi rezervnu kopiju**. Više informacija potražite u odeljku Pravljenje rezervne kopije ključeva za šifrovanje na stranici 34.

4. Dok je u toku pravljenje rezervne kopije ključa za šifrovanje, možete nastaviti sa radom. Nemojte ponovo pokretati računar.

NAPOMENA: Kod disk jedinica sa sopstvenim šifrovanjem, od vas će se tražiti da isključite računar.

Dodatne informacije potražite u pomoći za softver HP Client Security.

Deaktiviranje alatke Drive Encryption

1. Pokrenite alatku **Drive Encryption**. Više informacija potražite u odeljku Otvaranje alatke Drive Encryption na stranici 30.

2. Poništite izbor polja za potvrdu za sve šifrovane disk jedinice, a zatim kliknite ili dodirnite **Primeni**.

   Deaktivacija alatke Drive Encryption će započeti.

NAPOMENA: Ako je upotrebljeno softversko šifrovanje, započeće dešifrovanje. Ovaj proces može potrajati nekoliko sati, u zavisnosti od veličine particija na šifrovanom čvrstom disku. Kada se dešifrovanje završi, alatka Drive Encryption biće deaktivirana.

Ako je upotrebljeno hardversko šifrovanje, disk jedinica biće automatski dešifrovana, a nakon nekoliko minuta, alatka Drive Encryption će se deaktivirati.

Nakon što se alatka Drive Encryption deaktivira, od vas će se tražiti da isključite računar, u slučaju hardverskog šifrovanja, ili da ponovo pokrenete računar, u slučaju softverskog šifrovanja.

Prijavljivanje nakon što se aktivira Drive Encryption

Kada uključite računar nakon što se aktivira Drive Encryption, a vaš korisnički nalog je obuhvaćen, biće potrebno da se prijavite na ekranu za prijavljivanje alatke Drive Encryption.

NAPOMENA: Prilikom buđenja sistema iz režima spavanja ili mirovanja, provera identiteta pre pokretanja sistema alatke Drive Encryption ne prikazuje se ni kod softverskog, ni kod hardverskog šifrovanja. Hardversko šifrovanje nudi opciju **Onemogućite režim spavanja radi povećane bezbednosti**, koja, kada se omogući, sprečava da računar pređe u režim spavanja ili mirovanja.

Prilikom buđenja sistema iz hibernacije, provera identiteta pre pokretanja sistema alatke Drive Encryption prikazuje se i kod softverskog, i kod hardverskog šifrovanja.

NAPOMENA: Ako je administrator operativnog sistema Windows omogućio BIOS Pre-boot Security (Bezbednost pre pokretanja sistema u BIOS-u) u okviru programa HP Client Security, a omogućena je i opcija One-Step Logon (Prijavljivanje u jednom koraku) (podrazumevano), moći ćete da se prijavite na računar odmah nakon provere identiteta na ekranu BIOS Pre-boot, bez potrebe za ponovnom proverom identiteta na ekranu za prijavljivanje alatke Drive Encryption.

Prijavljivanje jednog korisnika:

- Na stranici **Prijava** unesite svoju Windows lozinku, PIN pametne kartice, SpareKey ili prevucite registrovanim prstom preko senzora.

Prijavljivanje ako postoji više korisnika:

1. Na ekranu **Izaberite korisnika za prijavljivanje** sa padajuće liste izaberite korisnika koji želi da se prijavi, a zatim kliknite ili dodirnite dugme **Dalje**.
2. Na stranici **Prijava** unesite svoju Windows lozinku, PIN pametne kartice ili prevucite registrovanim prstom preko senzora.

NAPOMENA: Podržani su sledeći tipovi pametnih kartica:

Podržane pametne kartice

- Gemalto Cyberflex Access 64k V2c

NAPOMENA: Ako se za prijavljivanje na ekranu za prijavljivanje alatke Drive Encryption koristi ključ za oporavak, na ekranu za prijavljivanje u operativni sistem Windows biće potrebno uneti dodatne akreditive za pristup korisničkim nalozima.

Šifrovanje dodatnih čvrstih diskova

Preporučujemo da koristite HP Drive Encryption da biste zaštitili svoje podatke šifrovanjem čvrstog diska. Nakon aktiviranja, možete šifrovati dodatne čvrste diskove ili kreirane particije tako što ćete pratiti sledeće korake:

1. Pokrenite alatku **Drive Encryption**. Više informacija potražite u odeljku Otvaranje alatke Drive Encryption na stranici 30.
2. Kod čvrstih diskova koji su šifrovani softverski, izaberite particije diska koje želite da šifrujete.

NAPOMENA: To važi i za scenarije sa mešanim disk jedinicama, kod kojih je prisutan jedan ili više standardnih čvrstih diskova i jedna ili više disk jedinica sa sopstvenim šifrovanjem.

– ili –

▲ Kod čvrstih diskova koji su šifrovani hardverski, izaberite dodatne disk jedinice koje želite da šifrujete.

Napredni zadaci

Upravljanje alatkom Drive Encryption (za administratore)

Administratori mogu da koriste Drive Encryption da bi pogledali i promenili status šifrovanja (Nije šifrovan ili Šifrovan) svih čvrstih diskova na računaru.

- Ako je status alatke Omogućeno, alatka Drive Encryption je aktivirana i konfigurisana. Disk jedinica može biti u nekom od sledećih stanja:

Softversko šifrovanje

- Nije šifrovan
- Šifrovan
- Šifrovanje
- Dešifrovanje

Hardversko šifrovanje

- Šifrovan
- Nije šifrovan (za dodatne disk jedinice)

Šifrovanje ili dešifrovanje pojedinačnih particija diska (samo za softversko šifrovanje)

Administratori mogu koristiti alatku Drive Encryption za šifrovanje jedne ili više particija čvrstih diskova na računaru ili dešifrovanje particija koje su već šifrovane.

1. Pokrenite alatku **Drive Encryption**. Više informacija potražite u odeljku Otvaranje alatke Drive Encryption na stranici 30.
2. U odeljku **Drive Status** (Status disk jedinice), izaberite ili poništite izbor polja za potvrdu pored particija čvrstog diska koje želite da šifrujete ili dešifrujete, a zatim kliknite ili dodirnite dugme **Primeni**.

NAPOMENA: Dok je u toku šifrovanje ili dešifrovanje particije, traka toka pokazuje koliko procenata particije je šifrovano.

NAPOMENA: Dinamičke particije nisu podržane. Ako se particija prikazuje kao dostupna, ali se ne može šifrovati kada je izabrana, to znači da je u pitanju dinamička particija. Dinamička particija nastaje usled smanjivanja particije kako bi se kreirala nova particija pomoću funkcije Upravljanje diskovima.

Pre konvertovanja particije u dinamičku particiju prikazuje se upozorenje.

Upravljanje diskovima

- **Nadimak**—Možete dodeliti imena disk jedinicama ili particijama radi lakše identifikacije.
- **Disk jedinice koje nisu povezane**—Drive Encryption može pratiti diskove koji su uklonjeni sa računara. Disk koji se ukloni sa računara automatski se premešta na listu Nije povezan. Ako disk bude vraćen u sistem, ponovo će se prikazivati na listi Povezan.
- Ako više ne budete želeli da pratite ili upravljate diskom koji nije povezan, možete ga ukloniti sa liste Nije povezan.
- Alatka Drive Encryption ostaće aktivirana sve dok ne poništite izbor polja za potvrdu za sve povezane disk jedinice i dok lista Nije povezan ne bude prazna.

Pravljenje rezervnih kopija i oporavak (za administratore)

Kada je alatka Drive Encryption aktivirana, administratori mogu da koriste stranicu Rezervna kopija ključa za šifrovanje kako bi napravili rezervnu kopiju ključeva za šifrovanje na prenosnim medijumima ili pokrenuli proces oporavka.

Pravljenje rezervne kopije ključeva za šifrovanje

Administratori mogu napraviti rezervnu kopiju ključa za šifrovanje za šifrovanu disk jedinicu i sačuvati je na prenosnom uređaju za skladištenje.

OPREZ: Uređaj za skladištenje sa rezervnom kopijom ključa čuvajte na bezbednom mestu jer vam on jedini omogućava da pristupite računaru u slučaju da zaboravite lozinku ili izgubite pametnu karticu, a niste registrovali prst. Mesto za skladištenje mora biti bezbedno jer uređaj za skladištenje omogućava pristupanje operativnom sistemu Windows.

1. Pokrenite alatku **Drive Encryption**. Više informacija potražite u odeljku Otvaranje alatke Drive Encryption na stranici 30.
2. Izaberite polje za potvrdu pored željene disk jedinice, a zatim kliknite ili dodirnite opciju **Napravi rezervnu kopiju ključa**.
3. U odeljku **Kreirajte ključ za oporavak za HP Drive Encryption**, izaberite jednu ili više opcija:
   - **Prenosno skladištenje**—Izaberite polje za potvrdu, a zatim izaberite uređaj za skladištenje na kojem će ključ za šifrovanje biti sačuvan.
   - **SkyDrive**—Izaberite polje za potvrdu. Potrebno je da budete povezani na Internet. Prijavite se na Microsoft SkyDrive, pa kliknite ili dodirnite **Da**.

     NAPOMENA: Da biste koristili rezervnu kopiju ključa iz alatke HP Drive Encryption koja je sačuvana u usluzi SkyDrive, potrebno je da je preuzmete sa usluge SkyDrive na prenosni uređaj za skladištenje, a zatim umetnete uređaj za skladištenje u računar.
   - **TPM** (samo na određenim modelima)—Omogućava vam da oporavite podatke pomoću TPM lozinke.

     OPREZ: Ako se TPM obriše ili se vaš računar ošteti, izgubićete pristup ovoj rezervnoj kopiji. Ako izaberete ovaj metod, trebalo bi da izaberete još jedan metod pravljenja rezervne kopije.
4. Kliknite ili dodirnite dugme **Napravi rezervnu kopiju**.

   Ključ za šifrovanje biće sačuvan na izabranom uređaju za skladištenje.

Ponovno omogućavanje pristupa aktiviranom računaru pomoću rezervne kopije ključeva

Administratori mogu obaviti oporavak pomoću ključa za Drive Encryption čija je rezervna kopija sačuvana na prenosnom uređaju za skladištenje ili tako što će izabrati opciju **Napravi rezervnu kopiju ključa** u okviru alatke Drive Encryption.

1. Umetnite prenosni uređaj za skladištenje na kojem se nalazi rezervna kopija ključa.
2. Uključite računar.
3. Kada se otvori dijalog za prijavljivanje alatke HP Drive Encryption, kliknite ili dodirnite **Oporavak**.
4. Unesite putanju do datoteke ili ime datoteke koje sadrži rezervnu kopiju ključa, a zatim kliknite ili dodirnite **Oporavak**.
5. Kada se otvori dijalog za potvrdu, kliknite ili dodirnite **U redu**.

   Prikazaće se ekran za prijavljivanje operativnog sistema Windows.

NAPOMENA: Ako se za prijavljivanje na ekranu za prijavljivanje alatke Drive Encryption koristi ključ za oporavak, na ekranu za prijavljivanje u operativni sistem Windows biće potrebno uneti dodatne akreditive za pristup korisničkim nalozima. Preporučujemo da resetujete lozinku nakon što obavite oporavak.

Obavljanje oporavka pomoću funkcije HP SpareKey

Oporavak pomoću funkcije HP SpareKey u okviru ekrana pre pokretanja sistema alatke Drive Encryption zahteva da tačno odgovorite na bezbednosna pitanja da biste pristupili računaru. Dodatne informacije o podešavanju oporavka pomoću funkcije HP SpareKey potražite u pomoći za softver HP Client Security.

Da biste obavili oporavak pomoću funkcije HP SpareKey ako zaboravite lozinku:

1. Uključite računar.
2. Kada se prikaže stranica HP Drive Encryption, idite na stranicu za prijavljivanje korisnika.
3. Kliknite na dugme **SpareKey** (U redu).

   NAPOMENA: Ako niste aktivirali SpareKey u okviru programa HP Client Security, dugme **SpareKey** neće biti dostupno.

4. Unesite tačne odgovore na prikazana pitanja, a zatim kliknite ili dodirnite **Logon** (Prijava).

   Prikazaće se ekran za prijavljivanje operativnog sistema Windows.

NAPOMENA: Ako se za prijavljivanje na ekranu za prijavljivanje alatke Drive Encryption koristi SpareKey, na ekranu za prijavljivanje u operativni sistem Windows biće potrebno uneti dodatne akreditive za pristup korisničkim nalozima. Preporučujemo da resetujete lozinku nakon što obavite oporavak.

6 HP File Sanitizer (samo na odabranim modelima)

File Sanitizer vam omogućuje da bezbedno obrišete sredstva (na primer: lične informacije ili datoteke, podatke iz istorije ili sa veba ili druge komponente koje sadrže podatke) na internom čvrstom disku računara, kao i da povremeno sakrijete slobodan prostor na internom čvrstom disku.

File Sanitizer ne može se koristiti za brisanje datoteka ili sakrivanje slobodnog prostora na sledećim tipovima disk jedinica:

- Solid-state uređajima (SSD), uključujući RAID volumene koji obuhvataju SSD uređaj
- Eksterne disk jedinice koje su povezane preko USB, Firewire ili eSATA interfejsa

Ako pokušate da obavite operaciju sigurnog brisanja ili sakrivanja slobodnog prostora na SSD disku, prikazaće se poruka upozorenja i operacija neće biti obavljena.

Sigurno brisanje

Sigurno brisanje razlikuje se od standardne radnje brisanja u operativnom sistemu Windows®. Kada sigurno obrišete neku stavku pomoću alatke File Sanitizer, datoteke će biti zamenjene besmislenim podacima, čime se u potpunosti onemogućava bilo kakvo buduće pristupanje originalnoj stavki. Nakon običnog brisanja u operativnom sistemu Windows, datoteka (ili stavka) može se zadržati netaknuta na čvrstom disku ili takva da se može preuzeti forenzičkim metodama.

Možete zakazati vreme u koje će se sigurno brisanje pokretati u budućnosti ili ga možete ručno pokrenuti tako što ćete izabrati ikonu **File Sanitizer** na početnom ekranu programa HP Client Security ili ikonu **File Sanitizer** na Windows radnoj površini. Za više informacija pogledajte odeljak Podešavanje rasporeda sigurnog brisanja na stranici 39, Sigurno brisanje desnim klikom na stranici 41 ili Ručno pokretanje operacije sigurnog brisanja na stranici 41.

NAPOMENA: .dll datoteke sigurno se brišu i uklanjaju iz sistema samo ako ste ih premestili u Korpu za otpatke.

Skrivanje slobodnog prostora

Brisanjem stavki u operativnom sistemu Windows sadržaj stavke ne uklanja se u potpunosti sa čvrstog diska. Windows briše samo reference na tu stavku ili njenu lokaciju na čvrstom disku. Sadržaj stavke ostaje na čvrstom disku sve dok se čuvanjem neke druge stavke ta oblast čvrstog diska ne zameni novim informacijama.

Skrivanje slobodnog prostora omogućava vam da bezbedno upišete nasumične podatke preko izbrisanih stavki, čime se sprečava pristupanje originalnom sadržaju izbrisane stavke.

NAPOMENA: Skrivanje slobodnog prostora ne pruža dodatnu bezbednost nakon sigurnog brisanja stavke.

Možete zakazati vreme u koje će se skrivanje slobodnog prostora pokretati u budućnosti ili ga možete ručno pokrenuti tako što ćete izabrati ikonu **File Sanitizer** na početnom ekranu programa HP Client Security ili ikonu **File Sanitizer** na Windows radnoj površini. Za dodatne informacije pogledajte Podešavanje rasporeda skrivanja slobodnog prostora na stranici 40, Ručno pokretanje skrivanja slobodnog prostora na stranici 42 ili Korišćenje ikone File Sanitizer na stranici 41.

Otvaranje alatke File Sanitizer

1. Na početnom ekranu, kliknite ili dodirnite stavku **HP Client Security** (Windows 8).

   – ili –

   Na Windows radnoj površini, dvaput kliknite ili dodirnite dvaput ikonu **HP Client Security** u polju za obaveštavanje, koje se nalazi u desnom uglu trake zadataka.

2. U odeljku **Data** (Podaci), kliknite ili dodirnite stavku **File Sanitizer**.

– ili –

▲ Dvaput kliknite ili dodirnite dvaput ikonu **File Sanitizer** na Windows radnoj površini.

– ili –

▲ Kliknite desnim tasterom miša ili dodirnite i držite ikonu **File Sanitizer** na Windows radnoj površini, pa izaberite opciju **Otvori File Sanitizer**.

Postupci podešavanja

Sigurno brisanje—File Sanitizer služi za sigurno brisanje izabranih kategorija stavki.

1. U odeljku **Sigurno brisanje**, izaberite polje za potvrdu za svaki tip datoteka koje želite sigurno da obrišete ili poništite izbor polja za potvrdu za datoteke koje ne želite da obrišete.

   - **Korpa za otpatke**—Sigurno brisanje svih stavki koje se nalaze u Korpi za otpatke.
   - **Privremene sistemske datoteke**—Sigurno brisanje svih stavki koje se nalaze u fascikli sa privremenim sistemskim datotekama. Sledeće promenljive okruženja pretražuju se sledećim redosledom, a prva pronađena putanja smatra se sistemskom fasciklom:
     - TMP
     - TEMP
   - **Privremene Internet datoteke**—Sigurno brisanje kopija veb stranica, slika i medijuma koje veb pregledači čuvaju radi bržeg prikazivanja stranica.
   - **Kolačići**—Sigurno brisanje svih datoteka koje veb lokacije skladište na računaru radi čuvanja željenih opcija, kao što su podaci za prijavljivanje.

2. Da biste započeli sigurno brisanje, kliknite ili dodirnite opciju **Sigurno brisanje datoteke**.

Skrivanje—Upisivanje nasumičnih podataka u slobodan prostor, čime se sprečava vraćanje izbrisanih stavki.

▲ Da biste započeli skrivanje, kliknite ili dodirnite opciju **Sakrij**.

File Sanitizer Options (Opcije alatke File Sanitizer)—Izaberite polje za potvrdu da biste omogućili sledeće opcije ili poništite izbor polja za potvrdu da biste onemogućili pojedine opcije:

- **Omogući ikonu na radnoj površini**—Prikazivanje ikone alatke File Sanitizer na Windows radnoj površini.
- **Enable right-click** (Omogući desni klik)—Omogućava vam da kliknete desnim tasterom miša ili da dodirnete i zadržite željenu stavku, a zatim da izaberete opciju **HP File Sanitizer – Sigurno obriši**.

- **Traži Windows lozinku pre ručnog sigurnog brisanja**—Pre ručnog pokretanja sigurnog brisanja, potrebno je uneti Windows lozinku radi provere identiteta.
- **Sigurno obriši kolačiće i privremene datoteke sa Interneta prilikom zatvaranja pregledača**—Sigurno brisanje svih stavki u vezi sa vebom, kao što je istorija posećenih URL adresa, prilikom zatvaranja veb pregledača.

Podešavanje rasporeda sigurnog brisanja

Možete zakazati vreme u koje će se automatski pokretati sigurno brisanje, a možete i ručno sigurno brisati stavke u bilo kom trenutku. Više informacija potražite u Postupci podešavanja na stranici 38.

1. Otvorite File Sanitizer, pa kliknite ili dodirnite **Postavke**.
2. Da biste zakazali vreme u koje će se ubuduće pokretati sigurno brisanje izabranih stavki, u okviru odeljka **Raspored sigurnog brisanja**, izaberite opciju **Nikada**, **Jednom**, **Svakog dana**, **Jednom nedeljno** ili **Jednom mesečno**, a zatim izaberite dan i vreme:
   a. Kliknite ili dodirnite polje za sate, minute ili AM/PM (prepodne/popodne).
   b. Krećite se kroz listu brojeva sve dok se željena vrednost ne prikaže u nivou ostalih polja.
   c. Kliknite ili dodirnite prazan prostor oko polja za podešavanje vremena.
   d. Ponovite ovaj postupak za svako polje sve dok ne podesite pravilan raspored.
3. Dostupna su sledeća četiri tipa stavki:
   - **Korpa za otpatke**—Sigurno brisanje svih stavki koje se nalaze u Korpi za otpatke.
   - **Privremene sistemske datoteke**—Sigurno brisanje svih stavki koje se nalaze u fascikli sa privremenim sistemskim datotekama. Sledeće promenljive okruženja pretražuju se sledećim redosledom, a prva pronađena putanja smatra se sistemskom fasciklom:
     - TMP
     - TEMP
   - **Privremene Internet datoteke**—Sigurno brisanje kopija veb stranica, slika i medijuma koje veb pregledači čuvaju radi bržeg prikazivanja stranica.
   - **Kolačići**—Sigurno brisanje svih datoteka koje veb lokacije skladište na računaru radi čuvanja željenih opcija, kao što su podaci za prijavljivanje.

   Ako ih izaberete, ove stavke biće sigurno obrisane u zakazano vreme.
4. Da biste izabrali dodatne stavke za sigurno brisanje:
   a. U odeljku **Stavke za zakazano brisanje**, kliknite ili dodirnite opciju **Dodaj fasciklu**, a zatim idite do željene datoteke ili fascikle.
   b. Kliknite ili dodirnite opciju **Otvori**, a zatim kliknite ili dodirnite **U redu**.

   Da biste uklonili određenu stavku sa liste stavki za koje je zakazano sigurno brisanje, poništite izbor polja za potvrdu pored te stavke.

Podešavanje rasporeda skrivanja slobodnog prostora

Skrivanje slobodnog prostora ne pruža dodatnu bezbednost nakon sigurnog brisanja stavke.

1. Otvorite File Sanitizer, pa kliknite ili dodirnite **Postavke**.
2. Da biste zakazali vreme u koje će se pokretati skrivanje slobodnog prostora na čvrstom disku, u okviru odeljka **Raspored skrivanja**, izaberite opciju **Nikada**, **Jednom**, **Svakog dana**, **Jednom nedeljno** ili **Jednom mesečno**, a zatim izaberite dan i vreme.
   a. Kliknite ili dodirnite polje za sate, minute ili AM/PM (prepodne/popodne).
   b. Krećite se kroz listu brojeva sve dok se željeno vreme ne prikaže u nivou ostalih polja.
   c. Kliknite ili dodirnite prazan prostor oko polja za podešavanje vremena.
   d. Ponovite ovaj postupak sve dok ne podesite pravilan raspored.

NAPOMENA: Operacija skrivanja slobodnog prostora može potrajati. Vodite računa da računar bude priključen na napajanje naizmeničnom strujom. Iako se skrivanje slobodnog prostora obavlja u pozadini, povećana zauzetost procesora može negativno uticati na performanse računara. Skrivanje slobodnog prostora možete obavljati nakon radnog vremena ili u periodu kada se računar ne koristi.

Zaštita datoteka od sigurnog brisanja

Da biste zaštitili datoteke ili fascikle od sigurnog brisanja:

1. Otvorite File Sanitizer, pa kliknite ili dodirnite **Postavke**.
2. U odeljku **Stavke koje nisu za sigurno brisanje**, kliknite ili dodirnite opciju **Dodaj fasciklu**, a zatim idite do željene datoteke ili fascikle.
3. Kliknite ili dodirnite opciju **Otvori**, a zatim kliknite ili dodirnite **U redu**.

NAPOMENA: Datoteke sa ove liste biće zaštićene sve dok se nalaze na listi.

Da biste uklonili određenu stavku sa liste izuzetaka, poništite izbor polja za potvrdu pored te stavke.

Opšti zadaci

Koristite File Sanitizer za obavljanje sledećih zadataka:

- **Pokretanje sigurnog brisanja pomoću ikone File Sanitizer**—Prevucite datoteke na ikonu **File Sanitizer** na Windows radnoj površini. Više detalja potražite u odeljku Korišćenje ikone File Sanitizer na stranici 41.
- **Ručno sigurno brisanje određene stavke ili svih izabranih stavki**—Sigurno obrišite željene stavke u bilo kom trenutku, bez potrebe da čekate zakazano sigurno brisanje. Više detalja potražite u odeljcima Sigurno brisanje desnim klikom na stranici 41 ili Ručno pokretanje operacije sigurnog brisanja na stranici 41.
- **Ručno pokretanje skrivanja slobodnog prostora**—Aktivirajte skrivanje slobodnog prostora u bilo kom trenutku. Više detalja potražite u odeljku Ručno pokretanje skrivanja slobodnog prostora na stranici 42.
- **Prikazivanje datoteka evidencije**—Prikažite datoteke evidencije za operacije sigurnog brisanja i skrivanja slobodnog prostora u kojima se nalaze zapisi o greškama i neuspelim pokušajima iz prethodne operacije sigurnog brisanja ili skrivanja slobodnog prostora. Više detalja potražite u odeljku Prikazivanje datoteka evidencije na stranici 42.

NAPOMENA: Operacija sigurnog brisanja ili skrivanja slobodnog prostora može potrajati. Iako se sigurno brisanje i skrivanje slobodnog prostora obavljaju u pozadini, povećana zauzetost procesora može negativno uticati na performanse računara.

Korišćenje ikone File Sanitizer

OPREZ: Sigurno izbrisane stavke ne mogu se vratiti. Vodite računa koje ćete stavke izabrati za ručno sigurno brisanje.

Kada ručno pokrenete operaciju sigurnog brisanja, biće obrisane stavke koje se nalaze na standardnoj listi za sigurno brisanje na ekranu File Sanitizer (pogledajte Postupci podešavanja na stranici 38).

Operaciju sigurnog brisanja možete pokrenuti ručno na neki od sledećih načina:

1. Otvorite File Sanitizer (pogledajte Otvaranje alatke File Sanitizer na stranici 38), pa kliknite ili dodirnite opciju **Sigurno brisanje datoteke**.
2. Kada se otvori dijalog za potvrdu, proverite da li su izabrane sve stavke koje želite sigurno da obrišete, pa kliknite ili dodirnite **U redu**.

– ili –

1. Kliknite desnim tasterom miša ili dodirnite i držite ikonu **File Sanitizer** na Windows radnoj površini, pa kliknite ili dodirnite opciju **Sigurno obriši odmah**.
2. Kada se otvori dijalog za potvrdu, proverite da li su izabrane sve stavke koje želite sigurno da obrišete, pa kliknite ili dodirnite opciju **Sigurno brisanje datoteke**.

Sigurno brisanje desnim klikom

OPREZ: Sigurno izbrisane stavke ne mogu se vratiti. Vodite računa koje ćete stavke izabrati za ručno sigurno brisanje.

Ako je opcija **Omogući sigurno brisanje desnim klikom** izabrana na ekranu File Sanitizer, možete sigurno obrisati željenu stavku na sledeći način:

1. Idite do dokumenta ili fascikle koju želite sigurno da obrišete.
2. Kliknite desnim tasterom miša ili dodirnite i držite željenu datoteku ili fasciklu, pa izaberite **HP File Sanitizer – Sigurno brisanje datoteke**.

Ručno pokretanje operacije sigurnog brisanja

OPREZ: Sigurno izbrisane stavke ne mogu se vratiti. Vodite računa koje ćete stavke izabrati za ručno sigurno brisanje.

Kada ručno pokrenete operaciju sigurnog brisanja, biće obrisane stavke koje se nalaze na standardnoj listi za sigurno brisanje na ekranu File Sanitizer (pogledajte Postupci podešavanja na stranici 38).

Operaciju sigurnog brisanja možete pokrenuti ručno na neki od sledećih načina:

1. Otvorite File Sanitizer (pogledajte Otvaranje alatke File Sanitizer na stranici 38), pa kliknite ili dodirnite opciju **Sigurno brisanje datoteke**.
2. Kada se otvori dijalog za potvrdu, proverite da li su izabrane sve stavke koje želite sigurno da obrišete, pa kliknite ili dodirnite **U redu**.

– ili –

1. Kliknite desnim tasterom miša ili dodirnite i držite ikonu **File Sanitizer** na Windows radnoj površini, pa kliknite ili dodirnite opciju **Sigurno obriši odmah**.
2. Kada se otvori dijalog za potvrdu, proverite da li su izabrane sve stavke koje želite sigurno da obrišete, pa kliknite ili dodirnite opciju **Sigurno brisanje datoteke**.

Ručno pokretanje skrivanja slobodnog prostora

Kada ručno pokrenete operaciju skrivanja, biće skrivene stavke koje se nalaze na standardnoj listi za sigurno brisanje na ekranu File Sanitizer (pogledajte Postupci podešavanja na stranici 38).

Operaciju skrivanja možete pokrenuti ručno na neki od sledećih načina:

1. Otvorite File Sanitizer (pogledajte Otvaranje alatke File Sanitizer na stranici 38), pa kliknite ili dodirnite opciju **Sakrij**.
2. Kada se otvori dijalog za potvrdu, kliknite ili dodirnite **U redu**.

– ili –

1. Kliknite desnim tasterom miša ili dodirnite i držite ikonu **File Sanitizer** na Windows radnoj površini, pa kliknite ili dodirnite opciju **Sakrij odmah**.
2. Kada se otvori dijalog za potvrdu, kliknite ili dodirnite **Sakrij**.

Prikazivanje datoteka evidencije

Prilikom svake operacije sigurnog brisanja ili skrivanje slobodnog prostora, generišu se datoteke evidencije u kojima se nalaze zapisi o greškama i neuspelim pokušajima. Datoteke evidencije ažuriraju se nakon svake operacije sigurnog brisanja ili skrivanja slobodnog prostora.

NAPOMENA: Datoteke koje su uspešno sigurno izbrisane ili skrivene neće biti prikazane u datotekama evidencije.

Jedna datoteka evidencije kreira se za operacije sigurnog brisanja, a druga za operacije skrivanja slobodnog prostora. Obe datoteke evidencije nalaze se u sledećim fasciklama na čvrstom disku:

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

Kod 64-bitnih sistema, datoteke evidencije nalaze se u sledećim fasciklama na čvrstom disku:

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

7 HP Device Access Manager (samo na odabranim modelima)

HP Device Access Manager upravlja pristupom podacima tako što onemogućava uređaje za prenos podataka.

NAPOMENA: Device Access Manager ne upravlja nekim uređajima za ljudski interfejs/uređajima za unos, kao što su miš, tastatura, dodirna tabla i čitač otiska prsta. Više informacija potražite u odeljku Klase uređaja za koje nije dostupno upravljanje na stranici 46.

Administratori operativnog sistema Windows® koriste alatku HP Device Access Manager za upravljanje pristupom uređajima na sistemu i za zaštitu od neovlašćenog pristupa:

- Za svakog korisnika kreiraju se profili uređaja u kojima se definiše kojim uređajima korisnik sme da pristupa, a kojima ne.
- Funkcija Just In Time Authentication (JITA) omogućuje unapred definisanim korisnicima da potvrde svoj identitet kako bi pristupili uređajima kojima inače ne mogu da pristupe.
- Administratori i pouzdani korisnici mogu biti izuzeti od ograničenja pristupa uređajima koje nameće Device Access Manager tako što će biti dodati grupi administratora uređaja. Članstvom u ovoj grupi se upravlja pomoću opcije Napredne postavke.
- Pristup uređaju dozvoljava se ili zabranjuje na osnovu članstva u grupi ili pojedinačnim korisnicima.
- Za klase uređaja kao što su CD-ROM jedinice i DVD jedinice, pristup čitanju i pisanju može se dozvoliti ili zabraniti zasebno.

HP Device Access Manager automatski će biti konfigurisan sledećim postavkama nakon završetka čarobnjaka za podešavanje programa HP Client Security:

- Funkcija Just In Time Authentication (JITA) za prenosne medijume omogućena je i za administratore i za korisnike.
- Smernice za uređaje dozvoljavaju pun pristup ostalim uređajima.

Otvaranje alatke Device Access Manager

1. Na početnom ekranu, kliknite ili dodirnite stavku **HP Client Security** (Windows 8).

   – ili –

   Na Windows radnoj površini, dvaput kliknite ili dodirnite dvaput ikonu **HP Client Security** u polju za obaveštavanje, koje se nalazi u desnom uglu trake zadataka.

2. U odeljku **Device** (Uređaj), kliknite ili dodirnite stavku **Device Permissions** (Dozvole za uređaje).

   - Standardni korisnici mogu pogledati svoje trenutne postavke pristupa uređajima (pogledajte Prikaz za korisnike na stranici 44).
   - Administratori mogu pogledati i promeniti postavke pristupa uređajima koje su trenutno konfigurisane na računaru tako što će kliknuti ili dodirnuti opciju **Change** (Promeni), a zatim uneti lozinku administratora (pogledajte Sistemski prikaz na stranici 44).

Prikaz za korisnike

Kada se izabere stavka **Device Permissions** (Dozvole za uređaje), otvoriće se Prikaz za korisnike. U zavisnosti od smernica, standardni korisnici i administratori mogu pogledati svoje postavke pristupa klasama uređajima ili pojedinačnim uređajima na računaru.

- **Current user** (Trenutni korisnik)—Prikazuje se ime trenutno prijavljenog korisnika.
- **Device Class** (Klasa uređaja)—Prikazuju se tipovi uređaja.
- **Access** (Pristup)—Prikazuju se vaše trenutno podešene postavke pristupa različitim tipovima uređaja ili određenim uređajima.
- **Duration** (Trajanje)—Prikazuje se vremensko ograničenje vašeg pristupa CD/DVD-ROM disk jedinicama ili prenosnim diskovima.
- **Settings** (Postavke)—Administratori mogu promeniti za koje uređaje Device Access Manager upravlja pristupom.

Sistemski prikaz

U Sistemskom prikazu, administratori mogu da odobre ili zabrane pristup uređajima na ovom računaru grupi Korisnici ili grupi Administratori.

▲ Administratori mogu pristupiti Sistemskom prikazu tako što će kliknuti ili dodirnuti opciju **Change** (Promeni), uneti lozinku administratora, a zatim izabrati neku od sledećih opcija:

- **Device Access Manager**—Da biste uključili ili isključili HP Device Access Manager sa funkcijom Just In Time Authentication, kliknite ili dodirnite opcije **On** (Uključeno) ili **Off** (Isključeno).
- **Users and groups on this PC** (Korisnici i grupe na ovom računaru)—Prikazivanje grupe Korisnici ili grupe Administratori kojima je dozvoljen ili zabranjen pristup izabranim klasama uređaja.
- **Device Class** (Klasa uređaja)—Prikazivanje klasa uređaja i uređaja koji su instalirani na sistemu, ili su ranije bili instalirani na sistemu. Da biste proširili listu, kliknite na ikonu **+**. Prikazuju se svi uređaji koji su povezani na računar, a grupe Administratori i Korisnici biće proširene kako bi se prikazali njihovi članovi. Da biste osvežili listu uređaja, kliknite na ikonu okrugle strelice (osvežavanje).
  - Zaštita se obično primenjuje na celu klasu uređaja. Ako je pristup podešen na **Allow** (Dozvoli), izabrani korisnik ili grupa korisnika moći će da pristupi bilo kom uređaju iz te klase uređaja.
  - Zaštita se takođe može primeniti i na određene uređaje.
  - Podesite funkciju Just In Time authentication (JITA) da biste izabranim korisnicima omogućili da pristupaju CD/DVD-ROM disk jedinicama ili prenosnim diskovima tako što će potvrditi svoj identitet. Više informacija potražite u odeljku Konfigurisanje funkcije JITA na stranici 45.
  - Dozvolite ili zabranite pristup drugim klasama uređaja, kao što su prenosni medijumi (npr. USB fleš diskovi), serijski i paralelni portovi, Bluetooth® uređaji, modemi, PCMCIA/ExpressCard uređaji, 1394 uređaji, čitači otiska prsta i čitači pametnih kartica. Ako se zabrani pristup čitaču otiska prsta i čitaču pametnih kartica, oni će moći da se koriste kao akreditivi za potvrdu identiteta, ali neće moći da se koriste na nivou smernica sesije.

NAPOMENA: Ako se Bluetooth uređaji koriste kao akreditivi za potvrdu identiteta, pristup Bluetooth uređajima ne treba ograničiti smernicama alatke Device Access Manager.

- Kada izaberite postavku na nivou grupe ili klase uređaja, a od vas se traži da izaberete da li će se postavka primenjivati i na podređene objekte:

  Yes (Da)—Postavka će biti preneta.

  No (Ne)—Postavka neće biti preneta.

- Pristup nekim klasama uređaja, kao što su DVD i CD-ROM, može se detaljnije kontrolisati tako što se pristup dozvoljava ili zabranjuje zasebno za operacije upisivanja i operacije čitanja.

NAPOMENA: Grupa Administratori ne može se dodati na listu Korisnici.

- **Access** (Pristup)—Kliknite ili dodirnite strelicu nadole, a zatim izaberite neki od sledećih tipova pristupa da biste dozvolili ili zabranili pristup:
  - **Allow – Full Access** (Dozvoli – Pun pristup)
  - **Allow – Read Only** (Dozvoli – Samo čitanje)
  - **Allow – JITA Required** (Dozvoli – Zahteva se JITA)—Dodatne informacije potražite u odeljku Konfigurisanje funkcije JITA na stranici 45.

    Ako se izabere ovaj tip pristupa, u odeljku **Duration** (Trajanje), kliknite ili dodirnite strelicu nadole da biste izabrali vremensko ograničenje.
  - **Deny** (Zabrani)
- **Duration** (Trajanje)—Kliknite ili dodirnite strelicu nadole da biste izabrali vremensko ograničenje za pristupanje DVD/CD-ROM disk jedinicama ili prenosnim diskovima (pogledajte Konfigurisanje funkcije JITA na stranici 45).

Konfigurisanje funkcije JITA

Konfigurisanje funkcije JITA omogućava administratoru da prikaže i izmeni liste korisnika i grupa kojima je dozvoljeno da pristupaju uređajima pomoću funkcije Just In Time Authentication (JITA).

Korisnici koji mogu da koriste funkciju JITA moći će da pristupe nekim uređajima za koje postoje ograničenja u prikazu **Device Class Configuration** (Konfigurisanje klasa uređaja).

JITA period može se postaviti na određeni broj minuta ili na postavku Unlimited (Neograničeno). Korisnici sa postavkom Unlimited (Neograničeno) imaće pristup uređaju od trenutka potvrde identiteta do trenutka kada se odjave sa sistema.

Ako korisnik ima ograničena JITA period, minut pre isteka JITA perioda korisnik će biti upitan da li želite da produži pristup. Čim se korisnik odjavi sa sistema ili se drugi korisnik prijavi, JITA period će isteći. Kada se korisnik sledeći put prijavi i pokuša da pristupi uređaju za koji je aktivirana funkcija JITA, od njega će se tražiti da unese akreditive.

Funkcija JITA dostupna je za sledeće klase uređaja:

- DVD/CD-ROM disk jedinice
- Prenosne diskove

Kreiranje JITA smernica za korisnika ili grupu

Pomoću funkcije Just In Time Authentication (JITA), administratori mogu dozvoliti korisnicima ili grupama korisnika da pristupaju uređajima.

1. Pokrenite **Device Access Manager**, a zatim kliknite ili dodirnite opciju **Change** (Promeni).
2. Izaberite željenog korisnika ili grupu, a zatim okviru opcije **Access** (Pristup) za stavku **Removable Disk drives** (Prenosni diskovi) ili **DVD/CD-ROM drives** (DVD/CD-ROM disk jedinice) kliknite ili dodirnite strelicu nadole, pa izaberite opciju **Allow – JITA Required** (Dozvoli – Zahteva se JITA).
3. U odeljku **Duration** (Trajanje), kliknite ili dodirnite strelicu nadole da biste izabrali vremenski period za pristup pomoću funkcije JITA.

Da bi se primenile nove postavke funkcije JITA, potrebno je da se korisnik odjavi sa sistema i ponovo prijavi.

Onemogućavanje JITA smernica za korisnika ili grupu

Pomoću funkcije Just In Time Authentication (JITA), administratori mogu onemogućiti korisnicima ili grupama korisnika da pristupaju uređajima.

1. Pokrenite **Device Access Manager**, a zatim kliknite ili dodirnite opciju **Change** (Promeni).
2. Izaberite željenog korisnika ili grupu, a zatim okviru opcije **Access** (Pristup) za stavku **Removable Disk drives** (Prenosni diskovi) ili **DVD/CD-ROM drives** (DVD/CD-ROM disk jedinice) kliknite ili dodirnite strelicu nadole, pa izaberite opciju **Deny** (Zabrani).

Kada se korisnik prijavi i pokuša da pristupi uređaju, pristup će mu biti zabranjen.

Postavke

Na ekranu **Settings** (Postavke), administratori mogu videti i promeniti za koje uređaje Device Access Manager upravlja pristupom.

NAPOMENA: Alatka Device Access Manager mora biti omogućena prilikom konfigurisanja liste oznaka disk jedinica (pogledajte Sistemski prikaz na stranici 44).

Klase uređaja za koje nije dostupno upravljanje

HP Device Access Manager ne upravlja sledećim klasama uređaja:

- Ulazni/izlazni uređaji
  - CD-ROM
  - Disk jedinica
  - Kontroler diskete (FDC)
  - Kontroler čvrstog diska (HDC)
  - Klasa uređaja sa korisničkim interfejsom (HID)
  - Infracrveni uređaji sa korisničkim interfejsom
  - Miš
  - Serijski adapteri sa više portova
  - Tastatura

- Plug and Play štampači
- Štampač
- Nadogradnja štampača

- Napajanje
  - Podrška za upravljanje napajanjem sa više opcija (APM)
  - Baterija
- Razno
  - Računar
  - Dekoder
  - Ekran
  - Intel® objedinjeni upravljački program za prikaz
  - Legacard
  - Upravljački program medijuma
  - Uređaji za promenu medijuma
  - Tehnologija memorije
  - Monitor
  - Više funkcijski uređaji
  - Net klijent
  - Net usluga
  - Net trans
  - Procesor
  - SCSI adapter
  - Bezbednosni akceleratori
  - Bezbednosni uređaji
  - Sistem
  - Nepoznato
  - Volumen
  - Snimak volumena

8 HP Trust Circles

HP Trust Circles je aplikacija za bezbednost datoteka i dokumenata koja spaja šifrovanje fascikli i datoteka sa praktičnom funkcijom za deljenje dokumenata unutar kruga poverenja. Ona šifruje datoteke iz fascikli koje korisnik sam definiše i tako ih štiti unutar kruga poverenja. Zaštićene datoteke mogu da koriste i dele samo članovi kruga poverenja. Ako zaštićena datoteka dospe u vlasništvo osobe koja nije član kruga poverenja, datoteka će ostati šifrovana, a ta osoba neće moći da pristupi njenom sadržaju.

Otvaranje aplikacije Trust Circles

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

   – ili –

   Na Windows radnoj površini, dvaput kliknite na ikonu **HP Client Security** u polju za obaveštavanje, koje se nalazi u desnom uglu trake zadataka.

2. U odeljku **Data** (Podaci), kliknite ili dodirnite stavku **Trust Circles**.

Prvi koraci

Postoje dva načina za slanje pozivnica putem e-pošte i odgovaranje na njih:

- **Pomoću programa Microsoft® Outlook**—Ako aplikaciju Trust Circles koristite sa programom Microsoft Outlook, obrada Trust Circle pozivnica i odgovora od drugih Trust Circle korisnika obavlja se automatski.
- **Pomoću usluga Gmail, Yahoo, Outlook.com i drugih usluga e-pošte (SMTP)**—Nakon što unesete svoje ime, e-adresu i lozinku, aplikacija Trust Circles koristiće vašu uslugu e-pošte za slanje pozivnica putem e-pošte na adrese korisnika koje želite da pozovete u svoj krug poverenja.

Da biste podesili svoj osnovni profil:

1. Unesite svoje ime i e-adresu, a zatim kliknite ili dodirnite dugme **Next** (Dalje).

   Uneto ime moći će da vide svi članovi koje pozovete u svoj krug poverenja. Uneta e-adresa koristiće se za slanje i primanje pozivnica i odgovaranje na njih.

2. Unesite lozinku za nalog e-pošte, a zatim kliknite ili dodirnite dugme **Next** (Dalje).

   Biće poslata probna e-poruka kako bi se proverilo da li su postavke e-pošte tačne.

   NAPOMENA: Računar mora biti povezan na mrežu.

3. U polje **Trust Circle Name** (Ime kruga poverenja) unesite ime kruga poverenja, a zatim kliknite ili dodirnite dugme **Next** (Dalje).

4. Dodajte željene članove i fascikle, pa kliknite ili dodirnite dugme **Next** (Dalje). Biće kreiran krug poverenja koji sadrži sve fascikle koje ste izabrali, a zatim će putem e-pošte biti poslate pozivnice članovima po vašem izboru. Ako iz bilo kog razloga nije moguće poslati pozivnice, prikazaće se obaveštenje. Sa ekrana Trust Circle (Krug poverenja) u bilo kom trenutku možete ponovo pozvati članove tako što ćete kliknuti na stavku **Your Trust Circles** (Vaši krugovi

poverenja), a zatim dvaput kliknuti ili dodirnuti dvaput željeni krug poverenja. Više informacija potražite u odeljku Trust Circles na stranici 49.

Trust Circles

Krug poverenja možete kreirati u toku početnog podešavanja, nakon unosa e-adrese, ili to možete učiniti na ekranu Trust Circle (Krug poverenja):

▲ Na ekranu Trust Circle (Krug poverenja), kliknite ili dodirnite opciju **Create Trust Circle** (Kreiraj krug poverenja), a zatim unesite ime za krug poverenja.

- Da biste dodali članove u krug poverenja, kliknite ili dodirnite ikonu **M+** pored stavke **Members** (Članovi), a zatim pratite uputstva na ekranu.
- Da biste dodali fascikle u krug poverenja, kliknite ili dodirnite ikonu **+** pored stavke **Folders** (Fascikle), a zatim pratite uputstva na ekranu.

Dodavanje fascikli u krug poverenja

Dodavanje fascikli u novi krug poverenja:

- Prilikom kreiranja kruga poverenja, možete dodati fascikle tako što ćete kliknuti ili dodirnuti ikonu **+** pored stavke **Folders** (Fascikle), a zatim pratiti uputstva na ekranu.

  – ili –

- U programu Windows Explorer, kliknite desnim tasterom miša ili dodirnite i držite fasciklu koja trenutno nije deo kruga poverenja, izaberite stavku **Trust Circle** (Krug poverenja), a zatim izaberite opciju **Create Trust Circle from Folder** (Kreiraj krug poverenja od fascikle).

SAVET: Možete izabrati jednu ili više fascikli.

Dodavanje fascikli u postojeći krug poverenja:

- Na ekranu Trust Circle (Krug poverenja), kliknite na stavku **Your Trust Circles** (Vaši krugovi poverenja), dvaput kliknite ili dodirnite dvaput postojeći krug poverenja da biste videli trenutne fascikle, kliknite ili dodirnite ikonu **+** pored stavke **Folders** (Fascikle), a zatim pratite uputstva na ekranu.

  – ili –

- U programu Windows Explorer, kliknite desnim tasterom miša ili dodirnite i držite fasciklu koja trenutno nije deo kruga poverenja, izaberite stavku **Trust Circle** (Krug poverenja), a zatim izaberite opciju **Add to existing Trust Circle from Folder** (Dodaj fasciklu u postojeći krug poverenja).

SAVET: Možete izabrati jednu ili više fascikli.

Nakon što dodate fasciklu u krug poverenja, aplikacija Trust Circles automatski će šifrovati fasciklu i njen sadržaj. Nakon šifrovanja svih datoteka, prikazaće se obaveštenje. Osim toga, zeleni simbol katanca biće prikazan na ikonama svih šifrovanih fascikli i datoteka unutar fascikli, što označava da su u potpunosti zaštićene.

Dodavanje članova u krug poverenja

Dodavanje članova u krug poverenja obavlja se u tri koraka:

1. **Pozivanje**—Kao prvo, vlasnik kruga poverenja šalje pozivnice članovima. Pozivnica se putem e-poruke šalje većem broju korisnika ili listama za distribuciju/grupama.
2. **Prihvatanje**—Pozvana osoba dobija pozivnicu i odlučuje da li će je prihvatiti ili ne. Ako pozvana osoba prihvati poziv, pozivalac prima odgovor e-poštom. Ako je pozivnica poslata grupi, svaki član će dobiti pozivnicu i odlučiti da li će je prihvatiti ili ne.
3. **Upisivanje**—Pozivalac ima finalno pravo odluke da li će dodati člana u krug poverenja. Ako pozivalac odluči da upiše člana, pozvana osoba dobiće e-poruku koja ga obaveštava o toj odluci. Pozivalac i pozvana osoba mogu, po želji, proveriti bezbednost procesa pozivanja. Pozvanoj osobi prikazuje se kôd za potvrdu koji on zatim mora preko telefona pročitati pozivaocu. Nakon potvrđivanja koda, pozivalac može da pošalje finalnu e-poruku o upisu.

Dodavanje članova u novi krug poverenja:

▲ Prilikom kreiranja kruga poverenja, možete dodati članove tako što ćete kliknuti ili dodirnuti ikonu **M+** pored stavke **Members** (Članovi), a zatim pratiti uputstva na ekranu.

- Ako koristite Outlook, izaberite željene adrese iz Outlook imenika, a zatim kliknite na **OK** (U redu)
- Ako koristite drugu uslugu e-pošte, dodajte nove e-adrese ručno u aplikaciju Trust Circle, ili ih možete preuzeti pomoću e-adrese registrovane u aplikaciji Trust Circle.

Dodavanje članova u postojeći krug poverenja:

▲ Na ekranu Trust Circle (Krug poverenja), kliknite na stavku **Your Trust Circles** (Vaši krugovi poverenja), dvaput kliknite ili dodirnite dvaput postojeći krug poverenja da biste videli trenutne članove, kliknite ili dodirnite ikonu **M+** pored stavke **Members** (Članovi), a zatim pratite uputstva na ekranu.

- Ako koristite Outlook, izaberite kontakte iz Outlook imenika, a zatim kliknite na **OK** (U redu).
- Ako koristite neku drugu uslugu e-pošte, dodajte nove e-adrese ručno u aplikaciju Trust Circle, ili ih možete preuzeti pomoću e-adrese registrovane u aplikaciji Trust Circle.

Dodavanje datoteka u krug poverenja

Možete dodati datoteke u krug poverenja na neki od sledećih načina:

- Kopirajte ili premestite datoteku u postojeću fasciklu unutar kruga poverenja.

  – ili –

- U programu Windows Explorer, kliknite desnim tasterom miša ili dodirnite i držite datoteku koja trenutno nije šifrovana, izaberite stavku **Trust Circle** (Krug poverenja), a zatim izaberite opciju **Encrypt** (Šifruj). Od vas će se tražiti da izaberete krug poverenja u koji će ta datoteka biti dodata.

SAVET: Možete izabrati jednu ili više datoteka.

Šifrovane fascikle

Svaki član kruga poverenja može da prikazuje i uređuje datoteke koje pripadaju tom krugu poverenja.

NAPOMENA: Aplikacija Trust Circle Manager/Reader ne sinhronizuje datoteke između članova.

Deljenje datoteka obavlja se na neki od već postojećih načina, kao što su e-pošta, ftp ili usluge za skladištenje u „oblaku“. Datoteke koje se kopiraju ili premeste u fasciklu iz kruga poverenja, kao i one koje se kreiraju unutar nje, biće istog trenutka zaštićene.

Uklanjanje fascikli iz kruga poverenja

Uklanjanjem fascikle iz kruga poverenja fascikla i sav njen sadržaj se dešifruje, a zaštita uklanja.

- Na ekranu Trust Circle (Krug poverenja), kliknite na stavku **Your Trust Circles** (Vaši krugovi poverenja), dvaput kliknite ili dodirnite dvaput postojeći krug poverenja da biste videli trenutne fascikle, kliknite ili dodirnite ikonu **korpe za otpatke** pored te fascikle.

  – ili –

- U programu Windows Explorer, kliknite desnim tasterom miša ili dodirnite i držite fasciklu koja je trenutno deo kruga poverenja, izaberite stavku **Trust Circle** (Krug poverenja), a zatim izaberite opciju **Remove from trust circle** (Ukloni iz kruga poverenja).

SAVET: Možete izabrati jednu ili više fascikli.

Uklanjanje datoteke iz kruga poverenja

Da biste uklonili određenu datoteku iz kruga poverenja, u programu Windows Explorer kliknite desnim tasterom miša ili dodirnite i držite datoteku koja trenutno nije šifrovana, izaberite stavku **Trust Circle** (Krug poverenja), a zatim izaberite opciju **Decrypt File** (Dešifruj datoteku).

Uklanjanje članova iz kruga poverenja

Član koji je upisan u potpunosti ne može se ukloniti iz kruga poverenja. Alternativa bi bila kreiranje novog kruga poverenja koji bi sadržao sve ostale članove, premeštanje svih datoteka i fascikli u novi krug poverenja, a zatim brisanje starog kruga poverenja. Time se postiže da taj član ne može da pristupi novim datotekama koje dobije, ali sve što je prethodno podeljeno ostaće dostupno članu starog kruga poverenja.

Ako član nije upisan u potpunosti (član je pozvan da se pridruži krugu poverenja ili nije prihvatio pozivnicu za krug poverenja), moći ćete da ga uklonite iz kruga poverenja na neki od sledećih načina:

- Na ekranu Trust Circle (Krug poverenja), kliknite ili dodirnite opciju **Your Trust Circles** (Vaši krugovi poverenja), a zatim dvaput kliknite ili dodirnite dvaput željeni krug poverenja da biste videli trenutnu listu članova. Kliknite ili dodirnite ikonu **korpe za otpatke** pored imena člana kojeg želite da uklonite.
- Na ekranu Trust Circle (Krug poverenja), kliknite ili dodirnite stavku **Members** (Članovi), a zatim dvaput kliknite ili dodirnite dvaput željenog člana da biste videli u kojim se krugovima poverenja nalazi. Kliknite ili dodirnite ikonu **korpe za otpatke** pored kruga poverenja iz kojeg želite da uklonite člana.

Brisanje kruga poverenja

Da biste izbrisali krug poverenja, potrebno je da budete njegov vlasnik.

▲ Na ekranu Trust Circle (Krug poverenja), kliknite ili dodirnite opciju **Your Trust Circles** (Vaši krugovi poverenja), a zatim kliknite ili dodirnite ikonu **kante za otpatke** pored kruga poverenja koji želite da izbrišete.

Krug poverenja biće uklonjen sa stranice, a svim njegovim članovima biće poslato obaveštenje o tome da je krug poverenja izbrisan. Sve datoteke i fascikle iz tog kruga poverenja biće dešifrovane.

Podešavanje željenih opcija

Na ekranu Trust Circle (Krug poverenja), kliknite ili dodirnite stavku **Preferences** (Željene opcije). Biće prikazane tri kartice:

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

Opcija	Opis
Username (Korisničko ime)	Prikazuje se korisničko ime koje se trenutno koristi. Da biste ga promenili, unesite novo korisničko ime u okvir za tekst. Promene će automatski biti sačuvane.
Email Address (E-adresa)	Prikazuje se nalog e-pošte koji se trenutno koristi. Da biste ga promenili, kliknite ili dodirnite opciju **Change Email Settings** (Promeni postavke e-pošte), a zatim pratite uputstva na ekranu.
New Member Confirmation (Potvrda novog člana)	Izaberite neku od sledećih opcija: ◦ **Confirm Automatically** (Automatski potvrdi)—Nakon prijema potvrdnog odgovora od pozvane osobe, osoba se automatski potvrđuje kao novi član kruga poverenja bez bilo kakvog ručnog unosa, a pozvanoj osobi šalje se potvrdna e-poruka. ◦ **Confirm Manually** (Ručno potvrdi)—Nakon prijema potvrdnog odgovora od pozvane osobe, osoba se upisuje kao novi član kruga poverenja tek nakon ručnog unosa, a pozvanoj osobi šalje se potvrdna e-poruka. ◦ **Require Verification** (Zahtevaj verifikaciju)—Nakon prijema potvrdnog odgovora od pozvane osobe, potreban je unos koda za verifikaciju da bi pozvana osoba bila u potpunosti upisana kao član. Vlasnik kruga poverenja mora stupiti u kontakt sa pozvanom osobom i dobiti kôd za verifikaciju od nje. Nakon unosa tačnog koda, šalju se potvrdne e-poruke.
Periodic Authentication (Periodična provera identiteta)	Periodična provera identiteta zahteva da korisnik unese Windows lozinku nakon izvesnog vremenskog perioda (izraženo u minutima), kao i prilikom obavljanja poverljivih operacija. Ova postavka omogućava uključivanje ili isključivanje provere identiteta.
Authentication Timeout (Vremensko ograničenje za proveru identiteta)	Izaberite navedeno vremensko ograničenje (izraženo u minutima) nakon čijeg isteka je potrebno obaviti proveru identiteta.
Don't show confirmation message (Ne prikazuj potvrdnu poruku)	Izaberite ovo polje za potvrdu da onemogućite prikazivanje potvrdnih poruka ili poništite izbor polja za potvrdu da bi se potvrdne poruke prikazivale.
I'd like to help improve the HP Trust Circle through anonymous usage tracking (Želim da pomognem u poboljšanju aplikacije HP Trust Circle pomoću anonimnog praćenja upotrebe)	Izaberite ovo polje za potvrdu da biste učestvovali u ovom programu ili poništite izbor polja za potvrdu ako ne želite da učestvujete.

- **Backup/Restore** (Rezervna kopija/vraćanje)

Opcija	Opis
Rezervna kopija	Kopiranje podataka iz aplikacije Trust Circle Manager/Reader (postavke i krugovi poverenja) u rezervnu datoteku. U slučaju pada sistema ili kvara računara, moći ćete da upotrebite ovu datoteku za vraćanje instalacije aplikacije Trust Circles u stanje koje je sačuvano u datoteci. **NAPOMENA:** Čuvaju se samo podaci iz aplikacije Trust Circles (krugovi poverenja, postavke i članovi). Za same datoteke iz fascikli u krugovima poverenja neće biti napravljena rezervna kopija. Njihovu kopiju morate posebno napraviti. Da biste napravili rezervnu kopiju postavki i korisničkih podataka iz aplikacije Trust Circles: **1.** Kliknite ili dodirnite dugme **Backup** (Napravi rezervnu kopiju). **2.** Izaberite ime i direktorijum za rezervnu datoteku, a zatim kliknite ili dodirnite opciju **Save** (Sačuvaj). **3.** Unesite lozinku po želji, potvrdite je, a zatim kliknite ili dodirnite dugme **OK** (U redu). Za vraćanje datoteke biće potrebno uneti tu lozinku.
Vraćanje u prvobitno stanje	Vraćanje postavki i krugova poverenja iz rezervne datoteke, obično nakon pada sistema ili migracije na drugi računar. Da biste vratili postavke i korisničke podatke iz aplikacije Trust Circle Manager: **1.** Kliknite ili dodirnite opciju **Restore** (Vrati). **2.** Izaberite ime i direktorijum za rezervnu datoteku, a zatim kliknite ili dodirnite opciju **Open** (Otvori). **3.** Unesite lozinku koju ste podesili prilikom pravljenja rezervne kopije.

- **About** (Osnovne informacije)—Prikazuje se verzija softvera Trust Circle Manager/Reader. Na ovoj stranici prikazuju se i veze za nadogradnju aplikacije Trust Circle Manager na verziju Pro, kao i za prikazivanje smernica privatnosti kompanije HP.

9 Vraćanje u slučaju krađe (samo na odabranim modelima)

Computrace (kupuje se odvojeno) omogućuje vam da daljinski pratite, upravljate i locirate svoj računar.

Kada se aktivira, Computrace se konfiguriše iz Absolute Software korisničkog centra. Iz korisničkog centra administrator može da konfiguriše Computrace tako da prati ili upravlja računarom. Ako se sistem zaturi ili ukrade, korisnički centar može da pomogne lokalnim vlastima da lociraju i vrate računar. Ako je konfigurisan, Computrace može da nastavi da funkcioniše čak i ako se čvrsti disk obriše ili zameni.

Da biste aktivirali Computrace:

1. Povežite se na internet.
2. Otvorite HP Client Security. Više informacija potražite u odeljku Otvaranje programa HP Client Security na stranici 9.
3. Kliknite na **Theft Recovery** (Vraćanje u slučaju krađe).
4. Da biste pokrenuli čarobnjaka za aktiviranje programa Computrace, kliknite na **Get Started** (Prvi koraci).
5. Unesite svoje podatke za kontakt i informacije o kreditnoj kartici za plaćanje, ili unesite unapred kupljenu šifru proizvoda.

Čarobnjak za aktiviranje bezbedno obrađuje transakciju i podešava vaš korisnički nalog na veb-sajtu Absolute Software Customer Center. Kada završite, dobijate potvrdu e-poštom koja sadrži informacije o vašem nalogu u korisničkom centru.

Ako ste ranije pokretali čarobnjaka za aktiviranje programa Computrace i vaš nalog u korisničkom centru već postoji, možete da se obratite svom predstavniku za HP nalog i kupite dodatne licence.

Da biste se prijavili na korisnički centar:

1. Idite na lokaciju https://cc.absolute.com/.
2. U poljima **Login ID** (ID za prijavu) i **Password** (Lozinka) unesite akreditive koje ste dobili u e-poruci sa potvrdom i zatim kliknite na **Log in** (Prijavljivanje).

Preko korisničkog centra možete da:

- Pratite svoje računare.
- Zaštitite svoje udaljene podatke.
- Prijavite krađu bilo kog računara koga štiti Computrace.

▲ Kliknite na **Learn More** (Saznajte više) za više informacija o Computrace-u.

10 Izuzeci za lokalizovane lozinke

Na nivou provere identiteta pri pokretanju sistema i nivou alatke HP Drive Encryption dostupna je ograničena podrška za lokalizovane lozinke. Više informacija potražite u odeljku Nepodržani Windows IME režimi na nivou provere identiteta pri pokretanju sistema i nivou alatke Drive Encryption na stranici 55.

Šta preduzeti ako lozinka bude odbijena

Lozinka može biti odbijena iz sledećih razloga:

- Korisnik koristi IME koji nije podržan. Ovo je čest problem kod jezika sa dvobajtnim znakovima (korejski, japanski, kineski). Da biste rešili ovaj problem:

  1. Pomoću menija **Kontrolna tabla**, dodajte neki od podržanih rasporeda tastera (dodajte tastaturu SAD/engleski u okviru kineskog kao jezika za unos).
  2. Podesite podržan raspored tastera kao podrazumevani raspored za unos.
  3. Pokrenite program HP Client Security, pa unesite Windows lozinku.

- Korisnik koristi znak koji nije podržan. Da biste rešili ovaj problem:

  1. Promenite Windows lozinku tako da sadrži samo podržane znakove. Dodatne informacije o nepodržanim znakovima potražite u odeljku Korišćenje specijalnih tastera na stranici 56.
  2. Pokrenite program HP Client Security, pa unesite Windows lozinku.

Nepodržani Windows IME režimi na nivou provere identiteta pri pokretanju sistema i nivou alatke Drive Encryption

U operativnom sistemu Windows, korisnik može da izabere IME (Input Method Editor, Uređivač metoda unosa) za unos složenih znakova i simbola, kao što su japanski ili kineski znakovi, preko standardne zapadnjačke tastature.

IME režimi nisu podržani na nivou provere identiteta pri pokretanju sistema i nivou alatke Drive Encryption. Windows lozinka ne može se uneti pomoću IME režima na ekranu za proveru identiteta pri pokretanju sistema i ekranu za prijavljivanje u okviru alatke HP Drive Encryption, a ako pokušate da to učinite, može doći do zaključavanja naloga. U nekim slučajevima Microsoft® Windows ne prikazuje IME kada korisnik unosi lozinku.

Rešenje je prelazak na neki od sledećih podržanih rasporeda tastera koji odgovara rasporedu tastera 00000411:

- Microsoft IME za japanski
- Raspored tastera za japanski
- Office 2007 IME za japanski—Ako Microsoft ili treća strana koristi termin IME ili Input Method Editor (Uređivač metoda unosa), ne mora značiti da je metod unosa zaista IME. To može dovesti do zabune, ali softver će moći da pročita oblik heksadecimalnog koda. Dakle, ako je IME mapiran podržanim rasporedom tastera, HP Client Security će moći da podrži konfiguraciju.

UPOZORENJE! Kada je program HP Client Security aktiviran, lozinke koje su unesu u nekom od Windows IME režima biće odbijene.

Promena lozinke pomoću drugog podržanog rasporeda tastera

Ako se lozinka prvobitno unese pomoću jednog rasporeda tastera, kao što je SAD engleski (409), a nakon toga korisnik promeni lozinku koristeći drugi raspored tastera koji je takođe podržan, kao što je latinoamerički (080A), promena lozinke će funkcionisati u okviru alatke HP Drive Encryption, ali ne i u BIOS-u ako korisnik upotrebi znakove koji postoje u novom rasporedu tastera, ali ne i u starom (na prime, ē).

NAPOMENA: Administratori mogu rešiti ovaj problem tako što će otvoriti stranicu Users (Korisnici) u okviru programa HP Client Security (kliknite na ikonu **zupčanika** na matičnoj stranici) kako bi uklonili korisnika iz programa HP Client Security, izabrali željeni raspored tastera u operativnom sistemu, a zatim ponovo pokrenuli Čarobnjak za podešavanje programa HP Client Security za tog korisnika. BIOS će sačuvati željeni raspored tastera, što znači da će i lozinke unete pomoću tog rasporeda tastera biti pravilno podešene u BIOS-u.

Drugi mogući problem je korišćenje različitih rasporeda tastera koji prikazuju iste znakove. Na primer, i SAD međunarodni (20409) i latinoamerički (080A) raspored tastera mogu da prikažu znak é, ali je za njegov unos potrebno pritisnuti različit niz tastera. Ako se lozinka prvobitno podesi u latinoameričkom rasporedu tastera, u BIOS-u će biti podešen latinoamerički raspored tastera, čak i ako se lozinka kasnije promeni u SAD međunarodnom rasporedu tastera.

Korišćenje specijalnih tastera

- Kineski, slovački, kanadski francuski i češki

  Kada korisnik izabere jedan od postojećih rasporeda tastera na tastaturi i zatim unese lozinku (na primer, abcdef), ista lozinka se mora uneti dok je pritisnut taster shift za mala slova i taster shift i caps lock za velika slova tokom autorizacije za vreme podizanja sistema i za alatku HP Drive Encryption. Numeričke tastature moraju se unositi pomoću numeričke tastature.

- Korejski

  Kada korisnik izabere podržani korejski raspored tastera na tastaturi i zatim unese lozinku, ista lozinka se mora uneti dok je pritisnut desni taster alt za mala slova i desni taster alt i caps lock za velika slova tokom autorizacije za vreme podizanja sistema i za alatku HP Drive Encryption.

- Nepodržani znakovi navedeni su u sledećoj tabeli:

Jezik	Windows	BIOS	Drive Encryption
Arapski	Tasteri ﻯ ,ﻰ i ﻯ generišu dva znaka.	Tasteri ﻯ ,ﻰ i ﻯ generišu jedan znak.	Tasteri ﻯ ,ﻰ i ﻯ generišu jedan znak.
Kanadski francuski	ç, è, à i é sa caps lock su Ç, È, À, and É u Windows-u.	ç, è, à i é sa caps lock su ç, è, à i é kod autorizacije za vreme podizanja sistema.	ç, è, à i é sa caps lock su ç, è, à i é u HP Drive Encryption.

Jezik	Windows	BIOS	Drive Encryption
Španski	Raspored 40a nije podržan. Međutim, on funkcioniše bez obzira na to pošto ga softver konvertuje u c0a. Ipak, zbog malih razlika između ova dva rasporeda tastera, preporučuje se da korisnici sa španskog govornog područja promene raspored tastera u operativnom sistemu Windows u 1040a (španska varijanta) ili 080a (latinoamerička varijanta).	nije dostupno	nije dostupno
SAD međunarodni	◦ Tasteri ¡, ¤, ‘, ’, ¥ i × u gornjem redu nisu podržani. ◦ Tasteri å, ® i Þ u drugom redu nisu podržani. ◦ Tasteri á, ð i ø u trećem redu nisu podržani. ◦ Taster æ u donjem redu nije podržan.	nije dostupno	nije dostupno
Czech	◦ Taster ğ nije podržan. ◦ Taster į nije podržan. ◦ Taster ų nije podržan. ◦ Tasteri ė, ı i ż nisu podržani. ◦ Tasteri ģ, ķ, ļ, ņ i ţ nisu podržani.	nije dostupno	nije dostupno
Slovački	Taster ż nije podržan.	◦ Tasteri š, ś i ş nisu podržani ako se unose na tastaturi, ali su podržani ako se unose softverskom tastaturom. ◦ Neaktivni taster ţ generiše dva znaka.	nije dostupno
Hungarian	Taster ż nije podržan.	Taster ţ generiše dva znaka.	nije dostupno
Slovenian	Taster żŻ nije podržan u operativnom sistemu Windows, a taster alt generiše neaktivan taster u BIOS-u.	Tasteri ú, Ú, ů, Ů, ş, Ş, ś, Ś, š i Š nisu podržani u BIOS-u.	nije dostupno
Japanski	Ako je dostupan, režim Microsoft Office 2007 IME predstavlja bolji izbor. Iako njegov naziv sadrži reč „IME“, reč je o rasporedu tastera 411 koji je podržan.	nije dostupno	nije dostupno

Rečnik

Windows administrator
Korisnik sa punim pravima za menjanje dozvola i upravljanje drugim korisnicima.

Windows korisnički nalog
Korisnik koji je ovlašćen za prijavljivanje na mrežu ili pojedinačni računar.

administrator
Pogledajte *Windows administrator*.

akreditiv
Specifičan skup informacija ili hardverski uređaj koji se koristi za potvrdu identiteta pojedinačnih korisnika.

aktiviranje
Zadatak koji se morate obaviti da biste mogli da pristupite funkcijama alatke Drive Encryption. Administratori mogu aktivirati alatku Drive Encryption pomoću čarobnjaka za podešavanje programa HP Client Security ili iz samog programa HP Client Security. Proces aktiviranja sastoji se od aktiviranja softvera, šifrovanja disk jedinice i kreiranja početne rezervne kopije ključa za šifrovanje na prenosnom uređaju za skladištenje.

arhiva za oporavak u hitnim slučajevima
Zaštićeno skladište koje omogućuje ponovno šifrovanje osnovnih korisničkih ključeva sa jedne platforme vlasničkog ključa na drugu.

automatsko sigurno brisanje
Sigurno brisanje koje je zakazano u okviru alatke File Sanitizer.

beskontaktna kartica
Plastična kartica koja sadrži računarski čip i može se koristiti za potvrdu identiteta.

Bezbednost prijave u Windows
Štiti vaš Windows nalog(e) tako što zahteva korišćenje specifičnih akreditiva za pristup.

Bluetooth
Tehnologija koja koristi radio talase za bežičnu komunikaciju računara, štampača, miševa, mobilnih telefona i drugih uređaja na maloj razdaljini.

dešifrovanje
Procedura koja se koristi u kriptografiji da se šifrovani podaci konvertuju u čisti tekst.

domen
Grupa računara koja pripada mreži i deli zajednički direktorijum sa bazom podataka. Domeni imaju jedinstvene nazive i svaki ima skup zajedničkih pravila i procedura.

Drive Encryption
Štiti vaše podatke tako što šifruje čvrsti disk/diskove i informacije čini nečitljivim za one koji nemaju odgovarajuću autorizaciju.

DriveLock
Bezbednosna funkcija koja povezuje čvrsti disk sa korisnikom i zahteva da korisnik pravilno upiše DriveLock lozinku kada se računar pokreće.

ekran za prijavljivanje alatke Drive Encryption
Pogledajte Provera identiteta pre pokretanja sistema alatke Drive Encryption.

Encryption File System (EFS)
Sistem koji šifruje sve datoteke i poddirektorijume u okviru odabranog direktorijuma.

Funkcija „Just In Time Authentication“
Pogledajte pomoć za softver HP Device Access Manager.

grupa
Grupa korisnika koja ima isti nivo pristupa ili zabrane pristupa određenoj klasi uređaja ili konkretnom uređaju.

hardversko šifrovanje
Korišćenje disk jedinica sa sopstvenim šifrovanjem koje ispunjavaju OPAL specifikaciju organizacije Trusted Computing Group za upravljanje disk jedinicama sa sopstvenim šifrovanjem za trenutno obavljanje šifrovanja. Hardversko šifrovanje obavlja se trenutno i može potrajati samo nekoliko minuta, dok softversko šifrovanje može potrajati nekoliko sati.

ID kartica
Gadžet na Windows radnoj površini koji služi da vizuelnu identifikaciju vaše radne površine pomoću korisničkog imena i izabrane slike.

identitet
Kod HP Client Security, grupa akreditiva i postavki koja se tretira kao nalog ili profil određenog korisnika.

klasa uređaja
Svi uređaji određenog tipa, npr. disk jedinice.

korisnik
Osoba koja je prijavljena za korišćenje alatke Drive Encryption. Korisnici koji nisu administratori imaju ograničena prava u okviru alatke Drive Encryption. Oni mogu samo da se prijave za korišćenje alatke (sa odobrenjem administratora) i da se prijave na sistem.

Matična stranica
Centralno mesto za pristupanje i upravljanje funkcijama i postavkama programa HP Client Security.

metod bezbedne prijave
Metod koji se koristi za prijavljivanje na računar.

mrežni nalog
Korisnički ili administratorski nalog u Windows-u, bilo na lokalnom računaru ili u radnoj grupi, ili na domenu.

obnavljanje
Proces koji kopira informacije o programu iz prethodno sačuvane rezervne kopije u ovaj program.

oporavak pomoću funkcije HP SpareKey
Mogućnost da pristupite svom računaru tako što ćete tačno odgovoriti na bezbednosna pitanja.

otisak prsta
Izdvojene digitalne informacije sa slike vašeg otiska prsta. HP Client Security ne čuva samu sliku vašeg otiska prsta.

pametna kartica
Hardverski uređaj koji se u kombinaciji sa PIN kodom može koristiti za proveru identiteta.

PIN
Lični identifikacioni broj koji upisani korisnici mogu koristiti za proveru identiteta.

PKI
Standard Public Key Infrastructure (Infrastruktura sistema javnih ključeva) koja definiše interfejse za kreiranje, korišćenje i administraciju sertifikata i kriptografskih ključeva.

podaci za prijavljivanje
Objekat unutar programa HP Client Security koji se sastoji od korisničkog imena i lozinke (i, eventualno, drugih informacija) koji se koristi za prijavljivanje na veb-sajtove ili druge programe.

ponovno pokretanje sistema
Proces ponovo pokreće računar.

potvrda identiteta
Proces pomoću kojeg potvrđujete da ste osoba za koju ste predstavljate tako što koristite akreditive, u koje spada vaša Windows lozinka, otisak prsta, pametna kartica, beskontaktna kartica ili proximity kartica.

povezani uređaj
Hardverski uređaj koji je povezan na neki od priključaka na računaru.

proximity kartica
Plastična kartica koja sadrži računarski čip i može se koristiti za potvrdu identiteta u kombinaciji sa ostalim akreditivima radi dodatne bezbednosti.

provera identiteta pre pokretanja sistema alatke Drive Encryption
Ekran za prijavljivanje koji se prikazuje pre pokretanja operativnog sistema Windows. Korisnici moraju uneti svoje korisničko ime i lozinku za Windows ili PIN pametne kartice, ili prevući registrovanim prstom preko senzora. Ako je izabrana opcija One-Step Logon (Prijavljivanje u jednom koraku), nakon unosa tačnih informacija na ekranu za prijavljivanje alatke Drive Encryption moći ćete direktno da pristupite operativnom sistemu Windows bez potrebe da se ponovo prijavljujete na ekranu za prijavljivanje operativnog sistema Windows.

provera identiteta pri pokretanju sistema
Bezbednosna funkcija koja zahteva neki oblik potvrde identiteta, na primer pametna kartica, bezbednosni čip ili lozinka, kada se računar uključuje.

rezervna kopija
Pomoću funkcije za pravljenje rezervne kopije možete sačuvati kopiju važnih informacija iz programa na lokaciji van programa. Dobijenu datoteku kasnije možete koristiti za vraćanje informacija u prethodno stanje na istom ili drugom računaru.

ručno sigurno brisanje
Trenutno sigurno brisanje jedne stavke ili izabranih stavki koje se obavlja mimo zakazanog sigurnog brisanja.

sigurno obriši
Izvršavanje algoritma koji zamenjuje podatke iz određene stavke besmislenim podacima.

Single Sign On
Funkcija koja skladišti podatke za potvrdu identiteta i omogućuje vam da koristite HP Client Security da pristupate internet i Windows aplikacijama koje zahtevaju potvrdu identiteta putem lozinke.

skrivanje slobodnog prostora
Upisivanje nasumičnih podataka preko izbrisanih stavki i neiskorišćenog prostora. Ovim procesom smanjuje se prisustvo izbrisane stavke pa je originalnu stavku teže vratiti.

smernice za kontrolu pristupa uređaju
Lista uređaja kojima je korisniku dozvoljeno ili zabranjeno da pristupa.

softversko šifrovanje
Korišćenje softvera za šifrovanje čvrstog diska sektor po sektor. Ovaj proces je sporiji od hardverskog šifrovanja

sredstvo
Komponenta koja sadrži lične informacije ili datoteke, podatke iz istorije ili sa veba i slično, a nalazi se na čvrstom disku.

šifrovanje
Postupak, kao što je korišćenje algoritma, koji se koristi u kriptografiji za konvertovanje čistog teksta u šifrovan tekst kako bi se sprečilo da neovlašćeni primaoci čitaju podatke. Postoji mnogo vrsta šifrovanja podataka koje predstavljaju osnovu za bezbednost mreže. U najčešće tipove spadaju Standard za šifrovanje podataka i šifrovanje javnim ključem.

Trust Circle

Sprečava širenje podataka tako što ih vezuje za podešenu grupu pouzdanih korisnika. Time se sprečava da podaci dođu u pogrešne ruke, bilo slučajno ili namerno. Podaci se obezbeđuju tehnologijom Zero Overhead Key Management kompanije CryptoMill i kriptografski vezuju za krug pouzdanih korisnika. Time se sprečava dešifrovanje dokumenata ili drugih poverljivih informacija izvan kruga poverenja

Trust Circle fascikla
Bilo koja fascikla koju štiti krug poverenja.

Trust Circle Manager/Reader
Trust Circle Reader prihvata samo pozivnice koje šalju korisnici aplikacije Trust Circle Manager. Međutim, Trust Circle Manager omogućava kreiranje krugova poverenja. U dostupne funkcije spada pozivanje osoba u krug poverenja e-poštom, kao i prihvatanje pozivnica za krug poverenja od drugih pošiljalaca. Nakon što se krug poverenja uspostavi među članovima, datoteke koje su zaštićene krugom poverenja moći će bezbedno da se dele.

Trusted Platform Module (TPM) ugrađeni bezbednosni čip
TPM autorizuje računar, a ne korisnika, tako što skladišti informacije specifične za matični sistem, kao što su ključevi za šifrovanje, digitalni sertifikati i lozinke. TPM svodi na minimum rizik da će informacije na računaru biti ugrožene fizičkom krađom ili napadom od strane spoljašnjeg hakera.

Indeks