HP ProtectTools
Korisnički priručnik

Prvo izdanje: studeni 2009.

Šifra dokumenta: 593308-BC1

Sadržaj

1 Uvod u sigurnost

Softver HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) donosi sigurnosne značajke koje pomažu u zaštiti od neovlaštenog pristupa računalu, mrežama i važnim podacima. Administracija u softveru HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) omogućena je kroz značajku konzole za administraciju.

Pomoću konzole za administraciju sustava HP ProtectTools lokalni administrator može obavljati sljedeće zadatke:

- omogućiti ili onemogućiti sigurnosne značajke
- unijeti otiske prstiju svih korisnika računala
- unijeti jednu ili više slika za provjeru autentičnosti pomoću lica
- postaviti pametnu karticu za provjeru autentičnosti
- odrediti potrebne vjerodajnice za provjeru autentičnosti
- upravljati korisnicima računala
- prilagoditi parametre specifične za uređaj
- konfigurirati instalirane aplikacija softvera Security Manager (upravitelj za sigurnost)
- dodati dodatne aplikacije softvera Security Manager (upravitelj za sigurnost)

Pomoću nadzorne ploče softvera Security Manager (Upravitelj za sigurnost) obični korisnici mogu obavljati sljedeće zadatke:

- konfigurirati mogućnosti koje im je ponudio administrator
- omogućiti ograničene kontrole za neke module sustava HP ProtectTools

Softverski moduli dostupni za vaše računalo mogu ovisiti o modelu računala.

Softverski moduli sustava HP ProtectTools mogu biti unaprijed instalirani, unaprijed učitani ili dostupni za preuzimanje s web-mjesta tvrtke HP. Više informacija potražite na adresi http://www.hp.com.

NAPOMENA: upute u ovom vodiču napisane su uz pretpostavku da ste već instalirali primjenjive softverske module ProtectTools.

Značajke softvera HP ProtectTools

Tablica u nastavku opisuje ključne značajke modula u sustavu HP ProtectTools.

Modul	Ključne značajke
Konzola za administraciju softvera HP ProtectTools Security Manager (Upravitelj aplikacija za sustav HP ProtectTools) – za administratore	• postavljanje i konfiguriranje razine sigurnosti i načina sigurnosne prijave pomoću čarobnjaka za postavljanje upravitelja za sigurnost • konfiguriranje mogućnosti skrivenih od osnovnih korisnika • konfiguriranje upravitelja pristupa uređajima i korisničkog pristupa • dodavanje ili uklanjanje korisnika sustava HP ProtectTools i prikaz statusa korisnika pomoću alata za administraciju
HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) – za obične korisnike	• organiziranje, postavljanje i promjena korisničkih imena i lozinki • konfiguriranje i promjena vjerodajnica korisnika, kao što su lozinka za sustav Windows i pametna kartica • konfiguriranje i promjena postavki te uništavanje i čišćenje pomoću programa File Sanitizer • prikaz postavki za upravitelja pristupa uređajima • konfiguriranje preferenci te mogućnosti sigurnosnog kopiranja i vraćanja
Credential Manager (Upravitelj vjerodajnica) za HP ProtectTools (Upravitelj lozinki)	• spremanje, organiziranje i zaštita korisničkih imena i lozinki • postavljanje zaslona za prijavu na web-mjesta i programe za brz i siguran pristup • spremanje korisničkih imena i lozinki za web-mjesto unosom u upravitelj lozinki. Kada sljedeći put posjetite to web-mjesto, upravitelj lozinki automatski će popuniti i poslati podatke • stvaranje jakih lozinki za veću sigurnost računa. Upravitelj lozinki popunjava automatski popunjava i šalje podatke
Drive Encryption(šifriranje pogona) za HP ProtectTools (samo odabrani modeli)	• potpuno šifriranje cijele jedinice tvrdog diska računala • traženje provjere autentičnosti prije podizanja sustava radi dešifriranja i pristupa podacima
Privacy Manager(upravitelj zaštite privatnosti) za HP ProtectTools (samo odabrani modeli)	• korištenje naprednih tehnika prijave za provjeru izvora, cjelovitosti i sigurnosti e-pošte, dokumenata sustava Microsoft® Office ili programa za razmjenu izravnih poruka (instant messaging – IM)
File Sanitizer za HP ProtectTools	• uništavanje digitalnih zapisa (povjerljivih podataka kao što su aplikacijske datoteke, povijest i web-sadržaj te ostali povjerljivi podaci) na računalu te povremeno čišćenje tvrdog diska
Device Access Manager(Upravitelj pristupa uređajima) za HP ProtectTools (samo odabrani modeli)	• omogućivanje IT upraviteljima da kontroliraju pristup uređajima na temelju korisničkih profila • sprječavanje neovlaštenih korisnika da uklanjaju podatke pomoću vanjskih medija za pohranu te da unose viruse u sustav s vanjskih medija • omogućivanje da administratori određenim pojedincima ili grupama korisnika onemoguće pristup uređajima za zapisivanje

Realizacija ključnih sigurnosnih ciljeva

Moduli sustava HP ProtectTools zajedno pružaju rješenje za razne probleme vezane uz sigurnost, uključujući sljedeće ključne sigurnosne ciljeve:

- zaštita od ciljane krađe
- ograničavanje pristupa osjetljivim podacima
- sprječavanje neovlaštenog pristupa s unutarnjih ili vanjskih lokacija
- stvaranje pravila jakih lozinki

Zaštita od ciljane krađe

Primjer ciljane krađe bila bi krađa računala koje sadrži povjerljive podatke i informacije o klijentima na sigurnosnom punktu u zračnoj luci. Sljedeće značajke pomažu u zaštiti od ciljane krađe:

- značajka provjere autentičnosti prije podizanja sustava, ako je omogućena, pomaže u sprječavanju pristupa operacijskom sustavu. Pogledajte sljedeće postupke:
  - Security Manager (Upravitelj za sigurnost)
  - Drive Encryption (Šifriranje pogona)

Ograničavanje pristupa povjerljivim podacima

Pretpostavimo da vanjski revizor radi na lokaciji klijenta i omogućen mu je pristup računalu radi pregleda povjerljivih financijskih podataka; ne želite da revizor ispisuje datoteke ili da ih sprema na uređaj za zapisivanje poput CD medija. Sljedeća značajka pomaže u ograničavanju pristupa podacima:

- Device Access Manager (Upravitelj pristupa uređajima) za HP ProtectTools omogućuje IT upraviteljima da ograniče pristup uređajima za zapisivanje da se povjerljive informacije ne bi mogle ispisivati ili kopirati s tvrdog diska na prijenosne medije.

Sprječavanje neovlaštenog pristupa s unutarnjih ili vanjskih lokacija

Neovlašteni pristup neosiguranom računalu tvrtke predstavlja vrlo konkretan rizik za korporativne mrežne resurse kao što su informacie iz odjela za financije, uprave, iz odjela za istraživanje i razvoj ili osobni podaci, npr. kartoni pacijenata ili osobni financijski podaci. Sljedeće značajke pomažu u sprječavanju neovlaštenog pristupa:

- značajka provjere autentičnosti prije podizanja sustava, ako je omogućena, pomaže u sprječavanju pristupa operacijskom sustavu. Pogledajte sljedeće postupke:
  - Password Manager (Upravitelj lozinki)
  - Drive Encryption (Šifriranje pogona)
- upravitelj lozinki onemogućuje neovlaštenim korisnicima da dobiju lozinke ili pristupaju aplikacijama koje su zaštićene lozinkama.
- upravitelj pristupa uređajima za HP ProtectTools omogućuje IT upraviteljima da ograniče pristup uređajima za zapisivanje da se povjerljive informacije ne bi mogle kopirati s tvrdog diska.

- File Sanitizer omogućuje sigurno brisanje podataka uništavanjem ključnih datoteka i mapa ili čišćenjem tvrdog diska (pisanjem preko podataka koji su izbrisani, ali ih je i dalje moguće oporaviti).
- DriveLock pomaže u sprječavanju pristupanja podacima, čak i ako se tvrdi disk izvadi i instalira u nezaštićeni sustav.

Stvaranje pravila jakih lozinki

Ako na snagu stupi nalog koji zahtijeva primjenu pravila jakih lozinki za desetke web-aplikacija i baza podataka, Security Manager (Upravitelj za sigurnost) donosi zaštićeni spremnik za lozinke i praktičnost jedinstvene prijave.

Dodatni sigurnosni elementi

Dodjeljivanje sigurnosnih uloga

Pri upravljanju sigurnošću računala (naročito za velike tvrtke) važan je postupak podjele odgovornosti i prava na razne vrste administratora i korisnika.

NAPOMENA: u malim tvrtkama ili na računalima za pojedinačnu upotrebu te uloge može imati ista osoba.

Sigurnosne obveze i ovlasti za HP ProtectTools, mogu se podijeliti na sljedeće uloge:

- direktor za sigurnost – definira razinu sigurnosti za tvrtku ili mrežu i određuje sigurnosne značajke koje će se koristiti, kao što su Java™ kartica, biometrijski čitač ili USB token.

  NAPOMENA: Brojne značajke paketa HP ProtectTools direktor za sigurnost može prilagoditi u suradnji s HP-om. Dodatne informacije potražite na HP-ovom web-mjestu na adresi http://www.hp.com.

- Administrator – primjenjuje sigurnosne značajke koje definira voditelj za sigurnost te njima upravlja. Može i omogućivati i onemogućivati neke značajke. Ako je, primjerice, voditelj za sigurnost odlučio koristiti Java kartice, IT upravitelj može u BIOS-u omogućiti sigurnosni način rada za Java karticu.

- Korisnici – koriste sigurnosne značajke. Ako su direktor za sigurnost i IT administrator, na primjer, omogućili Java kartice za sustav, tada korisnik može postaviti PIN za Java karticu i koristiti tu karticu za provjeru autentičnosti.

OPREZ: administratore se potiče da slijede "najbolje postupke" u ograničavanju ovlasti krajnjih korisnika i ograničavanju pristupa korisnicima.

Neovlaštenim korisnicima ne bi trebalo dodjeljivati administrativne ovlasti.

Upravljanje lozinkama sustava HP ProtectTools

Većina značajki softvera HP ProtectTools Security Manager osigurana je lozinkama. Sljedeća tablica sadrži popis lozinki koje se obično koriste, softverski modul u kojem se lozinka postavlja i funkciju lozinke.

U tablici su naznačene i lozinke koje postavljaju i koriste samo IT administratori. Sve ostale lozinke mogu postavljati obični korisnici ili administratori.

Lozinka sustava HP ProtectTools	Postavlja se u sljedećem modulu	Funkcija
Lozinka za prijavu u sustav Windows	Upravljačka ploča sustava Windows® ili softver HP ProtectTools Security Manager (upravitelj za sigurnost sustava HP ProtectTools)	Služi za ručnu prijavu i za provjeru autentičnosti prilikom pristupanja raznim značajkama softvera Security Manager (upravitelj za sigurnost).
Lozinka za značajku Security Manager Backup and Recovery (sigurnosno kopiranje i oporavak upravitelj za sigurnost)	Security Manager (upravitelj za sigurnost), pojedinačni korisnik	Štiti pristup datoteci sigurnosne kopije i oporavka softvera Security Manager (upravitelj za sigurnost).
PIN za Java™ karticu	Java Card Security	Štiti od pristupa sadržaju Java kartice i provjerava autentičnost korisnika Java kartice. Kada se koristi za provjeru

Lozinka sustava HP ProtectTools	Postavlja se u sljedećem modulu	Funkcija
		autentičnosti pri uključivanju, PIN Java kartice štiti i od pristupa pomoćnom programu Computer Setup te sadržaju računala. Provjerava autentičnost korisnika šifriranja pogona, ako je odabran token Java kartice.

Stvaranje sigurne lozinke

Pri stvaranju lozinki najprije morate slijediti sve specifikacije koje je program postavio. Međutim, smatrajte sljedeće smjernice kao općenitu pomoć pri stvaranju jakih lozinki i smanjenju mogućnosti ugrožavanja lozinke:

- koristite lozinku s više od 6 znakova, po mogućnosti više od 8.
- U lozinki rabite velika i mala slova.
- po mogućnosti kombinirajte alfanumeričke znakove te uključujte posebne i interpunkcijske znakove.
- Slova u ključnoj riječi zamijenite posebnim znakovima ili brojevima. Na primjer, za slova l i L možete koristiti broj 1.
- Kombinirajte riječi iz 2 ili više jezika.
- Razdvojite riječ ili frazu brojevima ili posebnim znakovima, na primjer “Mary2-2Cat45”.
- Nemojte koristiti lozinke koje se pojavljuju u rječniku.
- Za lozinku nemojte koristiti svoje ime ili druge osobne podatke poput datuma rođenja, imena kućnih ljubimaca ili majčinog djevojačkog prezimena kao što su datum rođenja, imena kućnih ljubimaca ili majčino djevojačko prezime, čak i ako ga napišete naopačke.
- Redovito mijenjanjte lozinke. Pri svakom mijenjanju možete promijeniti samo nekoliko znakova.
- Ako lozinku zapišete, ne pohranjujte je na vidljivim mjestima blizu računala.
- Ne spremajte lozinku u datoteku na računalu, kao što je e-pošte.
- Nemojte račune zajednički koristiti s drugim osobama račune i ne otkrivajte svoje lozinke.

Sigurnosno kopiranje i vraćanje vjerodajnica za sustav HP ProtectTools

Značajku Backup and Restore (Sigurnosno kopiranje i vraćanje) sustava HP ProtectTools možete koristiti da biste odabrali i sigurnosno kopirali podatke i postavke vjerodajnica za sustav HP ProtectTools.

2 Početak rada s čarobnjakom za postavljanje

Čarobnjak za postavljanje sustava HP ProtectTools vodi vas kroz postavljanje značajki softvera Security Manager (Upravitelj za sigurnost) koje se najčešće koriste. No administrativna konzola sustava HP ProtectTools donosi i bogatstvo dodatnih funkcija. Iste postavke koje se nalaze u čarobnjaku, kao i dodatne sigurnosne značajke, mogu se konfigurirati putem konzole kojoj se pristupa putem izbornika Start u sustavu Windows®. Te se postavke primjenjuju na računalo i na sve korisnike koji računalo zajednički koriste.

1. Tjedan dana nakon postavljanja računala ili kada korisnik s administrativnim pravima prvi put prijeđe prstom preko čitača otisaka prstiju, čarobnjak za postavljanje softvera Security Manager (Upravitelj za sigurnost) automatski će se pokrenuti i provesti vas kroz osnovne korake konfiguracije programa. Automatski se pokreće videotečaj o postavljanju računala.

   – ili –

   Otvorite HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) putem ikone **Gadget** (Programčić) na bočnoj traci sustava Windows ili ikone na programskoj traci u području obavijesti koje se nalazi na krajnjem desnom dijelu programske trake.

   

   Boja gornje trake na ikoni Gadget (Programčić) ukazuje na jedno od sljedećih stanja:

   - crveno – HP ProtectTools nije postavljen ili postoji pogreška u nekom od modula sustava ProtectTools
   - žuto – u softveru Security Manager na stranici stanja aplikacija provjerite koje je promjene postavki potrebno izvršiti
   - plavo – sustav HP ProtectTools postavljen je i ispravno funkcionira

   NAPOMENA: ikona Gadget (Programčić) nije dostupna u sustavu Windows XP.

   – ili –

Kliknite **Start**, zatim **Svi programi**, a potom **HP ProtectTools Administrative Console** (Konzola za administraciju sustava HP ProtectTools).

2. Pročitajte zaslon dobrodošlice, a zatim kliknite **Next** (Dalje).

NAPOMENA: Na zaslonu dobrodošlice odabirom jedne od mogućnosti možete onemogućiti prikazivanje čarobnjaka u budućnosti.

3. Čarobnjak za postavljanje zatražit će da potvrdite svoj identitet.

   Unesite svoju lozinku za sustav Windows ili skenirajte otiske prsta pomoću čitača otisaka prstiju, a zatim kliknite **Next** (Dalje).

   Ako nisu dostupni čitač otisaka prstiju ni pametna kartica, od vas će se tražiti da unesete lozinku za sustav Windows. Tu lozinku morate koristiti kad god se ubuduće od vas bude tražila provjera autentičnosti.

   Ako još niste stvorili lozinku za sustav Windows, zatražit će se da je stvorite. Lozinka za Windows neovlaštenim osobama onemogućuje pristup vašem računu u sustavu Windows, a obavezna je da bi se omogućilo korištenje značajki softvera HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools).

4. Čarobnjak za postavljanje vodi vas kroz postupak postavljanja sigurnosnih značajki koje se primjenjuju na sve korisnike računala.

   - Windows Logon Security (zaštita prijave u sustav Windows) štiti vaše račune u sustavu Windows pomoću određenih vjerodajnica za pristup
   - Drive Encryption (šifriranje pogona) štiti podatke šifriranjem tvrdog diska i na taj ih način čini nečitljivima osobama koje nemaju odgovarajuće ovlasti
   - Pre-Boot Security (zaštita prije pokretanja sustava) štiti računalo sprječavanjem pristupa neovlaštenim osobama prije pokretanja sustava Windows

   NAPOMENA: značajka Pre-Boot Security (zaštita prije pokretanja sustava) nije dostupna ako je BIOS računala ne podržava.

   Da biste omogućili neku sigurnosnu značajku, potvrdite njezin okvir. Što više značajki odaberete, računalo je sigurnije.

5. Na zadnjoj stranici čarobnjaka kliknite **Finish** (Završi).

   Prikazat će se nadzorna ploča softvera Security Manager (Upravitelj za sigurnost).

NAPOMENA: Ako čarobnjak ne prođete do kraja, on će se automatski pokrenuti još dva puta. Nakon toga čarobnjaku možete pristupiti iz informativnog balončića koji se prikazuje u području obavijesti sasvim desno na programskoj traci (osim ako ga niste onemogućili) sve dok ne dovršite postavljanje.

3 Konzola za administraciju softvera HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools)

Administracija u softveru HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) omogućena je putem konzole za administraciju.

NAPOMENA: za administraciju sustava HP ProtectTools potrebne su administratorske ovlasti.

Konzola nudi sljedeće značajke:

- omogućivanje i onemogućivanje sigurnosnih značajki
- upravljanje korisnicima računala
- prilagodba parametara specifičnih za uređaj
- konfiguriranje instaliranih aplikacija softvera Security Manager (Upravitelj za sigurnost)
- dodavanje dodatnih aplikacija softvera Security Manager (Upravitelj za sigurnost)

▲ Da biste koristili aplikacije softvera HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools), pokrenite HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) s izbornika Start ili desnom tipkom miša kliknite na ikonu softvera Security Manager (Upravitelj za sigurnost) u području obavijesti, smještenom na krajnjem desnom dijelu programske trake.

Konzola za administraciju sustava HP ProtectTools i njezine aplikacije dostupne su svim korisnicima koji zajednički koriste ovo računalo.

Otvaranje konzole za administraciju

Da biste obavljali administratorske zadatke, kao što su postavljanje pravila sustava ili konfiguriranje softvera, otvorite konzolu na sljedeći način:

- Kliknite **Start**, zatim **Svi programi**, pa **HP**, a potom **HP ProtectTools Administrative Console** (Konzola za administraciju sustava HP ProtectTools).

  – ili –

  U lijevom oknu softvera Security Manager (Upravitelj za sigurnost) kliknite **Administration** (Administracija).

Da biste obavljali korisničke zadatke, kao što su registracija otisaka prstiju ili korištenje softvera Security Manager (Upravitelj za sigurnost), otvorite konzolu na sljedeći način:

- Kliknite **Start**, zatim **Svi programi**, pa **HP**, a potom **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools).

  – ili –

  Dvokliknite ikonu **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools) u području obavijesti u krajnjem desnom dijelu programske trake.

Korištenje konzole za administraciju

Konzola za administraciju softvera Security Manager (Upravitelj za sigurnost) središnje je mjesto za administraciju softvera HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools).

Konzola je sastavljena od sljedećih komponenti:

- **Tools** (Alati) – ta komponenta prikazuje sljedeće kategorije za konfiguraciju sigurnosti na vašem računalu:
  - **Home** (Početno) – omogućuje odabir sigurnosnih zadataka koje treba izvesti.
  - **System** (Sustav) – omogućuje konfiguriranje sigurnosnih značajki te potvrdu autentičnosti korisnika i uređaja.
  - **Applications** (Aplikacije) – prikazuje opće postavke upravitelja za sigurnost sustava HP ProtectTools i aplikacija softvera Security Manager (Upravitelj za sigurnost).
  - **Data** (Podaci) – nudi proširivi izbornik veza na aplikacije softvera Security Manager (Upravitelj za sigurnost) koje čuvaju vaše podatke.
- **Management Tools** (Alati za upravljanje) – sadrži informacije o dodatnim alatima. Na ploči se prikazuju sljedeće mogućnosti:
  - **HP ProtectTools Security Manager Setup Wizard** (Čarobnjak za postavljanje upravitelja za sigurnost sustava HP ProtectTools) – vodi vas kroz postavljanje softvera HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools).
  - **Help** (Pomoć) – prikazuje ovu datoteku pomoći koja sadrži informacije o softveru Security Manager (Upravitelj za sigurnost) i unaprijed instaliranim aplikacijama. Pomoć za aplikacije koje naknadno dodajete nalazi se unutar tih aplikacija.
  - **About** (O programu) – prikazuje informacije o softveru HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools), kao što su broj verzije i obavijest o autorskim pravima.
- **Main area** (Glavno područje) – prikazuje zaslone određenih aplikacija.

4 Konfiguracija sustava

Sistemskoj grupi pristupate putem ploče izbornika Tools (alati) s lijeve strane zaslona konzole za administraciju sustava HP ProtectTools. Aplikacije u toj grupi služe za upravljanje pravilima i postavkama računala, njegovih korisnika i uređaja.

U sistemskoj grupi nalaze se sljedeće aplikacije:

- **Security (sigurnost)** – upravlja značajkama, provjerom autentičnosti i postavkama koje određuju interakciju korisnika s tim računalom.
- **Users (korisnici)** – postavljanje i registracija korisnika tog računala te upravljanje njima.
- **Devices (uređaji)** – upravljanje postavkama za sigurnosne uređaje ugrađene u računalo ili priključene na njega.

Postavljanje provjere autentičnosti za računalo

Unutar aplikacije za provjeru autentičnosti možete odabrati koje sigurnosne značajke treba implementirati na računalo, odrediti pravila koja upravljaju pristupom računalu i konfigurirati dodatne napredne postavke. Možete odrediti vjerodajnice koje su potrebne za provjeru autentičnosti svake klase korisnika prilikom prijave u sustav Windows ili prijave na web-stranice i programe tijekom korisničke sesije.

Da biste na računalo postavili provjeru autentičnosti, učinite sljedeće:

1. Na izborniku ploče Security (Sigurnost) kliknite **Authentication (Provjera autentičnosti)**.
2. Da biste konfigurirali provjeru autentičnosti prijave, kliknite karticu **Logon Policy (Pravila prijave)**, unesite promjene i kliknite **Apply (Primijeni)**.
3. Da biste konfigurirali provjeru autentičnosti sesije, kliknite karticu **Session Policy (Pravila sesije)**, unesite promjene i kliknite **Primijeni**.

Pravila prijave

Da biste definirali pravila koja upravljaju vjerodajnicama potrebnim za provjeru autentičnosti korisnika prilikom prijave u sustav Windows, učinite sljedeće:

1. Na izborniku Alati kliknite **Sigurnost**, a zatim kliknite **Provjera autentičnosti**.
2. Na kartici **Pravila prijave** kliknite kategoriju korisnika.
3. Navedite vjerodajnice za provjeru autentičnosti potrebne za odabranu kategoriju korisnika. Morate odrediti najmanje jednu vjerodajnicu.
4. Odredite je li potrebna BILO KOJA (samo jedna) od navedenih vjerodajnica ili su potrebne SVE Možete i bilo kojem korisniku onemogućiti pristup računalu.
5. Kliknite **Primijeni**.

Pravila sesije

Da biste definirali pravila koja upravljaju vjerodajnicama potrebnim za pristup aplikacijama sustava HP ProtectTools tijekom sesije sustava Windows, učinite sljedeće:

1. Na izborniku Alati kliknite **Sigurnost**, a zatim kliknite **Provjera autentičnosti**.
2. Na kartici **Pravila sesije** kliknite kategoriju korisnika.
3. Navedite vjerodajnice provjere autentičnosti potrebne za odabranu kategoriju korisnika.
4. Odredite je li za provjeru autentičnosti korisnika potrebna JEDNA ili su potrebne SVE navedene vjerodajnice. Možete postaviti i pristup softveru sustava HP ProtectTools bez provjere autentičnosti.
5. Kliknite **Primijeni**.

Postavke

Možete dopustiti jednu od sljedećih sigurnosnih postavki ili više njih:

- **Dopusti prijavu u jednom koraku** – dopušta korisnicima računala da preskoče prijavu u sustav Windows ako je provjera autentičnosti provedena u BIOS-u ili na razini šifriranog diska.
- **Dopusti provjeru autentičnosti putem značajke HP SpareKey za prijavu u sustav Windows** – korisnicima računala dopušta korištenje značajke HP SpareKey za prijavu u sustav Windows unatoč drugim pravilima provjere autentičnosti koje traži upravitelj za sigurnost.

Da biste uredili postavke, učinite sljedeće:

1. Kliknite određenu postavku da biste je omogućili ili onemogućili.
2. Kliknite **Primijeni** da biste spremili promjene koje ste učinili.

Upravljanje korisnicima

Unutar aplikacije Korisnici možete nadzirati korisnike sustava HP ProtectTools i upravljati njima.

Navedeni su svi korisnici sustava HP ProtectTools i provjereni prema pravilima postavljenim unutar upravitelj za sigurnost i su prema tome imaju li registrirane odgovarajuće vjerodajnice koje im omogućuju da budu usklađeni s tim pravilima.

Korisnicima upravljajte pomoću sljedećih postavki:

- da biste dodali dodatne korisnike, kliknite **Add** (Dodaj)
- da biste izbrisali korisnika, kliknite korisnika, a zatim **Delete** (Izbriši)
- da biste unijeli otisak prsta ili postavili dodatne vjerodajnice za korisnika, kliknite korisnika, a zatim **Enroll** (Unesi)
- da biste pregledali pravila za određenog korisnika, odaberite korisnika i pregledajte pravila u donjem prozoru

Određivanje postavki uređaja

Unutar aplikacije Uređaji možete navesti postavke dostupne za svaki ugrađeni ili priključeni sigurnosni uređaj koji upravitelj za sigurnost sustava HP ProtectTools prepoznaje.

Otisci prstiju

Stranica Otisci prstiju sadrži tri kartice: Prijava, Osjetljivost i Napredno.

Prijava

Možete odabrati najmanji i najveći broj otisaka prstiju koji je korisniku dopušteno prijaviti.

Možete i izbrisati sve podatke iz čitača otisaka prstiju.

△ **OPREZ:** ako očistite sve podatke iz čitača otisaka prstiju, izbrisat će se svi podaci o otiscima prstiju za sve korisnike, uključujući administratore. Ako pravila prijave traže samo otiske prstiju, nijedan korisnik neće se moći prijaviti na računalo.

Osjetljivost

Da biste prilagodili osjetljivost čitača otisaka prstiju prilikom skeniranja otisaka prstiju, pomaknite klizač.

Ako se otisak prsta prepoznaje nedosljedno, možda je potrebna postavka slabije osjetljivosti. Postavka veće osjetljivosti povećava osjetljivost na varijacije u snimkama otiska prstiju i stoga smanjuje mogućnost lažnog prihvaćanja. Srednje visoka postavka daje dobru kombinaciju sigurnosti i praktičnosti.

Napredno

Možete konfigurirati čitač otisaka prstiju da biste sačuvali napajanje dok se računalo napaja putem baterije.

Pametna kartica

Možete konfigurirati računalo tako da se automatski zaključava nakon uklanjanja pametne kartice. No računalo će se zaključati samo ako se pametna kartica koristi kao vjerodajnica za provjeru autentičnosti prilikom prijave u sustav Windows. Uklanjanje pametne kartice koja nije korištena za prijavu u sustav Windows neće zaključati računalo.

▲ Potvrdite okvir da biste omogućili ili onemogućili zaključavanje računala prilikom uklanjanja pametne kartice.

Lice

Razinu sigurnosti za prepoznavanje lica možete postaviti tako da istodobno osigurate jednostavnost korištenja, ali i složenost proboja sigurnosti računala.

1. Kliknite **Start**, zatim **Svi programi** pa **HP**, a potom **HP ProtectTools Administrative Console** (Konzola za administraciju sustava HP ProtectTools).
2. Kliknite **Devices** (Uređaji), a zatim **Face** (Lice).

3. Da bi prijava bila praktičnija, kliknite klizač i pomaknite ga ulijevo, a da bi prepoznavanje bilo točnije, kliknite klizač i pomaknite ga udesno.

   - **Convenience** (Praktičnost) – da biste unesenim korisnicima omogućili jednostavniji pristup u graničnim situacijama, kliknite traku klizača i pomaknite ga na položaj **Convenience** (Praktičnost).
   - **Balance** (Ravnoteža) – da biste našli kompromis između sigurnosti i jednostavnosti korištenja ili ako na računalu imate povjerljive informacije ili se pak računalo nalazi na mjestu gdje postoji mogućnost neovlaštene prijave, kliknite traku klizača i pomaknite ga na položaj **Balance** (Ravnoteža).
   - **Accuracy** (Točnost) — da bi korisnik teže dobio pristup ako je osvjetljenje unesenih slika ili trenutnog okruženja slabije te da biste smanjili mogućnost lažnog prihvaćanja, kliknite traku klizača i pomaknite ga na položaj **Accuracy** (Točnost).

   NAPOMENA: Razina sigurnosti primjenjuje se na sve korisnike

4. Kliknite **Apply** (Primijeni).

Napredne postavke

1. Kliknite **Start**, zatim **Svi programi** pa **HP**, a potom **HP ProtectTools Administrative Console** (Konzola za administraciju sustava HP ProtectTools).
2. Kliknite **Devices** (Uređaji), a zatim **Face** (Lice).
3. Kliknite **Advanced** (Napredno).

   - **Do not require user name for Windows logon** (za prijavu u sustav Windows nije potrebno korisničko ime)
     - Potvrdite okvir da biste korisnicima omogućili prijavu u sustav Windows bez korisničkog imena.
     - Poništite potvrdni okvir ako je za prijavu potrebno korisničko ime.
   - **Enforce the use of PIN for face logon** (Nametanje korištenja PIN-a za prijavu pomoću prepoznavanja lica) — potvrdite okvir ako je za prijavu potrebno da svaki korisnik postavi i koristi PIN (osobni identifikacijski broj).
     - **Minimum length allowed for PIN** (Minimalna duljina PIN-a) – kliknite strelicu gore da biste povećali ili strelicu dolje da biste smanjili minimalni broj znakova potrebnih za PIN.
     - **Maximum length allowed for PIN** (Maksimalna duljina PIN-a) – kliknite strelicu gore da biste povećali ili strelicu dolje da biste smanjili maksimalni broj znakova potrebnih za PIN.
     - **Maximum retries allowed for PIN** (Maksimalni broj pokušaja za PIN) – kliknite strelicu gore da biste povećali ili strelicu dolje da biste smanjili maksimalni broj pokušaja unosa PIN-a.

4. Kliknite **OK** (U redu).

5 Konfiguriranje aplikacija

Putem ploče izbornika Sigurnosne aplikacije s lijeve strane konzole za administraciju sustava HP ProtectTools pristupate grupi aplikacija. Možete koristiti postavke da biste prilagodili ponašanje trenutno instaliranih aplikacija upravitelj za sigurnost sustava HP ProtectTools.

Da biste uredili postavke svojih aplikacija:

1. S izbornika Alati u grupi **Aplikacije** kliknite **Postavke**.
2. Kliknite da biste omogućili ili onemogućili određenu postavku.
3. Kliknite **Primijeni** da biste spremili promjene koje ste učinili.

Kartica Općenito

Na kartici Općenito dostupne su sljedeće postavke:

- **Nemoj automatski pokretati čarobnjak za postavljanje za administratore** – odaberite tu mogućnost da biste spriječili automatsko otvaranje čarobnjaka nakon prijave.
- **Nemoj automatski pokretati čarobnjak za početak rada za korisnike** – odaberite tu mogućnost da biste spriječili automatsko otvaranje korisničkog postavljanja nakon prijave.

Kartica Aplikacije

Postavke koje se ovdje prikazuju mogu se promijeniti kada se u softver Security Manager (upravitelj za sigurnost) dodaju nove aplikacije. Minimalne postavke koje se prikazuju kao zadana postavka:

- **Applications status** (Stanje aplikacija) — omogućuje prikaz stanja svih aplikacija
- **Password Manager** (Upravitelj lozinki) — omogućuje aplikaciju Password Manager za sve korisnike na računalu
- **Privacy Manager** (Upravitelj zaštite privatnosti) — omogućuje aplikaciju Privacy Manager za sve korisnike na računalu
- **Enable the Discover more button** (Omogući gumb Saznajte više) — omogućuje svim korisnicima računala dodavanje aplikacija u softver HP ProtectTools Security Manager (upravitelj za sigurnost sustava HP ProtectTools) klikom na gumb **[+] Discover more** ([+] Saznajte više)

Da biste vratili tvorničke postavke svih aplikacija, kliknite gumb **Restore Defaults** (Vraćanje zadanih postavki).

6 Alati za upravljanje

Mogu biti dostupne dodatne aplikacije za dodavanje novih alata za upravljanje u Upravitelj za sigurnost. Administrator računala može onemogućiti tu značajku putem aplikacije Postavke.

Da biste dodali dodatne alate za upravljanje, kliknite **[+] Alati za upravljanje**.

Ažuriranja i poruke

Ako je računalo povezano s internetom, na web-mjestu DigitalPersona http://www.digitalpersona.com/ možete provjeriti postoje li nove aplikacije ili postaviti raspored automatskog ažuriranja.

1. Da biste zahtijevali informacije o novim aplikacijama i ažuriranjima, potvrdite okvir **Keep me informed about new applications and updates** (Želim primati informacije o novim aplikacijama i ažuriranjima).
2. Da biste postavili raspored automatskog ažuriranja, odaberite broj dana.
3. Da biste provjerili ažuriranja, kliknite **Check Now** (Provjeri sad).

7 Upravitelj za sigurnost sustava HP ProtectTools

Upravitelj za sigurnost sustava HP ProtectTools omogućuje vam da značajno povećate sigurnost svojeg računala.

Možete koristiti unaprijed instalirane aplikacije upravitelj za sigurnost te dodatne aplikacije koje su dostupne za trenutačno preuzimanje putem interneta:

- upravljanje prijavom i lozinkama
- jednostavna promjena lozinke operacijskog sustava Windows®
- postavljanje preferenci programa
- korištenje otisaka prstiju radi dodatne sigurnosti i praktičnosti
- unošenje jedne ili više slika za provjeru autentičnosti
- postavljanje provjere autentičnosti putem pametne kartice
- izrada sigurnosnih kopija i vraćanje programskih podataka
- dodavanje dodatnih aplikacija

Otvaranje upravitelja za sigurnost sustava HP ProtectTools

Upravitelj za sigurnost sustava HP ProtectTools možete otvoriti na bilo koji od sljedećih načina:

- Kliknite **Start**, zatim **Svi programi**, pa **HP**, a potom **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools).
- U području obavijesti, na krajnjoj desnoj strani alatne trake dvokliknite ikonu **HP ProtectTools**.
- Dvokliknite ikonu **HP ProtectTools**, pa kliknite **Otvori upravitelj za sigurnost sustava HP ProtectTools**.
- Na bočnoj traci sustava Windows kliknite programčić **Identifikacijska kartica upravitelja za sigurnost**.
- Pritisnite kombinaciju tipki ctrl+Windows+h da biste otvorili izbornik brzih veza upravitelja za sigurnost.

Korištenje nadzorne ploče upravitelja za sigurnost

Nadzorna ploča softvera Security Manager (Upravitelj za sigurnost) središnje je mjesto za jednostavan pristup značajkama, aplikacijama i postavkama softvera Security Manager (Upravitelj za sigurnost).

▲ Da biste otvorili nadzornu ploču softvera Security Manager (upravitelj za sigurnost), kliknite **Start**, zatim **Svi programi**, pa **HP**, a potom **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools).

Nadzorna ploča sastavljena je od sljedećih komponenti:

- **ID Card** (Identifikacijska kartica) – prikazuje korisničko ime za sustav Windows i sliku pridruženu računu prijavljenog korisnika
- **Security Applications** (Sigurnosne aplikacije) – prikazuje proširivi izbornik veza za konfiguraciju sljedećih kategorija sigurnosti:
  - **Credential Manager (Upravitelj vjerodajnica)**
  - **My data (Moji podaci)**
- **Discover more** (Saznajte više) – otvara stranicu na kojoj ćete pronaći dodatne aplikacije za poboljšanje sigurnosti svojeg identiteta, podataka i komunikacija
- **Main area** (Glavno područje) – prikazuje zaslone određenih aplikacija
- **Administration** (Administracija) – otvara konzolu za administraciju sustava HP ProtectTools
- **Help** (Pomoć) – taj gumb prikazuje informacije o trenutnom zaslonu
- **Advanced** (Dodatno) – omogućuje pristup sljedećim mogućnostima:
  - **Preferences** (Preference) – omogućuje personalizaciju postavki softvera Security Manager (Upravitelj za sigurnost)
  - **Backup and Restore** (Sigurnosno kopiranje i vraćanje) – omogućuje stvaranje sigurnosnih kopija ili vraćanje podataka
  - **About** (O programu) – prikazuje informacije o verziji softvera Security Manager (Upravitelj za sigurnost)

Postupci pri postavljanju

Registracija vjerodajnica

Možete koristiti stranicu "Moj identitet" da biste registrirali različite načine provjere autentičnosti ili vjerodajnice. Nakon registracije te načine možete koristiti za prijavu u Upravitelj za sigurnost.

Unošenje otisaka prstiju

Ako je u računalo ugrađen čitač otisaka prstiju ili je s njim povezan, čarobnjak za postavljanje softvera HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) vodit će vas kroz postupak postavljanja ili "unošenja" otisaka prstiju:

1. Prikazuju se obrisi dviju šaka. Prsti čiji su otisci već uneseni istaknuti su zelenom bojom. Kliknite prst na obrisu.

   NAPOMENA: da biste izbrisali prethodno unesen otisak prsta, kliknite taj prst.

2. Kada odaberete prst čiji ćete otisak unijeti, od vas će se tražiti da skenirate otisak sve dok se uspješno ne unese. Uneseni je prst na obrisu istaknut zelenom bojom.

3. Morate unijeti otiske najmanje dva prsta; preporučuju se kažiprst i srednji prst. Za sljedeći prst ponovite postupak od prvog do trećeg koraka.

4. Kliknite **Next** (Dalje) i slijedite upute na zaslonu.

NAPOMENA: prilikom unosa otisaka prstiju u postupku za početak rada podaci o otiscima spremit će se tek kada kliknete **Next** (Dalje). Ako računalo neko vrijeme ostavite bez nadzora ili zatvorite program, promjene koje ste izvršili **neće** se spremiti.

Unošenje slika

Da biste koristili prijavu pomoću prepoznavanja lica, morate unijeti jednu ili više slika.

Da biste iz čarobnjaka za postavljanje softvera HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) unijeli novu sliku, učinite sljedeće:

1. Na bočnoj traci na desnoj strani zaslona kliknite ikonu **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools).

2. Unesite lozinku za Windows®, a zatim kliknite **Next** (Dalje).

3. U odjeljku **Enable security features** (Omogućivanje sigurnosnih značajki) potvrdite okvir **Windows Logon Security** (Zaštita prijave u sustav Windows), a zatim kliknite **Next** (Dalje).

4. U odjeljku **Choose your credentials** (Odabir vjerodajnica) potvrdite okvir **Face** (Lice), a zatim kliknite **Next** (Dalje).

5. Kliknite **Enroll a new scene** (Unesi novu sliku).

Nakon uspješnog unosa možete unijeti i novu sliku ako tijekom prijave imate poteškoća zbog promjene nekih od sljedećih uvjeta:

- lice se znatno promijenilo od zadnjeg unošenja
- osvjetljenje se znatno razlikuje od onog prilikom prethodnih unošenja
- tijekom zadnjeg unošenja nosili ste naočale (ili niste)

NAPOMENA: Imate li poteškoća s unošenjem scena, pokušajte se pomaknuti bliže web-kameri. Osvjetljenje i kontrast iznimno su važni, kao i kod bilo kakvog oblika snimanja fotografija ili videozapisa. Provjerite je li osvjetljenje vaše sesije prvenstveno u prednjem planu, a ne u pozadini. Ako otkrijete da vas značajka prepoznavanja lica ne prepoznaje, preporučujemo da ponovno unesete svoju scenu s poboljšanim osvjetljenjem.

Da biste unijeli novu sliku iz softvera HP ProtectTools Security Manager (upravitelj za sigurnost sustava HP ProtectTools), učinite sljedeće:

1. Kliknite **Start**, zatim **Svi programi** pa **HP**, a potom **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools).
2. Kliknite **Credentials** (Vjerodajnice), a zatim **Face** (Lice).
3. Kliknite **Enroll a new scene** (Unesi novu sliku).

Dodatne korisničke postavke

1. Kliknite **Start**, zatim **Svi programi**, a potom **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools).
2. Kliknite **Set up your authentication credentials** (Postavite svoje vjerodajnice za provjeru autentičnosti), a zatim **Face** (Lice).
3. Kliknite gumb **Advanced** (Napredno), a zatim odaberite neku od sljedećih mogućnosti.

   a. Da biste postavili obavezan unos PIN-a prilikom prijave pomoću prepoznavanja lica, kliknite **Create PIN** (Stvori PIN), zatim unesite svoju lozinku za Windows, pa novi PIN, a potom ga potvrdite ponovnim unosom.

   b. Po želji odaberite dodatne postavke. Ove se postavke odnose samo na trenutnog korisnika:

   - **Play sound on face recognition events (Reproduciraj zvuk prilikom događaja prepoznavanja lica).**
     - Potvrdite okvir da bi se reproducirao zvuk kada prepoznavanje lica uspije ili ne uspije.
     - Poništite potvrdni okvir da biste onemogućili tu mogućnost.
   - **Prompt to update scenes when logon fails (Zatraži ažuriranje slika kada prijava ne uspije)**
     - Potvrdite okvir da biste korisniku omogućili ažuriranje slika ako prijava pomoću prepoznavanja lica ne uspije. Ako provjera dosegne prag "možda", od korisnika se traži da odluči želi li umetnuti slike uživo iz neuspjele prijave u trenutnu sliku da bi se povećala vjerojatnost za uspješnu prijavu sljedeći put.
     - Poništite potvrdni okvir da biste onemogućili tu mogućnost.
   - **Prompt to enroll a new scene when logon fails (Zatraži unos nove slike kada prijava ne uspije)**
     - Potvrdite okvir da bi se od korisnika zatražio unos nove slika ako prijava pomoću prepoznavanja lica ne uspije, a provjera dostigne prag "možda". Time se povećava vjerojatnost uspjeha prilikom sljedeće prijave.
     - Poništite potvrdni okvir da biste onemogućili tu mogućnost.

   c. Da biste unijeli novu sliku, kliknite **Enroll a new scene** (Unesi novu sliku), a zatim slijedite upute na zaslonu.

Promjena lozinke sustava Windows

Promjena lozinke za Windows pomoću softvera Security Manager (upravitelj za sigurnost) brža je i jednostavnija nego putem upravljačke ploče sustava Windows.

Da biste promijenili lozinku sustava Windows, slijedite ove korake:

1. Na nadzornoj ploči softvera Security Manager (upravitelj za sigurnost) kliknite **Credentials** (Vjerodajnice), a zatim **Password** (Lozinka).
2. Unesite trenutnu lozinku u tekstni okvir **Trenutačna lozinka sustava Windows**.

3. U tekstni okvir **Nova lozinka sustava Windows** unesite novu lozinku, a potom je ponovno unesite u tekstni okvir **Potvrdite novu lozinku**.

4. Kliknite **Promijeni** da biste trenutnu lozinku odmah zamijenili novom.

Postavljanje pametne kartice

Ako ste odabrali prijavu pomoću pametne kartice i u računalo je ugrađen čitač kartica ili je čitač povezan s računalom, čarobnjak za postavljanje softvera Security Manager (Upravitelj za sigurnost) tražit će da postavite PIN (osobni identifikacijski broj) za pametnu karticu.

Postavljanje PIN-a za pametnu karticu:

1. U odjeljku **Set up smart card** (Postavljanje pametne kartice) unesite i potvrdite PIN.

   PIN možete i promijeniti. Unesite trenutni PIN, a zatim unesite novi.

2. Da biste nastavili, kliknite **Next** (Dalje), a zatim slijedite upute na zaslonu.

– ili –

▲ Na nadzornoj ploči softvera Security Manager (upravitelj za sigurnost) kliknite **Credentials** (Vjerodajnice), a zatim **Smart Card** (Pametna kartica).

- Postavljanje PIN-a pametne kartice – u odjeljku **Set up smart card** (Postavljanje pametne kartice) unesite i potvrdite PIN.
- Promjena PIN-a – unesite trenutni PIN, a zatim unesite i potvrdite novi.

Opći zadaci

Aplikacije koje se nalaze u ovoj grupi omogućuju vam upravljanje različitim aspektima vašeg digitalnog identiteta.

- **Upravitelj za sigurnost** — stvara brze veze i upravlja njima, što vam omogućuje da pokrenete web-mjesta i programe te se prijavite na njih provodeći provjeru autentičnosti putem lozinke sustava Windows, otiska prsta ili pametne kartice.
- **Vjerodajnice** — ova postavka omogućuje da jednostavno promijenite lozinku sustava Windows, unesete svoje otiske prstiju ili postavite pametnu karticu.

Da biste dodali nove aplikacije, kliknite gumb [+] **Saznajte više** u donjem lijevom uglu nadzorne ploče. Administrator može onemogućiti taj gumb.

Upravitelj lozinki

Prijava u sustav Windows, na web-mjesta i u aplikacije mnogo je jednostavnija i sigurnija kada koristite upravitelj lozinki. Možete ga koristiti da biste stvorili jake lozinke koje ne morate pisati ili pamtiti i da biste se potom jednostavno i brzo prijavili putem otiska prsta, pametne kartice ili lozinke sustava Windows.

Upravitelj lozinki nudi sljedeće mogućnosti:

- dodavanje, uređivanje ili brisanje prijava putem kartice Upravljanje
- korištenje brzih veza za pokretanje zadanog preglednika i prijavu na bilo koju web-stranicu ili u bilo koji program, nakon što je program postavljen
- organiziranje brzih veza u kategorije putem značajke "povuci i ispusti"
- možete odmah vidjeti koja od vaših lozinki predstavlja sigurnosni rizik i možete automatski stvoriti složenu jaku lozinku koju možete koristiti za nova web-mjesta

Mnoge značajke upravitelja lozinki dostupne su i s ikone upravitelja lozinki koja se prikazuje kada su u središtu web-stranica ili zaslon za prijavu u program. Kliknite ikonu da biste prikazali kontekstni izbornik u kojem možete birati između sljedećih mogućnosti.

Za web-stranice ili programe za koje prijava još nije stvorena

Na kontekstnom izborniku prikazuju se sljedeće mogućnosti:

- **Dodaj [nekadomena.com] u upravitelj lozinki** — omogućuje vam da dodate prijavu u trenutni zaslon za prijavu.
- **Otvori upravitelj lozinki** — pokreće upravitelj lozinki.
- **Postavke ikone** — omogućuje vam da odredite uvjete u kojima se prikazuje ikona upravitelj lozinki.
- **Pomoć** – prikazuje softversku pomoć upravitelja lozinki.

Za web-stranice ili programe za koje je stvorena prijava

Na kontekstnom izborniku prikazuju se sljedeće mogućnosti:

- **Unesi podatke za prijavu** — stavlja vaše podatke za prijavu u polja za prijavu i potom šalje stranicu (ako je slanje navedeno prilikom zadnjeg stvaranja ili uređivanja prijave).
- **Uredi prijavu** — omogućuje vam uređivanje podataka za prijavu za tu web-stranicu.

- **Dodaj novi račun** — omogućuje vam da u prijavu dodate račun.
- **Otvori upravitelj lozinki** — pokreće aplikaciju upravitelj lozinki.
- **Pomoć** – prikazuje softversku pomoć upravitelja lozinki.

NAPOMENA: administrator računala možda je postavio upravitelj lozinki tako da traži više vjerodajnica kada utvrđuje vaš identitet.

Dodavanje prijava

Možete jednostavno dodati prijavu za web-mjesto ili program ako jednom unesete informacije za prijavu. Od tada upravitelj lozinki automatski unosi informacije za vas. Možete koristiti te prijave nakon pregledavanja web-mjesta ili programa ili na izborniku **Prijave** kliknuti prijavu da bi upravitelj lozinki otvorio web-mjesto ili program i prijavio vas.

Da biste dodali prijavu, učinite sljedeće:

1. Otvorite zaslon za prijavu web-mjesta ili programa.
2. Kliknite strelicu na ikoni **Upravitelj lozinki** a zatim kliknite jedno od sljedećeg, ovisno o tome pripada li zaslon za prijavu web-mjestu ili programu:
   - za web-mjesto kliknite **Dodaj [naziv domene] u upravitelj lozinki**
   - za program kliknite **Dodaj ovaj zaslon za prijavu u upravitelj lozinki**
3. Unesite podatke za prijavu. Polja za prijavu na zaslonu i odgovarajuća polja u dijaloškom okviru označena su podebljanim narančastim obrubom. Taj će se dijaloški okvir prikazati i ako na kartici **Password Manager Manage** (Upravljanje upraviteljem lozinki) kliknete **Add Logon** (Dodaj prijavu). Neke mogućnosti ovise o sigurnosnim uređajima povezanima s računalom, primjerice o tome koristite li kombinaciju tipki ctrl+Windows+h, skeniranje otiska prsta ili umetanje pametne kartice.
   a. Da biste polje za prijavu ispunili jednom od unaprijed oblikovanih mogućnosti, kliknite strelice desno od polja.
   b. Da biste vidjeli lozinku za prijavu, kliknite **Show password** (Pokaži lozinku).
   c. Da biste ispunili polja za prijavu, ali ne i poslali podatke, poništite potvrdni okvir **Automatically submit logon data** (Automatski šalji podatke za prijavu).
   d. Kliknite **OK** (U redu), zatim način provjere autentičnosti koji želite koristiti: **Fingerprints** (Otisci prstiju), **Password** (Lozinka) ili **Face** (Lice), a potom se prijavite pomoću odabranog načina provjere autentičnosti.

      S ikone softvera Password Manager (upravitelj lozinki) nestat će znak plus, što vas obavještava da je prijava stvorena.
   e. Ako Password Manager (upravitelj lozinki) ne prepozna polja za prijavu, kliknite **More fields** (Dodatna polja).
      i. Potvrdite okvir za svako polje koje je potrebno za prijavu, odnosno poništite potvrdni okvir za ona koja nisu potrebna.
      ii. Ako Password Manager (upravitelj lozinki) ne prepozna sva polja za prijavu, prikazat će se poruka s pitanjem želite li nastaviti. Kliknite **Yes** (Da).

iii. Prikazuje se dijaloški okvir s ispunjenim poljima za prijavu. Kliknite ikonu za svako polje i povucite je u odgovarajuće polje za prijavu, a zatim kliknite gumb za prijavu na web-mjesto.

NAPOMENA: kada podatke za prijavu na neko web-mjesto unesete ručno, taj način prijave morate i ubuduće koristiti za prijavu na to web-mjesto.

NAPOMENA: ručni način unosa podataka za prijavu dostupan je samo u pregledniku Internet Explorer 8.

iv. Kliknite **Close** (Zatvori).

Ikona softvera Password Manager (upravitelj lozinki) koja naznačuje da možete koristiti registrirane vjerodajnice za prijavu prikazat će se prilikom svakog pristupanja tom web-mjestu ili otvaranja programa.

Uređivanje prijava

Da biste uredili prijavu, slijedite ove korake:

1. Otvorite zaslon za prijavu na web-mjesto ili u program.
2. Da bi vam se prikazao dijaloški okvir u kojem možete urediti svoje informacije za prijavu, kliknite strelicu na ikoni **Upravitelj lozinki**, a zatim kliknite **Uredi lozinku**. Polja za prijavu na zaslonu i njima odgovarajuća polja u dijaloškom okviru prikazuju se s debelim narančastim obrubom.

   Taj će se dijaloški okvir prikazati i ako kliknete **Uredi za željenu prijavu** na kartici **Upravljanje upraviteljem lozinki**.
3. Uredite podatke za prijavu.
   - Da biste polje za prijavu ispunili jednim od unaprijed oblikovanih izbora, kliknite strelice s desne strane polja.
   - Da biste u prijavu dodali dodatna polja sa zaslona, kliknite **More fields** (Dodatna polja).
   - Da biste ispunili polja za prijavu, ali ne i poslali podatke, poništite potvrdni okvir **Pošalji podatke za prijavu**.
   - Da biste vidjeli lozinku za prijavu, kliknite **Show password** (Pokaži lozinku).
4. Kliknite **U redu**.

Korištenje izbornika za prijavu

Upravitelj lozinki omogućuje brz, jednostavan način pokretanja web-mjesta i programa za koje ste stvorili prijave. Dvokliknite prijavu za program ili web-mjesto s izbornika **Prijave** ili kartice **Upravljanje** u programu da biste otvorili zaslon za prijavu i potom unijeli svoje podatke za prijavu.

Kada stvorite prijavu, ona se automatski dodaje u vaš izbornik prijava upravitelj lozinki.

Da biste prikazali izbornik prijava, učinite sljedeće:

1. Pritisnite kombinaciju tipki koja otvara **Password Manager** (Upravitelj lozinki). Tvornička je postavka ctrl+Windows+h. Da biste promijenili kombinaciju tipki, kliknite **Password Manager** (Upravitelj lozinki), a zatim **Settings** (Postavke).
2. Skenirajte svoj otisak prsta (na računalima s ugrađenim ili povezanim čitačem otisaka prstiju).

Organizacija prijava u kategorije

Koristite kategorije da biste organizirali prijave stvarajući jednu ili više kategorija. Potom povucite i ispustite prijave u željene kategorije.

Da biste dodali kategoriju, učinite sljedeće:

1. Na nadzornoj ploči upravitelj za sigurnost kliknite **Upravitelj lozinki**.
2. Kliknite karticu **Manage** (Upravljanje), a zatim **Add Category** (Dodaj kategoriju).
3. Unesite naziv kategorije.
4. Kliknite **U redu**.

Da biste u kategoriju dodali prijavu, učinite sljedeće:

1. Stavite pokazivač miša iznad željene prijave.
2. Pritisnite i držite lijevu tipku miša.
3. Dok iznad kategorije povlačite miš, kategorija će se istaknuti.
4. Otpustite tipku miša kada se istakne željena kategorija.

Vaše se prijave ne premještaju u kategoriju, već se samo kopiraju u odabranu kategoriju. Možete dodati istu prijavu u više kategorija, a sve svoje prijave možete pogledati klikom na mogućnost **Sve**.

Upravljanje prijavama

Upravitelj lozinki pojednostavnjuje upravljanje informacijama za prijavu, odnosno korisničkim imenima, lozinkama i većim brojem računa za prijavu, s jedne središnje lokacije.

Vaše prijave nalaze se na popisu unutar kartice Upravljanje. Ako je za isto web-mjesto stvoreno više prijava, svaka se prijava nalazi na popisu ispod naziva web-mjesta i uvučena je na popisu prijava.

Da biste upravljali prijavama, učinite sljedeće:

na nadzornoj ploči upravitelj za sigurnost kliknite **Upravitelj lozinki**, a zatim kliknite karticu **Upravljanje**.

- **Dodaj prijavu** — kliknite **Dodaj prijavu** i slijedite upute na zaslonu.
- **Uredi prijavu** — kliknite prijavu, zatim kliknite **Uredi**, a potom promijenite podatke za prijavu.
- **Izbriši prijavu** — kliknite prijavu, a zatim **Izbriši**.

Da biste dodali dodatnu prijavu za web-mjesto ili program:

1. Otvorite zaslon za prijavu web-mjesta ili programa.
2. Kliknite ikonu **Upravitelj lozinki** da biste prikazali njegov izbornik prečaca.
3. Kliknite **Dodaj dodatnu prijavu**, a zatim slijedite upute na zaslonu.

Procjenjivanje snage lozinke

Korištenje jakih lozinki za prijavu na web-mjesta i u programe važan je dio zaštite identiteta.

Upravitelj lozinki pojednostavnjuje nadzor i poboljšanje sigurnosti zahvaljujući trenutačnoj i automatskoj analizi snage svake lozinke koja se koristi za prijavu na web-mjesta i u programe.

Postavke ikone upravitelj lozinki

Upravitelj lozinki pokušava identificirati zaslone za prijavu na web-mjesta u programe. Kada otkrije zaslon za prijavu za koji niste stvorili prijavu, upravitelj lozinki od vas traži da dodate prijavu za zaslon prikazujući ikonu upravitelj lozinki sa znakom "+".

Kliknite strelicu ikone, a zatim kliknite **Postavke ikone** da biste prilagodili kako **Upravitelj lozinki** upravlja mogućim mjestima za prijavu.

- **Zatraži dodavanje prijava za zaslone za prijavu** — kliknite tu mogućnost da bi vas upravitelj lozinki zatražio dodavanje prijave kada se prikaže zaslon za prijavu za koji još nije postavljena prijava.
- **Izuzmi ovaj zaslon** – potvrdite ovaj okvir tako da upravitelj lozinki ne traži od vas ponovno dodavanje prijave za taj zaslon za prijavu.

Da biste pristupili dodatnim postavkama upravitelj lozinki, kliknite **Upravitelj lozinki**, a zatim na nadzornoj ploči upravitelj za sigurnost kliknite **Postavke**.

Postavke

Možete navesti postavke za prilagođavanje upravitelj za sigurnost sustava HP ProtectTools:

1. **Zatraži dodavanje prijava za zaslone za prijavu** — ikona upravitelj lozinki sa znakom plus prikazat će se svaki put kad se otkrije zaslon za prijavu na web-mjesto ili u program, naznačavajući da u riznicu lozinki treba dodati prijavu za taj zaslon. Da biste onemogućili tu značajku, u dijaloškom okviru **Postavke ikone** poništite potvrdni okvir mogućnosti **Zatraži dodavanje prijava za zaslone za prijavu**.
2. **Otvori upravitelj lozinki pomoću tipki ctrl+Windows+h** – zadana je kombinacija tipki koja otvara brze veze upravitelja lozinki ctrl+Windows+h. Da biste promijenili kombinaciju, kliknite tu mogućnost i unesite novu kombinaciju tipki. Kombinacije mogu obuhvaćati: ctrl, alt ili shift te bilo koju slovnu ili numeričku tipku.
3. Kliknite **Primijeni** da biste spremili promjene.

Vjerodajnice

Koristite vjerodajnice za upravitelj za sigurnost da biste potvrdili da je uistinu riječ o vama. Lokalni administrator računala može postaviti vrstu vjerodajnica koje se mogu koristiti za dokazivanje identiteta prilikom prijave u račun sustava Windows, na web-mjesta ili u programe.

Dostupne vjerodajnice ovise o sigurnosnim uređajima koji su ugrađeni ili priključeni na računalo. Svaka podržana vjerodajnica imat će unos u grupi **Moj identitet, vjerodajnice**.

Na popisu se nalaze dostupne vjerodajnice, zahtjevi i trenutačni status, a mogu uključivati sljedeće:

- otiske prstiju
- lozinku
- pametnu karticu
- lice

Da biste unijeli ili promijenili vjerodajnicu, kliknite vezu i slijedite upute na zaslonu.

Vaša osobna identifikacijska kartica

Vaša identifikacijska kartica služi kao potvrda da ste vlasnik računa sustava Windows, prikazuje vaše ime i sliku koju ste odabrali. Ona je jasno vidljiva u gornjem lijevom kutu stranica upravitelj za sigurnost i kao programčić na bočnoj traci sustava Windows.

Klik na identifikacijsku karticu na bočnoj traci sustava Windows jedan je od mnogih načina da brzo pristupite upravitelju sigurnosti.

Možete promijeniti sliku i način prikaza svojeg imena. Prema zadanome, prikazuju se vaše puno korisničko ime u sustavu Windows i slika koju ste odabrali tijekom postavljanja sustava.

Da biste promijenili prikazano ime, učinite sljedeće:

1. Na nadzornoj ploči softvera Security Manager (upravitelj za sigurnost) u gornjem lijevom kutu kliknite ikonu **ID Card** (Identifikacijska kartica).
2. Kliknite potvrdni okvir u kojem je prikazano vaše ime koje ste unijeli za svoj račun u sustavu Windows. Sustav će prikazati vaše korisničko ime za Windows za taj račun.
3. Da biste promijenili to ime, unesite novo ime, a zatim kliknite gumb **Spremi**.

Da biste promijenili prikazanu sliku, učinite sljedeće:

1. Na nadzornoj ploči softvera Security Manager (upravitelj za sigurnost) u gornjem lijevom kutu kliknite **ID Card** (Identifikacijska kartica).
2. Kliknite gumb **Odaberi sliku**, kliknite sliku, a zatim kliknite gumb **Spremi**.

Postavljanje preferenci

Možete prilagoditi postavke upravitelja za sigurnost sustava HP ProtectTools. Na nadzornoj ploči upravitelja za sigurnost kliknite **Napredno**, a zatim kliknite **Preference**. Dostupne postavke prikazane su na dvije kartice: Općenito i Otisak prsta.

Općenito

Na kartici Općenito dostupne su sljedeće postavke:

Izgled – Prikaži ikonu na alatnoj traci

- Da biste omogućili prikaz ikone na alatnoj traci, potvrdite okvir.
- Da biste onemogućili prikaz ikone na alatnoj traci, poništite potvrdni okvir.

Otisak prsta

Na kartici Otisak prsta dostupne su sljedeće postavke:

- **Quick Actions** (Brze akcije) – pomoću brzih akcija odaberite zadatak koji će Security Manager (Upravitelj za sigurnost) izvršiti dok prilikom skeniranja otiska prsta držite tu tipku.

  Da biste brzu akciju dodijelili jednoj od tipki s popisa, kliknite mogućnost **(tipka) + Fingerprint** ((tipka)+otisak prsta), a zatim s izbornika odaberite jedan od dostupnih zadataka.

- **Fingerprint Scan Feedback** (Povratne informacije skeniranja otiska prsta) – prikazuje se samo kada je dostupan čitač otisaka prstiju. Pomoću te postavke možete prilagoditi povratne informacije skeniranja otiska prsta.

  - **Enable sound feedback** (Omogući zvukovne povratne informacije) – upravitelj za sigurnost daje vam zvukovne povratne informacije nakon skeniranja otiska prsta, reproducirajući različite zvukove za određene događaje programa. Na kartici Zvukovi upravljačke ploče sustava Windows događajima možete dodijeliti nove zvukove ili možete poništiti taj potvrdni okvir i tako onemogućiti zvukovne povratne informacije.

  - **Show scan quality feedback (Prikaži povratne informacije o kvaliteti skeniranja)**

    Da bi vam se prikazali svi skenirani dokumenti, bez obzira na kvalitetu, potvrdite okvir.

    Da bi vam se prikazali samo skenirani dokumenti dobre kvalitete, poništite potvrdni okvir.

Stvaranje sigurnosnih kopija i vraćanje podataka

Preporučuje se da redovno stvarate sigurnosne kopije podataka upravitelj za sigurnost. Koliko ćete često stvarati sigurnosne kopije ovisi o brzini promjene podataka. Primjerice, ako dnevno stvarate nove prijave, trebali biste svaki dan stvarati sigurnosne kopije podataka.

Sigurnosne kopije podataka mogu se koristiti za migriranje s jednog računala na drugo, što se još naziva izvoz i uvoz.

NAPOMENA: ovom značajkom stvaraju se samo sigurnosne kopije podataka.

Upravitelj za sigurnost sustava HP ProtectTools mora biti instaliran na svakom računalu koje će primiti sigurnosnu kopiju podataka prije nego se podaci vrate iz sigurnosne kopije.

Da biste stvorili sigurnosnu kopiju podataka, učinite sljedeće:

1. Na lijevoj ploči kliknite **Napredno**, a zatim kliknite **Stvaranje sigurnosne kopije i vraćanje**.
2. Kliknite **Stvori sigurnosnu kopiju podataka**.
3. Odaberite module koje želite uključiti u sigurnosnu kopiju. U većini slučajeva dobro je odabrati sve module.
4. Unesite naziv datoteke za pohranu. Po zadanome datoteka se sprema u mapu Dokumenti. Kliknite **Pregledaj** da biste naveli drugu lokaciju.
5. Unesite lozinku da biste zaštitili datoteku.
6. Potvrdite svoj identitet.
7. Kliknite **Završi**.

Da biste vratili podatke, učinite sljedeće:

1. Na lijevoj ploči kliknite **Napredno**, a zatim kliknite **Stvaranje sigurnosne kopije i vraćanje**.
2. Kliknite **Vrati podatke**.
3. Odaberite ranije stvorenu datoteku za pohranu. U odgovarajuće polje možete unijeti put ili kliknite **Pregledaj**.
4. Unesite lozinku koju ste koristili za zaštitu datoteke.
5. Odaberite module čije podatke želite vratiti. U većini slučajeva to će biti svi moduli s popisa.
6. Kliknite **Završi**.

Saznajte više

Mogu biti dostupne dodatne aplikacije koje pružaju nove značajke za taj program.

Na nadzornoj ploči upravitelja za sigurnost kliknite **[+] Saznajte više** da biste pregledali dodatne aplikacije.

NAPOMENA: ako u donjem lijevom dijelu nadzorne ploče ne postoji veza **[+] Saznajte više**, onemogućio ju je administrator računala.

Ažuriranja i poruke

1. Da biste zahtijevali informacije o novim aplikacijama i ažuriranjima, potvrdite okvir **Keep me informed about new applications and updates** (Želim primati informacije o novim aplikacijama i ažuriranjima).
2. Da biste postavili raspored automatskog ažuriranja, odaberite broj dana.
3. Da biste provjerili ažuriranja, kliknite **Check Now** (Provjeri sad).

Stanje sigurnosnih aplikacija

Na stranici stanja aplikacija softvera Security Manager (upravitelj za sigurnost) prikazuje se cjelokupno stanje instaliranih sigurnosnih aplikacija. Stranica sadrži postavljene aplikacije i stanje postavljanja svake od njih. Sažetak se prikazuje automatski kada otvorite nadzornu ploču softvera Security Manager (upravitelj za sigurnost) i kliknete **Check the status of the security applications** (Provjeri stanje sigurnosnih aplikacija), kada kliknete **Security Applications** (Sigurnosne aplikacije) ili **Check Now** (Provjeri sada) na ikoni **Gadget** (Programčić) na bočnoj traci sustava Windows na desnoj strani zaslona.

8 Šifriranje pogona za sustav HP ProtectTools (samo odabrani modeli)

△ **OPREZ:** Ako odlučite deinstalirati modul Šifriranje pogona, tada najprije morate dešifrirati sve šifrirane pogone. Ako to ne učinite, nećete moći pristupati podacima na šifriranim pogonima, osim ako niste registrirani za uslugu oporavka šifriranja pogona. Ponovno instaliranje modula Šifriranje pogona neće omogućiti pristup šifriranim pogonima.

Drive Encryption for HP ProtectTools (Šifriranje pogona za HP ProtectTools) omogućuje potpunu zaštitu podataka pomoću šifriranja tvrdog diska računala. Kada je značajka Drive Encryption (šifriranje pogona) omogućena, morate se prijaviti na zaslonu za prijavu značajke Drive Encryption (šifriranje pogona) koji se prikazuje prije pokretanja operacijskog sustava Windows®.

Čarobnjak za postavljanje sustava HP ProtectTools omogućuje administratorima sustava Windows da pokreću šifriranje pogona, izrade sigurnosnu kopiju šifre šifriranja, dodaju i uklanjaju korisnike te da isključuju šifriranje pogona. Dodatne informacije potražite u softverskoj pomoći za upravitelj za sigurnost sustava HP ProtectTools.

Pomoću značajke šifriranja diska moguće je obaviti sljedeće zadatke:

- upravljanje šifriranjem

  šifriranje ili dešifriranje pojedinačnih pogona

  NAPOMENA: moguće je šifrirati samo interne tvrde diskove.

- oporavak
  - stvaranje sigurnosnih kopija šifri
  - izvođenje oporavka

Postupci postavljanja

Otvaranje šifriranja pogona

1. Kliknite **Start**, zatim **Svi programi**, a potom kliknite **HP** pa kliknite **Konzola za administraciju sustava HP ProtectTools**.
2. U lijevom oknu kliknite **Šifriranje pogona**.

Opći zadaci

Pokretanje šifriranja pogona

Koristite čarobnjak za postavljanje sustava HP ProtectTools da biste pokrenuli šifriranje pogona.

NAPOMENA: taj se čarobnjak koristi i za dodavanje, odnosno uklanjanje korisnika.

– ili –

1. Kliknite **Start**, zatim **Svi programi**, a potom kliknite **HP** pa kliknite **Konzola za administraciju sustava HP ProtectTools**.
2. U lijevom oknu kliknite **Sigurnost**, a zatim kliknite **Značajke**.
3. Potvrdite okvir **Šifriranje pogona**, a zatim kliknite **Dalje**.
4. Unutar mogućnosti **Pogoni koje treba šifrirati** potvrdite okvir za tvrdi disk koji želite šifrirati.
5. U odgovarajući utor umetnite uređaj za pohranu.

   NAPOMENA: da biste spremili šifru za šifriranje, morate imati USB uređaj za pohranu s datotečnim sustavom FAT32.

6. Unutar mogućnosti **Vanjski uređaj za pohranu na koji treba spremiti šifru za šifriranje** potvrdite okvir uređaja za pohranu na koji ćete spremiti šifru za šifriranje.
7. Kliknite **Primijeni**.

   Započinje šifriranje pogona.

Dodatne informacije potražite u softverskoj pomoći za upravitelj za sigurnost sustava HP ProtectTools.

Isključivanje šifriranja pogona

Koristite čarobnjak za postavljanje sustava HP ProtectTools da biste isključili šifriranje pogona. Dodatne informacije potražite u softverskoj pomoći za upravitelj za sigurnost sustava HP ProtectTools

– ili –

1. Kliknite **Start**, zatim **Svi programi**, a potom kliknite **HP** pa kliknite **Konzola za administraciju sustava HP ProtectTools**.
2. U lijevom oknu kliknite **Sigurnost**, a zatim kliknite **Značajke**.
3. Poništite potvrdni okvir **Šifriranje pogona**, a zatim kliknite **Primijeni**.

   Započinje dešifriranje pogona.

Prijava nakon pokretanja šifriranja pogona

Kada nakon aktivacije značajke Drive Encryption (šifriranje pogona) i upisivanja korisničkog računa uključite računalo, morate se prijaviti na zaslonu za prijavu softvera Drive Encryption (šifriranje pogona):

NAPOMENA: ako je administrator sustava Windows u softveru HP ProtectTools Security Manager (upravitelj za sigurnost sustava HP ProtectTools) omogućio značajku Pre-Boot Security (zaštita prije pokretanja), na računalo ćete se prijaviti odmah nakon uključivanja računala, a ne na zaslonu značajke Drive Encryption (šifriranje pogona).

1. Kliknite svoje korisničko ime, a potom unesite lozinku sustava Windows ili PIN kartice Java™ ili učitajte registrirani prst.
2. Kliknite **U redu**.

NAPOMENA: ako se na zaslon za prijavu značajke Drive Encryption (šifriranje podataka) prijavljujete pomoću šifre za oporavak, od vas će se tražiti i da odaberete korisničko ime sustava Windows te da na zaslonu za prijavu u sustav Windows unesete lozinku.

Zaštita podataka šifriranjem tvrdog diska

Koristite čarobnjak za postavljanje sustava HP ProtectTools da biste zaštitili svoje podatke šifriranjem tvrdog diska:

1. U upravitelju za sigurnost kliknite **Početak rada**, a zatim kliknite ikonu **Postavljanje upravitelja za sigurnost**. Pokreće se prikaz koji opisuje značajke upravitelja za sigurnost. (Upravitelj za sigurnost možete pokrenuti i sa stranice "Šifriranje pogona".)
2. Na lijevom oknu kliknite **Šifriranje pogona**, a zatim kliknite **Upravljanje šifriranjem**.
3. Kliknite **Promijeni šifriranje**.
4. Odaberite pogon ili pogone koje treba šifrirati.

NAPOMENA: preporučuje se šifriranje tvrdog diska.

Prikaz stanja šifriranja

Korisnici mogu prikazati stanje šifriranja iz upravitelj za sigurnost sustava HP ProtectTools.

NAPOMENA: promjene stanja šifriranja moraju se učiniti putem konzole za administraciju sustava HP ProtectTools.

1. Otvorite **Upravitelj za sigurnost sustava HP ProtectTools**.
2. Unutar mogućnosti **Moji podaci** kliknite **Stanje šifriranja**.

   Ako je šifriranje pogona aktivno, stanje pogona prikazuje jednu od sljedećih šifri stanja:

   - Aktivno
   - Neaktivno
   - Nije šifrirano
   - Šifrirano
   - Šifriranje
   - Dešifriranje

   Ako je tvrdi disk u postupku šifriranja ili dešifriranja, traka prikaza tijeka prikazuje postotak dovršenog i preostalo vrijeme potrebno za dovršetak šifriranja ili dešifriranja.

Dodatni zadaci

Upravljanje šifriranjem pogona (zadatak administratora)

Stranica za upravljanje šifriranjem administratorima omogućuje pregled i promjenu statusa šifriranja pogona (aktivnog ili neaktivnog) te pregled stanja šifriranja svih tvrdih diskova na računalu.

- Ako je status Neaktivno, administrator sustava Windows još nije aktivirao šifriranje pogona u upravitelju za sigurnost sustava HP ProtectTools i tvrdi disk još nije zaštićen. Koristite čarobnjak za postavljanje upravitelj za sigurnost sustava HP ProtectTools da biste pokrenuli šifriranje pogona.
- Ako je status Aktivno, šifriranje je pogona aktivirano i konfigurirano. Pogon je u jednome od sljedećih stanja:
  - Nije šifrirano
  - Šifrirano
  - Šifriranje
  - Dešifriranje

Šifriranje ili dešifriranje pojedinačnih pogona

Da biste šifrirali jedan tvrdi disk na računalu ili više njih ili da biste dešifrirali pogon koji je već šifriran, koristite značajku Promjeni šifriranje:

1. Otvorite **Konzolu za administraciju sustava HP ProtectTools**, zatim kliknite **Šifriranje pogona**, a potom kliknite **Upravljanje šifriranjem**.
2. Kliknite **Promijeni šifriranje**.
3. U dijaloškom okviru Promijeni šifriranje potvrdite ili poništite potvrdni okvir pored svakog tvrdog diska koji želite šifrirati ili dešifrirati, a zatim kliknite **U redu**.

NAPOMENA: kada se pogon šifrira ili dešifrira, na traci prikaza tijeka pokazuje se vrijeme preostalo do dovršetka postupka tijekom trenutne sesije. Ako se računalo isključi ili ako tijekom postupka šifriranja uđe u stanje mirovanja ili hibernacije, a zatim se ponovno pokrene, prikaz preostalog vremena vraća se na početak, ali se postupak šifriranja nastavlja na mjestu gdje je prekinut. Preostalo vrijeme i prikaz tijeka mijenjat će se mnogo brže da bi odrazili prethodni napredak.

Sigurnosno kopiranje i oporavak (zadatak administratora)

Stranica za oporavak administratorima omogućuje stvaranje sigurnosnih kopija i oporavak šifri za šifriranje.

Stvaranje sigurnosne kopije šifre za šifriranje lokalnog diska — omogućuje vam da na prijenosnom mediju stvorite sigurnosnu kopiju šifri za šifriranje kada je aktivirano šifriranje pogona.

Stvaranje sigurnosnih kopija šifri

Šifru šifriranog pogona možete sigurnosno kopirati na prijenosni uređaj za pohranu:

△ **OPREZ:** pazite da uređaj za pohranu koji sadrži sigurnosnu kopiju šifre čuvate na sigurnom mjestu jer ako zaboravite svoju lozinku ili izgubite karticu Java, taj je uređaj jedini pristup vašem tvrdom disku.

1. Otvorite **Konzolu za administraciju sustava HP ProtectTools**, zatim kliknite **Šifriranje pogona**, a potom kliknite **Oporavak**.
2. Kliknite **Sigurnosna kopija šifre**.
3. Na stranici Odabir diska za sigurnosnu kopiju potvrdite okvir za uređaj na koji želite spremiti sigurnosnu kopiju šifre za šifriranje, a zatim kliknite **Dalje**.
4. Pročitajte informacije na sljedećoj stranici koja se prikaže, a zatim kliknite **Dalje**. Šifra za šifriranje sprema se na uređaj za pohranu koji ste odabrali.
5. Kada se otvori dijaloški okvir za potvrdu, kliknite **Završi**.

Izvođenje oporavka

Da biste izveli oporavak ako ste zaboravili lozinku, slijedite ove korake:

1. Uključite računalo.
2. Umetnite prijenosni uređaj za pohranu na kojem se nalazi sigurnosna kopija šifre.
3. Kada se otvori dijaloški okvir softvera Drive Encryption for HP ProtectTools, kliknite **Cancel** (Odustani).
4. U donjem lijevom kutu zaslona kliknite **Mogućnosti**, a zatim kliknite **Oporavak**.
5. Odaberite datoteku koja sadrži sigurnosnu kopiju šifre ili kliknite **Pregledaj** da biste je potražili, a zatim kliknite **Dalje**.
6. Kada se otvori dijaloški okvir za potvrdu, kliknite **U redu**.

   Računalo se pokreće.

NAPOMENA: preporučuje se da ponovno postavite lozinku nakon izvođenja oporavka.

9 Upravitelj zaštite privatnosti za HP ProtectTools (samo odabrani modeli)

Privacy Manager for HP ProtectTools (upravitelj zaštite privatnosti za HP ProtectTools) omogućuje vam korištenje napredne sigurnosne prijave (provjere autentičnosti) radi provjere izvora, cjelovitosti i sigurnosti komunikacije prilikom korištenja e-pošte, dokumenata iz sustava Microsoft® Office ili izravnih poruka.

Privacy Manager (upravitelj zaštite privatnosti) koristi sigurnosnu infrastrukturu softvera HP ProtectTools Security Manager (upravitelj za sigurnost sustava HP ProtectTools), a koja uključuje sljedeće načine sigurnosne prijave:

- provjera autentičnosti putem otiska prsta
- lozinka sustava Windows®
- kartica HP ProtectTools Java™

U softveru Privacy Manager (upravitelj zaštite privatnosti) možete koristiti bilo koji od navedenih načina sigurnosne prijave.

Za upravitelj zaštite privatnosti potrebno je sljedeće:

- HP ProtectTools Security Manager 5.00 ili noviji
- Operacijski sustav Windows® 7, Windows Vista® ili Windows XP
- Microsoft Outlook 2007 ili Microsoft Outlook 2003
- valjani račun e-pošte

NAPOMENA: da biste mogli pristupati sigurnosnim značajkama, od upravitelj zaštite privatnosti morate zatražiti i instalirati certifikat za upravitelj zaštite privatnosti (digitalni certifikat). Informacije o načinu traženja certifikata za upravitelj zaštite privatnosti potražite u odjeljku Traženje i instalacija certifikata za upravitelj zaštite privatnosti na stranici 47.

Postupci postavljanja

Otvaranje upravitelj zaštite privatnosti

Da biste otvorili upravitelj zaštite privatnosti:

1. Kliknite **Start**, a zatim **Svi programi**, kliknite **HP**, a zatim kliknite **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools).
2. Kliknite **Upravitelj zaštite privatnosti**

– ili –

desnom tipkom miša kliknite ikonu **HP ProtectTools** u području obavijesti na desnom kraju programske trake, kliknite **Upravitelj zaštite privatnosti**, a zatim kliknite **Konfiguracija**

– ili –

na alatnoj traci poruke e-pošte programa Microsoft Outlook kliknite strelicu usmjerenu prema dolje pored postavke **Pošalji sigurno**, a zatim kliknite **Certifikati** ili **Pouzdani kontakti**

– ili –

na alatnoj traci dokumenta iz sustava Microsoft Office kliknite strelicu uz postavku **Potpis i šifriranje**, a zatim kliknite **Certifikati** ili **Pouzdani kontakti**

Upravljanje certifikatima za upravitelj zaštite privatnosti

Certifikati za upravitelj zaštite privatnosti štite podatke i poruke korištenjem tehnologije šifriranja koja se naziva Public key infrastructure (PKI). PKI zahtijeva da korisnici nabave šifre za šifriranje i certifikat za upravitelj zaštite privatnosti koji izdaju ovlaštena tijela za izdavanje certifikata. Za razliku od većine softvera za šifriranje i provjeru autentičnosti koji zahtijevaju povremenu provjeru autentičnosti, upravitelj zaštite privatnosti zahtijeva provjeru autentičnosti svaki put kada pomoću šifre za šifriranje potpišete poruku e-pošte ili dokument iz sustava Microsoft Office. Upravitelj zaštite privatnosti čini postupak spremanja i slanja važnih informacija sigurnim i zaštićenim.

Možete obavljati sljedeće zadatke:

- zatražiti i instalirati certifikat za upravitelj zaštite privatnosti
- prikazati detalje o certifikatu za upravitelj zaštite privatnosti
- obnoviti certifikat za upravitelj zaštite privatnosti
- kada je dostupno više certifikata, možete postaviti zadani certifikat za upravitelj zaštite privatnosti koji će koristiti upravitelj zaštite privatnosti
- izbrisati i opozvati certifikat za upravitelj zaštite privatnosti (napredno)

Traženje i instalacija certifikata za upravitelj zaštite privatnosti

Da biste mogli koristiti značajke upravitelj zaštite privatnosti, morate zatražiti i instalirati certifikat za upravitelj zaštite privatnosti (iz sučelja upravitelj zaštite privatnosti) koristeći valjanu adresu e-pošte. Adresa e-pošte mora biti postavljena kao račun unutar programa Microsoft Outlook na istom računalu s kojeg tražite certifikat za upravitelj zaštite privatnosti.

Traženje certifikata za upravitelj zaštite privatnosti

1. Otvorite upravitelj zaštite privatnosti i kliknite **Certifikati**.
2. Kliknite **Zatraži certifikat za upravitelj zaštite privatnosti**.
3. Na stranici dobrodošlice pročitajte tekst, a zatim kliknite **Dalje**.
4. Na stranici "Licencni ugovor" pročitajte licencni ugovor.
5. Svakako potvrdite okvir pored mogućnosti **Označite ovdje da biste prihvatili uvjete ovog licencnog ugovora**, a zatim kliknite **Dalje**.
6. Na stranici Pojedinosti vašeg certifikata unesite tražene informacije, a zatim kliknite **Dalje**.
7. Na stranici "Prihvaćen zahtjev za certifikatom" kliknite **Završi**.
8. Kliknite **U redu** da biste zatvorili certifikat.

Primit ćete poruku e-pošte u program Microsoft Outlook s priloženim certifikatom za upravitelj zaštite privatnosti.

Dobivanje unaprijed dodijeljenog certifikata za upravitelj zaštite privatnosti za tvrtke i ustanove

1. U programu Outlook otvorite primljenu poruku e-pošte kojom vas se obavještava da vam je unaprijed dodijeljen certifikat za tvrtku ili ustanovu.
2. Kliknite **Preuzmi**.
3. Primit ćete poruku e-pošte u program Microsoft Outlook s priloženim certifikatom za upravitelj zaštite privatnosti.
4. Da biste instalirali certifikat, pogledajte odjeljak Instalacija certifikata za upravitelj zaštite privatnosti na stranici 48

Instalacija certifikata za upravitelj zaštite privatnosti

1. Kada primite poruku e-pošte s priloženim certifikatom za upravitelj zaštite privatnosti, otvorite poruku i kliknite gumb **Postavljanje** u donjem desnom kutu poruke u programu Outlook 2007, odnosno u gornjem lijevom kutu u programu Outlook 2003.
2. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.
3. Na stranici Instaliran certifikat kliknite **Dalje**.
4. Na stranici Sigurnosna kopija certifikata unesite lokaciju i naziv datoteke sa sigurnosnom kopijom ili kliknite **Pregledaj** da biste potražili lokaciju.

   △ **OPREZ:** datoteku svakako spremite na lokaciju koja nije vaš tvrdi disk i spremite je na sigurno. Ta datoteka trebala bi biti samo za vašu upotrebu i potrebna je samo u slučaju da morate izvesti oporavak svojeg certifikata za upravitelj zaštite privatnosti i povezanih šifri.

5. Unesite i potvrdite lozinku, a zatim kliknite **Dalje**.

6. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

7. Ako želite započeti postupak pozivanja pouzdanog kontakta, slijedite upute na zaslonu koje počinju s drugim. korakom teme Dodavanje pouzdanih kontakata pomoću kontakata programa Microsoft Outlook na stranici 52

   – ili –

   ako kliknete **Odustani**, u odjeljku Dodavanje pouzdanog kontakta na stranici 51 potražite informacije o kasnijem dodavanju pouzdanog kontakta.

Pregledavanje pojedinosti certifikata za upravitelj zaštite privatnosti

1. Otvorite upravitelj zaštite privatnosti i kliknite **Certifikati**.
2. Kliknite certifikat za upravitelj zaštite privatnosti.
3. Kliknite **Pojedinosti o certifikatu**.
4. Kada dovršite pregledavanje pojedinosti, kliknite **U redu**.

Obnova certifikata za upravitelj zaštite privatnosti

Kada se bliži istek roka trajanja vašeg certifikata za upravitelj zaštite privatnosti, primit ćete obavijest da ga je potrebno obnoviti:

1. Otvorite upravitelj zaštite privatnosti i kliknite **Certifikati**.
2. Kliknite **Obnovi certifikat**.
3. Slijedite upute na zaslonu da biste kupili novi certifikat za upravitelj zaštite privatnosti.

NAPOMENA: postupak obnove certifikata za upravitelj zaštite privatnosti ne zamjenjuje vaš stari certifikat za upravitelj zaštite privatnosti. Morat ćete kupiti novi certifikat za upravitelj zaštite privatnosti i instalirati ga koristeći iste postupke kao u odjeljku Traženje i instalacija certifikata za upravitelj zaštite privatnosti na stranici 47.

Postavljanje zadanog certifikata za upravitelj zaštite privatnosti

Unutar upravitelj zaštite privatnosti vidljivi su samo certifikati za upravitelj zaštite privatnosti, čak i ako su na računalu instalirani dodatni certifikati drugih ovlaštenih tijela za izdavanje certifikata.

Ako je na računalu unutar upravitelj zaštite privatnosti instalirano više certifikata za upravitelj zaštite privatnosti, morate odrediti zadani certifikat:

1. Otvorite upravitelj zaštite privatnosti i kliknite **Certifikati**.
2. Kliknite certifikat za upravitelj zaštite privatnosti koji želite koristiti kao zadani, a zatim kliknite **Postavi kao zadano**.
3. Kliknite **U redu**.

NAPOMENA: ne morate koristiti zadani certifikat za upravitelj zaštite privatnosti. Unutar različitih funkcija upravitelj zaštite privatnosti možete odabrati bilo koji certifikat za upravitelj zaštite privatnosti koji želite koristiti.

Brisanje certifikata za upravitelj zaštite privatnosti

Ako izbrišete certifikat za upravitelj zaštite privatnosti, nećete moći otvoriti nijednu datoteku ni pregledati podatke koje ste šifrirali putem tog certifikata. Ako ste slučajno izbrisali certifikat za upravitelj zaštite privatnosti, možete ga obnoviti koristeći datoteku sa sigurnosnom kopijom koju ste stvorili prilikom instaliranja certifikata. Dodatne informacije potražite u odjeljku Vraćanje certifikata za upravitelj zaštite privatnosti na stranici 50.

Da biste izbrisali certifikat za upravitelj zaštite privatnosti:

1. Otvorite upravitelj zaštite privatnosti i kliknite **Certifikati**.
2. Kliknite certifikat za upravitelj zaštite privatnosti koji želite izbrisati, a zatim kliknite **Napredno**.
3. Kliknite **Izbriši**.
4. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.
5. Kliknite **Zatvori**, a zatim kliknite **Primijeni**.

Vraćanje certifikata za upravitelj zaštite privatnosti

Tijekom instalacije certifikata za upravitelj zaštite privatnosti od vas se traži da stvorite sigurnosnu kopiju certifikata. Sigurnosnu kopiju možete stvoriti i sa stranice Migracija. Tu sigurnosnu kopiju možete koristiti prilikom migracija s računala na računalo ili da biste vratili certifikat na isto računalo.

1. Otvorite upravitelj zaštite privatnosti i kliknite **Migracija**.
2. Kliknite **Vrati**.
3. Na stranici Migracijska datoteka kliknite **Pregledaj** da biste potražili datoteku .dppsm koju ste stvorili tijekom postupka stvaranja sigurnosne kopije, a zatim kliknite **Dalje**.
4. Unesite lozinku koju ste koristili kada ste stvarali sigurnosnu kopiju, a zatim kliknite **Dalje**.
5. Kliknite **Završi**.
6. Kliknite **U redu**.

Dodatne informacije potražite u odjeljku Instalacija certifikata za upravitelj zaštite privatnosti na stranici 48 ili Sigurnosno kopiranje certifikata za upravitelj zaštite privatnosti i pouzdanih kontakata na stranici 65.

Opoziv certifikata za upravitelj zaštite privatnosti

Ako smatrate da je sigurnost vašeg certifikata za upravitelj zaštite sigurnosti ugrožena, možete opozvati certifikat:

NAPOMENA: Prilikom opoziva certifikata za upravitelj zaštite sigurnosti, certifikat se ne briše. Certifikat je i dalje moguće koristiti za pregledavanje šifriranih datoteka.

1. Otvorite upravitelj zaštite privatnosti i kliknite **Certifikati**.
2. Kliknite **Napredno**.
3. Kliknite certifikat za upravitelj zaštite privatnosti koji želite opozvati, a zatim kliknite **Opozovi**.
4. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

5. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

6. Slijedite upute na zaslonu.

Upravljanje pouzdanim kontaktima

Pouzdani se kontakti korisnici s kojima ste razmijenili certifikate za upravitelj zaštite privatnosti koji vam omogućuju da međusobno komunicirate na siguran način.

Upravitelj pouzdanim kontaktima omogućuje vam da obavite sljedeće zadatke:

- pregledate pojedinosti pouzdanog kontakta
- izbrišete pouzdane kontakte
- provjerite status opoziva za pouzdane kontakte (napredno)

Dodavanje pouzdanih kontakata

Dodavanje pouzdanih kontakata postupak je u tri koraka:

1. Putem e-pošte šaljete poziv primatelju pouzdanog kontakta.

2. Primatelj pouzdanog kontakta odgovara putem e-pošte.

3. Putem e-pošte primate odgovor primatelja pouzdanog kontakta i kliknete **Prihvati**.

Putem e-pošte možete poslati pozive za pouzdane kontakte pojedinačnim primateljima ili možete poslati pozive svim kontaktima u svojem adresaru programa Microsoft Outlook.

Da biste dodali pouzdane kontakte, pogledajte sljedeće odjeljke.

NAPOMENA: da bi odgovorili na vaš poziv da postanu pouzdani kontakti, primatelji pouzdanog kontakta moraju na računalima imati instaliran upravitelj zaštite privatnosti ili zamjenski klijent. Informacije o instalaciji zamjenskog klijenta potražite na web-mjestu DigitalPersona na adresi http://DigitalPersona.com/PrivacyManager.

Dodavanje pouzdanog kontakta

1. Otvorite upravitelj zaštite privatnosti, zatim kliknite **Upravitelj pouzdanim kontaktima**, a potom kliknite **Pozovi kontakte**

   – ili –

   u programu Microsoft Outlook kliknite strelicu usmjerenu prema dolje pored postavke **Pošalji sigurno** na alatnoj traci, a zatim kliknite **Pozovi kontakte**.

2. Ako se otvori dijaloški okvir Odaberi certifikat, otvorite certifikat za upravitelj zaštite privatnosti koji želite koristiti, a zatim kliknite **U redu**.

3. Kada se otvori dijaloški okvir za pozivanje pouzdanog kontakta, pročitajte tekst i potom kliknite **U redu**.

   Automatski se stvara poruka e-pošte.

4. Unesite adresu e-pošte jednog ili više primatelja koje želite dodati kao pouzdane kontakte.

5. Uredite tekst i potpišite se (neobavezno).

6. Kliknite **Pošalji**.

NAPOMENA: ako niste pribavili certifikat za upravitelj zaštite privatnosti, poruka vas izvješćuje da morate imati certifikat za upravitelj zaštite privatnosti da biste slali zahtjeve za pouzdane kontakte. Kliknite **U redu** da biste pokrenuli čarobnjak za zahtjev za certifikatom. Dodatne informacije potražite u odjeljku Traženje i instalacija certifikata za upravitelj zaštite privatnosti na stranici 47.

7. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

NAPOMENA: kada primatelj koji je naveden u pouzdanim kontaktima primi poruku e-pošte, mora je otvoriti i u donjem desnom kutu kliknuti **Prihvati**, a nakon otvaranja dijaloškog okvira za potvrdu kliknuti **U redu**.

8. Kada primite odgovor na poruku e-pošte od primatelja koji prihvaća poziv da postane pouzdani kontakt, u donjem desnom kutu poruke kliknite **Prihvati**.

   Otvara se dijaloški okvir kojim se potvrđuje da je primatelj uspješno dodan na popis pouzdanih kontakata.

9. Kliknite **U redu**.

Dodavanje pouzdanih kontakata pomoću kontakata programa Microsoft Outlook

1. Otvorite upravitelj zaštite privatnosti, zatim kliknite **Upravitelj pouzdanim kontaktima**, a potom kliknite **Pozovi kontakte**

   – ili –

   u programu Microsoft Outlook kliknite strelicu usmjerenu prema dolje pored postavke **Pošalji sigurno** na alatnoj traci, a zatim kliknite **Pozovi sve moje kontakte iz programa Outlook**.

2. Kada se otvori stranica Pozivanje pouzdanih kontakata, odaberite adrese e-pošte primatelja koje želite dodati kao pouzdane kontakte, a zatim kliknite **Dalje**.

3. Kada se otvori stranica Slanje pozivnica, kliknite **Završi**.

   Automatski se stvara poruka e-pošte s popisom odabranih adresa e-pošte iz programa Microsoft Outlook.

4. Uredite tekst i potpišite se (neobavezno).

5. Kliknite **Pošalji**.

NAPOMENA: ako niste pribavili certifikat za upravitelj zaštite privatnosti, poruka vas izvješćuje da morate imati certifikat za upravitelj zaštite privatnosti da biste slali zahtjeve za pouzdane kontakte. Kliknite **U redu** da biste pokrenuli čarobnjak za zahtjev za certifikatom. Dodatne informacije potražite u odjeljku Traženje i instalacija certifikata za upravitelj zaštite privatnosti na stranici 47.

6. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

NAPOMENA: kada primatelj koji je naveden u pouzdanim kontaktima primi poruku e-pošte, mora je otvoriti i u donjem desnom kutu kliknuti **Prihvati**, a nakon otvaranja dijaloškog okvira za potvrdu kliknuti **U redu**.

7. Kada primite odgovor na poruku e-pošte od primatelja koji prihvaća poziv da postane pouzdani kontakt, u donjem desnom kutu poruke kliknite **Prihvati**.

Otvara se dijaloški okvir kojim se potvrđuje da je primatelj uspješno dodan na popis pouzdanih kontakata.

8. Kliknite **U redu**.

Pregledavanje pojedinosti pouzdanog kontakta

1. Otvorite upravitelj za zaštitu privatnosti i kliknite **Pouzdani kontakti**.
2. Kliknite pouzdani kontakt.
3. Kliknite **Pojedinosti o kontaktu**.
4. Kada dovršite pregledavanje pojedinosti, kliknite **U redu**.

Brisanje pouzdanog kontakta

1. Otvorite upravitelj za zaštitu privatnosti i kliknite **Pouzdani kontakti**.
2. Kliknite pouzdani kontakt koji želite izbrisati.
3. Kliknite **Izbriši kontakt**.
4. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

Provjera statusa opoziva pouzdanog kontakta

Da biste vidjeli je li pouzdani kontakt opozovao svoj certifikat za upravitelj zaštite privatnosti:

1. Otvorite upravitelj za zaštitu privatnosti i kliknite **Pouzdani kontakti**.
2. Kliknite pouzdani kontakt.
3. Kliknite gumb **Napredno**.

   Otvara se dijaloški okvir Napredno upravljanje pouzdanim kontaktima.
4. Kliknite **Provjeri opozivanje**.
5. Kliknite **Zatvori**.

Opće odredbe

Upravitelj zaštite privatnosti možete koristiti sa sljedećim Microsoftovim proizvodima:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Korištenje upravitelj zaštite privatnosti u programu Microsoft Outlook

Kada se instalira upravitelj zaštite privatnosti, na alatnoj traci programa Microsoft Outlook prikazuje se gumb Privatnost, a na alatnoj traci svake poruke e-pošte u programu Microsoft Outlook prikazuje se gumb Pošalji sigurno. Kad kliknete strelicu usmjerenu prema dolje uz postavku **Privatnosti** ili **Pošalji sigurno**, možete odabrati jednu od sljedećih mogućnosti:

- Sign and Send (Potpiši i pošalji) (samo gumb Send Securely – Pošalji sigurno) — ta mogućnost dodaje digitalni potpis u poruku e-pošte i šalje je nakon provjere autentičnosti pomoću odabranog načina sigurnosne prijave
- Seal for Trusted Contacts and Send (Zapečati za pouzdane kontakte i pošalji) (samo gumb Send Securely – Pošalji sigurno) — ta mogućnost u poruku e-pošte dodaje digitalni potpis, šifrira je i šalje nakon provjere autentičnosti pomoću odabranog načina sigurnosne prijave
- Pozovi kontakte — ta vam mogućnost omogućuje da pošaljete poziv za pouzdani kontakt. Dodatne informacije potražite u odjeljku Dodavanje pouzdanog kontakta na stranici 51.
- Pozovi kontakte programa Outlook — ta vam mogućnost omogućuje da poziv za pouzdani kontakt pošaljete svim kontaktima u adresaru programa Microsoft Outlook. Dodatne informacije potražite u odjeljku Dodavanje pouzdanih kontakata pomoću kontakata programa Microsoft Outlook na stranici 52.
- Otvorite softver upravitelj zaštite privatnosti — mogućnosti certifikata, pouzdanih kontakata i postavki dozvoljavaju vam otvaranje tog softvera radi dodavanja, pregleda ili promjene trenutnih postavki. Dodatne informacije potražite u odjeljku Konfiguriranje upravitelj zaštite privatnosti za program Microsoft Outlook na stranici 54.

Konfiguriranje upravitelj zaštite privatnosti za program Microsoft Outlook

1. Otvorite upravitelj zaštite privatnosti, kliknite **Postavke**, a zatim kliknite karticu **E-pošta**

   – ili –

   na glavnoj alatnoj traci programa Microsoft Outlook kliknite strelicu usmjerenu prema dolje pored postavke **Pošalji sigurno** (**Privatnost** u programu Outlook 2003), a zatim kliknite **Postavke**

   – ili –

   na alatnoj traci Microsoftove poruke e-pošte kliknite strelicu usmjerenu prema dolje uz postavku **Pošalji sigurno**, a zatim kliknite **Postavke**.

2. Odaberite akcije koje želite izvesti kada pošaljete zaštićenu poruku e-pošte, a zatim kliknite **U redu**.

Potpisivanje i slanje poruke e-pošte

1. U programu Microsoft Outlook kliknite **Novo** ili **Odgovori**.
2. Napišite poruku.
3. Kliknite strelicu usmjerenu prema dolje pored postavke **Pošalji sigurno** (**Privatnost** u programu Outlook 2003), a zatim kliknite **Potpiši i pošalji**.
4. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

Pečaćenje i slanje poruke e-pošte

Zapečaćene poruke e-pošte koje su digitalno potpisane i zapečaćene (šifrirane) mogu vidjeti samo ljudi koje odaberete sa svoga popisa pouzdanih kontakata.

Da biste zapečatili i poslali poruku e-pošte pouzdanom kontaktu:

1. U programu Microsoft Outlook kliknite **Novo** ili **Odgovori**.
2. Napišite poruku.
3. Kliknite strelicu za dolje pored **Pošalji sigurno** (**Privatnost** u programu Outlook 2003), a zatim kliknite **Zapečati za pouzdane kontakte i pošalji**.
4. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

Pregled zapečaćene poruke e-pošte

Kada otvarate zapečaćenu poruku e-pošte, u zaglavlju poruke prikazuje se sigurnosna oznaka. Sigurnosna oznaka pruža sljedeće informacije:

- koje su se vjerodajnice koristile za potvrđivanje identiteta osobe koja je potpisala poruku
- proizvod korišten za potvrdu vjerodajnica osobe koja je potpisala poruku

Korištenje upravitelj zaštite privatnosti u dokumentu sustava Microsoft Office 2007

NAPOMENA: upravitelj zaštite privatnosti može se koristiti samo u dokumentima sustava Microsoft Office 2007.

Kada instalirate certifikat za upravitelj zaštite privatnosti, s desne strane alatne trake svih dokumenata iz programa Microsoft Word, Microsoft Excel i Microsoft PowerPoint prikazuje se gumb Potpis i šifriranje. Kad kliknete strelicu prema dolje uz **Potpis i šifriranje**, možete odabrati jednu od sljedećih mogućnosti:

- Potpisivanje dokumenta — ova mogućnost u dokument dodaje vaš digitalni potpis.
- Dodavanje crte za potpis prije potpisivanja (samo u programima Microsoft Word i Microsoft Excel) — prema zadanim postavkama crta za potpis dodaje se pri potpisivanju ili šifriranju dokumenta iz programa Microsoft Word ii Microsoft Excel. Da biste isključili tu mogućnost, kliknite **Dodaj crtu za potpis** da biste uklonili kvačicu.
- Šifriranje dokumenta — ova mogućnost dodaje vaš digitalni potpis u dokument i šifrira ga.
- Uklanjanje šifriranja — ova mogućnost uklanja šifriranje iz dokumenta.
- Otvorite softver upravitelj zaštite privatnosti — mogućnosti certifikata, pouzdanih kontakata i postavki dozvoljavaju vam otvaranje tog softvera radi dodavanja, pregleda ili promjene trenutnih

postavki. Dodatne informacije potražite u odjeljcima Upravljanje certifikatima za upravitelj zaštite privatnosti na stranici 47, Upravljanje pouzdanim kontaktima na stranici 51 ili Konfiguriranje upravitelj zaštite privatnosti za sustav Microsoft Office na stranici 56.

Konfiguriranje upravitelj zaštite privatnosti za sustav Microsoft Office

1. Otvorite upravitelj zaštite privatnosti, kliknite **Postavke**, a zatim kliknite karticu **Dokumenti**.

   – ili –

   na alatnoj traci dokumenta sustava Microsoft Office, kliknite strelicu za dolje uz **Potpis i šifriranje**, a zatim kliknite **Postavke**.

2. Odaberite aktivnosti koje želite konfigurirati, a zatim kliknite **U redu**.

Potpisivanje dokumenta sustava Microsoft Office

1. Stvorite i spremite dokument u nekom od programa: Microsoft Word, Microsoft Excel ili Microsoft PowerPoint.
2. Kliknite strelicu za dolje uz **Potpis i šifriranje**, a zatim kliknite **Potpiši dokument**.
3. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.
4. Kada se otvori dijaloški okvir za potvrdu, pročitajte tekst i potom kliknite **U redu**.

Ako kasnije odlučite urediti taj dokument, učinite sljedeće:

1. Kliknite gumb **Office** u gornjem lijevom kutu zaslona.
2. Kliknite **Pripremi**, a zatim **Označi kao konačno**.
3. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da** i nastavite s radom.
4. Kad ste završili uređivanje, ponovno potpišite dokument.

Dodavanje crte za potpis pri potpisivanju dokumenta programa Microsoft Word ili Microsoft Excel

Upravitelj zaštite privatnosti omogućuje vam dodavanje crte za potpis kad potpisujete dokument programa Microsoft Word ili Microsoft Excel:

1. Stvorite i spremite dokument u nekom od programa: Microsoft Word ili Microsoft Excel
2. Kliknite izbornik **Polazno**.
3. Kliknite strelicu za dolje uz **Potpis i šifriranje**, a zatim kliknite **Dodaj crtu za potpis prije potpisivanja**.

   NAPOMENA: pri odabiru ove mogućnosti prikazuje se kvačica uz Dodaj crtu za potpis prije potpisivanja. Ta je mogućnost omogućena prema zadanim postavkama.

4. Kliknite strelicu za dolje uz **Potpis i šifriranje**, a zatim kliknite **Potpiši dokument**.
5. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

Dodavanje predloženih potpisnika u dokument programa Microsoft Word ili Microsoft Excel

U svoj dokument možete dodati više od jedne crte za potpis tako što ćete imenovati predložene potpisnike. Predloženi potpisnik korisnik je kojega je odabrao vlasnik dokumenta programa Microsoft Word ili Microsoft Excel da u dokument doda crtu za potpis. To možete biti vi ili neka druga osoba za koju želite da potpiše vaš dokument. Primjerice, ako pripremate dokument kojega moraju potpisati svi članovi vašega odjela, na dnu posljednje stranice morate u njega uključiti crte za potpis za te korisnike s uputom da se potpišu do određenog datuma.

Da biste dodali predložene potpisnike u dokument programa Microsoft Word ili Microsoft Excel:

1. Stvorite i spremite dokument u nekom od programa: Microsoft Word ili Microsoft Excel.
2. Kliknite izbornik **Umetanje**.
3. Na alatnoj traci, u grupi **Tekst** kliknite strelicu uz **Crta za potpis**, a zatim kliknite **Davatelj potpisa za upravitelj zaštite privatnosti**.

   Otvara se dijaloški okvir Postavljanje potpisa.
4. U tekstni okvir ispod mogućnosti **Predloženi potpisnik** unesite ime predloženog potpisnika.
5. U tekstni okvir ispod mogućnosti **Upute za potpisnika** unesite poruku za predloženog potpisnika.

NAPOMENA: ova će se poruka pojaviti na mjestu naslova, a ona se pri potpisivanju dokumenta ili briše ili zamjenjuje korisnikovom titulom.

6. Potvrdite okvir **Pokaži datum potpisivanja na crti za potpis** da biste prikazali datum.
7. Potvrdite okvir **Pokaži titulu potpisnika na crti za potpis** da biste prikazali titulu.

NAPOMENA: budući da vlasnik dokumenta dodjeljuje predložene potpisnike svome dokumentu, ako se ne potvrde okviri **Pokaži datum potpisivanja na crti za potpis** i/ili **Pokaži titulu potpisnika na crti za potpis**, predloženi potpisnik neće moći prikazati datum i/ili titulu na crti za potpis čak i ako su postavke njegovog dokumenta konfigurirane da to učini.

8. Kliknite **U redu**.

Dodavanje crte za potpis za predloženog potpisnika

Kad predloženi potpisnici otvore dokument, vidjet će svoje ime u zagradi, što ukazuje na to da se traži njihov potpis.

Da biste potpisali dokument:

1. Dvokliknite odgovarajuću crtu za potpis.
2. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

   Crta za potpis prikazat će se prema postavkama koje je odredio vlasnik dokumenta.

Šifriranje dokumenta sustava Microsoft Office

Dokument sustava Microsoft Office možete šifrirati za svoje potrebe i za svoje pouzdane kontakte. Kada šifrirate dokument i zatvorite ga, vi i vaši pouzdani kontakti koje odaberete s popisa morate potvrditi autentičnost prije nego što ga otvorite.

Da biste šifrirali dokument sustava Microsoft Office:

1. Stvorite i spremite dokument u nekom od programa: Microsoft Word, Microsoft Excel ili Microsoft PowerPoint.
2. Kliknite izbornik **Polazno**.
3. Kliknite strelicu za dolje uz **Potpis i šifriranje**, a zatim kliknite **Šifriraj dokument**.

   Otvara se dijaloški okvir Odabir pouzdanih kontakata.
4. Kliknite ime pouzdanog kontakta koji će moći otvoriti dokument i pregledati njegov sadržaj.

NAPOMENA: da biste odabrali više imena pouzdanih kontakata, držite pritisnutom tipku ctrl i kliknite pojedinačna imena.

5. Kliknite **U redu**.

Ako kasnije odlučite urediti taj dokument, slijedite postupke u odjeljku Uklanjanje šifriranja iz dokumenta sustava Microsoft Office na stranici 58. Kada se šifriranje ukloni, možete uređivati dokument. Slijedite korake u ovom odjeljku da biste ponovno šifrirali dokument.

Uklanjanje šifriranja iz dokumenta sustava Microsoft Office

Kad uklonite šifriranje iz dokumenta sustava Microsoft Office, od vas i vaših pouzdanih kontakata više se ne traži provjera autentičnosti prilikom otvaranja i prikazivanja sadržaja tog dokumenta.

Da biste uklonili šifriranje iz dokumenta sustava Microsoft Office:

1. Otvorite šifrirani dokument iz jednog od programa: Microsoft Word, Microsoft Excel ili Microsoft PowerPoint.
2. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.
3. Kliknite izbornik **Polazno**.
4. Kliknite strelicu dolje uz **Potpis i šifriranje**, a zatim kliknite **Ukloni šifriranje dokumenta**.

Slanje šifriranog dokumenta sustava Microsoft Office

Poruci e-pošte možete priložiti šifrirani dokument sustava Microsoft Office bez potpisivanja ili šifriranja same poruke. Da biste to učinili, stvorite i pošaljite poruku e-pošte s potpisanim ili šifriranim dokumentom isto kao što biste poslali običnu poruku e-pošte s privitkom.

Ako, međutim, želite li optimalnu sigurnost, kada poruci e-pošte dodajete potpisani ili šifrirani dokument sustava Microsoft Office, preporučuje se da šifrirate i samu poruku.

Da biste poslali zapečaćenu poruku e-pošte s potpisanim i/ili šifriranim dokumentom sustava Microsoft Office u privitku, slijedite ove korake:

1. U programu Microsoft Outlook kliknite **Novo** ili **Odgovori**.
2. Napišite poruku.
3. Priložite dokument sustava Microsoft Office.
4. Dodatne upute potražite u odjeljku Pečaćenje i slanje poruke e-pošte na stranici 55.

Prikaz potpisanog dokumenta sustava Microsoft Office

NAPOMENA: da biste prikazali potpisani dokument sustava Microsoft Office, ne morate imati certifikat upravitelj zaštite privatnosti.

Kada se otvori potpisani dokument sustava Microsoft Office, ikona digitalnog potpisa prikazuje se na statusnoj traci na dnu prozora dokumenta.

1. Kliknite ikonu **Digitalni potpisi** da biste uključili ili isključili dijaloški okvir Potpisi koji prikazuje imena svih korisnika koji su potpisali dokument i datume kada je svaki od njih to učinio.
2. Da biste vidjeli dodatne pojedinosti o svakom potpisu, desnom tipkom miša kliknite ime u dijaloškom okviru Potpisi i odaberite Pojedinosti o potpisu.

Prikaz šifriranog dokumenta sustava Microsoft Office

Da biste na drugom računalu prikazali šifrirani dokument sustava Microsoft Office, na tom računalu mora biti instaliran upravitelj zaštite privatnosti. Uz to, morate obnoviti certifikat za upravitelj zaštite privatnosti koji se koristio za šifriranje datoteke.

Pouzdani kontakt koji želi prikazati šifrirani dokument sustava Microsoft Office mora imati certifikat za upravitelj zaštite privatnosti, a na računalu mora biti instaliran upravitelj zaštite privatnosti. Uz to, vlasnik šifriranog dokumenta sustava Microsoft Office mora odabrati osobu koja je pouzdani kontakt.

Korištenje upravitelj zaštite privatnosti u programu Windows Live Messenger

Upravitelj zaštite privatnosti dodaje u program Windows Live Messenger sljedeće značajke sigurne komunikacije:

- **Siguran razgovor** — poruke se prenose putem protokola SSL/TLS (Secure Sockets Layer/ Transport Layer Security) putem XML-a, iste one tehnologije koja osigurava zaštićenost transakcija u e-trgovini.
- **Identifikacija primatelja** — možete potvrditi nazočnost i identitet osobe prije slanja poruke.
- **Potpisane poruke** — svoje poruke možete elektronski potpisati. Ako to učinite, kada primatelj primi poruke kojima se neovlašteno pristupalo, bit će mu označeno da nisu valjane.
- **Značajka sakrij/prikaži** — možete sakriti bilo koju ili sve poruke u prozoru razgovora upravitelj zaštite privatnosti. Možete i poslati poruku sa skrivenim sadržajem. Prije prikaza poruke potrebna je potvrda autentičnosti.
- **Sigurna povijest razgovora** — evidencije vaših sesija razgovora šifrirane su prije spremanja te je potrebna potvrda autentičnosti ako ih se želi pregledati.
- **Automatsko zaključavanje/otključavanje** — možete zaključati i otključati prozor za razgovore upravitelj zaštite privatnosti ili odrediti postavke automatskog zaključavanja nakon određenog perioda neaktivnosti.

Pokretanje sesije razgovora u upravitelju zaštite privatnosti

NAPOMENA: da biste koristili razgovor u upravitelju zaštite privatnosti, obje strane moraju imati instaliran upravitelj zaštite privatnosti i certifikat za njega. Pojedinosti o instaliranju certifikata upravitelj zaštite privatnosti potražite u odjeljku Traženje i instalacija certifikata za upravitelj zaštite privatnosti na stranici 47.

1. Da biste pokrenuli razgovor u upravitelju zaštite privatnosti u programu Windows Live Messenger, slijedite jedan od ovih postupaka:

   a. Desnim klikom miša označite jedan mrežni kontakt u programu Live Messenger, a zatim odaberite **Pokretanje aktivnosti**.

   b. Kliknite **Pokreni razgovor**.

   – ili –

   a. Dvokliknite mrežni kontakt u programu Live Messenger, a zatim kliknite izbornik **Prikaz popisa aktivnosti**.

   b. Kliknite **Akcija**, a zatim kliknite **Pokreni razgovor**.

   – ili –

   a. Desnom tipkom miša kliknite ikonu **ProtectTools** u području obavijesti, zatim kliknite **Upravitelj zaštite privatnosti za HP ProtectTools**, a potom odaberite **Pokreni razgovor**.

   b. U programu Live Messenger kliknite **Akcije: pokretanje aktivnosti**, a zatim odaberite **Razgovor u upravitelju zaštite privatnosti**.

   NAPOMENA: svaki korisnik programa Live Messenger mora biti na mreži i svaki od korisnika mora biti prikazani drugome na mrežnom prozoru programa Live Messenger. Kliknite da biste odabrali korisnika koji je na mreži.

   Upravitelj zaštite privatnosti šalje pozivnicu kontaktu da pokrene razgovor u upravitelju. Kada pozvani kontakt prihvati, otvara se prozor za razgovor u upravitelju zaštite privatnosti. Ako pozvani kontakt nema upravitelj zaštite privatnosti, dobit će obavijest da ga preuzme.

2. Kliknite **Start** da biste započeli siguran razgovor.

Konfiguriranje upravitelj zaštite privatnosti u programu Windows Live Messenger

1. U razgovoru u upravitelju zaštite privatnosti kliknite gumb **Postavke**

   – ili –

   u upravitelju zaštite privatnosti, kliknite **Postavke**, a zatim kliknite karticu **Razgovor**

   – ili –

   u pregledniku povijesti upravitelj zaštite privatnosti u programu live Messenger kliknite gumb **Postavke**.

2. Da biste naveli vremensko razdoblje tijekom kojeg razgovor u upravitelju zaštite privatnosti ostaje aktivan prije nego što se sesija zaključa, odaberite broj s popisa **Zaključaj sesiju nakon sljedećeg broja minuta neaktivnosti: _**.

3. Da biste naveli mapu povijesti svojih sesija razgovora, kliknite **Pregledavanje** da biste potražili mapu, a zatim kliknite **U redu**.

4. Da biste automatski šifrirali i spremili svoje sesije kada ih zatvorite, potvrdite okvir **Automatski spremi sigurnu povijest razgovora**.

5. Kliknite **U redu**.

Razgovor u prozoru upravitelj zaštite privatnosti

Nakon pokretanja razgovora u upravitelju zaštite privatnosti, u programu Windows Live Messenger otvara se prozor upravitelj zaštite privatnosti. Korištenje razgovora u upravitelju zaštite privatnosti slično je korištenju osnovnog programa Windows Live Messenger, osim sljedećih dodatnih značajki koje su dostupne u prozoru za razgovor upravitelj:

- **Spremi** – kliknite taj gumb da biste spremili sesiju razgovora u mapu koja je navedena u vašim postavkama konfiguracije. Razgovor u upravitelju zaštite privatnosti možete konfigurirati i tako da automatski sprema svaku sesiju nakon zatvaranja.
- **Sakrij sve** i **Prikaži sve** – kliknite odgovarajući gumb da biste proširili ili saželi poruke prikazane u prozoru Sigurna komunikacija. Klikom na zaglavlje poruke možete sakriti ili prikazati pojedinačne poruke.
- **Jesi li tu?** – kliknite taj gumb da biste od svog kontakta zatražili provjeru autentičnosti.
- **Lock** (Zaključaj) – kliknite taj gumb da biste zatvorili prozor za razgovor u softveru Privacy Manager (upravitelj zaštite privatnosti) te se vratili u prozor za unos razgovora. Da biste ponovno prikazali prozor Secure Communications (Sigurna komunikacija), kliknite **Resume the session** (Nastavi sesiju), a zatim potvrdite autentičnost pomoću odabrane metode sigurnosne prijave
- **Pošalji** – kliknite taj gumb da biste kontaktu poslali šifriranu poruku.
- **Pošalji potpisano** – potvrdite taj okvir da biste elektronički potpisali i šifrirali poruke. Ako to učinite, kada primatelj primi poruke kojima se neovlašteno pristupalo, bit će mu označeno da nisu valjane. Provjeru autentičnosti morate izvršiti pri slanju svake potpisane poruke.
- **Pošalji skriveno** – potvrdite taj okvir da biste šifrirali i poslali poruku u kojoj se prikazuje samo zaglavlje. Da bi pročitao sadržaj takve poruke, kontakt mora izvršiti provjeru autentičnosti.

Pregled povijesti razgovora

Razgovor u upravitelju zaštite privatnosti: preglednik povijesti programa Live Messenger prikazuje šifrirane datoteke sesija razgovora iz upravitelj zaštite privatnosti. Sesije možete spremiti tako da u prozoru za razgovor u upravitelju zaštite privatnosti kliknete **Spremi** ili da na kartici Razgovor u upravitelju za privatnost konfigurirate automatsko spremanje. Svaka sesija u pregledniku prikazuje (šifrirano) zaslonsko ime kontakta te datum i vrijeme početka i završetka sesije. Sesije se po zadanom prikazuju za sve postavljene račune e-pošte. Da biste odabrali prikaz samo određenih računa, koristite izbornik **Prikaži povijest za**.

Preglednik vam omogućuje da obavite sljedeće zadatke:

- Otkrivanje svih sesija na stranici 62
- Otkrivanje sesija za određeni račun na stranici 62
- Prikaz ID-ja sesije na stranici 62
- Prikaz sesije na stranici 63
- Traženje određenog teksta u sesijama na stranici 63

- Brisanje sesije na stranici 63
- Dodavanje ili uklanjanje stupaca na stranici 63
- Filtriranje prikazanih sesija na stranici 64

Da biste pokrenuli preglednik povijesti programa Live Messenger:

▲ U području obavijesti, sasvim desno na traci zadataka, desnom tipkom miša kliknite ikonu **HP ProtectTools**, kliknite **Upravitelj zaštite privatnosti: za HP ProtectTools**, a zatim kliknite **Preglednik povijesti programa Live Messenger**

– ili –

▲ u sesiji razgovora kliknite **Preglednik povijesti** ili **Povijest**.

Otkrivanje svih sesija

Otkrivanje svih sesija prikazuje dešifrirano zaslonsko ime kontakta za trenutno odabrane sesije i sve sesije na istome računu.

Da biste otkrili sve spremljene sesije povijesti razgovora:

1. U pregledniku povijesti programa Live Messenger desnom tipkom miša kliknite sesiju, a zatim odaberite **Otkrij sve sesije**.
2. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

   Dešifrirat će se zaslonska imena kontakata.
3. Dvokliknite sesiju da biste prikazali njezin sadržaj.

Otkrivanje sesija za određeni račun

Otkrivanje sesije prikazuje dešifrirano zaslonsko ime kontakta za trenutno odabranu sesiju.

Da biste otkrili određenu sesiju iz povijesti razgovora:

1. U pregledniku povijesti programa Live Messenger desnim klikom miša kliknite sesiju, a zatim odaberite **Otkrij sesiju**.
2. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

   Dešifrirat će se zaslonsko ime kontakta.
3. Dvokliknite otkrivenu sesiju da biste prikazali njezin sadržaj.

NAPOMENA: dodatne sesije šifrirane putem istog certifikata prikazat će nezaključanu ikonu koja naznačuje da ih možete prikazati dvostrukim klikom na svaku od njih bez dodatne provjere autentičnosti. Sesije šifrirane putem različitog certifikata prikazat će zaključanu ikonu koja naznačuje da je potrebna daljnja provjera autentičnosti tih sesija prije prikazivanja zaslonskih imena kontakata ili sadržaja.

Prikaz ID-ja sesije

Da biste prikazali ID sesije:

▲ u pregledniku povijesti programa Live Messenger, desnom tipkom miša kliknite otkrivenu sesiju, a zatim odaberite **Prikaz ID-a sesije**.

Prikaz sesije

Ova funkcija otvara datoteku za prikaz. Ako sesija još nije otkrivena (prikaz dešifriranog zaslonskog imena kontakta), ona se otkriva u isto vrijeme.

Da biste prikazali sesiju iz povijesti programa Live Messenger:

1. U pregledniku povijesti programa Live Messenger, desnom tipkom miša kliknite sesiju, a zatim odaberite **Prikaz**.
2. Ako sustav to zatraži, potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.

   Dešifrira se sadržaj sesije.

Traženje određenog teksta u sesijama

Tekst možete tražiti samo u otkrivenim (dešifriranim) sesijama koje su prikazane u prozoru preglednika. To su sesije kod kojih je zaslonsko ime kontakta prikazano običnim tekstom.

Da biste tražili tekst u sesijama iz povijesti razgovora:

1. U pregledniku povijesti programa Live Messenger kliknite gumb **Pretraži**.
2. Unesite tekst koji tražite, konfigurirajte sve željene parametre pretraživanja, a zatim kliknite **U redu**.

   Sesije koje sadrže taj tekst istaknute su u prozoru preglednika.

Brisanje sesije

1. Odaberite sesiju iz povijesti razgovora.
2. Kliknite **Izbriši**.

Dodavanje ili uklanjanje stupaca

U pregledniku povijesti programa Live Messenger prema zadanim postavkama prikazuju se tri najčešće korištena stupca. Možete dodati još stupaca u taj prikaz ili iz njega možete ukloniti stupce.

Da biste dodali stupce u prikaz:

1. Desnom tipkom miša kliknite zaglavlje tog stupca i onda odaberite **Dodaj/Ukloni stupce**.
2. Odaberite zaglavlje stupca na lijevoj ploči, a zatim kliknite **Dodaj** da biste ga premjestili na desnu ploču.

Da biste uklonili stupce iz prikaza:

1. Desnom tipkom miša kliknite zaglavlje tog stupca i onda odaberite **Dodaj/Ukloni stupce**.
2. Odaberite zaglavlje stupca na desnoj ploči, a zatim kliknite **Ukloni** da biste ga premjestili na lijevu ploču.

Filtriranje prikazanih sesija

Popis sesija za sve vaše račune prikazan je u pregledniku povijesti programa Live Messenger. Možete i filtrirati prikazane sesije tražeći sljedeće:

- određene račune. Pojedinosti potražite u odjeljku Prikazivanje sesija vezanih uz određeni račun na stranici 64
- raspon datuma. Pojedinosti potražite u odjeljku Prikazivanje sesija vezanih za neki raspon datuma na stranici 64
- razne datoteke. Pojedinosti potražite u odjeljku Prikazivanje sesija spremljenih u mapu koja nije zadana na stranici 64

Prikazivanje sesija vezanih uz određeni račun

▲ U pregledniku povijesti programa Live Messenger odaberite račun iz izbornika **Prikaži povijest za**.

Prikazivanje sesija vezanih za neki raspon datuma

1. U pregledniku povijesti programa live Messenger kliknite ikonu **Napredni filtar**.

   Otvara se dijaloški okvir za napredni filtar.

2. Potvrdite okvir **Prikaži samo sesije unutar određenog raspona datuma**.
3. U okvirima **Od datuma** i **Do datuma** unesite dan, mjesec i/ili godinu ili kliknite strelicu uz kalendar da biste odabrali datume.
4. Kliknite **U redu**.

Prikazivanje sesija spremljenih u mapu koja nije zadana

1. U pregledniku povijesti programa live Messenger kliknite ikonu **Napredni filtar**.
2. Potvrdite okvir **Koristi zamjensku mapu za povijesne datoteke**.
3. Unesite lokaciju mape ili kliknite **Pregledaj** da biste potražili mapu.
4. Kliknite **U redu**.

Napredni zadaci

Migriranje Privacy Manager Certificates (certifikati Upravitelja privatnosti) i Trusted Contacts (provjereni kontakti) na drugo računalo

Možete bez brige migrirati svoje certifikate za upravitelj zaštite privatnosti i pouzdane kontakte na drugo računalo ili stvoriti sigurnosne kopije svojih podataka radi njihovog čuvanja. Da biste to učinili, stvorite sigurnosne kopije podataka u obliku datoteke zaštićene lozinkom na nekoj mrežnoj lokaciji ili nekom prijenosnom uređaju za pohranu, a potom vratite tu datoteku na novo računalo.

Sigurnosno kopiranje certifikata za upravitelj zaštite privatnosti i pouzdanih kontakata

Da biste stvorili sigurnosne kopije svojih certifikata za upravitelj zaštite privatnosti i pouzdanih kontakata u datoteci zaštićenoj lozinkom, slijedite ove korake:

1. Otvorite upravitelj zaštite privatnosti i kliknite **Migracija**.
2. Kliknite **Izrada sigurnosne kopije**.
3. Na stranici Odabir podataka odaberite kategorije podataka koje želite uključiti u migracijsku datoteku, a zatim kliknite **Dalje**.
4. Na stranici Migracijska datoteka unesite naziv datoteke ili kliknite **Pregledaj** da biste potražili lokaciju, a zatim kliknite **Dalje**.
5. Unesite i potvrdite lozinku, a zatim kliknite **Dalje**.

NAPOMENA: pohranite tu lozinku na sigurno mjesto jer ćete je trebati radi vraćanja migracijske datoteke.

6. Potvrdite autentičnosti pomoću odabranog načina sigurnosne prijave.
7. Na stranici Migracijska datoteka spremljena kliknite **Završi**.

Vraćanje certifikata za upravitelj zaštite privatnosti i pouzdanih kontakata

Da biste vratili certifikate za upravitelj zaštite privatnosti i pouzdane kontakte na drugo računalo kao dio procesa migracije ili da biste ih vratili na isto računalo, slijedite ove korake:

1. Otvorite upravitelj zaštite privatnosti i kliknite **Migracija**.
2. Kliknite **Vrati**.
3. Na stranici Migracijska datoteka kliknite **Pregledaj** da biste potražili datoteku, a zatim kliknite **Dalje**.
4. Unesite lozinku koju ste koristili pri izradi datoteke sigurnosne kopije, a zatim kliknite **Dalje**.
5. Na stranici Migracijska datoteka kliknite **Završi**.

Centralno upravljanje upraviteljem zaštite privatnosti

Instalacija upravitelj zaštite privatnosti može biti dio centralizirane instalacije koju je prilagodio vaš administrator. Moguće je omogućiti ili onemogućiti jednu ili više sljedećih značajki:

- **Pravila korištenja certifikata** — korištenje certifikata za upravitelj zaštite privatnosti može vam biti ograničeno na one koje je izdala tvrtka Comodo ili vam može biti dopušteno korištenje digitalnih certifikata koje su izdali drugi ovlašteni izdavatelji.
- **Pravila šifriranja** — mogućnosti šifriranja mogu biti pojedinačno omogućene ili onemogućene u sustavu Microsoft Office ili programima Outlook i Windows Live Messenger.

10 File Sanitizer za HP ProtectTools

File Sanitizer alat je koji vam omogućuje sigurno uništavanje zapisa na vašem računalu (osobnih podataka ili datoteka, povijesnih ili web-datoteka te ostalih komponenti koje sadrže podatke) i povremeno čišćenje vašeg tvrdog diska.

NAPOMENA: ova verzija programa File Sanitizer podržava samo sistemski tvrdi disk.

Uništavanje

Uništavanje se razlikuje od standardnog brisanja koje je dio sustava Windows® (također poznato i kao jednostavno brisanje u programu File Sanitizer) po tome što kada pomoću ovog programa uništite neki zapis, poziva se algoritam koji zatamnjuje podatke, što svako eventualno vraćanje izvornih podataka čini praktički nemogućim. Jednostavno brisanje koje ima sustav Windows može ostaviti datoteku (ili zapis) na tvrdom disku nedirnutima ili u stanju gdje bi se za njihovo vraćanje uspješno mogle koristiti forenzičke metode.

Pri odabiru profila uništavanja (Visoka sigurnost, Srednja sigurnost ili Niska sigurnost), za uništavanje se automatski odabire prethodno definirani popis zapisa i metoda brisanja. Moguće je i prilagoditi profil uništavanja, što vam daje priliku da navedete broj ciklusa uništavanja, koje zapise uvrstiti za uništavanje, koje zapise potvrditi prije uništavanja, kao i koje ćete iz njega isključiti. Više informacija potražite u odjeljku Odabir ili stvaranje profila uništavanja na stranici 71

Možete postaviti raspored za automatsko uništavanje, a možete i ručno uništavati zapise kad god to želite. Više informacija potražite u odjeljku Postavljanje rasporeda uništavanja na stranici 70, Ručno uništavanje jednog zapisa na stranici 75 ili Ručno uništavanje svih odabranih stavki na stranici 75.

NAPOMENA: datoteke oblika .dll uništavaju se i uklanjaju sa sustava samo ako su premještene u koš za smeće.

Čišćenje praznog prostora

Brisanje zapisa u sustavu Windows ne uklanja sadržaj zapisa s vašeg tvrdog diska u potpunosti. Windows briše samo referencu na taj zapis. Sadržaj zapisa i dalje ostaje na tvrdom disku, sve do trenutka kada drugi zapis novim informacijama prebriše to isto područje na njemu.

Brisanje praznog prostora dopušta vam da bezbrižno pišete nasumične podatke preko izbrisanih zapisa i sprječava korisnike da vide izvorni sadržaj izbrisanog zapisa.

NAPOMENA: čišćenje praznog prostora namijenjeno je onim zapisima koje brišete koristeći koš za smeće sustava Widnows ili ručnom brisanju zapisa. Čišćenje praznog prostora ne pruža dodatnu sigurnost za uništene zapise.

Možete postaviti raspored automatskog čišćenja praznog prostora ili ga ručno aktivirati pomoću ikone **HP Protect Tools** u području obavijesti, na krajnje desnom dijelu programske trake. Više informacija potražite u odjeljku Postavljanje rasporeda čišćenja praznog prostora na stranici 71 ili Ručno pokretanje čišćenja praznog prostora na stranici 76.

Postupci postavljanja

Otvaranje programa File Sanitizer

Da bite otvorili program File Sanitizer:

1. Kliknite **Start**, a zatim **Svi programi**, kliknite **HP**, a zatim kliknite **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools)
2. Kliknite **File Sanitizer**

– ili –

- dvokliknite ikonu **File Sanitizer** koja se nalazi na radnoj površini

– ili –

- desnom tipkom miša kliknite ikonu **HP ProtectTools** u području obavijesti na desnom kraju programske trake, potom kliknite **File Sanitizer**, a zatim kliknite **Otvori File Sanitizer**.

Postavljanje rasporeda uništavanja

NAPOMENA: informacije o odabiru ili stvaranju unaprijed definiranog profila uništavanja potražite u odjeljku Odabir ili stvaranje profila uništavanja na stranici 71.

NAPOMENA: informacije o ručnom uništavanju zapisa potražite u odjeljku Ručno uništavanje jednog zapisa na stranici 75-.

1. Otvorite File Sanitizer te kliknite **Uništi**.
2. Odaberite opciju uništavanja:
   - **Isključivanje sustava Windows** — ovu mogućnost odaberite da biste uništili sve odabrane zapise kada se isključi sustav Windows.

     NAPOMENA: kada odaberete tu mogućnost, prilikom isključivanja računala prikazuje se dijaloški okvir s upitom želite li nastaviti s uništavanjem odabranih zapisa ili želite zaobići taj postupak. Kliknite **Da** da biste zaobišli postupak uništavanja ili **Ne** da biste ga nastavili.
   - **Otvaranje web-preglednika** — odaberite ovu mogućnost da biste sve odabrane web-zapise, kao što je povijest URL adresa iz preglednika, uništili prilikom otvaranja web-preglednika.
   - **Zatvaranje web-preglednika** — odaberite ovu mogućnost da biste sve odabrane web-zapise, kao što je povijest URL adresa iz preglednika, uništili prilikom zatvaranja web-preglednika.
   - **Slijed tipki** — ovu mogućnost odaberite ako želite započeti uništavanje pomoću slijeda tipki.
   - **Raspored** — potvrdite okvir **Aktiviraj raspored**, unesite svoju lozinku za sustav Windows, a zatim unesite dan i vrijeme kad želite uništiti odabrane zapise.

   NAPOMENA: datoteke oblika .dll uništavaju se i uklanjaju sa sustava samo ako su premještene u koš za smeće.
3. Kliknite **Primijeni**, a zatim kliknite **U redu**.

Postavljanje rasporeda čišćenja praznog prostora

NAPOMENA: čišćenje praznog prostora namijenjeno je onim zapisima koje brišete koristeći koš za smeće sustava Widnows ili ručnom brisanju zapisa. Čišćenje praznog prostora ne pruža dodatnu sigurnost za uništene zapise.

Postavljanje rasporeda čišćenja praznog prostora:

1. Otvorite File Sanitizer te kliknite **Čišćenje praznog prostora**.
2. Potvrdite okvir **Aktiviraj raspored**, unesite svoju lozinku za sustav Windows, a potom unesite dan i vrijeme kad želite očistiti tvrdi disk.
3. Kliknite **Primijeni**, a zatim kliknite **U redu**.

NAPOMENA: čišćenje praznog prostora može potrajati. Premda se čišćenje praznog prostora izvodi u pozadini, računalo može raditi sporije zbog povećane opterećenosti procesora.

Odabir ili stvaranje profila uništavanja

Odabirom prethodno definiranog profila ili stvaranjem vlastitog možete odrediti način brisanja te odabrati zapise za uništavanje.

Odabir prethodno definiranog profila uništavanja

Pri odabiru prethodno definiranog profila uništavanja (Visoka sigurnost, Srednja sigurnost ili Niska sigurnost), automatski se odabiru prethodno definirani način brisanja i popis zapisa. Možete kliknuti gumb **Pogledaj pojedinosti** da biste prikazali prethodno definirane liste zapisa odabranih za uništavanje.

Da biste odabrali prethodno definirani profil uništavanja:

1. Otvorite File Sanitizer te kliknite **Postavke**.
2. Kliknite prethodno definirani profil uništavanja.
3. Kliknite **Pregledaj pojedinosti** da biste pogledali popis zapisa odabranih za uništavanje.
4. U odjeljku **Uništi sljedeće**, prije uništavanja potvrdite okvir pokraj svakog zapisa koji želite uništiti.
5. Kliknite **Primijeni**, a zatim kliknite **U redu**.

Prilagodba profila uništavanja

Kada stvarate profil uništavanja, navedite broj ciklusa uništavanja, koje zapise uvrstiti za uništavanje, koje ćete zapise potvrditi prije uništavanja, kao i koje ćete iz njega isključiti:

1. Otvorite File Sanitizer, kliknite **Postavke**, zatim kliknite **Napredne sigurnosne postavke**, a potom **Pogledaj pojedinosti**.
2. Navedite broj ciklusa uništavanja.

NAPOMENA: odabrani broj ciklusa uništavanja izvršit će se za svaki zapis. Primjerice, ako odaberete tri ciklusa uništavanja, algoritam koji zatamnjuje podatke izvršava se tri odvojena puta. Ako odaberete cikluse uništavanja više sigurnosti, uništavanje može trajati prilično dugo; međutim, što je veći broj ciklusa uništavanja koji odredite, manja je vjerojatnost da će podatke biti moguće vratiti.

3. Odaberite zapise koje želite uništiti:

   a. U odjeljku **Dostupne mogućnosti uništavanja** kliknite zapis, a zatim **Dodaj**.

   b. Da biste dodali prilagođeni zapis, kliknite **Dodaj prilagođenu mogućnost**, a zatim pronađite ili upišite put do naziva datoteke ili mape. Kliknite **Otvori**, a zatim kliknite **U redu**. U odjeljku **Dostupne mogućnosti uništavanja** kliknite prilagođeni zapis, a zatim **Dodaj**.

NAPOMENA: da biste neki zapis uklonili iz dostupnih mogućnosti uništavanja, kliknite ga, a zatim kliknite **Izbriši**.

4. U odjeljku **Uništi sljedeće**, prije uništavanja potvrdite okvir pored svakog zapisa koji želite uništiti.

NAPOMENA: da biste neki zapis uklonili s popisa za uništavanje, kliknite ga, a zatim kliknite **Ukloni**.

5. Da biste zaštitili datoteke ili mape od automatskog uništavanja, u odjeljku **Nemoj uništiti sljedeće**, kliknite **Dodaj**, a zatim pronađite ili upišite put do naziva datoteke ili mape. Kliknite **Otvori**, a zatim kliknite **U redu**.

NAPOMENA: da biste neki zapis uklonili s popisa za izuzimanja, kliknite ga, a zatim kliknite **Izbriši**.

6. Kada završite konfiguriranje profila uništavanja, kliknite **Primijeni**, a zatim **U redu**.

Prilagodba profila jednostavnog brisanja

Profil jednostavno brisanje na uobičajen način briše zapise bez uništavanja. Prilikom prilagođavanja profila jednostavnog brisanja određujete koje zapise treba uključiti za jednostavno brisanje, koje treba potvrditi prije uništavanja te koji će biti izuzeti od jednostavnog brisanja.

NAPOMENA: ako koristite mogućnost jednostavnog brisanja, čišćenje praznog prostora može se povremeno obavljati na zapisima koji su izbrisani ručno ili uz pomoć koša za smeće u sustavu Windows.

Da biste prilagodili profil jednostavnog brisanja, učinite sljedeće:

1. Otvorite File Sanitizer, kliknite **Postavke**, zatim kliknite **Postavljanje jednostavnog brisanja**, a potom **Pogledaj pojedinosti**.

2. Odaberite zapise koje želite izbrisati:

   a. U odjeljku **Dostupne mogućnosti brisanja** kliknite zapis, a zatim **Dodaj**.

   b. Da biste dodali prilagođeni zapis, kliknite **Dodaj prilagođenu mogućnost**, unesite naziv datoteke ili mape, a zatim kliknite **U redu**. Kliknite prilagođeni zapis, a potom **Dodaj**.

NAPOMENA: da biste neki zapis izbrisali iz dostupnih mogućnosti brisanja, kliknite ga, a zatim kliknite **Izbriši**.

3. U odjeljku **Izbriši sljedeće**, prije uništavanja odaberite potvrdni okvir pokraj svakog zapisa koji želite izbrisati.

NAPOMENA: da biste neki zapis uklonili s popisa za brisanje, kliknite ga, a zatim kliknite **Ukloni**.

4. U odjeljku **Nemoj izbrisati sljedeće**, kliknite **Dodaj** da biste odabrali zapise koje želite izuzeti od uništavanja.

NAPOMENA: da biste neki zapis uklonili s popisa za izuzimane, kliknite ga, a zatim kliknite **Izbriši**.

5. Kada završite konfiguriranje profila jednostavnog brisanja, kliknite **Primijeni**, a zatim **U redu**.

Opće odredbe

File Sanitizer možete koristiti za obavljanje sljedećih zadataka:

- pokretanje uništavanja pomoću slijeda tipki — pomoću ove značajke možete kreirati slijed tipki (primjerice, ctrl+alt+s) za pokretanje uništavanja. Pojedinosti potražite u odjeljku Korištenje slijeda tipki pri pokretanju uništavanja na stranici 74.
- pokretanje uništavanja koristeći File Sanitizer — ova značajka nalikuje značajci "povuci i ispusti" operacijskog sustava Windows. Pojedinosti potražite u odjeljku Korištenje ikone programa File Sanitizer na stranici 75.
- ručno uništavanje pojedinih ili svih odabranih zapisa — pomoću ove značajke možete ručno uništiti stavke, a da pri tome ne morate čekati pokretanje zakazanog uništavanja. Pojedinosti potražite u odjeljcima Ručno uništavanje jednog zapisa na stranici 75 ili Ručno uništavanje svih odabranih stavki na stranici 75.
- ručno pokretanje čišćenja praznog prostora — korištenjem ove značajke možete ručno aktivirati čišćenje praznog prostora. Pojedinosti potražite u odjeljku Ručno pokretanje čišćenja praznog prostora na stranici 76.
- prekidanje uništavanja ili čišćenja praznog prostora — ova značajka dopušta zaustavljanje uništavanja ili čišćenja praznog prostora. Pojedinosti potražite u odjeljku Prekidanje uništavanja ili čišćenja praznog prostora na stranici 76.
- prikaz datoteka zapisnika — pomoću ove značajke možete prikazati datoteke zapisnika uništavanja ili čišćenja praznog prostora koje sadrže pogreške ili neuspjehe zabilježene prilikom zadnjeg uništavanja ili čišćenja praznog prostora. Pojedinosti potražite u odjeljku Pregled datoteka zapisnika na stranici 76.

NAPOMENA: uništavanje i čišćenje praznog prostora dugo traju. Iako se uništavanje i čišćenje praznog prostora izvode u pozadini, računalo može raditi sporije zbog povećane opterećenosti procesora.

Korištenje slijeda tipki pri pokretanju uništavanja

Ovo su koraci za određivanje slijeda tipki:

1. Otvorite File Sanitizer te kliknite **Uništi**.
2. Potvrdite okvir **Slijed tipki**.
3. Unesite znak u tekstni okvir.
4. Potvrdite okvir za **CTRL** ili **ALT**, a zatim **SHIFT**.

   Da biste, primjerice, uništavanje pokretali pomoću tipki s i ctrl+shift, u tekstni okvir unesite `s`, a zatim potvrdite okvire **CTRL** i **SHIFT**.

NAPOMENA: provjerite razlikuje li se slijed tipki koji ste odabrali od prethodno konfiguriranih.

Pokretanje uništavanja pomoću slijeda tipki:

1. Dok pritišćete odabrani znak, držite pritisnute tipke shift i ctrl ili tipku alt (odnosno kombinaciju koju ste naveli).
2. Ako se otvori dijaloški okvir za potvrdu, kliknite **Da**.

Korištenje ikone programa File Sanitizer

△ **OPREZ:** uništeni zapisi ne mogu se oporaviti. Pažljivo birajte stavke za ručno uništavanje.

1. Pronađite dokument ili mapu koju želite uništiti.
2. Dovucite zapis do ikone programa **File Sanitizer** na radnoj površini.
3. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

Ručno uništavanje jednog zapisa

△ **OPREZ:** uništeni zapisi ne mogu se oporaviti. Pažljivo birajte stavke za ručno uništavanje.

1. Desnom tipkom miša kliknite ikonu **HP ProtectTools** u području obavijesti na desnom kraju programske trake, kliknite **File Sanitizer**, a zatim kliknite **Uništi jedan**.
2. Kada se otvori dijaloški okvir, potražite zapis koji želite uništiti, a potom kliknite **U redu**.

   NAPOMENA: zapis koji odaberete može biti samo jedna datoteka ili mapa.

3. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

– ili –

1. Desnom tipkom miša kliknite ikonu **File Sanitizer** na radnoj površini, a zatim kliknite **Uništi jedan**.
2. Kada se otvori dijaloški okvir, potražite zapis koji želite uništiti, a potom kliknite **U redu**.
3. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

– ili –

1. Otvorite File Sanitizer te kliknite **Uništi**.
2. Kliknite gumb **Pregledaj**.
3. Kada se otvori dijaloški okvir, potražite zapis koji želite uništiti, a potom kliknite **U redu**.
4. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

Ručno uništavanje svih odabranih stavki

1. Desnom tipkom miša kliknite ikonu **HP ProtectTools** u području obavijesti na desnom kraju programske trake, kliknite **File Sanitizer**, a zatim kliknite **Uništi odmah**.
2. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

– ili –

1. Desnom tipkom miša kliknite ikonu **File Sanitizer** na radnoj površini, a zatim kliknite **Uništi odmah**.
2. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

– ili –

1. Otvorite File Sanitizer te kliknite **Uništi**.
2. Kliknite gumb **Uništi odmah**.
3. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

Ručno pokretanje čišćenja praznog prostora

1. Desnom tipkom miša kliknite ikonu **HP ProtectTools** u području obavijesti na desnom kraju programske trake, kliknite **File Sanitizer**, a zatim kliknite **Očisti odmah**.
2. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

– ili –

1. Otvorite File Sanitizer te kliknite **Čišćenje praznog prostora**.
2. Kliknite **Očisti odmah**.
3. Kada se otvori dijaloški okvir za potvrdu, kliknite **Da**.

Prekidanje uništavanja ili čišćenja praznog prostora

Tijekom uništavanja ili čišćenja praznog prostora u području obavijesti iznad ikone softvera HP ProtectTools Security Manager (upravitelj za sigurnost sustava HP ProtectTools) pojavit će se poruka. Poruka sadrži pojedinosti o postupku uništavanja ili čišćenja praznog prostora (postotak dovršenosti) te vam omogućuje prekidanja postupka.

Da biste prekinuli postupak:

▲ kliknite poruku, a zatim kliknite **Zaustavi** da biste odustali od postupka.

Pregled datoteka zapisnika

Prilikom svakog uništavanja ili čišćenja praznog prostora stvaraju se datoteke zapisnika svih pogrešaka ili neuspjeha. Datoteke zapisnika uvijek se ažuriraju tako da sadrže podatke o zadnjem postupku uništavanja ili čišćenja praznog prostora.

NAPOMENA: datoteke koje su uspješno uništene ili očišćene ne pojavljuju se u datotekama zapisnika.

Jedna datoteka zapisnika stvara se za postupak uništavanja, a druga za postupak čišćenja praznog prostora. Obje datoteke zapisnika spremaju se na tvrdi disk u sljedeće mape:

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

11 Device Access Manager za HP ProtectTools (samo odabrani modeli)

Device Access Manager (upravitelj pristupa uređajima) za HP ProtectTools administratorima sustava Windows omogućuje kontrolu nad pristupom uređajima i sprječavanje neovlaštenog pristupa na sljedeće načine:

- za svakoga korisnika stvara se profil uređaja koji određuje kojim je uređajima korisniku dopušten, a kojim uskraćen pristup
- stvaraju se grupe korisnika, kao što je unaprijed definirana grupe administratora uređaja, ili se grupe mogu definirati pomoću mogućnosti Upravljanje računalom u odjeljku Administrativni alati upravljačke ploče
- pristup uređaju može biti dopušten ili uskraćen ovisno o pripadnosti pojednoj grupi
- pristup čitanja i pristup pisanja mogu se zasebno dopustiti ili uskratiti za uređaje poput CD-ROM i DVD pogona

Korisnici s ograničenim pristupom također mogu dobiti dopuštenje za čitanje i mijenjanje pravila kontrole pristupa uređaju.

Postupci pri postavljanju

Otvaranje upravitelj pristupa uređajima

Da biste otvorili upravitelj pristupa uređajima, slijedite ove korake:

1. Kliknite **Start**, zatim **Svi programi**, a potom kliknite **HP** pa kliknite **Konzola za administraciju sustava HP ProtectTools**.
2. U lijevom oknu kliknite **Upravitelj pristupa uređajima**.

Konfiguriranje pristupa uređajima

Upravitelj pristupa uređajima za HP ProtectTools pruža tri vrste prikaza:

- prikaz za jednostavnu konfiguraciju koristi se za dopuštanje ili uskraćivanje pristupa klasama uređaja za članove grupe administratora uređaja
- prikaz za konfiguraciju klase uređaja koristi se za dopuštanje ili uskraćivanje pristupa vrstama uređaja ili pojednim uređajima za pojedinačne korisnike ili grupe
- pomoću treće vrste prikaza, prikaza za postavke pristupa korisnika, određuju se korisnici koji mogu mijenjati podatke jednostavne konfiguracije i konfiguracije klase uređaja

Grupa administratora uređaja

Grupa administratora uređaja stvara se pri instalaciji upravitelj pristupa uređajima.

Administrator sustava može putem uskraćivanja pristupa skupini klasa uređaja primijeniti pravilo kontrole pristupa uređaju ako korisnik, s obzirom na pristup uređaju, nije pouzdan. Preporučeni način razlikovanja pouzdanih i nepouzdanih korisnika uključivanje je pouzdanih korisnika u skupinu administratora uređaja. Odobravanje pristupa uređajima članovima skupine administratora uređaja putem korištenja prikaza za jednostavnu konfiguraciju ili prikaza za konfiguraciju klasa uređaja svim će pouzdanim korisnicima osigurati puni pristup pojedinoj skupini klasa uređaja.

NAPOMENA: dodavanje korisnika u grupu administratora uređaja ne omogućuje automatski pristup uređajima. Međutim, prikaz za jednostavnu konfiguraciju može se koristiti za odobravanje pristupa potrebnoj skupini klasa uređaja za pouzdane korisnike.

Da biste u grupu administratora uređaja dodali novog korisnika, slijedite ove korake:

- u sustavima Windows 7, Vista ili XP Professional koristite standardni MMC dodatak "Lokalni korisnici i grupe".
- u verzijama Home sustava Windows 7, Vista® ili XP, s ovlaštenog računa, unesite sljedeće u naredbeni redak:

```
c:\> net localgroup “Device Administrators” username /ADD
```

Jednostavna konfiguracija

Administratori i ovlašteni korisnici mogu koristiti prikaz za jednostavnu konfiguraciju da bi promijenili pristup sljedećim klasama uređaja za sve one koji nisu administratori sustava:

NAPOMENA: da bi mogli koristiti ovaj prikaz za čitanje podataka o pristupu uređaju, korisniku ili grupi mora biti odobren pristup za "čitanje" u prikazu **Postavke pristupa korisnika**. Da bi mogli koristiti ovaj prikaz za mijenjanje podataka o pristupu uređaju, korisniku ili grupi mora biti odobren pristup za "mijenjanje" u prikazu **Postavke pristupa korisnika**.

- svim prijenosnim medijima (disketama, USB izbrisivim memorijskim pogonima i sl.)
- svim DVD/CD-ROM pogonima
- svim serijskim i paralelnim priključcima
- svim Bluetooth® uređajima
- svim infracrvenim uređajima
- svim modemskim uređajima
- svim PCMCIA uređajima
- svim 1394 uređajima

Da biste dopustili ili uskratili pristup klasi uređaja svima koji nisu administratori uređaja, učinite sljedeće:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Jednostavna konfiguracija**.
2. Da biste uskratili pristup određenoj klasi uređaja ili pojedinom uređaju, u desnom oknu potvrdite okvir pored klase ili uređaja. Poništite potvrdni okvir da biste dopustili pristup pojedinom uređaju ili klasi uređaja.

   Ako je potvrdni okvir sive boje, vrijednosti koje utječu na scenarij pristupa promijenjene su pomoću prikaza za konfiguraciju klase uređaja. Da biste vrijednosti ponovno postavili na jednostavne postavke, kliknite potvrdni okvir da biste ga potvrdili ili poništili, a zatim za potvrdu kliknite **Da**.
3. Kliknite ikonu **Spremi**.

   NAPOMENA: ako nije pokrenut pozadinski servis, otvara se dijaloški okvir pomoću kojeg ga možete pokrenuti ako želite. Kliknite **Da**.
4. Kliknite **U redu**.

Pokretanje pozadinskog servisa

Prije nego li je moguće primijeniti profile uređaja, pomoću upravitelj za sigurnost sustava HP ProtectTools pokreće se dijaloški okvir u kojemu možete pokrenuti pozadinski servis Zaključavanje/kontrola uređaja sustava HP ProtectTools. Kliknite **Da**. Pokreće se pozadinski servis te će se svaki puta prilikom pokretanja sustava automatski pokrenuti.

NAPOMENA: profil uređaja mora se odrediti prije prikazivanja upita za pokretanje pozadinskog servisa.

Servis mogu pokrenuti ili zaustaviti i administratori:

1. Kliknite **Start**, a zatim **Upravljačka ploča**.
2. Kliknite **Administrativni alati**, a zatim kliknite **Usluge**.
3. Potražite servis **Zaključavanje/kontrola uređaja sustava HP ProtectTools**.

Zaustavljanje usluge servisa Zaključavanja/kontrole uređaja ne zaustavlja zaključavanje uređaja. Dvije komponente nameću zaključavanje uređaja:

- usluga servis zaključavanja/kontrole uređaja
- upravljački program DAMDrv.sys

Pokretanje uređaja pokreće upravljački program uređaja, ali zaustavljanje servisa ne zaustavlja upravljački program.

Da biste utvrdili radi li pozadinski servis, otvorite naredbeni redak, a zatim upišite sc query flcdlock.

Da biste utvrdili je li pokrenut upravljački program uređaja, otvorite naredbeni redak, a zatim utipkajte sc query damdrv.

Konfiguracija klase uređaja

Administratori i autorizirani korisnici mogu pregledavati i mijenjati popis korisnika i grupa kojima je dopušten ili uskraćen pristup klasama uređaja ili pojedinim uređajima.

NAPOMENA: da bi mogli koristiti ovaj prikaz za čitanje podataka o pristupu uređaju, korisniku ili grupi mora biti odobren pristup za "čitanje" u prikazu **Postavke pristupa korisnika**. Da bi mogli koristiti ovaj prikaz za mijenjanje podataka o pristupu uređaju, korisniku ili grupi mora biti odobren pristup za "mijenjanje" u prikazu **Postavke pristupa korisnika**.

Prikaz za konfiguraciju klase uređaja ima sljedeće odjeljke:

- **Popis uređaja** — prikazuje sve klase uređaja prethodno ili trenutno instalirane u sustavu.
  - Zaštita se obično primjenjuje na klasu uređaja. Odabrani korisnik ili grupa moći će pristupiti bilo kojem uređaju u klasi uređaja.
  - Zaštita se može primijeniti i na pojedinačni uređaj.
- **Popis korisnika** — prikazuje sve korisnike ili grupe kojima je dopušten ili uskraćen pristup odabranim klasama uređaja ili pojedinačnim uređajima.
  - Stavka na popisu korisnika može se odnositi na pojedinačnog korisnika ili grupu u kojoj je korisnik.
  - Ako na popisu korisnika nije dostupan korisnik ili grupa, postavka je naslijeđena od klase uređaja na popisu uređaja ili iz mape Klasa.
  - Neke klase uređaja, poput DVD i CD-ROM pogona, mogu se dodatno kontrolirati odvojenim dopuštanjem ili uskraćivanjem pristupa za postupke čitanja ili pisanja.

    Kao i za druge uređaje i klase, prava pristupa za čitanje i pisanje mogu se naslijediti. Primjerice, pristup za čitanje može se naslijediti od više klase, ali pristup za pisanje može biti izričito uskraćen korisniku ili grupi.

    NAPOMENA: ako je potvrdni okvir čitanja prazan, tada unos kontrole pristupa ne utječe na pristup za čitanje pojedinom uređaju. To ni ne dopušta niti uskraćuje pristup za čitanje pojedinom uređaju.

    1. primjer — ako je korisniku ili grupi uskraćen pristup za pisanje nekom uređaju ili klasi uređaja:

    tom korisniku, grupi ili članu te grupe moguće je dopustiti pristup za pisanje ili pristup za čitanje +pisanje samo za uređaj koji je u hijerarhiji uređaja niže od ovog uređaja.

2. primjer — ako je korisniku ili grupi dopušten pristup za pisanje nekom uređaju ili klasi uređaja:

tom korisniku, grupi ili članu te grupe moguće je uskratiti pristup za pisanje ili pristup za čitanje +pisanje samo za isti uređaj ili uređaj koji je hijerarhijski niže od ovog uređaja.

3. primjer — ako je korisniku ili grupi dopušten pristup za čitanje nekom uređaju ili klasi uređaja:

tom korisniku, grupi ili članu te grupe moguće je uskratiti pristup za čitanje ili pristup za čitanje +pisanje samo za isti uređaj ili uređaj koji je hijerarhijski niže od ovog uređaja.

4. primjer — ako je korisniku ili grupi uskraćen pristup za čitanje nekom uređaju ili klasi uređaja:

taj korisnik, grupa ili član te grupe mogu dobiti pravo čitanja ili čitanja i pisanja samo za uređaj koji je hijerarhijski niže od tog uređaja.

5. primjer — ako je korisniku ili grupi dopušten pristup za čitanje+pisanje nekom uređaju ili klasi uređaja:

tom korisniku, grupi ili članu te grupe moguće je uskratiti pristup za pisanje ili pristup za čitanje +pisanje samo za isti uređaj ili uređaj koji je hijerarhijski niže od ovog uređaja.

6. primjer — ako je korisniku ili grupi uskraćen pristup za čitanje+pisanje nekom uređaju ili klasi uređaja:

tom korisniku, grupi ili članu te grupe moguće je dopustiti pristup za čitanje ili pristup za čitanje +pisanje samo za uređaj koji je hijerarhijski niže od ovog uređaja.

Uskraćivanje pristupa korisniku ili grupi

Da biste korisniku ili grupi spriječili pristup uređaju ili klasi uređaja, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Konfiguracija klase uređaja**.
2. Na popisu uređaja kliknite klasu uređaja koju želite konfigurirati.
   - Klasa uređaja
   - Svi uređaji
   - Pojedini uređaj
3. U odjeljku **Korisnik/grupe** kliknite korisnika ili grupu kojoj će pristup biti uskraćen.
4. Kliknite **Uskrati** pored korisnika ili grupe.
5. Kliknite ikonu **Spremi**.

NAPOMENA: kada su postavke uskrati i dopusti za korisnika postavljene na istoj razini uređaja, uskraćivanje pristupa ima prednost ispred dopuštanja pristupa.

Dopuštanje pristupa korisniku ili grupi

Da biste korisniku ili grupi dopustili pristup uređaju ili klasi uređaja, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Konfiguracija klase uređaja**.
2. Na popisu uređaja, kliknite sljedeće:
   - Klasa uređaja
   - Svi uređaji
   - Pojedini uređaj
3. Kliknite **Dodaj**.

   Otvara se dijaloški okvir **Odabir korisnika ili grupe**.
4. Kliknite **Napredno**, a zatim kliknite **Pronađi odmah** da biste pronašli i dodali korisnike ili grupe.
5. Kliknite korisnika ili grupu koje želite dodati na popis dostupnih korisnika ili skupina, a zatim kliknite **U redu**.
6. Ponovno kliknite **U redu**.
7. Kliknite **Dopusti** da biste korisniku ili grupi omogućili pristup.
8. Kliknite ikonu **Spremi**.

Uklanjanje pristupa korisniku ili grupi

Da biste uklonili pristup uređaju ili klasi uređaja za korisnika ili grupu, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Konfiguracija klase uređaja**.
2. Na popisu uređaja kliknite klasu uređaja koju želite konfigurirati.
   - Klasa uređaja
   - Svi uređaji
   - Pojedini uređaj
3. U odjeljku **Korisnik/grupe** kliknite korisnika ili grupu koju želite ukloniti, a zatim kliknite **Ukloni**.
4. Kliknite ikonu **Spremi**.

Dopuštanje pristupa klasi uređaja jednom korisniku ili grupi

Da biste jednom korisniku dopustili pristup klasi uređaja dok istovremeno uskraćujete pristup svim drugim članovima iste grupe, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Konfiguracija klase uređaja**.
2. Na popisu uređaja kliknite klasu uređaja koju želite konfigurirati.
   - Klasa uređaja
   - Svi uređaji
   - Pojedini uređaj
3. U odjeljku **Korisnik/grupe** odaberite skupinu kojoj želite uskratiti pristup, a zatim kliknite **Uskrati**.
4. Pronađite mapu ispod željene klase pa dodajte određenog korisnika.
5. Kliknite **Dopusti** da biste tom korisniku dodijelili pristup.
6. Kliknite ikonu **Spremi**.

Dopuštanje pristupa pojedinom uređaju jednom korisniku ili grupi

Administratori mogu korisniku odobriti pristup pojedinom uređaju uskraćujući istovremeno pristup svim drugim članovima iste grupe za sve uređaje u klasi:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Konfiguracija klase uređaja**.
2. Na popisu uređaja kliknite klasu uređaja koju želite konfigurirati, a zatim idite do mape ispod nje.
3. Kliknite **Dodaj**. Otvara se dijaloški okvir **Odabir korisnika ili grupe**.
4. Kliknite **Napredno**, a zatim **Pronađi odmah** da biste pronašli grupu korisnika kojoj će biti uskraćen pristup svim uređajima u klasi.
5. Odaberite grupu i kliknite **U redu**.
6. Idite do uređaja unutar klase uređaja kojem će korisniku biti dopušten pristup.
7. Kliknite **Dodaj**. Otvara se dijaloški okvir **Odabir korisnika ili grupe**.
8. Kliknite **Napredno**, a zatim kliknite **Pronađi odmah** da biste pronašli i dodali korisnike ili grupe.
9. Kliknite korisnika kojemu želite dopustiti pristup, a zatim kliknite **U redu**.
10. Kliknite **Dopusti** da biste tom korisniku dodijelili pristup.
11. Kliknite ikonu **Spremi**.

Ponovno postavljanje konfiguracije

△ **OPREZ:** ponovno postavljanje konfiguracije odbacuje sve dotadašnje promjene konfiguracije uređaja te vraća sve postavke na tvornički postavljene vrijednosti.

Da biste postavke konfiguracije vratili na tvornički postavljene vrijednosti, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Konfiguracija klase uređaja**.
2. Kliknite gumb **Ponovno postavi**.
3. Za potvrdu kliknite **Da**.
4. Kliknite ikonu **Spremi**.

Dodatni zadaci

Kontrola pristupa postavkama konfiguracije

U prikazu **Postavke pristupa korisnika**, administratori određuju koje grupe ili korisnici imaju pristup stranicama za jednostavnu konfiguraciju i za konfiguraciju klase uređaja.

NAPOMENA: korisnik ili grupa moraju imati "puna korisnička administratorska prava" da bi mijenjali postavke u prikazu Postavke pristupa korisnika.

- Korisnik ili grupa moraju imati pristup "Pogledaj postavke konfiguracije (samo za čitanje)" u prikazu za postavke pristupa korisnika da bi mogli pregledavati podatke o jednostavnoj konfiguraciji i konfiguraciji klase uređaja.
- Korisnik ili grupa moraju imati pristup "Promjena postavki konfiguracije" u prikazu za postavke pristupa korisnika da bi mogli pregledavati podatke o jednostavnoj konfiguraciji i konfiguraciji klase uređaja.

NAPOMENA: čak i članovi grupe administratora moraju imati pristup "za čitanje" da bi pregledavali prikaz za jednostavnu i konfiguraciju klase uređaja te pristup "za mijenjanje" da bi mogli mijenjati podatke koristeći prikaz za jednostavnu i konfiguraciju klase uređaja.

NAPOMENA: nakon procjene pristupnih razina za sve korisnike i grupe, ako za korisnika na određenoj razini pristupa nije postavljena ni mogućnost Dopusti niti Uskrati, korisniku je na toj razini uskraćen pristup.

Dopuštanje pristupa postojećoj grupi ili korisniku

Da biste postojećoj grupi ili korisniku dodijelili dopuštenje za prikaz ili promjenu postavki konfiguracije, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Postavke pristupa korisnika**.
2. Odaberite grupu ili korisnika kojima ćete dopustiti pristup.
3. U odjeljku **Dopuštenja** kliknite **Dopusti** za svaku vrstu dopuštenja koje dajete odabranoj grupi ili korisniku:

   NAPOMENA: dodijeljena su dopuštenja kumulativna. Primjerice, korisniku kojemu je dodijeljeno dopuštenje “Promijeni postavke konfiguracije”, automatski se dodjeljuje i dopuštenje “Pregledaj postavke konfiguracije (samo za čitanje)”. Korisniku kojemu su dodijeljena “puna korisnička administratorska prava" dodijeljena su i dopuštenja “Promijeni postavke konfiguracije” i “Pogledaj postavke konfiguracije (samo za čitanje)”.

   - puna korisnička administratorska prava
   - promijeni postavke konfiguracije
   - pogledaj postavke konfiguracije (samo za čitanje)
4. Kliknite ikonu **Spremi**.

Uskraćivanje pristupa postojećoj grupi ili korisniku

Da biste postojećoj grupi ili korisniku uskratili dopuštenje za pregled ili promjenu postavki konfiguracije, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Postavke pristupa korisnika**.
2. Odaberite grupu ili korisnika kojima će biti dopušten pristup.
3. U odjeljku **Dopuštenja** kliknite **Uskrati** za svaku vrstu dopuštenja koju želite uskratiti pojedinom korisniku ili grupi:
   - puna korisnička administratorska prava
   - promijeni postavke konfiguracije
   - pogledaj postavke konfiguracije (samo za čitanje)
4. Kliknite ikonu **Spremi**.

Dodavanje nove grupe ili korisnika

Da biste novoj grupi ili korisniku dodijelili dopuštenje za pregled ili promjenu postavki konfiguracije, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Postavke pristupa korisnika**.
2. Kliknite **Dodaj**. Otvara se dijaloški okvir **Odabir korisnika ili grupe**.
3. Kliknite **Napredno**, a zatim kliknite **Pronađi odmah** da biste pronašli i dodali korisnike ili grupe.
4. Kliknite grupu ili korisnika, kliknite **U redu**, a zatim ponovno **U redu**.
5. Kliknite **Dopusti** da biste tom korisniku dodijelili pristup.
6. Kliknite ikonu **Spremi**.

Uklanjanje grupe ili korisnika

Da biste uklonili dopuštenje grupi ili korisniku za pregled ili promjenu postavki konfiguracije, slijedite ove korake:

1. U lijevom oknu **konzole za administraciju sustava HP ProtectTools** kliknite **Upravitelj pristupa uređajima**, a zatim **Postavke pristupa korisnika**.
2. Odaberite grupu, a zatim kliknite **Ukloni**.
3. Kliknite ikonu **Spremi**.

Srodna dokumentacija

Upravitelj pristupa uređajima za HP ProtectTools kompatibilan je s poslovnim proizvodom Upravitelj pristupa uređajima za tvrtke sustava HP ProtectTools. U kombinaciji s poslovnim proizvodom, upravitelj pristupa uređajima za HP ProtectTools omogućuje svojim značajkama pristup samo za čitanje.

Dodatne informacije o Upravitelju pristupa uređajima za HP ProtectTools dostupne su na web-mjestu http://www.hp.com/hps/security/products.

12 LoJack Pro za HP ProtectTools

Serija proizvoda tvrtke Absolute Software sa značajkom Computrace korisnicima omogućuje praćenje njihovih HP računala i bolju zaštitu podataka. Proizvodi Computrace LoJack uz to smanjuju i broj izgubljenih računala te olakšavaju pronalaženje ukradenih.

Da biste aktivirali proizvod Computrace, učinite sljedeće:

1. Kliknite **Start**, zatim **Svi programi**, a potom **HP ProtectTools Security Manager** (Upravitelj za sigurnost sustava HP ProtectTools).
2. Kliknite **Theft Recovery** (Vraćanje ukradenog), a zatim kliknite **Activate Now** (Aktiviraj sada).

   Zadani web-preglednik otvorit će web-stranicu pretplate na kojoj možete odabrati i kupiti jedan od tri proizvoda Computrace dostupnih za sustav HP ProtectTools:

   - **Computrace Data Delete** (Brisanje podataka Computrace) – obuhvaća daljinsko brisanje podataka, zamrzavanje uređaja te osnovno praćenje računala i izvješćivanje.
   - **Computrace LoJack Pro** – obuhvaća daljinsko brisanje podataka, zamrzavanje uređaja, osnovno praćenje računala i izvješćivanje te kontrolirano vraćanje ukradenog računala.
   - **Computrace LoJack Pro Premium** – obuhvaća daljinsko brisanje podataka, zamrzavanje uređaja, osnovno praćenje računala i izvješća, zemljopisno lociranje i ograničavanje zemljopisnog područja te kontrolirano vraćanje ukradenog računala.

Computrace Agent ugrađuje se u BIOS HP-ovih poslovnih prijenosnika, ali se isključuje prilikom otpreme računala. Kada kupite pretplatu, Agent se može aktivirati. Ugrađeni agent može ponovno instalirati operacijski sustav te preformatirati tvrde diskove.

NAPOMENA: Pretplata je moguća na razdoblje od jedne do pet godina. Dodatne pojedinosti potražite u ugovoru za pretplatu s tvrtkom Absolute Software. Funkcioniranje značajke vraćanja ukradenog računala ovisi o zemljopisnom položaju. GPS praćenje podržano je na određenim modelima sa značajkom bežične mreže širokog područja (WWAN).

13 Rješavanje problema

Upravitelj za sigurnost sustava HP ProtectTools

Kratki opis	Pojedinosti	Rješenje
Pametne kartice i USB tokeni nisu dostupni u softveru Security Manager (upravitelj za sigurnost) ako su instalirani nakon softvera Security Manager.	Da biste u softveru Security Manager (upravitelj za sigurnost) koristili pametne kartice i USB tokene, prije instalacije softvera Security Manager (upravitelj za sigurnost) morate instalirati softvere koji ih podržavaju (upravljačke programe, PKCS#11 davatelje itd.). Ako već imate instaliran program Upravitelj za sigurnost, nakon instalacije pametne kartice ili tokena učinite sljedeće korake:	Prijavite se u program Upravitelj lozinki U Upravitelju za sigurnost sustava HP ProtectTools kliknite **Upravitelj lozinki**, kliknite **Vjerodajnice**, a zatim kliknite **Pametna kartica** Ako računalo to zatraži, ponovo ga pokrenite.
Neke web-stranice aplikacije uzrokuju pogreške koje korisnika sprječavaju u izvođenju ili dovršavanju zadataka.	Neke aplikacije temeljene na webu prestaju funkcionirati i izvještavaju o pogreškama zbog onemogućenja obrasca funkcija značajke Single Sign On (Jedinstvena prijava). Na primjer, u Internet Exploreru pojavljuje se **!** unutar žutog trokuta. Ovaj simbol znači da je došlo do pogreške.	Značajka Single Sign On (jedinstvena prijava) upravitelj za sigurnost ne podržava sva softverska web-sučelja. Onemogućite podršku za Single Sign On (jedinstvena prijava) za pojedinu web-stranicu isključivanjem podrške za Single Sign On (jedinstvena prijava). Pogledajte punu dokumentaciju o značajki Single Sign On (jedinstvena prijava) dostupnu u datotekama za pomoć Upravitelja za sigurnost. Ako se određena značajka Single Sign On (Jedna prijava) za danu aplikaciju ne može onemogućiti, obratite se tehničkoj podršci tvrtke HP i zatražite podršku treće razine putem svog servisnog kontakta tvrtke HP.
Mogućnost **Browse for Virtual Token** (Traži virtualni token) tijekom postupka prijave nije prikazana.	Korisnik ne može pomaknuti položaj registriranog virtualnog tokena u Upravitelju lozinki jer je mogućnost pregledavanja uklonjena radi smanjivanja sigurnosnih rizika.	Mogućnost pregledavanja uklonjena je jer je osobama koje nisu korisnici omogućivala brisanje i promjenu naziva datoteka te preuzimanje nadzora nad sustavom Windows.
Administratori domene ne mogu promijeniti lozinku sustava Windows čak ni uz autorizaciju.	To se događa nakon što se administrator domene prijavi na domeni i registrira identitet domene pomoću Upravitelja lozinki, koristeći račun s administratorskim pravima na domeni i lokalno računalo. Kada administrator domene pokuša promijenili lozinku sustava Windows iz Upravitelja lozinki, prima poruku o pogrešci zbog neuspjele prijave: **Ograničenje korisničkog računa**.	Upravitelj lozinki ne može promijeniti lozinku korisnika domene pomoću funkcije **Promjena lozinke sustava Windows**, Security Manager (Upravitelj za sigurnost) može promijeniti samo lozinke za račune na lokalnom računalu. Korisnik domene može promijeniti svoju lozinku putem mogućnosti **Promjena lozinke** u odjeljku **Sigurnost sustava Windows**, no budući da korisnik domene nema fizički račun na lokalnom računalu, Upravitelj lozinki može promijeniti samo lozinku koja se koristi za prijavu.

Kratki opis	Pojedinosti	Rješenje
Postoje problemi u kompatibilnosti između Upravitelja lozinki i lozinke GINA u programu Corel WordPerfect 12.	Ako se korisnik prijavi u Upravitelj lozinki, stvori dokument u programu WordPerfect i spremi ga uz zaštitu lozinkom, Upravitelj lozinki neće moći otkriti ili prepoznati lozinku GINA, bilo ručno ili automatski.	HP traži rješenje kako bi u budućnosti poboljšao proizvod.
Upravitelj lozinki ne prepoznaje gumb **Poveži se** na zaslonu.	Ako su Single Sign On (Jedinstvena prijava) vjerodajnice za Remote Desktop Connection (RDP) prilikom ponovnog pokretanja značajke Single Sign On (Jedinstvena prijava) postavljene na **Connect (Poveži)**, umjesto **Connect (Poveži)** uvijek se unosi **Save As (Spremi kao)**.	HP traži rješenje kako bi u budućnosti poboljšao proizvod.
Nakon prelaska iz stanja čekanja u hibernaciju u sustavu Windows XP Service Pack 1 korisnik se ne može prijaviti u Password Manager (Upravitelj lozinki).	Kada sustav prijeđe prijeđe u hibernaciju i stanje mirovanja, administrator ili korisnik ne može se prijaviti u Upravitelj lozinki, a zaslon za prijavu u sustav Windows prikazuje se bez obzira na odabranu vjerodajnicu za prijavu (lozinka, otisak prsta ili Java kartica).	Ažurirajte Windows na Service Pack 2 putem značajke Windows Update. Dodatne informacije o uzroku problema pronaći ćete u članku 813301 baze znanja tvrtke Microsoft na adresi http://www.microsoft.com. Da bi se mogao prijaviti, korisnik mora odabrati Upravitelj lozinki i prijaviti se u njega. Nakon prijave u Upravitelj lozinki, od korisnika se traži da se prijavi u sustav Windows (korisnik će možda trebati odabrati mogućnost prijave u sustav Windows) da bi dovršio postupak prijave. Ako se korisnik najprije prijavi u sustav Windows, morat će se ručno prijaviti u Upravitelj lozinki.
Sigurnosti postupak **Restore Identity (Vraćanje identiteta)** gubi vezu s virtualnim tokenom.	Nakon što korisnik obnovi svoj identitet, Upravitelj lozinki može izgubiti vezu s lokacijom virtualnog tokena na zaslonu za prijavu. Čak i ako je Upravitelj lozinki registrirao virtualni token, korisnik će morati registrirati token da bi obnovio vezu.	Ovo je trenutno zadana postavka. Prilikom deinstalacije softvera Security Manager (Upravitelj za sigurnost) bez zadržavanja identiteta, dio tokena koji se odnosi na sustav (poslužitelj) bit će uništen i token se više ne može koristiti za prijavu, čak ni ako se dio tokena koji se odnosi na klijentsko računalo obnovi kroz obnavljanje identiteta. HP istražuje dugoročne mogućnosti rješenja problema.

Upravitelj pristupa uređajima za HP ProtectTools

Korisnicima je uskraćen pristup uređajima u Upravitelju pristupa uređajima, ali se uređajima i dalje može pristupati.

- **Objašnjenje** — za zabranu korisnicima da pristupaju uređajima u Upravitelju pristupa uređajima korištena je jednostavna konfiguracija i/ili konfiguracija klase uređaja. Iako im je pristup zabranjen, korisnici i dalje mogu pristupati uređajima.
- **Rješenje:**
  - provjerite je li pokrenuta značajka HP ProtectTools Device Locking
  - kao korisnik-administrator, kliknite **Upravljačka ploča**, a zatim kliknite **Sustav i održavanje**. U prozoru Administrativni alati kliknite **Servisi** i potražite servis **Zaključavanje/kontrola uređaja za HP ProtectTools**. Provjerite je li servis pokrenut i je li vrsta pokretanja **Automatsko**

Korisnik neočekivano ima pristup uređaju ili mu je pristup uređaju neočekivano zabranjen.

- **Objašnjenje** — Upravitelj pristupa uređajima korišten je za zabranu pristupanja korisnika nekim uređajima i dopuštanje pristupanja korisnika drugim uređajima. Kada korisnik radi u sustavu, može pristupati uređajima za koje je mislio da mu je pristup njima zabranjen u Upravitelju pristupa uređajima, a ne može pristupiti uređajima za koje smatra da bi mu Upravitelj pristupa uređajima trebao dopustiti pristup.
- **Rješenje:**
  - pomoću konfiguracije klase uređaja u Upravitelju pristupa uređajima provjerite postavke korisnika za uređaj
  - kliknite **Security Manager** (Upravitelj za sigurnost), kliknite **Upravitelj pristupa uređajima**, a zatim kliknite **Konfiguracija klase uređaja**. Proširite razine u hijerarhiji klase uređaja i pregledajte postavke koje se odnose na tog korisnika. Provjerite nije li za korisnika ili za bilo koju grupu sustava Windows koje je korisnik možda član, npr. Korisnici ili Administratori, postavljeno dopuštenje "Uskrati"

Dopuštanje ili uskraćivanje - što ima prednost?

- **Objašnjenje** — u konfiguraciji klase uređaja postavljena je sljedeće konfiguracija:
  - grupi sustava Windows (npr. BUILTIN\Administratori) dodijeljeno je dopuštenje Dopusti, a drugoj grupi sustava Windows (npr. BUILTIN\Korisnici) dodijeljeno je dopuštenje Uskrati na istoj razini u hijerarhiji klasa uređaja (npr. DVD/CD-ROM pogoni)
  - ako je korisnik član obiju tih grupa (npr. administrator), koje dopuštenje ima prednost?
- **Rješenje:**
  - korisniku je zabranjen pristup uređaju. Uskraćivanje ima prednost nad dopuštanjem
  - pristup je zabranjen zbog načina na koji sustav Windows rukovodi postojećim dopuštenjima za uređaje. Jednoj je grupi pristup zabranjen, a drugoj dopušten, ali korisnik je član obiju grupa. Korisniku će pristup biti zabranjen jer uskraćivanje pristupa ima prednost nad dopuštanjem pristupa

- jedno je rješenje uskraćivanje pristupa grupi Korisnici na razini DVD/CD-ROM pogona i dopuštanje pristupa grupi Administratori na razinama nižim od razine DVD/CD-ROM pogona
- alternativno je rješenje stvaranje posebnih grupa u sustavu Windows, jedne za omogućivanje pristupa DVD/CD pogonima, a druge za uskraćivanje pristupa DVD/CD pogonima. Određeni se korisnici nakon toga mogu dodati u odgovarajuću grupu

Prikaz jednostavne konfiguracije korišten je za definiranje pravila kontrole pristupanja uređajima, ali korisnici-administratori ne mogu pristupati uređajima.

- **Objašnjenje** — jednostavna konfiguracija uskraćuje pristup grupama Korisnici i Gosti, a dopušta ga grupi Administratori uređaja.
- **Rješenje:** korisnika-administratora dodajte u grupu Administratori uređaja.

Razno

Utjecaj softvera – kratki opis	Pojedinosti	Rješenje
Program Security Manager – primljeno upozorenje: **Sigurnosna aplikacija nije mogla biti instalirana dok se ne instalira HP Protect Tools Security Manager (Upravitelj sigurnosti)**.	Sve sigurnosne aplikacije, kao zaštita Java karticom ili biometrija, proširivi su dodaci za sučelje softvera Security Manager (Upravitelj za sigurnost). Prije učitavanja sigurnosnog dodatka koji je odobrio HP mora se instalirati softver Security Manager (Upravitelj za sigurnost).	Program Security Manager (Upravitelj sigurnosti) mora biti instaliran prije instaliranja bilo kakvog sigurnosnog dodatka.
HP ProtectTools Security Manager - povremeno se prilikom zatvaranja sučelja programa Security Manager (Upravitelj sigurnosti) javlja pogreška.	Povremeno se (u jednom od dvanaest slučajeva) koristeći gumb u gornjem desnom kutu zaslona za zatvaranje programa Security Manager (Upravitelj sigurnosti) pojavljuje pogreška prije dovršetka učitavanja svih aplikacija dodataka.	To je povezano s vremenom učitavanja servisa dodataka prilikom zatvaranja i ponovnog pokretanja programa Security Manager (Upravitelj sigurnosti). Budući je PTHOST.exe ljuska drugih aplikacija (dodataka), ovisi o mogućnosti dovršavanja učitavanja dodatka (servisi). Glavni je uzrok zatvaranje ljuske prije dovršenog učitavanja dodatka. Programu Security Manager (Upravitelj sigurnosti) dozvolite da dovrši poruku učitavanja servisa (prikazanu na vrhu prozora programa Security Manager) i svih dodataka navedenih u lijevom stupcu. Da biste izbjegli pogrešku, pričekajte neko vrijeme da se ti dodaci učitaju.
HP ProtectTools - neograničeni pristup ili nekontrolirane ovlasti administratora mogu predstavljati sigurnosnu opasnost.	Kod neograničenog pristupa računalu klijentu moguće su brojne opasnosti, uključujući i sljedeće: • brisanje PSD-a • zlonamjerne promjene korisničkih postavki • onemogućivanje sigurnosnih pravila i funkcija	Administratore se potiče da slijede "najbolje postupke" u ograničavanju ovlasti krajnjih korisnika i ograničavanju pristupa korisnicima. Neovlaštenim korisnicima ne bi trebalo dodjeljivati administrativne ovlasti.

Rječnik

administrator Pogledajte: administrator sustava Windows.

administrator sustava Windows Korisnik s punim pravima za izmjenu dopuštenja i upravljanje ostalim korisnicima.

aktivacija Zadatak koji se treba izvršiti da bi se moglo pristupati funkcijama šifriranja pogona. Šifriranje pogona aktivira se pomoću čarobnjaka za postavljanje sustava HP ProtectTools. Šifriranje pogona može aktivirati samo administrator. Postupak aktivacije sastoji se od aktiviranja softvera, šifriranja pogona, stvaranja korisničkog računa i stvaranja početnog ključa za šifriranje sigurnosne kopije na prijenosnom uređaju za pohranu.

arhiva za hitni oporavak Zaštićeno područje za pohranu koje omogućuje ponovno šifriranje osnovnih ključeva korisnika od vlasnika jedne platforme vlasniku druge.

ATM Automatski tehnološki upravitelj (Automatic Technology Manager) koji administratorima mreže omogućuje daljinsko upravljanje sustavima na BIOS razini.

automatsko uništavanje Planirano uništavanje koje korisnik postavlja u programu File Sanitizer.

biometrijski Kategorija provjere autentičnosti vjerodajnica koja rabi fizičku osobinu poput otiska prsta za identificiranje korisnika.

certifikat za upravitelj zaštite privatnosti Digitalni certifikat koji zahtijeva provjeru autentičnosti svaki put kada ga rabite za kriptografske postupke poput potpisivanja i šifriranja poruka e-pošte i dokumenata sustava Microsoft Office.

ciklus uništavanja Broj koliko se puta izvršava algoritam uništavanja nad svakim zapisom. Što je veći odabrani broj ciklusa uništavanja, to je računalo sigurnije.

crta za potpis Mjesto za vizualni prikaz digitalnog potpisa. Nakon potpisivanja dokumenta prikazuju se ime potpisnika i način provjere. Mogu se uključiti i datum te titula potpisnika.

čišćenje praznog prostora Sigurno pisanje nasumičnih podataka preko izbrisanih sredstava da bi se izobličio sadržaj izbrisanog zapisa.

davatelj usluga šifriranja (CSP) Davatelj ili biblioteka kriptografskih algoritama koji se mogu rabiti u dobro definiranom sučelju za provođenje određenih kriptografskih funkcija.

dešifriranje Postupak uporabe kriptografije za pretvaranje šifriranih podataka u običan tekst.

digitalni certifikat Elektroničke vjerodajnice koje potvrđuju identitet pojedinca ili tvrtke povezivanjem identiteta vlasnika digitalnog certifikata s parom elektroničkih ključeva koji se rabe za potpisivanje digitalnih informacija.

digitalni potpis Podaci koji se šalju uz datoteku za provjeru pošiljatelja materijala i za provjeru neizmijenjenosti datoteke nakon njezina potpisivanja.

domena Grupa računala koja je dio neke mreže i dijeli istu bazu podataka imenika. Domene imaju jedinstvena imena, a svaka ima skup zajedničkih pravila i postupaka.

DriveLock Sigurnosna značajka koja povezuje tvrdi disk s korisnikom te zahtijeva od korisnika da ispravno upiše lozinku za DriveLock pri pokretanju računala.

grupa Grupa korisnika s jednakom razinom pristupa ili zabrane pristupa klasi uređaja ili određenom uređaju.

gumb Potpis i šifriranje Softverski gumb koji se prikazuje na alatnoj traci aplikacija sustava Microsoft Office. Klik na ovaj gumb omogućuje potpisivanje, šifriranje ili uklanjanje šifriranja u dokumentu iz sustsava Microsoft Office.

gumb Zaštićeno slanje Softverski gumb koji se prikazuje na alatnoj traci poruka e-pošte programa Microsoft Outlook. Klik na ovaj gumb omogućuje potpisivanje i/ili šifriranje poruke e-pošte programa Microsoft Outlook.

HP SpareKey Sigurnosna kopija šifriranog ključa pogona.

identitet U softveru HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools), grupa vjerodajnica i postavki kojom se rukuje poput računa ili profila određenog korisnika.

ID kartica Programčić na bočnoj traci sustava Windows koji služi za vizualnu identifikaciju radne površine pomoću vašeg korisničkog imena i odabrane slike. Kliknite na ID karticu da biste otvorili Konzolu za administraciju sustava HP ProtectTools.

Java kartica Uklonjiva kartica koja se umeće u računalo. Ona sadrži identifikacijske informacije za prijavu. Prijavljivanje s Java karticom na zaslonu za prijavu za šifriranje pogona zahtijeva umetanje Java kartice i upisivanje korisničkog imena i PIN-a Java kartice.

jedinstvena prijava Značajka koja pohranjuje informacije o provjeri autentičnosti omogućuje korištenje softvera Security Manager (Upravitelj za sigurnost) za pristupanje internetu i aplikacijama sustava Windows koje zahtijevaju potvrdu autentičnosti lozinkom.

jednostavno brisanje Brisanje reference sustava Windows za neki zapis. Sadržaj zapisa ostaje na tvrdom disku dok se preko njega zapisuju zakriveni podaci "čišćenjem" slobodnog prostora.

klasa uređaja Svi uređaji određene vrste, poput pogona.

konzola Središnje mjesto s kojeg možete pristupati značajkama i postavkama konzole za administraciju sustava HP ProtectTools i njima upravljati.

korisnički račun u sustavu Windows Profil za pojedinca ovlaštenog za prijavljivanje na mrežu ili na pojedinačno računalo.

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

migracija Zadatak koji dopušta upravljanje, obnavljanje i prijenos Privacy Manager Certificates (Certifikati upravitelj privatnosti) i Trusted Contacts (Provjereni kontakti).

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

način sigurnosne prijave Način prijave na računalo.

nadzorna ploča Središnje mjesto s kojeg možete pristupati značajkama i postavkama softvera Security Manager for HP ProtectTools (upravitelj za sigurnost za HP ProtectTools) i njima upravljati.

obnavljanje Postupak koji kopira informacije programa iz prethodno spremljene datoteke sigurnosne kopije u ovaj program.

opoziv lozinke Lozinka koja je stvorena kada korisnik zahtijeva digitalni certifikat. Lozinka je potrebna kada korisnik želi opozvati svoj digitalni certifikat. Ovime se osigurava da jedino korisnik može opozvati certifikat.

otisak prsta Digitalni izvadak slike otiska vašeg prsta. Security Manager (Upravitelj za sigurnost) nikada ne pohranjuje stvarnu sliku otiska vašeg prsta.

otkrivanje Zadatak koji korisniku dopušta dešifriranje jedne ili više povijesnih razgovornih sesija prikazujući zaslonska imena kontakata kao običan tekst i omogućujući pregledavanje sesije.

ovlašteni korisnik Korisnik kojemu je u pregledu Postavke pristupa korisnika dano ovlaštenje da pregledava ili mijenja postavke konfiguracije u pregledu jednostavne konfiguracije ili konfiguracije klase uređaja.

pametna kartica Mali komad hardvera, po veličini i obliku sličan kreditnoj kartici, koji pohranjuje identifikacijske informacije o vlasniku. Rabi se za provjeru autentičnosti vlasnika na računalu.

pečat za pouzdane kontakte Zadatak koji dodaje digitalni potpis, šifrira e-poštu te je šalje nakon što potvrdite vlastitu autentičnost uporabom odabranog sigurnosnog načina prijave.

PIN Osobni identifikacijski broj.

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

ponovno pokretanje Postupak ponovnog pokretanja računala.

popis pouzdanih kontakata Popis provjerenih kontakata.

pouzdana komunikacija izravnim porukama Komunikacijska sesija tijekom koje pouzdani pošiljatelj šalje pouzdane poruke pouzdanom kontaktu.

pouzdana poruka Komunikacijska sesija tijekom koje pouzdani pošiljatelj šalje pouzdane poruke pouzdanom kontaktu.

pouzdani kontakt Osoba koja je prihvatila poziv za pouzdanog kontakta.

pouzdani pošiljatelj Pouzdani kontakt koji šalje potpisane i/ili šifrirane poruke e-pošte i dokumente aplikacija Microsoft Officea.

pozadinska usluga Pozadinska usluga Zaključavanje/kontrola uređaja sustava HP ProtectTools koja se mora pokrenuti da bi se mogla primijeniti pravila kontrole pristupanja uređajima. Može se prikazati iz aplikacije Usluge, u opciji Upravljačke ploče Administrativni alati. Ako nije pokrenuta, HP ProtectTools Security Manager (Upravitelj za sigurnost sustava HP ProtectTools) pokušava je pokrenuti prilikom primjene pravila kontrole pristupanja uređajima.

pozivnica za pouzdani kontakt E-pošta poslana osobi u kojoj se osobu traži da postane pouzdani kontakt.

pravila kontrole pristupanja uređajima Popis uređaja za koje je korisniku dopušten ili uskraćen pristup.

predloženi potpisnik Korisnik kojega je za dodavanje retka potpisa u dokumenta programa Microsoft Word ili Microsoft Excel

Preglednik povijesti programa Live Messenger Komponenta Privacy Manager Chata (upravitelj privatnosti razgovora) koja omogućuje traženje i pregledavanje povijesti šifriranih razgovornih sesija.

prijava Objekt u softveru Security Manager (Upravitelj za sigurnost) koji se sastoji od korisničkog imena i lozinke (moguće su i druge odabrane informacije), a koristi se za prijavu na web-mjesta ili u druge programe.

primatelj s popisa pouzdanih kontakata Osoba koja prima poziv da postane pouzdani kontakt.

profil uništavanja Zadani način brisanja i popis sredstava.

provjera autentičnosti Postupak provjere ovlaštenja korisnika za provođenje nekog zadatka poput pristupa računalu, izmjene postavki za određeni program ili pregledavanja sigurnih podataka.

provjera pri uključivanju Sigurnosna značajka koja zahtijeva neki oblik provjere autentičnosti poput Java kartice, sigurnosnog čipa ili lozinke pri uključivanju računala.

PSD Osobni zaštićeni pogon koji pruža zaštićeno područje za pohranu povjerljivih podataka.

redoslijed tipki Kombinacija posebnih tipki koje, kada se pritisnu, pokreću automatsko uništavanje – na primjer, ctrl+alt+s.

ručno uništavanje Neposredno uništavanje zapisa ili odabranih zapisa, koje zaobilazi vremenski planirano automatsko uništavanje.

SATA način rada uređaja Način prijenosa podatka između računala i uređaja za masovnu pohranu podataka poput tvrdih diskova i optičkih pogona.

sesija povijesti razgovora Šifrirana datoteka koja sadrži zapis konverzacije obje strane u razgovornoj sesiji.

sigurnosno kopiranje Korištenje značajke sigurnosnog kopiranja radi spremanja kopije važnih informacija iz programa na lokaciju izvan programa. Može se koristiti za kasnije obnavljanje tih informacija, na istom ili na drugom računalu.

slika Fotografija unesenog korisnika koja se koristi za provjeru autentičnosti.

sustav za šifriranje datoteka (EFS) Sustav koji šifrira sve datoteke i podmape unutar odabrane mape.

šifriranje Praksa šifriranja ili dešifriranja podataka kako bi ih mogli dešifrirati samo određeni pojedinci.

šifriranje Postupak, poput uporabe algoritma, koji se primjenjuje u kriptografiji za pretvaranje običnog u cifrirani tekst kako bi se neovlaštene primatelje spriječilo u čitanju odnosnih podataka. Postoji mnogo vrsta šifriranja podataka, a one su temelj sigurnosti mreže. Uobičajene vrste uključuju šifriranje prema standardu za šifriranje podataka i šifriranje javnim ključem.

Šifriranje pogona Štiti vaše podatke šifriranjem pogona tvrdog diska, što će spriječiti čitanje informacije od strane osoba koje nemaju odgovarajuće ovlasti.

token Pogledajte metodu zaštićene prijave.

TXT Trusted Execution Technology.

uništavanje Izvršavanje algoritma koji zakriva podatke sadržane u zapisu.

USB token Sigurnosni uređaj koji pohranjuje identifikacijske informacije o korisniku. Poput Java kartice ili biometrijskog čitača, uređaj se rabi za provjeru autentičnosti vlasnika na računalu.

ustanova za izdavanje certifikata Ustanova koja izdaje certifikate potrebne za vođenje infrastrukture javnog ključa.

virtualni token Sigurnosna značajka koja funkcionira poput Java kartice ili čitača kartice. Token se sprema na tvrdom disku računala ili u registru sustava Windows. Kada se prijavljujete s virtualnim tokenom, od vas će se za dovršetak provjere autentičnosti tražiti PIN korisnika.

vjerodajnice Način na koji korisnik dokazuje ispunjavanje uvjeta za određeni zadatak u postupku provjere autentičnosti.

zapis Podatkovna komponenta koja se sastoji od osobnih informacija ili datoteka, povijesnih ili podataka vezanih uz web.

zaslon za prijavu za šifriranje pogona Zaslon za prijavu koji se prikazuje prije pokretanja sustava Windows. Korisnici moraju unijeti korisničko ime i lozinku za sustav Windows ili PIN Java kartice. Unos točnih podataka na zaslonu za prijavu značajke Drive Encryption (šifriranje pogona) najčešće izravno omogućuje pristup u sustav Windows i nije potrebno ponovna prijava na zaslonu za prijavu sustava Windows.

Zaštita prijave u sustav Windows Štiti vaše račune sustava Windows kroz zahtijevanje korištenja određenih vjerodajnica za pristup.

Kazalo

V

W

Z