HP ProtectTools
Uporabniški priročnik

Prva izdaja: oktober 2009

Št. dokumenta: 572661-BA1

Kazalo

1 Uvod o varnosti

Programska oprema upravitelja varnosti HP ProtectTools Security Manager zagotavlja varnostne funkcije, ki pomagajo varovati pred nepooblaščenim dostopom do računalnika, omrežij in ključnih podatkov. Upravljanje orodja HP ProtectTools Security Manager je na voljo prek funkcije Administrative Console (Skrbniška konzola).

Konzola lokalnemu skrbniku omogoča naslednja opravila:

- omogočanje ali onemogočanje varnostnih funkcij,
- uvajanje uporabe prstnih odtisov za uporabnike tega računalnika,
- nastavitev pametne kartice,
- določanje zahtevanih poverilnic za preverjanje pristnosti,
- upravljanje uporabnikov računalnika,
- prilagajanje parametrov, značilnih za napravo,
- konfiguracijo nameščenih aplikacij upravitelja Security Manager,
- dodajanje novih aplikacij upravitelja Security Manager.

Razpoložljivi moduli programske opreme za računalnik so lahko odvisni od modela.

Moduli programske opreme HP ProtectTools so morda že vnaprej nameščeni ali naloženi, drugače pa jih lahko prenesete s HP-jevega spletnega mesta. Za več informacij obiščite http://www.hp.com.

OPOMBA: Navodila v tem priročniku so napisana ob predpostavki, da ste že namestili vse potrebne programske module HP ProtectTools.

Lastnosti HP ProtectTools

V spodnji tabeli so opisane ključne funkcije modulov HP ProtectTools.

Modul	Glavne lastnosti
Credential Manager (Upravitelj poverilnic) HP ProtectTools	• Modul Password Manager za upravljanje gesel deluje kot vaša osebna zakladnica gesel. S funkcijo za enkraten vpis Single Sign On, ki si samodejno zapomni in uporabi uporabniške poverilnice, racionalizira postopek prijave. • Funkcija Single Sign On ponuja tudi dodatno zaščito, tako da za preverjanje pristnosti uporabnika uporablja kombinacije različnih varnostnih tehnologij, na primer kartico Java™ Card in biometrijo. • Pomnilnik gesel je zaščiten s šifriranjem programske opreme in ga lahko izboljšate s preverjanjem pristnosti varnostne naprave, kakršnega zagotavljata kartica Java ali biometrija. **OPOMBA:** Funkcijo Credential Manager (Upravitelj poverilnic) najdete v možnosti Password Manager (Upravitelj gesel) v orodju HP ProtectTools Security Manager
Drive Encryption (Šifriranje pogonov) za HP ProtectTools (samo pri izbranih modelih)	• Modul Drive Encryption (Šifriranje pogonov) zagotavlja popolno šifriranje celotnega trdega diska. • Modul Drive Encryption (Šifriranje pogonov) vsili preverjanje pristnosti pred zagonom za dešifriranje in dostop do podatkov.
Privacy Manager (Upravitelj zasebnosti) za HP ProtectTools (samo pri izbranih modelih)	• Modul Privacy Manager (Upravitelj zasebnosti) uporablja napredne tehnike za prijavo, s katerimi preveri vir, neokrnjenost in varnost povezave pri uporabi e-pošte, dokumentov Microsoft® Office ali izmenjavi neposrednih sporočil (IM).
File Sanitizer (Orodje za čiščenje datoteke) za HP ProtectTools	• Z orodjem za čiščenje datotek File Sanitizer lahko varno izbrišete digitalna sredstva v računalniku (informacije občutljive narave (vključno s programskimi datotekami), vsebine v zvezi z zgodovino ali spletom ter druge zaupne podatke) in občasno varno počistite trdi disk s prepisovanjem.
Device Access Manager za HP ProtectTools (samo pri izbranih modelih)	• Modul Device Access Manager vodjem oddelka za IT omogoča, da nadzirajo dostop do naprav na podlagi uporabniških profilov. • Modul Device Access Manager nepooblaščenim uporabnikom onemogoča, da bi z zunanjimi pomnilniškimi mediji odstranili podatke in z njimi v sistem prinesli viruse. • Administrator lahko določenim posameznikom ali skupinam uporabnikov onemogoči dostop do zapisljivih naprav.

Kako doseči ključne cilje

Moduli HP ProtectTools lahko delujejo povezano in ponudijo rešitve za različne težave z varnostjo, vključno z naslednjimi ključnimi varnostnimi cilji:

- zaščita pred namensko krajo,
- omejevanje dostopa do občutljivih podatkov,
- preprečevanje nepooblaščenega dostopa prek internih ali eksternih lokacij,
- izdelava močnih politik glede gesel,
- vprašanje nadzornih varnostnih pooblastil.

Zaščita pred namensko krajo

Primer namenske kraje bi bil kraja računalnika, ki vsebuje zaupne podatke in informacije o stranki na varnostni kontrolni točki letališča. Naslednje funkcije pomagajo pri zaščiti pred namensko krajo:

- Funkcija preverjanja pristnosti pred zagonom, če je vključena, preprečuje dostop do operacijskega sistema. Glejte naslednje postopke:
  - Security Manager (Upravitelj varnosti)
  - Drive Encryption (Šifriranje pogonov) Drive Encryption (Šifriranje pogonov)

Omejevanje dostopa do občutljivih podatkov

Recimo, da pregledovalec pogodb dela na lokaciji stranke in je dobil računalniški dostop za pregledovanje občutljivih finančnih podatkov; verjetno ne želite, da bi imel možnost te datoteke natisniti ali shraniti na zapisljivo napravo, kot je CD. Naslednja funkcija pomaga pri omejevanju dostopa do podatkov:

- Device Access Manager (Upravitelj dostopa do naprav) HP ProtectTools omogoča upraviteljem IT, da omejijo dostop do zapisljivih naprav, tako da občutljivih informacij ni mogoče tiskati ali kopirati s trdega diska na odstranljive medije.

Preprečevanje nepooblaščenega dostopa prek internih ali eksternih lokacij

Nepooblaščen dostop do nezaščitenega poslovnega računalnika predstavlja zelo otipljivo tveganje virov omrežja podjetja, kot so podatki finančnih storitev, nadrejenega ali skupine za raziskave in razvoj, in osebnih podatkov, na primer kartotek pacientov in podatkov o finančnem stanju. Nepooblaščen dostop lahko preprečite z naslednjimi funkcijami:

- Funkcija preverjanja pristnosti pred zagonom, če je vključena, omogoča preprečiti dostop do operacijskega sistema. Glejte naslednje postopke:
  - Password Manager (Upravitelj gesel)
  - Drive Encryption (Šifriranje pogonov)
- Password Manager (Upravitelj gesel) pomaga zagotoviti, da nepooblaščen uporabnik ne more dobiti gesel ali dostopati do aplikacij, zaščitenih z gesli.

- Device Access Manager (Upravitelj dostopa do naprav) HP ProtectTools omogoča upraviteljem IT, da omejijo dostop do zapisljivih naprav, tako da občutljivih informacij ni mogoče kopirati s trdega diska.
- Funkcija DriveLock zagotavlja, da dostop do podatkov ni mogoč, tudi če je trdi disk odstranjen in nameščen v nezaščiten sistem.

Oblikovanje strogih pravilnikov glede gesel

Če začne veljati ukaz, ki zahteva uporabo strogega pravilnika glede gesel za več deset spletnih aplikacij in zbirk podatkov, orodje Security Manager (Upravitelj varnosti) zagotovi zaščiten pomnilnik za gesla in funkcijo enkratnega vpisa Single Sign On.

Dodatni varnostni elementi

Dodeljevanje varnostnih vlog

Pri upravljanju računalniške varnosti (zlasti v velikih organizacijah) je eden od pomembnih postopkov delitev odgovornosti in pravic na različne vrste skrbnikov in uporabnikov.

OPOMBA: V manjših organizacijah ali pri osebni rabi so lahko vse te vloge združene v isti osebi.

V orodju HP ProtectTools lahko varnostne zadolžitve in pravice razdelimo v naslednje vloge:

- Vodja varnosti - definira varnostne ravni za podjetje ali omrežje in določi varnostne ukrepe, ki bodo v rabi, npr. kartice Java™, biometrični bralniki ali žetoni USB.

  OPOMBA: Veliko funkcij HP ProtectTools lahko v sodelovanju s HP-jem prilagodi uradna oseba za varnost. Več informacij najdete na HP-jevem spletnem mestu http://www.hp.com.

- Skrbnik za IT - uporablja in upravlja varnostne ukrepe, ki jih definira vodja varnosti. Lahko pa tudi omogoča ali onemogoča določene funkcije. Če se na primer vodja varnosti odloči za uporabo kartic Java, lahko skrbnik za IT omogoči varnostni način BIOS za kartice Java.

- Uporabnik - uporablja varnostne funkcije. Če sta na primer vodja varnosti in skrbnik za IT omogočila kartice Java, si uporabnik lahko nastavi PIN za kartico Java in kartico uporablja za preverjanje pristnosti.

POZOR: Skrbniki naj uporabljajo »najboljšo prakso« pri omejevanju prednosti končnih uporabnikov in uporabniškega dostopa.

Nepooblaščenim uporabnikom ne smejo dajati skrbniških pravic.

Upravljanje gesel za HP ProtectTools

Večina funkcij orodja HP ProtectTools je zaščitena z gesli. V spodnji tabeli so navedena najpogosteje uporabljena gesla, moduli programske opreme, v katerih se geslo nastavi, in funkcija gesla.

Gesla, ki jih nastavijo in uporabljajo samo skrbniki IT, so prav tako prikazana v tej tabeli. Vsa ostala gesla lahko nastavijo navadni uporabniki ali skrbniki.

Geslo za HP ProtectTools	Nastavljena v tem modulu HP ProtectTools	Namen
Geslo za prijavo v Security Manager (Upravitelj varnosti)	Security Manager (Upravitelj varnosti)	To geslo nudi dve možnosti: • Uporabite ga lahko kot prijavo za upravitelja varnosti za dostop do tega orodja po prijavi v operacijski sistem Windows. • Uporabite ga lahko za hkratno dovoljenje dostopa v operacijski sistem Windows in v upravitelja varnosti.
Geslo za obnovitveno datoteko Security Manager (Upravitelj varnosti)	Security Manager (Upravitelj varnosti), s strani skrbnika IT	Ščiti dostop do obnovitvene datoteke upravitelja varnosti.
Številka PIN za kartico Java™	Java Card Security	Varuje dostop do vsebine kartice Java in preverja pristnost uporabnika kartice Java. Številka PIN kartice Java varuje tudi dostop

Geslo za HP ProtectTools	Nastavljena v tem modulu HP ProtectTools	Namen
		do orodja Computer Setup in do vsebine računalnika, če se uporablja za preverjanje pristnosti ob vklopu. Preveri pristnost uporabnikov modula Drive Encryption, če ni izbran žeton kartice Java.
Geslo za prijavo v Windows	Nadzorna plošča Windows®	Lahko se uporablja za ročno prijavo ali pa je shranjeno na kartici Java.

Ustvarjanje varnega gesla

Pri ustvarjanju gesel morate najprej upoštevati pravila, ki jih določa program. Na splošno pa upoštevajte naslednja priporočila, ki vam bodo pomagala ustvariti zanesljiva gesla in zmanjšati možnost razkritja vaših gesel:

- Uporabljajte gesla, ki imajo vsaj šest znakov ali še bolje, več kot osem znakov.
- V geslu naj bodo pomešane velike in male črke.
- Če je mogoče, v geslu pomešajte črke in številke ter jim dodajte posebne znake in ločila.
- V ključnih besedah zamenjajte črke s posebnimi znaki ali številkami. Na primer, številko 1 lahko uporabljate namesto črk I ali L.
- Združujte besede iz dveh ali več jezikov.
- Besedo ali stavek razdelite s številkami ali posebnimi znaki na sredini, na primer »Mojca2-2Cat45.«
- Za gesla ne uporabljajte besed, ki jih lahko najdete v slovarju.
- Za geslo ne uporabljajte svojega imena ali drugega osebnega podatka, npr. rojstnega datuma, imena ljubljencev, dekliškega priimka matere, četudi jih črkujete vzvratno.
- Redno spreminjajte gesla. Spremenite lahko le nekaj znakov, ki naraščajo.
- Če si geslo zapišete, ga ne shranjujte na lahko vidnih mestih blizu računalnika.
- Ne shranjujte gesla v datoteko, na primer kot e-pošto v računalniku.
- Dostopa do računa ne delite z drugimi in gesla ne povejte nikomur.

Varnostno kopiranje in obnovitev poverilnic za HP ProtectTools

Z orodjem Drive Encryption (Šifriranje pogonov) HP ProtectTools lahko izberete in izdelate varnostne kopije poverilnic za HP ProtectTools.

2 Prvi koraki

OPOMBA: Za upravljanje orodja HP ProtectTools potrebujete skrbniške pravice.

Čarovnik za nastavitev orodja HP ProtectTools vas vodi skozi nastavitev najbolj pogosto rabljenih funkcij orodja Security Manager (Upravitelj varnosti). Konzola HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools) pa vam omogoča še veliko dodatnih funkcij. Enake nastavitve, kot jih najdete v čarovniku, in tudi dodatne varnostne funkcije lahko konfigurirate s konzolo, do katere pridete prek menija Start v operacijskem sistemu Windows®. Nastavitve veljajo za računalnik in vse njegove uporabnike.

1. Na pozdravni strani lahko onemogočite nadaljnje prikazovanje čarovnika, in sicer tako, da izberete eno od možnosti.
2. En teden po namestitvi računalnika ali ko uporabnik s skrbniškimi pravicami prvič postavi prst na bralnik prstnih odtisov, vas bo čarovnik za namestitev orodja HP ProtectTools samodejno začel voditi po osnovnih korakih konfiguriranja programa. Video predstavitev nastavljanja računalnika se zažene samodejno.
3. Sledite navodilom na zaslonu, dokler se namestitev ne zaključi.

Če postopka s čarovnikom ne zaključite, se bo samodejno zagnal še dvakrat. Nato lahko do čarovnika dostopate prek obvestilnega balona, ki se prikaže v bližini področja za obvestila v opravilni vrstici (razen, če ste ga onemogočili, kot je opisano zgoraj v 2. koraku), dokler se nastavitev ne dokonča.

Če želite uporabljati aplikacije orodja HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools), ga zaženite iz menija Start ali pa z desno miškino tipko kliknite ikono Security Manager (Upravitelj varnosti) v področju za obvestila na skrajni desni strani opravilne vrstice. Konzola HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools) in njene aplikacije so na voljo vsem uporabnikom računalnika.

Odpiranje konzole HP ProtectTools Administrative Console

Za skrbniška opravila, kot je nastavljanje pravilnika sistema ali konfiguriranje programske opreme, odprite konzolo na naslednji način:

- Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools)**.

  – ali –

  V levem podoknu orodja Security Manager (Upravitelj varnosti) kliknite **Administration (Skrbništvo)**.

Za uporabniška opravila, kot je registriranje prstnih odtisov ali uporaba orodja Security Manager (Upravitelj varnosti), odprite konzolo tako:

- Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools)**.

  – ali –

  Dvokliknite ikono **HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools)** v področju za obvestila na skrajni desni strani opravilne vrstice.

Omogočanje varnostnih funkcij

Čarovnik za nastavitev bo od vas zahteval potrditev identitete.

1. Preberite pozdravni zaslon in nato kliknite **Next (Naprej)**.
2. Potrdite identiteto tako, da vtipkate svoje geslo za Windows, če še niste shranili prstnih odtisov, če pa ste to že naredili, identiteto potrdite tako, da položite prst na bralnik prstnih odtisov. Kliknite **Next (Naprej)**.

   Če gesla za Windows nimate, ga boste morali ustvariti. Geslo za Windows potrebujete za zaščito računa Windows pred dostopom nepooblaščenih oseb in za uporabo funkcij orodja HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).

Čarovnik za namestitev vas bo vodil skozi postopek omogočanja varnostnih funkcij, ki veljajo za vse uporabnike računalnika:

- Windows Logon Security (Zaščita prijave v operacijski sistem Windows) ščiti vaše račune Windows tako, da za dostop zahteva posebne poverilnice.
- Drive Encryption (Šifriranje pogona) zaščiti podatke tako, da šifrira trde diske, in tako tisti, ki nimajo pooblastil, ne morejo prebirati informacij.
- Pre-Boot Security (Zaščita pred zagonom) zaščiti računalnik tako, da prepove dostop nepooblaščenim osebam pred zagonom operacijskega sistema Windows.

Varnostno funkcijo omogočite tako, da označite ustrezno potrditveno polje. Več funkcij kot izberete, bolj varen bo računalnik.

OPOMBA: Pre-Boot Security (Zaščita pred zagonom) ne bo na voljo, če je ne podpira BIOS.

Uvajanje prstnih odtisov

Če ste izbrali možnost »Fingerprint« (Prstni odtis) in ima računalnik vgrajen ali povezan bralnik prstnih odtisov, vas bo sistem vodil skozi postopek nastavitve ali »uveljavitve« prstnih odtisov:

1. Prikaže se obris dveh rok. Prsti, ki ste jih že uveljavili, so označeni zeleno. Kliknite prst v obrisu.

   OPOMBA: Če želite izbrisati že uveljavljen prstni odtis, kliknite ustrezni prst.

2. Ko izberete prst za uveljavitev, morate ta prst položiti na optični bralnik in ga držati, dokler se ne uveljavi uspešno. Uveljavljeni prst je na obrisu prikazan zeleno.

3. Uveljaviti morate najmanj dva prsta, najbolje kazalec ali sredinec. Za uveljavitev novega prsta ponovite korake od 1 do 3.

4. Kliknite **Next (Naprej)**.

OPOMBA: Ko uveljavljate prstne odtise pri postopku Getting Started (Prvi koraki), se informacije o prstnih odtisih ne shranijo, dokler ne kliknete **Next (Naprej)**. Če za nekaj časa računalnik pustite v stanju nedelovanja ali zaprete nadzorno ploščo, se spremembe, ki jih opravite, **ne** shranijo.

Nastavitev pametne kartice

Če ste izbrali možnost »Smart card« (Pametna kartica) in ima računalnik vgrajen ali povezan bralnik pametnih kartic, vas bo čarovnik za nastavitev HP ProtectTools Setup Wizard pozval, da nastavite kodo PIN (osebna identifikacijska številka) za pametno kartico.

Nastavitev kode PIN za pametno kartico:

1. Na strani »Set up smart card« (Nastavitev pametne kartice) vnesite in potrdite kodo PIN.

   Kodo PIN lahko tudi spreminjate. Vnesite staro kodo in nato izberite novo.

2. Za nadaljevanje kliknite **Next (Naprej)**.

Uporaba skrbniške konzole

Konzola HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools) je središčna lokacija za upravljanje funkcij in aplikacij orodja HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).

Konzolo sestavljajo naslednje komponente:

- **Tools (Orodja)** – prikazuje naslednje kategorije za konfiguriranje varnosti v računalniku:
  - **Home (Domov)** – omogoča izbiro želenih varnostnih opravil.
  - **System (Sistem)** – omogoča konfiguriranje varnostnih funkcij in preverjanje pristnosti za uporabnike in naprave.
  - **Applications (Aplikacije)** – prikazuje splošne nastavitve za orodje HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools) in za aplikacije tega orodja.
  - **Data (Podatki)** – omogoča razširljiv meni povezav na aplikacije orodja Security Manager (Upravitelj varnosti), ki ščitijo vaše podatke.
- **Management Tools (Orodja za upravljanje)** – informacije o dodatnih orodjih. Spodaj so prikazane naslednje možnosti:
  - **HP ProtectTools Setup Wizard (Čarovnik za nastavitev HP ProtectTools** – vodi vas po nastavitvi orodja HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).
  - **Help (Pomoč)** – prikazuje datoteko s pomočjo, kjer najdete informacije o orodju Security Manager (Upravitelj varnosti) in o prednastavljenih aplikacijah tega orodja. V teh aplikacijah najdete tudi pomoč za aplikacije, ki jih lahko dodate.
  - **About (Vizitka)** – prikazuje informacije o orodju HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools), kot je številka različice ali obvestilo o avtorskih pravicah.
- **Main area (Glavno območje)** – prikazuje zaslone, ki so vezani na določeno aplikacijo.

Konzolo HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools) odprete tako, da kliknete **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools)**.

3 Konfiguriranje sistema

Do skupine System (Sistem) pridete s plošče menija Tools (Orodja) na levi strani zaslona konzole HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools). Aplikacije v tej skupini lahko uporabljate za upravljanje pravilnikov in nastavitev računalnika, njegovih uporabnikov in naprav.

V skupini System (Sistem) so naslednje aplikacije:

- **Security (Varnost)** – upravljanje funkcij, preverjanja pristnosti in nastavitev, s katerimi upravljate način interakcije med uporabniki in računalnikom.
- **Users (Uporabniki)** – nastavljanje, upravljanje in registriranje uporabnikov računalnika.
- **Devices (Naprave)** – upravljanje nastavitev za varnostne naprave, vgrajene v računalnik ali priključene nanj.

Nastavljanje preverjanja pristnosti za računalnik

V aplikaciji Authentication (Preverjanje pristnosti) lahko izberete, katere varnostne funkcije naj se izvajajo v računalniku, nastavite pravilnike, ki upravljajo dostop do računalnika, in konfigurirate dodatne napredne nastavitve. Določite lahko poverilnice, potrebne za preverjanje pristnosti vseh razredov uporabnikov ob prijavi v operacijski sistem Windows ali ob prijavi na spletna mesta in programe med uporabniško sejo.

Nastavljanje preverjanja pristnosti v računalniku:

1. V meniju plošče Security (Varnost) kliknite **Authentication (Preverjanje pristnosti)**.
2. Za konfiguriranje preverjanje pristnosti ob prijavi kliknite jeziček **Logon Policy (Pravilnik za prijavo)**, opravite spremembe in kliknite **Apply (Uporabi)**.
3. Za konfiguriranje preverjanje pristnosti za sejo kliknite jeziček **Session Policy (Pravilnik za sejo)**, opravite spremembe in kliknite **Apply (Uporabi)**.

Pravilnik za prijavo

Če želite določiti pravilnik za upravljanje poverilnic, potrebnih za preverjanje pristnosti uporabnika ob prijavi v operacijski sistem Windows:

1. V meniju Tools (Orodja) kliknite **Security (Varnost)** in nato **Authentication (Preverjanje pristnosti)**.
2. Na kartici **Logon Policy (Pravilnik za prijavo)** kliknite kategorijo uporabnikov.
3. Določite poverilnice preverjanja pristnosti, ki naj bodo potrebne za izbrano kategorijo uporabnikov. Določiti morate vsaj eno poverilnico.
4. Izberite, ali naj bo za preverjanje pristnosti uporabnika potrebna ANY (KATERA KOLI) (le ena) od določenih poverilnic ali ALL (VSE) določene poverilnice. Vsakemu uporabniku lahko tudi preprečite dostop do računalnika.
5. Kliknite **Apply (Uporabi)**.

Pravilnik za sejo

Če želite določiti pravilnik za upravljanje poverilnic, potrebnih za dostop do aplikacij HP ProtectTools med sejo v operacijskem sistemu Windows:

1. V meniju Tools (Orodja) kliknite **Security (Varnost)** in nato **Authentication (Preverjanje pristnosti)**.
2. Na kartici **Session Policy (Pravilnik za sejo)** kliknite kategorijo uporabnikov.
3. Določite poverilnice preverjanja pristnosti, ki naj bodo potrebne za izbrano kategorijo uporabnikov.
4. Izberite, ali naj bo za preverjanje pristnosti uporabnika potrebna ANY (KATERA KOLI) (le ena) od določenih poverilnic ali ALL (VSE) določene poverilnice. Lahko se odločite tudi, da za dostop do programske opreme HP ProtectTools ni potrebno preverjanje pristnosti.
5. Kliknite **Apply (Uporabi)**.

Nastavitve

Dovolite lahko eno ali več od naslednjih varnostnih nastavitev:

- **Allow One Step logon (Dovoli prijavo v enem koraku)** – uporabnikom računalnika omogoča preskok prijave v operacijski sistem Windows, če je bilo preverjanje pristnosti izvedeno na ravni BIOS ali šifriranega diska.
- **Allow HP SpareKey authentication for Windows logon (Dovoli preverjanje pristnosti HP SpareKey za prijavo v operacijski sistem Windows** – uporabnikom računalnika omogoča uporabo funkcije HP SpareKey za prijavo v operacijski sistem Windows kljub drugačnemu pravilniku glede preverjanja pristnosti, ki ga zahteva orodje Security Manager (Upravitelj varnosti).

Nastavitve uredite tako:

1. Kliknite za omogočanje ali onemogočanje določene nastavitve.
2. Kliknite **Apply (Uporabi)**, da shranite spremembe, ki ste jih naredili.

Upravljanje uporabnikov

V aplikaciji Users (Uporabniki) lahko nadzirate in upravljate uporabnike programa HP ProtectTools.

Vsi uporabniki programa HP ProtectTools so na seznamu in so potrjeni v skladu s pravilnikom, nastavljenim v orodju Security Manager (Upravitelj varnosti), ne glede na to, ali so registrirali ustrezne poverilnice, ki jim omogočajo, da ustrezajo pravilniku.

Če želite dodati nove uporabnike, kliknite **Add (Dodaj)**.

Če želite izbrisati uporabnika, ga kliknite in nato kliknite **Delete (Izbriši)**.

Če želite uveljaviti prstne odtise ali nastaviti dodatne poverilnice za uporabnika, kliknite uporabnika in nato kliknite **Enroll (Uveljavi)**.

Če si želite ogledati pravilnike za določenega uporabnika, izberite uporabnika in nato kliknite **View Policies (Ogled pravilnika)**.

Določanje nastavitev naprave

V aplikaciji Device (Naprava) lahko določite nastavitve, ki bodo na voljo za kakršne koli vgrajene ali priključene varnostne naprave, ki jih prepozna orodje HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).

Prstni odtisi

Stran Fingerprints (Prstni odtisi) ima tri jezičke: Enrollment (Uveljavitev), Sensitivity (Občutljivost) in Advanced (Napredno).

Enrollment (Uveljavitev)

Izberete lahko najmanjše in največje število prstnih odtisov, ki jih lahko uporabnik uveljavi.

Iz bralnika prstnih odtisov lahko izbrišete vse podatke.

⚠ **OPOZORILO!** Vsi podatki o prstnih odtisih vseh uporabnikov, vključno s skrbniki, bodo izbrisani. Če pravilnik prijave zahteva samo prstne odtise, se lahko zgodi, da bo vsem uporabnikom preprečena prijava v računalnik.

Sensitivity (Občutljivost)

Če želite prilagoditi občutljivost bralnika prstnih odtisov, ko optično prebira prstne odtise, premaknite drsnik.

Če bralnik vašega prstnega odtisa vedno znova ne prepozna, boste morda morali uporabljati nižjo nastavitev občutljivosti. Višja nastavitev poveča občutljivost na spremembe pri prebiranju prstnih odtisov in tako zmanjša možnost napačnega sprejema. Nastavitev Medium-High (Srednja-visoka) omogoča dobro mešanico varnosti in udobnosti.

Advanced (Napredno)

Bralnik prstnih odtisov lahko konfigurirate tako, da bo varčeval z energijo, ko računalnik deluje na akumulator.

Pametna kartica

Računalnik lahko konfigurirate tako, da se bo samodejno zaklenil, ko odstranite pametno kartico. Računalnik se bo zaklenil le, če ste pametno kartico uporabili kot poverilnico za preverjanje pristnosti pri prijavi v operacijski sistem Windows. Če odstranite pametno kartico, ki je niste uporabili za prijavo v operacijski sistem Windows, se računalnik ne bo zaklenil.

- Označite potrditveno polje za omogočanje ali onemogočanje zaklepanja računalnika ob odstranitvi pametne kartice.

4 Konfiguriranje aplikacij

Do skupine Applications (Aplikacije) pridete s plošče menija Security Applications (Varnostne aplikacije) na levi strani konzole HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools). Nastavitve lahko uporabljate za prilagajanje delovanja trenutno nameščenih aplikacij orodja HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).

Nastavitve aplikacij uredite tako:

1. V meniju Tools (Orodja), v skupini **Applications (Aplikacije)** kliknite **Settings (Nastavitve)**.
2. Kliknite za omogočanje ali onemogočanje določene nastavitve.
3. Kliknite **Apply (Uporabi)**, da shranite spremembe, ki ste jih naredili.

Kartica General (Splošno)

Na kartici General (Splošno) so na voljo naslednje nastavitve:

- **Do not automatically launch the Setup Wizard for administrators (Čarovnika za nastavitev za skrbnike ne zaženi samodejno)** – izberite to možnost, če želite čarovniku preprečiti, da se ob prijavi samodejno odpre.
- **Do not automatically launch the Getting Started wizard for users (Čarovnika za prve korake za uporabnike ne zaženi samodejno)** – izberite to možnost, če želite preprečiti, da se ob prijavi samodejno odpre nastavitev uporabnikov.

Kartica Applications (Aplikacije)

Nastavitve, ki so prikazane tukaj, se lahko spremenijo, ko v orodje Security Manager (Upravitelj varnosti) dodate nove aplikacije. Minimalne nastavitve, ki so privzeto prikazane, so:

- **Security Manager (Upravitelj varnosti)** – aplikacijo Security Manager (Upravitelj varnosti) omogoča vsem uporabnikom računalnika.
- **Enable the Discover more button (Omogoči gumb za odkrivanje več možnosti)** – vsem uporabnikom računalnika omogoča dodajanje aplikacij v orodje HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools), in sicer tako, da kliknejo gumb **[+] Discover more (Odkrij več)**.

Če želite, da se vse aplikacije vrnejo na tovarniške nastavitve, kliknite gumb **Restore Defaults (Obnovi privzete nastavitve)**.

5 Dodajanje orodij za upravljanje

Za dodajanje novih orodij za upravljanje za orodje Security Manager (Upravitelj varnosti) so morda na voljo dodatne aplikacije. Skrbnik računalnika lahko to funkcijo onemogoči prek aplikacije Settings (Nastavitve).

Če želite dodati nova orodja za upravljanje, kliknite **[+] Management tools (Orodja za upravljanje)**.

Za preverjanje novih aplikacij lahko obiščete spletno mesto DigitalPersona ali pa nastavite urnik za samodejne posodobitve.

6 HP ProtectTools Security Manager

Orodje HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools) vam omogoča bistveno povečanje varnosti računalnika.

Uporabite lahko predhodno naložene aplikacije orodja Security Manager (Upravitelj varnosti) in dodatne aplikacije, ki so na voljo za neposreden prenos s spleta:

- Upravljajte podatke za prijavo in gesla
- Enostavno spremenite geslo za operacijski sistem Windows®
- Določite nastavitve programa
- Uporabljajte prstne odtise za dodatno varnost in udobje
- Nastavite pametno kartico za preverjanje pristnosti
- Naredite varnostno kopijo in obnovite podatke o programu
- Dodajte več aplikacij

Nastavitev

Prvi koraki

Čarovnik za nastavitev HP ProtectTools Setup Wizard se prikaže samodejno kot privzeta stran v orodju HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools), dokler ne dokončate namestitve.

Za namestitev orodja Security Manager (Upravitelj varnosti) sledite tem korakom:

OPOMBA: Če nimate na voljo ne bralnika prstnih odtisov ne pametne kartice, opravite le korake 1, 5 in 6.

1. Na pozdravni strani kliknite **Next (Naprej)**.
2. Na naslednji strani so našteti načini preverjanja pristnosti, ki so na voljo v računalniku. Za nadaljevanje kliknite **Next (Naprej)**.
3. Na strani »Verify Your Identity« (Potrdite svojo identiteto) vnesite geslo za Windows in nato kliknite **Next (Naprej)**.
4. Oglejte si eno ali več naslednjih tem, odvisno od konfiguracije računalnika.
   - Če imate na voljo bralnik prstnih odtisov, glejte razdelek Uvajanje prstnih odtisov na strani 24.
   - Če imate na voljo pametno kartico, glejte razdelek Nastavitev pametne kartice na strani 25.
5. Če nimate na voljo ne bralnika prstnih odtisov ne pametne kartice, boste morali vnesti geslo za Windows. To geslo morate uporabljati v prihodnosti, kadar koli potrebujete preverjanje pristnosti.
6. Na zadnji strani čarovnika kliknite **Finish (Dokončaj)**.

   Prikaže se nadzorna plošča orodja Security Manager (Upravitelj varnosti).

Registriranje poverilnic

Stran »My Identity« (Moja identiteta) lahko uporabljate za registriranje različnih načinov preverjanja pristnosti ali poverilnic. Ko načine registrirate, jih lahko uporabljate za prijavo v orodje Security Manager (Upravitelj varnosti).

Uvajanje prstnih odtisov

Če ima računalnik vgrajen ali povezan bralnik prstnih odtisov, vas bo čarovnik za namestitev HP ProtectTools Setup Wizard vodil skozi postopek nastavljanja ali »uvajanja« prstnih odtisov.

1. Preberite pozdravni zaslon in nato kliknite **Next (Naprej)**.
2. Potrdite identiteto tako, da vtipkate svoje geslo Windows, če še niste shranili prstnih odtisov, če pa ste to že naredili, identiteto potrdite tako, da položite prst na bralnik prstnih odtisov. Kliknite **Next (Naprej)**.

   Če gesla Windows nimate, ga boste morali ustvariti. Geslo Windows potrebujete za zaščito računa Windows pred dostopom nepooblaščenih oseb in za uporabo funkcij orodja HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).
3. Prikaže se obris dveh rok. Prsti, ki ste jih že uveljavili, so označeni zeleno. Kliknite prst v obrisu.

OPOMBA: Če želite izbrisati že uveljavljen prstni odtis, kliknite ustrezni prstni odtis.

4. Ko izberete prst za uveljavitev, morate ta prst položiti na optični bralnik in ga držati, dokler se ne uveljavi uspešno. Uveljavljen prst je na obrisu prikazan zeleno.
5. Uveljaviti morate najmanj dva prsta, najbolje kazalec ali sredinec. Za uveljavitev novega prsta ponovite koraka 3 in 4.
6. Kliknite **Next (Naprej)**.

OPOMBA: Ko uveljavljate prstne odtise pri postopku Getting Started (Prvi koraki), se informacije o prstnih odtisih ne shranijo, dokler ne kliknete **Next (Naprej)**. Če za nekaj časa računalnik pustite v stanju nedelovanja ali zaprete nadzorno ploščo, se spremembe, ki jih opravite, **ne** shranijo.

Spreminjanje gesla za Windows

Orodje Security Manager (Upravitelj varnosti) poenostavlja spreminjanje gesla za operacijski sistem Windows, poleg tega bo spreminjanje tudi hitrejše kot prek nadzorne plošče operacijskega sistema Windows.

Za spreminjanje gesla za Windows sledite tem korakom:

1. Na nadzorni plošči orodja Security Manager (Upravitelj varnosti) kliknite **My Identity (Moja identiteta)**, **Credentials (Poverilnice)** in nato **Password (Geslo)**.
2. V polje **Current Windows password (Trenutno geslo za Windows)** vnesite trenutno geslo.
3. Vnesite novo geslo v polje **New Windows password (Novo geslo za Windows)** in ga nato znova vnesite v polje **Confirm new password (Potrdi novo geslo)**.
4. Kliknite **Change (Spremeni)**, če želite takoj spremeniti trenutno geslo v tistega, ki ste ga pravkar vnesli.

Nastavitev pametne kartice

Če je v računalnik vgrajen ali povezan bralnik pametnih kartic, vas bo orodje Security Manager (Upravitelj varnosti) pozvalo, da nastavite kodo PIN (osebna identifikacijska številka) varnostne kartice.

- Nastavitev kode PIN za pametno kartico – na strani »Set up smart card« (Nastavitev pametne kartice) vnesite in potrdite kodo PIN.
- Spreminjanje kode PIN – najprej vnesite staro kodo PIN in nato izberite novo.

Uporaba nadzorne plošče orodja Security Manager

Nadzorna plošča orodja Security Manager (Upravitelj varnosti) je osrednja lokacija za enostaven dostop do funkcij, aplikacij in nastavitev orodja Security Manager (Upravitelj varnosti).

Nadzorno ploščo sestavljajo naslednje komponente:

- **ID Card (Kartica ID)** – prikazuje uporabniško ime za operacijski sistem Windows in izbrano sliko, s katero prepoznate račun prijavljenega uporabnika.
- **Security Applications (Varnostne aplikacije)** – prikazuje razširjeni meni povezav za konfiguriranje naslednjih kategorij varnosti:
  - **My Identity (Moja identiteta)**
  - **My Data (Moji podatki)**
  - **My Computer (Moj računalnik)**
- **Discover more (Odkrij več)** – odpre stran, kjer lahko najdete dodatne aplikacije za izboljšanje varnosti identitete, podatkov in komunikacij.
- **Main area (Glavno območje)** – prikazuje zaslone, ki so vezani na določeno aplikacijo.
- **Administration (Skrbništvo)** – odpre konzolo HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools).
- **Help button (Gumb za pomoč)** – prikazuje informacije o trenutnem zaslonu.
- **Advanced (Napredno)** – omogoča dostop do naslednjih možnosti:
  - **Preferences (Nastavitve)** – omogoča spreminjanje nastavitev orodja Security Manager (Upravitelj varnosti) po lastnih željah.
  - **Backup and Restore (Varnostno kopiranje in obnovitev)** – omogoča varnostno kopiranje ali obnovitev podatkov.
  - **About (Vizitka)** – prikazuje informacije o različici orodja Security Manager (Upravitelj varnosti).

Nadzorno ploščo orodja Security Manager (Upravitelj varnosti) odprete tako, da kliknete **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools)**.

Odpiranje orodja HP ProtectTools Security Manager

Orodje HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools) lahko odprete na katerega koli od naslednjih načinov:

- Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools)**.
- Dvokliknite ikono **HP ProtectTools** v področju za obvestila na skrajni desni strani opravilne vrstice.
- Z desno miškino tipko kliknite ikono **HP ProtectTools** in nato **Open HP ProtectTools Security Manager (Odpri upravitelja varnosti HP ProtectTools)**.
- Kliknite pripomoček **Security Manager ID Card (Kartica ID upravitelja varnosti)** v stranski vrstici »Windows Sidebar«.
- Pritisnite kombinacijo bližnjičnih tipk ctrl + alt + h, da odprete meni Security Manager Quick Links (Hitre povezave upravitelja varnosti).

Splošna opravila

Aplikacije v tej skupini vam pomagajo pri upravljanju različnih vidikov digitalne identitete.

- **Security Manager (Upravitelj varnosti)** – ustvarja in upravlja hitre povezave, ki vam omogočajo zagon in prijavo na spletna mesta in programe prek preverjanja pristnosti z geslom Windows, prstnimi odtisi ali pametno kartico.
- **Credentials (PoveriInice)** – omogočajo hitro spreminjanje gesla za operacijski sistem Windows, uveljavitev prstnih odtisov ali nastavljanje pametne kartice.

Če želite dodati več aplikacij, kliknite gumb [+] **Discover more (Odkrij več)** v levem spodnjem kotu nadzorne plošče. Skrbnik lahko ta gumb onemogoči.

Password Manager

Prijava v operacijski sistem Windows, spletna mesta in aplikacije je enostavnejša in varnejša z uporabo orodja Password Manager (Upravitelj gesel). Uporabljate ga lahko za ustvarjanje bolj varnih gesel, ki vam jih ni treba zapisati ali si jih zapomniti, nato pa se lahko prijavite enostavno in hitro s prstnim odtisom, pametno kartico ali geslom za operacijski sistem Windows.

Orodje Password Manager (Upravitelj gesel) ponuja naslednje možnosti:

- Dodajanje, urejanje ali brisanje prijav s kartice Manage (Upravljanje).
- Uporaba hitrih povezav za zagon privzetega brskalnika in prijavo na katero koli spletno mesto ali program, ko je nastavljen.
- Vlečenje in spuščanje za organiziranje hitrih povezav v kategorije.
- Hitro preverjanje tega, ali kakšno geslo predstavlja varnostno tveganje, in samodejno proizvajanje zapletenega varnega gesla za uporabo pri novih spletnih mestih.

Veliko funkcij orodja Password Manager (Upravitelj gesel) je na voljo prek ikone tega orodja, ki se prikaže, ko je pozornost usmerjena na spletno stran ali prijavni zaslon programa. Kliknite ikono, da se odpre kontekstni meni, kjer lahko izbirate med naslednjimi možnostmi.

Za spletna mesta ali programe, za katere prijave še niso ustvarjene

V kontekstnem meniju so prikazane naslednje možnosti:

- **Add [somedomain.com] to the Password Manager (Dodaj [nekodomeno.com] v upravitelja gesel)** – omogoča dodajanje prijave za trenutni prijavni zaslon.
- **Open Password Manager (Odpri upravitelja gesel)** – zažene orodje Password Manager (Upravitelj gesel).
- **Icon settings (Nastavitve ikon)** – omogoča določanje pogojev, pod katerimi se prikaže ikona orodja Password Manager (Upravitelj gesel).
- **Help (Pomoč)** – prikazuje pomoč za programsko opremo orodja Password Manager (Upravitelj gesel).

Za spletna mesta ali programe, za katere so prijave že ustvarjene

V kontekstnem meniju so prikazane naslednje možnosti:

- **Fill in logon data (Izpolnjevanje podatkov za prijavo)** – podatke za prijavo postavi v polja za prijavo in nato pošlje stran (če je bilo pošiljanje določeno ob ustvarjanju ali zadnjem urejanju prijave).
- **Edit logon (Urejanje prijave)** – omogoča urejanje podatkov za prijavo za to spletno mesto.
- **Add a New Account (Dodajanje novega računa)** – omogoča dodajanje računa za prijavo.
- **Open Password Manager (Odpri upravitelja gesel)** – zažene aplikacijo Password Manager (Upravitelj gesel).
- **Help (Pomoč)** – prikazuje pomoč za programsko opremo orodja Password Manager (Upravitelj gesel).

OPOMBA: Skrbnik računalnika je morda nastavil orodje Security Manager (Upravitelj varnosti) tako, da pri preverjanju identitete zahteva več kot eno poverilnico.

Dodajanje prijav

Prijavo za spletno mesto ali program lahko brez težav dodate tako, da enkrat vnesete prijavne informacije. Od tega trenutka orodje Password Manager (Upravitelj gesel) samodejno vnese te informacije namesto vas. Prijave lahko uporabljate po brskanju do spletnega mesta ali programa, ali pa kliknete prijavo v meniju **Logons (Prijave)**, da orodje Password Manager (Upravitelj gesel) odpre spletno mesto ali program in vas prijavi.

Dodajanje prijave:

1. Odprite prijavni zaslon za spletno mesto ali program.
2. Kliknite puščico na ikoni **Password Manager (Upravitelj gesel)** in nato kliknite nekaj od naslednjega, odvisno od tega, ali prijavni zaslon velja za spletno mesto ali program.
   - Za spletno mesto kliknite **Add [domain name] to Password Manager (Dodaj [ime domene] v upravitelja gesel)**.
   - Za program kliknite **Add this logon screen to Password Manager (Dodaj ta prijavni zaslon v upravitelja gesel)**.
3. Vnesite svoje prijavne podatke. Prijavna polja na zaslonu in ustrezna polja v pogovornem oknu prepoznate po krepki oranžni obrobi. To pogovorno okno lahko odprete tudi tako, da na kartici **Password Manager Manage (Upravljanje upravitelja gesel)** kliknete **Add Logon (Dodaj prijavo)**. Nekatere možnosti so odvisne od varnostnih naprav, povezanih v računalnik, npr. z bližnjično tipko ctrl + alt + H, optičnim prebiranjem prstnega odtisa ali vstavljanjem pametne kartice.
   - Če želite prijavno polje zapolniti z eno od predhodno oblikovanih izbir, kliknite puščice na desni strani polja.
   - Če želite z zaslona v prijavo dodati še več polj, kliknite **Choose other fields (Izberi druga polja)**.

- Če želite, da se prijavna polja izpolnijo, vendar ne pošljejo, počistite potrditveno polje **Submit logon data (Pošlji prijavne podatke)**.
- Če si želite ogledati geslo za to prijavo, kliknite **Show password (Prikaži geslo)**.

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

   Z ikone orodja Password Manager (Upravitelj gesel) se odstrani znak »plus«; sistem vas tako obvesti, da je bila prijava ustvarjena.

Vsakič, ko obiščete to spletno mesto ali odprete ta program, se prikaže ikona orodja Password Manager (Upravitelj gesel), kar pomeni, da lahko za prijavo uporabite registrirane poverilnice.

Urejanje prijav

Za urejanje prijave sledite naslednjim korakom:

1. Odprite prijavni zaslon za spletno mesto ali program.
2. Če želite odpreti pogovorno okno, kjer boste lahko uredili prijavne informacije, kliknite puščico na ikoni **Password Manager (Upravitelj gesel)** in nato kliknite **Edit logon (Uredi prijavo)**. Prijavna polja na zaslonu in ustrezna polja v pogovornem oknu prepoznate po krepki oranžni obrobi.

   To pogovorno okno lahko odprete tudi tako, da na kartici **Password Manager Manage (Upravljanje upravitelja gesel)** kliknete **Edit for the desired logon (Urejanje za želeno prijavo)**.
3. Uredite svoje prijavne podatke.
   - Če želite prijavno polje zapolniti z eno od predhodno oblikovanih izbir, kliknite puščice na desni strani polja.
   - Če želite z zaslona v prijavo dodati še več polj, kliknite **Choose other fields (Izberi druga polja)**.
   - Če želite, da se prijavna polja izpolnijo, vendar ne pošljejo, počistite potrditveno polje **Submit logon data (Pošlji prijavne podatke)**.
   - Če si želite ogledati geslo za to prijavo, kliknite **Show password (Prikaži geslo)**.
4. Kliknite **OK (V redu)**.

Uporaba menija prijav

Orodje Password Manager (Upravitelj gesel) omogoča hiter, enostaven način zagona spletnih mest in programov, za katere ste ustvarili prijave. V meniju **Logons (Prijave)** ali na kartici **Manage (Upravljanje)** v orodju **Password Manager (Upravitelj gesel)** dvokliknite prijavo za program ali spletno mesto, da se odpre prijavni zaslon, nato pa vnesite prijavne podatke.

Ko ustvarite prijavo, se samodejno doda v meni Password Manager Logons (Prijave upravitelja gesel).

Meni Logons (Prijave) prikažete tako:

1. Pritisnite kombinacijo bližnjičnih tipk za orodje **Password Manager (Upravitelj gesel)**. Tovarniško nastavljena kombinacija je »ctrl + alt + h«. Če želite spremeniti kombinacijo bližnjičnih tipk, kliknite **Password Manager (Upravitelj gesel)** in nato **Settings (Nastavitve)**.
2. Optično preberite prstni odtis (pri računalnikih, ki imajo vgrajen ali priključen bralnik prstnih odtisov).

Organiziranje prijav v kategorije

Uporabljajte kategorije, da bodo vaše prijave urejene; to naredite tako, da ustvarite eno ali več kategorij. Nato povlecite in spustite prijave v želene kategorije.

Kategorijo dodate tako:

1. Na nadzorni plošči orodja Security Manager (Upravitelj varnosti) kliknite **Password Manager (Upravitelj gesel)**.
2. Kliknite kartico **Manage (Upravljanje)** in nato **Add Category (Dodaj kategorijo)**.
3. Vnesite ime za kategorijo.
4. Kliknite **OK (V redu)**.

Če želite dodati prijavo kategoriji:

1. Postavite kazalec miške čez želeno prijavo.
2. Pritisnite in držite levo miškino tipko.
3. Prijavo povlecite na seznam kategorij. Ko premikate miško čez kategorije, se bodo označile.
4. Sprostite miškino tipko, ko je označena želena kategorija.

Prijave se ne premaknejo v kategorijo, ampak se samo kopirajo v izbrano kategorijo. Isto prijavo lahko dodate v več kategorij, vse prijave pa lahko prikažete, če kliknete **All (Vse)**.

Upravljanje prijav

Orodje Password Manager (Upravitelj gesel) poenostavlja upravljanje prijavnih informacij za uporabniška imena, gesla in račune z več prijavami iz ene, središčne lokacije.

Prijave so naštete na kartici Manage (Upravljanje). Če je bilo za isto spletno mesto ustvarjenih več prijav, je vsaka prijava navedena pod imenom spletnega mesta in je na seznamu prijav zamaknjena.

Prijave upravljate tako:

Na nadzorni plošči orodja Security Manager (Upravitelj varnosti) kliknite **Password Manager (Upravitelj gesel)** in nato kartico **Manage (Upravljanje)**.

- **Add a logon (Dodaj prijavo)** – kliknite **Add Logon (Dodaj prijavo)** in sledite navodilom na zaslonu.
- **Edit a logon (Uredi prijavo)** – kliknite prijavo, nato **Edit (Uredi)** in nato spremenite prijavne podatke.
- **Delete a logon (Izbriši prijavo)** – kliknite prijavo in nato **Delete (Izbriši)**.

Če želite dodati novo prijavo za spletno mesto ali program:

1. Odprite prijavni zaslon za spletno mesto ali program.
2. Kliknite ikono **Password manager (Upravitelj gesel)**, da prikažete njen bližnjični meni.
3. Kliknite **Add additional logon (Dodaj novo prijavo)** in sledite navodilom na zaslonu.

Ocenjevanje moči gesla

Uporaba močnih gesel za prijavo na spletna mesta in programe je pomemben vidik varovanja identitete.

Orodje Password Manager (Upravitelj gesel) z neposredno in samodejno analizo moči vsakega gesla, ki ga uporabljate za prijavo na spletna mesta in programe, poenostavlja nadziranje in izboljševanje varnosti.

Nastavitve ikone orodja Password Manager

Orodje Password Manager (Upravitelj gesel) poskuša prepoznati prijavne zaslone spletnih mest in programov. Ko zazna prijavni zaslon, za katerega še niste ustvarili prijave, vas orodje Password Manager (Upravitelj gesel) pozove, da dodate prijavo za zaslon, kar naredi tako, da prikaže svojo ikono z znakom »+«.

Kliknite puščico ikone in nato **Icon Settings (Nastavitve ikone)**, da prilagodite način, kako orodje **Password Manager (Upravitelj gesel)** obravnava potencialna spletna mesta s prijavo.

- **Prompt to add logons for logon screens (Poziv za dodajanje prijav za prijavne zaslone** – kliknite to možnost, da vas orodje Password Manager (Upravitelj gesel) pozove k dodajanju prijave, ko se odpre prijavni zaslon, za katerega še niste nastavili prijave.
- **Exclude this screen (Izvzemi ta zaslon)** – označite to potrditveno polje, da vas orodje Password Manager (Upravitelj gesel) ne bo več pozivalo k dodajanju prijave za ta prijavni zaslon.

Za dostop do dodatnih nastavitev orodja Password Manager (Upravitelj gesel) kliknite **Password Manager (Upravitelj gesel)** in nato na nadzorni plošči orodja Security Manager (Upravitelj varnosti) kliknite **Settings (Nastavitve)**.

Nastavitve

Določite lahko nastavitve za prilagajanje orodja HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools) po meri:

1. **Prompt to add logons for logon screens (Poziv za dodajanje prijav za prijavne zaslone)** – ikona orodja Password Manager (Upravitelj gesel) z znakom »+« se prikaže, ko je zaznan prijavni zaslon za spletno mesto ali program, in prikazuje, da v pomnilnik gesel lahko dodate prijavo za ta zaslon. To funkcijo onemogočite tako, da v pogovornem oknu **Icon Settings (Nastavitve ikone)** počistite potrditveno polje poleg možnosti **Prompt to add logons for logon screens (Poziv za dodajanje prijav za prijavne zaslone)**.
2. **Open Password Manager with ctrl+alt+H (Odpri upravitelja gesel s kombinacijo ctrl + alt + H)** – privzeta kombinacija bližnjičnih tipk za odpiranje hitrih povezav orodja Password Manager (Upravitelj gesel) je ctrl + alt + H. Če želite spremeniti kombinacijo bližnjičnih tipk, kliknite to možnost in vnesite novo kombinacijo tipk. Kombinacije lahko vsebujejo eno ali več od naslednjih možnosti: ctrl, alt ali shift in katera koli tipka črke ali številke.
3. Kliknite **Apply (Uporabi)**, da shranite spremembe.

Poverilnice

Poverilnice orodja Security Manager (Upravitelj varnosti) uporabljate, da potrdite svojo istovetnost. Lokalni skrbnik tega računalnika lahko nastavi poverilnice, ki se lahko uporabijo za dokazovanje identitete pri prijavi v račun Windows, spletna mesta ali programe.

Razpoložljive poverilnice so lahko različne, odvisno od varnostnih naprav, ki so vgrajene ali priključene v računalnik. Za vsako podprto poverilnico se bo ustvaril vnos v skupini **My Identity, Credentials (Moja identiteta, poverilnice)**.

Na seznamu so razpoložljive poverilnice, zahteve in trenutno stanje, ki lahko vsebujejo naslednje stvari:

- Prstni odtisi
- Geslo
- Pametna kartica

Če želite uveljaviti ali spremeniti poverilnico, kliknite povezavo in sledite navodilom na zaslonu.

Vaša osebna kartica ID

Vaša kartica ID vas identificira kot lastnika tega računa Windows in prikazuje vaše ime in sliko po vaši izbiri. Prikazana je v levem zgornjem kotu strani orodja Security Manager (Upravitelj varnosti) in kot pripomoček v stranski vrstici Windows Sidebar.

Če kliknete kartico ID v stranski vrstici Windows Sidebar, je to eden od načinov za hitri dostop do orodja Security Manager (Upravitelj varnosti).

Spremenite lahko sliko in način prikaza imena. Privzeto je, da je prikazano polno uporabniško ime za Windows in slika, ki ste jo izbrali med nastavitvijo Windows.

Prikazano ime spremenite tako:

1. Na nadzorni plošči orodja Security Manager (Upravitelj varnosti) kliknite možnost **ID Card (Kartica ID)** v levem zgornjem kotu.
2. Kliknite polje, v katerem je prikazano ime, ki ste ga vnesli za svoj račun v operacijskem sistemu Windows. Sistem bo prikazal vaše uporabniško ime Windows za ta račun.
3. Če želite spremeniti to ime, vnesite novo ime in nato kliknite gumb **Save (Shrani)**.

Prikazano sliko spremenite tako:

1. Na nadzorni plošči orodja Security Manager (Upravitelj varnosti) kliknite možnost **My Identity (Moja identiteta)** in nato v levem zgornjem kotu kliknite možnost **ID Card (Kartica ID)**.
2. Kliknite gumb **Choose picture (Izberi sliko)**, kliknite sliko in nato kliknite gumb **Save (Shrani)**.

Določanje nastavitev

Nastavitve za orodje HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools) lahko spremenite po meri. Na nadzorni plošči orodja Security Manager (Upravitelj varnosti) kliknite **Advanced (Napredno)** in nato **Preferences (Nastavitve)**. Razpoložljive nastavitve so prikazane na dveh karticah: General (Splošno) in Fingerprint (Prstni odtis).

General (Splošno)

Na kartici General (Splošno) so na voljo naslednje nastavitve:

Appearance – **Show icon on taskbar (Videz – prikaz ikone v opravilni vrstici)**

Če želite omogočiti prikaz ikone v opravilni vrstici, izberite potrditveno polje.

Če želite onemogočiti prikaz ikone v opravilni vrstici, počistite potrditveno polje.

Fingerprint (Prstni odtis)

Na kartici Fingerprint (prstni odtis) so na voljo naslednje nastavitve:

Quick Actions (Hitra dejanja) – uporabite to možnost, da izberete opravilo orodja Security Manager (Upravitelj varnosti), ki naj se izvede, ko pridržite določeno tipko med optičnim prebiranjem prstnega odtisa.

Če želite dodeliti hitro dejanje eni od naštetih tipk:

- Kliknite možnost **(Key)+Fingerprint ((Tipka)+prstni odtis)** in nato v meniju kliknite eno od razpoložljivih opravil.

Fingerprint Scan Feedback (Povratne informacije o optičnem prebiranju prstnega odtisa) – prikaže se le, ko je na voljo bralnik prstnih odtisov. Uporabite to nastavitev, da prilagodite povratne informacije, ki jih dobite, ko optično preberete prstni odtis.

- **Enable sound feedback (Omogoči zvočne povratne informacije)** – orodje Security Manager (Upravitelj varnosti) vam ponudi zvočne povratne informacije, ko je bil optično prebran prstni odtis; in sicer predvaja različne zvoke za določene dogodke programa. Prek kartice Sounds (Zvoki) na nadzorni plošči operacijskega sistema Windows lahko tem dogodkom dodelite nove zvoke ali onemogočite zvočne povratne informacije, če počistite to možnost.
- **Show scan quality feedback (Prikaži povratne informacije o kakovosti optičnega branja)** – privzeto je, da orodje Security Manager (Upravitelj varnosti) zaradi preverjanja pristnosti prikaže sliko prstnega odtisa, kadar koli je kakovost optičnega branja prstnega odtisa nezadovoljiva. Če počistite to možnost, onemogočite prikaz te slike.

Varnostno kopiranje in obnovitev podatkov

Priporočamo, da redno ustvarjate varnostne kopije podatkov orodja Security Manager (Upravitelj varnosti). Pogostnost izdelave varnostnih kopij je odvisna od tega, kako pogosto se podatki spreminjajo. Primer: če vsak dan dodajate nove prijave, bi bilo dobro, da vsak dan izdelujete tudi varnostne kopije podatkov.

Varnostne kopije lahko uporabljate tudi za prenašanje podatkov iz enega računalnika v drugega, imenovano tudi uvažanje in izvažanje.

OPOMBA: Ta funkcija izdeluje le varnostne kopije podatkov.

V vsak računalnik, ki bo prejel varnostne kopije podatkov, morate namestiti orodje HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools), da lahko obnovite podatke iz datoteke varnostne kopije.

Varnostne kopije podatkov izdelate tako:

1. V levem podoknu kliknite **Advanced (Napredno)** in nato **Backup and Restore (Varnostno kopiranje in obnovitev)**.
2. Kliknite **Back up data (Varnostno kopiranje podatkov)**.
3. Izberite module, ki jih želite vključiti v varnostno kopiranje. V večini primerov je najbolje, da izberete vse.
4. Vnesite ime za datoteko pomnilnika. Datoteka se bo privzeto shranila v mapo Documents (Dokumenti) Če želite določiti drugo lokacijo, kliknite **Browse (Prebrskaj)**.
5. Vnesite geslo, da zaščitite datoteko.
6. Potrdite svojo identiteto.
7. Kliknite **Finish (Dokončaj)**.

Podatke obnovite tako:

1. V levem podoknu kliknite **Advanced (Napredno)** in nato **Backup and Restore (Varnostno kopiranje in obnovitev)**.
2. Kliknite **Restore data (Obnovi podatke)**.
3. Izberite predhodno ustvarjeno datoteko za shranjevanje. Pot lahko vnesete v polje, ki je na voljo, ali pa kliknite **Edit (Uredi)**.

4. Vnesite geslo za zaščito datoteke.
5. Izberite module, katerih podatke želite obnoviti. V večini primerov boste izbrali vse naštete module.
6. Kliknite **Finish (Dokončaj)**.

Dodajanje aplikacij

Morda imate na voljo dodatne aplikacije, ki omogočajo nove funkcije za ta program.

Na nadzorni plošči orodja Security Manager (Upravitelj varnosti kliknite **[+] Discover more (Odkrij več)**, da poiščete dodatne aplikacije.

OPOMBA: Če v levem spodnjem delu nadzorne plošče ni povezave **[+] Discover more (Odkrij več)**, jo je onemogočil skrbnik računalnika.

Stanje varnostnih aplikacij

Na strani Security Manager Applications Status (Stanje aplikacij upravitelja varnosti) je prikazano celotno stanje nameščenih varnostnih aplikacij. Tam so prikazane nastavljene aplikacije in stanje nastavitve za vsako od njih. Povzetek se prikaže samodejno, ko odprete nadzorno ploščo orodja Security Manager (Upravitelj varnosti), ali ko kliknete **Security Applications (Varnostne aplikacije)**.

7 Drive Encryption za HP ProtectTools (samo pri izbranih modelih)

△ **POZOR:** Če se odločite, da boste odstranili modul Drive Encryption (Šifriranje pogonov), morate najprej dešifrirati vse šifrirane pogone. Če tega ne storite, ne boste mogli dostopati do podatkov na šifriranih pogonih, razen če se niste prijavili v storitev za obnovitev šifriranja pogonov. S ponovno namestitvijo modula Drive Encryption (Šifriranje pogonov) dostop do šifriranih pogonov ne bo omogočen.

Modul Drive Encryption for HP ProtectTools (Šifriranje pogonov za HP ProtectTools) ponuja celovito zaščito podatkov, tako da šifrira trdi disk vašega računalnika. Ko je šifriranje pogonov aktivirano, se morate prijaviti na prijavnem zaslonu modula Drive Encryption (Šifriranje pogonov), ki se odpre pred zagonom operacijskega sistema Windows®.

Čarovnik za nastavitev HP ProtectTools Setup Wizard omogoča skrbnikom operacijskega sistema Windows, da aktivirajo šifriranje pogonov, izdelajo varnostno kopijo ključa za šifriranje, dodajajo in odstranjujejo uporabnike in deaktivirajo šifriranje pogonov. Dodatne informacije poiščite v pomoči za programsko opremo HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).

Z modulom Drive Encryption (Šifriranje pogonov) lahko izvajate naslednja opravila:

- upravljanje šifriranja
  - šifriranje in dešifriranje posameznih pogonov

    OPOMBA: šifrirate lahko samo notranje trde diske.
- obnovitev
  - izdelavo varnostnih kopij ključev
  - obnovitev

Nastavitev

Odpiranje modula Drive Encryption (Šifriranje pogonov)

1. Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools)**.
2. V levem podoknu kliknite **Drive Encryption (Šifriranje pogonov)**.

Splošna opravila

Aktiviranje orodja Drive Encryption (Šifriranje pogonov)

Drive Encryption (Šifriranje pogonov) aktivirate s čarovnikom HP ProtectTools Setup Wizard.

OPOMBA: S tem čarovnikom lahko tudi dodajate in odstranjujete uporabnike.

– ali –

1. Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools)**.
2. V levem podoknu kliknite **Security (Varnost)**, nato pa kliknite **Features (Funkcije)**.
3. Izberite potrditveno polje **Drive Encryption (Šifriranje pogonov)** in nato kliknite **Next (Naprej)**.
4. V možnosti **Drives to be encrypted (Pogoni za šifriranje)** označite potrditveno polje za trdi disk, ki ga želite šifrirati.
5. Pomnilniško napravo vstavite v ustrezno režo.

   OPOMBA: Če želite shraniti ključ šifriranja, morate uporabljati pomnilniško napravo USB s formatom FAT32.

6. V možnosti **External storage device on which to save encryption key (Zunanja pomnilniška naprava za shranjevanje ključa za šifriranje)** označite potrditveno polje za pomnilniško napravo, kamor boste shranili ključ za šifriranje).
7. Kliknite **Apply (Uporabi)**.

   Šifriranje pogona se začne.

Dodatne informacije poiščite v pomoči za programsko opremo HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).

Deaktiviranje orodja Drive Encryption (Šifriranje pogonov)

Drive Encryption (Šifriranje pogonov) deaktivirate s čarovnikom HP ProtectTools Setup Wizard. Dodatne informacije poiščite v pomoči za programsko opremo HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools).

– ali –

1. Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools)**.
2. V levem podoknu kliknite **Security (Varnost)**, nato pa kliknite **Features (Funkcije)**.
3. Počistite potrditveno polje **Drive Encryption (Šifriranje pogonov)** in nato kliknite **Apply (Uporabi)**.

   Dešifriranje pogona se začne.

Prijava po aktivaciji orodja Drive Encryption (Šifriranje pogonov)

Ko po aktivaciji orodja Drive Encryption (Šifriranje pogonov) in vpisu uporabniškega računa zaženete računalnik, se morate prijaviti na zaslonu za prijavo v orodje Drive Encryption (Šifriranje pogonov):

OPOMBA: Če je skrbnik za Windows v upravitelju varnosti HP ProtectTools Security Manager omogočil varnost pred zagonom Pre-boot Security, se boste prijavili takoj po zagonu računalnika in ne prek zaslona za prijavo v orodje Drive Encryption (Šifriranje pogonov).

1. Kliknite svoje uporabniško ime in nato vnesite geslo za Windows ali kodo PIN kartice Java™ ali pa uporabite registrirani prst.
2. Kliknite **OK (V redu)**.

OPOMBA: Če se na zaslonu za prijavo v orodje Drive Encryption (Šifriranje pogonov) prijavite z obnovitvenim ključem, boste pozvani tudi, da izberete svoje uporabniško ime za Windows in na zaslonu za prijavo v sistem Windows vnesete še svoje geslo.

Zaščita podatkov s šifriranjem trdega diska

Za zaščito podatkov s šifriranjem trdega diska uporabite čarovnik HP ProtectTools Setup Wizard:

1. V orodju Security Manager (Upravitelj varnosti) kliknite **Getting Started (Prvi koraki)** in nato kliknite ikono **Security Manager Setup (Nastavitev upravitelja varnosti)**. Začne se predstavitev, ki opisuje funkcije orodja Security Manager (Upravitelj varnosti). (Orodje Security Manager (Upravitelj varnosti) lahko zaženete tudi s strani »Drive Encryption« (Šifriranje pogonov).)
2. V levem podoknu kliknite **Drive Encryption (Šifriranje pogonov)**, nato pa kliknite **Encryption Management (Upravljanje šifriranja)**.
3. Kliknite **Change Encryption (Spremeni šifriranje)**.
4. Izberite pogon ali pogone, ki jih boste šifrirali.

OPOMBA: Šifriranje trdega diska vam toplo priporočamo.

Prikaz stanja šifriranja

Uporabniki lahko z orodjem HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools) prikažejo stanje šifriranja.

OPOMBA: Spremembe stanja šifriranja pogonov morate narediti s konzolo HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools).

1. Odprite orodje **HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools**.
2. V možnosti **My Data (Moji podatki)** kliknite **Encryption Status (Stanje šifriranja)**.

   Če je šifriranje pogonov aktivno, stanje pogonov prikaže eno od naslednjih šifer stanja:

   - Active (Aktivno)
   - Inactive (Neaktivno)
   - Not encrypted (Ni šifrirano)
   - Encrypted (Šifrirano)

- Encrypting (Poteka šifriranje)
- Decrypting (Poteka dešifriranje)

Če se trdi disk pravkar šifrira ali dešifrira, se v kazalniku poteka prikaže odstotek dokončanosti in čas do dokončanja šifriranja ali dešifriranja.

Napredna opravila

Upravljanje orodja Drive Encryption (Šifriranje pogonov) (skrbniško opravilo)

Na strani »Encryption Management« (Upravljanje šifriranja) si lahko skrbniki ogledajo in spreminjajo stanje orodja Drive Encryption (Šifriranje pogonov) (dejavno ali nedejavno) ter preverijo stanje šifriranja vseh trdih diskov v računalniku.

- Če je stanje »Inactive« (Neaktivno), skrbnik za Windows še ni aktiviral orodja Drive Encryption (Šifriranje pogonov) v orodju HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools), in trdi disk ni zaščiten. Drive Encryption (Šifriranje pogonov) aktivirate s čarovnikom za namestitev upravitelja varnosti HP ProtectTools Security Manager.
- Če je stanje »Active« (Aktivno), je bilo orodje Drive Encryption (Šifriranje pogonov) aktivirano in konfigurirano. Pogon je v enem od naslednjih stanj:
  - Not encrypted (Ni šifrirano)
  - Encrypted (Šifrirano)
  - Encrypting (Poteka šifriranje)
  - Decrypting (Poteka dešifriranje)

Šifriranje in dešifriranje posameznih pogonov

Če želite šifrirati enega ali več trdih diskov v računalniku ali dešifrirati pogon, ki ste ga že šifrirali, uporabite funkcijo Change Encryption (Spremeni šifriranje):

1. Odprite konzolo **HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools)**, kliknite **Drive Encryption (Šifriranje pogonov)** in nato **Encryption Management (Upravljanje šifriranja)**.
2. Kliknite **Change Encryption (Spremeni šifriranje)**.
3. V pogovornem oknu Change Encryption (Spremeni šifriranje) potrdite ali počistite potrditveno polje ob pogonih, ki jih želite šifrirati ali dešifrirati, in nato kliknite **OK (V redu)**.

OPOMBA: Med šifriranjem ali dešifriranjem pogona je v kazalniku poteka prikazan čas, potreben za dokončanje trenutnega opravila. Če računalnik med šifriranjem izklopite ali preklopite v stanje pripravljenosti ali mirovanja in ga nato ponovno vklopite, prikaz časa do dokončanja opravila skoči na začetek, dejansko šifriranje pa se začne izvajati tam, kjer se je ustavilo. Prikaz preostalega časa in poteka se bo spreminjal hitreje in tako prikazal tudi že dokončani del opravila.

Varnostno kopiranje in obnovitev (skrbniško opravilo)

Na strani »Recovery« (Obnovitev) lahko skrbniki za Windows varnostno kopirajo in obnavljajo ključe za šifriranje.

Local Drive Encryption Key Backup (Varnostno kopiranje ključa za šifriranje lokalnega pogona) – omogoča varnostno kopiranje ključev za šifriranje v odstranljive medije, ko je aktivirano orodje Drive Encryption (Šifriranje pogonov).

Izdelava varnostnih kopij ključev

Ključ za šifriranje za šifrirani pogon lahko varnostno kopirate v odstranljivo pomnilniško napravo:

△ **POZOR:** Napravo za shranjevanje z varnostno kopijo ključa hranite na varnem mestu, saj v primeru, da pozabite svoje geslo ali izgubite kartico Java, ta predstavlja edini dostop do trdega diska.

1. Odprite konzolo **HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools**, kliknite **Drive Encryption (Šifriranje pogonov)** in nato **Recovery (Obnovitev)**.
2. Kliknite **Backup Keys (Varnostne kopije ključev)**.
3. Na strani »Select Backup Disk« (Izberite ploščo za varnostno kopiranje) označite potrditveno polje za napravo, v katero želite shraniti varnostno kopijo ključa za šifriranje, in nato kliknite **Next (Naprej)**.
4. Preberite informacije na naslednji strani in kliknite **Next (Naprej)**. Šifrirni ključ se shrani v izbrano napravo za shranjevanje.
5. Ko se odpre potrditveno pogovorno okno, kliknite **Finish (Dokončaj)**.

Obnovitev

Če ste pozabili geslo in želite izvesti obnovitev, sledite tem korakom:

1. Vklopite računalnik.
2. Vstavite izmenljivo napravo za shranjevanje, v kateri je shranjena varnostna kopija ključa.
3. Ko se odpre pogovorno okno za prijavo v orodje Drive Encryption (Šifriranje pogonov) za HP ProtectTools, kliknite **Cancel (Prekliči)**.
4. V spodnjem levem kotu zaslona kliknite **Options (Možnosti)** in nato **Recovery (Obnovitev)**.
5. Izberite datoteko, v kateri je varnostna kopija ključa, ali kliknite **Browse (Prebrskaj)**, da jo poiščete, in nato kliknite **Next (Naprej)**.
6. Ko se odpre potrditveno pogovorno okno, kliknite **OK (V redu)**.

   Računalnik se zažene.

OPOMBA: Priporočljivo je, da po obnovitvi ponastavite svoje geslo.

8 Privacy Manager za HP ProtectTools (samo pri izbranih modelih)

Upravitelj zasebnosti Privacy Manager za HP ProtectTools omogoča napredne načine varne prijave (preverjanja pristnosti), s katerimi se preveri vir, neokrnjenost in varnost povezave pri uporabi e-pošte, dokumentov Microsoft® Office ali izmenjavi neposrednih sporočil (IM).

Privacy Manager (Upravitelj zasebnosti) uporablja varnostno infrastrukturo, ki jo zagotavlja upravitelj varnosti HP ProtectTools Security Manager, ki omogoča naslednje načine varne prijave:

- Preverjanje pristnosti s prstnimi odtisi
- Geslo za Windows®
- Kartica HP ProtectTools Java™

Za prijavo v upravitelja zasebnosti Privacy Manager lahko uporabite katerega koli od zgoraj omenjenih načinov.

Za orodje Privacy Manager (Upravitelj zasebnosti) potrebujete:

- Orodje HP ProtectTools Security Manager različice 5.00 ali novejše
- Operacijski sistem Windows® 7, Windows Vista® ali Windows XP
- Microsoft Outlook 2007 ali Microsoft Outlook 2003
- Veljaven e-poštni račun

OPOMBA: Preden lahko dostopate do varnostnih funkcij, morate v orodju Privacy Manager (Upravitelj zasebnosti) zahtevati in namestiti certifikat upravitelja zasebnosti (digitalni certifikat). Informacije o zahtevanju certifikata orodja Privacy Manager (Upravitelj zasebnosti) najdete v razdelku Zahteva za potrdilo orodja Privacy Manager (Upravitelj zasebnosti) in njegova namestitev na strani 44.

Nastavitev

Odpiranje orodja Privacy Manager (Upravitelj zasebnosti)

Orodje Privacy Manager (Upravitelj zasebnosti) odprete tako:

1. Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools)**.
2. Kliknite **Privacy Manager (Upravitelj zasebnosti)**:

– ali –

V področju za obvestila na skrajni desni strani opravilne vrstice z desno miškino tipko kliknite ikono **HP ProtectTools**, možnost **Privacy Manager (Upravitelj zasebnosti)** in nato kliknite možnost **Configuration (Konfiguracija)**.

– ali –

V orodni vrstici e-poštnega sporočila programa Microsoft Outlook kliknite navzdol obrnjeno puščico ob napisu **Send Securely (Varno pošiljanje)** in kliknite možnost **Certificates (Potrdila)** ali **Trusted Contacts Manager (Zaupni stiki)**.

– ali –

V orodni vrstici dokumenta Microsoft Office kliknite navzdol obrnjeno puščico ob napisu **Sign and Encrypt (Podpiši in šifriraj)** in kliknite možnost **Certificates (Potrdila)** ali **Trusted Contacts (Zaupni stiki)**.

Upravljanje potrdil orodja Privacy Manager (Upravitelj zasebnosti)

Potrdila orodja Privacy Manager (Upravitelj zasebnosti) s šifrirno tehnologijo, ki se imenuje infrastruktura javnih ključev (PKI), varujejo podatke in sporočila. PKI od uporabnikov zahteva, da pridobijo šifrirne ključe in potrdilo orodja Privacy Manager (Upravitelj zasebnosti), ki ga izda overitelj potrdil (CA). V nasprotju z večino postopkov šifriranja podatkov in programske opreme za preverjanje pristnosti, ki zahteva le občasno preverjanje pristnosti, orodje Privacy Manager (Upravitelj zasebnosti) preveri pristnost uporabnika vsakič, ko s šifrirnim ključem podpišete e-poštno sporočilo ali dokument Microsoft Office. Tako je shranjevanje in pošiljanje pomembnih podatkov varno.

Izvajate lahko naslednja opravila:

- Zahteva za potrdilo upravitelja zasebnosti Privacy Manager in njegova namestitev
- Ogled podrobnosti potrdila orodja Privacy Manager (Upravitelj zasebnosti)
- Obnovitev potrdil orodja Privacy Manager (Upravitelj zasebnosti)
- Ko je na voljo več potrdil, nastavite privzeto potrdilo orodja Privacy Manager (Upravitelj zasebnosti), ki naj ga uporablja to orodje.
- Izbris in preklic potrdila orodja Privacy Manager (Upravitelj zasebnosti) (napredno)

Zahteva za potrdilo orodja Privacy Manager (Upravitelj zasebnosti) in njegova namestitev

Če želite uporabljati funkcije orodja Privacy Manager (Upravitelj zasebnosti), morate znotraj njega z veljavnim e-poštnim naslovom poslati zahtevo za potrdilo in potrdilo nato tudi namestiti. E-poštni naslov

mora biti nastavljen kot račun znotraj programa Microsoft Outlook v istem računalniku, iz katerega pošljete zahtevo za potrdilo orodja Privacy Manager (Upravitelj zasebnosti).

Zahteva za potrdilo orodja Privacy Manager (Upravitelj zasebnosti)

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Certificates (Potrdila)**.
2. Kliknite možnost **Request a Privacy Manager certificate (Zahteva za potrdilo upravitelja zasebnosti)**.
3. Na pozdravni strani preberite besedilo in kliknite **Next (Naprej)**.
4. Na strani »License Agreement« (Licenčna pogodba) preberite licenčno pogodbo.
5. Potrdite polje ob napisu **Check here to accept the terms of this license agreement (Potrdite to polje, da sprejmete pogoje licenčne pogodbe)**, nato pa kliknite **Next (Naprej)**.
6. Na strani »Your Certificate Details« (Podrobnosti potrdila) vnesite zahtevane podatke o potrdilu in kliknite **Next (Naprej)**.
7. Na strani »Certificate Request Accepted« (Zahteva za potrdilo sprejeta) kliknite **Finish (Dokončaj)**.
8. Kliknite **OK (V redu)**, da zaprete potrdilo.

V programu Microsoft Outlook boste prejeli e-poštno sporočilo s pripetim potrdilom orodja Privacy Manager (Upravitelj zasebnosti).

Pridobitev predhodno dodeljenega poslovnega potrdila orodja Privacy Manager (Upravitelj zasebnosti)

1. V programu Outlook odprite e-poštno sporočilo, ki ste ga prejeli in ki govori o tem, da vam je bilo predhodno dodeljeno poslovno potrdilo.
2. Kliknite **Obtain (Pridobi)**.
3. V programu Microsoft Outlook boste prejeli e-poštno sporočilo s pripetim potrdilom orodja Privacy Manager (Upravitelj zasebnosti).
4. Za namestitev potrdila glejte razdelek Nameščanje potrdila orodja Privacy Manager (Upravitelj zasebnosti) na strani 45

Nameščanje potrdila orodja Privacy Manager (Upravitelj zasebnosti)

1. Ko prejmete e-poštno sporočilo s pripetim potrdilom orodja Privacy Manager (Upravitelj zasebnosti), ga odprite in v spodnjem desnem kotu sporočila v programu Outlook 2007 ali v zgornjem levem kotu v programu Outlook 2003 kliknite gumb **Setup (Namestitev)**.
2. Potrdite pristnost s svojim načinom za varno prijavo.
3. Na strani »Certificate Installed« (Potrdilo je nameščeno) kliknite **Next (Naprej)**.
4. Na strani »Certificate Backup« (Varnostna kopija potrdila) vnesite mesto in ime za varnostno datoteko ter kliknite **Browse (Prebrskaj)**, da poiščete mesto zanjo.

△ **POZOR:** Datoteko shranite na katero koli varno mesto, razen na trdi disk. Datoteka je namenjena samo vaši uporabi in jo potrebujete v primeru, da boste morali obnoviti potrdilo orodja Privacy Manager (Upravitelj zasebnosti) in povezanih ključev.

5. Vnesite geslo in ga potrdite ter nato kliknite **Next (Naprej)**.
6. Potrdite pristnost s svojim načinom za varno prijavo.
7. Če se odločite, da boste začeli postopek pošiljanja povabil zaupnim virom, sledite navodilom na zaslonu; začnite pri 2. koraku v razdelku Dodajanje zaupnih stikov s stiki programa Microsoft Outlook na strani 49.

   – ali –

   Če kliknete **Cancel (Prekliči)**, preberite razdelek Dodajanje zaupnega stika na strani 48 za informacije o dodajanju zaupnega stika pozneje.

Ogled podrobnosti potrdila orodja Privacy Manager (Upravitelj zasebnosti)

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Certificates (Potrdila)**.
2. Kliknite Privacy Manager Certificate (Potrdilo upravitelja zasebnosti).
3. Kliknite **Certificate details (Podrobnosti o potrdilu)**.
4. Ko si podrobnosti ogledate, kliknite **OK (V redu)**.

Obnovitev potrdila orodja Privacy Manager (Upravitelj zasebnosti)

Ko se bo potrdilu orodja Privacy Manager (Upravitelj zasebnosti) bližal iztek roka trajanja, boste dobili obvestilo, da ga je treba obnoviti:

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Certificates (Potrdila)**.
2. Kliknite **Renew certificate (Obnovi potrdilo)**.
3. Novo potrdilo kupite tako, da sledite navodilom na zaslonu.

OPOMBA: Z obnovitvenim postopkom potrdila ne zamenjate starega potrdila. Morali boste kupiti novo potrdilo in ga namestiti po enakem postopku, kot je opisan v razdelku Zahteva za potrdilo orodja Privacy Manager (Upravitelj zasebnosti) in njegova namestitev na strani 44.

Nastavitev privzetega potrdila orodja Privacy Manager (Upravitelj zasebnosti)

Znotraj orodja Privacy Manager (Upravitelj zasebnosti) so vidna le njegova potrdila, tudi če so v vašem računalniku nameščena potrdila drugih overiteljev potrdil.

Če imate v računalniku več potrdil orodja Privacy Manager (Upravitelj zasebnosti), ki so bila nameščena tem orodju, lahko enega določite kot privzetega:

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Certificates (Potrdila)**.
2. Kliknite potrdilo orodja Privacy Manager (Upravitelj zasebnosti), ki ga želite uporabiti kot privzetega, nato pa kliknite **Set default (Nastavi kot privzeto)**.
3. Kliknite **OK (V redu)**.

OPOMBA: Ni vam treba uporabiti privzetega potrdila orodja Privacy Manager (Upravitelj zasebnosti). V različnih funkcijah orodja Privacy Manager (Upravitelj zasebnosti) lahko izberete katero koli potrdilo.

Brisanje potrdila orodja Privacy Manager (Upravitelj zasebnosti)

Če potrdilo orodja Privacy Manager (Upravitelj zasebnosti) izbrišete, ne boste mogli odpirati datotek in si ogledovati podatkov, ki ste jih šifrirali s tem potrdilom. Če ste potrdilo pomotoma izbrisali, ga lahko obnovite z varnostno datoteko, ki ste jo ustvarili med namestitvijo potrdila. Če vas zanima več o tem, preberite Obnovitev potrdila orodja Privacy Manager (Upravitelj zasebnosti) na strani 47.

Potrdilo orodja Privacy Manager (Upravitelj zasebnosti) izbrišete tako:

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Certificates (Potrdila)**.
2. Kliknite potrdilo orodja Privacy Manager (Upravitelj zasebnosti), ki ga želite izbrisati, in kliknite **Advanced (Napredno)**.
3. Kliknite **Delete (Izbriši)**.
4. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.
5. Kliknite **Close (Zapri)** in nato **Apply (Uporabi)**.

Obnovitev potrdila orodja Privacy Manager (Upravitelj zasebnosti)

Med nameščanjem potrdila orodja Privacy Manager (Upravitelj zasebnosti) morate ustvariti varnostno kopijo potrdila. Varnostno kopijo lahko izdelate tudi na strani Migration (Migracija). To varnostno kopijo lahko uporabljate pri selitvi v drug računalnik ali za obnovitev potrdila v istem računalniku.

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Migration (Migracija)**.
2. Kliknite **Restore (Obnovi)**.
3. Na strani »Migration File« (Datoteka za migracijo) kliknite **Browse (Prebrskaj)**, da poiščete datoteko .dppsm, ki ste jo ustvarili med varnostnim kopiranjem, in nato kliknite **Next (Naprej)**.
4. Vnesite geslo, ki ste ga uporabili pri varnostnem kopiranju, in kliknite **Next (Naprej)**.
5. Kliknite **Finish (Dokončaj)**.
6. Kliknite **OK (V redu)**.

Za več informacij glejte razdelka Nameščanje potrdila orodja Privacy Manager (Upravitelj zasebnosti) na strani 45 ali Varnostno kopiranje potrdil orodja Privacy Manager (Upravitelj zasebnosti) in zaupnih stikov na strani 63.

Preklic potrdila orodja Privacy Manager (Upravitelj zasebnosti)

Če se vam zdi, da je bila varnost potrdila orodja Privacy Manager (Upravitelj zasebnosti) ogrožena, lahko potrdilo prekličete:

OPOMBA: Preklicano potrdilo se ne izbriše. Še vedno ga lahko uporabite za ogledovanje šifriranih datotek.

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Certificates (Potrdila)**.
2. Kliknite **Advanced (Napredno)**.
3. Kliknite potrdilo orodja Privacy Manager (Upravitelj zasebnosti), ki ga želite preklicati, in nato **Revoke (Prekliči)**.
4. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

5. Potrdite pristnost s svojim načinom za varno prijavo.
6. Sledite navodilom na zaslonu.

Upravljanje zaupnih stikov

Zaupni stiki (Trusted Contacts) so uporabniki, s katerimi ste izmenjali potrdila orodja Privacy Manager (Upravitelj zasebnosti), s čimer ste omogočili varno komunikacijo.

Orodje Trusted Contacts Manager (Upravitelj zaupnih stikov) vam omogoča izvajanje naslednjih opravil:

- Ogledovanje podrobnosti o zaupnem stiku
- Brisanje zaupnih stikov
- Preverjanje stanja preklica za zaupne stike (napredno)

Dodajanje zaupnih stikov

Postopek dodajanja zaupnih stikov ima 3 korake:

1. Prejemniku zaupnega stika pošljete e-poštno povabilo.
2. Prejemnik se odzove na e-poštno povabilo.
3. Od prejemnika zaupnega stika ste prejeli odgovor. Kliknite **Accept (Sprejmi)**.

E-poštno povabilo za zaupne stike lahko pošljete posameznemu prejemniku ali pa vsem stikom v svojem adresarju programa Microsoft Outlook.

Za dodajanje zaupnih stikov glejte razdelke v nadaljevanju.

OPOMBA: Prejemniki povabila zaupnega stika morajo imeti nameščeno orodje Privacy Manager (Upravitelj zasebnosti) ali kakšno drugo orodje, da bodo lahko odgovorili na vaše povabilo. Informacije o nameščanju nadomestnega orodja najdete na spletnem mestu DigitalPersona na naslovu http://DigitalPersona.com/PrivacyManager.

Dodajanje zaupnega stika

1. Odprite modul Privacy Manager (Upravitelj zasebnosti), kliknite **Trusted Contacts Manager (Upravitelj zaupnih stikov)** in nato **Invite Contacts (Povabi stike)**.

   – ali –

   V programu Microsoft Outlook v orodni vrstici kliknite navzdol obrnjeno puščico ob napisu **Send Securely (Varno pošiljanje)** in nato **Invite Contacts (Povabi stike)**.

2. Če se odpre pogovorno okno za izbiranje potrdila Select Certificate, kliknite potrdilo upravitelja zasebnosti Privacy Manager, ki ga želite uporabiti, nato pa kliknite **OK (V redu)**.
3. Ko se odpre pogovorno okno za povabilo zaupnim stikom Trusted Contact Invitation, kliknite **OK (V redu)**.

   E-poštno sporočilo se samodejno ustvari.

4. Vnesite enega ali več e-poštnih naslovov prejemnikov, ki jih želite dodati kot zaupne stike.
5. Uredite besedilo in se podpišite (izbirno).

6. Kliknite **Send (Pošlji)**.

OPOMBA: Če nimate potrdila orodja Privacy Manager (Upravitelj zasebnosti), se prikaže sporočilo, ki vas obvesti, da morate imeti potrdilo tega orodja, če želite poslati zahtevo za zaupni stik. Kliknite **OK (V redu)**, da zaženete čarovnika za zahtevo za potrdilo Certificate Request Wizard. Če vas zanima več o tem, preberite Zahteva za potrdilo orodja Privacy Manager (Upravitelj zasebnosti) in njegova namestitev na strani 44.

7. Potrdite pristnost s svojim načinom za varno prijavo.

OPOMBA: Ko prejemnik zahteve za zaupni stik prejme e-poštno sporočilo, ga mora odpreti, v spodnjem desnem kotu sporočila klikniti možnost **Accept (Sprejmi)** in, ko se odpre potrditveno pogovorno okno, klikniti **OK (V redu)**.

8. Ko prejmete odgovor na e-poštno sporočilo prejemnika, ki je sprejel povabilo, da postane zaupni stik, v spodnjem desnem kotu sporočila kliknite možnost **Accept (Sprejmi)**.

   Odpre se pogovorno okno z obvestilom o tem, da je bil prejemnik uspešno dodan na vaš seznam Trusted Contacts (Zaupni stiki).

9. Kliknite **OK (V redu)**.

Dodajanje zaupnih stikov s stiki programa Microsoft Outlook

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti), kliknite **Trusted Contacts Manager (Upravitelj zaupnih stikov)** in nato **Invite Contacts (Povabi stike)**.

   – ali –

   V programu Microsoft Outlook v orodni vrstici kliknite navzdol obrnjeno puščico ob napisu **Send Securely (Varno pošiljanje)** in nato **Invite All My Outlook Contacts (Povabi vse Outlookove stike)**.

2. Ko se odpre stran »Trusted Contact Invitation« (Povabilo zaupnih stikov), izberite e-poštne naslove prejemnikov, ki jih želite dodati kot zaupne stike, in kliknite **Next (Naprej)**.

3. Ko se odpre stran »Sending Invitation« (Pošiljanje povabila), kliknite **Finish (Dokončaj)**.

   E-poštno sporočilo z izbranimi e-poštnimi naslovi iz programa Microsoft Outlook se samodejno ustvari.

4. Uredite besedilo in se podpišite (izbirno).

5. Kliknite **Send (Pošlji)**.

OPOMBA: Če nimate potrdila orodja Privacy Manager (Upravitelj zasebnosti), se prikaže sporočilo, ki vas obvesti, da morate imeti potrdilo tega orodja, če želite poslati zahtevo za zaupni stik. Kliknite **OK (V redu)**, da zaženete čarovnika za zahtevo za potrdilo Certificate Request Wizard. Če vas zanima več o tem, preberite Zahteva za potrdilo orodja Privacy Manager (Upravitelj zasebnosti) in njegova namestitev na strani 44.

6. Potrdite pristnost s svojim načinom za varno prijavo.

OPOMBA: Ko prejemnik zahteve za zaupni stik prejme e-poštno sporočilo, ga mora odpreti, v spodnjem desnem kotu sporočila klikniti možnost **Accept (Sprejmi)** in, ko se odpre potrditveno pogovorno okno, klikniti **OK (V redu)**.

7. Ko prejmete odgovor na e-poštno sporočilo prejemnika, ki je sprejel povabilo, da postane zaupni stik, v spodnjem desnem kotu sporočila kliknite možnost **Accept (Sprejmi)**.

Odpre se pogovorno okno z obvestilom o tem, da je bil prejemnik uspešno dodan na vaš seznam Trusted Contacts (Zaupni stiki).

8. Kliknite **OK (V redu)**.

Ogled podrobnosti o zaupnem stiku

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Trusted Contacts (Zaupni stiki)**.
2. Kliknite zaupni stik.
3. Kliknite **Contact details (Podrobnosti o stiku)**.
4. Ko si podrobnosti ogledate, kliknite **OK (V redu)**.

Brisanje zaupnega stika

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Trusted Contacts (Zaupni stiki)**.
2. Kliknite zaupni stik, ki ga želite izbrisati.
3. Kliknite **Delete contact (Izbriši stik)**.
4. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

Preverjanje stanja preklicev zaupnih stikov

Če si želite ogledati, ali je zaupni stik preklical potrdilo orodja Privacy Manager (Upravitelj zasebnosti):

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Trusted Contacts (Zaupni stiki)**.
2. Kliknite zaupni stik.
3. Kliknite gumb **Advanced (Napredno)**.

   Odpre se pogovorno okno Advanced Trusted Contact Management (Napredno upravljanje zaupnih stikov).
4. Kliknite **Check Revocation (Preveri preklic)**.
5. Kliknite **Close (Zapri)**.

Splošna opravila

Orodje Privacy Manager (Upravitelj zasebnosti) lahko uporabljate z naslednjimi izdelki Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Uporaba orodja Privacy Manager (Upravitelj zasebnosti) v programu Microsoft Outlook

Ko je orodje Privacy Manager (Upravitelj zasebnosti) nameščeno, se v orodni vrstici programa Microsoft Outlook prikaže gumb Privacy (Zasebnost), v orodni vrstici vsakega e-poštnega sporočila pa gumb Send Securely (Varno pošiljanje). Ko kliknete navzdol obrnjeno puščico poleg gumba **Privacy (Zasebnost)** ali **Send Securely (Varno pošiljanje)**, lahko izbirate med naslednjimi možnostmi:

- Sign and Send (Podpiši in pošlji) (Samo gumb Send Securely (Varno pošiljanje)) – ta možnost e-poštnemu sporočilu doda digitalni podpis in ga pošlje, ko preverite pristnost z izbranim načinom varne prijave.
- Seal for Trusted Contacts and Send (Zapečati za zaupne stike in pošlji) (Samo gumb Send Securely (Varno pošiljanje)) – ta možnost doda digitalni podpis, šifrira e-poštno sporočilo in ga pošlje, ko preverite pristnost z izbranim načinom varne prijave.
- Invite Contacts (Povabi stike) – ta možnost vam omogoča pošiljanje vabil za zaupne stike. Če vas zanima več o tem, preberite Dodajanje zaupnega stika na strani 48.
- Invite Outlook Contacts (Povabi stike v programu Outlook) – ta možnost vam omogoča pošiljanje vabil za zaupne stike vsem stikom v adresarju programa Outlook. Če vas zanima več o tem, preberite Dodajanje zaupnih stikov s stiki programa Microsoft Outlook na strani 49.
- Open the Privacy Manager software (Odpri programsko opremo upravitelja zasebnosti) – možnosti potrdil, zaupnih stikov in nastavitev vam omogočajo odpiranje programske opreme orodja Privacy Manager (Upravitelj zasebnosti), da dodate, si ogledate ali spremenite trenutne nastavitve. Če vas zanima več o tem, preberite Konfiguriranje orodja Privacy Manager (Upravitelj zasebnosti) za program Microsoft Outlook na strani 51.

Konfiguriranje orodja Privacy Manager (Upravitelj zasebnosti) za program Microsoft Outlook

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti), kliknite **Settings (Nastavitve)** in nato jeziček **E-mail (E-pošta)**.

   – ali –

   V glavni orodni vrstici programa Microsoft Outlook kliknite navzdol obrnjeno puščico ob napisu **Send Securely (Varno pošiljanje)** (**Privacy (Zasebnost)** v programu Outlook 2003) in nato možnost **Settings (Nastavitve)**.

   – ali –

   V orodni vrstici e-poštnega sporočila kliknite navzdol obrnjeno puščico ob napisu **Send Securely (Varno pošiljanje)** in nato možnost **Settings (Nastavitve)**.

2. Izberite opravila, ki jih želite izvesti pri pošiljanju varne e-pošte, in nato kliknite **OK (V redu)**.

Podpisovanje in pošiljanje e-poštnega sporočila

1. V programu Microsoft Outlook kliknite **New (Novo)** ali **Reply (Odgovori)**.
2. Vnesite svoje sporočilo.
3. Kliknite navzdol obrnjeno puščico ob napisu **Send Securely (Varno pošiljanje)** (**Privacy (Zasebnost)** v programu Outlook 2003) in nato **Sign and Send (Podpiši in pošlji)**.
4. Potrdite pristnost s svojim načinom za varno prijavo.

Zapečatenje in pošiljanje e-poštnega sporočila

Zapečatena e-poštna sporočila, ki imajo digitalni podpis in so zapečatena (šifrirana), si lahko ogledajo le tisti, ki jih izberete s seznama z zaupnimi stiki.

E-poštno sporočilo zapečatite in pošljete zaupnemu stiku tako:

1. V programu Microsoft Outlook kliknite **New (Novo)** ali **Reply (Odgovori)**.
2. Vnesite svoje sporočilo.
3. Kliknite navzdol obrnjeno puščico ob napisu **Send Securely (Varno pošiljanje)** (**Privacy (Zasebnost)** v programu Outlook 2003) in nato **Seal for Trusted Contacts and Send (Zapečati za zaupne stike in pošlji)**.
4. Potrdite pristnost s svojim načinom za varno prijavo.

Ogled zapečatenega e-poštnega sporočila

Ko odprete zapečateno e-poštno sporočilo, so v naslovu e-pošte izpisani varnostni podatki. Na varnostni oznaki so podatki o:

- poverilnicah, uporabljenih za preverjanje identitete osebe, ki je podpisala e-poštno sporočilo, in
- izdelku, uporabljenem za preverjanje poverilnic osebe, ki je podpisala e-poštno sporočilo.

Uporaba orodja Privacy Manager (Upravitelj zasebnosti) v dokumentu Microsoft Office 2007

OPOMBA: Orodje Privacy Manager (Upravitelj zasebnosti) lahko uporabljate le z dokumenti Microsoft Office 2007

Ko namestite potrdilo orodja Privacy Manager (Upravitelj zasebnosti), se na desni strani orodne vrstice vseh dokumentov Microsoft Word, Microsoft Excel in Microsoft PowerPoint prikaže gumb Sign and Encrypt (Podpiši in šifriraj). Ko kliknete navzdol obrnjeno puščico poleg gumba **Sign and Encrypt (Podpiši in šifriraj)**, lahko izbirate med naslednjimi možnostmi:

- Sign Document (Podpiši dokument) – ta možnost dokumentu doda digitalni podpis.
- Add Signature Line Before Signing (Dodaj vrstico za podpis pred podpisovanjem) (samo Microsoft Word in Microsoft Excel) – privzeto je, da se ob podpisu ali šifriranju dokumenta Microsoft Word ali Microsoft Excel doda vrstica za podpis. Če želite to funkcijo izklopiti, kliknite **Add Signature Line (Dodaj vrstico za podpis)**, da odstranite kljukico.
- Encrypt Document (Šifriraj dokument) – ta možnost doda digitalni podpis in šifrira dokument.

- Remove Encryption (Odstrani šifriranje) – ta možnost iz dokumenta odstrani šifriranje.
- Open the Privacy Manager software (Odpri programsko opremo upravitelja zasebnosti) – možnosti potrdil, zaupnih stikov in nastavitev vam omogočajo odpiranje programske opreme orodja Privacy Manager (Upravitelj zasebnosti), da dodate, si ogledate ali spremenite trenutne nastavitve. Za več informacij glejte razdelke Upravljanje potrdil orodja Privacy Manager (Upravitelj zasebnosti) na strani 44, Upravljanje zaupnih stikov na strani 48 ali Konfiguriranje orodja Privacy Manager (Upravitelj zasebnosti) za program Microsoft Office na strani 53.

Konfiguriranje orodja Privacy Manager (Upravitelj zasebnosti) za program Microsoft Office

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti), kliknite **Settings (Nastavitve)** in nato jeziček **Documents (Dokumenti)**.

   – ali –

   V orodni vrstici dokumenta Microsoft Office kliknite navzdol obrnjeno puščico ob napisu **Sign and Encrypt (Podpiši in šifriraj)** in nato možnost **Settings (Nastavitve)**.

2. Izberite opravila, ki jih želite konfigurirati, in nato kliknite **OK (V redu)**.

Podpisovanje dokumenta Microsoft Office

1. V programu Microsoft Word, Microsoft Excel ali Microsoft PowerPoint izdelajte dokument in ga shranite.
2. Kliknite navzdol obrnjeno puščico ob napisu **Sign and Encrypt (Podpiši in šifriraj)** in nato **Sign Document (Podpiši dokument)**.
3. Potrdite pristnost s svojim načinom za varno prijavo.
4. Ko se odpre potrditveno pogovorno okno, preberite besedilo in kliknite **OK (V redu)**.

Če se pozneje odločite, da boste dokument uredili, sledite naslednjim navodilom.

1. V zgornjem levem kotu zaslona kliknite gumb **Office**.
2. Kliknite **Prepare (Pripravi)** in nato **Mark as Final (Označi kot zadnje)**.
3. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)** in nadaljujte delo.
4. Ko urejanje končate, dokument ponovno podpišite.

Dodajanje vrstice za podpis pri podpisovanju dokumenta Microsoft Word ali Microsoft Excel

Z orodjem Privacy Manager (Upravitelj zasebnosti) lahko dodate vrstico za podpis pri podpisovanju dokumenta Microsoft Word ali Microsoft Excel:

1. V programu Microsoft Word ali Microsoft Excel izdelajte dokument in ga shranite.
2. Kliknite meni **Home (Domov)**.
3. Kliknite navzdol obrnjeno puščico ob napisu **Sign and Encrypt (Podpiši in šifriraj)** in nato možnost **Add Signature Line Before Signing (Dodaj vrstico za podpis pred podpisovanjem)**.

OPOMBA: Ko je ta možnost izbrana, je v polju ob njej kljukica. Ta možnost je privzeto vklopljena.

4. Kliknite navzdol obrnjeno puščico ob napisu **Sign and Encrypt (Podpiši in šifriraj)** in nato **Sign Document (Podpiši dokument)**.

5. Potrdite pristnost s svojim načinom za varno prijavo.

Dodajanje predlaganih podpisnikov dokumentu Microsoft Word ali Microsoft Excel

Dokumentu lahko dodate več vrstic za podpis, tako da določite predlagane podpisnike. Predlagani podpisnik je uporabnik, ki ga lastnik dokumenta Microsoft Word ali Microsoft Excel določi, da mora dodati podpis v vrstico za podpis. Predlagani podpisnik ste lahko vi sami ali kakšna druga oseba, ki želite, da podpiše vaš dokument. Če na primer pripravite dokument, ki ga morajo podpisati vsi člani vašega oddelka, lahko na dnu zadnje strani dodate vrstice za podpis teh uporabnikov skupaj z navodili, do kdaj je treba dokument podpisati.

Predlaganega podpisnika dokumentu Microsoft Word ali Microsoft Excel dodate tako:

1. V programu Microsoft Word ali Microsoft Excel izdelajte dokument in ga shranite.

2. Kliknite meni **Insert (Vstavljanje)**.

3. V skupini **Text (Besedilo)** v orodni vrstici kliknite puščico ob napisu **Signature Line (Vrstica za podpis)** in nato **Privacy Manager Signature Provider (Ponudnik podpisov za upravitelja zasebnosti)**.

   Odpre se pogovorno okno Signature Setup (Nastavitev podpisa).

4. V polje pod napisom **Suggested signer (Predlagani podpisnik)** vnesite ime predlaganega podpisnika.

5. V polje pod napisom **Instructions to the signer (Navodila za podpisnika)** vnesite sporočilo za predlaganega podpisnika.

   OPOMBA: Sporočilo bo prikazano na mestu za naziv uporabnika in je izbrisano ali zamenjano z nazivom uporabnika, ko je dokument podpisan.

6. Potrdite polje **Show sign date in signature line (Prikaži datum podpisa v vrstici za podpis)**, da prikažete datum.

7. Potrdite polje **Show signer's title in signature line (Prikaži naziv podpisnika v vrstici za podpis)**, da prikažete naziv podpisnika.

   OPOMBA: Ker lastnik dokumenta določi predlagane podpisnike svojega dokumenta, v primeru, da polji **Show sign date in signature line (Prikaži datum podpisa v vrstici za podpis)** in/ali **Show signer's title in signature line (Prikaži naziv podpisnika v vrstici za podpis)** nista potrjeni, predlagani podpisnik v vrstici za podpis ne bo mogel prikazati datuma in/ali naziva, tudi če so njegove nastavitve dokumenta tako konfigurirane.

8. Kliknite **OK (V redu)**.

Dodajanje vrstice za podpis predlaganega podpisnika

Ko predlagani podpisniki odprejo dokument, bodo videli svoje ime v oklepajih, kar pomeni, da morajo podpisati dokument.

Dokument podpišete tako:

1. Dvokliknite primerno vrstico za podpis.

2. Potrdite pristnost s svojim načinom za varno prijavo.

Vrstica za podpis bo prikazana v skladu z nastavitvami, ki jih je določil lastnik dokumenta.

Šifriranje dokumenta Microsoft Office

Zase in za svoje zaupne stike lahko šifrirate dokument Microsoft Office. Ko šifrirate dokument in ga zaprete, se, preden ga vi ali zaupni stiki s seznama ponovno odprete, opravi preverjanje pristnosti.

Dokument Microsoft Office šifrirate tako:

1. V programu Microsoft Word, Microsoft Excel ali Microsoft PowerPoint izdelajte dokument in ga shranite.
2. Kliknite meni **Home (Domov)**.
3. Kliknite navzdol obrnjeno puščico ob napisu **Sign and Encrypt (Podpiši in šifriraj)** in nato **Encrypt Document (Šifriraj dokument)**.

   Odpre se pogovorno okno Select Trusted Contacts (Izbiranje zaupnih stikov).
4. Kliknite ime zaupnega stika, ki bo lahko odprl dokument in si ogledal njegovo vsebino.

OPOMBA: Če želite izbrati več imen zaupnih stikov, zadržite tipko ctrl in kliknite posamezna imena.

5. Kliknite **OK (V redu)**.

Če se pozneje odločite, da boste dokument uredili, sledite navodilom v razdelku Odstranjevanje šifriranja iz dokumenta Microsoft Office na strani 55. Ko odstranite šifriranje, lahko urejate dokument. Če želite znova šifrirati dokument, sledite korakom v tem razdelku.

Odstranjevanje šifriranja iz dokumenta Microsoft Office

Ko iz dokumenta Microsoft Office odstranite šifriranje, pri odpiranju in ogledovanju vsebine preverjanje pristnosti ni več potrebno.

Šifriranje iz dokumenta Microsoft Office odstranite tako:

1. Odprite šifrirani dokument Microsoft Word, Microsoft Excel ali Microsoft PowerPoint.
2. Potrdite pristnost s svojim načinom za varno prijavo.
3. Kliknite meni **Home (Domov)**.
4. Kliknite navzdol obrnjeno puščico ob napisu **Sign and Encrypt (Podpiši in šifriraj)** in nato **Remove Encryption (Odstrani šifriranje)**.

Pošiljanje šifriranega dokumenta Microsoft Office

Šifrirani dokument Microsoft Office lahko pripnete e-poštnemu sporočilu, ne da bi pri tem morali podpisati ali šifrirati samo e-pošto. To storite tako, da ustvarite in pošljete e-poštno sporočilo skupaj s podpisanim ali šifriranim sporočilom, podobno kot bi to storili pri pošiljanju običajnega e-poštnega sporočila brez priponke.

Vendar pa zaradi optimalne varnosti priporočamo, da e-poštno sporočilo šifrirate, kadar pripnete podpisani ali šifrirani dokument Microsoft Office.

Če želite poslati zapečateno e-poštno sporočilo s pripetim podpisanim in/ali šifriranim dokumentom Microsoft Office, sledite tem korakom:

1. V programu Microsoft Outlook kliknite **New (Novo)** ali **Reply (Odgovori)**.
2. Vnesite svoje sporočilo.
3. Pripnite dokument Microsoft Office.
4. Za dodatna navodila glejte razdelek Zapečatenje in pošiljanje e-poštnega sporočila na strani 52.

Ogled podpisanega dokumenta Microsoft Office

OPOMBA: Za ogled podpisanega dokumenta Microsoft Office ne potrebujete potrdila orodja Privacy Manager (Upravitelj zasebnosti).

Ko odprete podpisan dokument Microsoft Office, se v vrstici stanja na dnu okna dokumenta prikaže ikona digitalnega podpisa.

1. Kliknite ikono **Digital Signatures (Digitalni podpisi)**, da preklopite prikaz pogovornega okna Signatures (Podpisi), kjer so prikazana imena vseh uporabnikov, ki so podpisali dokument, in datum, ko ga je vsak uporabnik podpisal.
2. Če si želite ogledati še več podrobnosti glede vsakega podpisa, z desno miškino tipko kliknite ime v pogovornem oknu Signatures (Podpisi) in izberite možnost Signature Details (Podrobnosti podpisa).

Ogled šifriranega dokumenta Microsoft Office

Šifrirani dokument Microsoft Office iz drugega računalnika si lahko ogledate le, če je v tistem računalniku nameščeno orodje Privacy Manager (Upravitelj zasebnosti). Poleg tega je treba obnoviti tudi potrdilo orodja Privacy Manager (Upravitelj zasebnosti), ki je bilo uporabljeno pri šifriranju datoteke.

Zaupni stik, ki si želi ogledati šifrirani dokument Microsoft Office, mora imeti potrdilo orodja Privacy Manager (Upravitelj zasebnosti) in v računalniku nameščeno to orodje. Poleg tega mora lastnik šifriranega dokumenta Microsoft Office ta zaupni stik tudi izbrati.

Uporaba orodja Privacy Manager (Upravitelj zasebnosti) v programu Windows Live Messenger

Orodje Privacy Manager (Upravitelj zasebnosti) v program Windows Live Messenger doda naslednje funkcije varnih komunikacij:

- **Secure chat (Varen klepet)** – sporočila se prenašajo s protokolom SSL/TLS (Secure Sockets Layer/Transport Layer Security) over XML, isto tehnologijo, ki zagotavlja varnost transakcij e-trgovine.
- **Recipient identification (Prepoznavanje prejemnika)** – pred pošiljanjem sporočila lahko preverite prisotnost in identiteto osebe.
- **Signed messages (Podpisana sporočila)** – svoja sporočila lahko elektronsko podpišete. Če je potem sporočilo kakor koli spremenjeno, se ob prejemu označi kot neveljavno.
- **Hide/show feature (Funkcija skrij/prikaži)** – v oknu Privacy Manager Chat (Klepet upravitelja zasebnosti) lahko skrijete katero koli ali vsa sporočila. Pošljete lahko tudi sporočilo s skrito vsebino. Pred prikazom sporočila je potrebno preverjanje pristnosti.

- **Secure chat history (Zgodovina varnih klepetov)** – zapisi v dnevniku vaših sej klepetov se pred shranjevanjem šifrirajo in potrebujete preverjanje pristnosti, da si jih lahko ogledate.
- **Automatic locking/unlocking (Samodejno zaklepanje/odklepanje)** – okno Privacy Manager Chat (Klepet upravitelja zasebnosti) lahko zaklenete in odklenete ali ga nastavite, da se samodejno zaklene po določenem času nedejavnosti.

Začetek seje Privacy Manager Chat

OPOMBA: Če želite uporabiti funkcijo Privacy Manager Chat (Klepet upravitelja zasebnosti), morata obe strani imeti nameščeno orodje Privacy Manager (Upravitelj zasebnosti) in potrdilo tega orodja. Podrobnosti o nameščanju potrdila orodja Privacy Manager (Upravitelj zasebnosti) najdete v razdelku Zahteva za potrdilo orodja Privacy Manager (Upravitelj zasebnosti) in njegova namestitev na strani 44.

1. Če želite v programu Windows Live Messenger zagnati funkcijo Privacy Manager Chat (Klepet upravitelja zasebnosti), izvedite enega od naslednjih postopkov:

   a. Z desno miškino tipko kliknite prijavljen stik v programu Live Messenger in izberite možnost **Start an Activity (Zaženi dejavnost)**.

   b. Kliknite **Start Chat (Začni klepet)**.

   – ali –

   a. V programu Live Messenger dvakrat kliknite dosegljiv stik in nato izberite meni **See a list of activities (Prikaži seznam dejavnosti)**.

   b. Kliknite **Action (Dejanje)** in nato **Start Chat (Začni klepet)**.

   – ali –

   a. Z desno miškino tipko kliknite ikono ProtectTools v področju za obvestila, kliknite **Privacy Manager for HP ProtectTools (Upravitelj zasebnosti za HP ProtectTools)** in nato izberite **Start Chat (Začni klepet)**.

   b. V programu Live Messenger kliknite **Actions: Start an Activity (Dejanja: začni dejavnost)** in nato izberite **Privacy Manager Chat (Klepet upravitelja zasebnosti)**.

   OPOMBA: Vsak uporabnik mora biti dosegljiv v programu Live Messenger in uporabniki morajo biti prikazani v oknu programa Live Messenger drugih uporabnikov. Kliknite, da izberete dosegljivega uporabnika.

   Privacy Manager (Upravitelj zasebnosti) pošlje povabilo stiku za zagon funkcije Privacy Manager Chat (Klepet upravitelja zasebnosti). Ko stik povabilo sprejme, se odpre okno funkcije Privacy Manager Chat (Klepet upravitelja zasebnosti). Če povabljeni stik nima orodja Privacy Manager (Upravitelj zasebnosti), bo pozvan, da ga prenese.

2. Kliknite **Start (Začni)**, da začnete varen klepet.

Konfiguriranje orodja Privacy Manager za program Windows Live Messenger

1. V funkciji Privacy Manager Chat (Klepet upravitelja zasebnosti) kliknite gumb **Settings (Nastavitve)**.

   – ali –

   V orodju Privacy Manager (Upravitelj zasebnosti) kliknite **Settings (Nastavitve)** in nato jeziček **Chat (Klepet)**.

   – ali –

   V pregledovalniku zgodovine Privacy Manager: Live Messenger History Viewer kliknite gumb **Settings (Nastavitve)**.

2. Če želite določiti čas, po preteku katerega bo funkcija Privacy Manager Chat (Klepet upravitelja zasebnosti) zaklenila sejo, v polju **Lock session after _ minutes of inactivity (Zakleni sejo po _ minutah nedejavnosti)** izberite število.

3. Mapo za shranjevanje zgodovine klepeta določite tako, da kliknete **Browse (Prebrskaj)** in mapo poiščete, nato pa kliknete **OK (V redu)**.

4. Če želite, da se seja samodejno šifrira in shrani, ko jo zaprete, potrdite polje **Automatically save secure chat history (Samodejno shrani varno zgodovino klepeta)**.

5. Kliknite **OK (V redu)**.

Klepet v oknu funkcije Privacy Manager Chat

Ko zaženete funkcijo Privacy Manager Chat (Klepet upravitelja zasebnosti), se v programu Windows Live Messenger odpre okno te funkcije. Uporaba funkcije Privacy Manager Chat (Klepet upravitelja zasebnosti) je podobna uporabi osnovnega programa Windows Live Messenger, le da so v oknu te funkcije na voljo še dodatne možnosti:

- **Save (Shrani)** – Kliknite ta gumb, če želite shraniti klepet v mapo, določeno v konfiguracijskih nastavitvah. Funkcijo Privacy Manager Chat (Klepet upravitelja zasebnosti) lahko konfigurirate tudi tako, da samodejno shrani vsak klepet, ko ga zaprete.
- **Hide all (Skrij vse)** in **Show all (Prikaži vse)** – Kliknite ustrezen gumb, da prikažete ali skrijete sporočila v oknu Secure Communications (Varno komuniciranje). Posamezna sporočila lahko skrijete tudi tako, da kliknete glavo sporočila.
- **Are you there? (Si tam?)** – Kliknite ta gumb, če želite preveriti pristnost stika.
- **Lock (Zakleni)** – Kliknite ta gumb, če želite zapreti okno funkcije Privacy Manager Chat (Klepet upravitelja zasebnosti) in znova odpreti okno Chat Entry (Vnos klepeta). Okno Secure Communications (Varne komunikacije) znova prikažete tako, da kliknete možnost **Resume the session (Nadaljuj sejo)** in nato z izbranim načinom za varno prijavo potrdite pristnost.
- **Send (Pošlji)** – Kliknite ta gumb, če želite stiku poslati šifrirano sporočilo.
- **Send signed (Pošlji podpisano)** – Označite to potrditveno polje, če želite sporočilom dodati elektronski podpis in jih šifrirati. Če je potem sporočilo kakor koli spremenjeno, se ob prejemu označi kot neveljavno. Pristnost se preveri ob vsakem pošiljanju podpisanega sporočila.
- **Send hidden (Pošlji skrito)** – Označite to potrditveno polje, če želite šifrirati in poslati sporočilo, na katerem bo prikazana samo glava. Za ogled vsebine sporočila se mora preveriti pristnost stika.

Ogled zgodovine klepeta

V pregledovalniku zgodovine klepeta Privacy Manager Chat: Live Messenger History Viewer so prikazane šifrirane datoteke sej klepeta Privacy Manager Chat (Klepet upravitelja zasebnosti). Klepete lahko shranjujete tako, da v oknu funkcije Privacy Manager Chat (Klepet upravitelja zasebnosti) kliknete možnost **Save (Shrani)** ali da na kartici Chat (Klepet) v orodju Privacy Manager (Upravitelj zasebnosti) nastavite samodejno shranjevanje. V pregledovalniku se za vsak klepet prikaže (šifrirano) ime zaslona stika ter datum in čas začetka in konca klepeta. Privzeto so klepeti prikazani za vse e-poštne račune, ki ste jih nastavili. Za prikaz samo določenih računov uporabite meni **Display history for (Prikaži zgodovino za)**.

Pregledovalnik vam omogoča izvajanje naslednjih opravil:

- Razkrivanje vseh sej na strani 59
- Razkrivanje sej za določene račune na strani 59
- Ogled ID-ja seje na strani 60
- Ogled seje na strani 60
- Iskanje določenega besedila v sejah na strani 60
- Brisanje seje na strani 60
- Dodajanje in odstranjevanje stolpcev na strani 61
- Filtriranje sej za prikaz na strani 61

Pregledovalnik zgodovine Live Messenger History Viewer zaženete tako:

▲ V področju za obvestila na skrajni desni strani opravilne vrstice kliknite ikono **HP ProtectTools**, nato pa **Privacy Manager: for HP ProtectTools (Upravitelj zasebnosti: za HP ProtectTools)** in nato **Live Messenger History Viewer (Pregledovalnik zgodovine Live Messenger)**.

– ali –

▲ Med klepetom kliknite **History Viewer (Pregledovalnik zgodovine)** ali **History (Zgodovina)**.

Razkrivanje vseh sej

Če razkrijete vse seje, za trenutno izbrano sejo in vse seje v tem računu prikažete dešifrirano zaslonsko ime stika Contact Screen Name.

Če želite razkriti vse shranjene seje zgodovine klepetov:

1. V pregledovalniku zgodovine Live Messenger History Viewer z desno miškino tipko kliknite katero koli sejo in izberite možnost **Reveal All Sessions (Razkrij vse seje)**.
2. Potrdite pristnost s svojim načinom za varno prijavo.

   Zaslonska imena stikov so dešifrirana.
3. Dvokliknite katero koli sejo za ogled njene vsebine.

Razkrivanje sej za določene račune

Če razkrijete sejo, za trenutno izbrano sejo prikažete dešifrirano zaslonsko ime stika Contact Screen Name.

Točno določeno sejo zgodovine klepetov razkrijete tako:

1. V pregledovalniku zgodovine Live Messenger History Viewer z desno miškino tipko kliknite katero koli sejo in izberite možnost **Reveal Session (Razkrij sejo)**.
2. Potrdite pristnost s svojim načinom za varno prijavo.

   Zaslonsko ime stika je dešifrirano.
3. Dvokliknite razkrito sejo za ogled njene vsebine.

OPOMBA: Pri dodatnih sejah, šifriranih z istim potrdilom, bodo prikazane nezaklenjene ikone, kar pomeni, da lahko seje preprosto dvokliknete brez dodatnega potrjevanja pristnosti in si jih ogledate. Pri sejah, šifriranih z drugim potrdilom, pa bo prikazana zaklenjena ikona, kar pomeni, da je pri teh sejah pred ogledom zaslonskih imen stikov ali vsebine potrebna potrditev pristnosti.

Ogled ID-ja seje

Če si želite ogledati ID seje:

- V pregledovalniku zgodovine klepeta Live Messenger History Viewer z desno miškino tipko kliknite katero koli razkrito sejo in izberite možnost **View Session ID (Ogled ID-ja seje)**.

Ogled seje

Pri ogledu seje se odpre datoteka za ogled. Če seja še ni bila razkrita (v tem primeru je prikazano dešifrirano zaslonsko ime stika Contact Screen Name), je istočasno z ogledom tudi razkrita.

Za ogled seje zgodovine Live Messenger:

1. V pregledovalniku zgodovine Live Messenger History Viewer z desno miškino tipko kliknite katero koli sejo in izberite možnost **View (Ogled)**.
2. Če boste pozvani, potrdite svojo pristnost s svojim načinom za varno prijavo.

   Vsebina seje je dešifrirana.

Iskanje določenega besedila v sejah

Besedilo lahko iščete le v razkritih (dešifriranih) sejah, ki so prikazane v oknu pregledovalnika. To so seje, v katerih je zaslonsko ime stika prikazano z navadnim besedilom.

Iskanje besedila v sejah zgodovine klepetov:

1. V pregledovalniku zgodovine Live Messenger History Viewer kliknite gumb **Search (Išči)**.
2. Vnesite iskano besedilo, konfigurirajte želene parametre in kliknite **OK (V redu)**.

   Seje z vsebovanim besedilom so v oknu pregledovalnika označene.

Brisanje seje

1. Izberite sejo zgodovine klepeta.
2. Kliknite **Delete (Izbriši)**.

Dodajanje in odstranjevanje stolpcev

Privzeto so trije najbolj uporabljeni stolpci prikazani v pregledovalniku Live Messenger History Viewer. Prikazu lahko dodate dodatne stolpce ali pa jih z njega odstranite.

Prikazu dodate stolpce tako:

1. Z desno miškino tipko kliknite katero koli glavo stolpca in izberite **Add/Remove Columns (Dodajanje/odstranjevanje stolpcev)**.
2. V levem podoknu izberite glavo stolpca in kliknite **Add (Dodaj)**, da ga premaknete v desno podokno.

Stolpce s prikaza odstranite tako:

1. Z desno miškino tipko kliknite katero koli glavo stolpca in izberite **Add/Remove Columns (Dodajanje/odstranjevanje stolpcev)**.
2. V desnem podoknu izberite glavo stolpca in kliknite gumb **Remove (Odstrani)**, da ga premaknete v levo podokno.

Filtriranje sej za prikaz

Seznam sej za vse vaše račune je prikazan v pregledovalniku Live Messenger History Viewer. Prikazane seje lahko filtrirate po naslednjih elementih:

- Posebni računi. Za podrobnosti glejte razdelek Prikazovanje sej za določene račune na strani 61.
- Obseg datumov. Za podrobnosti glejte razdelek Prikazovanje sej za obseg datumov na strani 61.
- Različne mape. Za podrobnosti glejte razdelek Prikazovanje sej, ki niso shranjene v privzeti mapi na strani 62.

Prikazovanje sej za določene račune

▲ V pregledovalniku zgodovine Live Messenger History Viewer izberite račun iz menija **Display history for (Prikaži zgodovino za)**.

Prikazovanje sej za obseg datumov

1. V pregledovalniku zgodovine Live Messenger History Viewer kliknite ikono **Advanced Filter (Napredni filter)**.

   Odpre se pogovorno okno Advanced Filter (Napredni filter).

2. Potrdite polje **Display only sessions within specified date range (Prikaži le seje znotraj določenega datumskega obsega)**.
3. V polji **From date (Od datuma)** in **To date (Do datuma)** vnesite dan, mesec in/ali leto ali pa kliknite puščico ob koledarju in izberite datuma.
4. Kliknite **OK (V redu)**.

Prikazovanje sej, ki niso shranjene v privzeti mapi

1. V pregledovalniku zgodovine Live Messenger History Viewer kliknite ikono **Advanced Filter (Napredni filter)**.
2. Potrdite polje **Use an alternate history files folder (Uporabi nadomestno mapo za datoteke z zgodovino)**.
3. Vnesite mesto mape ali kliknite **Browse (Prebrskaj)**, da mapo poiščete.
4. Kliknite **OK (V redu)**.

Napredna opravila

Migracija potrdil Privacy Manager Certificates in zaupnih stikov v drug računalnik

Potrdila orodja Privacy Manager (Upravitelj zasebnosti) in zaupne stike lahko varno prenesete v drug računalnik ali varnostno kopirate podatke, da bodo na varnem. To naredite tako, da podatke varnostno kopirate kot datoteko, zaščiteno z geslom, ki jo nato izvozite na omrežno mesto ali v katero koli izmenljivo napravo za shranjevanje, in jo nato obnovite v novem računalniku.

Varnostno kopiranje potrdil orodja Privacy Manager (Upravitelj zasebnosti) in zaupnih stikov

Če želite svoja potrdila orodja Privacy Manager (Upravitelj zasebnosti) in zaupne stike varnostno kopirati v datoteko, zaščiteno z geslom, sledite naslednjim navodilom:

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Migration (Migracija)**.
2. Kliknite **Backup (Varnostno kopiraj)**.
3. Na strani »Select Data« (Izbiranje podatkov) izberite podatkovne kategorije, ki jih želite vključiti v datoteko za migracijo, in nato kliknite **Next (Naprej)**.
4. Na strani »Migration File« (Datoteka za migracijo) izberite ime datoteke ali kliknite **Browse (Prebrskaj)**, da jo poiščete, in nato kliknite **Next (Naprej)**.
5. Vnesite geslo in ga potrdite ter nato kliknite **Next (Naprej)**.

OPOMBA: Geslo shranite na varno mesto, ker ga boste potrebovali pri obnovitvi datoteke za migracijo.

6. Potrdite pristnost s svojim načinom za varno prijavo.
7. Na strani »Migration File Saved« (Datoteka za migracijo je shranjena) kliknite **Finish (Dokončaj)**.

Obnovitev potrdil orodja Privacy Manager in zaupnih stikov

Če želite potrdila orodja Privacy Manager (Upravitelj zasebnosti) in zaupne stike obnoviti v drugem računalniku kot del migracijskega postopka ali v istem računalniku, sledite tem korakom:

1. Odprite orodje Privacy Manager (Upravitelj zasebnosti) in kliknite **Migration (Migracija)**.
2. Kliknite **Restore (Obnovi)**.
3. Na strani »Migration File« (Datoteka za migracijo) kliknite **Browse (Prebrskaj)**, da poiščete datoteko, nato kliknite **Next (Naprej)**.
4. Vnesite geslo, ki ste ga uporabili pri varnostnem kopiranju, in kliknite **Next (Naprej)**.
5. Na strani »Migration File« (Datoteka za migracijo) kliknite **Finish (Dokončaj)**.

Osrednje upravljanje orodja Privacy Manager (Upravitelj zasebnosti)

Vaša namestitev orodja Privacy Manager (Upravitelj zasebnosti) je lahko del centralizirane namestitve, ki jo je prilagodil vaš skrbnik. Ena ali več od naslednjih funkcij je lahko omogočenih ali onemogočenih:

- **Certificate use policy (Pravilnik uporabe potrdil)** – morda bo vaša uporaba potrdil orodja Privacy Manager (Upravitelj zasebnosti) omejena na tista, ki jih izda overitelj Comodo, morda pa boste lahko uporabljali digitalna potrdila, ki jih izdajajo drugi overitelji potrdil.
- **Encryption policy (Pravilnik šifriranja)** – v programih Microsoft Office ali Outlook in Windows Live Messenger so lahko zmogljivosti šifriranja posamezno omogočene ali onemogočene.

9 File Sanitizer za HP ProtectTools

File Sanitizer (Orodje za čiščenje datoteke) je orodje, s katerim varno izbrišete sredstva (osebne informacije ali datoteke, zgodovino in spletno vsebino ali druge podatkovne komponente) v računalniku in varno očistite trdi disk s prepisovanjem.

OPOMBA: Ta različica orodja File Sanitizer (Orodje za čiščenje datoteke) podpira samo sistemski trdi disk.

Varno brisanje

Varno brisanje se od običajnega brisanja Windows® (ki je v orodju za čiščenje datoteke File Sanitizer znano pod imenom preprosto brisanje) razlikuje v tem, da algoritem pri varnem brisanju z orodjem za čiščenje datoteke File Sanitizer zakrije podatke, zato je pridobitev prvotnih sredstev dejansko nemogoča. Pri preprostem brisanju Windows je lahko datoteka (ali sredstvo) v trdem disku nedotaknjena ali v stanju, ko lahko s forenzičnimi načini delovanja obnovite datoteko (ali sredstvo).

Ko izberete profil varnega brisanja (High Security – visoka stopnja varnosti, Medium Security – srednja stopnja varnost ali Low Security – nizka stopnja varnosti), se za varno brisanje samodejno izberejo predhodno določen seznam sredstev in načini za brisanje. Profil varnega brisanja lahko tudi prilagodite, kar omogoča, da določite število ciklov varnega brisanja, sredstva za varno brisanje, sredstva, ki jih želite pred varnim brisanjem potrditi, in sredstva, ki jih ne želite vključiti. Več informacij najdete v razdelku Izbiranje ali ustvarjanje profila za varno brisanje na strani 69.

Nastavite lahko tudi načrtovano samodejno varno brisanje in sredstvo kadar koli ročno varno izbrišete. Več informacij najdete v razdelkih Nastavljanje urnika varnega brisanja orodja na strani 68, Ročno varno brisanje enega sredstva na strani 73 ali Ročno varno brisanje vseh izbranih elementov na strani 74.

OPOMBA: Datoteka .dll se varno izbriše in odstrani iz sistema samo v primeru, če ste jo premaknili v koš.

Varno čiščenje nezasedenega prostora s prepisovanjem

Z brisanjem sredstva v sistemu Windows njegove vsebine s trdega diska ne odstranite v celoti. Sistem izbriše le sklic na sredstvo. Vsebina pa ostane na trdem disku, dokler mesta na trdem disku ne prepišete z novimi podatki.

Z varnim čiščenjem nezasedenega prostora s prepisovanjem lahko čez izbrisano sredstvo napišete naključne podatke, kar uporabnikom onemogoči ogledovanje prvotne vsebine izbrisanega sredstva.

OPOMBA: Varno čiščenje nezasedenega prostora s prepisovanjem se uporablja pri tistih sredstvih, ki jih izbrišete s košem v operacijskem sistemu Windows, ali pri ročno izbrisanih sredstvih. Z njim ne zagotovite dodatne varnosti varno izbrisanih podatkov.

Nastavite lahko načrtovano samodejno varno čiščenje nezasedenega prostora s prepisovanjem ali pa z ikono **HP ProtectTools** na skrajni desni strani opravilne vrstice v področju za obvestila ročno aktivirate varno čiščenje s prepisovanjem. Več informacij najdete v razdelkih Nastavljanje urnika varnega čiščenja nezasedenega prostora s prepisovanjem na strani 69 ali Ročno aktiviranje varnega čiščenja nezasedenega prostora s prepisovanjem na strani 74.

Nastavitev

Odpiranje orodja za čiščenje datoteke File Sanitizer

File Sanitizer (Orodje za čiščenje datoteke) odprete tako:

1. Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools)**.
2. Kliknite **File Sanitizer (Orodje za čiščenje datoteke)**.

– ali –

▲ Dvokliknite ikono **File Sanitizer (Orodje za čiščenje datoteke)** na namizju.

– ali –

▲ V področju za obvestila z desno miškino tipko kliknite ikono **HP ProtectTools**, na skrajni desni strani opravilne vrstice kliknite **File Sanitizer (Orodje za čiščenje datoteke)** in nato še **Open File Sanitizer (Odpri orodje za čiščenje datoteke)**.

Nastavljanje urnika varnega brisanja orodja

OPOMBA: Za informacije o izbiranju predhodno določenega profila varnega brisanja ali ustvarjanju profila varnega brisanja glejte razdelek Izbiranje ali ustvarjanje profila za varno brisanje na strani 69.

OPOMBA: Za informacije o ročnem varnem brisanju sredstev glejte razdelek Ročno varno brisanje enega sredstva na strani 73.

1. Odprite orodje za čiščenje datoteke File Sanitizer in kliknite možnost **Shred (Varno izbriši)**.
2. Izberite možnost varnega brisanja:
   - **Windows shutdown (Zaustavitev operacijskega sistema Windows)** – izberite to možnost, če želite ob zaustavitvi operacijskega sistema Windows varno izbrisati vsa izbrana sredstva.

     OPOMBA: Če izberete to možnost, se pri zaustavitvi sistema prikaže pogovorno okno z vprašanjem, ali želite nadaljevati s postopkom varnega brisanja izbranih sredstev oziroma ali želite postopek preskočiti. Če želite preskočiti postopek varnega brisanja, kliknite **Yes (Da)**, za nadaljevanje postopka pa kliknite **No (Ne)**.
   - **Web browser open (Odpiranje spletnega brskalnika)** – izberite to možnost, če želite ob odpiranju spletnega brskalnika varno izbrisati vsa izbrana sredstva.
   - **Web browser quit (Izhod iz spletnega brskalnika)** – izberite to možnost, če želite ob izhodu iz spletnega brskalnika varno izbrisati vsa izbrana spletna sredstva.
   - **Key sequence (Zaporedje tipk)** – izberite to možnost, da zaženete varno brisanje z zaporedjem tipk.
   - **Scheduler (Urnik)** – potrdite polje **Activate Scheduler (Aktivni urnik)**, vnesite svoje geslo za Windows in nato še dan in uro za varno brisanje izbranega sredstva.

   OPOMBA: Datoteka .dll se varno izbriše in odstrani iz sistema samo v primeru, če ste jo premaknili v koš.
3. Kliknite **Apply (Uporabi)** in nato **OK (V redu)**.

Nastavljanje urnika varnega čiščenja nezasedenega prostora s prepisovanjem

OPOMBA: Varno čiščenje nezasedenega prostora s prepisovanjem se uporablja pri tistih sredstvih, ki jih izbrišete s košem v operacijskem sistemu Windows, ali pri ročno izbrisanih sredstvih. Z njim ne zagotovite dodatne varnosti varno izbrisanih sredstev.

Urnik varnega čiščenja nezasedenega prostora s prepisovanjem nastavite tako:

1. Odprite orodje za čiščenje datoteke File Sanitizer in kliknite **Free Space Bleaching (Varno čiščenje nezasedenega prostora s prepisovanjem)**.
2. Potrdite polje **Activate Scheduler (Aktiviraj urnik)**, vnesite svoje geslo za Windows in nato še dan in uro za varno čiščenje trdega diska s prepisovanjem.
3. Kliknite **Apply (Uporabi)** in nato **OK (V redu)**.

OPOMBA: Varno čiščenje nezasedenega prostora s prepisovanjem lahko traja nekaj časa. Čeprav se postopek izvaja v ozadju, lahko vaš računalnik nekoliko počasneje deluje zaradi povečane uporabe procesorja.

Izbiranje ali ustvarjanje profila za varno brisanje

Določite lahko način za brisanje in izberete sredstvo, ki ga želite varno izbrisati, tako da izberete predhodno določen profil ali ustvarite svojega.

Izbiranje predhodno določenega profila za varno brisanje

Ko izberete predhodno določen profil za varno brisanje (High Security – visoka stopnja varnosti, Medium Security – srednja stopnja varnost ali Low Security – nizka stopnja varnosti), se samodejno izberejo predhodno določen seznam sredstev in načini za brisanje. Kliknete lahko gumb **View Details (Ogled podrobnosti)**, da si ogledate predhodno določen seznam sredstev, ki so izbrana za varno brisanje.

Predhodno določen profil za varno brisanje izberete tako:

1. Odprite orodje za čiščenje datoteke File Sanitizer in kliknite možnost **Settings (Nastavitve)**.
2. Kliknite predhodno določen profil za varno brisanje.
3. Kliknite gumb **View Details (Ogled podrobnosti)**, da si ogledate seznam sredstev, ki so izbrana za varno brisanje.
4. V razdelku **Shred the following (Varno izbriši naslednje)** potrdite polje ob sredstvu, katerega varno brisanje želite potrditi.
5. Kliknite **Apply (Uporabi)** in nato **OK (V redu)**.

Prilagajanje profila za varno brisanje

Ko ustvarite profil za varno brisanje, določite število ciklov varnega brisanja, sredstva za varno brisanje, sredstva, ki jih želite pred varnim brisanjem potrditi, in sredstva, ki jih ne želite vključiti.

1. Odprite orodje za čiščenje datoteke File Sanitizer, kliknite **Settings (Nastavitve)**, nato **Advanced Security Settings (Napredne varnostne nastavitve)** in nazadnje še **View Details (Ogled podrobnosti)**.
2. Določite število ciklov varnega brisanja.

OPOMBA: Za vsako sredstvo bo izvedeno izbrano število ciklov varnega brisanja. Če na primer izberete tri cikle, se algoritem, ki zakrije podatke, izvede trikrat. Če izberete cikel z višjo varnostno stopnjo, lahko varno brisanje traja zelo dolgo, vendar pa večje število ciklov pomeni tudi večjo verjetnost, da podatkov ne bo mogoče obnoviti.

3. Izberite sredstvo, ki ga želite varno izbrisati.
   a. V razdelku **Available shred options (Razpoložljive možnosti varnega brisanja)** kliknite sredstvo in nato gumb **Add (Dodaj)**.
   b. Če želite dodati sredstvo po meri, kliknite **Add Custom Option (Dodaj možnost po meri)** in se nato pomaknite do imena datoteke ali mape ali pa vnesite pot do njiju. Kliknite možnost **Open (Odpri)** in nato kliknite **OK (V redu)**. Pod možnostjo **Available shred options (Razpoložljive možnosti varnega brisanja)** kliknite sredstvo po meri in nato kliknite **Add (Dodaj)**.

OPOMBA: Če želite odstraniti sredstvo s seznama razpoložljivih možnosti varnega brisanja, ga kliknite in nato kliknite **Delete (Izbriši)**.

4. V razdelku **Shred the following (Varno izbriši naslednje)** potrdite polje ob sredstvu, katerega varno brisanje želite potrditi.

OPOMBA: Sredstvo s seznama razpoložljivih možnosti varnega brisanja odstranite tako, da ga kliknete in nato kliknete še **Remove (Odstrani)**.

5. Če želite zaščititi datoteke ali mape pred samodejnim varnim brisanjem, pod možnostjo **Do not shred the following (Ne izbriši navedenega)** kliknite **Add (Dodaj)** in poiščite ali vnesite pot do imena datoteke ali mape. Kliknite možnost **Open (Odpri)** in nato kliknite **OK (V redu)**.

OPOMBA: Sredstvo s seznama za izločitev odstranite tako, da ga kliknete in nato kliknete še **Delete (Izbriši)**.

6. Ko končate konfiguracijo profila za varno brisanje, kliknite **Apply (Uporabi)** in nato **OK (V redu)**.

Prilagajanje profila za preprosto brisanje

S profilom za preprosto brisanje izvedete standardno brisanje sredstva brez varnega brisanja. Ko prilagodite profil za preprosto brisanje, določite sredstva, ki jih želite izbrisati, sredstva, ki jih želite pred brisanjem potrditi, in sredstva, ki jih ne želite vključiti v preprosto brisanje.

OPOMBA: Če uporabljate preprosto možnost brisanja, lahko za sredstva, ki ste jih izbrisali ročno ali s funkcijo Recycle Bin (Koš) v sistemu Windows, občasno uporabite možnost čiščenja nezasedenega prostora s prepisovanjem.

Profil za preprosto brisanje prilagodite tako:

1. Odprite orodje za čiščenje datoteke File Sanitizer, kliknite **Settings (Nastavitve)**, nato **Simple Delete Setting (Nastavitve preprostega brisanja)** in nazadnje še **View Details (Ogled podrobnosti)**.

2. Izberite sredstvo, ki ga želite izbrisati.

   a. V razdelku **Available delete options (Razpoložljive možnosti brisanja)** kliknite sredstvo in nato gumb **Add (Dodaj)**.

   b. Sredstvo po meri dodate tako, da kliknete **Add Custom Option (Dodaj možnost po meri)**, vnesete ime datoteke ali mape in nato kliknete **OK (V redu)**. Kliknite sredstvo po meri in nato **Add (Dodaj)**.

OPOMBA: Sredstvo s seznama razpoložljivih možnosti brisanja izbrišete tako, da ga kliknete in nato kliknete še **Delete (Izbriši)**.

3. V razdelku **Delete the following (Izbriši naslednje)** potrdite polje ob sredstvu, katerega brisanje želite potrditi.

OPOMBA: Sredstvo s seznama za brisanja odstranite tako, da ga kliknete in nato kliknete še **Remove (Odstrani)**.

4. V razdelku **Do not delete the following (Ne izbriši naslednje)** kliknite **Add (Dodaj)**, da izberete določeno sredstvo, ki ga ne želite izbrisati.

OPOMBA: Sredstvo s seznama za izločitev odstranite tako, da ga kliknete in nato kliknete še **Delete (Izbriši)**.

5. Ko končate konfiguracijo profila za preprosto brisanje, kliknite **Apply (Uporabi)** in nato **OK (V redu)**.

Splošna opravila

Orodje za čiščenje datoteke File Sanitizer lahko uporabljate za naslednja opravila:

- Uporaba zaporedja tipk za zagon varnega brisanja – ta funkcija vam omogoča ustvarjanje zaporedja tipk (npr. ctrl + alt s) za zagon varnega brisanja. Za podrobnosti glejte razdelek Zagon varnega brisanja z zaporedjem tipk na strani 72.
- Uporaba ikone orodja za čiščenje datoteke File Sanitizer za zagon varnega brisanja – ta funkcija je podobna funkciji »povleci in spusti« v operacijskem sistemu Windows. Za podrobnosti glejte razdelek Uporaba ikone orodja za čiščenje datoteke File Sanitizer+ na strani 73.
- Ročno varno brisanje določenega sredstva ali vseh izbranih sredstev – ta funkcija vam omogoča ročno varno brisanje elementov brez čakanja uporabe rednega urnika varnega brisanja. Za podrobnosti glejte razdelka Ročno varno brisanje enega sredstva na strani 73 ali Ročno varno brisanje vseh izbranih elementov na strani 74.
- Ročno aktiviranje varnega čiščenja nezasedenega prostora s prepisovanjem – ta funkcija vam omogoča ročno aktiviranje varnega čiščenja nezasedenega prostora s prepisovanjem. Za podrobnosti glejte razdelek Ročno aktiviranje varnega čiščenja nezasedenega prostora s prepisovanjem na strani 74.
- Prekinitev postopka varnega brisanja ali varnega čiščenja nezasedenega prostora s prepisovanjem – ta funkcija vam omogoča zaustavitev postopka varnega brisanja ali varnega čiščenja nezasedenega prostora s prepisovanjem. Za podrobnosti glejte razdelek Preklic varnega brisanja in varnega čiščenja nezasedenega prostora s prepisovanjem na strani 74.
- Ogled datotek dnevnika – ta funkcija vam omogoča ogled datotek dnevnika varnega brisanja in varnega čiščenja nezasedenega prostora s prepisovanjem, ki vsebujejo kakršne koli napake, do katerih je prišlo med zadnjim postopkom varnega brisanja ali varnega čiščenja nezasedenega prostora s prepisovanjem. Za podrobnosti glejte razdelek Ogled datotek dnevnika na strani 74.

OPOMBA: Postopek varnega brisanja ali varnega čiščenja nezasedenega prostora s prepisovanjem lahko traja precej časa. Čeprav se postopka izvajata v ozadju, lahko vaš računalnik nekoliko počasneje deluje zaradi povečane uporabe procesorja.

Zagon varnega brisanja z zaporedjem tipk

Če želite določiti zaporedje tipk, sledite naslednjim korakom:

1. Odprite orodje za čiščenje datoteke File Sanitizer in kliknite možnost **Shred (Varno izbriši)**.
2. Potrdite polje **Key sequence (Zaporedje tipk)**.
3. V razpoložljivo polje vnesite znak.
4. Označite polje **CTRL** ali **ALT** in nato označite še polje **SHIFT**.

   Če želite varno brisanje na primer zagnati s kombinacijo tipk s in ctrl + shift, v polje vnesite črko s in nato izberite možnosti **CTRL** in **SHIFT**.

OPOMBA: Pazite, da ne izberete zaporedja tipk, ki ste ga že konfigurirali.

Varno brisanje z zaporedjem tipk zaženete tako:

1. Pritisnite in držite tipki shift in ctrl ali alt (odvisno od kombinacije, ki ste jo določili) in pritisnite izbrani znak.
2. Če se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

Uporaba ikone orodja za čiščenje datoteke File Sanitizer+

△ **POZOR:** Sredstev, ki so bila varno izbrisana, ni mogoče obnoviti. Dobro premislite, preden izberete predmete za ročno varno brisanje.

1. Pomaknite se do dokumenta ali mape, ki jo želite varno izbrisati.
2. Sredstvo povlecite do ikone orodja za čiščenje datoteke File Sanitizer na namizju.
3. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

Ročno varno brisanje enega sredstva

△ **POZOR:** Sredstev, ki so bila varno izbrisana, ni mogoče obnoviti. Dobro premislite, preden izberete predmete za ročno varno brisanje.

1. V področju za obvestila na skrajni desni strani opravilne vrstice kliknite ikono orodij **HP ProtectTools**, nato **File Sanitizer (Orodje za čiščenje datoteke)** in nazadnje še **Shred One (Varno izbriši eno sredstvo)**.
2. Ko se odpre pogovorno okno Browse (Prebrskaj), se pomaknite do sredstva, ki ga želite varno izbrisati, in nato kliknite **OK (V redu)**.

   OPOMBA: Izbrano sredstvo je lahko ena datoteka ali mapa.

3. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

– ali –

1. Na namizju z desno miškino tipko kliknite ikono **File Sanitizer (Orodje za čiščenje datoteke)** in nato **Shred One (Varno izbriši eno sredstvo)**.
2. Ko se odpre pogovorno okno Browse (Prebrskaj), se pomaknite do sredstva, ki ga želite varno izbrisati, in nato kliknite **OK (V redu)**.
3. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

– ali –

1. Odprite orodje za čiščenje datoteke File Sanitizer in kliknite možnost **Shred (Varno izbriši)**.
2. Kliknite gumb **Browse (Prebrskaj)**.
3. Ko se odpre pogovorno okno Browse (Prebrskaj), se pomaknite do sredstva, ki ga želite varno izbrisati, in nato kliknite **OK (V redu)**.
4. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

Ročno varno brisanje vseh izbranih elementov

1. V področju za obvestila z desno miškino tipko kliknite ikono **HP ProtectTools**, na skrajni desni strani opravilne vrstice kliknite **File Sanitizer (Orodje za čiščenje datoteke)** in nato še **Shred Now (Varno izbriši zdaj)**.
2. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

– ali –

1. Na namizju z desno miškino tipko kliknite ikono **File Sanitizer (Orodje za čiščenje datoteke)** in nato **Shred Now (Varno izbriši zdaj)**.
2. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

– ali –

1. Odprite orodje za čiščenje datoteke File Sanitizer in kliknite možnost **Shred (Varno izbriši)**.
2. Kliknite gumb **Shred now (Varno izbriši zdaj)**.
3. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

Ročno aktiviranje varnega čiščenja nezasedenega prostora s prepisovanjem

1. V področju za obvestila z desno miškino tipko kliknite ikono **HP ProtectTools**, na skrajni desni strani opravilne vrstice kliknite **File Sanitizer (Orodje za čiščenje datoteke)** in nazadnje še **Bleach Now (Varno počisti s prepisovanjem zdaj)**.
2. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

– ali –

1. Odprite orodje za čiščenje datoteke File Sanitizer in kliknite **Free Space Bleaching (Varno čiščenje nezasedenega prostora s prepisovanjem)**.
2. Kliknite **Bleach Now (Varno počisti s prepisovanjem zdaj)**.
3. Ko se odpre potrditveno pogovorno okno, kliknite **Yes (Da)**.

Preklic varnega brisanja in varnega čiščenja nezasedenega prostora s prepisovanjem

Ko se izvaja varno brisanje ali čiščenje nezasedenega prostora s prepisovanjem, je v področju za obvestila nad ikono orodja HP ProtectTools Security Manager (Upravitelj varnosti HP ProtectTools) prikazano sporočilo. V njem so navedene podrobnosti o postopkih in njihovem poteku (odstotek dokončanega dela). Prav tako pa lahko tam operacijo tudi prekličete.

Operacijo prekličete tako:

▲ Če želite preklicati operacijo, kliknite sporočilo in nato kliknite **Stop (Ustavi)**.

Ogled datotek dnevnika

Po vsakem varnem brisanju ali čiščenju nezasedenega prostora s prepisovanjem se ustvarijo dnevniške datoteke napak in okvar, ki se posodabljajo glede na najnovejše varno brisanje ali čiščenje nezasedenega prostora s prepisovanjem.

OPOMBA: Uspešno izbrisane in počiščene datoteke niso prikazane v datotekah dnevnika.

Ena datoteka dnevnika se ustvari za varno brisanje in ena za varno čiščenje nezasedenega prostora s prepisovanjem. Obe najdete na trdem disku:

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

10 Device Access Manager za HP ProtectTools (samo pri izbranih modelih)

Skrbniki operacijskega sistema Windows® uporabljajo orodje Device Access Manager for HP ProtectTools (Upravitelj dostopa do naprav za HP ProtectTools), da nadzirajo dostop do naprav v sistemu in za zaščito pred nepooblaščenim dostopom:

- Za vsakega uporabnika se ustvarijo profili naprav, kjer se določajo naprave, do katerih imajo ti uporabniki omogočen ali preprečen dostop.
- Uporabniki so organizirani v skupine, kot je vnaprej določena skupina Device Administrators (Skrbniki naprav), skupine pa so lahko določene znotraj možnosti Computer Management (Upravljanje računalnika) v razdelku Administrative Tools (Skrbniška orodja) na nadzorni plošči.
- Dostop do naprav se lahko omogoči ali prepreči na podlagi članstva v skupinah.
- Pri napravah, kot so pogoni CD-ROM in DVD, se lahko ločeno omogoči ali onemogoči dostop za branje in zapisovanje.

Uporabniki z omejenim dostopom lahko dobijo dovoljenje za prebiranje in spreminjanje pravilnika o nadzoru dostopa do naprav.

Nastavitev

Odpiranje orodja Device Access Manager (Upravitelj dostopa do naprav)

Orodje Device Access Manager (Upravitelj dostopa do naprav) odprete tako:

1. Kliknite **Start**, **Vsi programi**, **HP** in nato **HP ProtectTools Administrative Console (Skrbniška konzola HP ProtectTools)**.
2. V levem podoknu kliknite **Device Access Manager (Upravitelj dostopa do naprav)**.

Konfiguriranje dostopa do naprav

Orodje Device Access Manager for HP ProtectTools (Upravitelj dostopa do naprav za HP ProtectTools) omogoča tri poglede:

- pogled Simple Configuration (Preprosta konfiguracija) se uporablja za omogočanje ali onemogočanje dostopa do razredov naprav za člane skupine Device Administrators (Skrbniki naprav),
- pogled Device Class Configuration (Konfiguracija razreda naprav) se uporablja za dodelitev ali preprečevanje dostopa do vrst naprav ali posebnih naprav za točno določene uporabnike ali skupine,
- pogled User Access Settings (Nastavitve uporabniškega dostopa) se uporablja za določanje tega, kateri uporabniki si lahko ogledajo ali spreminjajo informacije o preprosti konfiguraciji in konfiguraciji razreda naprav.

Skupina Device Administrators (Skrbniki naprav)

Ob namestitvi orodja Device Access Manager (Upravitelj dostopa do naprav) se ustvari skupina Device Administrators (Skrbniki naprav).

Skrbnik sistema lahko uporablja preprost pravilnik nadzora dostopa do naprav tako, da preprečuje dostop do nekaterih razredov naprav, razen v primeru, če je uporabnik označen za zaupnega (glede dostopa do naprav). Priporočen način razločevanja med uporabniki, ki se jim naprave zaupajo, in med tistimi, ki se jim ne, je ta, da vse uporabnike, ki se jim naprave zaupajo, včlanite v skupino Device Administrators (Skrbniki naprav). Če članom skupine Device Administrators (Skrbniki naprav) omogočite dostop do naprav prek pogledov Simple Configuration (Preprosta konfiguracija) ali Device Class Configuration (Konfiguracija razreda naprav), boste zagotovili, da imajo uporabniki, ki se jim naprave zaupajo, popoln dostop do določenega nabora razredov naprav.

OPOMBA: Dodajanje uporabnika v skupino Device Administrators (Skrbniki naprav) še ne pomeni, da mu samodejno dovolite dostop do naprav. Pogled Simple Configuration (Preprosta konfiguracija) lahko uporabljate za omogočanje dostopa do zahtevanega nabora razredov naprav za uporabnike, ki jim naprave zaupajo.

Če želite dodati uporabnike v skupino Device Administrators (Skrbniki naprav), sledite tem korakom:

- Za operacijski sistem Windows 7, Vista ali XP Professional uporabite standardni »snap-in« (vgradek) »Local Users and Groups« (Lokalni uporabniki in skupine).
- Za domače različice operacijskih sistemov Windows 7, Vista® ali XP v prednostnem računu vnesite naslednji niz v okno ukaznega poziva:

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

Simple Configuration (Preprosta konfiguracija)

Skrbniki in pooblaščeni uporabniki lahko s preprosto konfiguracijo spreminjajo dostop za vse, ki niso skrbniki naprav, do spodnjih razredov naprav:

OPOMBA: Če želita uporabnik ali skupina uporabnikov uporabljati ta pogled za branje informacij o dostopu do naprave, morata imeti v pogledu **User Access Settings (Nastavitve uporabniškega dostopa)** dovoljen dostop za branje. Če želita uporabnik ali skupina uporabnikov uporabljati ta pogled za branje informacij o dostopu do naprave, morata imeti v pogledu **User Access Settings (Nastavitve uporabniškega dostopa)** dovoljen dostop za branje.

- Vsi odstranljivi mediji (diskete, ključi USB itd.)
- Vsi pogoni DVD/CD-ROM
- Vsa zaporedna in vzporedna vrata
- Vse naprave Bluetooth®
- Vse infrardeče naprave
- Vse modemske naprave
- Vse naprave PCMCIA
- Vse naprave 1394

Če želite dovoliti ali zavrniti dostop do razredov naprav za vse, ki niso skrbniki naprav, storite naslednje:

1. V levem podoknu kliknite **HP ProtectTools Administrative Console** in nato **Device Access Manager (Upravitelj dostopa do naprav)** ter **Simple Configuration (Preprosta konfiguracija)**.
2. Dostop zavrnete tako, da v desnem podoknu označite potrditveno polje za razred naprave ali posebno napravo. Če želite dovoliti dostop do tega razreda naprave ali do posebne naprave, potrditveno polje počistite.

   Če je potrditveno polje označeno s sivo barvo, so bile vrednosti, ki vplivajo na scenarije dostopa, spremenjene v pogledu konfiguracije razreda naprave. Vrednosti ponovno nastavite nazaj na enostavne nastavitve tako, da potrditveno polje, ki ga želite počistiti ali nastaviti, kliknete in nato kliknete **Yes (Da)** za potrditev.
3. Kliknite ikono **Save (Shrani)**.

   OPOMBA: Če storitev v ozadju ne teče, se odpre pogovorno okno, ki vpraša, ali jo želite zagnati. Kliknite **Yes (Da)**.
4. Kliknite **OK (V redu)**.

Zagon storitev v ozadju

Preden se lahko uveljavijo profili naprav, orodje HP ProtectTools Security Manager odpre pogovorno okno in vpraša, ali bi želeli zagnati storitev v ozadju HP ProtectTools Device Locking/Auditing (Zaklepanje/revidiranje HP ProtectTools). Kliknite **Yes (Da)**. Storitev v ozadju se zažene in se bo od zdaj dalje samodejno zagnala ob vsakem zagonu operacijskega sistema.

OPOMBA: Preden se lahko prikaže poziv storitve v ozadju, mora biti nastavljen profil naprave.

To storitev lahko zaganjajo in ustavljajo tudi skrbniki:

1. Kliknite **Start** in nato **Nadzorna plošča**.
2. Kliknite **Skrbniška orodja** in nato **Storitve**.
3. Poiščite storitev **HP ProtectTools Device Locking/Auditing (Zaklepanje/revidiranje HP ProtectTools)**.

Zaustavitev storitve zaklepanja/revidiranja naprave ne zaustavi tudi zaklepanja naprave. Dve komponenti uveljavljata zaklepanje naprave:

- storitev Device Locking/Auditing (Zaklepanje/revidiranje naprave) in
- gonilnik DAMDrv.sys.

Zagon naprave zažene njen gonilnik, vendar zaustavitev naprave ne zaustavi gonilnika.

Če želite ugotoviti, ali storitev v ozadju deluje, odprite okno ukaznega poziva in vanj vnesite sc query flcdlock.

Če želite ugotoviti, ali gonilnik naprave deluje, odprite okno ukaznega poziva in vanj vnesite sc query damdrv.

Konfiguracija razreda naprave

Skrbniki in pooblaščeni uporabniki lahko pregledujejo in spreminjajo sezname uporabnikov in skupin, ki jim je dostop do razredov naprav ali posebnih naprav dovoljen ali zavrnjen.

OPOMBA: Če želita uporabnik ali skupina uporabnikov uporabljati ta pogled za branje informacij o dostopu do naprave, morata imeti v pogledu **User Access Settings (Nastavitve uporabniškega dostopa)** dovoljen dostop za branje. Če želita uporabnik ali skupina uporabnikov uporabljati ta pogled za branje informacij o dostopu do naprave, morata imeti v pogledu **User Access Settings (Nastavitve uporabniškega dostopa)** dovoljen dostop za branje.

Pogled Device Class Configuration (Konfiguracija razreda naprave) ima naslednje razdelke:

- **Device List (Seznam naprav)** – kaže vse razrede naprav in naprave, ki so nameščene v sistemu ali pa so bile v njem nameščene prej.
  - Za razred naprave je ponavadi uveljavljena zaščita. Izbrana uporabnik ali skupina bosta lahko dostopala do katere koli naprave v razredu naprave.
  - Zaščita se lahko uveljavlja tudi na posebnih napravah.
- **User List (Seznam uporabnikov)** – prikazuje vse uporabnike in skupine, ki jim je dostop do izbranega razreda naprave ali posebne naprave dovoljen ali zavrnjen.
  - Seznam uporabnikov je lahko sestavljen za določenega uporabnika ali pa za skupino, katere član je uporabnik.
  - Če vnos uporabnika ali skupine v seznamu uporabnikov ni na voljo, nastavitev izhaja iz razreda naprave v seznamu naprav ali pa iz mape Class (Razred).
  - Nekatere razrede naprav, na primer DVD in CD-ROM, je mogoče nadzirati še tako, da jim dostop dovolite ali zavrnete ločeno za operaciji branja in pisanja.

Tako kot za druge naprave in razrede se lahko tudi tu pravice dostopa za branje in pisanje nasledijo. Dostop za branje se lahko na primer nasledi od višjega razreda, medtem ko je dostop za pisanje za uporabnika ali skupino izrecno prepovedan.

OPOMBA: Če potrditveno polje ni označeno, vneseni nadzor nad dostopom nima vpliva na dostop do naprave za branje. Dostopa do naprave za branje niti podeljuje niti ne zavrača.

Primer 1 – če je uporabniku ali skupini dostop za pisanje do naprave ali razreda naprav zavrnjen:

Istemu uporabniku, isti skupini ali članu iste skupine se lahko dostop za pisanje ali za branje in pisanje dodeli samo za napravo, ki je tej napravi v hierarhiji naprav podrejena.

Primer 2 – če je uporabniku ali skupini dostop za pisanje do naprave ali razreda naprav dovoljen:

Istemu uporabniku, isti skupini ali članu iste skupine se lahko dostop za pisanje ali za branje in pisanje zavrne samo za isto napravo ali za napravo, ki ji je v hierarhiji naprav podrejena.

Primer 3 – če je uporabniku ali skupini dostop za branje do naprave ali razreda naprav dovoljen:

Istemu uporabniku, isti skupini ali članu iste skupine se lahko dostop za branje ali za branje in pisanje zavrne samo za isto napravo ali za napravo, ki ji je v hierarhiji naprav podrejena.

Primer 4 – če je uporabniku ali skupini dostop za branje do naprave ali razreda naprav zavrnjen:

Istemu uporabniku, isti skupini ali članu iste skupine se lahko dostop za branje ali za branje in pisanje dodeli samo za napravo, ki je tej napravi v hierarhiji naprav podrejena.

Primer 5 – če je uporabniku ali skupini dostop za branje in pisanje do naprave ali razreda naprav dovoljen:

Istemu uporabniku, isti skupini ali članu iste skupine se lahko dostop za pisanje ali za branje in pisanje zavrne samo za isto napravo ali za napravo, ki ji je v hierarhiji naprav podrejena.

Primer 6 – če je uporabniku ali skupini dostop za branje in pisanje do naprave ali razreda naprav zavrnjen:

Istemu uporabniku, isti skupini ali članu iste skupine se lahko dostop za branje ali za branje in pisanje dodeli samo za napravo, ki je tej napravi v hierarhiji naprav podrejena.

Zavrnitev dostopa uporabniku ali skupini

Če želite uporabniku ali skupini preprečiti dostop do naprave ali razreda naprav, naredite naslednje:

1. V levem podoknu kliknite **HP ProtectTools Administrative Console** in nato **Device Access Manager (Upravitelj dostopa do naprav)** ter **Device Class Configuration (Konfiguracija razreda naprave)**.
2. Na seznamu naprav kliknite razred naprave, ki jo želite konfigurirati.
   - Razred naprave
   - Vse naprave
   - Posamezna naprava

3. V možnosti **User/Groups (Uporabnik/Skupina)** kliknite uporabnika ali skupino, ki naj ima zavrnjen dostop.

4. Ob imenu uporabnika ali skupine kliknite **Deny (Zavrni)**.

5. Kliknite ikono **Save (Shrani)**.

OPOMBA: Kadar so nastavitve za zavrnitev in omogočanje dostopa za uporabnika nastavljene na ravni iste naprave, ima zavrnitev dostopa prednost pred omogočanjem.

Omogočanje dostopa za uporabnika ali skupino

Če želite uporabniku ali skupini dovoliti dostop do naprave ali razreda naprav, naredite naslednje:

1. V levem podoknu kliknite **HP ProtectTools Administrative Console** in nato **Device Access Manager (Upravitelj dostopa do naprav)** ter **Device Class Configuration (Konfiguracija razreda naprave)**.

2. Na seznamu naprav kliknite eno od naslednjih možnosti:

   - Razred naprave
   - Vse naprave
   - Posamezna naprava

3. Kliknite **Add (Dodaj)**.

   Odpre se pogovorno okno **Select Users or Groups (Izberi uporabnike ali skupine)**.

4. Kliknite možnost **Advanced (Napredno)** in nato kliknite **Find Now (Najdi zdaj)**, da poiščete uporabnike ali skupine, ki jih želite dodati.

5. Kliknite uporabnika ali skupino, ki jo želite dodati na seznam razpoložljivih uporabnikov ali skupin, nato pa kliknite **OK (V redu)**.

6. Ponovno kliknite **OK (V redu)**.

7. Dostop za tega uporabnika ali skupino dovolite tako, da kliknete **Allow (Dovoli)**.

8. Kliknite ikono **Save (Shrani)**.

Odstranjevanje dovoljenja za dostop za uporabnika ali skupino

Če želite uporabniku ali skupini odstraniti dovoljenje za dostop do naprave ali razreda naprav, naredite naslednje:

1. V levem podoknu kliknite **HP ProtectTools Administrative Console** in nato **Device Access Manager (Upravitelj dostopa do naprav)** ter **Device Class Configuration (Konfiguracija razreda naprave)**.

2. Na seznamu naprav kliknite razred naprave, ki jo želite konfigurirati.

   - Razred naprave
   - Vse naprave
   - Posamezna naprava

3. V možnosti **User/Groups (Uporabnik/Skupina)** kliknite uporabnika ali skupino, ki ju želite odstraniti, nato pa kliknite **Remove (Odstrani)**.

4. Kliknite ikono **Save (Shrani)**.

Omogočanje dostopa do razreda naprav za enega uporabnika iz skupine

Če želite enemu od uporabnikov iz skupine dovoliti dostop do razreda naprav, drugim uporabnikom te skupine pa ga zavrniti, naredite naslednje:

1. V levem podoknu kliknite **HP ProtectTools Administrative Console** in nato **Device Access Manager (Upravitelj dostopa do naprav)** ter **Device Class Configuration (Konfiguracija razreda naprave)**.

2. Na seznamu naprav kliknite razred naprave, ki jo želite konfigurirati.

   - Razred naprave
   - Vse naprave
   - Posamezna naprava

3. V možnosti **User/Groups (Uporabnik/Skupina)** izberite skupino, ki naj ima zavrnjen dostop, in nato kliknite **Deny (Zavrni)**.

4. Pomaknite se do mape, ki je pod mapo za zahtevani razred, in dodajte tega posebnega uporabnika.

5. Dostop za tega uporabnika dovolite tako, da kliknete **Allow (Dovoli)**.

6. Kliknite ikono **Save (Shrani)**.

Omogočanje dostopa do določene naprave za enega uporabnika iz skupine

Skrbniki lahko za vse naprave v razredu enemu od uporabnikov iz skupine dovolijo dostop do določene naprave, drugim pa ga zavrnejo:

1. V levem podoknu kliknite **HP ProtectTools Administrative Console** in nato **Device Access Manager (Upravitelj dostopa do naprav)** ter **Device Class Configuration (Konfiguracija razreda naprave)**.

2. Na seznamu naprav kliknite razred naprave, ki jo želite konfigurirati in se nato pomaknite do mape, ki je en nivo nižje.

3. Kliknite **Add (Dodaj)**. Odpre se pogovorno okno **Select Users or Groups (Izberi uporabnike ali skupine)**.

4. Kliknite možnost **Advanced (Napredno)** in nato **Find Now (Najdi zdaj)**, da poiščete skupino uporabnika, ki ji želite preprečiti dostop do vseh naprav v razredu.

5. Izberite skupino in kliknite **OK (V redu)**.

6. Pomaknite se do tiste naprave v razredu naprav, do katere želite uporabniku omogočiti dostop.

7. Kliknite **Add (Dodaj)**. Odpre se pogovorno okno **Select Users or Groups (Izberi uporabnike ali skupine)**.

8. Kliknite možnost **Advanced (Napredno)** in nato kliknite **Find Now (Najdi zdaj)**, da poiščete uporabnike ali skupine, ki jih želite dodati.

9. Kliknite uporabnika, ki mu želite omogočiti dostop, in nato **OK (V redu)**.

10. Dostop za tega uporabnika dovolite tako, da kliknete **Allow (Dovoli)**.

11. Kliknite ikono **Save (Shrani)**.

Ponovna nastavitev konfiguracije

△ **POZOR:** Ponovna nastavitev konfiguracije razveljavi vse do zdaj opravljene spremembe konfiguracij naprav in vse nastavitve vrne na tovarniško nastavljene vrednosti.

Če želite ponovno nastaviti konfiguracijo na tovarniške nastavitve, sledite naslednjim korakom:

1. V levem podoknu kliknite **HP ProtectTools Administrative Console** in nato **Device Access Manager (Upravitelj dostopa do naprav)** ter **Device Class Configuration (Konfiguracija razreda naprave)**.

2. Kliknite gumb **Reset (Ponastavi)**.

3. Kliknite **Yes (Da)** za potrditev.

4. Kliknite ikono **Save (Shrani)**.

Napredna opravila

Nadzor nad dostopom do nastavitev konfiguracije

V pogledu **User Access Settings (Nastavitve uporabniškega dostopa)** skrbniki določijo uporabnike ali skupine, ki jim je omogočena uporaba strani za preprosto nastavitev in konfiguracijo razreda naprave.

OPOMBA: Za spreminjanje nastavitev v tem pogledu morata uporabnik ali skupina imeti polne skrbniške pravice.

- Ogled informacij o preprosti konfiguraciji in konfiguraciji razreda naprav je uporabniku ali skupini omogočen le, če imata v nastavitvah konfiguracije dovoljen dostop za ogled (samo za branje).
- Spreminjanje informacij o preprosti konfiguraciji in konfiguraciji razreda naprav je uporabniku ali skupini omogočeno le, če imata v nastavitvah konfiguracije dovoljen dostop za spreminjanje.

OPOMBA: Celo člani skrbniške skupine morajo imeti za ogled preproste konfiguracije in konfiguracije razreda naprav dovoljen dostop za branje, za spreminjanje omenjenih konfiguracij pa dovoljen dostop za spreminjanje.

OPOMBA: Če uporabnik po določitvi ravni dostopa za vse uporabnike in skupine nima niti zavrnjenega niti omogočenega dostopa do posamezne ravni, je temu uporabniku dostop na tej ravni zavrnjen.

Omogočanje dostopa za obstoječega uporabnika ali skupino

Če želite obstoječi skupini ali uporabniku dovoliti ogled ali spreminjanje nastavitev konfiguracije, sledite tem korakom:

1. V levem podoknu konzole **HP ProtectTools Administrative Console** kliknite **Device Access Manager (Upravitelj dostopa do naprav)** in nato **User Access Settings (Nastavitve uporabniškega dostopa)**.
2. Kliknite skupino ali uporabnika, ki jima želite omogočiti dostop.
3. V razdelku **Permissions (Dovoljenja)** kliknite **Allow (Dovoli)** za vsako od vrst dovoljenj, ki jih želite dodeliti izbrani skupini ali uporabniku:

   OPOMBA: Dovoljenja se kopičijo. Na primer: uporabniku, ki mu je omogočeno spreminjanje nastavitev konfiguracije, je samodejno omogočen tudi ogled teh nastavitev (samo za branje). Uporabnik, ki ima polne skrbniške pravice, ima tudi dovoljenje za spreminjanje in ogled (samo za branje) nastavitev konfiguracije.

   - Polne skrbniške pravice
   - Spreminjanje nastavitev konfiguracije
   - Ogled nastavitev konfiguracije (samo za branje)
4. Kliknite ikono **Save (Shrani)**.

Zavrnitev dostopa za obstoječega uporabnika ali skupino

Če želite obstoječi skupini ali uporabniku zavrniti ogled ali spreminjanje nastavitev konfiguracije, sledite tem korakom:

1. V levem podoknu konzole **HP ProtectTools Administrative Console** kliknite **Device Access Manager (Upravitelj dostopa do naprav)** in nato **User Access Settings (Nastavitve uporabniškega dostopa)**.
2. Kliknite skupino ali uporabnika, ki jima želite zavrniti dostop.
3. V razdelku **Permissions (Dovoljenja)** kliknite **Deny (Zavrni)** za vsako od zavrnitev, ki jih želite dodeliti izbrani skupini ali uporabniku:
   - Polne skrbniške pravice
   - Spreminjanje nastavitev konfiguracije
   - Ogled nastavitev konfiguracije (samo za branje)
4. Kliknite ikono **Save (Shrani)**.

Dodajanje nove skupine ali uporabnika

Če želite novi skupini ali uporabniku dovoliti ogled ali spreminjanje nastavitev konfiguracije, sledite tem korakom:

1. V levem podoknu konzole **HP ProtectTools Administrative Console** kliknite **Device Access Manager (Upravitelj dostopa do naprav)** in nato **User Access Settings (Nastavitve uporabniškega dostopa)**.
2. Kliknite **Add (Dodaj)**. Odpre se pogovorno okno **Select Users or Groups (Izberi uporabnike ali skupine)**.
3. Kliknite možnost **Advanced (Napredno)** in nato kliknite **Find Now (Najdi zdaj)**, da poiščete uporabnike ali skupine, ki jih želite dodati.
4. Kliknite skupino ali uporabnika, nato **OK (V redu)** in še enkrat **OK (V redu)**.
5. Dostop za tega uporabnika dovolite tako, da kliknete **Allow (Dovoli)**.
6. Kliknite ikono **Save (Shrani)**.

Odstranjevanje dostopa za skupino ali uporabnika

Če želite uporabniku ali skupini odstraniti dovoljenje za ogled ali spreminjanje nastavitev konfiguracije, sledite tem korakom:

1. V levem podoknu konzole **HP ProtectTools Administrative Console** kliknite **Device Access Manager (Upravitelj dostopa do naprav)** in nato **User Access Settings (Nastavitve uporabniškega dostopa)**.
2. Izberite skupino ali uporabnika in kliknite **Remove (Odstrani)**.
3. Kliknite ikono **Save (Shrani)**.

Povezana dokumentacija

Orodje Device Access Manager for HP ProtectTools (Upravitelj dostopa do naprav za HP ProtectTools) je združljivo z izdelkom za poslovna okolja HP ProtectTools Enterprise Device Access Manager. Pri delu v poslovnem okolju orodje Device Access Manager for HP ProtectTools dovoli samo bralni dostop do svojih funkcij.

Več informacij o orodju Device Access Manager for HP ProtectTools je na voljo na spletni strani http://www.hp.com/hps/security/products.

11 LoJack Pro za HP ProtectTools

Storitev Computrace LoJack Pro, ki deluje s programsko opremo Absolute Software (naprodaj posebej) rešuje naraščajoče težave z izgubljenimi ali ukradenimi računalniki.

Z aktivacijo te programske opreme začne delovati agent Computrace, ki deluje tudi, če je trdi disk ponovno formatiran ali zamenjan.

LoJack Pro omogoča, da računalnik lahko nadzirate, z njim upravljate in mu sledite na daljavo. V primeru izgube ali kraje računalnika vam ga bo ekipa za programsko opremo Absolute Recovery Team pomagala najti.*

OPOMBA: *Ta funkcija je odvisna od geografske lokacije. Podrobnosti si oglejte v naročniški pogodbi za programsko opremo Absolute Software.

12 Odpravljanje težav

Upravitelj varnosti HP ProtectTools Security Manager

Kratek opis	Podrobnosti	Rešitev
Pametne kartice in žetoni USB so zdaj na voljo v upravitelju varnosti Security Manager, če so bili nameščeni po namestitvi upravitelja varnosti.	Pametne kartice in žetone USB lahko v upravitelju varnosti Security Manager uporabljate le, če ste pred namestitvijo upravitelja Security Manager namestili podporno programsko opremo (gonilnike, ponudnike PKCS#11 itd.). Če imate upravitelja Security Manager že nameščenega, po namestitvi podporne programske opreme za pametno kartico ali žeton sledite naslednjim navodilom:	Prijavite se v upravitelja gesel Password Manager. V upravitelju varnosti HP ProtectTools Security Manager kliknite **Password Manager (Upravitelj gesel)** in nato **Credentials (Poverilnice)** ter **Smart Card (Pametna kartica)** Če bo zahtevano, ponovno zaženite računalnik.
Nekatere aplikacijske spletne strani ustvarijo napake, ki uporabnikom preprečujejo izvajanje ali izvrševanje opravil.	Nekatere spletne aplikacije prenehajo delovati in javijo napake zaradi vzorca onemogočanja delovanja enojne prijave SSO. Na primer **!** v rumenem trikotniku, ki se prikaže na Internet Explorerju, pomeni, da je prišlo do napake.	Funkcija Security Manager Single Sign On ne podpira vseh spletnih vmesnikov programske opreme. Podporo funkcije Single Sign On za določeno spletno stran onemogočite tako, da izklopite podporo Single Sign On. Oglejte si celotno dokumentacijo funkcije za enkraten vpis, ki je v datotekah pomoči za programsko opremo upravitelja varnosti Security Manager. Če določene enojne prijave (SSO) ni možno onemogočiti za določeno aplikacijo, pokličite tehnično pomoč podjetja HP in zahtevajte podporo 3. ravni.
Med postopkom prijave možnost **Browse for Virtual Token (Išči navidezni žeton)**.	Uporabnik ne more spremeniti lokacije registriranega virtualnega žetona v upravitelju gesel Password Manager, ker je zaradi zmanjšanja varnostnih tveganj možnost brskanja odstranjena.	Možnost brskanja je bila odstranjena, ker je tem, ki niso uporabniki, omogočala, da zbrišejo in preimenujejo datoteke in nadzirajo program Windows.
Skrbniki domene ne morejo spremeniti gesla za Windows, četudi imajo pooblastilo.	To se zgodi, kadar se skrbnik domene prijavi v domeno in registrira njeno identiteto z upraviteljem gesel Password Manager ter pri tem uporabi račun s skrbniškimi pravicami v domeni in lokalnem računalniku. Če skrbnik domene skuša spremeniti geslo za Windows iz upravitelja gesel Password Manager, dobi sporočilo o napaki pri prijavi: **User account restriction (Omejitev uporabniškega računa)**.	Z upraviteljem gesel Password Manager ne morete spremeniti gesla računa uporabnika domene z možnostjo **Change Windows password (Spremeni geslo za Windows)**. Z njim lahko spremenite le geslo računa lokalnega računalnika. Uporabnik domene lahko spremeni svoje geslo z možnostjo **Change password (Spremeni geslo)** v **Windows security (Varnost za Windows)**, ker pa v lokalnem računalniku nima računa, lahko v upravitelju Password Manager spremenite le geslo za prijavo.
Upravitelj gesel Password Manager ni popolnoma združljiv z geslom GINA za Corel WordPerfect 12.	Če se uporabnik prijavi v upravitelja gesel Password Manager, ustvari dokument s programom WordPerfect in ga shrani kot zaščitenega z geslom,	HP išče načine, kako bi se temu izognil pri prihodnjih razširitvah izdelka.

Kratek opis	Podrobnosti	Rešitev
	Password Manager ne more ne ročno ne samodejno odkriti ali zaznati gesla GINA.	
Password Manager ne prepozna gumba **Connect (Poveži)** na zaslonu.	Če so nastavitve za enojno prijavo za daljinsko povezavo namizja (RDP) nastavljene na **Connect (Poveži)**, ko ponovno zaženete enojno prijavo, zmeraj vnese **Save As (Shrani kot)** namesto **Connect (Poveži)**.	HP išče načine, kako bi se temu izognil pri prihodnjih razširitvah izdelka.
Samo pri paketu Windows XP Service Pack 1 velja, da se uporabnik po prehodu iz načina varčevanja v način mirovanja ne more prijaviti v upravitelja gesel Password Manager.	Ko je sistemu omogočen prehod v način mirovanja in varčevanja, se skrbnik ali uporabnik ne moreta prijaviti v upravitelja gesel Password Manager; ne glede na to, katere poverilnice za prijavo so izbrane (geslo, prstni odtis ali kartica Java), ostane prijavni zaslon Windows prikazan.	Posodobite operacijski sistem Windows na Service Pack 2 z možnostjo Windows Update. Več informacij o vzroku težave najdete v članku 813301 zbirke Microsoft Knowledge Base na spletni strani http://www.microsoft.com. Uporabnik se lahko prijavi šele potem, ko izbere upravitelja gesel Password Manager in se prijavi prek njega. Po prijavi v Password Manager je uporabnik pozvan, naj se prijavi v sistem Windows (morda bo moral možnost za prijavo v sistem Windows posebej izbrati) in tako zaključi postopek prijave. Če se uporabnik naprej prijavi v sistem Windows, se mora nato ročno prijaviti v Password Manager.
Varnostni postopek **Restore Identity (Obnovi identiteto)** izgubi povezavo z navideznim žetonom.	Ko uporabnik obnovi svojo identiteto, lahko Password Manager izgubi povezavo z lokacijo virtualnega žetona na prijavnem zaslonu. Čeprav ima Password Manager registriran virtualni žeton, mora uporabnik žeton ponovno registrirati in tako obnoviti povezavo.	Postopek je trenutno takšen. Ob odstranjevanju upravitelja varnosti Security Manager brez ohranjevanja identitet se sistemski (strežniški) del žetona uniči, zato žetona ni mogoče več uporabljati za prijavo, pa čeprav se odjemalčev del žetona z obnovitvijo identitete obnovi. HP trenutno išče dolgoročne rešitve.

Device Access Manager za HP ProtectTools

Uporabnikom je dostop do naprav v upravitelju dostopa do naprav Device Access Manager onemogočen, naprave pa so še vedno dostopne.

- **Razlaga**: v upravitelju dostopa do naprav Device Access Manager se za preprečevanje uporabniškega dostopa do naprav uporabljata preprosta konfiguracija in konfiguracija razreda naprav. Čeprav jim je dostop zavrnjen, uporabniki do naprav še vedno lahko pridejo.
- **Rešitev:**
  - Prepričajte se, da se je storitev HP ProtectTools Device Locking (Zaklepanje naprave HP ProtectTools) zagnala.
  - Kot skrbniški uporabnik kliknite **Nadzorna plošča** in nato **Sistem in vzdrževanje**. V oknu Skrbniška orodja kliknite **Storitve** in poiščite storitev **HP ProtectTools Device Locking/ Auditing (Zaklepanje/revidiranje naprav HP ProtectTools)**. Preverite, ali ste storitev zagnali in ali je vrsta zagona nastavljena na **Automatic** (Samodejno).

Uporabniku je nepričakovano dovoljen ali zavrnjen dostop do naprave.

- **Razlaga**: upravitelj dostopa do naprav Device Access Manager se uporablja za preprečevanje uporabniškega dostopa do nekaterih naprav in za omogočanje tega dostopa do drugih naprav. Ko je uporabnik v sistemu, lahko dostopa do naprav, za katere misli, da mu je Device Access Manager zavrnil dostop do njih, zavrnjen pa mu je dostop do naprav, za katere misli, da bi mu jih moral Device Access Manager omogočiti.
- **Rešitev:**
  - S konfiguracijo razreda naprave Device Class Configuration v upravitelju dostopa do naprav Device Access Manager raziščite, kakšne so nastavitve uporabnika za napravo.
  - Kliknite **Security Manager (Upravitelj varnosti)**, **Device Access Manager (Upravitelj dostopa do naprave)** in kliknite **Device Class Configuration (Konfiguracija razreda naprave)**. Razširite ravni drevesa Device Class in preglejte nastavitve, uporabljene za tega uporabnika. Preverite, ali je kakšno od dovoljenj uporabnika ali katere koli skupine Windows, katere član je uporabnik (na primer uporabniške – Users ali skrbniške – Administrators) zavrnjeno (nastavljeno na »Deny«).

Omogočanje ali zavrnitev – kaj ima prednost?

- **Razlaga**: v konfiguraciji razreda naprav je nastavljena ta konfiguracija:
  - Skupini Windows (na primer vgrajenim skrbnikom, BUILTIN/Administrators) je bilo podeljeno dovoljenje Allow (Dovoli), drugi skupini Windows (na primer vgrajenim uporabnikom, BUILTIN \Users) pa je bilo podeljeno dovoljenje Deny (Zavrni) na isti ravni znotraj hierarhije naprav (na primer pri pogonih DVD/CD-ROM).
  - Če je uporabnik član obeh skupin (na primer skrbnik), katero članstvo ima prednost?
- **Rešitev:**
  - Uporabniku je dostop do naprave zavrnjen. Zavrnitev ima prednost pred omogočanjem.
  - Dostop je zavrnjen zaradi načina, kako sistem Windows izvaja veljavno dovoljenje za napravo. Eni od skupin je dostop zavrnjen, drugi je omogočen, uporabnik pa je član obeh skupin. Uporabniku je dostop zavrnjen, ker ima zavrnitev dostopa prednost pred omogočanjem.

- Ena od zvijač je zavrnitev dostopa za skupino uporabnikov na ravni pogonov DVD/CD-ROM in omogočanje dostopa za skupino skrbnikov na eni ravni nižje od ravni pogonov DVD/CD-ROM.
- Druga možnost je, da ustvarite posebni skupini Windows, eno za omogočanje dostopa do pogonov DVD/CD in drugo za zavrnitev dostopov do teh pogonov. Ustrezni skupini nato dodajte ustrezne uporabnike.

Pogled preproste konfiguracije Simple Configuration se uporablja za določanje pravilnika nadzora nad dostopom do naprav, vendar skrbniški uporabniki do naprav ne morejo dostopati.

- **Razlaga**: preprosta konfiguracija zavrača dostop uporabnikom in gostom, omogoča pa ga skrbnikom naprav.
- **Rešitev:** Skrbniškega uporabnika dodajte v skupino skrbnikov naprav.

Razno

Prizadeta programska oprema – kratek opis	Podrobnosti	Rešitev
Upravitelj varnosti – prejeto opozorilo: **The security application can not be installed until the HP Protect Tools Security Manager is installed (Namestitev varnostne aplikacije ni možna, dokler ne namestite upravitelja varnosti HP ProtectTools Security Manager)**.	Vse varnostne aplikacije, kakršni sta modul Java Card Security in biometrija, so razširljivi vtičniki za vmesnik Security Manager. Varnostnega vtičnika, ki ga je odobrilo podjetje HP, ne morete naložiti, dokler ne namestite upravitelja varnosti Security Manager.	Preden namestite varnostne vtičnike, morate namestiti programsko opremo upravitelja varnosti Security Manager.
HP ProtectTool Security Manager – prekinjeno; pojavi se napaka, ko zaprete vmesnik programa Security Manager.	V presledkih (1 od 12 poskusih) se pojavlja napaka, ko pritisnete tipko Zapri zgoraj desno na zaslonu, da bi zaprti Security Manager, preden se naložijo vse aplikacije vtičnikov.	To je povezano s časovno uskladitvijo nalaganja storitve vtičnika, ko zaprete in ponovno zaženete program Security Manager. Ker je PTHOST.exe lupina, v kateri so še ostale aplikacije (vtičniki), je odvisno od sposobnosti vtičnika, da zaključi svoj čas nalaganja (storitve). Glavni razlog napake je, če lupino zaprete, preden se je vtičnik naložil. Počakajte, da Security Manager zaključi sporočilo o nalaganju storitev (vidno na vrhu okna programa Security Manager) in da se vsi vtičniki pojavijo v levem stolpcu. Da bi preprečili napake, pustite vtičniku dovolj časa za nalaganje.
HP ProtectTools – neomejen dostop ali nenadzorovani skrbniški privilegiji predstavljajo tveganje za varnost.	Med številna tveganja, možna pri neomejenem dostopu do računalnika, spadajo: • izbris PSD, • zlobne spremembe uporabniških nastavitev, • izklop varnostnih pravilnikov in funkcij.	Skrbniki naj uporabljajo »najboljšo prakso« pri omejevanju prednosti končnih uporabnikov in uporabniškega dostopa. Nepooblaščenim uporabnikom ne smete dajati skrbniških pravic.

Besednjak

aktiviranje Opravilo mora biti dokončano, preden so katere koli funkcije modula za šifriranje pogonov Drive Encryption dostopne. Modul Drive Encryption (Šifriranje pogonov) aktivirate s čarovnikom za namestitev HP ProtectTools Setup Wizard. in ga lahko aktivira le skrbnik. Proces aktivacije vključuje aktivacijo programske opreme, šifriranje pogona, ustvarjanje uporabniškega računa in izdelavo varnostne kopije začetnega šifrirnega ključa v izmenljivi napravi za shranjevanje.

arhiv za obnovitev v nujnem primeru Zaščiteno področje za shranjevanje, ki omogoča ponovno šifriranje osnovnih uporabniških ključev z ene platforme lastniškega ključa na drugo.

ATM Orodje Automatic Technology Manager (Upravitelj samodejne tehnologije), ki skrbnikom omrežja omogoča oddaljeno upravljanje sistemov na ravni BIOS.

biometrično Zvrst poverilnic preverjanja pristnosti, ki za prepoznavanje uporabnika uporablja fizično lastnost, npr. prstni odtis.

cikel varnega brisanja Število, ki pove, kolikokrat se algoritem varnega brisanja izvede pri vsakem sredstvu. Večje število ciklov varnega brisanja izberete, bolj varen bo računalnik.

dešifriranje Postopek, ki se uporablja v kriptografiji, za pretvarjanje šifriranih podatkov v navadno besedilo.

digitalni podpis Podatki, poslani skupaj z datoteko, s katerimi se preveri pristnost pošiljatelja materiala in če je bila datoteka po podpisu spremenjena.

digitalno potrdilo Elektronske poverilnice, ki potrjujejo identiteto posameznika ali podjetja, tako da identiteto lastnika digitalnega potrdila povežejo s parom elektronskih ključev, s katerimi se podpišejo digitalni podatki.

domena Skupina računalnikov, ki so del omrežja in imajo skupno zbirko podatkov imenika. Domene imajo edinstvena imena in zbirko skupnih pravil in postopkov.

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

funkcija Single Sign On (Enkratna prijava) Funkcija, v kateri so shranjeni podatki za preverjanje pristnosti in s katero lahko prek upravitelja varnosti Security Manager dostopate do programov v spletu in operacijskem sistemu Windows, ki preverjajo pristnost z gesli.

funkcija za zaklepanje pogona DriveLock Varnostna funkcija, ki poveže trdi disk z uporabnikom in zahteva, da uporabnik ob zagonu računalnika pravilno vnese geslo funkcije za zaklepanje pogona DriveLock.

geslo za preklic Geslo, ustvarjeno pri zahtevi za digitalno potrdilo. Geslo se zahteva, ko želi uporabnik razveljaviti svoje digitalno potrdilo. Tako je zagotovljeno, da lahko potrdilo prekliče le uporabnik.

gumb Send Security Gumb programske opreme, ki je prikazan v orodni vrstici e-poštnih sporočil programa Microsoft Outlook. S klikom gumba podpišete in/ali šifrirate e-poštno sporočilo programa Microsoft Outlook.

gumb Sign and Encrypt Gumb programske opreme, ki je prikazan v orodni vrstici programov Microsoft Office. S klikom gumba podpišete, šifrirate ali odstranite šifriranje v dokumentu Microsoft Office.

HP SpareKey Varnostna kopija ključa za šifriranje pogonov.

identiteta V upravitelju varnosti HP ProtectTools Security Manager je to skupina poverilnic in nastavitev, ki je obravnavana kot račun ali profil določenega uporabnika.

kartica ID Pripomoček v stranski vrstici Windows Sidebar, ki namizje opremi z vašim uporabniškim imenom in izbrano sliko in mu tako podeli vizualno identiteto. Skrbniško konzolo HP ProtectTools Administrative Console odprete s klikom na kartico ID.

kartica Java Odstranljiva kartica, vstavljena v računalnik. Na njej so podatki za identifikacijo za prijavo. Pri prijavi s kartico Java zaslon za prijavo v orodje Drive Encryption (Šifriranje pogonov) zahteva, da vstavite kartico Java ter vnesete svoje uporabniško ime in PIN kartice.

konzola Osrednje mesto, odkoder lahko dostopate do funkcij in nastavitev tega programa in jih upravljate.

kriptografija Šifriranje in dešifriranje podatkov, da jih lahko razberejo le določeni posamezniki.

migracija Opravilo, s katerim lahko upravljate, obnavljate in prenašate potrdila upravitelja zasebnosti Privacy Manager in zaupne stike.

način naprave SATA Način prenosa podatkov med računalnikom in napravami za masovno shranjevanje, na primer trdimi in optičnimi diski.

način varne prijave Način, uporabljen za prijavo v računalnik.

nadzorna plošča Osrednje mesto, odkoder lahko dostopate do funkcij in nastavitev tega programa in jih upravljate.

navidezni žeton Varnostna funkcija, ki deluje podobno kot bralnik kartice Java ali kartice. Žeton je shranjen na trdem disku v računalniku ali v registru sistema Windows. Ko se prijavljate z virtualnim žetonom, morate za dokončanje preverjanja pristnosti vnesti kodo PIN.

obnovitev Postopek, ki kopira informacije o programu s predhodno shranjene datoteke varnostne kopije v ta program.

omrežni račun Uporabniški ali skrbniški račun programa Windows v lokalnem računalniku, v delovni skupini ali pa v domeni.

overitelj Storitev, ki izdaja potrdila, zahtevana za zagon infrastrukture javnega ključa.

pametna kartica Majhen kos strojne opreme, podobne velikosti in oblike kot plačilna kartica, ki shranjuje informacije za prepoznavanje lastnika. Uporablja se za preverjanje pristnosti lastnika za uporabo računalnika.

pečat za zaupne stike Opravilo, s katerim dodate digitalni podpis, šifrirate e-poštno sporočilo in ga pošljete, potem ko potrdite pristnost z izbranim načinom varne prijave.

PKI Public Key Infrastructure (Infrastruktura javnih ključev) je standard, ki določa vmesnike za ustvarjanje, uporabo in urejanje potrdil in šifrirnih ključev.

ponovni zagon Postopek ponovnega zagona računalnika.

ponudnik storitve šifriranja (CSP) Ponudnik ali zbirka kriptografskih algoritmov, ki se lahko uporabi v dobro določenemu vmesniku za izvajanje določenih kriptografskih funkcij.

pooblaščeni uporabnik Uporabnik, ki mu je bilo v pogledu nastavitve dostopa za uporabnika User Access Settings izdano dovoljenje za ogled ali spreminjanje nastavitev konfiguracije v pogledih preproste konfiguracije ali konfiguracije razreda naprav.

potrdilo Privacy Manager Digitalno potrdilo, ki zahteva preverjanje pristnosti vsakič, ko ga uporabite za šifriranje, na primer zapisovanje in šifriranje e-poštnih sporočil in dokumentov Microsoft Office.

povabilo za zaupni stik E-poštno sporočilo, poslano osebi, za katero želite, da postane zaupni stik.

poverilnice Metoda, s katero uporabnik dokaže sposobnost za določeno nalogo v postopku preverjanja pristnosti.

pravilnik nadzora nad dostopom do naprav Seznam naprav, do katerih ima uporabnik dostop dovoljen ali pa zavrnjen.

predlagani podpisnik Uporabnik, ki ga lastnik dokumenta Microsoft Word ali Microsoft Excel določi, da doda podpis v vrstico za podpis.

pregledovalnik zgodovine Live Messenger History Viewer Komponenta za klepet Privacy Manager Chat, s katero poiščete in si ogledate šifrirano zgodovino klepeta.

prejemnik povabila za zaupni stik Oseba, ki prejme povabilo, da postane zaupni stik.

preprosto brisanje Brisanje sklica operacijskega sistema Windows na sredstvo. Vsebina sredstva ostane na trdem disku, dokler ni s pomočjo varnega čiščenja nezasedenega prostora s prepisovanjem prekrita s podatki.

preverjanje pristnosti Postopek preverjanja, ali je uporabnik pooblaščen za izvedbo opravil, kot so na primer dostop do računalnika, spreminjanje nastavitev določenega programa ali ogledovanje zavarovanih podatkov.

preverjanje pristnosti ob zagonu Varnostna funkcija, ki ob vklopu računalnika zahteva neko obliko preverjanja pristnosti, npr. kartico Java, varnostni čip ali geslo.

prijava Objekt v upravitelju varnosti Security Manager, ki ga sestavljata uporabniško ime in geslo (lahko pa tudi druge izbrane informacije) in ki se lahko uporablja za prijavo na spletna mesta ali v druge programe.

profil varnega brisanja Določen način brisanja in seznam sredstev.

prstni odtis Digitalni zapis slike prstnega odtisa. Security Manager nikoli ne shranjuje dejanske slike prstnega odtisa.

PSD Osebni varni pogon, ki zagotavlja zaščiteno območje za shranjevanje zaupnih podatkov.

razkrivanje Opravilo, ki uporabniku omogoča dešifriranje ene ali več zgodovin klepeta, tako da z navadnim besedilom prikaže zaslonsko ime stika Contact Screen Name in omogoči ogled klepeta.

razred naprave Vse naprave ene vrste, na primer gonilniki.

ročno varno brisanje Takojšnje varno brisanje sredstva ali izbranih sredstev, ki zaobide načrtovano samodejno varno brisanje.

samodejno varno brisanje Načrtovano varno brisanje, ki ga uporabnik nastavi v orodju za čiščenje datoteke File Sanitizer.

seja zgodovine klepeta Šifrirana datoteka, v kateri je poročilo o vsebini pogovora obeh strani v klepetu.

seznam zaupnih stikov Seznam vseh zaupanja vrednih stikov.

sistem šifriranja datotek (EFS) Sistem, ki šifrira vse datoteke in podmape v izbrani mapi.

skrbnik *Glej* »skrbnik sistema Windows«.

skrbnik sistema Windows Uporabnik z vsemi pravicami za spreminjanje dovoljenj in upravljanje drugih uporabnikov.

skupina Skupina uporabnikov, ki imajo enako raven omogočenega ali zavrnjenega dostopa do razreda naprav ali do določene naprave.

sredstvo Podatkovna komponenta, ki vključuje osebne podatke ali datoteke, podatke o zgodovini in spletni vsebini itn., je na trdem disku.

storitev v ozadju Storitev v ozadju HP ProtectTools Device Locking/Auditing (Zaklepanje/revidiranje naprav HP ProtectTools), ki mora delovati, če naj bo pravilnik za nadzor dostopa do naprav uveljavljen. Možno si jo je ogledati na nadzorni plošči, v aplikaciji Storitve znotraj možnosti Skrbniška orodja. Če ne deluje, jo bo upravitelj HP ProtectTools Security Manager ob poskusu uveljavljanja pravilnika za nadzor dostopa do naprav skušal zagnati.

šifriranje Postopek, kot je uporaba algoritma, ki se uporablja v kriptografiji za pretvarjanje navadnega besedila v šifrirano besedilo, da se onemogoči nepooblaščenim prejemnikom branje teh podatkov. Obstaja veliko vrst šifriranja podatkov, ki so osnova varnosti omrežja. Navadne vrste vključujejo Data Encryption Standard in šifriranje javnega ključa.

TXT Trusted Execution Technology (Tehnologija za zaupno izvedbo).

uporabnik Vsi vpisani v modul Drive Encryption (Šifriranje pogonov). Uporabniki, ki niso skrbniki, imajo omejene pravice v modulu Drive Encryption (Šifriranje pogonov). Lahko se le vpišejo (z dovoljenjem skrbnika) in prijavijo.

uporabniški račun Windows Profil posameznika z odobreno prijavo v omrežje ali v posamezni računalnik.

varno brisanje Izvedba algoritma, ki zakrije podatke v sredstvu.

varno čiščenje nezasedenega prostora s prepisovanjem Varno pisanje naključnih podatkov čez izbrisana sredstva za popačenje vsebine izbrisanih sredstev.

varnostna kopija Funkcija varnostnega kopiranja za shranjevanje kopije pomembnih informacij o programu na mesto zunaj programa. To kopijo je mogoče kasneje v istem ali drugem računalniku uporabiti za obnovitev informacij.

vrstica za podpis Označba mesta za prikaz digitalnega podpisa. Ko je dokument podpisan, se prikažeta ime podpisnika in način preverjanja. Dodate lahko tudi datum podpisa in naziv podpisnika.

Windows Logon Security (Zaščita prijave v operacijski sistem Windows) Ščiti vaše račune Windows tako, da za dostop zahteva posebne poverilnice.

zaporedje tipk Kombinacija določenih tipk, ki ob pritisku sprožijo samodejno varno brisanje, na primer ctrl + alt + s.

zaslon za prijavo v orodje Drive Encryption Zaslon za prijavo, ki je prikazan pred zagonom operacijskega sistema Windows. Uporabniki morajo vnesti svoje uporabniško ime in geslo za Windows ali PIN kartice Java. V večini primerov vnos pravilnih informacij na zaslonu za prijavo v orodje Drive Encryption (Šifriranje pogonov) omogoča neposreden dostop v operacijski sistem Windows, ne da bi se bilo treba na zaslonu za prijavo v operacijski sistem Windows ponovno prijaviti.

zaupna komunikacija IM (neposredno sporočanje) Komunikacija, pri kateri so zaupna sporočila poslana od zaupnega pošiljatelja zaupnemu stiku.

zaupni pošiljatelj Zaupni stik, ki pošilja podpisana in/ali šifrirana e-poštna sporočila in dokumente Microsoft Office.

zaupni stik Oseba, ki je sprejela povabilo zaupnega stika.

zaupno sporočilo Komunikacija, pri kateri so zaupna sporočila poslana od zaupnega pošiljatelja zaupnemu stiku.

žeton Glejte način varne prijave.

žeton USB Varnostna naprava, v kateri so shranjeni podatki za identifikacijo uporabnika. Uporablja se za preverjanje pristnosti uporabnika računalnika, podobno kot bralnik kartice Java ali biometrije.

Stvarno kazalo

W

Z