HP ProtectTools
Používateľská príručka

Prvé vydanie: október 2009

Katalógové číslo dokumentu: 572661-231

Obsah

1 Úvod do zabezpečenia

Softvér HP ProtectTools Security Manager poskytuje funkcie zabezpečenia, ktoré pomáhajú chrániť pred nepovoleným prístupom k počítaču, sieťam a dôležitým údajom. Spravovanie nástroja HP ProtectTools Security Manager sa vykonáva prostredníctvom funkcie Administrative Console (Spravovacia konzola).

Použitím konzoly môže lokálny správca vykonávať nasledujúce úlohy:

- Povolenie alebo zakázanie funkcií zabezpečenia
- Registrácia odtlačkov prstov používateľov tohto počítača
- Nastavenie karty Smart Card
- Zadanie požadovaných poverení na overovanie
- Spravovanie používateľov počítača
- Úprava parametrov špecifických pre dané zariadenie
- Konfigurácia nainštalovaných aplikácií softvéru Security Manager
- Pridávanie ďalších aplikácií softvéru Security Manager

Dostupnosť jednotlivých softvérových modulov sa líši podľa modelu počítača.

Moduly pre softvér HP ProtectTools môžu byť vopred nainštalované, vopred zavedené alebo dostupné na prevzatie z webovej lokality spoločnosti HP. Ďalšie informácie nájdete na webovej lokalite http://www.hp.com.

POZNÁMKA: Pokyny v tejto príručke sú napísané s predpokladom, že už máte nainštalované príslušné softvérové moduly HP ProtectTools.

Funkcie modulov HP ProtectTools

V nasledujúcej tabuľke sú uvedené podrobnosti o kľúčových funkciách modulov nástroja HP ProtectTools.

Modul	Kľúčové funkcie
HP ProtectTools – modul Credential Manager	• Aplikácia Password Manager slúži ako osobný trezor pre heslá, pričom zjednodušuje proces prihlasovania pomocou funkcie jediného prihlásenia, ktorá automaticky ukladá a používa používateľské poverenia. • Funkcia jediného prihlásenia tiež ponúka doplnkovú ochranu tým, že vyžaduje na overovanie používateľov kombinácie rôznych technológií zabezpečenia, napríklad Java™ Card a biometrické údaje. • Ukladací priestor pre heslá je chránený softvérovým šifrovaním a jeho ochrana sa dá ďalej zlepšiť overovaním pomocou bezpečnostného zariadenia, ako sú napríklad karty Java Card alebo biometrické údaje. **POZNÁMKA:** Funkcia Credential Manager je k dispozícii v module Password Manager nástroja HP ProtectTools Security Manager
HP ProtectTools – modul Drive Encryption (len niektoré modely)	• Modul Drive Encryption poskytuje kompletné šifrovanie celých zväzkov pevného disku. • Modul Drive Encryption vyžaduje overovanie pred zavedením systému na dešifrovanie a prístup k údajom.
HP ProtectTools – modul Privacy Manager (len niektoré modely)	• Aplikácia Privacy Manager využíva pokročilé prihlasovacie postupy na kontrolu zdroja, integrity a zabezpečenia komunikácie pri používaní e-mailov, dokumentov balíka programov Microsoft® Office alebo okamžitých správ (IM).
HP ProtectTools – modul File Sanitizer	• Modul File Sanitizer umožňuje bezpečne skartovať digitálne aktíva (citlivé údaje vrátane aplikačných súborov, historického alebo webového obsahu alebo iných dôverných údajov) v počítači a pravidelne dôkladne vymazávať údaje z pevného disku.
HP ProtectTools – modul Device Access Manager (len niektoré modely)	• Modul Device Access Manager umožňuje manažérom IT kontrolovať prístup k zariadeniam pomocou používateľských profilov. • Modul Device Access Manager zabraňuje neautorizovaným používateľom odstrániť údaje pomocou externých ukladacích médií a zavedeniu vírusov do systému z externých médií. • Správca môže vypnúť prístup na zapisovateľné médiá pre určité osoby alebo skupiny používateľov.

Dosiahnutie kľúčových bezpečnostných cieľov

Moduly HP ProtectTools môžu fungovať spolu, aby poskytli riešenia rôznych bezpečnostných problémov vrátane týchto kľučových bezpečnostných cieľov:

- Ochrana pred cielenou krádežou
- Obmedzenie prístupu k citlivým údajom
- Zabránenie neoprávnenému prístupu z vnútorných a vonkajších miest
- Vytvorenie silných hesiel
- Priraďovanie regulačných bezpečnostných poverení

Ochrana pred cielenou krádežou

Príkladom cielenej krádeže môže byť krádež počítača obsahujúceho dôverné údaje a informácie o zákazníkoch na bezpečnostnom kontrolnom bode letiska. Pred cielenou krádežou pomáhajú chrániť nasledujúce funkcie:

- Ak je zapnutá funkcia overovania pred zavedením systému, tak pomáha zabrániť prístupu k operačnému systému. Viac sa dozviete v týchto témach:
  - Security Manager
  - Drive Encryption

Obmedzenie prístupu k citlivým údajom

Predstavte si, že zmluvný audítor pracuje u zákazníka a bol mu poskytnutý prístup na kontrolu citlivých finančných údajov; nechcete, aby audítor mohol tlačiť súbory alebo ich ukladať na zapisovateľné zariadenie, ako je napríklad disk CD. Prístup k údajom pomáha obmedziť nasledujúca funkcia:

- Aplikácia Device Access Manager pre nástroj HP ProtectTools umožňuje manažérom IT obmedziť prístup k zapisovateľným zariadeniam, aby sa citlivé údaje nedali vytlačiť alebo skopírovať z pevného disku na vymeniteľné médiá.

Zabránenie neoprávnenému prístupu z vnútorných a vonkajších miest

Neoprávnený prístup do nezabezpečeného počítača predstavuje veľmi konkrétne riziko pre firemné sieťové prostriedky, ako sú napríklad údaje oddelenia finančných služieb, vedúcich pracovníkov alebo tímu pre výskum a vývoj, a pre súkromné údaje, ako sú napríklad záznamy o pacientoch alebo osobné finančné záznamy. Nasledujúce funkcie pomáhajú zabrániť neoprávnenému prístupu:

- Ak je zapnutá funkcia overovania pred zavedením systému, tak pomáha zabrániť prístupu k operačnému systému. Viac sa dozviete v týchto témach:
  - Password Manager
  - Drive Encryption
- Password Manager pomáha zaručiť, aby neoprávnený používateľ nemohol získať heslá alebo prístup k aplikáciám chráneným heslom.

- Aplikácia Device Access Manager pre nástroj HP ProtectTools umožňuje manažérom IT obmedziť prístup k zapisovateľným zariadeniam, aby sa citlivé údaje nedali skopírovať z pevného disku.
- Funkcia DriveLock pomáha zaručiť, aby údaje neboli dostupné ani v prípade vybratia pevného disku a jeho nainštalovania do nezabezpečeného systému.

Tvorba politík silných hesiel

Ak začne platiť pravidlo, ktoré vyžaduje používanie politiky silných hesiel pre množstvo webových aplikácií a databáz, aplikácia Security Manager poskytuje chránený odkladací priestor pre heslá a pohodlie jediného prihlásenia.

Doplnkové bezpečnostné prvky

Priradenie bezpečnostných úloh

Pri správe počítačovej bezpečnosti (najmä v prípade veľkých organizácií) je dôležitým pravidlom rozdelenie zodpovednosti a práv medzi rôzne typy správcov a používateľov.

POZNÁMKA: V malých organizáciách alebo pri individuálnom použití môže mať tieto úlohy ta istá osoba.

V programe HP ProtectTools môžu byť bezpečnostné povinnosti a práva rozdelené do týchto úloh:

- Vedúci bezpečnosti – definuje bezpečnostné úrovne spoločnosti alebo siete a určuje, ktoré bezpečnostné prvky sa použijú, napríklad karty Java™, biometrické čítače alebo súkromné kľúče USB.

  POZNÁMKA: Mnohé z funkcií nástroja HP ProtectTools môže prispôsobiť správca zabezpečenia v spolupráci so spoločnosťou HP. Ďalšie informácie získate na webovej lokalite spoločnosti HP na adrese http://www.hp.com.

- Správca IT – aplikuje a spravuje bezpečnostné prvky definované vedúcim bezpečnosti. Tiež môže zapnúť alebo vypnúť niektoré prvky. Napríklad vedúci bezpečnosti sa rozhodne zaviesť karty Java, správca IT môže zapnúť bezpečnostný režim kariet Java systému BIOS.

- Používateľ – používa bezpečnostné prvky. Napríklad ak vedúci bezpečnosti a správca IT zaviedli v systéme karty Java, používateľ môže nastaviť kód PIN karty Java a kartu použiť na overenie.

UPOZORNENIE: Správcom sa odporúča dodržiavať „najlepšie postupy“ pri obmedzovaní oprávnení koncových používateľov a obmedzovaní prístupu používateľov.

Neoprávnení používatelia by nemali mať pridelené správcovské oprávnenia.

Správa hesiel HP ProtectTools

Väčšina funkcií modulu HP ProtectTools Security Manager je zabezpečená heslami. Nasledujúci zoznam uvádza bežne používané heslá, softvérové moduly, v ktorých sa nastavuje heslo a funkciu hesla.

Takisto sú tu uvedené heslá nastavované a používané výlučne správcami IT. Ostatné heslá môžu byť nastavené obyčajnými používateľmi alebo správcami.

Heslo modulu HP ProtectTools	Nastavte ho v tomto module HP ProtectTools	Funkcia
Prihlasovacie heslo aplikácie Security Manager	Security Manager	Toto heslo má dve možnosti použitia: • Dá sa použiť ako prihlasovacie poverenie aplikácie Security Manager na prístup k aplikácii Security Manager po prihlásení do systému Windows. • Dá sa použiť na súčasné povolenie prístupu do systému Windows a aplikácie Security Manager.
Heslo obnovovacieho súboru aplikácie Security Manager	Security Manager, správcom IT	Chráni prístup k obnovovaciemu súboru aplikácie Security Manager.

Heslo modulu HP ProtectTools	Nastavte ho v tomto module HP ProtectTools	Funkcia
Kód PIN karty Java™ Card	Java Card Security	Chráni prístup k obsahu karty Java Card a slúži na overenie používateľov karty Java Card. Keď sa použije na overovanie pri zapnutí, kód PIN karty Java Card tiež chráni prístup k pomôcke Computer Setup a k obsahu počítača. Autorizuje používateľov programu Drive Encryption, ak bol vybraný súkromný kľúč Java Card.
Prihlasovacie heslo systému Windows	Ovládací panel systému Windows®	Môže sa použiť na ručné prihlásenie alebo môže byť uložené na karte Java Card.

Vytvorenie bezpečného hesla

Pri tvorbe hesiel sa v prvom rade riaďte požiadavkami programu. Vo všeobecnosti však majte na pamäti tieto rady, ktoré vám pomôžu vytvoriť silné heslá a znížiť riziko vzniku slabých hesiel:

- Používajte heslá s viac ako 6 znakmi, najlepšie s viac ako 8 znakmi.
- V hesle striedajte veľkosť písmen.
- Ak je to možné, striedajte alfanumerické znaky, použite špeciálne znaky a interpunkčné znamienka.
- Nahraďte písmená v slove špeciálnymi znakmi alebo číslami. Napríklad číslo 1 použite namiesto písmena I alebo L.
- Kombinujte slová z 2 alebo viacerých jazykov.
- Slovo alebo frázu rozdeľte číslami alebo špeciálnymi znakmi v strede, napríklad „Mary2-2Cat45“.
- Nepoužívajte slovo, ktoré sa nachádza v slovníku.
- Nepoužívajte svoje meno ako heslo, alebo iné osobné informácie, napríklad dátum narodenia, mená zvierat, priezvisko matky za slobodna, dokonca ani v prevrátenom poradí písmen.
- Heslá pravidelne meňte. Môžete zmeniť len niekoľko znakov, ktoré sa zvyšujú.
- Ak si heslo zapíšete, neukladajte ho na viditeľné miesto blízko počítača.
- Neuchovávajte si heslo v súbore, ako je e-mail, v počítači.
- Nezdieľajte kontá a heslo nikomu nehovorte.

Zálohovanie a obnovenie poverení nástroja HP ProtectTools

Pomocou aplikácie Drive Encryption pre nástroj HP ProtectTools môžete vybrať a zálohovať poverenia nástroja HP ProtectTools.

2 Úvodné informácie

POZNÁMKA: Spravovanie nástroja HP ProtectTools vyžaduje oprávnenia správcu.

Sprievodca inštaláciou nástroja HP ProtectTools vás bude sprevádzať nastavením najčastejšie používaných funkcií aplikácie Security Manager. Avšak prostredníctvom spravovacej konzoly nástroja HP ProtectTools máte k dispozícii množstvo ďalších funkčností. Rovnaké nastavenia ako v sprievodcovi, ako aj ďalšie funkcie zabezpečenia, môžete nakonfigurovať prostredníctvom konzoly, ktorá je dostupná z ponuky Štart systému Windows®. Tieto nastavenia sa použijú pre počítač a všetkých používateľov, ktorí zdieľajú počítač.

1. Na úvodnej stránke môžete zakázať ďalšie zobrazovanie sprievodcu výberom jednej z možností.
2. Po týždni nastavovania počítača, alebo keď používateľ s právami správcu prvý raz potiahne prst po snímači odtlačkov prstov, sa automaticky spustí Sprievodca inštaláciou nástroja HP ProtectTools, ktorý vás bude sprevádzať základnými krokmi konfigurácie tohto programu. Automaticky sa spustí videokurz nastavení počítača.
3. Postupujte podľa pokynov na obrazovke, až kým sa nedokončí inštalácia.

Ak nedokončíte sprievodcu, automaticky sa spustí ešte dvakrát. Potom môžete otvoriť sprievodcu z oznamovacieho kontextového okna (vo forme bubliny), ktoré sa zobrazí v blízkosti oblasti oznámení na paneli úloh (pokiaľ ste ho nezakázali podľa popisu v kroku 2 uvedenom vyššie), až kým sa nedokončí inštalácia.

Ak chcete použiť aplikácie nástroja HP ProtectTools Security Manager, spustite nástroj HP ProtectTools Security Manager z ponuky Štart alebo kliknutím pravým tlačidlom myši na ikonu aplikácie Security Manager v oblasti oznámení úplne vpravo na paneli úloh. Spravovacia konzola nástroja HP ProtectTools a jej aplikácie sú k dispozícii všetkým používateľom, ktorí zdieľajú tento počítač.

Otvorenie spravovacej konzoly nástroja HP ProtectTools

Ak chcete vykonávať správcovské úlohy, ako napríklad nastavenie systémových politík alebo konfiguráciu softvéru, otvorte konzolu nasledovne:

- Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools).

  – alebo –

  Na ľavom paneli aplikácie Security Manager kliknite na položku **Administration** (Spravovanie).

Ak chcete vykonávať používateľské úlohy, ako napríklad zaregistrovanie odtlačkov prstov alebo používanie aplikácie Security Manager, otvorte konzolu nasledovne:

- Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Security Manager** (Správca zabezpečenia nástroja HP ProtectTools).

  – alebo –

  Dvakrát kliknite na ikonu aplikácie **HP ProtectTools Security Manager** v oblasti oznámení úplne vpravo na paneli úloh.

Povolenie funkcií zabezpečenia

Sprievodca inštaláciou vás požiada o overenie vašej identity.

1. Prečítajte si úvodnú obrazovku a potom kliknite na tlačidlo **Next** (Ďalej).
2. Overte vašu identitu, buď zadaním hesla systému Windows, ak ešte nemáte zaregistrované žiadne odtlačky prstov, alebo naskenovaním odtlačku prsta pomocou snímača odtlačkov prstov. Kliknite na tlačidlo **Next** (Ďalej).

   Ak je heslo systému Windows prázdne, budete požiadaní o jeho vytvorenie. Heslo systému Windows sa vyžaduje na ochranu konta systému Windows pred prístupom neoprávnených osôb a na používanie funkcií nástroja HP ProtectTools Security Manager.

Sprievodca inštaláciou vás bude sprevádzať procesom povolenia funkcií zabezpečenia, ktoré platia pre všetkých používateľov počítača:

- Prihlasovacie zabezpečenie systému Windows chráni kontá systému Windows vyžadovaním používania špecifických prístupových poverení.
- Aplikácia Drive Encryption chráni vaše údaje prostredníctvom šifrovania pevných diskov, takže údaje si nemôžu prečítať neoprávnené osoby.
- Aplikácia Pre-Boot Security chráni počítač zakázaním prístupu neoprávnených osôb pred spustením systému Windows.

Ak chcete povoliť funkciu zabezpečenia, začiarknite príslušné začiarkavacie políčko. Čím viac funkcií zvolíte, tým bezpečnejší bude váš počítač.

POZNÁMKA: Aplikácia Pre-Boot Security nebude k dispozícii, ak ju nepodporuje systém BIOS.

Registrácia odtlačkov prstov

Ak zvolíte „odtlačok prsta“ a ak má počítač zabudovaný alebo pripojený snímač odtlačkov prstov, zobrazí sa sprievodca procesom nastavenia alebo „registrácie“ odtlačkov prstov:

1. Zobrazí sa obrys dvoch rúk. Prsty, ktoré sú už zaregistrované, sú zvýraznené zelenou farbou. Kliknite na prst na obryse.

   POZNÁMKA: Ak chcete odstrániť predtým zaregistrovaný odtlačok prsta, kliknite na príslušný prst.

2. Po vybratí prsta na registráciu sa zobrazí výzva na nasnímanie daného odtlačku prsta, až kým nebude úspešne zaregistrovaný. Zaregistrovaný prst sa zvýrazní na obryse zelenou farbou.

3. Musíte zaregistrovať aspoň dva prsty; odporúča sa použiť ukazovák alebo prostredník. Zopakujte kroky 1 až 3 pre ďalší prst.

4. Kliknite na tlačidlo **Next** (Ďalej).

POZNÁMKA: Pri registrácii odtlačkov prstov prostredníctvom úvodného procesu sa informácie o odtlačkoch prstov neuložia, kým neklikníte na tlačidlo **Next** (Ďalej). Ak necháte počítač chvíľu nečinný alebo zatvoríte tabuľu, vykonané zmeny sa **neuložia**.

Nastavenie karty Smart Card

Ak zvolíte kartu Smart Card a ak má počítač zabudovanú alebo pripojenú čítačku kariet Smart Card, Sprievodca inštaláciou nástroja HP ProtectTools zobrazí výzvu na nastavenie kódu PIN (osobné identifikačné číslo) karty Smart Card.

Nastavenie kódu PIN karty Smart Card:

1. Na stránke Set up smart card (Nastavenie karty Smart Card) zadajte a potvrďte kód PIN.

   Kód PIN môžete tiež zmeniť. Zadajte starý kód PIN a potom zvoľte nový.

2. Ak chcete pokračovať, kliknite na tlačidlo **Next** (Ďalej).

Používanie spravovacej konzoly

Spravovacia konzola nástroja HP ProtectTools je centrálne umiestnenie na správu funkcií a aplikácií nástroja HP ProtectTools Security Manager.

Konzola obsahuje nasledujúce súčasti:

- **Tools** (Nástroje) – slúži na zobrazenie nasledujúcich kategórií na konfiguráciu zabezpečenia počítača:
  - **Home** (Úvod) – umožňuje vybrať úlohy zabezpečenia na vykonanie.
  - **System** (Systém) – umožňuje konfigurovať funkcie zabezpečenia a overovanie pre používateľov a zariadenia.
  - **Applications** (Aplikácie) – slúži na zobrazenie všeobecných nastavení nástroja HP ProtectTools Security Manager a aplikácií nástroja Security Manager.
  - **Data** (Údaje) – poskytuje rozbaľovaciu ponuku prepojení na aplikácie nástroja Security Manager, ktoré chránia vaše údaje.
- **Management Tools** (Spravovacie nástroje) – poskytuje informácie o ďalších nástrojoch. Panel uvedený nižšie zobrazuje nasledujúce voľby:
  - **HP ProtectTools Setup Wizard** (Sprievodca inštaláciou nástroja HP ProtectTools) – sprevádza vás procesom nastavenia nástroja HP ProtectTools Security Manager.
  - **Help** (Pomocník) – slúži na zobrazenie súboru Pomocníka, ktorý poskytuje informácie o nástroji Security Manager a jeho predinštalovaných aplikáciách. Pomocník pre aplikácie, ktoré môžete pridať, je súčasťou týchto aplikácií.
  - **About** (Informácie) – slúži na zobrazenie informácií o nástroji HP ProtectTools Security Manager, napríklad o čísle verzie a upozornení na autorské práva.
- **Main area** (Hlavná oblasť) – slúži na zobrazenie obrazoviek špecifických pre danú aplikáciu.

Ak chcete otvoriť spravovaciu konzolu nástroja HP ProtectTools, kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools).

3 Konfigurácia systému

Skupina System (Systém) je dostupná z panela ponuky Tools (Nástroje) na ľavej strane obrazovky spravovacej konzoly nástroja HP ProtectTools. Aplikácie v tejto skupine môžete použiť na spravovanie politík a nastavení počítača, jeho používateľov a zariadení.

V skupine System (Systém) sú zahrnuté nasledujúce aplikácie:

- **Security** (Zabezpečenie) – spravovanie funkcií, overovania a nastavení interakcie používateľov s týmto počítačom.
- **Users** (Používatelia) – nastavenie, spravovanie a registrovanie používateľov tohto počítača.
- **Devices** (Zariadenia) – spravovanie nastavení pre bezpečnostné zariadenia zabudované alebo pripojené k počítaču.

Nastavenie overovania pre počítač

V overovacej aplikácii môžete vybrať, ktoré funkcie zabezpečenia majú byť implementované v tomto počítači, nastaviť politiky riadiace prístup k počítaču a konfigurovať ďalšie rozšírené nastavenia. Môžete zadať poverenia vyžadované na overenie identity každej triedy používateľov pri prihlasovaní do systému Windows alebo na webové lokality a do programov počas používateľskej relácie.

Nastavenie overovania pre počítač:

1. V ponuke panela Security (Zabezpečenie) kliknite na položku **Authentication** (Overovanie).
2. Ak chcete konfigurovať overovanie pri prihlasovaní, kliknite na kartu **Logon Policy** (Politika prihlasovania), vykonajte požadované zmeny a kliknite na tlačidlo **Apply** (Použiť).
3. Ak chcete konfigurovať overovanie relácie, kliknite na kartu **Session Policy** (Politika relácie), vykonajte požadované zmeny a kliknite na tlačidlo **Apply** (Použiť).

Politika prihlasovania

Definovanie politík riadiacich poverenia vyžadované na overovanie identity používateľa pri prihlasovaní do systému Windows:

1. V ponuke Tools (Nástroje) kliknite na položku **Security** (Zabezpečenie) a potom kliknite na položku **Authentication** (Overovanie).
2. Na karte **Logon Policy** (Politika prihlasovania) kliknite na kategóriu používateľa.
3. Zadajte overovacie poverenia vyžadované pre vybratú kategóriu používateľa. Musíte zadať aspoň jedno poverenie.
4. Vyberte, či sa vyžaduje na overenie identity používateľa ĽUBOVOĽNÉ (iba jedno) zo zadaných poverení, alebo či sa vyžadujú VŠETKY zo zadaných poverení. Môžete tiež zakázať ľubovoľnému používateľovi prístup k počítaču.
5. Kliknite na tlačidlo **Apply** (Použiť).

Politika relácií

Definovanie politík riadiacich poverenia vyžadované na prístup k aplikáciám nástroja HP ProtectTools počas relácie systému Windows:

1. V ponuke Tools (Nástroje) kliknite na položku **Security** (Zabezpečenie) a potom kliknite na položku **Authentication** (Overovanie).
2. Na karte **Session Policy** (Politika relácií) kliknite na kategóriu používateľa.
3. Zadajte overovacie poverenia vyžadované pre vybratú kategóriu používateľa.
4. Vyberte, či sa vyžaduje na overenie identity používateľa ĽUBOVOĽNÉ (iba jedno) zo zadaných poverení, alebo či sa vyžadujú VŠETKY zo zadaných poverení. Môžete tiež nastaviť, aby sa nevyžadovalo žiadne overovanie na prístup k softvéru HP ProtectTools.
5. Kliknite na tlačidlo **Apply** (Použiť).

Nastavenia

Môžete povoliť jedno alebo viacero z nasledujúcich nastavení zabezpečenia:

- **Allow One Step logon** (Povoliť jednokrokové prihlásenie) – umožňuje používateľom tohto počítača vynechať prihlasovanie do systému Windows, ak bolo overovanie vykonané na úrovni systému BIOS alebo šifrovaného disku.
- **Allow HP SpareKey authentication for Windows logon** (Povoliť overovanie HP SpareKey pre prihlasovanie do systému Windows) – umožňuje používateľom tohto počítača používať funkciu HP SpareKey na prihlásenie do systému Windows napriek ľubovoľnej inej politike overovania vyžadovanej aplikáciou Security Manager.

Úprava nastavení:

1. Kliknutím môžete povoliť alebo zakázať špecifické nastavenie.
2. Kliknutím na tlačidlo **Apply** (Použiť) uložíte vykonané zmeny.

Spravovanie používateľov

V aplikácii Users (Používatelia) môžete monitorovať a spravovať používateľov nástroja HP ProtectTools tohto počítača.

Všetci používatelia nástroja HP ProtectTools sú uvedení a overovaní na základe politík nastavených v aplikácii Security Manager a podľa toho, či majú zaregistrované príslušné poverenia, ktoré im umožňujú splniť tieto politiky.

Ak chcete pridať ďalších používateľov, kliknite na položku **Add** (Pridať).

Ak chcete odstrániť používateľa, kliknite na používateľa a potom kliknite na položku **Delete** (Odstrániť).

Ak chcete zaregistrovať odtlačky prstov alebo nastaviť ďalšie poverenia pre používateľa, kliknite na používateľa a potom kliknite na položku **Enroll** (Zaregistrovať).

Ak chcete zobraziť politiky pre konkrétneho používateľa, vyberte používateľa a potom kliknite na položku **View Policies** (Zobraziť politiky).

Definovanie nastavení zariadení

V aplikácii Device (Zariadenie) môžete definovať nastavenia dostupné pre ľubovoľné zabudované alebo pripojené bezpečnostné zariadenia rozpoznané aplikáciou HP ProtectTools Security Manager.

Odtlačky prstov

Stránka Fingerprints (Odtlačky prstov) obsahuje tri karty: Enrollment (Registrácia), Sensitivity (Citlivosť) a Advanced (Rozšírené).

Enrollment (Registrácia)

Môžete zvoliť minimálny a maximálny počet odtlačkov prstov, ktoré má používateľ povolené zaregistrovať.

Môžete tiež vymazať všetky údaje zo snímača odtlačkov prstov.

⚠ **VAROVANIE!** Všetky údaje o odtlačkoch prstov pre všetkých používateľov vrátane správcov budú vymazané. Ak prihlasovacia politika vyžaduje iba odtlačky prstov, všetkým používateľom môže byť zabránené v prihlásení sa do počítača.

Sensitivity (Citlivosť)

Posunutím jazdca môžete upraviť citlivosť používanú snímačom odtlačkov prstov pri skenovaní odtlačkov prstov.

Ak sa odtlačok prsta nerozpoznáva konzistentne, môže byť potrebné nastaviť nižšiu citlivosť. Vyššie nastavenie zvyšuje citlivosť na variácie snímania odtlačkov prstov, a preto znižuje možnosť falošných prijatí. Stredne vysoké nastavenie poskytuje dobré vyváženie zabezpečenia a pohodlia.

Advanced (Rozšírené)

Môžete konfigurovať snímač odtlačkov prstov na šetrenie energie, keď je počítač napájaný z batérie.

Karta Smart Card

Počítač môžete konfigurovať tak, aby sa automaticky uzamkol pri odstránení karty Smart Card. Avšak počítač sa uzamkne iba v prípade, ak sa ako overovacie poverenie pri prihlasovaní do systému Windows používala karta Smart Card. Odstránenie karty Smart Card, ktorá sa nepoužívala na prihlásenie do systému Windows, nespôsobí uzamknutie počítača.

▲ Začiarknutím tohto políčka môžete povoliť alebo zakázať uzamykanie počítača pri odstránení karty Smart Card.

4 Konfigurácia aplikácií

Skupina Applications (Aplikácie) je dostupná z panela ponuky Security Applications (Bezpečnostné aplikácie) na ľavej strane spravovacej konzoly nástroja HP ProtectTools. Nastavenia môžete použiť na prispôsobenie správania aktuálne nainštalovaných aplikácií nástroja HP ProtectTools Security Manager.

Úprava nastavení aplikácie:

1. V ponuke Tools (Nástroje) v skupine **Applications** (Aplikácie) kliknite na položku **Settings** (Nastavenia).
2. Kliknutím môžete povoliť alebo zakázať špecifické nastavenie.
3. Kliknutím na tlačidlo **Apply** (Použiť) uložíte vykonané zmeny.

Karta General (Všeobecné)

Na karte General (Všeobecné) sú k dispozícii nasledujúce nastavenia:

- **Do not automatically launch the Setup Wizard for administrators** (Nespúšťať automaticky sprievodcu inštaláciou pre správcov) – výberom tejto možnosti môžete zabrániť automatickému otváraniu sprievodcu po prihlásení.
- **Do not automatically launch the Getting Started wizard for users** (Nespúšťať automaticky úvodného sprievodcu pre používateľov) – výberom tejto možnosti môžete zabrániť automatickému otváraniu používateľských nastavení po prihlásení.

Karta Applications (Aplikácie)

Nastavenia zobrazené v tejto časti sa môžu zmeniť pri pridaní nových aplikácií do nástroja Security Manager. Minimálne nastavenia zobrazené v predvolenom nastavení sú nasledovné:

- **Security Manager** – povoľuje aplikáciu Security Manager pre všetkých používateľov počítača.
- **Enable the Discover more button** (Povoliť tlačidlo Zistiť ďalšie) – umožňuje všetkým používateľom tohto počítača pridať aplikácie do nástroja HP ProtectTools Security Manager kliknutím na tlačidlo **[+] Discover more** ([+] Zistiť ďalšie).

Ak chcete obnoviť predvolené nastavenia od výrobcu pre všetky aplikácie, kliknite na tlačidlo **Restore Defaults** (Obnoviť predvolené nastavenia).

5 Pridávanie spravovacích nástrojov

Na pridávanie nových spravovacích nástrojov do nástroja Security Manager môžu byť k dispozícii ďalšie aplikácie. Správca tohto počítača môže zakázať túto funkciu prostredníctvom aplikácie Settings (Nastavenia).

Ak chcete pridať ďalšie spravovacie nástroje, kliknite na položku **[+] Management tools** ([+] Spravovacie nástroje).

Na kontrolu nových aplikácií môžete použiť webovú lokalitu DigitalPersona alebo môžete nastaviť plán automatických aktualizácií.

6 HP ProtectTools Security Manager

Nástroj HP ProtectTools Security Manager umožňuje významne zlepšiť zabezpečenie počítača.

Môžete použiť vopred načítané aplikácie nástroja Security Manager, ako aj ďalšie aplikácie dostupné na okamžité prevzatie z webu:

- Spravovanie prihlasovania a hesiel
- Jednoduchá zmena hesla pre operačný systém Windows®
- Nastavenie predvolieb programu
- Používanie odtlačkov prstov na zvýšenie zabezpečenia a pohodlia
- Nastavenie overovania pomocou karty Smart Card
- Zálohovanie a obnovenie údajov programu
- Pridanie ďalších aplikácií

Inštalačné postupy

Úvodné informácie

Sprievodca inštaláciou nástroja HP ProtectTools sa zobrazí automaticky ako predvolená stránka v nástroji HP ProtectTools Security Manager, až kým nebude dokončená inštalácia.

Pri inštalácii nástroja Security Manager postupujte podľa nasledujúcich krokov:

POZNÁMKA: Ak nie je k dispozícii snímač odtlačkov prstov ani karta Smart Card, vykonajte iba kroky 1, 5 a 6.

1. Na úvodnej stránke kliknite na tlačidlo **Next** (Ďalej).
2. Na nasledujúcej stránke sa zobrazí zoznam metód overovania, ktoré sú k dispozícii v tomto počítači. Pokračujte kliknutím na tlačidlo **Next** (Ďalej).
3. Na stránke Verify Your Identity (Overenie identity) zadajte heslo systému Windows a potom kliknite na tlačidlo **Next** (Ďalej).
4. Pozrite si aspoň jednu z nasledujúcich tém v závislosti od konfigurácie počítača.
   - Ak je k dispozícii snímač odtlačkov prstov, pozrite si časť Registrácia odtlačkov prstov na strane 24.
   - Ak je k dispozícii karta Smart Card, pozrite si časť Nastavenie karty Smart Card na strane 25.
5. Ak nie je k dispozícii snímač odtlačkov prstov ani karta Smart Card, zobrazí sa výzva na zadanie hesla systému Windows. Toto heslo musíte používať v budúcnosti pri každom vyžadovaní overovania.
6. Na poslednej stránke sprievodcu kliknite na tlačidlo **Finish** (Dokončiť).

   Zobrazí sa tabuľa nástroja Security Manager.

Registrácia poverení

Na registráciu rôznych metód overovania alebo poverení môžete použiť stránku My Identity (Moja identita). Po zaregistrovaní metód ich môžete použiť na prihlasovanie do programu Security Manager.

Registrácia odtlačkov prstov

Ak má počítač zabudovaný alebo pripojený snímač odtlačkov prstov, procesom nastavenia alebo registrácie odtlačkov prstov vás bude sprevádzať Sprievodca inštaláciou nástroja HP ProtectTools.

1. Prečítajte si úvodnú obrazovku a potom kliknite na tlačidlo **Next** (Ďalej).
2. Overte vašu identitu, buď zadaním hesla systému Windows, ak ešte nemáte zaregistrované žiadne odtlačky prstov, alebo naskenovaním odtlačku prsta pomocou snímača odtlačkov prstov. Kliknite na tlačidlo **Next** (Ďalej).

   Ak je heslo systému Windows prázdne, budete požiadaní o jeho vytvorenie. Heslo systému Windows sa vyžaduje na ochranu konta systému Windows pred prístupom neoprávnených osôb a na používanie funkcií nástroja HP ProtectTools Security Manager.
3. Zobrazí sa obrys dvoch rúk. Prsty, ktoré sú už zaregistrované, sú zvýraznené zelenou farbou. Kliknite na prst na obryse.

POZNÁMKA: Ak chcete odstrániť predtým zaregistrovaný odtlačok prsta, kliknite na príslušný odtlačok prsta.

4. Po vybratí prsta na registráciu sa zobrazí výzva na nasnímanie daného odtlačku prsta, až kým nebude úspešne zaregistrovaný. Zaregistrovaný prst sa zvýrazní na obryse zelenou farbou.
5. Musíte zaregistrovať aspoň dva prsty; odporúča sa použiť ukazovák alebo prostredník. Zopakujte kroky 3 a 4 pre ďalší prst.
6. Kliknite na tlačidlo **Next** (Ďalej).

POZNÁMKA: Pri registrácii odtlačkov prstov prostredníctvom úvodného procesu sa informácie o odtlačkoch prstov neuložia, kým nekliknite na tlačidlo **Next** (Ďalej). Ak necháte počítač chvíľu nečinný alebo zatvoríte tabuľu, vykonané zmeny sa **neuložia**.

Zmena hesla systému Windows

Security Manager umožňuje jednoduchšiu a rýchlejšiu zmenu hesla systému Windows než prostredníctvom Ovládacieho panela systému Windows.

Ak chcete zmeniť heslo systému Windows, postupujte podľa nasledujúcich krokov:

1. Na tabuli nástroja Security Manager kliknite na položku **My Identity** (Moja identita), kliknite na položku **Credentials** (Poverenia) a potom kliknite na položku **Password** (Heslo).
2. Zadajte aktuálne heslo do textového poľa **Current Windows password** (Aktuálne heslo systému Windows).
3. Zadajte nové heslo do textového poľa **New Windows password** (Nové heslo systému Windows) a potom ho zadajte znova do textového poľa **Confirm new password** (Potvrdiť nové heslo).
4. Kliknutím na položku **Change** (Zmeniť) môžete ihneď zmeniť aktuálne heslo na nové, ktoré ste zadali.

Nastavenie karty Smart Card

Ak má počítač zabudovanú alebo pripojenú čítačku kariet Smart Card, nástroj Security Manager zobrazí výzvu na nastavenie kódu PIN (osobné identifikačné číslo) karty Smart Card.

- Nastavenie kódu PIN karty Smart Card – na stránke Set up smart card (Nastavenie karty Smart Card) zadajte a potvrďte kód PIN.
- Zmena kódu PIN – najprv zadajte starý kód PIN a potom zvoľte nový.

Používanie tabule nástroja Security Manager

Tabuľa nástroja Security Manager je centrálne umiestnenie na jednoduchý prístup k funkciám, aplikáciám a nastaveniam nástroja Security Manager.

Tabuľa obsahuje nasledujúce súčasti:

- **ID Card** (Identifikačná karta) – slúži na zobrazenie mena používateľa systému Windows a vybratého obrázka identifikujúceho konto prihláseného používateľa.
- **Security Applications** (Bezpečnostné aplikácie) – slúži na zobrazenie rozbaľovacej ponuky prepojení na konfiguráciu nasledujúcich kategórií zabezpečenia:
  - **My Identity (Moja Identita)**
  - **My Data (Moje údaje)**
  - **My Computer (Tento počítač)**
- **Discover more** (Zistiť ďalšie) – slúži na otvorenie stránky, na ktorej môžete nájsť ďalšie aplikácie na zlepšenie zabezpečenia vašej identity, údajov a komunikácie.
- **Main area** (Hlavná oblasť) – slúži na zobrazenie obrazoviek špecifických pre danú aplikáciu.
- **Administration** (Spravovanie) – slúži na otvorenie Spravovacej konzoly nástroja HP ProtectTools.
- **Help button** (Tlačidlo Pomocníka) – slúži na zobrazenie informácií o aktuálnej obrazovke.
- **Advanced** (Rozšírené) – umožňuje prístup k nasledujúcim možnostiam:
  - **Preferences** (Predvoľby) – umožňuje prispôsobiť nastavenia nástroja Security Manager.
  - **Backup and Restore** (Zálohovanie a obnovenie) – umožňuje zálohovať alebo obnoviť údaje.
  - **About** (Informácie) – slúži na zobrazenie informácií o verzii nástroja Security Manager.

Ak chcete otvoriť tabuľu nástroja Security Manager, kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Security Manager**.

Otvorenie nástroja HP ProtectTools Security Manager

Nástroj HP ProtectTools Security Manager môžete otvoriť ľubovoľným z nasledujúcich spôsobov:

- Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Security Manager** (Správca zabezpečenia nástroja HP ProtectTools).
- Dvakrát kliknite na ikonu nástroja **HP ProtectTools** v oblasti oznámení úplne vpravo na paneli úloh.
- Kliknite pravým tlačidlom myši na ikonu nástroja **HP ProtectTools** a kliknite na položku **Open HP ProtectTools Security Manager** (Otvoriť nástroj HP ProtectTools Security Manager).
- Kliknite na miniaplikáciu **Security Manager ID Card** (Identifikačná karta nástroja Security Manager) na bočnom paneli systému Windows.
- Stlačením klávesovej skratky ctrl+alt+h môžete otvoriť ponuku rýchlych prepojení nástroja Security Manager.

Všeobecné úlohy

Aplikácie zahrnuté v tejto skupine pomáhajú pri spravovaní rozličných aspektov vašej digitálnej identity.

- **Security Manager** – vytvára a spravuje rýchle prepojenia, ktoré umožňujú spustiť a prihlásiť sa na webové lokality a do programov prostredníctvom overenia heslom systému Windows, odtlačku prsta alebo karty Smart Card.
- **Credentials** (Poverenia) – umožňuje jednoducho zmeniť heslo systému Windows, zaregistrovať odtlačky prstov alebo nastaviť kartu Smart Card.

Ak chcete pridať ďalšie aplikácie, kliknite na tlačidlo [+] **Discover more** (Zistiť ďalšie) v ľavom dolnom rohu tabule. Toto tlačidlo môže zakázať správca.

Password Manager

Prihlasovanie do systému Windows, aplikácií a na webové lokality je jednoduchšie a bezpečnejšie pri používaní nástroja Password Manager. Môžete ho použiť na vytváranie silnejších hesiel, ktoré si nemusíte poznačiť ani zapamätať, a potom sa jednoducho a rýchlo prihlásiť pomocou odtlačku prsta, karty Smart Card alebo hesla systému Windows.

Nástroj Password Manager ponúka nasledujúce možnosti:

- Pridávanie, úprava alebo odstraňovanie prihlasovaní z karty Manage (Spravovanie).
- Pomocou rýchlych prepojení môžete spustiť predvolený prehľadávač a prihlásiť sa na ľubovoľnú webovú lokalitu alebo do ľubovoľného programu po nastavení tejto funkcie.
- Uchopením a presunutím myšou môžete organizovať rýchle prepojenia do kategórií.
- Môžete prehľadne zobraziť, či ľubovoľné z vašich hesiel predstavujú bezpečnostné riziko, a automaticky generovať zložité silné heslo na použitie pre nové lokality.

Mnoho funkcií nástroja Password Manager je tiež k dispozícii z ikony nástroja Password Manager, ktorá sa zobrazí pri aktivácii prihlasovacej obrazovky webovej stránky alebo programu. Kliknutím na ikonu môžete zobraziť kontextovú ponuku, v ktorej môžete vybrať z nasledujúcich možností.

Pre webové stránky alebo programy, pre ktoré ešte nebolo vytvorené prihlasovacie konto

V kontextovej ponuke sú zobrazené nasledujúce možnosti:

- **Add [somedomain.com] to the Password Manager** (Pridať [nejakádoména.com] do nástroja Password Manager) – umožňuje pridať prihlasovacie konto pre aktuálnu prihlasovaciu obrazovku.
- **Open Password Manager** (Otvoriť nástroj Password Manager) – slúži na spustenie nástroja Password Manager.
- **Icon settings** (Nastavenia ikony) – umožňuje definovať podmienky, pri ktorých sa zobrazí ikona nástroja Password Manager.
- **Help** (Pomocník) – slúži na zobrazenie pomocníka softvéru Password Manager.

Pre webové stránky alebo programy, pre ktoré už bolo vytvorené prihlasovacie konto

V kontextovej ponuke sú zobrazené nasledujúce možnosti:

- **Fill in logon data** (Vyplniť prihlasovacie údaje) – umiestni prihlasovacie údaje do prihlasovacích polí a potom odošle stránku (ak bolo odoslanie zadané pri vytvorení alebo poslednej úprave prihlasovacieho konta).
- **Edit logon** (Upraviť prihlasovacie konto) – umožňuje upraviť prihlasovacie údaje pre túto webovú lokalitu.
- **Add a New Account** (Pridať nové konto) – umožňuje pridať konto do prihlasovacích poverení.
- **Open Password Manager** (Otvoriť nástroj Password Manager) – slúži na spustenie aplikácie Password Manager.
- **Help** (Pomocník) – slúži na zobrazenie pomocníka softvéru Password Manager.

POZNÁMKA: Správca tohto počítača môže nastaviť nástroj Security Manager tak, aby vyžadoval viac než jedno poverenie pri overovaní vašej identity.

Pridávanie prihlasovacích poverení

Prihlasovacie poverenie pre webovú lokalitu alebo program môžete jednoducho pridať jedným zadaním prihlasovacích údajov. Od tohto okamihu bude nástroj Password Manager automaticky zadávať tieto údaje za vás. Tieto prihlasovacie poverenia môžete použiť po prejdení na webovú lokalitu alebo do programu alebo kliknutí na prihlásenie v ponuke **Logons** (Prihlasovacie poverenia), čím nástroj Password Manager otvorí webovú lokalitu alebo program a prihlási vás.

Pridanie prihlasovacieho poverenia:

1. Otvorte prihlasovaciu obrazovku webovej lokality alebo programu.
2. Kliknite na šípku na ikone nástroja **Password Manager** a potom kliknite na jednu z nasledujúcich možností, v závislosti od toho, či je prihlasovacia obrazovka určená pre webovú lokalitu alebo program:
   - Pre webovú lokalitu kliknite na položku **Add [domain name] to Password Manager** (Pridať [názov domény] do nástroja Password Manager).
   - Pre program kliknite na položku **Add this logon screen to Password Manager** (Pridať túto prihlasovaciu obrazovku do nástroja Password Manager).
3. Zadajte prihlasovacie údaje. Prihlasovacie polia na obrazovke a ich príslušné polia v dialógovom okne sú identifikované tučným oranžovým orámovaním. Toto dialógové okno môžete tiež zobraziť kliknutím na položku **Add Logon** (Pridať prihlasovacie poverenie) z karty **Password Manager Manage** (Spravovanie nástroja Password Manager). Niektoré možnosti závisia od bezpečnostných zariadení pripojených k počítaču; napríklad od použitia klávesovej skratky ctrl+alt +H, nasnímania odtlačku prsta alebo vloženia karty Smart Card.
   - Ak chcete vyplniť prihlasovacie pole jednou z vopred formátovaných volieb, kliknite na šípky vpravo od poľa.
   - Ak chcete pridať ďalšie polia z obrazovky do prihlasovacieho poverenia, kliknite na položku **Choose other fields** (Vybrať ďalšie polia).

- Ak chcete vyplniť prihlasovacie polia, ale neodoslať ich, zrušte začiarknutie políčka **Submit logon data** (Odoslať prihlasovacie údaje).
- Ak chcete zobraziť heslo pre tieto prihlasovacie údaje, kliknite na položku **Show password** (Zobraziť heslo).

4. Kliknite na tlačidlo **OK**.

   Z ikony nástroja Password Manager sa odstráni znak plus, čo signalizuje, že bolo vytvorené prihlasovacie poverenie.

Pri každom prístupe na danú webovú lokalitu alebo pri každom otvorení daného programu sa zobrazí ikona nástroja Password Manager, ktorá signalizuje, že môžete použiť vaše zaregistrované poverenia na prihlásenie.

Úprava prihlasovacích poverení

Ak chcete upraviť prihlasovacie poverenie, postupujte podľa nasledujúcich krokov:

1. Otvorte prihlasovaciu obrazovku webovej lokality alebo programu.
2. Ak chcete zobraziť dialógové okno, v ktorom môžete upraviť prihlasovacie poverenia, kliknite na šípku na ikone nástroja **Password Manager** a potom kliknite na položku **Edit logon** (Upraviť prihlasovacie poverenia). Prihlasovacie polia na obrazovke a ich príslušné polia v dialógovom okne sú identifikované tučným oranžovým orámovaním.

   Toto dialógové okne môžete tiež zobraziť kliknutím na položku **Edit for the desired logon** (Upraviť pre požadované prihlasovacie poverenia) z karty **Password Manager Manage** (Spravovanie nástroja Password Manager).
3. Upravte prihlasovacie poverenia.
   - Ak chcete vyplniť prihlasovacie pole jednou z vopred formátovaných volieb, kliknite na šípky vpravo od poľa.
   - Ak chcete pridať ďalšie polia z obrazovky do prihlasovacieho poverenia, kliknite na položku **Choose other fields** (Vybrať ďalšie polia).
   - Ak chcete vyplniť prihlasovacie polia, ale neodoslať ich, zrušte začiarknutie políčka **Submit logon data** (Odoslať prihlasovacie údaje).
   - Ak chcete zobraziť heslo pre tieto prihlasovacie údaje, kliknite na položku **Show password** (Zobraziť heslo).
4. Kliknite na tlačidlo **OK**.

Používanie ponuky prihlasovacích poverení

Nástroj Password Manager poskytuje rýchly, jednoduchý spôsob spúšťania webových lokalít a programov, pre ktoré máte vytvorené prihlasovacie poverenia. Dvakrát kliknite na prihlasovacie poverenie programu alebo webovej lokality v ponuke **Logons** (Prihlasovacie poverenia) alebo na karte **Manage** (Spravovať) v nástroji **Password Manager**, čím otvoríte prihlasovaciu obrazovku, na ktorej môžete vyplniť vaše prihlasovacie poverenia.

Keď vytvoríte prihlasovacie poverenie, automaticky sa pridá do ponuky prihlasovacích poverení nástroja Password Manager.

Zobrazenie ponuky prihlasovacích poverení:

1. Stlačte klávesovú skratku nástroja **Password Manager**. Od výrobcu je nastavená skratka ctrl+alt +h. Ak chcete zmeniť klávesovú skratku, kliknite na položku **Password Manager** a potom kliknite na položku **Settings** (Nastavenia).
2. Nasnímajte svoj odtlačok prsta (na počítačoch so zabudovaným alebo pripojeným snímačom odtlačkov prstov).

Usporiadanie prihlasovacích poverení do kategórií

Prihlasovacie poverenia môžete usporiadať do jednej alebo viacerých kategórií, ktoré vytvoríte. Potom uchopte a presuňte myšou prihlasovacie poverenia do požadovaných kategórií.

Pridanie kategórie:

1. Na tabuli nástroja Security Manager kliknite na položku **Password Manager**.
2. Kliknite na kartu **Manage** (Spravovať) a potom kliknite na položku **Add Category** (Pridať kategóriu).
3. Zadajte názov kategórie.
4. Kliknite na tlačidlo **OK**.

Pridanie prihlasovacieho poverenia do kategórie:

1. Nastavte ukazovateľ myši nad požadované prihlasovacie poverenie.
2. Stlačte a podržte ľavé tlačidlo myši.
3. Presuňte myšou prihlasovacie poverenie do zoznamu kategórií. Kategórie sa budú zvýrazňovať počas presúvania ukazovateľa myši cez ne.
4. Uvoľnite tlačidlo myši po zvýraznení požadovanej kategórie.

Prihlasovacie poverenia sa nepresunú do vybratej kategórie, ale sa do nej iba skopírujú. Rovnaké prihlasovacie poverenie môžete pridať do viacerých kategórií a všetky prihlasovacie poverenia môžete zobraziť kliknutím na položku **All** (Všetky).

Spravovanie prihlasovacích poverení

Nástroj Password Manager umožňuje jednoducho spravovať mená používateľov, heslá a viaceré prihlasovacie kontá prihlasovacích poverení z jedného centrálneho umiestnenia.

Prihlasovacie poverenia sú uvedené na karte Manage (Spravovanie). Ak boli vytvorené viaceré prihlasovacie poverenia pre rovnakú webovú lokalitu, každé prihlasovacie poverenie je potom uvedené pod názvom danej webovej lokality a odsadené v zozname prihlasovacích poverení.

Spravovanie prihlasovacích poverení:

Na tabuli nástroja Security Manager kliknite na položku **Password Manager** a potom kliknite na kartu **Manage** (Spravovanie).

- **Pridanie prihlasovacieho poverenia** – kliknite na položku **Add Logon** (Pridať prihlasovacie poverenie) a postupujte podľa pokynov na obrazovke.
- **Úprava prihlasovacieho poverenia** – kliknite na prihlasovacie poverenie, kliknite na položku **Edit** (Upraviť) a potom zmeňte prihlasovacie údaje.
- **Odstránenie prihlasovacieho poverenia** – kliknite na prihlasovacie poverenie a potom kliknite na položku **Delete** (Odstrániť).

Pridanie ďalšieho prihlasovacieho poverenia pre webovú lokalitu alebo program:

1. Otvorte prihlasovaciu obrazovku webovej lokality alebo programu.
2. Kliknutím na ikonu nástroja **Password Manager** zobrazte jeho ponuku odkazov.
3. Kliknite na položku **Add additional logon** (Pridať ďalšie prihlasovacie poverenie) a potom postupujte podľa pokynov na obrazovke.

Vyhodnotenie sily hesla

Používanie silných hesiel na prihlasovanie na webové lokality a do programov je dôležitým aspektom ochrany vašej identity.

Nástroj Password Manager umožňuje jednoduché monitorovanie a zlepšenia zabezpečenia prostredníctvom okamžitej a automatizovanej analýzy sily každého z hesiel používaných na prihlásenie na webové lokality a do programov.

Nastavenia ikony nástroja Password Manager

Nástroj Password Manager sa pokúša identifikovať prihlasovacie obrazovky pre webové lokality a programy. Keď zistí prihlasovaciu obrazovku, pre ktorú nemáte vytvorené prihlasovacie poverenie, nástroj Password Manager zobrazí výzvu na pridanie prihlasovacieho poverenia pre danú obrazovku zobrazením ikony nástroja Password Manager so znakom „+“.

Kliknite na šípku na ikone a potom kliknutím na položku **Icon Settings** (Nastavenia ikony) prispôsobte, ako bude nástroj **Password Manager** spracovávať možné prihlasovacie lokality.

- **Prompt to add logons for logon screens** (Výzva na pridanie prihlasovacích poverení pre prihlasovacie obrazovky) – kliknutím na túto možnosť nastavíte, aby nástroj Password Manager zobrazil výzvu na pridanie prihlasovacieho poverenia pri zobrazení prihlasovacej obrazovky, ktorá ešte nemá nastavené prihlasovacie poverenie.
- **Exclude this screen** (Vylúčiť túto obrazovku) – ak začiarknete toto políčko, nástroj Password Manager nebude viac zobrazovať výzvu na pridanie prihlasovacieho poverenia pre túto prihlasovaciu obrazovku.

Ak chcete otvoriť ďalšie nastavenia nástroja Password Manager, kliknite na položku **Password Manager** a potom kliknite na položku **Settings** (Nastavenia) na tabuli nástroja Security Manager.

Nastavenia

Môžete zadať nastavenia na prispôsobenie nástroja HP ProtectTools Security Manager:

1. **Prompt to add logons for logon screens** (Výzva na pridanie prihlasovacích poverení pre prihlasovacie obrazovky) – ikona nástroja Password Manager so znakom plus sa zobrazí pri každom zistení prihlasovacej obrazovky webovej lokality alebo programu, čo signalizuje, že môžete pridať prihlasovacie poverenie pre túto obrazovku do trezora hesiel. Ak chcete zakázať túto funkciu, v dialógovom okne **Icon Settings** (Nastavenia ikony) zrušte začiarknutie políčka vedľa položky **Prompt to add logons for logon screens** (Výzva na pridanie prihlasovacích poverení pre prihlasovacie obrazovky).

2. **Open Password Manager with ctrl+alt+H** (Otvorenie nástroja Password Manager pomocou klávesovej skratky ctrl+alt+H) – predvolená klávesová skratka, ktorá slúži na otvorenie ponuky rýchlych prepojení nástroja Password Manager, je ctrl+alt+H. Ak chcete zmeniť túto klávesovú skratku, kliknite na túto možnosť a zadajte novú kombináciu klávesov. Kombinácie môžu zahŕňať jeden alebo viacero z nasledujúcich klávesov: ctrl, alt alebo shift a ľubovoľný abecedný alebo numerický kláves.

3. Kliknutím na tlačidlo **Apply** (Použiť) uložte vykonané zmeny.

Poverenia

Poverenia nástroja Security Manager môžete použiť na overenie vašej identity. Lokálny správca tohto počítača môže nastaviť, ktoré poverenia sa môžu používať na overenie vašej identity pri prihlasovaní do konta systému Windows, na webové lokality alebo do programov.

Dostupné poverenia sa môžu líšiť v závislosti od bezpečnostných zariadení zabudovaných alebo pripojených k tomuto počítaču. Každé podporované poverenie bude mať príslušnú položku v skupine **My Identity, Credentials** (Moja identita, poverenia).

Sú tu uvedené dostupné poverenia, požiadavky a aktuálny stav a môžu zahŕňať nasledujúce:

- Odtlačky prstov
- Heslo
- Karta Smart Card

Ak chcete zaregistrovať alebo zmeniť poverenie, kliknite na prepojenie a postupujte podľa pokynov na obrazovke.

Vaša osobná identifikačná karta

Vaša identifikačná karta vás jedinečne identifikuje ako vlastníka tohto konta systému Windows, pričom zobrazuje vaše meno a obrázok podľa vašej voľby. Je výrazne zobrazená v ľavom hornom rohu stránok nástroja Security Manager a ako miniaplikácia bočného panela systému Windows.

Kliknutie na identifikačnú kartu na bočnom paneli systému Windows je jeden z mnohých spôsobov, ako získať rýchly prístup k nástroju Security Manager.

Môžete zmeniť obrázok a spôsob zobrazenia vášho mena. V predvolenom nastavení sa zobrazuje celé meno používateľa systému Windows a obrázok, ktorý ste vybrali počas inštalácie systému Windows.

Zmena zobrazeného mena:

1. Na tabuli nástroja Security Manager kliknite na položku **ID Card** (Identifikačná karta) v ľavom hornom rohu.
2. Kliknite na pole zobrazujúce meno, ktoré ste zadali pre vaše konto v systéme Windows. Systém zobrazí meno používateľa systému Windows pre toto konto.
3. Ak chcete zmeniť toto meno, zadajte nové meno a potom kliknite na tlačidlo **Save** (Uložiť).

Zmena zobrazeného obrázka:

1. Na tabuli nástroja Security Manager kliknite na položku **My Identity** (Moja identita) a potom kliknite na položku **ID Card** (Identifikačná karta) v ľavom hornom rohu.
2. Kliknite na tlačidlo **Choose picture** (Vybrať obrázok), kliknite na obrázok a potom kliknite na tlačidlo **Save** (Uložiť).

Nastavenie predvolieb

Môžete prispôsobiť nastavenia nástroja HP ProtectTools Security Manager. Na tabuli nástroja Security Manager kliknite na položku **Advanced** (Rozšírené) a potom kliknite na položku **Preferences** (Predvoľby). Dostupné nastavenia sa zobrazia na dvoch kartách: General (Všeobecné) a Fingerprint (Odtlačok prsta).

General (Všeobecné)

Na karte General (Všeobecné) sú k dispozícii nasledujúce nastavenia:

Appearance (Vzhľad) – **Show icon on taskbar** (Zobraziť ikonu na paneli úloh)

Ak chcete povoliť zobrazenie ikony na paneli úloh, začiarknite toto políčko.

Ak chcete zakázať zobrazenie ikony na paneli úloh, zrušte začiarknutie tohto políčka.

Fingerprint (Odtlačok prsta)

Na karte Fingerprint (Odtlačok prsta) sú k dispozícii nasledujúce nastavenia:

Quick Actions (Rýchle akcie) – pomocou položky Quick Actions (Rýchle akcie) vyberte úlohu nástroja Security Manager, ktorá sa má vykonať pri stlačení a podržaní nastaveného klávesu počas snímania odtlačku prsta.

Priradenie rýchlej akcie jednému z uvedených klávesov:

- Kliknite na **(kláves)+odtlačok prsta** a potom kliknite na jednu z dostupných úloh v ponuke.

Fingerprint Scan Feedback (Spätná väzba pri snímaní odtlačkov prstov) – zobrazí sa iba v prípade, keď je k dispozícii snímač odtlačkov prstov. Pomocou tohto nastavenia môžete upraviť spätnú väzbu pri snímaní odtlačku prsta.

- **Enable sound feedback** (Povoliť zvukovú spätnú väzbu) – nástroj Security Manager poskytuje zvukovú spätnú väzbu po nasnímaní odtlačku prsta, pričom prehráva rôzne zvuky pre konkrétne programové udalosti. Nové zvuky pre tieto udalosti môžete priradiť prostredníctvom karty Sounds (Zvuky) v Ovládacom paneli systému Windows, prípadne môžete zakázať zvukovú spätnú väzbu vymazaním tejto možnosti.
- **Show scan quality feedback** (Zobraziť spätnú väzbu kvality snímania) – v predvolenom nastavení nástroj Security Manager zobrazuje obrázok odtlačku prsta s otáznikom vždy, keď je kvalita snímania odtlačku prsta nedostatočná na overenie vašej identity. Zobrazenie tohto obrázka môžete zakázať zrušením tejto možnosti.

Zálohovanie a obnovenie údajov

Odporúča sa pravidelne zálohovať údaje nástroja Security Manager. Ako často treba zálohovať závisí od toho, ako často sa menia údaje. Ak napríklad každý deň pridávate nové prihlasovacie poverenia, mali by ste zrejme zálohovať údaje každý deň.

Zálohy môžete použiť aj na migráciu z jedného počítača na druhý, čo sa nazýva aj importovanie a exportovanie.

POZNÁMKA: Táto funkcia zálohuje iba údaje.

Ak chcete obnoviť údaje zo záložného súboru, nástroj HP ProtectTools Security Manager musí byť nainštalovaný na každom počítači, ktorý bude prijímať zálohované údaje.

Zálohovanie údajov:

1. Na ľavom paneli kliknite na položku **Advanced** (Rozšírené) a potom kliknite na položku **Backup and Restore** (Zálohovanie a obnovenie).
2. Kliknite na položku **Back up data** (Zálohovať údaje).
3. Vyberte moduly, ktoré chcete zahrnúť v zálohe. Vo väčšine prípadov ich budete chcieť vybrať všetky.
4. Zadajte názov súboru ukladacieho priestoru. V predvolenom nastavení sa súbor uloží do priečinka Documents (Dokumenty). Kliknite na tlačidlo **Browse** (Prehľadávať) a zadajte iné umiestnenie.
5. Zadajte heslo na ochranu súboru.
6. Overte vašu identitu.
7. Kliknite na tlačidlo **Finish** (Dokončiť).

Obnovenie údajov:

1. Na ľavom paneli kliknite na položku **Advanced** (Rozšírené) a potom kliknite na položku **Backup and Restore** (Zálohovanie a obnovenie).
2. Kliknite na položku **Restore data** (Obnoviť údaje).
3. Vyberte predtým vytvorený súbor ukladacieho priestoru. Môžete zadať cestu do zobrazeného poľa alebo kliknúť na položku **Edit** (Upraviť).
4. Zadajte heslo používané na ochranu súboru.

5. Vyberte moduly, ktorých údaje chcete obnoviť. Vo väčšine prípadov to budú všetky uvedené moduly.

6. Kliknite na tlačidlo **Finish** (Dokončiť).

Pridávanie aplikácií

Môžu byť k dispozícii ďalšie aplikácie, ktoré poskytujú nové funkcie pre tento program.

Na tabuli nástroja Security Manager kliknite na položku **[+] Discover more** ([+] Zistiť ďalšie) a vyhľadajte ďalšie aplikácie.

POZNÁMKA: Ak nie je uvedené žiadne prepojenie **[+] Discover more** ([+] Zistiť ďalšie) v ľavej dolnej časti tabule, bolo zakázané správcom tohto počítača.

Stav bezpečnostnej aplikácie

Stránka Security Manager Applications Status (Stav aplikácií nástroja Security Manager) slúži na zobrazenie celkového stavu nainštalovaných bezpečnostných aplikácií. Zobrazuje nainštalované aplikácie a stav inštalácie každej z nich. Súhrn sa zobrazí automaticky po otvorení tabule nástroja Security Manager alebo po kliknutí na položku **Security Applications** (Bezpečnostné aplikácie).

7 Aplikácia Drive Encryption pre nástroj HP ProtectTools (len vybrané modely)

△ **UPOZORNENIE:** Ak sa rozhodnete odinštalovať modul Drive Encryption, musíte najprv dešifrovať všetky zašifrované jednotky. Ak to neurobíte, nebudete môcť získať prístup k údajom na zašifrovaných jednotkách, pokiaľ ste sa nezaregistrovali v službe obnovy šifrovania jednotky. Preinštalovanie modulu Drive Encryption neumožní prístup k zašifrovanej jednotke.

Aplikácia Drive Encryption pre nástroj HP ProtectTools poskytuje kompletnú ochranu údajov šifrovaním pevného disku počítača. Keď je aktivovaná aplikácia Drive Encryption, musíte sa prihlásiť na prihlasovacej obrazovke aplikácie Drive Encryption, ktorá sa zobrazí pred spustením operačného systému Windows®.

Sprievodca inštaláciou nástroja HP ProtectTools umožňuje správcom systému Windows aktivovať aplikáciu Drive Encryption, zálohovať šifrovací kľúč, pridať a odstrániť používateľov a deaktivovať aplikáciu Drive Encryption. Ďalšie informácie nájdete v pomocníkovi softvéru HP ProtectTools Security Manager.

Aplikácia Drive Encryption umožňuje vykonávať nasledujúce úlohy:

- Správa šifrovania
  - Šifrovanie alebo dešifrovanie jednotlivých jednotiek

    POZNÁMKA: Šifrovať môžete iba interné pevné disky.
- Obnovenie
  - Vytvorenie záložných kľúčov
  - Vykonanie obnovenia

Inštalačné postupy

Otvorenie aplikácie Drive Encryption

1. Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools).
2. Na ľavej table kliknite na položku **Drive Encryption** (Šifrovanie jednotky).

Všeobecné úlohy

Aktivácia aplikácie Drive Encryption

Na aktiváciu aplikácie Drive Encryption použite sprievodcu inštaláciou nástroja HP ProtectTools.

POZNÁMKA: Tento sprievodca sa používa aj na pridanie a odstránenie používateľov.

– alebo –

1. Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools).
2. Na ľavej table kliknite na položku **Security** (Zabezpečenie) a potom kliknite na položku **Features** (Funkcie).
3. Začiarknite políčko **Drive Encryption** (Šifrovanie jednotky) a potom kliknite na tlačidlo **Next** (Ďalej).
4. V časti **Drives to be encrypted** (Jednotky na šifrovanie) začiarknite políčko pre pevný disk, ktorý chcete šifrovať.
5. Vložte pamäťové zariadenie do príslušnej zásuvky.

   POZNÁMKA: Ak chcete uložiť šifrovací kľúč, musíte použiť pamäťové zariadenie USB s formátom FAT32.
6. V časti **External storage device on which to save encryption key** (Externé pamäťové zariadenie, na ktoré sa má uložiť šifrovací kľúč) začiarknite políčko pre pamäťové zariadenie, na ktoré sa uloží šifrovací kľúč.
7. Kliknite na tlačidlo **Apply** (Použiť).

   Spustí sa šifrovanie jednotky.

Ďalšie informácie nájdete v pomocníkovi softvéru HP ProtectTools Security Manager.

Deaktivácia aplikácie Drive Encryption

Na deaktiváciu aplikácie Drive Encryption použite sprievodcu inštaláciou nástroja HP ProtectTools. Ďalšie informácie nájdete v pomocníkovi softvéru HP ProtectTools Security Manager.

– alebo –

1. Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools).
2. Na ľavej table kliknite na položku **Security** (Zabezpečenie) a potom kliknite na položku **Features** (Funkcie).
3. Zrušte začiarknutie políčka **Drive Encryption** (Šifrovanie jednotky) a potom kliknite na tlačidlo **Apply** (Použiť).

   Spustí sa dešifrovanie jednotky.

Prihlásenie po aktivácii aplikácie Drive Encryption

Ak zapnete počítač po aktivácii aplikácie Drive Encryption a vaše používateľské konto je zaregistrované, musíte sa prihlásiť na prihlasovacej obrazovke aplikácie Drive Encryption:

POZNÁMKA: Ak správca systému Windows zapol funkciu Pre-boot Security (Zabezpečenie pred zavedením systému) v nástroji HP ProtectTools Security Manager, do počítača sa prihlásite hneď po zapnutí počítača, a nie na prihlasovacej obrazovke aplikácie Drive Encryption.

1. Kliknite na meno používateľa a potom zadajte heslo pre systém Windows alebo kód PIN pre kartu Java™ Card alebo priložte zaregistrovaný prst na snímač.
2. Kliknite na tlačidlo **OK**.

POZNÁMKA: Ak použijete obnovovací kľúč na prihlásenie na prihlasovacej obrazovke aplikácie Drive Encryption, na prihlasovacej obrazovke systému Windows budete musieť zadať aj meno používateľa a heslo systému Windows.

Ochrana údajov šifrovaním pevného disku

Pomocou Sprievodcu inštaláciou nástroja HP ProtectTools môžete chrániť svoje údaje šifrovaním pevného disku:

1. V nástroji Security Manager kliknite na položku **Getting Started** (Úvodné informácie) a potom kliknite na ikonu **Security Manager Setup** (Inštalácia nástroja Security Manager). Spustí sa ukážka, ktorá popisuje funkcie nástroja Security Manager. (Nástroj Security Manager môžete tiež spustiť zo stránky Drive Encryption (Šifrovanie jednotky).)
2. Na ľavej table kliknite na položku **Drive Encryption** (Šifrovanie jednotky) a potom kliknite na položku **Encryption Management** (Spravovanie šifrovania).
3. Kliknite na položku **Change Encryption** (Zmeniť šifrovanie).
4. Vyberte jednotky, ktoré sa majú šifrovať.

   POZNÁMKA: Dôrazne sa odporúča šifrovať pevný disk.

Zobrazenie stavu šifrovania

Používatelia môžu zobraziť stav šifrovania pomocou nástroja HP ProtectTools Security Manager.

POZNÁMKA: Zmeny stavu šifrovania jednotky je nutné vykonať pomocou Spravovacej konzoly nástroja HP ProtectTools.

1. Otvorte nástroj **HP ProtectTools Security Manager**.
2. V časti **My Data** (Moje údaje) kliknite na položku **Encryption Status** (Stav šifrovania).

   Ak je aplikácia Drive Encryption aktívna, stav jednotky sa zobrazí ako jeden z nasledujúcich kódov stavu:

   - Active (Aktívne)
   - Inactive (Neaktívne)
   - Not encrypted (Nešifrované)
   - Encrypted (Šifrované)

- Encrypting (Prebieha šifrovanie)
- Decrypting (Prebieha dešifrovanie)

Ak prebieha šifrovanie alebo dešifrovanie pevného disku, indikátor priebehu zobrazuje percentuálnu hodnotu dokončenia a čas zostávajúci do dokončenia šifrovania alebo dešifrovania.

Rozšírené úlohy

Správa modulu Drive Encryption (úloha pre správcu)

Stránka Encryption Management (Správa šifrovania) umožňuje správcom zobraziť a zmeniť stav aplikácie Drive Encryption (aktívny alebo neaktívny) a zobraziť stav šifrovania všetkých pevných diskov v počítači.

- Ak je stav Inactive (Neaktívne), aplikácia Drive Encryption ešte nebola aktivovaná v nástroji HP ProtectTools Security Manager správcom systému Windows a nechráni pevný disk. Na aktiváciu aplikácie Drive Encryption použite Sprievodcu inštaláciou nástroja HP ProtectTools Security Manager.
- Ak je stav Active (Aktívne), aplikácia Drive Encryption bola aktivovaná a nakonfigurovaná. Jednotka je v jednom z nasledujúcich stavov:
  - Not encrypted (Nešifrované)
  - Encrypted (Šifrované)
  - Encrypting (Prebieha šifrovanie)
  - Decrypting (Prebieha dešifrovanie)

Šifrovanie alebo dešifrovanie jednotlivých jednotiek

Ak chcete šifrovať jeden alebo viacero pevných diskov v počítači alebo dešifrovať jednotku, ktorá už je šifrovaná, použite funkciu Change Encryption (Zmeniť šifrovanie):

1. Otvorte okno **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools), kliknite na položku **Drive Encryption** (Šifrovanie jednotky) a potom kliknite na položku **Encryption Management** (Spravovanie šifrovania).
2. Kliknite na položku **Change Encryption** (Zmeniť šifrovanie).
3. V dialógovom okne Change Encryption (Zmena šifrovania) začiarknite alebo zrušte začiarknutie políčka vedľa každého pevného disku, ktorý chcete šifrovať alebo dešifrovať, a potom kliknite na tlačidlo **OK**.

POZNÁMKA: Pri šifrovaní alebo dešifrovaní jednotky bude indikátor priebehu zobrazovať čas zostávajúci do dokončenia procesu počas aktuálnej relácie. Ak počas procesu šifrovania vypnete počítač alebo ak sa aktivuje režim spánku alebo dlhodobého spánku a potom sa reštartuje počítač, zobrazený zostávajúci čas sa obnoví na pôvodnú hodnotu, ale aktuálne šifrovanie bude pokračovať od bodu, kde bolo naposledy zastavené. Zobrazenie zostávajúceho času a priebehu sa bude meniť rýchlejšie, aby sa zohľadnil predchádzajúci priebeh.

Zálohovanie a obnovenie zálohy (úloha pre správcu)

Stránka Recovery (Obnovenie) umožňuje správcom zálohovať a obnoviť šifrovacie kľúče.

Local Drive Encryption Key Backup (Záloha šifrovacieho kľúča lokálnej jednotky) – umožňuje zálohovať šifrovacie kľúče na vymeniteľné médium, keď je aktivovaná aplikácia Drive Encryption.

Vytvorenie záložných kľúčov

Šifrovací kľúč šifrovanej jednotky môžete zálohovať na vymeniteľné pamäťové zariadenie:

△ **UPOZORNENIE:** Pamäťové zariadenie obsahujúce záložný kľúč uchovávajte na bezpečnom mieste, pretože ak zabudnete heslo alebo stratíte kartu Java Card, jedine toto zariadenie vám poskytne prístup k pevnému disku.

1. Otvorte okno **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools), kliknite na položku **Drive Encryption** (Šifrovanie jednotky) a potom kliknite na položku **Recovery** (Obnovenie).
2. Kliknite na položku **Backup Keys** (Zálohovať kľúče).
3. Na stránke Select Backup Disk (Výber zálohovacieho disku) začiarknite políčko pre názov zariadenia, na ktoré chcete zálohovať svoj šifrovací kľúč, a potom kliknite na tlačidlo **Next** (Ďalej).
4. Prečítajte si informácie zobrazené na nasledujúcej stránke a potom kliknite na tlačidlo **Next** (Ďalej). Šifrovací kľúč sa uloží na vybraté pamäťové zariadenie.
5. Keď sa otvorí potvrdzujúce dialógové okno, kliknite na tlačidlo **Finish** (Dokončiť).

Vykonanie obnovenia

Ak chcete vykonať obnovenie v prípade zabudnutého hesla, postupujte podľa nasledujúcich krokov:

1. Zapnite počítač.
2. Vložte vymeniteľné pamäťové zariadenie obsahujúce zálohovací kľúč.
3. Po otvorení dialógového okna aplikácie Drive Encryption pre nástroj HP ProtectTools kliknite na tlačidlo **Cancel** (Zrušiť).
4. Kliknite na tlačidlo **Options** (Možnosti) v ľavom dolnom rohu obrazovky a potom kliknite na tlačidlo **Recovery** (Obnovenie).
5. Vyberte súbor, ktorý obsahuje zálohovací kľúč, alebo ho vyhľadajte kliknutím na tlačidlo **Browse** (Prehľadávať) a potom kliknite na tlačidlo **Next** (Ďalej).
6. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **OK**.

   Počítač sa spustí.

POZNÁMKA: Po vykonaní obnovenia sa dôrazne odporúča nastaviť nové heslo.

8 HP ProtectTools – modul Privacy Manager (len niektoré modely)

Aplikácia Privacy Manager pre nástroj HP ProtectTools umožňuje použiť pokročilé metódy bezpečného prihlasovania (overovania) na kontrolu zdroja, integrity a zabezpečenia komunikácie pri používaní e-mailov, dokumentov balíka programov Microsoft® Office alebo okamžitých správ (IM).

Aplikácia Privacy Manager využíva bezpečnostnú infraštruktúru poskytovanú v nástroji HP ProtectTools Security Manager, ktorá obsahuje nasledujúce metódy bezpečného prihlasovania:

- Overovanie odtlačkov prstov
- Heslo pre systém Windows®
- Karta HP ProtectTools Java™ Card

V aplikácii Privacy Manager môžete použiť ktorékoľvek z vyššie uvedených metód bezpečného prihlasovania.

Privacy Manager vyžaduje nasledujúce položky:

- HP ProtectTools Security Manager 5.00 alebo vyšší
- Operačný systém Windows® 7, Windows Vista® alebo Windows XP
- Microsoft Outlook 2007 alebo Microsoft Outlook 2003
- Platné e-mailové konto

POZNÁMKA: Pred prístupom k funkciám zabezpečenia je nutné vyžiadať certifikát aplikácie Privacy Manager (digitálny certifikát) a nainštalovať ho z aplikácie Privacy Manager. Informácie o vyžiadaní certifikátu aplikácie Privacy Manager nájdete v časti Vyžiadanie a inštalácia certifikátu aplikácie Privacy Manager na strane 44.

Inštalačné postupy

Otvorenie aplikácie Privacy Manager

Otvorenie aplikácie Privacy Manager:

1. Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Security Manager** (Správca zabezpečenia nástroja HP ProtectTools).
2. Kliknite na položku **Privacy Manager**.

– alebo –

Kliknite pravým tlačidlom myši na ikonu nástroja **HP ProtectTools** v oblasti oznámení úplne vpravo na paneli úloh, kliknite na položku **Privacy Manager** (Správca osobných údajov) a potom kliknite na položku **Configuration** (Konfigurácia).

– alebo –

Na paneli s nástrojmi e-mailových správ programu Microsoft Outlook kliknite na šípku nadol vedľa položky **Send Securely** (Odoslať bezpečne) a potom kliknite na položku **Certificates** (Certifikáty) alebo **Trusted Contacts** (Dôveryhodné kontakty).

– alebo –

Na paneli s nástrojmi dokumentov balíka programov Microsoft Office kliknite na šípku nadol vedľa položky **Sign and Encrypt** (Podpísať a šifrovať) a potom kliknite na položku **Certificates** (Certifikáty) alebo **Trusted Contacts** (Dôveryhodné kontakty).

Správa certifikátov aplikácie Privacy Manager

Certifikáty aplikácie Privacy Manager chránia údaje a správy použitím šifrovacej technológie s názvom infraštruktúra verejného kľúča (PKI, public key infrastructure). PKI vyžaduje od používateľov získanie šifrovacích kľúčov a certifikátu aplikácie Privacy Manager vydaného certifikačným úradom (CA). Na rozdiel od väčšiny programov na šifrovania a overovanie údajov, ktoré vyžadujú iba pravidelné overovanie, aplikácia Privacy Manager vyžaduje overovanie identity pri každom podpisovaní e-mailovej správy alebo dokumentu balíka programov Microsoft Office použitím šifrovacieho kľúča. Aplikácia Privacy Manager zabezpečuje a chráni proces ukladania a odosielania dôležitých údajov.

Môžete vykonať nasledujúce úlohy:

- Vyžiadanie a nainštalovanie certifikátu aplikácie Privacy Manager
- Zobrazenie detailov certifikátu aplikácie Privacy Manager
- Obnovenie certifikátov aplikácie Privacy Manager
- Keď je k dispozícii viac certifikátov, nastavenie predvoleného certifikátu aplikácie Privacy Manager na použitie prostredníctvom aplikácie Privacy Manager
- Odstránenie a zrušenie certifikátu aplikácie Privacy Manager (rozšírené)

Vyžiadanie a inštalácia certifikátu aplikácie Privacy Manager

Pred použitím funkcií aplikácie Privacy Manager si musíte vyžiadať a nainštalovať certifikát aplikácie Privacy Manager (z aplikácie Privacy Manager) použitím platnej e-mailovej adresy. E-mailovú adresu

musíte nastaviť ako konto v programe Microsoft Outlook na rovnakom počítači, z ktorého žiadate o vydanie certifikátu aplikácie Privacy Manager.

Vyžiadanie certifikátu aplikácie Privacy Manager

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Certificates** (Certifikáty).
2. Kliknite na položku **Request a Privacy Manager certificate** (Vyžiadať certifikát aplikácie Privacy Manager).
3. Na stránke Welcome (Úvod) si prečítajte zobrazený text a potom kliknite na tlačidlo **Next** (Ďalej).
4. Na stránke License Agreement (Licenčná zmluva) si prečítajte licenčnú zmluvu.
5. Začiarknite políčko vedľa položky **Check here to accept the terms of this license agreement** (Začiarknutím tohto políčka odsúhlasíte ustanovenia tejto licenčnej zmluvy) a potom kliknite na tlačidlo **Next** (Ďalej).
6. Na stránke Your Certificate Details (Detaily certifikátu) zadajte potrebné údaje a potom kliknite na tlačidlo **Next** (Ďalej).
7. Na stránke Certificate Request Accepted (Žiadosť o certifikát bola prijatá) kliknite na tlačidlo **Finish** (Dokončiť).
8. Kliknutím na tlačidlo **OK** zatvorte certifikát.

Dostanete e-mail do programu Microsoft Outlook s vaším certifikátom aplikácie Privacy Manager v prílohe.

Získanie vopred priradeného firemného certifikátu aplikácie Privacy Manager

1. V aplikácii Outlook otvorte prijatý e-mail s oznámením, že vám bol vopred priradený firemný certifikát.
2. Kliknite na položku **Obtain** (Získať).
3. Dostanete e-mail do programu Microsoft Outlook s vaším certifikátom aplikácie Privacy Manager v prílohe.
4. Ak chcete nainštalovať tento certifikát, pozrite si časť Inštalácia certifikátu aplikácie Privacy Manager na strane 45

Inštalácia certifikátu aplikácie Privacy Manager

1. Ak dostanete e-mail s vaším certifikátom aplikácie Privacy Manager v prílohe, otvorte tento e-mail a kliknite na tlačidlo **Setup** (Inštalácia) v pravom dolnom rohu správy v aplikácii Outlook 2007 alebo v ľavom hornom rohu v aplikácii Outlook 2003.
2. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.
3. Na stránke Certificate Installed (Certifikát bol nainštalovaný) kliknite na tlačidlo **Next** (Ďalej).
4. Na stránke Certificate Backup (Zálohovanie certifikátu) zadajte umiestnenie a názov zálohovacieho súboru alebo kliknutím na tlačidlo **Browse** (Prehľadávať) vyhľadajte umiestnenie.

△ **UPOZORNENIE:** Nezabudnite uložiť súbor do iného umiestnenia než na váš pevný disk a umiestnite ho na bezpečné miesto. Tento súbor by mal byť určený iba na vaše použitie a vyžaduje sa v prípade potreby obnovenia vášho certifikátu aplikácie Privacy Manager a priradených kľúčov.

5. Zadajte a potvrďte heslo a potom kliknite na tlačidlo **Next** (Ďalej).

6. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

7. Ak vyberiete možnosť začať proces pozvania dôveryhodného kontaktu, postupujte podľa pokynov na obrazovke od kroku 2 témy Pridanie dôveryhodných kontaktov použitím kontaktov aplikácie Microsoft Outlook na strane 49.

   – alebo –

   Ak kliknete na tlačidlo **Cancel** (Zrušiť), informácie o neskoršom pridaní dôveryhodného kontaktu nájdete v časti Pridanie dôveryhodného kontaktu na strane 48.

Zobrazenie podrobností o certifikáte aplikácie Privacy Manager

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Certificates** (Certifikáty).

2. Kliknite na položku Privacy Manager Certificate (Certifikát aplikácie Privacy Manager).

3. Kliknite na položku **Certificate details** (Podrobnosti o certifikáte).

4. Po skončení prezerania podrobností kliknite na tlačidlo **OK**.

Obnovenie certifikátu aplikácie Privacy Manager

Ak sa blíži skončenie platnosti certifikátu aplikácie Privacy Manager, dostanete upozornenie, že ho musíte obnoviť:

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Certificates** (Certifikáty).

2. Kliknite na položku **Renew certificate** (Obnoviť certifikát).

3. Podľa pokynov na obrazovke si zakúpte nový certifikát aplikácie Privacy Manager.

POZNÁMKA: Proces obnovenia certifikátu aplikácie Privacy Manager nenahrádza váš starý certifikát aplikácie Privacy Manager. Budete si musieť kúpiť nový certifikát aplikácie Privacy Manager a nainštalovať ho použitím rovnakých postupov ako v časti Vyžiadanie a inštalácia certifikátu aplikácie Privacy Manager na strane 44.

Nastavenie predvoleného certifikátu aplikácie Privacy Manager

V aplikácii Privacy Manager sú viditeľné iba certifikáty aplikácie Privacy Manager, aj keď máte nainštalované v počítači ďalšie certifikáty od iných certifikačných úradov.

Ak máte v počítači viac certifikátov aplikácie Privacy Manager, ktoré boli nainštalované z aplikácie Privacy Manager, jeden z nich môžete určiť ako predvolený certifikát:

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Certificates** (Certifikáty).

2. Kliknite na certifikát aplikácie Privacy Manager, ktorý chcete použiť ako predvolený, a potom kliknite na tlačidlo **Set default** (Predvoliť).

3. Kliknite na tlačidlo **OK**.

POZNÁMKA: Nemusíte použiť predvolený certifikát aplikácie Privacy Manager. Pri používaní rozličných funkcií aplikácie Privacy Manager môžete vybrať a použiť ktorýkoľvek z certifikátov aplikácie Privacy Manager.

Odstránenie certifikátu aplikácie Privacy Manager

Ak odstránite certifikát aplikácie Privacy Manager, nemôžete otvoriť žiadne súbory ani zobraziť žiadne údaje, ktoré ste zašifrovali pomocou daného certifikátu. Ak náhodne odstránite certifikát aplikácie Privacy Manager, môžete ho obnoviť použitím záložného súboru, ktorý ste vytvorili počas inštalácie certifikátu. Ďalšie informácie nájdete v časti Obnovenie certifikátu aplikácie Privacy Manager na strane 47.

Odstránenie certifikátu aplikácie Privacy Manager:

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Certificates** (Certifikáty).
2. Kliknite na certifikát aplikácie Privacy Manager, ktorý chcete odstrániť, a potom kliknite na položku **Advanced** (Rozšírené).
3. Kliknite na položku **Delete** (Odstrániť).
4. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).
5. Kliknite na položku **Close** (Zavrieť) a potom kliknite na položku **Apply** (Použiť).

Obnovenie certifikátu aplikácie Privacy Manager

Počas inštalácie certifikátu aplikácie Privacy Manager sa vyžaduje, aby ste vytvorili záložnú kópiu certifikátu. Záložnú kópiu môžete vytvoriť aj zo stránky Migration (Migrácia). Túto záložnú kópiu môžete použiť pri migrácii na iný počítač alebo na obnovenie certifikátu do rovnakého počítača.

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Migration** (Migrácia).
2. Kliknite na položku **Restore** (Obnoviť).
3. Na stránke Migration File (Migračný súbor) kliknutím na tlačidlo **Browse** (Prehľadávať) vyhľadajte súbor .dppsm, ktorý ste vytvorili počas procesu zálohovania, a potom kliknite na tlačidlo **Next** (Ďalej).
4. Zadajte heslo, ktoré ste použili pri tvorbe zálohy, a potom kliknite na tlačidlo **Next** (Ďalej).
5. Kliknite na tlačidlo **Finish** (Dokončiť).
6. Kliknite na tlačidlo **OK**.

Ďalšie informácie nájdete v časti Inštalácia certifikátu aplikácie Privacy Manager na strane 45 alebo Zálohovanie dôveryhodných kontaktov a certifikátov aplikácie Privacy Manager na strane 63.

Zrušenie certifikátu aplikácie Privacy Manager

Ak si myslíte, že zabezpečenie certifikátu aplikácie Privacy Manager bolo ohrozené, môžete zrušiť svoj vlastný certifikát:

POZNÁMKA: Zrušený certifikát aplikácie Privacy Manager sa neodstráni. Tento certifikát môžete stále používať na zobrazovanie súborov, ktoré sú šifrované.

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Certificates** (Certifikáty).
2. Kliknite na položku **Advanced** (Rozšírené).
3. Kliknite na certifikát aplikácie Privacy Manager, ktorý chcete zrušiť, a potom kliknite na položku **Revoke** (Zrušiť).

4. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).
5. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.
6. Postupujte podľa pokynov na obrazovke.

Správa dôveryhodných kontaktov

Dôveryhodné kontakty sú používatelia, s ktorými ste si vymenili certifikáty aplikácie Privacy Manager, čo umožňuje bezpečne komunikovať medzi sebou.

Aplikácia Trusted Contacts Manager umožňuje vykonávať nasledujúce úlohy:

- Zobrazenie detailov dôveryhodných kontaktov
- Odstránenie dôveryhodných kontaktov
- Kontrola stavu zrušenia dôveryhodného kontaktu (rozšírené)

Pridanie dôveryhodných kontaktov

Pridávanie dôveryhodných kontaktov je 3-krokový proces:

1. Odošlete e-mailovú pozvánku príjemcovi z dôveryhodných kontaktov.
2. Príjemca z dôveryhodných kontaktov odpovie na tento e-mail.
3. Keď dostanete e-mailovú odpoveď od príjemcu z dôveryhodných kontaktov, kliknite na položku **Accept** (Prijať).

E-mailové pozvánky pre dôveryhodné kontakty môžete odoslať jednotlivým príjemcom alebo všetkým kontaktom v adresári programu Microsoft Outlook.

Informácie o pridávaní dôveryhodných kontaktov nájdete v nasledujúcich častiach.

POZNÁMKA: Na odpovedanie na vašu pozvánku, aby sa mohol stať dôveryhodným kontaktom, musí mať príjemca z dôveryhodných kontaktov nainštalovanú v počítači aplikáciu Privacy Manager alebo alternatívneho klienta. Informácie o inštalácii alternatívneho klienta získate na webovej lokalite DigitalPersona na adrese http://DigitalPersona.com/PrivacyManager.

Pridanie dôveryhodného kontaktu

1. Otvorte aplikáciu Privacy Manager, kliknite na položku **Trusted Contacts Manager** (Správca dôveryhodných kontaktov) a potom kliknite na položku **Invite Contacts** (Pozvať kontakty).

   – alebo –

   V programe Microsoft Outlook kliknite na šípku nadol vedľa položky **Send Securely** (Odoslať bezpečne) na paneli s nástrojmi a potom kliknite na položku **Invite Contacts** (Pozvať kontakty).
2. Ak sa otvorí dialógové okno Select Certificate (Výber certifikátu), kliknite na certifikát aplikácie Privacy Manager, ktorý chcete použiť, a potom kliknite na tlačidlo **OK**.
3. Keď sa otvorí dialógové okno Trusted Contact Invitation (Pozvánka pre dôveryhodný kontakt), prečítajte si zobrazený text a potom kliknite na tlačidlo **OK**.

   Automaticky sa vygeneruje e-mail.

4. Zadajte jednu alebo viac e-mailových adries príjemcov, ktorých chcete pridať ako dôveryhodné kontakty.

5. Upravte text a prihláste sa pod svojím menom (voliteľné).

6. Kliknite na položku **Send** (Odoslať).

POZNÁMKA: Ak nemáte certifikát aplikácie Privacy Manager, hlásenie vás informuje, že pred odoslaním žiadosti o dôveryhodný kontakt musíte mať certifikát aplikácie Privacy Manager. Kliknutím na tlačidlo **OK** spustite sprievodcu Certificate Request Wizard (Sprievodca žiadosťou o certifikát). Ďalšie informácie nájdete v časti Vyžiadanie a inštalácia certifikátu aplikácie Privacy Manager na strane 44.

7. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

POZNÁMKA: Keď tento e-mail prijme príjemca z dôveryhodných kontaktov, musí ho otvoriť a kliknúť na tlačidlo **Accept** (Prijať) v pravom dolnom rohu e-mailu a potom po otvorení potvrdzujúceho dialógového okna kliknúť na tlačidlo **OK**.

8. Keď dostanete e-mailovú odpoveď od príjemcu, ktorý prijal pozvánku stať sa dôveryhodným kontaktom, kliknite na tlačidlo **Accept** (Prijať) v pravom dolnom rohu e-mailu.

   Otvorí sa dialógové okno potvrdzujúce úspešné pridanie príjemcu do zoznamu dôveryhodných kontaktov.

9. Kliknite na tlačidlo **OK**.

Pridanie dôveryhodných kontaktov použitím kontaktov aplikácie Microsoft Outlook

1. Otvorte aplikáciu Privacy Manager, kliknite na položku **Trusted Contacts Manager** (Správca dôveryhodných kontaktov) a potom kliknite na položku **Invite Contacts** (Pozvať kontakty).

   – alebo –

   V programe Microsoft Outlook kliknite na šípku nadol vedľa položky **Send Securely** (Odoslať bezpečne) na paneli s nástrojmi a potom kliknite na položku **Invite All My Outlook Contacts** (Pozvať všetky kontakty programu Outlook).

2. Po otvorení stránky Trusted Contact Invitation (Pozvánka pre dôveryhodný kontakt) vyberte e-mailové adresy príjemcov, ktorých chcete pridať ako dôveryhodné kontakty, a potom kliknite na tlačidlo **Next** (Ďalej).

3. Keď sa otvorí stránka Sending Invitation (Odoslanie pozvánky), kliknite na tlačidlo **Finish** (Dokončiť).

   Automaticky sa vygeneruje e-mail s výpisom vybratých e-mailových adries programu Microsoft Outlook.

4. Upravte text a prihláste sa pod svojím menom (voliteľné).

5. Kliknite na položku **Send** (Odoslať).

POZNÁMKA: Ak nemáte certifikát aplikácie Privacy Manager, hlásenie vás informuje, že pred odoslaním žiadosti o dôveryhodný kontakt musíte mať certifikát aplikácie Privacy Manager. Kliknutím na tlačidlo **OK** spustite sprievodcu Certificate Request Wizard (Sprievodca žiadosťou o certifikát). Ďalšie informácie nájdete v časti Vyžiadanie a inštalácia certifikátu aplikácie Privacy Manager na strane 44.

6. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

POZNÁMKA: Keď tento e-mail prijme príjemca z dôveryhodných kontaktov, musí ho otvoriť a kliknúť na tlačidlo **Accept** (Prijať) v pravom dolnom rohu e-mailu a potom po otvorení potvrdzujúceho dialógového okna kliknúť na tlačidlo **OK**.

7. Keď dostanete e-mailovú odpoveď od príjemcu, ktorý prijal pozvánku stať sa dôveryhodným kontaktom, kliknite na tlačidlo **Accept** (Prijať) v pravom dolnom rohu e-mailu.

   Otvorí sa dialógové okno potvrdzujúce úspešné pridanie príjemcu do zoznamu dôveryhodných kontaktov.

8. Kliknite na tlačidlo **OK**.

Zobrazenie detailov dôveryhodných kontaktov

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Trusted Contacts** (Dôveryhodné kontakty).
2. Kliknite na dôveryhodný kontakt.
3. Kliknite na tlačidlo **Contact details** (Podrobnosti o kontakte).
4. Po skončení prezerania podrobností kliknite na tlačidlo **OK**.

Odstránenie dôveryhodného kontaktu

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Trusted Contacts** (Dôveryhodné kontakty).
2. Kliknite na dôveryhodný kontakt, ktorý chcete odstrániť.
3. Kliknite na tlačidlo **Delete contact** (Odstrániť kontakt).
4. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

Kontrola stavu zrušenia dôveryhodného kontaktu

Postup zistenia, či dôveryhodný kontakt zrušil svoj certifikát aplikácie Privacy Manager:

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Trusted Contacts** (Dôveryhodné kontakty).
2. Kliknite na dôveryhodný kontakt.
3. Kliknite na tlačidlo **Advanced** (Rozšírené).

   Otvorí sa dialógové okno Advanced Trusted Contact Management (Rozšírená správa dôveryhodných kontaktov).

4. Kliknite na tlačidlo **Check Revocation** (Skontrolovať zrušenie).
5. Kliknite na tlačidlo **Close** (Zavrieť).

Všeobecné úlohy

Aplikáciu Privacy Manager môžete použiť s nasledujúcimi produktmi spoločnosti Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Používanie aplikácie Privacy Manager v programe Microsoft Outlook

Ak je nainštalovaná aplikácia Privacy Manager, na paneli s nástrojmi programu Microsoft Outlook sa zobrazí tlačidlo Privacy (Ochrana osobných údajov) a na paneli s nástrojmi každej e-mailovej správy v programe Microsoft Outlook sa zobrazí tlačidlo Send Securely (Odoslať bezpečne). Keď kliknite na šípku nadol vedľa položky **Privacy** (Ochrana osobných údajov) alebo **Send Securely** (Odoslať bezpečne), môžete vybrať z nasledujúcich možností:

- Sign and Send (Podpísať a odoslať) (iba tlačidlo Send Securely (Odoslať bezpečne)) – táto možnosť pridá digitálny podpis do e-mailu a odošle ho po overení identity používateľa použitím zvolenej metódy bezpečného prihlásenia.
- Seal for Trusted Contacts and Send (Zapečatiť pre dôveryhodné kontakty a odoslať) (iba tlačidlo Securely (Odoslať bezpečne)) – táto možnosť pridá digitálny podpis, zašifruje e-mail a odošle ho po overení identity používateľa použitím zvolenej metódy bezpečného prihlásenia.
- Invite Contacts (Pozvať kontakty) – táto možnosť umožňuje odoslať pozvánku pre dôveryhodné kontakty. Ďalšie informácie nájdete v časti Pridanie dôveryhodného kontaktu na strane 48.
- Invite Outlook Contacts (Pozvať kontakty aplikácie Outlook) – táto možnosť umožňuje odoslať pozvánku pre dôveryhodné kontakty všetkým kontaktom v adresári aplikácie Microsoft Outlook. Ďalšie informácie nájdete v časti Pridanie dôveryhodných kontaktov použitím kontaktov aplikácie Microsoft Outlook na strane 49.
- Open the Privacy Manager software (Otvoriť softvér Privacy Manager) – možnosti Certificates (Certifikáty), Trusted Contacts (Dôveryhodné kontakty) a Settings (Nastavenia) umožňujú otvoriť softvér Privacy Manager a pridať, zobraziť alebo zmeniť aktuálne nastavenia. Ďalšie informácie nájdete v časti Konfigurácia aplikácie Privacy Manager pre program Microsoft Outlook na strane 51.

Konfigurácia aplikácie Privacy Manager pre program Microsoft Outlook

1. Otvorte aplikáciu Privacy Manager, kliknite na položku **Settings** (Nastavenia) a potom kliknite na kartu **E-mail**.

   – alebo –

   Na hlavnom paneli s nástrojmi programu Microsoft Outlook kliknite na šípku nadol vedľa položky **Send Securely** (Odoslať bezpečne) (**Privacy** (Ochrana osobných údajov) v aplikácii Outlook 2003) a potom kliknite na tlačidlo **Settings** (Nastavenia).

   – alebo –

   Na paneli s nástrojmi e-mailových správ programu Microsoft Outlook kliknite na šípku nadol vedľa položky **Send Securely** (Odoslať bezpečne) a potom kliknite na tlačidlo **Settings** (Nastavenia).

2. Ak odosielate zabezpečený e-mail, vyberte akcie, ktoré chcete vykonať, a potom kliknite na tlačidlo **OK**.

Podpísanie a odoslanie e-mailovej správy

1. V programe Microsoft Outlook kliknite na tlačidlo **New** (Nová) alebo **Reply** (Odpovedať).
2. Napíšte e-mailovú správu.
3. Kliknite na šípku nadol vedľa položky **Send Securely** (Odoslať bezpečne) (**Privacy** (Ochrana osobných údajov) v aplikácii Outlook 2003) a potom kliknite na tlačidlo **Sign and Send** (Podpísať a odoslať).
4. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

Zapečatenie a odoslanie e-mailovej správy

Zapečatené e-mailové správy, ktoré sú digitálne podpísané a zapečatené (zašifrované), môžu zobraziť iba ľudia, ktorých vyberiete v zozname dôveryhodných kontaktov.

Zapečatenie a odoslanie e-mailovej správy dôveryhodnému kontaktu:

1. V programe Microsoft Outlook kliknite na tlačidlo **New** (Nová) alebo **Reply** (Odpovedať).
2. Napíšte e-mailovú správu.
3. Kliknite na šípku nadol vedľa položky **Send Securely** (Odoslať bezpečne) (**Privacy** (Ochrana osobných údajov) v aplikácii Outlook 2003) a potom kliknite na tlačidlo **Seal for Trusted Contacts and Send** (Zapečatiť pre dôveryhodné kontakty a odoslať).
4. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

Zobrazenie zapečatenej e-mailovej správy

Ak otvoríte zapečatenú e-mailovú správu, v záhlaví e-mailu sa zobrazia informácie o zabezpečení. Označenie zabezpečenia poskytuje nasledujúce informácie:

- Ktoré poverenia boli použité na overenie identity osoby, ktorá podpísala tento e-mail
- Produkt použitý na overenie poverení osoby, ktorá podpísala tento e-mail

Používanie aplikácie Privacy Manager v dokumente balíka programov Microsoft Office 2007

POZNÁMKA: Aplikáciu Privacy Manager môžete používať iba s dokumentmi balíka programov Microsoft Office 2007.

Po nainštalovaní certifikátu aplikácie Privacy Manager sa na pravej strane panela s nástrojmi všetkých dokumentov programov Microsoft Word, Microsoft Excel a Microsoft PowerPoint zobrazí tlačidlo Sign and Encrypt (Podpísať a šifrovať). Keď kliknite na šípku nadol vedľa položky **Sign and Encrypt** (Podpísať a šifrovať), môžete vybrať jednu z nasledujúcich možností:

- Sign Document (Podpísať dokument) – táto možnosť pridá do dokumentu váš digitálny podpis.
- Add Signature Line Before Signing (Pridať riadok pre podpis pred podpísaním) (iba Microsoft Word a Microsoft Excel) – v predvolenom nastavení sa pridá riadok pre podpis, keď podpíšete alebo zašifrujete dokument programu Microsoft Word alebo Microsoft Excel. Ak chcete vypnúť túto možnosť, kliknutím na položku **Add Signature Line** (Pridať riadok pre podpis) odstráňte značku začiarknutia.

- Encrypt Document (Šifrovať dokument) – táto možnosť pridá do dokumentu váš digitálny podpis a zašifruje dokument.
- Remove Encryption (Odstrániť šifrovanie) – táto možnosť odstráni šifrovanie z dokumentu.
- Open the Privacy Manager software (Otvoriť softvér Privacy Manager) – možnosti Certificates (Certifikáty), Trusted Contacts (Dôveryhodné kontakty) a Settings (Nastavenia) umožňujú otvoriť softvér Privacy Manager a pridať, zobraziť alebo zmeniť aktuálne nastavenia. Ďalšie informácie nájdete v časti Správa certifikátov aplikácie Privacy Manager na strane 44, Správa dôveryhodných kontaktov na strane 48 alebo Konfigurovanie aplikácie Privacy Manager pre balík programov Microsoft Office na strane 53.

Konfigurovanie aplikácie Privacy Manager pre balík programov Microsoft Office

1. Otvorte aplikáciu Privacy Manager, kliknite na tlačidlo **Settings** (Nastavenia) a potom kliknite na kartu **Documents** (Dokumenty).

   – alebo –

   Na paneli s nástrojmi dokumentov balíka programov Microsoft Office kliknite na šípku nadol vedľa položky **Sign and Encrypt** (Podpísať a šifrovať) a potom kliknite na tlačidlo **Settings** (Nastavenia).

2. Vyberte činnosti, ktoré chcete konfigurovať, a potom kliknite na tlačidlo **OK**.

Podpísanie dokumentu balíka programov Microsoft Office

1. V programe Microsoft Word, Microsoft Excel alebo Microsoft PowerPoint vytvorte a uložte dokument.
2. Kliknite na šípku nadol vedľa tlačidla **Sign and Encrypt** (Podpísať a šifrovať) a potom kliknite na tlačidlo **Sign Document** (Podpísať dokument).
3. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.
4. Keď sa otvorí potvrdzujúce dialógové okno, prečítajte si zobrazený text a potom kliknite na tlačidlo **OK**.

Ak sa neskôr rozhodnete upraviť dokument, postupujte podľa nasledujúcich krokov:

1. Kliknite na tlačidlo **Office** v ľavom hornom rohu obrazovky.
2. Kliknite na tlačidlo **Prepare** (Pripraviť) a potom kliknite na tlačidlo **Mark as Final** (Označiť ako finálne).
3. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno) a pokračujte v práci.
4. Po dokončení úprav znova podpíšte dokument.

Pridanie riadka pre podpis pri podpisovaní dokumentu programu Microsoft Word alebo Microsoft Excel

Aplikácia Privacy Manager umožňuje pridať riadok pre podpis pri podpisovaní dokumentu programu Microsoft Word alebo Microsoft Excel:

1. V programe Microsoft Word alebo Microsoft Excel vytvorte a uložte dokument.
2. Kliknite na ponuku **Home** (Úvod).

3. Kliknite na šípku nadol vedľa položky **Sign and Encrypt** (Podpísať a šifrovať) a potom kliknite na tlačidlo **Add Signature Line Before Signing** (Pred podpísaním pridať riadok pre podpis).

POZNÁMKA: Ak zvolíte túto možnosť, vedľa tlačidla Add Signature Line Before Signing (Pred podpísaním pridať riadok pre podpis) sa zobrazí značka začiarknutia. V predvolenom nastavení je táto možnosť zapnutá.

4. Kliknite na šípku nadol vedľa tlačidla **Sign and Encrypt** (Podpísať a šifrovať) a potom kliknite na tlačidlo **Sign Document** (Podpísať dokument).

5. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

Pridanie odporúčaných signatárov do dokumentu programu Microsoft Word alebo Microsoft Excel

Do dokumentu môžete pridať viac ako jeden riadok pre podpis, a to menovaním odporúčaných signatárov. Odporúčaný signatár je používateľ, ktorý bol určený vlastníkom dokumentu programu Microsoft Word alebo Microsoft Excel na pridanie riadka pre podpis do dokumentu. Odporúčanými signatármi môžete byť vy alebo iná osoba, od ktorej chcete, aby podpísala váš dokument. Ak napríklad pripravíte dokument, ktorý musí byť podpísaný všetkými členmi vášho oddelenia, môžete zahrnúť riadok pre podpis pre týchto používateľov v dolnej časti poslednej stránky dokumentu s pokynmi na podpísanie do stanoveného dátumu.

Pridanie odporúčaného signatára do dokumentu programu Microsoft Word alebo Microsoft Excel:

1. V programe Microsoft Word alebo Microsoft Excel vytvorte a uložte dokument.

2. Kliknite na ponuku **Insert** (Vložiť).

3. V skupine **Text** na paneli s nástrojmi kliknite na šípku vedľa položky **Signature Line** (Riadok pre podpis) a potom kliknite na tlačidlo **Privacy Manager Signature Provider** (Poskytovateľ podpisov aplikácie Privacy Manager).

   Otvorí sa dialógové okno Signature Setup (Nastavenie podpisu).

4. V poli pod položkou **Suggested signer** (Odporúčaný signatár) zadajte názov odporúčaného signatára.

5. V poli pod položkou **Instructions to the signer** (Pokyny pre signatára) zadajte správu pre tohto odporúčaného signatára.

POZNÁMKA: Táto správa sa zobrazí namiesto titulu a po podpísaní dokumentu sa buď odstráni, alebo nahradí za titul používateľa.

6. Začiarknutím políčka **Show sign date in signature line** (Zobraziť dátum podpisu v riadku pre podpis) môžete zobraziť dátum.

7. Začiarknutím políčka **Show signer's title in signature line** (Zobraziť titul signatára v riadku pre podpis) môžete zobraziť titul.

POZNÁMKA: Keďže odporúčaných signatárov priraďuje k dokumentu jeho vlastník, ak nie sú začiarknuté políčka **Show sign date in signature line** (Zobraziť dátum podpisu v riadku pre podpis) alebo **Show signer's title in signature line** (Zobraziť titul signatára v riadku pre podpis), odporúčaný signatár nebude môcť zobraziť dátum ani titul v riadku pre podpis, a to ani v prípade, ak sú takto nakonfigurované nastavenia dokumentu odporúčaného signatára.

8. Kliknite na tlačidlo **OK**.

Pridanie riadka pre podpis odporúčaného signatára

Keď odporúčaní signatári otvoria dokument, uvidia svoje meno v zátvorkách, čo naznačuje, že sa vyžaduje ich podpis.

Podpísanie dokumentu:

1. Dvakrát kliknite na príslušný riadok pre podpis.
2. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

   Riadok pre podpis sa zobrazí na základe nastavení zadaných vlastníkom dokumentu.

Šifrovanie dokumentu balíka programov Microsoft Office

Dokument balíka programov Microsoft Office môžete šifrovať pre seba a pre vaše dôveryhodné kontakty. Ak zašifrujete dokument a zavriete ho, vy a dôveryhodné kontakty, ktoré vyberiete v zozname, musia pred jeho otvorením overiť svoju identitu.

Postup šifrovania dokumentu balíka programov Microsoft Office:

1. V programe Microsoft Word, Microsoft Excel alebo Microsoft PowerPoint vytvorte a uložte dokument.
2. Kliknite na ponuku **Home** (Úvod).
3. Kliknite na šípku nadol vedľa tlačidla **Sign and Encrypt** (Podpísať a šifrovať) a potom kliknite na tlačidlo **Encrypt Document** (Šifrovať dokument).

   Otvorí sa dialógové okno Select Trusted Contacts (Výber dôveryhodných kontaktov).
4. Kliknite na meno dôveryhodného kontaktu, ktorý bude môcť otvoriť dokument a zobraziť jeho obsah.

POZNÁMKA: Ak chcete vybrať viac mien dôveryhodných kontaktov, podržte kláves ctrl a kliknite na jednotlivé mená.

5. Kliknite na tlačidlo **OK**.

Ak sa neskôr rozhodnete upraviť dokument, postupujte podľa krokov v časti Odstránenie šifrovania z dokumentu balíka programov Microsoft Office na strane 55. Po odstránení šifrovania môžete upraviť dokument. Podľa krokov v tento časť znova zašifrujte dokument.

Odstránenie šifrovania z dokumentu balíka programov Microsoft Office

Ak odstránite šifrovanie z dokumentu balíka programov Microsoft Office, vy ani vaše dôveryhodné kontakty nebudú musieť viac overovať svoju identitu pred otvorením a zobrazením obsahu dokumentu.

Odstránenie šifrovania z dokumentu balíka programov Microsoft Office:

1. Otvorte šifrovaný dokument programu Microsoft Word, Microsoft Excel alebo Microsoft PowerPoint.
2. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.
3. Kliknite na ponuku **Home** (Úvod).
4. Kliknite na šípku nadol vedľa položky **Sign and Encrypt** (Podpísať a šifrovať) a potom kliknite na tlačidlo **Remove Encryption** (Odstrániť šifrovanie).

Odoslanie šifrovaného dokumentu balíka programov Microsoft Office

Šifrovaný dokument balíka programov Microsoft Office môžete priložiť do e-mailovej správy bez podpísania alebo šifrovania samotného e-mailu. Na tento účel vytvorte a odošlite e-mail s podpísaným alebo šifrovaným dokumentom rovnako ako v prípade bežného e-mailu s prílohou.

Avšak z dôvodu optimálneho zabezpečenia sa odporúča zašifrovať e-mail po priložení podpísaného alebo šifrovaného dokumentu balíka programov Microsoft Office.

Ak chcete odoslať zapečatený e-mail s priloženým podpísaným alebo šifrovaným dokumentom balíka programov Microsoft Office, postupujte podľa nasledujúcich krokov:

1. V programe Microsoft Outlook kliknite na tlačidlo **New** (Nová) alebo **Reply** (Odpovedať).
2. Napíšte e-mailovú správu.
3. Priložte dokument balíka programov Microsoft Office.
4. Ďalšie pokyny nájdete v časti Zapečatenie a odoslanie e-mailovej správy na strane 52.

Zobrazenie podpísaného dokumentu balíka programov Microsoft Office

POZNÁMKA: Na zobrazenie podpísaného dokumentu balíka programov Microsoft Office nemusíte mať certifikát aplikácie Privacy Manager.

Pri otvorení podpísaného dokumentu balíka programov Microsoft Office sa zobrazí ikona digitálneho podpisu v stavovom riadku v dolnej časti okna s dokumentom.

1. Kliknutím na ikonu **Digital Signatures** (Digitálne podpisy) môžete prepnúť zobrazenie dialógového okna Signatures (Podpisy), slúžiaceho na zobrazenie mien všetkých používateľov, ktorí podpísali dokument, a dátumu podpísania každým z používateľov.
2. Ak chcete zobraziť ďalšie podrobnosti o každom z podpisov, kliknite pravým tlačidlom myši na meno v dialógovom okne Signatures (Podpisy) a vyberte položku Signature Details (Podrobnosti o podpise).

Zobrazenie šifrovaného dokumentu balíka programov Microsoft Office

Ak chcete zobraziť šifrovaný dokument balíka programov Microsoft Office z iného počítača, v tomto počítači musí byť nainštalovaná aplikácia Privacy Manager. Okrem toho musíte obnoviť certifikát aplikácie Privacy Manager, ktorý bol použitý na šifrovanie súboru.

Dôveryhodný kontakt, ktorý chce zobraziť šifrovaný dokument balíka programov Microsoft Office, musí mať certifikát aplikácie Privacy Manager a v jeho počítači musí byť nainštalovaná aplikácia Privacy Manager. Okrem toho musí vlastník šifrovaného dokumentu balíka programov Microsoft Office vybrať tento dôveryhodný kontakt.

Používanie aplikácie Privacy Manager v programe Windows Live Messenger

Aplikácia Privacy Manager pridá do aplikácie Windows Live Messenger nasledujúce funkcie bezpečnej komunikácie:

- **Secure chat** (Bezpečná konverzácia) – správy sa odosielajú použitím protokolu SSL/TLS (Secure Sockets Layer/Transport Layer Security) cez XML, čo je rovnaká technológia, ktorá zaručuje zabezpečenie transakcií elektronického obchodovania.
- **Recipient identification** (Identifikácia príjemcu) – pred odoslaním správy môžete overiť prítomnosť a identitu osoby.
- **Signed messages** (Podpísané správy) – môžete elektronicky podpísať vaše správy. Potom v prípade, ak dôjde k neoprávnenej úprave správy, bude po jej prijatí príjemcom označená ako neplatná.
- **Hide/show feature** (Skryť/zobraziť funkciu) – môžete skryť ľubovoľné alebo všetky správy v okne aplikácie Privacy Manager Chat. Môžete tiež odoslať správu so skrytým obsahom. Pred zobrazením správy sa vyžaduje overenie.
- **Secure chat history** (Bezpečná história konverzácií) – denníky relácií konverzácií sú pred ich uložením zašifrované a ich zobrazenie vyžaduje overenie.
- **Automatic locking/unlocking** (Automatické uzamknutie/odomknutie) – môžete uzamknúť a odomknúť okno aplikácie Privacy Manager Chat alebo nastaviť jeho automatické uzamknutie po zadanom intervale nečinnosti.

Spustenie relácie konverzácií aplikácie Privacy Manager

POZNÁMKA: Ak chcete použiť aplikáciu Privacy Manager Chat, obe strany musia mať nainštalovanú aplikáciu Privacy Manager a certifikát aplikácie Privacy Manager. Podrobnosti o inštalácii certifikátu aplikácie Privacy Manager nájdete v časti Vyžiadanie a inštalácia certifikátu aplikácie Privacy Manager na strane 44.

1. Ak chcete spustiť aplikáciu Privacy Manager Chat v aplikácii Windows Live Messenger, vykonajte jeden z nasledujúcich postupov:

   a. Kliknite pravým tlačidlom myši na kontakt online v aplikácii Live Messenger a potom vyberte položku **Start an Activity** (Začať aktivitu).

   b. Kliknite na položku **Start Chat** (Začať konverzáciu).

   – alebo –

   a. Dvakrát kliknite na kontakt online v aplikácii Live Messenger a potom vyberte ponuku **See a list of activities** (Zobraziť zoznam aktivít).

   b. Kliknite na položku **Action** (Akcia) a potom kliknite na položku **Start Chat** (Začať konverzáciu).

– alebo –

a. Kliknite pravým tlačidlom myši na ikonu nástroja ProtectTools v oblasti oznámení, kliknite na položku **Privacy Manager for HP ProtectTools** (Modul Privacy Manager pre nástroj HP ProtectTools) a potom vyberte položku **Start Chat** (Začať konverzáciu).

b. V aplikácii Live Messenger kliknite na položku **Actions: Start an Activity** (Akcie: začať aktivitu) a potom vyberte položku **Privacy Manager Chat**.

POZNÁMKA: Každý používateľ musí byť online v aplikácii Live Messenger a používatelia musia byť vzájomne zobrazení v okne online ich aplikácií Live Messenger. Kliknutím vyberte používateľa online.

Aplikácia Privacy Manager odošle pozvánku kontaktu na spustenie aplikácie Privacy Manager Chat. Keď ju pozvaný kontakt prijme, otvorí sa okno aplikácie Privacy Manager Chat. Ak pozvaný kontakt nemá nainštalovanú aplikáciu Privacy Manager, zobrazí sa mu výzva na jej prevzatie.

2. Kliknutím na položku **Start** (Štart) môžete začať bezpečnú konverzáciu.

Konfigurácia nástroja Privacy Manager pre aplikáciu Windows Live Messenger

1. V aplikácii Privacy Manager Chat kliknite na položku **Settings** (Nastavenia).

   – alebo –

   V aplikácii Privacy Manager kliknite na položku **Settings** (Nastavenia) a potom kliknite na kartu **Chat** (Konverzácia).

   – alebo –

   V aplikácii Privacy Manager Live Messenger History Viewer kliknite na tlačidlo **Settings** (Nastavenia).

2. Ak chcete zadať dobu čakania, po uplynutí ktorej aplikácia Privacy Manager Chat uzamkne reláciu, vyberte číslo v poli **Lock session after _ minutes of inactivity** (Uzamknúť reláciu po _ minútach nečinnosti).

3. Ak chcete zadať priečinok histórie pre relácie konverzácií, kliknutím na tlačidlo **Browse** (Prehľadávať) vyhľadajte priečinok a potom kliknite na tlačidlo **OK**.

4. Ak chcete automaticky šifrovať a ukladať relácie pri ich zatvorení, začiarknite políčko **Automatically save secure chat history** (Automaticky ukladať históriu bezpečných konverzácií).

5. Kliknite na tlačidlo **OK**.

Konverzovanie v okne aplikácie Privacy Manager Chat

Po spustení aplikácie Privacy Manager Chat sa v programe Windows Live Messenger otvorí okno aplikácie Privacy Manager Chat. Používanie aplikácie Privacy Manager Chat je podobné používaniu

základného programu Windows Live Messenger, s tým rozdielom, že v okne aplikácie Privacy Manager Chat sú k dispozícii nasledujúce doplnkové funkcie:

- **Save** (Uložiť) – kliknutím na toto tlačidlo môžete uložiť reláciu konverzácií do priečinka uvedeného v konfiguračných nastaveniach. Môžete tiež konfigurovať aplikáciu Privacy Manager Chat tak, aby automaticky ukladala každú reláciu pri jej zatvorení.
- **Hide all** (Skryť všetky) a **Show all** (Zobraziť všetky) – kliknutím na príslušné tlačidlo môžete rozbaliť alebo zbaliť správy zobrazené v okne Secure Communications (Bezpečná komunikácia). Jednotlivé správy môžete tiež skryť alebo zobraziť kliknutím na hlavičku správy.
- **Are you there?** (Ste tam?) – kliknutím na toto tlačidlo môžete požiadať váš kontakt o overenie.
- **Lock** (Uzamknúť) – kliknutím na toto tlačidlo môžete zatvoriť okno aplikácie Privacy Manager Chat a vrátiť sa do okna Chat Entry (Vstup do konverzácie). Ak chcete znova zobraziť okno Secure Communications (Bezpečná komunikácia), kliknite na položku **Resume the session** (Pokračovať v relácii) a potom overte svoju identitu použitím zvoleného spôsobu bezpečného prihlásenia.
- **Send** (Odoslať) – kliknutím na toto tlačidlo môžete odoslať šifrovanú správu vášmu kontaktu.
- **Send signed** (Odoslať podpísané) – začiarknutím tohto políčka môžete elektronicky podpísať a šifrovať správy. Potom v prípade, ak dôjde k neoprávnenej úprave správy, bude po jej prijatí príjemcom označená ako neplatná. Svoju identitu musíte overiť pri každom odosielaní podpísanej správy.
- **Send hidden** (Odoslať skryté) – začiarknutím tohto políčka môžete zašifrovať a odoslať správu so zobrazením iba hlavičky správy. Váš kontakt musí overiť svoju identitu pred prečítaním obsahu správy.

Zobrazenie histórie konverzácií

Aplikácia Privacy Manager Chat: Live Messenger History Viewer slúži na zobrazenie šifrovaných súborov relácií konverzácie aplikácie Privacy Manager Chat. Relácie môžete uložiť kliknutím na tlačidlo **Save** (Uložiť) v okne aplikácie Privacy Manager Chat alebo nakonfigurovaním automatického ukladania na karte Chat (Konverzácia) v aplikácii Privacy Manager. Každá relácia v zobrazovači zobrazuje (šifrované) zobrazované meno kontaktu a dátum a čas začatia a skončenia relácie. V predvolenom nastavení sa relácie zobrazujú pre všetky e-mailové kontá, ktoré máte nastavené. Ponuku **Display history for** (Zobraziť históriu pre) môžete použiť na výber a zobrazenie iba určitých kont.

Zobrazovač umožňuje vykonávať nasledujúce úlohy:

- Odhalenie všetkých relácií na strane 60
- Odhalenie relácií pre špecifické konto na strane 60
- Zobrazenie identifikácie relácie na strane 60
- Zobrazenie relácie na strane 61
- Vyhľadanie konkrétneho textu v reláciách na strane 61
- Odstránenie relácie na strane 61
- Pridanie alebo odstránenie stĺpcov na strane 61
- Filtrovanie zobrazených relácií na strane 62

Spustenie aplikácie Live Messenger History Viewer:

- V oblasti oznámení úplne vpravo na paneli úloh kliknite pravým tlačidlom myši na ikonu nástroja **HP ProtectTools**, kliknite na položku **Privacy Manager: for HP ProtectTools** (Privacy Manager pre HP ProtectTools) a potom kliknite na položku **Live Messenger History Viewer** (Zobrazovač histórie aplikácie Live Messenger).

– alebo –

- V relácii konverzácií kliknite na položku **History Viewer** (Zobrazovač histórie) alebo **History** (História).

Odhalenie všetkých relácií

Odhalenie všetkých relácií zobrazí dešifrované zobrazované meno kontaktu pre momentálne vybraté relácie a všetky relácie v rovnakom konte.

Odhalenie všetkých uložených relácií histórie konverzácií:

1. V okne programu Live Messenger History Viewer kliknite pravým tlačidlom myši na ľubovoľnú reláciu a potom vyberte položku **Reveal All Sessions** (Odhaliť všetky relácie).
2. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

   Zobrazované mená kontaktov sa dešifrujú.
3. Dvojitým kliknutím na ľubovoľnú reláciu môžete zobraziť jej obsah.

Odhalenie relácií pre špecifické konto

Odhalenie relácie zobrazí dešifrované zobrazované meno kontaktu pre momentálne vybratú reláciu.

Odhalenie špecifickej relácie histórie konverzácií:

1. V okne programu Live Messenger History Viewer kliknite pravým tlačidlom myši na ľubovoľnú reláciu a potom vyberte položku **Reveal Session** (Odhaliť reláciu).
2. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.

   Zobrazované meno kontaktu sa dešifruje.
3. Dvojitým kliknutím na odhalenú reláciu môžete zobraziť jej obsah.

POZNÁMKA: Ďalšie relácie zašifrované pomocou rovnakého certifikátu budú zobrazené s odomknutou ikonou, ktorá signalizuje, že ich môžete zobraziť dvojitým kliknutím na ľubovoľnú z týchto relácií bez ďalšieho overovania. Relácie zašifrované pomocou iného certifikátu sa zobrazia s uzamknutou ikonou, čo signalizuje, že pre tieto relácie sa vyžaduje ďalšie overovanie pred zobrazením zobrazovaných mien kontaktov alebo obsahu.

Zobrazenie identifikácie relácie

Zobrazenie identifikácie relácie:

- V okne programu Live Messenger History Viewer kliknite pravým tlačidlom myši na ľubovoľnú odhalenú reláciu a vyberte položku **View session ID** (Zobraziť identifikáciu relácie).

Zobrazenie relácie

Zobrazenie relácie otvorí súbor na zobrazenie. Ak relácia nebola predtým odhalená (so zobrazením dešifrovaného zobrazovaného mena kontaktu), zároveň sa odhalí.

Zobrazenie relácie histórie aplikácie Live Messenger:

1. V okne programu Live Messenger History Viewer kliknite pravým tlačidlom myši na ľubovoľnú reláciu a potom vyberte položku **View** (Zobraziť).
2. Ak sa zobrazí výzva, vykonajte overenie identity použitím vami zvoleného spôsobu bezpečného prihlásenia.

   Obsah relácie sa dešifruje.

Vyhľadanie konkrétneho textu v reláciách

Text môžete hľadať iba v odhalených (dešifrovaných) reláciách, ktoré sa zobrazia v okne zobrazovača. Toto sú relácie, pre ktoré sa zobrazované meno kontaktu zobrazuje obyčajným textom.

Vyhľadanie textu v reláciách histórie konverzácií:

1. V okne programu Live Messenger History Viewer kliknite na tlačidlo **Search** (Hľadať).
2. Zadajte hľadaný text, nakonfigurujte všetky požadované parametre vyhľadávania a potom kliknite na tlačidlo **OK**.

   Relácie, ktoré obsahujú text, sú v okne zobrazovača zvýraznené.

Odstránenie relácie

1. Vyberte reláciu histórie konverzácií.
2. Kliknite na položku **Delete** (Odstrániť).

Pridanie alebo odstránenie stĺpcov

V predvolenom nastavení sa v okne programu Live Messenger History Viewer zobrazia 3 najčastejšie používané stĺpce. Do zobrazenia môžete pridať ďalšie stĺpce alebo môžete odstrániť stĺpce zo zobrazenia.

Pridanie stĺpcov do zobrazenia:

1. Kliknite pravým tlačidlom myši na ľubovoľné záhlavie stĺpca a potom vyberte položku **Add/Remove Columns** (Pridať alebo odstrániť stĺpce).
2. Na ľavom paneli vyberte záhlavie stĺpca a potom ho kliknutím na položku **Add** (Pridať) premiestnite na pravý panel.

Odstránenie stĺpcov zo zobrazenia:

1. Kliknite pravým tlačidlom myši na ľubovoľné záhlavie stĺpca a potom vyberte položku **Add/Remove Columns** (Pridať alebo odstrániť stĺpce).
2. Na pravom paneli vyberte záhlavie stĺpca a potom ho kliknutím na položku **Remove** (Odstrániť) premiestnite na ľavý panel.

Filtrovanie zobrazených relácií

V okne programu Live Messenger History Viewer sa zobrazí zoznam relácií pre všetky kontá. Môžete tiež filtrovať zobrazené relácie podľa nasledujúcich položiek:

- Špecifické kontá. Podrobnosti nájdete v časti Zobrazenie relácií pre špecifické konto na strane 62.
- Rozsah dátumov. Podrobnosti nájdete v časti Zobrazenie relácií pre rozsah dátumov na strane 62.
- Rôzne priečinky. Podrobnosti nájdete v časti Zobrazenie relácií uložených v inom než predvolenom priečinku na strane 62.

Zobrazenie relácií pre špecifické konto

▲ V okne programu Live Messenger History Viewer vyberte konto v ponuke **Display history for** (Zobraziť históriu pre).

Zobrazenie relácií pre rozsah dátumov

1. V okne programu Live Messenger History Viewer kliknite na ikonu **Advanced Filter** (Rozšírený filter).

   Otvorí sa dialógové okno Advanced Filter (Rozšírený filter).

2. Začiarknite políčko **Display only sessions within specified date range** (Zobraziť iba relácie zo zadaného rozsahu dátumov).

3. Do polí **From date** (Od dátumu) a **To date** (Do dátumu) zadajte deň, mesiac alebo rok, prípadne kliknutím na šípku vedľa kalendára vyberte dátumy.

4. Kliknite na tlačidlo **OK**.

Zobrazenie relácií uložených v inom než predvolenom priečinku

1. V okne programu Live Messenger History Viewer kliknite na ikonu **Advanced Filter** (Rozšírený filter).

2. Začiarknite políčko **Use an alternate history files folder** (Použiť alternatívny priečinok pre súbory histórie).

3. Zadajte umiestnenie priečinka alebo kliknutím na tlačidlo **Browse** (Prehľadávať) vyhľadajte priečinok.

4. Kliknite na tlačidlo **OK**.

Rozšírené úlohy

Migrácia certifikátov modulu Privacy Manager a dôveryhodných kontaktov do iného počítača

Dôveryhodné kontakty a certifikáty aplikácie Privacy Manager môžete bezpečne migrovať do iného počítača alebo zálohovať údaje na ich bezpečné uloženie. Na tento účel zálohujte údaje ako heslom chránený súbor do sieťového umiestnenia alebo akéhokoľvek vymeniteľného pamäťového zariadenia a potom obnovte súbor do nového počítača.

Zálohovanie dôveryhodných kontaktov a certifikátov aplikácie Privacy Manager

Ak chcete zálohovať dôveryhodné kontakty a certifikáty aplikácie Privacy Manager do heslom chráneného súboru, postupujte podľa nasledujúcich krokov:

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Migration** (Migrácia).
2. Kliknite na položku **Backup** (Zálohovať).
3. Na stránke Select Data (Výber údajov) vyberte kategórie údajov, ktoré chcete zahrnúť do migračného súboru, a potom kliknite na tlačidlo **Next** (Ďalej).
4. Na stránke Migration File (Migračný súbor) zadajte názov súboru alebo kliknutím na tlačidlo **Browse** (Prehľadávať) vyhľadajte umiestnenie a potom kliknite na tlačidlo **Next** (Ďalej).
5. Zadajte a potvrďte heslo a potom kliknite na tlačidlo **Next** (Ďalej).

POZNÁMKA: Uložte toto heslo na bezpečnom mieste, pretože ho budete potrebovať pri obnovení migračného súboru.

6. Vykonajte overenie identity použitím zvolenej metódy bezpečného prihlásenia.
7. Na stránke Migration File Saved (Migračný súbor bol uložený) kliknite na tlačidlo **Finish** (Dokončiť).

Obnovenie dôveryhodných kontaktov a certifikátov aplikácie Privacy Manager

Ak chcete obnoviť dôveryhodné kontakty a certifikáty aplikácie Privacy Manager do rovnakého počítača alebo do iného počítača v rámci procesu migrácie, postupujte podľa nasledujúcich krokov:

1. Otvorte aplikáciu Privacy Manager a kliknite na položku **Migration** (Migrácia).
2. Kliknite na položku **Restore** (Obnoviť).
3. Na stránke Migration File (Migračný súbor) kliknutím na tlačidlo **Browse** (Prehľadávať) vyhľadajte súbor a potom kliknite na tlačidlo **Next** (Ďalej).
4. Zadajte heslo, ktoré ste použili pri tvorbe záložného súboru, a potom kliknite na tlačidlo **Next** (Ďalej).
5. Na stránke Migration File (Migračný súbor) kliknite na tlačidlo **Finish** (Dokončiť).

Centrálne spravovanie aplikácie Privacy Manager

Inštalácia aplikácie Privacy Manager môže byť súčasťou centralizovanej inštalácie, ktorú prispôsobil správca. Najmenej jedna z nasledujúcich funkcií môže byť povolená alebo zakázaná:

- **Certificate use policy** (Politika používania certifikátov) – môže platiť obmedzenie používania certifikátov aplikácie Privacy Manager vydaných certifikačným úradom Comodo alebo môže byť povolené používanie digitálnych certifikátov vydaných inými certifikačnými úradmi.
- **Encryption policy** (Politika šifrovania) – možnosti šifrovania môžete individuálne povoliť alebo zakázať v balíku programov Microsoft Office alebo v aplikácii Outlook a Windows Live Messenger.

9 HP ProtectTools – modul File Sanitizer

File Sanitizer je nástroj, ktorý umožňuje bezpečne skartovať aktíva (osobné údaje alebo súbory, historické alebo webové údaje alebo iné dôverné údaje) v počítači a pravidelne dôkladne vymazávať údaje z pevného disku.

POZNÁMKA: Táto verzia programu File Sanitizer podporuje iba systémový pevný disk.

Skartovanie údajov

Skartovanie údajov sa líši od štandardného príkazu Delete (Odstrániť) systému Windows® (tiež známy ako jednoduché odstránenie v programe File Sanitizer) tým, že ak skartujete aktívum použitím programu File Sanitizer, spustí sa algoritmus prepísania údajov náhodnými údajmi, ktorý prakticky znemožňuje získať pôvodné aktívum. Jednoduché odstránenie v systéme Windows môže ponechať súbor (alebo aktívum) neporušený na pevnom disku alebo v stave, kedy je možné pomocou forenzných metód obnoviť súbor (alebo aktívum).

Ak zvolíte profil skartovania (vysoké zabezpečenie, stredné zabezpečenie alebo nízke zabezpečenie), pre skartovanie sa automaticky zvolí preddefinovaný zoznam aktív a spôsob vymazania. Môžete tiež prispôsobiť skartovací profil, ktorý umožňuje zadať počet skartovacích cyklov, to, ktoré aktíva sa zahrnú do skartovania, ktoré aktíva sa majú potvrdiť pred skartovaním a ktoré aktíva sa vylúčia zo skartovania. Ďalšie informácie nájdete v časti Výber alebo tvorba profilu skartovania na strane 69.

Môžete nastaviť automatický plán skartovania a môžete tiež kedykoľvek manuálne skartovať aktíva. Ďalšie informácie nájdete v časti Nastavenie plánu skartovania na strane 68, Manuálne skartovanie jedného aktíva na strane 73 alebo Manuálne skartovanie všetkých vybratých položiek na strane 74.

POZNÁMKA: Súbor .dll sa skartuje a odstráni zo systému iba v prípade, ak bol presunutý do koša.

Dôkladné vymazanie voľného miesta

Odstránením aktíva v systéme Windows sa obsah aktíva úplne neodstráni z pevného disku. Systém Windows odstráni iba odkaz na aktívum. Obsah aktíva stále zostane na pevnom disku, až kým iné aktívum neprepíše rovnakú oblasť na pevnom disku novými údajmi.

Dôkladné vymazanie voľného miesta umožňuje bezpečne prepísať náhodnými údajmi odstránené aktíva, čo zabraňuje používateľom zobraziť pôvodný obsah odstráneného aktíva.

POZNÁMKA: Dôkladné vymazanie voľného miesta je určené pre tie aktíva, ktoré odstránite použitím koša systému Windows, alebo pre manuálne odstraňované aktíva. Dôkladné vymazanie voľného miesta neposkytuje žiadne ďalšie zabezpečenie pre skartované aktíva.

Môžete nastaviť automatický plán dôkladného vymazávania voľného miesta alebo môžete manuálne aktivovať dôkladné vymazanie voľného miesta použitím ikony nástroja **HP ProtectTools** v oblasti oznámení úplne vpravo na paneli úloh. Ďalšie informácie nájdete v časti Nastavenie plánu dôkladného vymazávania voľného miesta na strane 69 alebo Manuálna aktivácia dôkladného vymazania voľného miesta na strane 74.

Inštalačné postupy

Otvorenie aplikácie File Sanitizer

Otvorenie aplikácie File Sanitizer:

1. Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Security Manager** (Správca zabezpečenia nástroja HP ProtectTools).
2. Kliknite na položku **File Sanitizer**.

– alebo –

- Dvakrát kliknite na ikonu aplikácie **File Sanitizer** umiestnenú na pracovnej ploche.

– alebo –

- Kliknite pravým tlačidlom myši na ikonu aplikácie **HP ProtectTools** v oblasti oznámení úplne vpravo na paneli úloh, kliknite na položku **File Sanitizer** a potom kliknite na položku **Open File Sanitizer** (Otvoriť aplikáciu File Sanitizer).

Nastavenie plánu skartovania

POZNÁMKA: Informácie o výbere preddefinovaného profilu skartovania alebo tvorbe profilu skartovania nájdete v časti Výber alebo tvorba profilu skartovania na strane 69.

POZNÁMKA: Informácie o manuálnom skartovaní aktív nájdete v časti Manuálne skartovanie jedného aktíva na strane 73.

1. Otvorte aplikáciu File Sanitizer a kliknite na položku **Shred** (Skartovať).
2. Vyberte možnosť skartovania:
   - **Windows shutdown** (Vypnutie systému Windows) – táto možnosť slúži na skartovanie všetkých vybratých aktív pri vypnutí systému Windows.

     POZNÁMKA: Po vybratí tejto možnosti sa pri vypnutí systému zobrazí dialógové okno s otázkou, či chcete pokračovať v skartovaní vybratých aktív alebo či chcete tento postup vynechať. Kliknutím na tlačidlo **Yes** (Áno) môžete obísť postup skartovania alebo kliknutím na tlačidlo **No** (Nie) môžete pokračovať v skartovaní.
   - **Web browser open** (Otvorenie webového prehľadávača) – táto možnosť slúži na skartovanie všetkých vybratých webových aktív, ako napríklad histórie adries URL prehľadávača, pri otvorení webového prehľadávača.
   - **Web browser quit** (Ukončenie webového prehľadávača) – táto možnosť slúži na skartovanie všetkých vybratých webových aktív, ako napríklad histórie adries URL prehľadávača, pri zatvorení webového prehľadávača.
   - **Key sequence** (Klávesová skratka) – vyberte túto možnosť na aktiváciu skartovania použitím klávesovej skratky.
   - **Scheduler** (Plánovač) – začiarknite políčko **Activate Scheduler** (Aktivovať plánovač), zadajte heslo pre systém Windows a potom zadajte deň a čas skartovania vybratých aktív.

POZNÁMKA: Súbor .dll sa skartuje a odstráni zo systému iba v prípade, ak bol presunutý do koša.

3. Kliknite na tlačidlo **Apply** (Použiť) a potom kliknite na tlačidlo **OK**.

Nastavenie plánu dôkladného vymazávania voľného miesta

POZNÁMKA: Dôkladné vymazávanie voľného miesta je určené pre tie aktíva, ktoré odstránite použitím koša systému Windows, alebo pre manuálne odstraňované aktíva. Dôkladné vymazanie voľného miesta neposkytuje žiadne ďalšie zabezpečenie pre skartované aktíva.

Nastavenie plánu dôkladného vymazávania voľného miesta:

1. Otvorte aplikáciu File Sanitizer a kliknite na položku **Free Space Bleaching** (Dôkladné vymazávanie voľného miesta).
2. Začiarknite políčko **Activate Scheduler** (Aktivovať plánovač), zadajte heslo pre systém Windows a potom zadajte deň a čas dôkladného vymazania voľného miesta na pevnom disku.
3. Kliknite na tlačidlo **Apply** (Použiť) a potom kliknite na tlačidlo **OK**.

POZNÁMKA: Dôkladné vymazanie voľného miesta môže trvať veľmi dlho. Aj keď dôkladné vymazanie voľného miesta sa vykonáva na pozadí, počítač môže pracovať pomalšie z dôvodu zvýšenej záťaže procesora.

Výber alebo tvorba profilu skartovania

Výberom preddefinovaného profilu alebo vytvorením vlastného profilu môžete zadať metódu vymazávania a vybrať aktíva na skartovanie.

Výber preddefinovaného profilu skartovania

Ak zvolíte preddefinovaný profil skartovania (vysoké zabezpečenie, stredné zabezpečenie alebo nízke zabezpečenie), automaticky sa zvolí preddefinovaný zoznam aktív a metóda vymazávania. Kliknutím na tlačidlo **View Details** (Zobraziť podrobnosti) môžete zobraziť preddefinovaný zoznam aktív, ktoré sú vybraté na skartovanie.

Výber preddefinovaného profilu skartovania:

1. Otvorte aplikáciu File Sanitizer a kliknite na položku **Settings** (Nastavenia).
2. Kliknite na preddefinovaný profil skartovania.
3. Kliknutím na položku **View Details** (Zobraziť podrobnosti) môžete zobraziť zoznam aktív, ktoré sú vybraté na skartovanie.
4. V časti **Shred the following** (Skartovať nasledujúce) začiarknite políčko vedľa každého aktíva, ktoré chcete potvrdiť pred skartovaním.
5. Kliknite na tlačidlo **Apply** (Použiť) a potom kliknite na tlačidlo **OK**.

Prispôsobenie profilu skartovania

Ak vytvoríte profil skartovania, zadáte počet skartovacích cyklov, to, ktoré aktíva sa zahrnú do skartovania, ktoré aktíva sa majú potvrdiť pred skartovaním a ktoré aktíva sa vylúčia zo skartovania:

1. Otvorte aplikáciu File Sanitizer a kliknite na položku **Settings** (Nastavenia), kliknite na položku **Advanced Security Settings** (Rozšírené nastavenia zabezpečenia) a potom kliknite na položku **View Details** (Zobraziť podrobnosti).

2. Zadajte počet cyklov skartovania.

POZNÁMKA: Vybratý počet cyklov skartovania sa vykoná pre každé aktívum. Ak vyberiete napríklad 3 cykly skartovania, algoritmus, ktorý prepisuje pôvodné údaje náhodnými údajmi, sa spustí 3-krát za sebou. Ak zvolíte cykly skartovania s vyšším zabezpečením, skartovanie môže trvať výrazne dlhšie; avšak čím vyšší počet cyklov skartovania zadáte, tým menej pravdepodobná bude možnosť obnovenia údajov.

3. Vyberte aktíva, ktoré chcete skartovať:

   a. V časti **Available shred options** (Dostupné možnosti skartovania) kliknite na aktívum a potom kliknite na tlačidlo **Add** (Pridať).

   b. Ak chcete pridať vlastné aktívum, kliknite na položku **Add Custom Option** (Pridať vlastnú možnosť) a potom vyhľadajte alebo zadajte cestu k názvu súboru alebo priečinku. Kliknite na tlačidlo **Open** (Otvoriť) a potom kliknite na tlačidlo **OK**. V časti **Available shred options** (Dostupné možnosti skartovania) kliknite na vlastné aktívum a potom kliknite na položku **Add** (Pridať).

POZNÁMKA: Ak chcete odstrániť aktívum z dostupných možností skartovania, kliknite na aktívum a potom kliknite na tlačidlo **Delete** (Odstrániť).

4. V časti **Shred the following** (Skartovať nasledujúce) začiarknite políčko vedľa každého aktíva, ktoré chcete potvrdiť pred skartovaním.

POZNÁMKA: Ak chcete odstrániť aktívum zo zoznamu aktív určených na skartovanie, kliknite na aktívum a potom kliknite na tlačidlo **Remove** (Odstrániť).

5. Ak chcete chrániť súbory alebo priečinky pred automatickým skartovaním, v časti **Do not shred the following** (Neskartovať nasledujúce) kliknite na tlačidlo **Add** (Pridať) a potom prehľadajte alebo zadajte cestu k názvu súboru alebo priečinku. Kliknite na tlačidlo **Open** (Otvoriť) a potom kliknite na tlačidlo **OK**.

POZNÁMKA: Ak chcete odstrániť aktívum zo zoznamu vylúčených aktív, kliknite na aktívum a potom kliknite na tlačidlo **Delete** (Odstrániť).

6. Po dokončení konfigurácie profilu skartovania kliknite na tlačidlo **Apply** (Použiť) a potom kliknite na tlačidlo **OK**.

Prispôsobenie profilu jednoduchého odstránenia

Profil jednoduchého odstránenia vykonáva štandardné odstránenie aktíva bez skartovania. Ak prispôsobíte profil jednoduchého odstránenia, určíte, ktoré aktíva sa zahrnú do jednoduchého odstránenia, ktoré aktíva treba potvrdiť pred vykonaním jednoduchého odstránenia a ktoré aktíva treba vylúčiť z jednoduchého odstránenia.

POZNÁMKA: Ak použijete možnosť jednoduchého odstránenia, dôkladné vymazanie voľného miesta je možné vykonávať z času na čas pre aktíva, ktoré boli odstránené manuálne, alebo pomocou koša systému Windows.

Prispôsobenie profilu jednoduchého odstránenia:

1. Otvorte program File Sanitizer, kliknite na položku **Settings** (Nastavenia), kliknite na položku **Simple Delete Setting** (Nastavenie jednoduchého odstránenia) a potom kliknite na položku **View Details** (Zobraziť podrobnosti).

2. Vyberte aktíva, ktoré chcete odstrániť:

   a. V časti **Available delete options** (Dostupné možnosti odstránenia) kliknite na aktívum a potom kliknite na tlačidlo **Add** (Pridať).

   b. Ak chcete pridať vlastné aktívum, kliknite na položku **Add Custom Option** (Pridať vlastnú možnosť), zadajte názov súboru alebo priečinka a potom kliknite na tlačidlo **OK**. Kliknite na vlastné aktívum a potom kliknite na tlačidlo **Add** (Pridať).

POZNÁMKA: Ak chcete odstrániť aktívum z dostupných možností odstránenia, kliknite na aktívum a potom kliknite na tlačidlo **Delete** (Odstrániť).

3. V časti **Delete the following** (Odstrániť nasledujúce) začiarknite políčko vedľa každého aktíva, ktoré chcete potvrdiť pred odstránením.

POZNÁMKA: Ak chcete odstrániť aktívum zo zoznamu aktív na odstránenie, kliknite na aktívum a potom kliknite na tlačidlo **Remove** (Odstrániť).

4. V časti **Do not delete the following** (Neodstrániť nasledujúce) kliknutím na tlačidlo **Add** (Pridať) vyberte konkrétne aktíva, ktoré chcete vylúčiť zo skartovania.

POZNÁMKA: Ak chcete odstrániť aktívum zo zoznamu vylúčených aktív, kliknite na aktívum a potom kliknite na tlačidlo **Delete** (Odstrániť).

5. Po dokončení konfigurácie profilu jednoduchého odstránenia kliknite na tlačidlo **Apply** (Použiť) a potom kliknite na tlačidlo **OK**.

Všeobecné úlohy

Program File Sanitizer môžete použiť na vykonávanie nasledujúcich úloh:

- Aktivácia skartovania pomocou klávesovej skratky – táto funkcia umožňuje vytvoriť klávesovú skratku (napríklad ctrl+alt+s) na aktiváciu skartovania. Podrobnosti nájdete v časti Použitie klávesovej skratky aktivácie skartovania na strane 72.
- Aktivácia skartovania pomocou ikony programu File Sanitizer – táto funkcia je podobná funkcii uchopenia a presunutia myšou v systéme Windows. Podrobnosti nájdete v časti Používanie ikony programu File Sanitizer na strane 73.
- Manuálne skartovanie konkrétneho aktíva alebo všetkých vybratých aktív – tieto funkcie umožňujú manuálne skartovať položky bez čakania na spustenie pravidelného plánu skartovania. Podrobnosti nájdete v časti Manuálne skartovanie jedného aktíva na strane 73 alebo Manuálne skartovanie všetkých vybratých položiek na strane 74.
- Manuálna aktivácia dôkladného vymazania voľného miesta – táto funkcia umožňuje manuálne aktivovať dôkladné vymazanie voľného miesta. Podrobnosti nájdete v časti Manuálna aktivácia dôkladného vymazania voľného miesta na strane 74.
- Zrušenie operácie skartovania alebo dôkladného vymazania voľného miesta – táto funkcia umožňuje zastaviť operáciu skartovania alebo dôkladného vymazania voľného miesta. Podrobnosti nájdete v časti Zrušenie skartovania alebo dôkladného vymazania voľného miesta na strane 74.
- Zobrazenie súborov denníka – táto funkcia umožňuje zobraziť súbory denníka skartovania a dôkladného vymazania voľného miesta, ktoré obsahujú všetky chyby alebo zlyhania od poslednej operácie skartovania alebo dôkladného vymazania voľného miesta. Podrobnosti nájdete v časti Zobrazenie súborov denníka na strane 74.

POZNÁMKA: Operácia skartovania alebo dôkladného vymazania voľného miesta môže trvať veľmi dlho. Aj keď operácia skartovania a dôkladného vymazania voľného miesta sa vykonáva na pozadí, počítač môže pracovať pomalšie z dôvodu zvýšenej záťaže procesora.

Použitie klávesovej skratky aktivácie skartovania

Ak chcete zadať klávesovú skratku, postupujte podľa nasledujúcich krokov:

1. Otvorte aplikáciu File Sanitizer a kliknite na položku **Shred** (Skartovať).
2. Začiarknite políčko **Key sequence** (Klávesová skratka).
3. Zadajte znak do zobrazeného poľa.
4. Začiarknite políčko **CTRL** alebo **ALT** a začiarknite políčko **SHIFT**.

   Napríklad na aktiváciu automatického skartovania použitím klávesu s a ctrl+shift zadajte do poľa s a potom vyberte možnosti **CTRL** a **SHIFT**.

POZNÁMKA: Dbajte na to, aby ste vybrali klávesovú skratku odlišnú od ostatných nakonfigurovaných klávesových skratiek.

Aktivácia skartovania použitím klávesovej skratky:

1. Podržte kláves shift a ctrl alebo alt (alebo ľubovoľnú nastavenú kombináciu) počas stlačenia klávesu so zvoleným znakom.
2. Ak sa otvorí potvrdzujúce dialógové okno, kliknite na možnosť **Yes** (Áno).

Používanie ikony programu File Sanitizer

△ **UPOZORNENIE:** Skartované aktíva sa nedajú obnoviť. Dôkladne zvážte, ktoré položky zvolíte pre manuálne skartovanie.

1. Prejdite na dokument alebo priečinok, ktorý chcete skartovať.
2. Presuňte aktívum myšou na ikonu programu File Sanitizer na pracovnej ploche.
3. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

Manuálne skartovanie jedného aktíva

△ **UPOZORNENIE:** Skartované aktíva sa nedajú obnoviť. Dôkladne zvážte, ktoré položky zvolíte pre manuálne skartovanie.

1. Kliknite pravým tlačidlom myši na ikonu nástroja **HP ProtectTools** v oblasti oznámení úplne vpravo na paneli úloh, kliknite na položku **File Sanitizer** a potom kliknite na položku **Shred One** (Skartovať jedno).
2. Keď sa otvorí dialógové okno Browse (Prehľadávať), prejdite na aktívum, ktoré chcete skartovať, a potom kliknite na tlačidlo **OK**.

POZNÁMKA: Ako aktívum môžete vybrať jeden súbor alebo priečinok.

3. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

– alebo –

1. Pravým tlačidlom kliknite na ikonu programu **File Sanitizer** na pracovnej ploche a potom kliknite na položku **Shred One** (Skartovať jedno).
2. Keď sa otvorí dialógové okno Browse (Prehľadávať), prejdite na aktívum, ktoré chcete skartovať, a potom kliknite na tlačidlo **OK**.
3. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

– alebo –

1. Otvorte aplikáciu File Sanitizer a kliknite na položku **Shred** (Skartovať).
2. Kliknite na tlačidlo **Browse** (Prehľadávať).
3. Keď sa otvorí dialógové okno Browse (Prehľadávať), prejdite na aktívum, ktoré chcete skartovať, a potom kliknite na tlačidlo **OK**.
4. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

Manuálne skartovanie všetkých vybratých položiek

1. Kliknite pravým tlačidlom myši na ikonu **HP ProtectTools** v oblasti oznámení úplne vpravo na paneli úloh, kliknite na tlačidlo **File Sanitizer** a potom kliknite na tlačidlo **Shred Now** (Skartovať teraz).
2. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

– alebo –

1. Pravým tlačidlom kliknite na ikonu **File Sanitizer** na pracovnej ploche a potom kliknite na položku **Shred Now** (Skartovať teraz).
2. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

– alebo –

1. Otvorte aplikáciu File Sanitizer a kliknite na položku **Shred** (Skartovať).
2. Kliknite na tlačidlo **Shred now** (Skartovať teraz).
3. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

Manuálna aktivácia dôkladného vymazania voľného miesta

1. Kliknite pravým tlačidlom myši na ikonu programu **HP ProtectTools** v oblasti oznámení úplne vpravo na paneli úloh, kliknite na položku **File Sanitizer** a potom kliknite na položku **Bleach Now** (Dôkladne vymazať teraz).
2. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

– alebo –

1. Otvorte aplikáciu File Sanitizer a kliknite na položku **Free Space Bleaching** (Dôkladné vymazávanie voľného miesta).
2. Kliknite na položku **Bleach Now** (Dôkladne vymazať teraz).
3. Pri otvorení potvrdzujúceho dialógového okna kliknite na tlačidlo **Yes** (Áno).

Zrušenie skartovania alebo dôkladného vymazania voľného miesta

Ak prebieha skartovanie alebo dôkladné vymazanie voľného miesta, nad ikonou nástroja HP ProtectTools Security Manager v oblasti oznámení sa zobrazí hlásenie. Toto hlásenie poskytuje bližšie informácie o procese skartovania alebo dôkladného vymazania voľného miesta (percentuálna hodnota dokončenia) a poskytuje možnosť zrušiť túto operáciu.

Zrušenie operácie:

▲ Kliknite na hlásenie a potom kliknutím na položku **Stop** (Zastaviť) zrušte operáciu.

Zobrazenie súborov denníka

Pri každom skartovaní alebo dôkladnom vymazaní voľného miesta sa generujú súbory denníka obsahujúce všetky chyby alebo zlyhania. Súbory denníka sú vždy aktualizované podľa najnovšieho skartovania alebo dôkladného vymazania voľného miesta.

POZNÁMKA: Súbory, ktoré sú úspešne skartované alebo dôkladne vymazané, sa nezobrazujú v súboroch denníka.

Jeden súbor denníka sa vytvorí pre operáciu skartovania a druhý súbor denníka sa vytvorí pre operáciu dôkladného vymazania voľného miesta. Oba súbory denníka sú umiestnené na pevnom disku v nasledujúcom priečinku:

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

10 HP ProtectTools – modul Device Access Manager (len niektoré modely)

Správcovia operačného systému Windows® používajú súčasť Device Access Manager pre nástroj HP ProtectTools na ovládanie prístupu k zariadeniam v systéme a na ochranu pred neoprávneným prístupom:

- Pre každého používateľa sa vytvárajú profily zariadení s cieľom definovať zariadenia, pre ktoré majú povolený alebo zakázaný prístup.
- Používatelia sú tiež organizovaní do skupín, ako je napríklad preddefinovaná skupina Device Administrator (Správca zariadení), prípadne skupiny môžu byť definované v Ovládacom paneli v časti Administrative Tools (Nástroje na správu), Computer Management (Správa počítača).
- Prístup k zariadeniu je možné povoliť alebo zakázať na základe členstva v skupine.
- Pre triedy zariadení, ako sú napríklad jednotky CD-ROM a DVD, je možné povoliť alebo zakázať prístup na čítanie a zápis samostatne.

Obmedzení používatelia môžu tiež získať povolenie na čítanie a úpravu politiky riadenia prístupu k zariadeniam.

Inštalačné postupy

Otvorenie aplikácie Device Access Manager

Ak chcete otvoriť aplikáciu Device Access Manager, postupujte podľa nasledujúcich krokov:

1. Kliknite na tlačidlo **Start** (Štart), kliknite na položku **All Programs** (Všetky programy), kliknite na položku **HP** a potom kliknite na položku **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools).
2. Na ľavej table kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam).

Konfigurácia prístupu k zariadeniam

Aplikácia Device Access Manager pre nástroj HP ProtectTools ponúka tri zobrazenia:

- Zobrazenie Simple Configuration (Jednoduchá konfigurácia) sa používa na povolenie alebo zakázanie prístupu k triedam zariadení pre členov skupiny Device Administrators (Správcovia zariadení).
- Zobrazenie Device Class Configuration (Konfigurácia tried zariadení) sa používa na udelenie alebo zakázanie prístupu k typom zariadení alebo konkrétnym zariadeniam pre konkrétnych používateľov alebo skupiny.
- Zobrazenie User Access Settings (Nastavenia prístupu používateľov) sa používa na definovanie, ktorí používatelia môžu zobraziť alebo upraviť informácie o jednoduchej konfigurácii a konfigurácii tried zariadení.

Skupina správcov zariadení

Keď je nainštalovaný program Device Access Manager, vytvorí sa skupina Device Administrators (Správcovia zariadení).

Správca systému môže implementovať politiku riadenia jednoduchého prístupu k zariadeniam prostredníctvom zakázania prístupu k skupine tried zariadení, pokiaľ používateľ nie je klasifikovaný ako dôveryhodný (ohľadom prístupu k zariadeniu). Odporúčaný spôsob rozlišovania medzi používateľmi „dôveryhodnými pre dané zariadenie“ a „nedôveryhodnými pre dané zariadenie“ je nastavenie všetkých používateľov „dôveryhodných pre dané zariadenie“ ako členov skupiny Device Administrators (Správcovia zariadení). Udelenie prístupu k zariadeniam pre členov skupiny Device Administrators (Správcovia zariadení) prostredníctvom zobrazenia Simple Configuration (Jednoduchá konfigurácia) alebo Device Class Configuration (Konfigurácia tried zariadení) preto zaručí, že používatelia „dôveryhodní pre dané zariadenie“ budú mať úplný prístup k zadanej skupine tried zariadení.

POZNÁMKA: Pridanie používateľa do skupiny Device Administrators (Správcovia zariadení) nepovolí používateľovi automaticky prístup k zariadeniam. Avšak zobrazenie Simple Configuration (Jednoduchá konfigurácia) môžete použiť na udelenie prístupu k požadovanej skupine tried zariadení pre používateľov „dôveryhodných pre dané zariadenie“.

Ak chcete pridať používateľov do skupiny Device Administrators (Správcovia zariadení), postupujte podľa nasledujúcich krokov:

- V systéme Windows 7, Vista alebo XP Professional použite štandardný doplnok MMC „Local Users and Groups (Lokálni používatelia a skupiny)“.
- V prípade systémov Windows 7, Vista® alebo XP verzie Home zadajte do okna príkazového riadka z oprávneného konta nasledujúci príkaz:

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

Simple Configuration (Jednoduchá konfigurácia)

Správcovia a oprávnení používatelia môžu použiť zobrazenie Simple Configuration (Jednoduchá konfigurácia) na úpravu prístupu k nasledujúcim triedam zariadení pre všetkých používateľov, ktorí nie sú členmi skupiny Device Administrators (Správcovia zariadení):

POZNÁMKA: Ak chcete použiť toto zobrazenie na čítanie informácií o prístupe k zariadeniam, pre používateľa alebo skupinu sa vyžaduje udelený prístup „na čítanie“ v zobrazení **User Access Settings** (Nastavenia prístupu používateľov). Ak chcete použiť toto zobrazenie na úpravu informácií o prístupe k zariadeniam, pre používateľa alebo skupinu sa vyžaduje udelený prístup „na zmenu“ v zobrazení **User Access Settings** (Nastavenia prístupu používateľov).

- Všetky vymeniteľné médiá (diskety, jednotky USB flash atď.)
- Všetky jednotky DVD-ROM/CD-ROM
- Všetky sériové a paralelné porty
- Všetky zariadenia Bluetooth®
- Všetky infračervené zariadenia
- Všetky modemové zariadenia
- Všetky zariadenia PCMCIA
- Všetky zariadenia 1394

Ak chcete povoliť alebo zakázať prístup k niektorej triede zariadení pre všetkých používateľov mimo skupiny Device Administrators (Správcovia zariadení), postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **Simple Configuration** (Jednoduchá konfigurácia).
2. Na pravej table, ak chcete zakázať prístup, začiarknite políčko pre triedu zariadení alebo konkrétne zariadenie. Zrušte začiarknutie políčka, aby sa umožnil prístup k danej triede zariadení alebo konkrétnemu zariadeniu.

   Ak je začiarkavacie políčko neaktívne, hodnoty ovplyvňujúce scenár prístupu boli zmenené v zobrazení Device Class Configuration (Konfigurácia tried zariadení). Ak chcete obnoviť hodnoty späť na jednoduché nastavenia, kliknutím na začiarkavacie políčko zrušte jeho začiarknutie alebo ho začiarknite a potom kliknutím na položku **Yes** (Áno) vykonajte potvrdenie.
3. Kliknite na ikonu **Save** (Uložiť).

   POZNÁMKA: Ak nie je spustená služba na pozadí, otvorí sa dialógové okno s otázkou, či ju chcete spustiť. Kliknite na tlačidlo **Yes** (Áno).
4. Kliknite na tlačidlo **OK**.

Spustenie služby na pozadí

Pred použitím profilov zariadení nástroj HP ProtectTools Security Manager otvorí dialógové okno s otázkou, či chcete spustiť službu na pozadí s názvom HP ProtectTools Device Locking/Auditing (Uzamknutie a audit zariadenia HP ProtectTools). Kliknite na tlačidlo **Yes** (Áno). Spustí sa služba na pozadí a následne sa bude spúšťať automaticky pri každom spustení systému.

POZNÁMKA: Pred zobrazením výzvy ohľadom služby na pozadí musí byť definovaný profil zariadenia.

Túto službu môžu spustiť alebo zastaviť aj správcovia:

1. Kliknutím na tlačidlo **Start** (Štart) a potom kliknutím na položku **Control Panel** (Ovládací panel).
2. Kliknite na položku **Administrative Tools** (Nástroje na správu) a potom kliknite na položku **Services** (Služby).
3. Vyhľadajte službu **HP ProtectTools Device Locking/Auditing** (Uzamknutie a audit zariadenia HP ProtectTools).

Zastavenie služby uzamknutia a auditu zariadenia nezastaví uzamykanie zariadenia. Uzamykanie zariadenia si vynucujú dve súčasti:

- Služba uzamykania a auditu zariadenia
- Ovládač DAMDrv.sys

Spustením služby sa spustí ovládač zariadenia, ale zastavením služby sa nezastaví ovládač.

Ak chcete zistiť, či je spustená služba na pozadí, otvorte okno s príkazovým riadkom a potom zadajte príkaz sc query flcdlock.

Ak chcete zistiť, či je spustený ovládač zariadenia, otvorte okno s príkazovým riadkom a potom zadajte príkaz sc query damdrv.

Konfigurácia tried zariadení

Správcovia a oprávnení používatelia môžu zobraziť a upraviť zoznamy používateľov a skupín, ktoré majú povolený alebo zakázaný prístup k triedam zariadení alebo konkrétnym zariadeniam.

POZNÁMKA: Ak chcete použiť toto zobrazenie na čítanie informácií o prístupe k zariadeniam, pre používateľa alebo skupinu sa vyžaduje udelený prístup „na čítanie“ v zobrazení **User Access Settings** (Nastavenia prístupu používateľov). Ak chcete použiť toto zobrazenie na úpravu informácií o prístupe k zariadeniam, pre používateľa alebo skupinu sa vyžaduje udelený prístup „na zmenu“ v zobrazení **User Access Settings** (Nastavenia prístupu používateľov).

Zobrazenie Device Class Configuration (Konfigurácia tried zariadení) má nasledujúce časti:

- **Device List** (Zoznam zariadení) – zobrazuje všetky triedy zariadení a zariadenia, ktoré sú nainštalované v systéme alebo ktoré mohli byť nainštalované v systéme predtým.
  - Ochrana sa zvyčajne použije pre určitú triedu zariadení. Vybratý používateľ alebo skupina bude mať prístup k ľubovoľnému zariadeniu v danej triede zariadení.
  - Ochrana sa môže použiť aj pre konkrétne zariadenia.
- **User List** (Zoznam používateľov) – zobrazuje všetkých používateľov a skupiny, ktoré majú povolený alebo zakázaný prístup k vybratej triede zariadení alebo ku konkrétnemu zariadeniu.
  - Položka zoznamu používateľov môžete byť vytvorená pre konkrétneho používateľa alebo pre skupinu, ktorej je daný používateľ členom.
  - Ak používateľ alebo skupina v zozname používateľov nie sú k dispozícii, nastavenie bolo zdedené z triedy zariadení v zozname zariadení alebo z priečinka Class (Trieda).
  - Niektoré triedy zariadení, ako napríklad DVD a CD-ROM, je možné ďalej ovládať povolením alebo zakázaním prístupu samostatne pre operácie čítania a zápisu.

    Tak ako v prípade iných zariadení a tried, aj prístupové práva na čítanie a zápis je možné zdediť. Napríklad prístup na čítanie môže byť zdedený z vyššej triedy, ale prístup na zápis môže byť špecificky zakázaný pre určitého používateľa alebo určitú skupinu.

    POZNÁMKA: Ak je začiarkavacie políčko Read (Čítanie) prázdne, potom položka riadenia prístupu nemá žiadny vplyv na prístup k zariadeniu na čítanie. Nepovoľuje ani nezakazuje prístup k zariadeniu na čítanie.

    Príklad 1 – ak má používateľ alebo skupina zakázaný prístup na zápis k zariadeniu alebo triede zariadení:

    Rovnaký používateľ, rovnaká skupina alebo člen rovnakej skupiny môže mať udelený prístup na zápis alebo prístup na čítanie aj zápis iba pre zariadenie pod týmto zariadením v hierarchii zariadení.

    Príklad 2 – ak má používateľ alebo skupina povolený prístup na zápis k zariadeniu alebo triede zariadení:

    Rovnaký používateľ, rovnaká skupina alebo člen rovnakej skupiny môže mať zakázaný prístup na zápis alebo prístup na čítanie aj zápis iba pre rovnaké zariadenie alebo zariadenie pod týmto zariadením v hierarchii zariadení.

    Príklad 3 – ak má používateľ alebo skupina povolený prístup na čítanie k zariadeniu alebo triede zariadení:

    Rovnaký používateľ, rovnaká skupina alebo člen rovnakej skupiny môže mať zakázaný prístup na čítanie alebo prístup na čítanie aj zápis iba pre rovnaké zariadenie alebo zariadenie pod týmto zariadením v hierarchii zariadení.

    Príklad 4 – ak má používateľ alebo skupina zakázaný prístup na čítanie k zariadeniu alebo triede zariadení:

    Rovnaký používateľ, rovnaká skupina alebo člen rovnakej skupiny môže mať udelený prístup na čítanie alebo prístup na čítanie aj zápis iba pre zariadenie pod týmto zariadením v hierarchii zariadení.

Príklad 5 – ak má používateľ alebo skupina povolený prístup na čítanie aj zápis k zariadeniu alebo triede zariadení:

Rovnaký používateľ, rovnaká skupina alebo člen rovnakej skupiny môže mať zakázaný prístup na zápis alebo prístup na čítanie aj zápis iba pre rovnaké zariadenie alebo zariadenie pod týmto zariadením v hierarchii zariadení.

Príklad 6 – ak má používateľ alebo skupina zakázaný prístup na čítanie aj zápis k zariadeniu alebo triede zariadení:

Rovnaký používateľ, rovnaká skupina alebo člen rovnakej skupiny môže mať udelený prístup na čítanie alebo prístup na čítanie aj zápis iba pre zariadenie pod týmto zariadením v hierarchii zariadení.

Zakázanie prístupu používateľovi alebo skupine

Ak chcete zabrániť používateľovi alebo skupine v prístupe k zariadeniu alebo triede zariadení, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **Device Class Configuration** (Konfigurácia tried zariadení).
2. V zozname zariadení kliknite na triedu zariadení, ktorú chcete konfigurovať.
   - Trieda zariadení
   - Všetky zariadenia
   - Jednotlivé zariadenie
3. Pod položkou **User/Groups** (Používateľ/skupiny) kliknite na používateľa alebo skupinu, ktorej chcete zakázať prístup.
4. Kliknite na položku **Deny** (Zakázať) vedľa používateľa alebo skupiny.
5. Kliknite na ikonu **Save** (Uložiť).

POZNÁMKA: Keď sú nastavenia zakázania a povolenia nastavené na rovnakej úrovni zariadení pre určitého používateľa, zakázanie prístupu má prednosť pred povolením prístupu.

Povolenie prístupu používateľovi alebo skupine

Ak chcete udeliť povolenie pre používateľa alebo skupinu na prístup k zariadeniu alebo triede zariadení, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **Device Class Configuration** (Konfigurácia tried zariadení).
2. V zozname zariadení kliknite na jednu z nasledujúcich možností:
   - Trieda zariadení
   - Všetky zariadenia
   - Jednotlivé zariadenie
3. Kliknite na tlačidlo **Add** (Pridať).

Otvorí sa dialógové okno **Select Users or Groups** (Výber používateľov alebo skupín).

4. Kliknite na položku **Advanced** (Rozšírené) a potom kliknutím na tlačidlo **Find Now** (Vyhľadať) vyhľadajte používateľov alebo skupiny, ktoré sa majú pridať.
5. Kliknite na používateľa alebo skupinu, ktorú chcete pridať do zoznamu dostupných používateľov a skupín, a potom kliknite na tlačidlo **OK**.
6. Znova kliknite na tlačidlo **OK**.
7. Kliknutím na položku **Allow** (Povoliť) môžete udeliť prístup pre tohto používateľa alebo túto skupinu.
8. Kliknite na ikonu **Save** (Uložiť).

Odstránenie prístupu pre používateľa alebo skupinu

Ak chcete odstrániť povolenie pre používateľa alebo skupinu na prístup k zariadeniu alebo triede zariadení, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **Device Class Configuration** (Konfigurácia tried zariadení).
2. V zozname zariadení kliknite na triedu zariadení, ktorú chcete konfigurovať.
   - Trieda zariadení
   - Všetky zariadenia
   - Jednotlivé zariadenie
3. V časti **User/Groups** (Používateľ/skupiny) kliknite na používateľa alebo skupinu, ktorú chcete odstrániť, a potom kliknite na položku **Remove** (Odstrániť).
4. Kliknite na ikonu **Save** (Uložiť).

Povolenie prístupu k triede zariadení pre jedného používateľa zo skupiny

Ak chcete povoliť používateľovi prístup k triede zariadení a zároveň zakázať prístup všetkým ostatným členom danej skupiny používateľov, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **Device Class Configuration** (Konfigurácia tried zariadení).
2. V zozname zariadení kliknite na triedu zariadení, ktorú chcete konfigurovať.
   - Trieda zariadení
   - Všetky zariadenia
   - Jednotlivé zariadenie
3. V časti **User/Groups** (Používateľ/skupiny) vyberte skupinu, ktorej chcete zakázať prístup, a potom kliknite na položku **Deny** (Zakázať).
4. Prejdite do priečinka pod požadovanou triedou a potom pridajte konkrétneho používateľa.

5. Kliknutím na položku **Allow** (Povoliť) udeľte tomuto používateľovi prístup.

6. Kliknite na ikonu **Save** (Uložiť).

Povolenie prístupu ku konkrétnemu zariadeniu pre jedného používateľa zo skupiny

Správcovia môžu udeliť prístup jednému používateľovi ku konkrétnemu zariadeniu a zároveň zakázať ostatným členom danej skupiny používateľov prístup ku všetkým zariadeniam v danej triede:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **Device Class Configuration** (Konfigurácia tried zariadení).

2. V zozname zariadení kliknite na triedu zariadení, ktorú chcete konfigurovať, a potom prejdite do priečinka pod ňou.

3. Kliknite na tlačidlo **Add** (Pridať). Otvorí sa dialógové okno **Select Users or Groups** (Výber používateľov alebo skupín).

4. Kliknite na položku **Advanced** (Rozšírené) a potom kliknutím na položku **Find Now** (Hľadať teraz) vyhľadajte skupinu používateľov, pre ktorú chcete zakázať prístup ku všetkým zariadeniam v danej triede.

5. Kliknite na skupinu a potom kliknite na tlačidlo **OK**.

6. Prejdite na konkrétne zariadenie v triede zariadení, pre ktorú má byť povolený prístup danému používateľovi.

7. Kliknite na tlačidlo **Add** (Pridať). Otvorí sa dialógové okno **Select Users or Groups** (Výber používateľov alebo skupín).

8. Kliknite na položku **Advanced** (Rozšírené) a potom kliknutím na tlačidlo **Find Now** (Vyhľadať) vyhľadajte používateľov alebo skupiny, ktoré sa majú pridať.

9. Kliknite na používateľa, ktorému chcete povoliť prístup, a potom kliknite na tlačidlo **OK**.

10. Kliknutím na položku **Allow** (Povoliť) udeľte tomuto používateľovi prístup.

11. Kliknite na ikonu **Save** (Uložiť).

Obnovenie nastavení konfigurácie

△ **UPOZORNENIE:** Obnovenie nastavení konfigurácie zruší všetky vykonané zmeny konfigurácie zariadení a vráti všetky nastavenia na hodnoty nastavené od výrobcu.

Ak chcete obnoviť nastavenia konfigurácie na hodnoty od výrobcu, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **Device Class Configuration** (Konfigurácia tried zariadení).

2. Kliknite na tlačidlo **Reset** (Obnoviť nastavenie).

3. Kliknutím na položku **Yes** (Áno) vykonajte potvrdenie.

4. Kliknite na ikonu **Save** (Uložiť).

Rozšírené úlohy

Ovládanie prístupu k nastaveniam konfigurácie

V zobrazení **User Access Settings** (Nastavenia prístupu používateľov) môžu správcovia definovať skupiny alebo používateľov, ktorí majú povolené používať stránky Simple Configuration (Jednoduchá konfigurácia) a Device Class Configuration (Konfigurácia tried zariadení).

POZNÁMKA: Používateľ alebo skupina musí mať „úplné práva správcu používateľov“, inak nebude môcť upraviť nastavenia v zobrazení User Access Settings (Nastavenia prístupu používateľov).

- Používateľ alebo skupina musí mať udelený prístup na „zobrazenie (iba čítanie) nastavení konfigurácie“ v zobrazení User Access Settings (Nastavenia prístupu používateľov), inak nebude môcť zobraziť informácie na stránke Simple Configuration (Jednoduchá konfigurácia) a Device Class Configuration (Konfigurácia tried zariadení).
- Používateľ alebo skupina musí mať udelený prístup na „zmenu nastavení konfigurácie“ v zobrazení User Access Settings (Nastavenia prístupu používateľov), inak nebude môcť zmeniť informácie na stránke Simple Configuration (Jednoduchá konfigurácia) a Device Class Configuration (Konfigurácia tried zariadení).

POZNÁMKA: Aj členovia skupiny Administrators (Správcovia) musia mať udelený prístup „na čítanie“, aby mohli zobraziť zobrazenia Simple Configuration (Jednoduchá konfigurácia) a Device Class Configuration (Konfigurácia tried zariadení), a musia mať udelený prístup „na zmenu“, aby mohli zmeniť údaje použitím zobrazení Simple Configuration (Jednoduchá konfigurácia) a Device Class Configuration (Konfigurácia tried zariadení).

POZNÁMKA: Po vyhodnotení úrovní prístupu pre všetkých používateľov a všetky skupiny a ak používateľ nemá vybraté povolenie alebo zakázanie konkrétnej úrovne prístupu, bude mať tento používateľ zakázaný prístup na danej úrovni.

Udelenie prístupu existujúcej skupine alebo používateľovi

Ak chcete udeliť povolenie pre existujúcu skupinu alebo používateľa na zobrazenie alebo zmenu nastavení konfigurácie, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **User Access Settings** (Nastavenia prístupu používateľov).
2. Kliknite na skupinu alebo používateľa, ktorému chcete povoliť prístup.
3. V časti **Permissions** (Povolenia) kliknite na položku **Allow** (Povoliť) pre každý typ povolenia, ktorý chcete udeliť vybratej skupine alebo vybratému používateľovi:

POZNÁMKA: Udelené povolenia sú kumulatívne. Napríklad používateľ, ktorý má udelené povolenie na „zmenu nastavení konfigurácie“, má automaticky udelené povolenie na „zobrazenie (iba čítanie) nastavení konfigurácie“. Používateľ, ktorý má udelené „úplné práva správcu používateľov“, má tiež udelené povolenia na „zmenu nastavení konfigurácie“ a „zobrazenie (iba čítanie) nastavení konfigurácie“.

- Úplné práva správcu používateľov
- Zmena nastavení konfigurácie
- Zobraziť (iba čítanie) nastavenia konfigurácie

4. Kliknite na ikonu **Save** (Uložiť).

Zakázanie prístupu existujúcej skupine alebo používateľovi

Ak chcete zakázať povolenie pre existujúcu skupinu alebo používateľa na zobrazenie alebo zmenu nastavení konfigurácie, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **User Access Settings** (Nastavenia prístupu používateľov).
2. Kliknite na skupinu alebo používateľa, ktorému chcete zakázať prístup.
3. V časti **Permissions** (Povolenia) kliknite na položku **Deny** (Zakázať) pre každý typ povolenia, ktorý chcete zakázať vybratej skupine alebo používateľovi:
   - Úplné práva správcu používateľov
   - Zmena nastavení konfigurácie
   - Zobraziť (iba čítanie) nastavenia konfigurácie
4. Kliknite na ikonu **Save** (Uložiť).

Pridanie novej skupiny alebo používateľa

Ak chcete udeliť povolenie pre novú skupinu alebo používateľa na zobrazenie alebo zmenu nastavení konfigurácie, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **User Access Settings** (Nastavenia prístupu používateľov).
2. Kliknite na tlačidlo **Add** (Pridať). Otvorí sa dialógové okno **Select Users or Groups** (Výber používateľov alebo skupín).
3. Kliknite na položku **Advanced** (Rozšírené) a potom kliknutím na tlačidlo **Find Now** (Vyhľadať) vyhľadajte používateľov alebo skupiny, ktoré sa majú pridať.
4. Kliknite na skupinu alebo používateľa, kliknite na tlačidlo **OK** a potom znova kliknite na tlačidlo **OK**.
5. Kliknutím na položku **Allow** (Povoliť) udeľte tomuto používateľovi prístup.
6. Kliknite na ikonu **Save** (Uložiť).

Odstránenie prístupu skupiny alebo používateľa

Ak chcete odstrániť povolenie pre skupinu alebo používateľa na zobrazenie alebo zmenu nastavení konfigurácie, postupujte podľa nasledujúcich krokov:

1. Na ľavej table okna **HP ProtectTools Administrative Console** (Spravovacia konzola nástroja HP ProtectTools) kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **User Access Settings** (Nastavenia prístupu používateľov).
2. Kliknite na skupinu alebo používateľa a potom kliknite na položku **Remove** (Odstrániť).
3. Kliknite na ikonu **Save** (Uložiť).

Súvisiaca dokumentácia

Aplikácia Device Access Manager pre nástroj HP ProtectTools je kompatibilná s podnikovým produktom HP ProtectTools Enterprise Device Access Manager. Pri práci s podnikovým produktom Device Access Manager pre nástroj HP ProtectTools umožňuje prístup iba na čítanie k jeho vlastným funkciám.

Ďalšie informácie o aplikácii Device Access Manager pre nástroj HP ProtectTools sú k dispozícii na webovej lokalite http://www.hp.com/hps/security/products.

11 LoJack Pro pre nástroj HP ProtectTools

Computrace LoJack Pro od spoločnosti Absolute Software (kupuje sa samostatne) rieši rastúci problém s odcudzenými alebo stratenými počítačmi.

Aktivácia tohto softvéru povoľuje agenta Computrace, ktorý zostáva aktívny v počítači aj po naformátovaní alebo výmene pevného disku.

LoJack Pro umožňuje vzdialené monitorovanie, spravovanie a sledovanie počítača. Ak sa počítač stratí alebo bude odcudzený, záchranný tím zo spoločnosti Absolute vám pomôže pri jeho záchrane.*

POZNÁMKA: *Táto funkcia závisí od geografického umiestnenia. Ďalšie podrobnosti nájdete v zmluve o predplatnom softvéru od spoločnosti Absolute Software.

12 Riešenie problémov

HP ProtectTools Security Manager

Krátky popis	Podrobnosti	Riešenie
Karty Smart Card a tokeny USB nie sú k dispozícii v aplikácii Security Manager, ak boli nainštalované až po inštalácii aplikácie Security Manager.	Ak chcete použiť karty Smart Card alebo tokeny USB v aplikácii Security Manager, podporný softvér (ovládače, poskytovatelia kľúčov PKCS#11 atď.) musí byť nainštalovaný pred nainštalovaním aplikácie Security Manager. Ak už máte nainštalovanú aplikáciu Security Manager, po inštalácii podporného softvéru pre karty Smart Card alebo tokeny vykonajte nasledujúce kroky:	Prihláste sa do nástroja Password Manager. V nástroji HP ProtectTools Security Manager kliknite na položku **Password Manager**, kliknite na položku **Credentials** (Poverenia) a potom kliknite na položku **Smart Card** (Karta Smart Card) Ak sa zobrazí výzva na reštartovanie počítača, reštartujte ho.
Niektoré webové stránky aplikácií vytvárajú chyby, ktoré neumožňujú používateľovi vykonať alebo dokončiť úlohy.	Niektoré webové aplikácie prestanú fungovať a hlásia chyby pre prejavy nefunkčnosti funkcie Single Sign On (Jediné prihlásenie) Napríklad znak **!** v žltom trojuholníku v programe Internet Explorer indikuje výskyt chyby.	Funkcia Security Manager Single Sign On (Jediné prihlásenie do nástroja Security Manager) nepodporuje všetky webové rozhrania softvéru. Vypnite podporu funkcie jediného prihlásenia pre konkrétnu webovú stránku vypnutím podpory tejto funkcie. Pozrite si kompletnú dokumentáciu k funkcii jediného prihlásenia, ktorá je k dispozícii v súboroch pomocníka softvéru Security Manager. Ak nie je možné vypnúť funkciu Single Sign On (Jediné prihlásenie) pre danú aplikáciu, zavolajte technickú podporu HP a požiadajte o podporu tretej úrovne prostredníctvom vášho kontaktu na servis spoločnosti HP.
Počas prihlasovania možnosť **Browse for Virtual Token** (Vyhľadať virtuálny kľúč) nie je zobrazená.	Používateľ nemôže presunúť umiestnenie zaregistrovaného virtuálneho tokenu v nástroji Password Manager, pretože možnosť prehľadávania bola odstránená z dôvodu zníženia bezpečnostných rizík.	Možnosť na vyhľadanie bola odstránená, pretože umožňovala neoprávneným používateľom odstrániť a premenovať súbory a prevziať kontrolu nad systémom Windows.
Správcovia domény nemôžu zmeniť heslo systému Windows ani s overením.	K tomu dochádza, keď sa správca domény prihlási do domény a zaregistruje identitu domény v nástroji Password Manager použitím konta s právami správcu v danej doméne a lokálnom počítači. Keď sa správca domény pokúsi zmeniť heslo systému Windows z nástroja Password Manager, správcovi sa zobrazí chyba spôsobená	Softvér Password Manager nemôže zmeniť heslo konta používateľa domény prostredníctvom možnosti **Change Windows Password** (Zmeniť heslo systému Windows). Softvér Security Manager môže zmeniť iba heslá pre kontá lokálneho počítača. Používateľ domény môže zmeniť svoje heslo prostredníctvom položky **Change Password** (Zmeniť heslo) v časti **Windows Security** (Zabezpečenie systému Windows), ale keďže používateľ domény nemá fyzické

Krátky popis	Podrobnosti	Riešenie
	zlyhaním prihlásenia: **Obmedzenie používateľského konta**.	konto na lokálnom počítači, softvér Password Manager môže zmeniť iba heslo používané na prihlásenie.
Nástroj Password Manager má problémy s kompatibilitou s heslom GINA softvéru Corel WordPerfect 12.	Ak sa používateľ prihlási do nástroja Password Manager, vytvorí dokument v programe WordPerfect a uloží ho chránený heslom, nástroj Password Manager nemôže zistiť ani rozpoznať, či už manuálne alebo automaticky, heslo GINA.	Spoločnosť HP pracuje na riešení pre budúce zlepšenia produktu.
Nástroj Password Manager nerozpozná tlačidlo **Connect** (Pripojiť) na obrazovke.	Ak sú poverenia Single Sign On (Jediné prihlásenie) pre funkciu Remote Desktop Connection (RDP) nastavené na hodnotu **Connect** (Pripojiť), pri spustenej funkcii Single Sign On sa vždy zadá položka **Save As** (Uložiť ako) namiesto **Connect**.	Spoločnosť HP pracuje na riešení pre budúce zlepšenia produktu.
Používateľ sa nedokáže prihlásiť do nástroja Password Manager po prechode z režimu spánku do režimu dlhodobého spánku iba v systéme Windows XP Service Pack 1.	Po povolení prechodu systému do režimu dlhodobého spánku a režimu spánku sa správca alebo používateľ nedokáže prihlásiť do nástroja Password Manager a prihlasovacia obrazovka systému Windows zostane zobrazená bez ohľadu na to, ktoré prihlasovacie poverenie (heslo, odtlačok prsta alebo karta Java Card) zvolíte.	Aktualizujte systém Windows na Service Pack 2 prostredníctvom služby aktualizácie systému Windows. Ďalšie informácie o príčine tohto problému nájdete v článku databázy znalostí Microsoft Knowledge Base číslo 813301 na adrese http://www.microsoft.com. Ak sa chce používateľ prihlásiť, musí vybrať nástroj Password Manager a prihlásiť sa v ňom. Po prihlásení v nástroji Password Manager sa používateľovi zobrazí výzva na prihlásenie do systému Windows (od používateľa sa môže vyžadovať výber možnosti prihlásenia do systému Windows) na dokončenie procesu prihlásenia. Ak sa používateľ najprv prihlási do systému Windows, potom sa musí manuálne prihlásiť do nástroja Password Manager.
Bezpečnostný proces **Restore Identity** (Obnoviť identitu) stráca spojenie s virtuálnym kľúčom.	Keď používateľ obnoví identitu, nástroj Password Manager môže stratiť priradenie s umiestnením virtuálneho tokenu na prihlasovacej obrazovke. Aj keď nástroj Password Manager má zaregistrovaný virtuálny token, používateľ musí znova zaregistrovať token na obnovenie priradenia.	Toto správanie je aktuálne v poriadku. Pri odinštalovaní nástroja Security Manager bez zachovania identít sa systémová (serverová) časť tokenu zničí, takže token sa nebude dať viac použiť na prihlásenie, a to ani v prípade, ak sa klientska časť tokenu obnoví prostredníctvom obnovenia identity. Spoločnosť HP skúma dlhodobé možnosti riešenia.

Aplikácia Device Access Manager pre nástroj HP ProtectTools

Používateľom bol zakázaný prístup k zariadeniami v aplikácii Device Access Manager (Správca prístupu k zariadeniam), ale zariadenia sú stále dostupné.

- **Vysvetlenie** – na zakázanie prístupu používateľov k zariadeniam boli použité funkcie Simple Configuration (Jednoduchá konfigurácia) alebo Device Class Configuration (Konfigurácia tried zariadení) v súčasti Device Access Manager (Správca prístupu k zariadeniam). Napriek zakázanému prístupu môžu používatelia stále pristupovať k zariadeniam.
- **Riešenie:**
  - Overte, či je spustená služba HP ProtectTools Device Locking (Uzamykanie zariadenia HP ProtectTools).
  - Ako používateľ s právami správcu kliknite na položku **Control Panel** (Ovládací panel) a potom kliknite na položku **System and Maintenance** (Systém a údržba). V okne Administrative Tools (Nástroje na správu) kliknite na položku **Services** (Služby) a vyhľadajte službu **HP ProtectTools Device Locking/Auditing** (Uzamknutie a audit zariadenia HP ProtectTools). Dbajte na to, aby bola služba spustená a aby typ spustenia bol **Automatic** (Automaticky).

Používateľ má neočakávaný prístup k zariadeniu alebo používateľ má neočakávane zakázaný prístup k zariadeniu.

- **Vysvetlenie** – na zakázanie prístupu používateľov k niektorým zariadeniam a povolenie prístupu používateľov k iným zariadeniam bola použitá aplikácia Device Access Manager (Správca prístupu k zariadeniam). Keď používateľ používa systém, môže pristupovať k zariadeniam, o ktorých si myslí, že aplikácia Device Access Manager (Správca prístupu k zariadeniam) zakázala prístup, a má zakázaný prístup k zariadeniam, o ktorých si myslí, že aplikácia Device Access Manager (Správca prístupu k zariadeniam) povolila prístup.
- **Riešenie:**
  - Nastavenia používateľských zariadení môžete skontrolovať pomocou stránky Device Class Configuration (Konfigurácia tried zariadení) v aplikácii Device Access Manager (Správca prístupu k zariadeniam).
  - Kliknite na položku **Security Manager** (Správca zabezpečenia), kliknite na položku **Device Access Manager** (Správca prístupu k zariadeniam) a potom kliknite na položku **Device Class Configuration** (Konfigurácia tried zariadení). Rozbaľte úrovne v strome Device Class (Trieda zariadení) a skontrolujte nastavenia týkajúce sa používateľa. Skontrolujte všetky povolenia typu Deny (Zakázať), ktoré môžu byť nastavené pre používateľa alebo ľubovoľnú skupinu používateľov systému Windows, ktorej môže byť členom, napríklad Users (Používatelia), Administrators (Správcovia).

Povolenie alebo zakázanie – čo má prednosť?

- **Vysvetlenie** – v zobrazení Device Class Configuration (Konfigurácia tried zariadení) bola nastavená nasledujúca konfigurácia:
  - Jednej skupine systému Windows (napríklad BUILTIN\Administrators) bolo udelené povolenie typu Allow (Povoliť) a inej skupine systému Windows (napríklad BUILTIN\Users) na rovnakej úrovni v hierarchii tried zariadení (napríklad jednotky DVD/CD-ROM) bolo udelené povolenie typu Deny (Odmietnuť).
  - Ak je používateľ členom oboch týchto skupín (napríklad správca), čo má prednosť?
- **Riešenie:**
  - Používateľ má zakázaný prístup k zariadeniu. Zakázanie má prednosť pred povolením.
  - Prístup je zakázaný z dôvodu spôsobu, akým systém Windows nastavuje efektívne povolenie pre zariadenie. Jedna skupina má zakázaný prístup a jedna skupina má povolený prístup, ale používateľ je členom oboch skupín. Používateľ má zakázaný prístup, pretože zakázanie prístupu má prednosť pred povolením prístupu.
  - Jedným z riešení je zakázanie prístupu pre skupinu Users (Používatelia) na úrovni jednotiek DVD/CD-ROM a povolenie prístupu pre skupinu Administrators (Správcovia) na úrovni pod jednotkami DVD/CD-ROM.
  - Alternatívnym riešením je vytvorenie určitej skupiny používateľov systému Windows a povolenie prístupu jednej skupine k jednotkám DVD/CD a zakázanie prístupu k jednotkám DVD/CD druhej skupine. Konkrétni používatelia potom budú pridaní do príslušnej skupiny.

Zobrazenie Simple Configuration (Jednoduchá konfigurácia) bolo použité na definovanie politiky riadenia prístupu k zariadeniam, ale používatelia s právami správcu nemajú prístup k zariadeniam.

- **Vysvetlenie** – zobrazenie Simple Configuration (Jednoduchá konfigurácia) zakazuje prístup pre skupiny Users (Používatelia) a Guests (Hostia) a povoľuje prístup pre skupinu Device Administrators (Správcovia zariadení).
- **Riešenie:** Pridajte používateľa s právami správcu do skupiny Device Administrators (Správcovia zariadení).

Rôzne

Ovplyvnený softvér – krátky popis	Podrobnosti	Riešenie
Security Manager – prijaté varovanie: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (Bezpečnostná aplikácia sa nemôže nainštalovať, až kým sa nenainštaluje program HP Protect Tools Security Manager).	Všetky bezpečnostné aplikácie, ako napríklad zabezpečenie kartami Java Card a biometrickými údajmi, sú rozšíriteľné doplnky pre rozhranie nástroja Security Manager. Nástroj Security Manager musí byť nainštalovaný pred načítaním bezpečnostného doplnku schváleného spoločnosťou HP.	Program Security Manager sa musí nainštalovať pred inštaláciou bezpečnostného doplnku.
HP ProtectTools Security Manager – pri ukončovaní rozhrania programu Security Manager sa občasne vyskytne chyba.	Občasne (1 z 12 prípadov) sa vyskytne chyba spôsobená použitím tlačidla zatvoriť v pravom hornom rohu obrazovky pri ukončovaní programu Security Manager prv, než sa dokončí zavedenie všetkých doplnkových aplikácií.	Táto chyba súvisí s časovou závislosťou na dobe zavedenia doplnkových služieb pri ukončovaní a reštartovaní programu Security Manager. Keďže súbor PTHOST.exe program typu shell zastrešujúci ostatné aplikácie (doplnky), závisí na dostupnosti doplnkov na dokončenie času zavedenia (služieb). Ukončenie programu shell predtým, než doplnky majú čas na zavedenie je základnou príčinou. Umožnite programu Security Manager dokončenie služieb zavedením hlásenia (zobrazuje sa v hornej časti okna programu Security Manager) a všetkých doplnkov zobrazených v ľavom stĺpci. Aby nedošlo k zlyhaniu, poskytnite dostatok času na zavedenie týchto doplnkov.
HP ProtectTools – neobmedzený prístup alebo nekontrolované práva správcu predstavujú bezpečnostné riziko.	Neobmedzený prístup ku klientskemu počítaču spôsobuje rôzne riziká, vrátane týchto: • Vymazanie jednotky PSD • Škodlivá modifikácia nastavení používateľa • Vypnutie bezpečnostných pravidiel a funkcií	Správcom sa odporúča dodržiavať „najlepšie postupy“ pri obmedzovaní oprávnení koncových používateľov a obmedzovaní prístupu používateľov. Neoprávnení používatelia by nemali mať pridelené správcovské oprávnenia.

Slovník

aktivácia Úloha, ktorá musí byť dokončená pred dostupnosťou ľubovoľných funkcií aplikácie Drive Encryption. Aplikácia Drive Encryption sa aktivuje použitím sprievodcu inštaláciou nástroja HP ProtectTools. Aplikáciu Drive Encryption môže aktivovať iba správca. Proces aktivácie zahŕňa aktiváciu softvéru, šifrovanie jednotky, vytvorenie používateľského konta a vytvorenie počiatočného kľúča na šifrovanie zálohy na vymeniteľnom pamäťovom zariadení.

aktívum Dátový komponent obsahujúci osobné údaje alebo súbory, historické a webové údaje a podobne, ktorý je umiestnený na pevnom disku.

archív núdzovej obnovy Ukladací priestor umožňujúci opätovné šifrovanie základných používateľských kľúčov z jedného vlastníckeho kľúča na iný.

ATM Automatic Technology Manager, ktorý umožňuje správcom siete spravovať systémy vzdialene na úrovni systému BIOS.

automatické skartovanie Naplánované skartovanie, ktoré používateľ nastavuje v aplikácii File Sanitizer.

biometrické údaje Kategória overovania poverení, ktoré používajú fyzické prvky, napríklad odtlačky prstov, na identifikáciu používateľa.

certifikačná autorita Služba, ktorá vydáva certifikáty na používanie infraštruktúry verejných kľúčov.

certifikát modulu Privacy Manager Digitálny certifikát, ktorý vyžaduje overovanie pri každom jeho použití pre šifrovacie operácie, ako je napríklad podpísanie a šifrovanie e-mailových správ a dokumentov balíka programov Microsoft Office.

cyklus skartovania Počet vykonaní skartovacieho algoritmu pre každé aktívum. Čím zvolíte vyšší počet skartovacích cyklov, tým je počítač bezpečnejší.

dešifrovanie Postup v kryptografii, ktorý konvertuje zašifrované údaje na obyčajný text.

digitálny certifikát Elektronické poverenia, ktoré potvrdzujú identitu jednotlivca alebo spoločnosti previazaním identity vlastníka digitálneho certifikátu na spárovanie elektronických kľúčov, ktoré sa používajú na podpisovanie digitálnych údajov.

digitálny podpis Údaje odosielané so súborom, ktoré overujú odosielateľa daného materiálu a to, že súbor nebol upravený od jeho podpísania.

doména Skupina počítačov, ktoré sú súčasťou siete a zdieľajú spoločnú databázu adresárov. Domény sú jedinečne pomenované a každá z nich má nastavené spoločné pravidlá a postupy.

dôkladné vymazanie voľného miesta Bezpečné prepísanie odstráneného aktíva náhodnými údajmi na zničenie jeho obsahu.

dôveryhodná komunikáciu prostredníctvom okamžitých správ Komunikačná relácia, počas ktorej sa odosielajú dôveryhodné správy od dôveryhodného odosielateľa dôveryhodnému kontaktu.

dôveryhodná správa Komunikačná relácia, počas ktorej sa odosielajú dôveryhodné správy od dôveryhodného odosielateľa dôveryhodnému kontaktu.

dôveryhodný kontakt Osoba, ktorá prijala pozvánku od dôveryhodného kontaktu.

dôveryhodný odosielateľ Dôveryhodný kontakt, ktorý odosiela podpísané alebo zašifrované e-maily a dokumenty balíka programov Microsoft Office.

Drive Encryption Chráni údaje prostredníctvom šifrovania pevných diskov, takže údaje si nemôžu prečítať neoprávnené osoby.

DriveLock Bezpečnostná funkcia, ktorá prepája pevný disk k používateľovi a vyžaduje od používateľa správne zadanie hesla funkcie DriveLock pri spustení počítača.

Encryption File System (EFS) Systém, ktorý zašifruje všetky súbory a podpriečinky v rámci vybraného priečinku.

heslo na zrušenie Heslo, ktoré sa vytvorí, keď používateľ žiada o digitálny certifikát. Toto heslo sa vyžaduje, keď používateľ chce zrušiť svoj digitálny certifikát. To zaručuje, že certifikát môže zrušiť iba príslušný používateľ.

HP SpareKey Záložná kópia kľúča modulu Drive Encryption.

identifikačná karta Miniaplikácia pre bočný panel systému Windows, ktorá slúži na vizuálnu identifikáciu pracovnej plochy menom používateľa a zvoleným obrázkom. Kliknutím na identifikačnú kartu otvorte Spravovaciu konzolu nástroja HP ProtectTools.

identita V programe HP ProtectTools Security Manager je to skupina poverení a nastavení, s ktorou sa narába podobne ako s kontom alebo profilom konkrétneho používateľa.

Java Card Vymeniteľná karta, ktoré sa vkladá do počítača. Obsahuje identifikačné údaje potrebné na prihlásenie. Prihlásenie pomocou karty Java Card na prihlasovacej obrazovke modulu Drive Encryption vyžaduje, aby ste vložili kartu Java Card a zadali meno používateľa a PIN karty Java Card.

jediné prihlásenie Funkcia, ktorá ukladá overovacie údaje a umožňuje použiť softvér Security Manager na prístup na Internet a k aplikáciám systému Windows, ktoré vyžadujú overovanie heslom.

jednoduché odstránenie Vymazanie odkazu systému Windows na aktívum. Obsah aktíva zostane na pevnom disku, až kým nebude prepísaný náhodnými údajmi prostredníctvom dôkladného vymazania voľného miesta.

karta Smart Card Malé zariadenie (hardvér), ktoré má veľkosť a tvar kreditnej karty, ktoré obsahuje identifikačné údaje o vlastníkovi. Používa sa na overovanie vlastníka počítača.

klávesová skratka Kombinácia konkrétnych klávesov, ktorých stlačenie aktivuje automatické skartovanie – napríklad ctrl+alt+s.

konzola Centrálne umiestnenie, v ktorom môžete pristupovať k funkciám a nastaveniam tohto programu a spravovať ich.

kryptografia Technológia šifrovania a dešifrovania údajov, ktoré môžu byť dekódované len určitými osobami.

Live Messenger History Viewer Komponent modulu Privacy Manager Chat, ktorý umožňuje vyhľadať a zobraziť históriu šifrovaných diskusných relácií.

manuálne skartovanie Okamžité skartovanie aktíva alebo vybratých aktív, ktoré obchádza automatický plán skartovania.

metóda bezpečného prihlásenia Spôsob používaný na prihlásenie na počítač.

migrácia Úloha, ktorá umožňuje spravovanie, obnovenie a prenos certifikátov modulu Privacy Manager a dôveryhodných kontaktov.

obnovenie Proces, ktorý kopíruje programové informácie z predtým uloženého záložného súboru do tohto programu.

odhalenie Úloha, ktorá umožňuje používateľovi dešifrovať najmenej jednu z histórie diskusných relácií, so zobrazením zobrazovaných mien kontaktov vo formáte obyčajného textu a sprístupnením relácie na zobrazenie.

odporúčaný signatár Používateľ, ktorý bol určený vlastníkom dokumentu programu Microsoft Word alebo Microsoft Excel na pridanie riadku pre podpis do dokumentu.

odtlačok prsta Digitálna extrakcia obrázka odtlačku prsta. Nástroja Security Manager nikdy neuloží skutočný obrázok odtlačku prsta.

oprávnený používateľ Používateľ, ktorý má udelené povolenie v zobrazení User Access Settings (Nastavenia prístupu používateľov) na zobrazenie alebo úpravu nastavení konfigurácie v zobrazení Simple Configuration (Jednoduchá konfigurácia) alebo Device Class Configuration (Konfigurácia tried zariadení).

overovanie Proces overovania, či je používateľ oprávnený vykonať danú úlohu, ako napríklad prístup k počítaču, úpravu nastavení konkrétneho programu alebo zobrazenie zabezpečených údajov.

overovanie pri zapnutí počítača Bezpečnostný prvok, ktorý vyžaduje použitie určitej formy overovania pri zapnutí počítača, napríklad kartu Java, bezpečnostný čip alebo heslo.

pečať pre dôveryhodné kontakty Úloha, ktorá pridá digitálny podpis, zašifruje e-mail a odošle ho po overení identity používateľa použitím zvoleného spôsobu bezpečného prihlásenia.

PKI Štandard Public Key Infrastructure, ktorý definuje rozhranie na tvorbu, používanie a riadenie certifikátov a kryptografických kľúčov.

politika riadenia prístupu k zariadeniam Zoznam zariadení, ku ktorým má používateľ povolený alebo zakázaný prístup.

poskytovateľ šifrovacích služieb (CSP) Poskytovateľ alebo knižnica kryptografických algoritmov, ktorá sa môže použiť v dobre definovanom rozhraní na vykonanie určitých kryptografických funkcií.

používateľ Každý, kto je zaregistrovaný v module Drive Encryption. Používatelia bez práv správcu majú obmedzené práva v module Drive Encryption. Môžu sa iba zaregistrovať (so schválením správcu) a prihlásiť.

používateľské konto systému Windows Profil pre individuálne overené prihlásenie do siete alebo do konkrétneho počítača.

poverenia Metóda, pomocou ktorej používateľ v procese overovania dokazuje svoje práva na určitú úlohu.

pozvánka od dôveryhodného kontaktu E-mail odoslaný osobe so žiadosťou, aby sa stala dôveryhodným kontaktom.

prihlásenie Objekt v rámci nástroja Security Manager, obsahujúci meno používateľa a heslo (prípadne aj ďalšie vybraté informácie), ktoré môžete použiť na prihlásenie na webové lokality alebo do iných programov.

prihlasovacia obrazovka modulu Drive Encryption Prihlasovacia obrazovka, ktorá sa zobrazí pred spustením systému Windows. Používatelia musia zadať svoje meno a heslo používateľa systému Windows alebo PIN karty Java Card. Vo väčšine prípadov zadanie správnych údajov na prihlasovacej obrazovke modulu Drive Encryption umožňuje prístup priamo do systému Windows bez nutnosti opätovného prihlasovania sa na prihlasovacej obrazovke systému Windows.

príjemca z dôveryhodných kontaktov Osoba, ktorá prijme pozvánku stať sa dôveryhodným kontaktom.

profil skartovania Definovaný spôsob vymazania a zoznam aktív.

PSD Osobná bezpečná jednotka, ktorá poskytuje chránený ukladací priestor pre citlivé informácie.

relácia histórie konverzácií Zašifrovaný súbor, ktorý obsahuje záznam oboch strán konverzácie v diskusnej relácii.

reštartovanie Proces reštartovania počítača.

režim zariadenia SATA Režim prenosu údajov medzi počítačom a veľkokapacitnými pamäťovými zariadeniami, ako sú napríklad pevné disky a optické jednotky.

riadok pre podpis Zástupný znak pre vizuálne zobrazenie digitálneho podpisu. Pri podpísaní dokumentu sa zobrazí meno signatára a spôsob overenia. Dátum podpísania a meno signatára môžu byť tiež zahrnuté.

sieťové konto Konto používateľa alebo správcu systému Windows buď na lokálnom počítači, v pracovnej skupine alebo doméne.

skartovanie Vykonanie algoritmu, ktorý prepíše údaje obsiahnuté v aktíve náhodnými údajmi.

skupina Skupina používateľov, ktorí majú rovnakú úroveň prístupu alebo zakázaného prístupu k triede zariadení alebo konkrétnemu zariadeniu.

služba na pozadí Služba HP ProtectTools Device Locking/Auditing (Uzamykanie a audit zariadenia HP ProtectTools) spustená na pozadí, ktorá musí byť spustená pre politiky riadenia prístupu k zariadeniam, ktoré sa majú použiť. Dá sa zobraziť z aplikácie Services (Služby) v rámci možnosti Administrative Tools (Nástroje na správu) v Ovládacom paneli. Ak nie je spustená, nástroj HP ProtectTools Security Manager sa ju pokúsi spustiť pri použití politík riadenia prístupu k zariadeniam.

správca *Pozrite* „správca systému Windows“.

správca systému Windows Používateľ s úplnými právami na úpravu povolení a správu ostatných používateľov.

šifrovanie Postup, napríklad použitie algoritmu, využívaného v kryptografii na konverziu obyčajného textu do kódovaného textu, ktorý zabraňuje jeho čitateľnosti nepovolenými osobami. Je veľa spôsobov šifrovania dát. Sú základom bezpečnosti siete. K bežným metódam patrí štandard dátového šifrovania (Data Encryption Standard) a šifrovanie pomocou verejných kľučov.

tabuľa Centrálne umiestnenie, v ktorom môžete pristupovať k funkciám a nastaveniam tohto programu a spravovať ich.

tlačidlo Send Securely (Odoslať bezpečne) Softvérové tlačidlo, ktoré sa zobrazí na paneli s nástrojmi e-mailových správ programu Microsoft Outlook. Kliknutím na toto tlačidlo môžete podpísať alebo zašifrovať e-mailovú správu programu Microsoft Outlook.

tlačidlo Sign and Encrypt (Podpísať a zašifrovať) Softvérové tlačidlo, ktoré sa zobrazí na paneli s nástrojmi aplikácií balíka programov Microsoft Office. Kliknutím na toto tlačidlo môžete podpísať, zašifrovať alebo odstrániť šifrovanie v dokumente balíka programov Microsoft Office.

token Pozrite si heslo „spôsob bezpečného prihlásenia“.

token USB Bezpečnostné zariadenie, ktoré ukladá identifikačné údaje používateľa. Používa sa, podobne ako karta Java Card alebo biometrická čítačka, na overovanie vlastníka počítača.

trieda zariadení Všetky zariadenia konkrétneho typu, ako napríklad jednotky.

TXT Trusted Execution Technology (Technológia dôveryhodného spustenia).

virtuálny token Bezpečnostná funkcia, ktorá pracuje veľmi podobne ako karta Java Card a čítačka kariet. Token je uložený buď na pevnom disku počítača, alebo v databáze Registry systému Windows. Ak sa prihlásite pomocou virtuálneho tokenu, budete musieť zadať používateľský kód PIN na dokončenie overovania.

zabezpečenie prihlasovania do systému Windows Chráni kontá systému Windows vyžadovaním používania špecifických prístupových poverení.

zálohovanie Používanie funkcie zálohovania na uloženie kópie dôležitých programových informácií do umiestnenia mimo programu. Potom sa dá použiť na neskoršie obnovenie informácií do rovnakého alebo iného počítača.

zoznam dôveryhodných kontaktov Výpis dôveryhodných kontaktov.

Register