HP Client Security

Úvodné informácie

Prvé vydanie: august 2013

Katalógové číslo dokumentu: 735339-231

Obsah

1 Úvod do softvéru HP Client Security Manager

HP Client Security vám umožňuje chrániť údaje, zariadenie a identitu, čím zvyšuje zabezpečenie vášho počítača.

Softvérové moduly, ktoré sú pre váš počítač k dispozícii, sa môžu líšiť v závislosti od vášho modelu.

Softvérové moduly aplikácie HP Client Security môžu byť predinštalované, vopred načítané alebo k dispozícii na prevzatie z webovej stránky spoločnosti HP. Ďalšie informácie nájdete v časti http://www.hp.com.

POZNÁMKA: Pokyny uvedené v tejto príručke sú napísané s predpokladom, že už máte nainštalované použiteľné softvérové moduly aplikácie HP Client Security.

Funkcie aplikácie HP Client Security

V nasledujúcej tabuľke sú uvedené hlavné funkcie modulov aplikácie HP Client Security.

Modul	Hlavné funkcie
softvér HP Client Security Manager	Administrátori môžu vykonávať tieto funkcie: • Ochrana počítača pred spustením systému Windows® • Ochrana konta systému Windows pomocou dôkladného overovania • Spravovanie prihlasovacích údajov a hesiel pre webové stránky a aplikácie • Ľahká zmena hesla do operačného systému Windows • Používanie odtlačkov prstov pre špeciálne zabezpečenie a pohodlie • Nastavenie overovania kartou Smart, bezkontaktnou kartou alebo kartou Proximity • Používanie telefónu s funkciou Bluetooth ako spôsobu identifikácie • Nastavenie kódu PIN v rámci rozšírenia volieb overovania • Konfigurácia zásad prihlasovania a relácie • Zálohovanie a obnovenie programových údajov • Pridávanie ďalších aplikácií, ako sú HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager a HP Computrace Bežní používatelia môžu vykonávať tieto funkcie: • Prezeranie nastavení Stav šifrovania a Správcu prístupu k zariadeniam • Aktivovanie funkcie Computrace • Konfigurácia Predvolieb a možností zálohovania a obnovenia

Modul	Hlavné funkcie
Správca hesiel	Bežní používatelia môžu vykonávať tieto funkcie: • Usporiadanie a nastavenie používateľských mien a hesiel. • Vytváranie silnejších hesiel pre vylepšené zabezpečenia konta pre e-mailové a webové kontá. Správca hesiel automaticky vypĺňa a odosiela údaje. • Zjednodušenie procesu prihlasovania funkciou jedno prihlásenie, ktorá si dokáže automaticky zapamätať a použiť používateľské poverenia. • Označenie konta ako prezradeného, takže dostanete upozornenie k ďalším kontám s podobnými povereniami. • Import prihlasovacích údajov z podporovaného prehľadávača.
HP Drive Encryption (len vybrané modely)	• Poskytuje kompletné šifrovanie všetkých jednotiek na pevnom disku. • Vynútenie overovania pri spustení za účelom dešifrovania a prístupu k údajom. • Ponúka možnosť aktivovať samošifrovacie jednotky (len vybrané modely).
HP Device Access Manager	• Umožňuje správcom IT ovládať prístup k zariadeniam na základe používateľských profilov. • Zabraňuje nepovoleným používateľom odstraňovať údaje pomocou externého pamäťového média a chráni pred vniknutím vírusov do systému z externého média. • Umožňuje administrátorom zakázať konkrétnym osobám alebo skupinám používateľov prístup ku komunikačným zariadeniam.
HP Trust Circles	• Poskytuje zabezpečenie súborov a dokumentov. • Šifruje súbory umiestnené v používateľom určených priečinkoch a chráni ich v rámci dôveryhodného okruhu. • Umožňuje používanie a zdieľanie súborov len medzi členmi dôveryhodného okruhu.
Theft Recovery (Computrace, kupuje sa samostatne)	• Pri aktivácii sa vyžaduje osobitný nákup predplatného pre sledovanie. • Poskytuje bezpečné sledovanie majetku. • Monitoruje činnosť používateľa, ako aj hardvérové a softvérové zmeny. • Zostáva aktívne, aj keď sa pevný disk preformátuje alebo vymení.

Popis produktu HP Client Security a príklady najčastejšieho používania

Väčšina produktov aplikácie HP Client Security obsahuje používateľské overovanie (zvyčajne heslo) a administratívnu zálohu, vďaka ktorej je možné získať prístup v prípade straty hesiel, ich nedostupnosti alebo zabudnutia, prípadne ak kedykoľvek firemné zabezpečenie vyžaduje prístup.

POZNÁMKA: Niektoré produkty aplikácie HP Client Security sú určené na obmedzenie prístupu k údajom. Údaje by mali byť zašifrované, keď je to dôležité, aby ich používateľ radšej stratil než by mali byť prezradené. Odporúča sa, aby boli všetky údaje zálohované na bezpečnom mieste.

Správca hesiel

Správca hesiel ukladá mená používateľov a heslá a je možné ho používať na nasledovné:

- Ukladanie prihlasovacích mien a hesiel pre prístup na internet a do e-mailu.
- Automatické prihlasovanie používateľa na webovú stránku alebo do e-mailu.
- Spravovanie a organizovanie overení.
- Voľba webového alebo sieťového aktíva a priamy prístup cez prepojenie.
- Prezeranie mien a hesiel v prípade potreby.
- Označenie konta ako prezradeného, takže dostanete upozornenie k ďalším kontám s podobnými povereniami.
- Import prihlasovacích údajov z podporovaného prehľadávača.

Príklad 1: Nákupca u veľkého výrobcu robí väčšinu firemných transakcií cez internet. Navštevuje tiež často viaceré obľúbené webové stránky, ktoré vyžadujú prihlasovacie údaje. Je si veľmi dobre vedomý bezpečnosti, takže nepoužíva na všetkých kontách rovnaké heslo. Nákupca sa rozhodol používať funkciu Správca hesiel pre webové prepojenia s rozličnými menami používateľa a heslami. Keď príde na webovú stránku s prihlásením, Správca hesiel automaticky uvedie poverenia. Ak chcete prezerať mená používateľa a heslá, Správca hesiel sa dá nakonfigurovať na ich zobrazenie.

Správca hesiel sa tiež dá využiť na spravovanie a organizovanie overení. Tento nástroj umožňuje používateľovi vybrať webové alebo sieťové aktívum a priamo otvoriť prepojenie. Používateľ tiež môže v prípade potreby prezerať mená používateľa a heslá.

Príklad 2: Tvrdo pracujúci zamestnanec bol povýšený a teraz spravuje celé účtovné oddelenie. Tím sa musí prihlasovať na veľký počet klientskych webových kont, z ktorých každé používa rozličné prihlasovacie údaje. Tieto prihlasovacie údaje je potrebné zdieľať s ostatnými pracovníkmi, takže ich dôvernosť je problém. Zamestnanec sa rozhodol organizovať všetky webové prepojenia, firemné mená používateľov a heslá vo funkcii Správca hesiel. Po dokončení zamestnanec nasadí funkciu Správca hesiel zamestnancom, aby mohli pracovať na webových kontách a nikdy nemusia poznať prihlasovacie poverenia, ktoré používajú.

HP Drive Encryption (len vybrané modely)

Aplikácia HP Drive Encryption sa používa na obmedzenie prístupu k údajom na celom pevnom disku počítača alebo na sekundárnej jednotke. Šifrovanie jednotky tiež dokáže spravovať samošifrovacie jednotky.

Príklad 1: Lekár chce zabezpečiť, aby len on mal prístup k údajom na pevnom disku počítača. lekár aktivuje funkciu Šifrovanie jednotky, pri ktorom sa vyžaduje overenie pri spustením ešte pred prihlásením sa do systému Windows. Po nastavení nie je prístup na pevný disk pred spustením operačného systému bez hesla možný. Lekár chce ešte viac zlepšiť zabezpečenie jednotky a zvolí možnosť šifrovania údajov samošifrovacou jednotkou.

Príklad 2: Administrátor v nemocnici chce zaistiť, aby len lekári a poverený personál mali prístup k údajom na ich lokálnom počítači bez zdieľania osobných hesiel. IT oddelenie pridá administrátora, lekárov a všetok poverený personál medzi používateľov funkcie Šifrovanie jednotky. Teraz len poverený personál môže spustiť počítač alebo doménu pomocou svojho osobného mena používateľa a hesla.

HP Device Access Manager (len vybrané modely)

Aplikácia HP Device Access Manager umožňuje administrátorovi obmedziť a spravovať prístup k hardvéru. Aplikácia Device Access Manager sa dá využiť na zablokovanie nepovoleného prístupu k USB flash jednotkám, na ktoré by sa dali skopírovať údaje. Obmedzuje tiež prístup k jednotkám CD/DVD, ovláda USB zariadenia, sieťové pripojenia atď. Príkladom môže byť situácia, keď externý dodávateľ potrebuje prístup k firemným počítačom, ale nesmie mať možnosť kopírovať údaje na USB jednotku.

Príklad 1: Manažér spoločnosti dodávajúcej lieky často pracuje s osobnými lekárskymi záznamami spolu s informáciami o spoločnosti. Zamestnanci potrebujú prístup k týmto údajom, je však veľmi dôležité, aby neboli údaje z počítača odstránené cez USB jednotku ani žiadne iné externé pamäťové médium. Sieť je bezpečná, ale počítače sú vybavené CD napaľovačkami a USB portami, ktoré umožňujú kopírovanie alebo odcudzenie údajov. Manažér používa funkciu Správca prístupu k zariadeniam na zakázanie USB portov a CD napaľovačiek, takže nemôžu byť použité. Hoci sú porty USB zablokované, myš a klávesnica ďalej fungujú.

Príklad 2: Poisťovacia spoločnosť nechce, aby jej zamestnanci inštalovali osobný softvér alebo údaje z domu. Niektorí zamestnanci potrebujú prístup k portu USB na všetkých počítačoch. Správca IT využíva funkciu Správca prístupu k zariadeniam na umožnenie prístupu niektorých zamestnancov, zatiaľ čo externý prístup ostatných je zablokovaný.

Computrace (kupuje sa samostatne)

Computrace (kupuje sa samostatne) je služba, ktorá umožňuje sledovať polohu odcudzeného počítača vždy, keď má používateľ prístup na internet. Služba Computrace tiež dokáže na diaľku spravovať a vyhľadávať počítače, ako aj monitorovať používanie počítača a aplikácií.

Príklad 1: Riaditeľ školy dal pokyn oddeleniu IT, aby sledovalo všetky počítače na škole. Po vykonaní inventúry počítačov administrátor IT zaregistroval všetky počítače do služby Computrace, takže ich bude možné vysledovať v prípade ich odcudzenia. Nedávno si škola uvedomila, že niekoľko počítačov chýba, takže administrátori IT upozornili úrady a zástupcov služby Computrace. Počítače boli vyhľadané a boli úradmi vrátené do školy.

Príklad 2: Spoločnosť zaoberajúca sa nehnuteľnosťami potrebuje spravovať a aktualizovať počítača po celom svete. Použije službu Computrace na monitorovanie a aktualizáciu počítačov bez toho, aby musela ku každému počítaču poslať osobu z oddelenia IT.

Dosiahnutie kľúčových cieľov zabezpečenia

Moduly aplikácie HP Client Security dokážu spolu poskytnúť riešenia pre množstvo bezpečnostných problémov vrátane kľúčových cieľov zabezpečenia:

- Ochrana pred cielenými krádežami
- Obmedzenie prístupu k citlivým údajom
- Zamedzenie neoprávneného prístupu z interných a externých miest
- Vytváranie zásad silného hesla

Ochrana pred cielenými krádežami

Príkladom cielenej krádeže môže byť odcudzenie počítača obsahujúceho dôverné údaje a informácie o zákazníkoch na bezpečnostnej kontrole na letisku. Nasledujúce funkcie pomáhajú chrániť pred cielenou krádežou:

- Ak je zapnutá funkcia overovania pri spustení, pomáha chrániť prístup k operačnému systému.
  - HP Client Security – viď HP Client Security na strane 12.
  - HP Drive Encryption – viď HP Drive Encryption (len vybrané modely) na strane 30.
- Šifrovanie pomáha zaistiť, že nebude možný prístup k údajom ani v prípade, že bude pevný disk vytiahnutý a nainštalovaný do nezabezpečeného systému.
- Služba Computrace dokáže vysledovať polohu počítača po odcudzení.
  - Computrace – viď Obnovenie pri krádeži (len vybrané modely) na strane 55.

Obmedzenie prístupu k citlivým údajom

Predpokladajme, že zmluvný audítor pracuje vo firme a bol mu umožnený prístup k počítaču, aby skontroloval citlivé finančné údaje. Nechcete, aby mal audítor možnosť tlačiť súbory ani ich ukladať do zapisovateľného zariadenia, napríklad na disk CD. Nasledujúca funkcia vám pomôže obmedziť prístup k údajom:

- Aplikácia HP Device Access Manager umožňuje správcom IT obmedziť prístup ku komunikačným zariadeniam, takže citlivé údaje sa nebudú dať skopírovať z pevného disku. Pozrite si časť Systémové zobrazenie na strane 45.

Zamedzenie neoprávneného prístupu z interných a externých miest

Neoprávnený prístup k nezabezpečenému firemnému počítaču predstavuje veľmi veľké riziko pre firemné sieťové zdroje, ako sú informácie z finančných služieb, vedenia alebo tímu výskumu a vývoja, a pre súkromné údaje, ako sú napríklad záznamy o pacientoch a osobné finančné záznamy. Nasledujúce funkcie pomáhajú chrániť pred neoprávneným prístupom:

- Ak je zapnutá funkcia overovania pri spustení, pomáha chrániť prístup k operačnému systému. (Pozrite si časť HP Drive Encryption (len vybrané modely) na strane 30.)
- Aplikácia HP Client Security pomáha zaistiť, aby neoprávnený používateľ nemohol získať heslá a nemal prístup k aplikáciám chráneným heslom. Pozrite si časť HP Client Security na strane 12.
- Aplikácia HP Device Access Manager umožňuje správcom IT obmedziť prístup k zapisovateľným zariadeniam, takže citlivé údaje sa nebudú dať skopírovať z pevného disku. Pozrite si časť HP Device Access Manager (len vybrané modely) na strane 44.

Vytváranie zásad silného hesla

Ak nadobudne platnosť firemná zásada, ktorá vyžaduje používanie silných hesiel pre desiatky webových aplikácií a databáz. Správca hesiel poskytuje chránené uloženie hesiel a pohodlie jedným prihlásením. Pozrite si časť Správca hesiel na strane 18.

Ďalšie bezpečnostné prvky

Priradenie bezpečnostných úloh

Pri spravovaní zabezpečenia počítačov najmä vo veľkých organizáciách) je dôležitou praxou rozdeliť zodpovednosť a práva medzi rôzne typy administrátorov a používateľov.

POZNÁMKA: V malej organizácii alebo pri používaní jednotlivcom môžu byť tieto úlohy pridelené jednej osobe.

Pre aplikáciu HP Client Security môžu byť bezpečnostné povinnosti a práva rozdelené na nasledujúce úlohy:

- Zástupca bezpečnosti – určuje úroveň zabezpečenia pre spoločnosť alebo sieť a stanovuje rozmiestnenie bezpečnostných funkcií, napríklad funkcie Šifrovanie jednotky.

  POZNÁMKA: Mnohé funkcie aplikácie HP Client Security môže zástupca bezpečnosti v spolupráci so spoločnosťou HP prispôsobiť. Ďalšie informácie nájdete v časti http://www.hp.com.

- Administrátor IT – aplikuje a spravuje bezpečnostné funkcie určené zástupcom bezpečnosti. Môže tiež aktivovať a deaktivovať niektoré funkcie. Ak napríklad zástupca bezpečnosti rozhodol rozmiestniť karty Smart, administrátor IT môže aktivovať režim hesla aj režim karty Smart.
- Používateľ – používa bezpečnostné funkcie. Ak napríklad zástupca bezpečnosti a administrátor IT aktivovali karty Smart pre systém, používateľ môže nastaviť kód PIN pre kartu Smart a použiť kartu Smart na overenie.

UPOZORNENIE: Administrátorom sa odporúča riadiť sa „najlepšími praktikami“ pri obmedzení práv koncového používateľa a obmedzení používateľského prístupu.

Neoprávneným používateľom nesmú byť pridelené práva administrátora.

Spravovanie hesiel aplikácie HP Client Security Manager

Väčšina funkcií aplikácie HP Client Security je zabezpečená heslami. V nasledujúcej tabuľke sú uvedené najčastejšie používané heslá, softvérový modul, v ktorom je heslo nastavené a funkcia hesla.

Heslá, ktoré nastavujú a používajú len administrátori IT, sú v tabuľke tiež vyznačené. Všetky ostatné heslá môžu byť nastavené bežnými používateľmi alebo administrátormi.

Heslo aplikácie HP Client Security	Nastavené v tomto module	Funkcia
Prihlasovacie heslo systému Windows	Ovládací panel Windows alebo HP Client Security	Dá sa použiť na ručné prihlasovanie a overovanie prístupu k rozličným funkciám aplikácie HP Client Security.
Heslo zálohy a obnovenia aplikácie HP Client Security	HP Client Security, jednotlivý používateľ	Chráni prístup k súboru zálohovania a obnovenia aplikácie HP Client Security.
Kód PIN pre kartu Smart	Credential Manager (Správca poverení)	Môže byť použité ako viacfaktorové overovanie. Môže byť použité ako overovanie pre systém Windows. Overuje používateľov funkcie Šifrovanie jednotky, ak je zvolená karta Smart.

Vytvorenie bezpečného hesla

Pri vytváraní hesiel je v prvom rade potrebné dodržiavať všetky parametre nastavené programom. Vo všeobecnosti je však potrebné zobrať do úvahy nasledujúce pokyny, ktoré vám pomôžu vytvoriť silné heslá a znížiť šancu, že bude vaše heslo prezradené:

- Používajte heslá obsahujúce viac než 6 znakov, najlepšie viac ako 8 znakov.
- V hesle zmiešajte veľké a malé písmená.
- Ak je to možné, zmiešajte abecedné a číselné znaky a zahrňte do hesla špeciálne znaky a interpunkciu.
- Nahraďte špeciálne znaky alebo čísla za písmená v kľúčovom slove. Použite napríklad číslo 1 pre písmená I alebo L.
- Skombinujte slová z 2 alebo viacerých jazykov.
- Rozdeľte v strede slovo alebo frázu číslami alebo špeciálnymi znakmi, napríklad „Mary2-2Cat45“.
- Nepoužívajte slová zo slovníka.
- Nepoužívajte v hesle meno ani iné osobné údaje, napríklad dátum narodenia, mená domácich zvierat ani rodné meno matky, a to ani napísané odzadu.
- Heslá pravidelne meňte. Pri každej zmene môžete zmeniť pár znakov.
- Ak si heslo zapisujete, neukladajte ho na bežne viditeľné miesto veľmi blízko počítača.
- Neukladajte si heslo do súboru v počítači, napríklad ako e-mail.
- Nezdieľajte kontá ani nikomu svoje heslo nehovorte.

Zálohovanie poverení a nastavení

Môžete použiť nástroj Backup and Recovery (Zálohovanie a Obnovenie) v aplikácii HP Client Security ako centrum, z ktorého môžete zálohovať a obnovovať bezpečnostné poverenia z niektorých nainštalovaných modulov aplikácie HP Client Security.

2 Úvodné informácie

Ak chcete nakonfigurovať aplikáciu HP Client Security na používanie vašich poverené, spustite jedným z týchto spôsobov aplikáciu HP Client Security. Keď používateľ prejde sprievodcom, už ho daný používateľ nemôže spustiť znova.

1. Na obrazovke Štart alebo Aplikácie kliknite alebo klepnite na aplikáciu **HP Client Security** (Windows 8).

   – alebo –

   Na pracovnej ploche systému Windows kliknite alebo klepnite na pomôcku **HP Client Security** (Windows 7).

   – alebo –

   Na pracovnej ploche systému Windows dvakrát kliknite alebo dvakrát klepnite na ikonu aplikácie **HP Client Security** v oblasti oznámení na paneli úloh úplne vpravo.

   – alebo –

   Na pracovnej ploche systému Windows kliknite alebo klepnite na ikonu aplikácie **HP Client Security** v oblasti oznámení a potom vyberte položku **Open HP Client Security** (Otvoriť HP Client Security).

2. Spustí sa Sprievodca nastavením aplikácie HP Client Security a zobrazí sa stránka Vitajte.

3. Prečítajte si obrazovku Vitajte, overte svoju identitu zadaním hesla do systému Windows a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).

   Ak ešte nemáte vytvorené heslo systému Windows, zobrazí sa výzva na jeho vytvorenie. Heslo systému Windows sa vyžaduje na ochranu konta systému Windows pred prístupom neoprávnených osôb a na používanie funkcií aplikácie HP Client Security.

4. Na stránke HP SpareKey vyberte tri bezpečnostné otázky. Zadajte odpovede na jednotlivé otázky a potom kliknite na tlačidlo **Next** (Ďalej). Povolené sú tiež vlastné otázky. Ďalšie informácie nájdete v časti HP SpareKey – Obnovenie hesla na strane 14.

5. Na stránke Fingerprints (Odtlačky prstov) zaregistrujte aspoň minimálny počet potrebných odtlačkov prsta a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej). Ďalšie informácie nájdete v časti Odtlačky prstov na strane 12.

6. Na stránke Drive Encryption (Šifrovanie jednotky) aktivujte šifrovanie, zálohujte šifrovací kľúč a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej). Ďalšie informácie nájdete v Pomocníkovi k softvéru HP Drive Encryption.

POZNÁMKA: Týka sa to tiež situácie, kedy je používateľom administrátor a ešte nebol administrátorom nakonfigurovaný Sprievodca nastavením aplikácie HP Client Security.

7. Na poslednej stránke sprievodcu kliknite alebo klepnite na tlačidlo **Finish** (Dokončiť).

   Na tejto stránke je uvedený stav funkcií a poverení.

8. Sprievodca nastavením aplikácie HP Client Security zaisťuje aktiváciu funkcie jednorazového overenia a skartovača súborov. Ďalšie informácie nájdete v Pomocníkovi k softvérom HP Device Access Manager a HP File Sanitizer.

POZNÁMKA: Týka sa to tiež situácie, kedy je používateľom administrátor a ešte nebol administrátorom nakonfigurovaný Sprievodca nastavením aplikácie HP Client Security.

Otvorenie aplikácie HP Client Security

Aplikáciu HP Client Security môžete otvoriť jedným z týchto spôsobov:

POZNÁMKA: Pred spustením aplikácie HP Client Security musí byť dokončený Sprievodca nastavením aplikácie HP Client Security.

- Na obrazovke Štart alebo Aplikácie kliknite alebo klepnite na aplikáciu **HP Client Security**.

  – alebo –

  Na pracovnej ploche systému Windows kliknite alebo klepnite na pomôcku **HP Client Security** (Windows 7).

  – alebo –

  Na pracovnej ploche systému Windows dvakrát kliknite alebo dvakrát klepnite na ikonu aplikácie **HP Client Security** v oblasti oznámení na paneli úloh úplne vpravo.

  – alebo –

  Na pracovnej ploche systému Windows kliknite alebo klepnite na ikonu aplikácie **HP Client Security** v oblasti oznámení a potom vyberte položku **Open HP Client Security** (Otvoriť HP Client Security).

3 Návod na ľahké nastavenie pre malé firmy

V tejto kapitole je vysvetlený základný postup aktivovania najpoužívanejších a užitočných možností v rámci aplikácie HP Client Security pre malé firmy. Množstvo nástrojov a volieb v tomto softvéri vám umožňuje vyladiť svoje predvoľby a nastaviť ovládanie prístupu. Tento návod na ľahké nastavenie je zameraný na to, aby ste jednotlivé moduly spustili s čo najmenším úsilím a čo najskôr. Ak potrebujete ďalšie informácie, vyberte modul, o ktorý sa zaujímate, a potom kliknite na tlačidlo **?** alebo Pomocník v pravom hornom rohu. Týmto tlačidlom automaticky zobrazíte informácie, ktoré vám pomôžu s práve zobrazeným oknom.

Úvodné informácie

1. Na pracovnej ploche systému Windows otvorte aplikáciu HP Client Security dvojitým kliknutím alebo dvojitým klepnutím na ikonu aplikácie **HP Client Security** v oblasti oznámení na paneli úloh úplne vpravo.
2. Zadajte svoj heslo do systému Windows, prípadne vytvorte heslo do systému Windows.
3. Prejdite nastavením aplikácie HP Client Security.

Ak má aplikácia HP Client Security vyžadovať overenie len raz počas prihlasovania do systému Windows, pozrite Bezpečnostné funkcie na strane 27.

Správca hesiel

Každý má množstvo hesiel – najmä ak pravidelne navštevujete webové stránky alebo používate aplikácie vyžadujúce prihlásenie. Bežný používateľ buď využíva rovnaké heslo pre všetky aplikácie a webové stránky alebo je tvorivý a rýchlo zabúda, ktoré heslo patrí ktorej aplikácii.

Správca hesiel si dokáže automaticky zapamätať vaše heslá alebo vám dáva možnosť rozlíšiť, ktoré stránky si má pamätať a ktoré má vynechať. Keď sa prihlásite na počítač, Správca hesiel poskytne vaše heslá alebo poverenia zapojeným aplikáciám alebo webovým stránkam.

Keď otvoríte aplikáciu alebo webovú stránku vyžadujúce poverenia, Správca hesiel automaticky stránku rozpozná a zobrazí otázku, či chcete, aby si softvér zapamätal vaše údaje. Ak sa rozhodnete niektoré stránky vynechať, môžete žiadosť zamietnuť.

Ako začať ukladať webové lokality, mená používateľa a heslá:

1. Napríklad prejdete na požadovanú webovú stránku alebo aplikáciu a potom kliknete na ikonu funkcie Správca hesiel v ľavom hornom rohu webovej stránky, ktorej overovanie chcete pridať.
2. Pomenujte prepojenie (nepovinné) a zadajte meno používateľa a heslo do funkcie Správca hesiel.
3. Po dokončení kliknite na tlačidlo **OK**.
4. Správca hesiel tiež dokáže uložiť meno používateľa a heslá pre sieťové zdieľanie alebo namapované sieťové jednotky.

Zobrazenie a spravovanie uložených overení vo funkcii Správca hesiel

Správca hesiel umožňuje prezerať, spravovať, zálohovať a spúšťať vaše overenia z centrálneho miesta. Správca hesiel tiež podporuje spúšťanie uložených stránok zo systému Windows.

Ak chcete otvoriť funkciu Správca hesiel, použite kombináciu klávesov Ctrl+kláves Windows+h, čím otvoríte Správcu hesiel, a potom kliknutím na tlačidlo **Log in** (Prihlásiť sa) spustite a overte uložený odkaz.

Možnosť **Edit** (Upraviť) vo funkcii Správca hesiel vám umožňuje zobraziť a zmeniť názov, prihlasovacie meno a odkryť tiež heslá.

Aplikácia HP Client Security pre malé firmy umožňuje zálohovať všetky poverenia a nastavenia a skopírovať ich na iný počítač.

HP Device Access Manager

Aplikácia Device Access Manager sa dá využiť na obmedzenie používania rôznych interných a externých pamäťových zariadení, takže vaše údaje zostávajú zabezpečené na pevnom disku a neputujú za dvere vašej firmy. Používateľ má napríklad povolený prístup k vašim údajom, ale má zablokované ich kopírovanie na disk CD, do osobného hudobného prehrávača alebo na USB pamäťové zariadenie.

1. Otvorte aplikáciu **Device Access Manager** (viď Otvorenie programu Device Access Manager na strane 44).

   Zobrazí sa prístup pre aktuálneho používateľa.

2. Ak chcete zmeniť prístup pre používateľov, skupiny alebo zariadenia, kliknite alebo klepnite na tlačidlo **Zmeniť**. Ďalšie informácie nájdete v časti Systémové zobrazenie na strane 45.

HP Drive Encryption

Aplikácia HP Drive Encryption sa používa na ochranu vašich údajov pomocou šifrovania celého pevného disku. Údaje na pevnom disku zostávajú chránené aj v prípade, že je počítač odcudzený alebo je z pôvodného počítača pevný disk vytiahnutý a umiestnený do iného počítača.

Výhoda ďalšieho zabezpečenia je, že funkcia Šifrovanie jednotky vyžaduje správne overenie pomocou mena používateľa a hesla ešte pred spustením operačného systému. Tento proces sa nazýva overovanie pri spustení.

V rámci uľahčenia sú heslá automaticky synchronizované medzi softvérovými modulmi vrátane používateľských kont systému Windows, overovania pre domény, aplikácie HP Drive Encryption, funkcie Správca hesiel a aplikácie HP Client Security.

Ak chcete nastaviť aplikáciu HP Drive Encryption počas prvotného nastavenia pomocou Sprievodcu nastavením aplikácie HP Client Security, pozrite Úvodné informácie na strane 8.

4 HP Client Security

Úvodná stránka aplikácie HP Client Security je centrum pre ľahký prístup k funkciám, aplikáciám a nastaveniam aplikácie HP Client Security. Úvodná stránka je rozdelená na tri časti:

- **DATA** (ÚDAJE) – poskytuje prístup k aplikáciám používaným na spravovanie zabezpečenia údajov.
- **DEVICE** (ZARIADENIE) – poskytuje prístup k aplikáciám používaným na spravovanie zabezpečenia zariadenia.
- **IDENTITY** (IDENTITA) – poskytuje možnosť registrácie a spravovania poverení.

Ukázaním kurzorom na dlaždicu aplikácie zobrazíte popis aplikácie.

Aplikácia HP Client Security môže poskytovať prepojenia na používateľské a administrátorské nastavenia naspodku stránky. Aplikácia HP Client Security poskytuje prístup k Rozšíreným nastaveniam, stačí klepnúť alebo kliknúť na ikonu **ozubeného kolieska** (nastavenia).

Funkcie, aplikácie a nastavenia identity

Funkcie, aplikácie a nastavenia identity obsiahnuté v aplikácii HP Client Security vám pomôžu spravovať rôzne aspekty vašej digitálnej identity. Kliknite alebo klepnite na jednu z týchto dlaždíc na úvodnej stránke aplikácie HP Client Security a potom zadajte svoje heslo do systému Windows

- **Fingerprints** (Odtlačky prstov) – registrácia a spravovanie poverení odtlačkom prsta.
- **SpareKey** – nastavenie a spravovanie poverenia HP SpareKey, ktoré sa dá použiť na prihlásenie na počítač v prípade, že boli ostatné poverenia stratené. Umožňuje tiež vynulovať zabudnuté heslo.
- **Windows Password** (Heslo do systému Windows) – poskytuje ľahký prístup k zmene hesla do systému Windows.
- **Bluetooth Devices** (Zariadenia Bluetooth) – umožňuje registrovať a spravovať zariadenia s funkciou Bluetooth.
- **Cards** (Karty) – umožňuje registrovať a spravovať karty Smart, bezkontaktné karty a karty Proximity.
- **PIN** – umožňuje registrovať a spravovať poverenie kódom PIN.
- **RSA SecurID** – umožňuje registrovať a spravovať poverenie RSA SecurID (ak je na mieste príslušné nastavenie).
- **Password Manager** (Správca hesiel) – umožňuje spravovať heslá pre kontá ona internete a aplikácie.

Odtlačky prstov

Sprievodca nastavením aplikácie HP Client Security vás bude sprevádzať procesom nastavenia (alebo „registrácie“) vašich odtlačkov prsta.

Odtlačky prsta môžete tiež registrovať a odstraňovať na stránke odtlačky prstov, ktorú môžete otvoriť kliknutím alebo klepnutím na ikonu **Fingerprints** (Odtlačky prstov) na úvodnej stránke aplikácie HP Client Security.

1. Na stránke Fingerprints (Odtlačky prstov) nasnímajte prst, kým nebude úspešne zaregistrovaný.

   Počet prstov, ktoré je potrebné zaregistrovať, je vyznačený na stránke. Preferujú sa ukazováky a prostredníky.

2. Ak chcete odstrániť predtým zaregistrované odtlačky prstov, kliknite alebo klepnite na tlačidlo **Delete** (Odstrániť).

3. Ak chcete zaregistrovať ďalšie prsty, kliknite alebo klepnite na tlačidlo **Enroll an additional fingerprint** (Zaregistrovať ďalší odtlačok prsta).

4. Pred zatvorením stránky kliknite alebo klepnite na tlačidlo **Save** (Uložiť).

⚠ **UPOZORNENIE:** Pri registrácii odtlačkov prstov prostredníctvom sprievodcu sa informácie o odtlačkoch prstov neuložia, kým nekliknete na tlačidlo **Next** (Ďalej). Ak necháte počítač chvíľu nečinný alebo zatvoríte program, vykonané zmeny sa **neuložia**.

- ▲ Ak chcete otvoriť Administratívne nastavenia odtlačkov prstov, kde môžu administrátori určovať registráciu, presnosť a ďalšie nastavenia, kliknite alebo klepnite na tlačidlo **Administrative Settings** (Administratívne nastavenia) (vyžaduje administrátorské práva).
- ▲ Ak chcete otvoriť Používateľské nastavenia odtlačkov prstov, kde môžete určovať nastavenia týkajúce sa vzhľadu a správania rozpoznávania, kliknite alebo klepnite na tlačidlo **User Settings** (Používateľské nastavenia).

Administratívne nastavenia odtlačkov prstov

Administrátori môžu určovať registráciu, presnosť a ďalšie nastavenia čítačky odtlačkov prstov. Sú potrebné administrátorské práva.

- ▲ Ak chcete otvoriť Administratívne nastavenia pre poverenie odtlačkom prsta, kliknite alebo klepnite na tlačidlo **Administrative Settings** (Administratívne nastavenia) na stránke Odtlačky prstov.

- **User enrollment** (Registrácia používateľa) – zvoľte minimálny a maximálny počet odtlačkov prstov, ktoré môže používateľ zaregistrovať.
- **Recognition** (Rozpoznávanie) – ťahaním posúvača upravte citlivosť používanú čítačkou odtlačkov prstov pri snímaní prsta.

  Ak váš odtlačok prsta nie je dobre rozpoznávaný, možno by ste mali vybrať nižšie nastavenie rozpoznávania. Vyššie nastavenie zvyšuje citlivosť na variácie snímania odtlačku prsta a teda znižuje možnosť falošného prijatia. Nastavenie **Medium-High** (Stredne vysoká) poskytuje kombináciu bezpečnosti a pohodlia.

Používateľské nastavenia odtlačkov prstov

Na stránke Používateľské nastavenia odtlačkov prstov môžete určiť nastavenia týkajúce sa vzhľadu a správania rozpoznávania odtlačkov prstov.

▲ Ak chcete otvoriť Používateľské nastavenia pre poverenie odtlačkom prsta, kliknite alebo klepnite na tlačidlo **User Settings** (Používateľské nastavenia) na stránke Odtlačky prstov.

- **Enable sound feedback** (Povoliť zvukovú spätnú väzbu) – aplikácia HP Client Security 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 položke Control panel (Ovládací panel) systému Windows, prípadne môžete zakázať zvukovú spätnú väzbu zrušením začiarknutia políčka
- **Show scan quality feedback** (Zobraziť odozvu kvality skenovania) – ak chcete zobrazovať všetky snímania bez ohľadu na kvalitu, začiarknite toto políčko. Ak chcete zobraziť iba snímania s dobrou kvalitou, zrušte začiarknutie tohto políčka.

HP SpareKey – Obnovenie hesla

Aplikácia HP SpareKey vám umožňuje získať prístup k počítaču (na podporovaných platformách) odpovedaním nna tri bezpečnostné otázky.

Aplikácia HP Client Security vás vyzve na nastavenie osobného HP SpareKey počas prvotného nastavenia v Sprievodcovi nastavením aplikácie HP Client Security.

Nastavenie HP SpareKey:

1. Na stránke HP SpareKey v sprievodcovi vyberte tri bezpečnostné otázky a potom zadajte odpoveď na jednotlivé otázky.

   Otázku môžete vybrať z vopred definovaného zoznamu alebo napíšte svoju otázku.

2. Kliknite alebo klepnite na tlačidlo **Enroll** (Registrovať).

Odstránenie HP SpareKey:

▲ Kliknite alebo klepnite na tlačidlo **Delete your SpareKey** (Odstrániť SpareKey).

Po nastavení SpareKey môžete získať prístup k počítaču pomocou svojho SpareKey na prihlasovacej obrazovke overovania pri spustení alebo na obrazovke Víta vás systém Windows.

Na stránke SpareKey môžete vybrať rozličné otázky alebo zmeniť odpovede. Stránku otvoríte z dlaždice Obnovenie hesla na úvodnej stránke aplikácie HP Client Security.

Ak chcete otvoriť nastavenia HP SpareKey, kde môže administrátor určiť nastavenia týkajúce sa poverenia HP SpareKey, kliknite na tlačidlo **Settings** (Nastavenia) (vyžaduje administrátorské práva).

HP SpareKey Settings

Na stránke Nastavenia HP SpareKey môžete určiť nastavenia týkajúce sa správania a používania poverenia HP SpareKey.

▲ Ak chcete spustiť stránku Nastavenia HP SpareKey, kliknite alebo klepnite na tlačidlo **Settings** (Nastavenia) na stránke HP SpareKey (vyžaduje administrátorské práva).

Administrátori môžu vybrať tieto nastavenia:

- Vybrať otázky, ktoré budú predložené jednotlivým používateľom počas nastavenia HP SpareKey.
- Pridať najviac tri vlastné bezpečnostné otázky do zoznamu predkladaného používateľom.

- Vybrať, či môžu používatelia napísať vlastné bezpečnostné otázky.
- Určiť, ktoré overovacie prostredie (Windows alebo Overovanie pri spustení) umožňuje používať na obnovenie hesla HP SpareKey.

Heslo do systému Windows

Aplikácia HP Client Security zjednodušuje a urýchľuje zmenu hesla do systému Windows v porovnaní so zmenou hesla pomocou Ovládacieho panela systému Windows.

Zmena hesla do systému Windows:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na tlačidlo **Windows Password** (Heslo do systému Windows).
2. Do textového políčka **Current Windows password** (Aktuálne heslo do systému Windows) zadajte svoje súčasné heslo.
3. Do textového políčka **New Windows password** (Nové heslo do systému Windows) napíšte nové heslo a potom ho napíšte znova do textového políčka **Confirm new password** (Potvrdenie nového hesla).
4. Kliknite alebo klepnite na tlačidlo **Change** (Zmeniť), čím okamžite zmeníte aktuálne heslo na práve zadané.

Zariadenia Bluetooth

Ak administrátor povolil Bluetooth ako overovacie poverenie, môžete pre ďalšiu bezpečnosť k ostatným povereniam nastaviť telefón s funkciou Bluetooth.

POZNÁMKA: Podporované sú len zariadenia s funkciou Bluetooth.

1. Uistite sa, či je na počítači aktivovaná funkcia Bluetooth a či je telefón s funkciou Bluetooth nastavený do režimu zistiteľnosti. Pri pripájaní telefónu možno bude potrebné zadať automaticky generovaný kód na zariadení Bluetooth. V závislosti od konfiguračných nastavení zariadenia s funkciou Bluetooth môže byť potrebné porovnanie párovacích kódov medzi počítačom a telefónom.
2. Ak chcete zaregistrovať telefón, zvoľte ho a potom kliknite alebo klepnite na tlačidlo **Enroll** (Registrovať).

Ak chcete otvoriť stránku Nastavenia zariadení Bluetooth na strane 15, na ktorej môže administrátor určiť nastavenia pre zariadenia Bluetooth, kliknite alebo klepnite na tlačidlo **Settings** (Nastavenia) (vyžaduje administrátorské práva).

Nastavenia zariadení Bluetooth

Administrátori môžu určiť nasledujúce nastavenia týkajúce sa správania a používania poverení zariadením Bluetooth:

Tiché overovanie

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Automaticky použiť pripojené zaregistrované zariadenie Bluetooth počas overovania identity) – začiarknite políčko, ak chcete umožniť používateľom používať pri overovaní poverenie Bluetooth bez nutnosti úkonu používateľa. Ak chcete túto možnosť zakázať, zrušte začiarknutie políčka.

Vzdialenosť Bluetooth

- **Lock computer when your enrolled Bluetooth device moves out of range of your computer** (Uzamknúť počítač, keď sa zariadenie Bluetooth dostane mimo dosah počítača) – začiarknite políčko, ak chcete zamykať počítač, keď sa zariadenie Bluetooth, ktoré bolo pripojené počas prihlásenia, dostane mimo dosah. Ak chcete túto možnosť zakázať, zrušte začiarknutie políčka.

POZNÁMKA: Modul Bluetooth na počítači musí podporovať túto funkciu, ak ju chcete využívať.

Karty

Aplikácia HP Client Security podporuje množstvo rozličných identifikačných kariet, čo sú malé plastové karty obsahujúce počítačový čip. Patria sem karty Smart, bezkontaktné karty a karty Proximity. Ak je k počítaču pripojená jedna z týchto kariet a príslušná čítačka kariet, a administrátor nainštaloval príslušný ovládač od výrobcu, a ak administrátor povolil kartu ako overovacie poverenie, môžete použiť kartu ako overovacie poverenie.

Pre karty Smart by mal výrobca poskytnúť nástroje na inštaláciu bezpečnostného certifikátu a správu kódov PIN, ktoré aplikácia využíva vo svojom bezpečnostnom algoritme. Počet a typ znakov používaných ako kódy PIN môžu byť rôzne. Administrátor musí pred jej použitím kartu Smart inicializovať.

Aplikácia HP Client Security podporuje nasledujúce formáty kariet Smart:

- CSP
- PKCS11

Aplikácia HP Client Security podporuje nasledujúce formáty bezkontaktných kariet:

- Bezkontaktné pamäťové karty HID iCLASS
- Bezkontaktné karty MiFare Classic 1k, 4k a mini pamäťové karty

Aplikácia HP Client Security podporuje nasledujúce karty Proximity:

- Karty HID Proximity

Registrácia karty Smart:

1. Vložte kartu do pripojenej čítačky kariet Smart.
2. Keď je karta rozpoznaná, zadajte kód PIN pre kartu a potom kliknite alebo klepnite na tlačidlo **Enroll** (Registrovať).

Zmena kódu PIN karty Smart:

1. Vložte kartu do pripojenej čítačky kariet Smart.
2. Keď je karta rozpoznaná, zadajte kód PIN pre kartu a potom kliknite alebo klepnite na tlačidlo **Authenticate** (Overiť).
3. Kliknite alebo klepnite na tlačidlo **Change PIN** (Zmeniť kód PIN) a potom zadajte nový kód PIN.

Registrácia bezkontaktnej karty alebo karty Proximity:

1. Položte kartu na príslušnú čítačku alebo veľmi blízko k nej.
2. Keď je karta rozpoznaná, kliknite alebo klepnite na tlačidlo **Enroll** (Registrovať).

Odstránenie zaregistrovanej karty:

1. Vložte kartu do čítačky.
2. Pri kartách Smart zadajte kód PIN pre kartu a potom kliknite alebo klepnite na tlačidlo **Authenticate** (Overiť).
3. Kliknite alebo klepnite na tlačidlo **Delete** (Odstrániť).

Keď je karta zaregistrovaná, podrobnosti o nej sú zobrazené v časti **Enrolled Cards** (Zaregistrované karty). Keď je karta odstránená, zmizne zo zoznamu.

Ak chcete otvoriť Nastavenia kariet Proximity, bezkontaktných kariet a kariet Smart, kde môžu administrátori určiť nastavenia týkajúce sa poverení kartou, kliknite alebo klepnite na tlačidlo **Settings** (Nastavenia) (vyžaduje administrátorské práva).

Nastavenia kariet Proximity, bezkontaktných kariet a kariet Smart

Ak chcete otvoriť nastavenia karty, kliknite alebo klepnite na kartu v zozname a potom kliknite alebo klepnite na šípku, ktorá sa zobrazí.

Zmena kódu PIN karty Smart:

1. Vložte kartu do čítačky.
2. Zadajte kód PIN priradený karte a potom kliknite alebo klepnite na tlačidlo **Continue** (Pokračovať).
3. Zadajte a potvrďte nový kód PIN a potom kliknite alebo klepnite na tlačidlo **Continue** (Pokračovať).

Inicializácia kódu PIN karty Smart:

1. Vložte kartu do čítačky.
2. Zadajte kód PIN priradený karte a potom kliknite alebo klepnite na tlačidlo **Continue** (Pokračovať).
3. Zadajte a potvrďte nový kód PIN a potom kliknite alebo klepnite na tlačidlo **Continue** (Pokračovať).
4. Kliknutím alebo klepnutím na tlačidlo **Yes** (Áno) potvrďte inicializáciu.

Vymazanie údajov o karte:

1. Vložte kartu do čítačky.
2. Zadajte kód PIN priradený karte (len pri kartách Smart) a potom kliknite alebo klepnite na tlačidlo **Continue** (Pokračovať).
3. Kliknutím alebo klepnutím na tlačidlo **Yes** (Áno) potvrďte odstránenie.

PIN

Ak administrátor povolil kód PIN ako overovacie poverenie, môžete pre ďalšiu bezpečnosť k ostatným povereniam nastaviť kód PIN.

Nastavenie nového kódu PIN:

- Zadajte kód PIN, opätovným zadaním ho potvrďte a potom kliknite alebo klepnite na tlačidlo **Apply** (Použiť).

Odstránenie kódu PIN:

▲ Kliknite alebo klepnite na tlačidlo **Delete** (Odstrániť) a potom potvrďte kliknutím alebo klepnutím na tlačidlo **Yes** (Áno).

Ak chcete otvoriť Nastavenia kódu PIN, kde môžu administrátori určiť nastavenia týkajúce sa poverení kódom PIN, kliknite alebo klepnite na tlačidlo **Settings** (Nastavenia) (vyžaduje administrátorské práva).

Nastavenia systému PIN

Na stránke Nastavenia kódu PIN môžete stanoviť minimálnu a maximálnu prijateľnú dĺžku poverenia kódom PIN.

RSA SecurID

Ak administrátor povolil RSA ako overovacie poverenie a sú splnené nasledujúce podmienky, môžete zaregistrovať alebo odstrániť poverenie RSA SecurID.

POZNÁMKA: Je potrebné príslušné nastavenie.

- Používateľ musí byť vytvorený na serveri RSA.
- Token RSA SecurID priradený používateľovi a počítač musia byť pripojené k doméne servera RSA.
- Softvér SecurID musí byť v počítači nainštalovaný.
- Je k dispozícii pripojenie k správne nakonfigurovanému serveru RSA.

Registrácia poverenia RSA SecurID:

▲ Zadajte svoje meno používateľa a heslo pre RSA SecurID (kód RSA SecurID Token alebo kód PIN+Token, v závislosti od prostredia) a potom kliknite alebo klepnite na tlačidlo **Apply** (Použiť).

Po úspešnom zaregistrovaní sa zobrazí hlásenie „Your RSA SecurID credential has been successfully enrolled“ (Vaše poverenie RSA SecurID bolo úspešne zaregistrované) a aktivuje sa tlačidlo Delete (Odstrániť).

Odstránenie poverenia RSA SecurID:

▲ Kliknite na tlačidlo **Delete** (Odstrániť) a potom v dialógovom okne s výzvou „Are you sure you want to delete your RSA SecurID credential?“ (Naozaj chcete odstrániť poverenie RSA SecurID?) vyberte možnosť **Yes** (Áno).

Správca hesiel

Prihlasovanie na webové stránky a do aplikácií je ľahšie a bezpečnejšie, ak použijete funkciu Správca hesiel. Môžete vytvárať silnejšie heslá, ktoré si nemusíte zapisovať ani pamätať, a potom sa ľahko prihlasujete odtlačkom prsta, kartou Smart, kartou Proximity, bezkontaktnou kartou, telefónom s funkciou Bluetooth, kódom PIN, poverením RSA alebo heslom do systému Windows.

POZNÁMKA: Pretože štruktúra prihlasovacích obrazoviek na webových stránkach sa neustále mení, Správca hesiel nemusí vždy podporovať všetky webové stránky.

Správca hesiel ponúka tieto možnosti:

Stránka Správca hesiel

- Kliknutím alebo klepnutím na konto automaticky otvoríte webovú stránku alebo aplikáciu a prihlásite sa.
- Pomocou kategórií usporiadajte svoje kontá.

Sila hesla

- Máte prehľad, či niektoré vaše heslá nepredstavujú bezpečnostné riziko.
- Pri pridávaní prihlasovacích údajov kontrolujete silu jednotlivých hesiel používaných na webových stránkach a v aplikáciách.
- Sila hesla je znázornená červeným, žltým alebo zeleným indikátorom stavu.

Ikona **Password Manager** (Správca hesiel) je zobrazená v ľavom hornom rohu prihlasovacej obrazovky na webovej stránke alebo v aplikácii. Ak zatiaľ nebolo pre danú webovú stránku alebo aplikáciu vytvorené prihlásenie, na ikone sa zobrazuje znak plus.

▲ Kliknutím alebo klepnutím na ikonu **Password Manager** (Správca hesiel) zobrazíte miestnu ponuku, v ktorej môžete vybrať spomedzi týchto možností:

- Add [somedomain.com] to Password Manager (Pridať [somedomain.com] do Správcu hesiel)
- Open Password Manager (Otvoriť Správcu hesiel)
- Icon Settings (Nastavenia ikony)
- Pomocník

Pre webové stránky alebo programy, pre ktoré ešte nebolo vytvorené prihlásenie

V kontextovej ponuke sú zobrazené tieto možnosti:

- **Pridať [nejakadomena.com] do Správcu hesiel** – umožňuje pridať prihlásenie pre aktuálnu prihlasovaciu obrazovku.
- **Otvoriť Správcu hesiel** – spustí Správcu hesiel.
- **Nastavenia ikony** – umožňuje určiť podmienky, pri ktorých je zobrazená ikona **Správca hesiel**.
- **Pomocník** – zobrazí Pomocníka k aplikácii HP Client Security.

Pre webové stránky alebo programy, ku ktorým už bolo vytvorené prihlásenie

V kontextovej ponuke sú zobrazené tieto možnosti:

- **Vyplniť údaje prihlasovania** – zobrazí stránku **Overiť vašu identitu**. V prípade úspešného overenia sú do prihlasovacích políčok umiestnené prihlasovacie údaje a potom je stránka odoslaná (ak bolo určené odoslanie v prípade vytvorenia alebo poslednej úpravy prihlásenia).
- **Upraviť prihlásenie** – umožňuje upraviť prihlasovacie údaje pre danú webovú stránku.
- **Pridať prihlásenie** – umožňuje pridať konto do Správcu hesiel.
- **Otvoriť Správcu hesiel** – spustí Správcu hesiel.
- **Pomocník** – zobrazí Pomocníka k aplikácii HP Client Security.

POZNÁMKA: Administrátor tohto počítača mohol nakonfigurovať aplikáciu HP Client Security tak, že sa pri overovaní vašej identity vyžaduje viac než jedno poverenie.

Pridávanie prihlásení

Ľahko môžete pridať prihlásenie pre webovú stránku alebo program, stačí raz zadať prihlasovacie údaje. Potom už Správca hesiel zadáva údaje za vás. Po otvorení webovej stránky alebo programu potom môžete tieto prihlásenia používať.

Pridanie prihlásenia:

1. Otvorte prihlasovaciu obrazovku pre webovú stránku alebo program.
2. Kliknite alebo klepnite na ikonu **Správca hesiel** a potom kliknite alebo klepnite na jedno z nasledujúceho, podľa toho, či ide o prihlasovaciu obrazovku pre webovú stránku alebo program:
   - Pri webovej stránke kliknite alebo klepnite na položku **Pridať [názov domény] do Správcu hesiel**.
   - Pri programe kliknite alebo klepnite na položku **Pridať prihlasovaciu obrazovku do Správcu hesiel**.
3. Zadajte prihlasovacie údaje. Prihlasovacie políčka na obrazovke a príslušné políčka v dialógovom okne sú označené tučným oranžovým okrajom.
   a. Ak chcete vyplniť prihlasovacie políčko jednou z vopred naformátovaných volieb, kliknite alebo klepnite na šípky napravo od políčka.
   b. Ak chcete zobraziť heslo pre toto prihlásenie, kliknite alebo klepnite na možnosť **Zobraziť heslo**.
   c. Ak majú byť prihlasovacie políčka vyplnené, ale neodoslané, zrušte začiarknutie políčka **Automatically submit logon data** (Automaticky odoslať údaje prihlásenia).
   d. Kliknutím alebo klepnutím na tlačidlo **OK** vyberte spôsob overenia, ktorý chcete použiť (odtlačky prsta, karta Smart, karta Proximity, bezkontaktná karta, telefón s funkciou Bluetooth, kód PIN alebo heslo) a potom sa pomocou vybraného spôsobu overenia prihláste.

      Znak plus je z ikony **Password Manager** (Správca hesiel) odstránený, čo znamená, že prihlásenie bolo vytvorené.
   e. Ak Správca hesiel nezistil prihlasovacie políčka, kliknite alebo klepnite na položku **More fields** (Ďalšie políčka).
      - Začiarknite políčko pre každé pole, ktoré sa vyžaduje na prihlasovanie, alebo zrušte začiarknutie políčka pre ľubovoľné polia, ktoré sa nevyžadujú na prihlasovanie.
      - Kliknite alebo klepnite na tlačidlo **Close** (Zavrieť).

Pri každej návšteve webovej stránky alebo pri každom otvorení programu sa v ľavom hornom rohu prihlasovacej obrazovky na webovej stránke alebo v programe zobrazuje ikona **Password Manager** (Správca hesiel) označujúca, že na prihlásenie môžete použiť svoje registrované poverenia.

Úprava prihlásení

Úprava prihlásenia:

1. Otvorte prihlasovaciu obrazovku pre webovú stránku alebo program.
2. Kliknutím alebo klepnutím na ikonu **Password Manager** (Správca hesiel) zobrazte dialógové okno, v ktorom môžete upraviť prihlasovacie údaje, a potom kliknite alebo klepnite na položku **Edit Logon** (Upraviť prihlásenie).

   Prihlasovacie políčka na obrazovke a príslušné políčka v dialógovom okne sú označené tučným oranžovým okrajom.

   Údaje konta tiež môžete upraviť na stránke Správca hesiel. Kliknutím alebo klepnutím na prihlásenie zobrazte možnosti úpravy a potom vyberte položku **Edit** (Upraviť).
3. Upravte prihlasovacie údaje.
   - Ak chcete upraviť **Account name** (Názov konta), zadajte do políčka nový názov.
   - Ak chcete pridať alebo upraviť názov **Category** (Kategória), zadajte alebo upravte názov v políčku **Category** (Kategória).
   - Ak chcete vybrať prihlasovacie políčko **Username** (Meno používateľa) s jednou z vopred formátovaných volieb, kliknite alebo klepnite na šípku nadol napravo od políčka.

     Vopred formátované voľby sú k dispozícii len vtedy, keď sa upravuje prihlásenie z príkazu Edit (Upraviť) v kontextovej ponuke ikony Správca hesiel.
   - Ak chcete vybrať prihlasovacie políčko **Password** (Heslo) s jednou z vopred formátovaných volieb, kliknite alebo klepnite na šípku nadol napravo od políčka.

     Vopred formátované voľby sú k dispozícii len vtedy, keď sa upravuje prihlásenie z príkazu Edit (Upraviť) v kontextovej ponuke ikony Správca hesiel.
   - Ak chcete do prihlásenia pridať ďalšie políčka z obrazovky, kliknite alebo klepnite na položku **More fields** (Ďalšie políčka).
   - Ak chcete zobraziť heslo pre toto prihlásenie, kliknite alebo klepnite na ikonu **Show password** (Zobraziť heslo).
   - Ak majú byť prihlasovacie políčka vyplnené, ale neodoslané, zrušte začiarknutie políčka **Automatically submit logon data** (Automaticky odoslať údaje prihlásenia).
   - Ak chcete označiť, že pri tomto prihlásení je prezradené heslo, začiarknite políčko **This password is compromised** (Toto heslo je prezradené).

     Po uložení zmien sú všetky ostatné prihlásenia používajúce rovnaké heslo tiež označené ako prezradené. Potom môžete navštíviť každé takéto konto a podľa potreby zmeniť heslá.
4. Kliknite alebo klepnite na tlačidlo **OK**.

Používanie ponuky Rýchle prepojenia Správcu hesiel

Správca hesiel poskytuje rýchly a ľahký spôsob otvárania webových stránok a programov, pre ktoré ste vytvorili prihlásenie. Dvojitým kliknutím alebo dvojitým klepnutím na prihlásenie do programu alebo na webovú stránku v ponuke **Password Manager Quick Links** (Rýchle prepojenia Správcu hesiel), prípadne zo stránky Správca hesiel v aplikácii HP Client Security otvorte prihlasovaciu obrazovku a potom vyplňte prihlasovacie údaje.

Keď vytvoríte prihlásenie, automaticky bude pridané do ponuky **Rýchle prepojenia** Správcu hesiel.

Zobrazenie ponuky **Quick Links** (Rýchle prepojenia):

▲ Stlačte klávesovú skratku funkcie **Password Manager** (Správca hesiel) . Od výrobcu je nastavená klávesová skratka Ctrl+kláves Windows+h. Ak chcete zmeniť kombináciu klávesovej skratky, na úvodnej stránke aplikácie HP Client Security kliknite na položku **Password Manager** (Správca hesiel)a potom kliknite alebo klepnite na **Settings** (Nastavenia).

Usporiadanie prihlásení do kategórií

Vytvorte si jednu alebo viac kategórií a udržiavajte svoje prihlásenia usporiadané.

Priradenie prihlásenia do kategórie:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na položku **Password Manager** (Správca hesiel).
2. Kliknite alebo klepnite na konto a potom kliknite alebo klepnite na položku **Edit** (Upraviť).
3. Do políčka **Category** (Kategória) zadajte názov kategórie.
4. Kliknite alebo klepnite na tlačidlo **Save** (Uložiť).

Odstránenie konta z kategórie:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na položku **Password Manager** (Správca hesiel).
2. Kliknite alebo klepnite na konto a potom kliknite alebo klepnite na položku **Edit** (Upraviť).
3. V políčku **Category** (Kategória) vymažte názov kategórie.
4. Kliknite alebo klepnite na tlačidlo **Save** (Uložiť).

Premenovanie kategórie:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na položku **Password Manager** (Správca hesiel).
2. Kliknite alebo klepnite na konto a potom kliknite alebo klepnite na položku **Edit** (Upraviť).
3. V políčku **Category** (Kategória) zmeňte názov kategórie.
4. Kliknite alebo klepnite na tlačidlo **Save** (Uložiť).

Spravovanie prihlásení

Správca hesiel uľahčuje spravovanie prihlasovacích údajov pre mená používateľa, heslá a kontá s viacerými prihláseniami z jedného centrálneho miesta.

Vaše prihlásenia sú uvedené na stránke Správca hesiel.

Spravovanie prihlásení:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na položku **Password Manager** (Správca hesiel).
2. Kliknite alebo klepnite na existujúce prihlásenie, vyberte jednu z nasledujúcich možností a potom postupujte podľa pokynov na obrazovke:
   - **Edit** (Upraviť) – upravte prihlásenie. Ďalšie informácie nájdete v časti Úprava prihlásení na strane 21.
   - **Log in** (Prihlásiť sa) – prihlásenie na vybrané konto.
   - **Delete** (Odstrániť) – odstránenie prihlásenia pre vybrané konto.

Pridanie ďalšieho prihlásenia na webovú stránku alebo do programu:

1. Otvorte prihlasovaciu obrazovku pre webovú stránku alebo program.
2. Kliknutím alebo klepnutím na ikonu **Password Manager** (Správca hesiel) zobrazte jej kontextovú ponuku.
3. Kliknite alebo klepnite na položku **Add Logon** (Pridať prihlásenie) a potom postupujte podľa pokynov na obrazovke.

Vyhodnotenie sily hesla

Používanie silných hesiel pri prihlasovaní na webové stránky a do programov je dôležitý aspekt ochrany vašej identity.

Správca hesiel monitoruje a ľahko vylepšuje vašu bezpečnosť okamžitou a automatizovanou analýzou sily jednotlivých hesiel používaných na prihlásenie na webové stránky a do programov.

Počas zadávania hesla pri vytváraní prihlásenia na konto v Správcovi hesiel sa pod heslom zobrazuje farebný pásik signalizujúci silu hesla. Farby signalizujú nasledujúce hodnoty:

- **Červená** – slabé
- **Žltá** – priemerné
- **Zelená** – silné

Nastavenia ikony Správcu hesiel

Správca hesiel sa pokúša identifikovať prihlasovacie obrazovky na webových stránkach a v programoch. Keď sa zistí prihlasovacia obrazovka, pre ktorú ste nevytvorili prihlásenie, Správca hesiel zobrazí pomocou ikony **Password Manager** (Správca hesiel) so znakom plus výzvu, aby ste pridali prihlásenie pre danú obrazovku.

1. Kliknite alebo klepnite na ikonu a potom kliknutím alebo klepnutím na položku **Icon Settings** (Nastavenia ikony) prispôsobte, ako Správca hesiel spracuje možné prihlasovacie stránky.
   - **Prompt to add logons for logon screens** (Vyzvať na pridanie prihlasovacích údajov na prihlasovacích obrazovkách) – kliknite alebo klepnite na túto možnosť, ak má Správca hesiel vyzvať na pridanie prihlásenia, keď je zobrazená prihlasovacia obrazovka, pre ktorú ešte nebolo nastavené prihlásenie.
   - **Exclude this screen** (Nezahrnúť túto obrazovku) – začiarknite políčko, ak chcete, aby vás už Správca hesiel nevyzýval znova na pridanie prihlásenia pre túto prihlasovaciu obrazovku.
   - **Do not prompt to add logons for logon screens** (Nevyzvať na pridanie prihlasovacích údajov na prihlasovacích obrazovkách) – vyberte, ak chcete zvoliť túto možnosť.
2. Pridanie prihlásenia pre obrazovku, ktorá bola predtým vyňatá:
   a. Prihláste sa na predtým vyňatú webovú stránku.
   b. Ak si má Správca hesiel zapamätať heslo pre túto stránku, kliknite alebo klepnite na tlačidlo **Remember** (Zapamätať) v kontextovom dialógovom okne, čím uložíte heslo a vytvoríte prihlásenie pre danú obrazovku.
3. Ak chcete otvoriť ďalšie nastavenia Správcu hesiel, kliknite alebo klepnite na ikonu Správcu hesiel, kliknite alebo klepnite na položku **Open Password Manager** (Otvoriť Správcu hesiel) a potom kliknite alebo klepnite na položku **Settings** (Nastavenia) na stránke Správca hesiel.

Import a export prihlásení

Na stránke Import a export v programe HP Password Manager môžete importovať prihlásenia uložené webovými prehľadávačmi do počítača. Môžete tiež importovať údaje zo súbory zálohy aplikácie HP Client Security a exportovať údaje do súboru zálohy aplikácie HP Client Security.

▲ Ak chcete otvoriť stránku Import a export, kliknite alebo klepnite na položku **Import and export** (Import a export) na stránke Správca hesiel.

Import hesiel z prehľadávača:

1. Kliknite alebo klepnite na prehľadávač, z ktorého chcete importovať heslá (zobrazujú sa len nainštalované prehľadávače).
2. Zrušte začiarknutie pri všetkých kontách, z ktorých heslá nechcete importovať.
3. Kliknite alebo klepnite na tlačidlo **Import** (Importovať).

Import údajov do súboru zálohy aplikácie HP Client Security (alebo ich export) môže byť vykonávaný prostredníctvom priradených prepojení (v časti **Other Options)** (Ďalšie možnosti)) na stránke Import a export.

POZNÁMKA: Touto funkciou sa importujú a exportujú len údaje Správcu hesiel. Informácie o zálohovaní a obnovení ďalších údajov aplikácie HP Client Security nájdete v časti Zálohovanie a obnovenie údajov na strane 28.

Import údajov zo súboru zálohy aplikácie HP Client Security:

1. Na stránke Import a export v programe HP Password Manager kliknite alebo klepnite na položku **Import data from an HP Client Security backup file** (Importovať údaje zo súboru zálohy aplikácie HP Client Security).
2. Overte svoju identitu.
3. Vyberte predtým uložený súbor zálohy alebo do uvedeného políčka zadajte cestu a potom kliknite alebo klepnite na tlačidlo **Browse** (Prehľadávať).
4. Zadajte heslo použité na ochranu súboru a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).
5. Kliknite alebo klepnite na tlačidlo **Restore** (Obnoviť).

Export údajov do súboru zálohy aplikácie HP Client Security:

1. Na stránke Import a export v programe HP Password Manager kliknite alebo klepnite na položku **Export data from an HP Client Security backup file** (Exportovať údaje do súboru zálohy aplikácie HP Client Security).
2. Overte svoju identitu a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).
3. Zadajte názov súboru zálohy. Štandardne je súbor uložený do priečinka Dokumenty. Ak chcete určiť iné miesto, kliknite alebo klepnite na tlačidlo **Browse** (Prehľadávať).
4. Zadajte a potvrďte heslo na ochranu súboru a potom kliknite alebo klepnite na tlačidlo **Save** (Uložiť).

Nastavenia

Môžete určiť nastavenia a prispôsobiť si tak Správcu hesiel:

- **Prompt to add logons for logon screens** (Vyzvať na pridanie prihlasovacích údajov na prihlasovacích obrazovkách) – ikona **Password Manager** (Správca hesiel)so znakom plus je zobrazená vždy, keď sa zistí prihlasovacia obrazovka webovej stránky alebo programu, čo znamená, že môžete pridať prihlásenie pre túto obrazovku do ponuky **Logons** (Prihlásenia).

  Ak chcete vypnúť túto funkciu, zrušte začiarknutie políčka vedľa položky **Prompt to add logons for logon screens** (Vyzvať na pridanie prihlasovacích údajov na prihlasovacích obrazovkách)

- **Open Password Manager with Ctrl+Win+h** (Otvárať Správcu hesiel kombináciou Ctrl+Win+h) – predvolená klávesová skratka, ktorou sa otvára ponuka **Password Manager Quick Links** (Rýchle prepojenia Správcu hesiel) je Ctrl+kláves Windows+h.

  Ak chcete klávesovú skratku zmeniť, kliknite alebo klepnite na túto možnosť a potom zadajte novú klávesovú kombináciu. Kombinácia sa môže skladať z jedného alebo viacerých týchto klávesov: ctrl, alt alebo shift a ľubovoľný abecedný alebo číselný kláves.

  Kombinácie vyhradené pre systém Windows alebo aplikácie systému Windows nie je možné použiť.

- Ak chcete vrátiť nastavenia na predvolené hodnoty, kliknite alebo klepnite na položku **Restore defaults** (Obnoviť predvolené).

Rozšírené nastavenia

Administrátori majú prístup k nasledujúcim možnostiam cez ikonu **ozubeného kolieska** (nastavenia) na úvodnej stránke aplikácie HP Client Security.

- **Administrator Policies** (Zásady administrátorov) – umožňuje konfigurovať zásady prihlasovania a relácií pre administrátorov.
- **Standard User Policies** (Zásady bežných používateľov) – umožňuje konfigurovať zásady prihlasovania a relácií pre bežných používateľov.
- **Security Features** (Bezpečnostné funkcie) – umožňuje zvýšiť zabezpečenie počítača ochranou konta systému Windows pomocou silného overovania alebo aktivovaním overenia pred spustením systému Windows.
- **Users** (Používatelia) – umožňuje spravovať používateľov a ich poverenia.
- **My Policies** (Moje zásady) – umožňuje prezerať vaše zásady prihlasovania a stav registrácie.
- **Backup and Restore** (Zálohovať a obnoviť) – umožňuje zálohovať alebo obnoviť údaje aplikácie HP Client Security.
- **About HP Client Security** (Informácie o HP Client Security) – zobrazuje informácie o verzii aplikácie HP Client Security Manager.

Zásady administrátorov

Môžete nakonfigurovať zásady prihlasovania a relácií pre administrátorov tohto počítača. Tu nastavené zásady prihlasovania sa týkajú poverení potrebných na prihlásenie lokálneho administrátora do systému Windows. Tu nastavené zásady relácií sa týkajú poverení potrebných overenie identity lokálneho administrátora v rámci relácie systému Windows.

Štandardne sú nové alebo zmenené zásady presadené okamžite po klepnutí alebo kliknutí na tlačidlo **Apply** (Použiť).

Pridanie novej zásady:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na ikonu **ozubeného kolieska**.
2. Na stránke Advanced Settings (Rozšírené nastavenia) kliknite alebo klepnite na položku **Administrator Policies** (Zásady administrátorov).
3. Kliknite alebo klepnite na položku **Add new policy** (Pridať novú zásadu).
4. Kliknutím na šípky nadol vyberte primárne a sekundárne (nepovinné) poverenia pre novú zásadu a potom kliknite alebo klepnite na tlačidlo **Add** (Pridať).
5. Kliknite na tlačidlo **Použiť**.

Oneskorenie presadenia novej alebo zmenenej zásady:

1. Kliknite alebo klepnite na položku **Enforce this policy immediately** (Vynútiť túto zásadu okamžite).
2. Vyberte možnosť **Enforce this policy on the specific date** (Vynútiť túto zásadu v určený deň).
3. Zadajte dátum alebo použite kontextový kalendár a vyberte dátum, kedy má byť táto zásada presadená.
4. V prípade potreby vyberte, kedy má byť používateľovi pripomenutá nová zásada.
5. Kliknite na tlačidlo **Použiť**.

Zásady bežných používateľov

Môžete nakonfigurovať zásady prihlasovania a relácií pre bežných používateľov tohto počítača. Tu nastavené zásady prihlasovania sa týkajú poverení potrebných na prihlásenie bežného používateľa do systému Windows. Tu nastavené zásady relácií sa týkajú poverení potrebných overenie identity bežného používateľa v rámci relácie systému Windows.

Štandardne sú nové alebo zmenené zásady presadené okamžite po klepnutí alebo kliknutí na tlačidlo **Apply** (Použiť).

Pridanie novej zásady:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na ikonu **ozubeného kolieska**.
2. Na stránke Advanced Settings (Rozšírené nastavenia) kliknite alebo klepnite na položku **Standard User Policies** (Zásady bežných používateľov).
3. Kliknite alebo klepnite na položku **Add new policy** (Pridať novú zásadu).
4. Kliknutím na šípky nadol vyberte primárne a sekundárne (nepovinné) poverenia pre novú zásadu a potom kliknite alebo klepnite na tlačidlo **Add** (Pridať).
5. Kliknite na tlačidlo **Použiť**.

Oneskorenie presadenia novej alebo zmenenej zásady:

1. Kliknite alebo klepnite na položku **Enforce this policy immediately** (Vynútiť túto zásadu okamžite).
2. Vyberte možnosť **Enforce this policy on the specific date** (Vynútiť túto zásadu v určený deň).
3. Zadajte dátum alebo použite kontextový kalendár a vyberte dátum, kedy má byť táto zásada presadená.

4. V prípade potreby vyberte, kedy má byť používateľovi pripomenutá nová zásada.
5. Kliknite na tlačidlo **Použiť**.

Bezpečnostné funkcie

Môžete aktivovať bezpečnostné funkcie aplikácie HP Client Security, ktoré pomáhajú ochrániť pred nepovoleným prístupom k počítaču.

Nastavenie bezpečnostných funkcií:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na ikonu **ozubeného kolieska**.
2. Na stránke Advanced Settings (Rozšírené nastavenia) kliknite alebo klepnite na položku **Security Features** (Bezpečnostné funkcie).
3. Začiarknutím políčok aktivujte bezpečnostné funkcie a potom kliknite alebo klepnite na tlačidlo **Apply** (Použiť). Čím viac funkcií vyberiete, tým bezpečnejší počítač bude.

   Tieto nastavenia sa týkajú všetkých používateľov.

   - **Windows Logon Security** (Zabezpečenie prihlásenia do systému Windows) – chráni vaše kontá systému Windows vyžadovaním poverení aplikácie HP Client Security pri prístupe ku kontu.
   - **Pre-Boot Security (Power-on authentication)** (Zabezpečenie pri spúšťaní (overovanie pri zapnutí)) – chráni váš počítač pred spustením systému Windows. Táto voľba nie je k dispozícii, ak ju BIOS nepodporuje.
   - **Allow One Step logon** (Povoliť prihlásenie v jednom kroku) – toto nastavenie umožňuje preskočiť prihlasovanie do systému Windows, ak bolo predtým urobené overenie pri zapnutí alebo na úrovni funkcie Šifrovanie jednotky.
4. Kliknite alebo klepnite na položku **Users** (Používatelia) a potom kliknite alebo klepnite na dlaždicu používateľa.

Používatelia

Môžete monitorovať a spravovať používateľov aplikácie HP Client Security na tomto počítači.

Pridanie ďalšieho používateľa systému Windows do aplikácie HP Client Security:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na ikonu **ozubeného kolieska**.
2. Na stránke Advanced Settings (Rozšírené nastavenia) kliknite alebo klepnite na položku **Users** (Používatelia).
3. Kliknite alebo klepnite na položku **Add another Windows user to HP Client Security** (Pridať ďalšieho používateľa Windows do aplikácie HP Client Security).
4. Zadajte meno používateľa, ktorého chcete pridať, a potom kliknite alebo klepnite na tlačidlo **OK**.
5. Zadajte heslo používateľa do systému Windows.

   Dlaždica pridaného používateľa sa zobrazuje na stránke Používatelia.

Odstránenie používateľa systému Windows z aplikácie HP Client Security:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na ikonu **ozubeného kolieska**.
2. Na stránke Advanced Settings (Rozšírené nastavenia) kliknite alebo klepnite na položku **Users** (Používatelia).
3. Kliknite alebo klepnite na meno používateľa, ktorého chcete odstrániť.
4. Kliknite alebo klepnite na tlačidlo **Delete User** (Odstrániť používateľa) a potom potvrďte kliknutím alebo klepnutím na tlačidlo **Yes** (Áno).

Zobrazenie prehľadu zásad prihlasovania a relácií vynútených pre používateľa:

- ▲ Kliknite alebo klepnite na položku **Users** (Používatelia) a potom kliknite alebo klepnite na dlaždicu používateľa.

Moje zásady

Môžete zobraziť svoje zásady overovania a stav registrácie. Stránka Moje zásady tiež obsahuje prepojenia na stránky Zásady administrátorov a Zásady bežných používateľov.

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na ikonu **ozubeného kolieska**.
2. Na stránke Advanced Settings (Rozšírené nastavenia) kliknite alebo klepnite na položku **My Policies** (Moje zásady).

   Zobrazujú sa zásady prihlasovania a relácií pre práve prihláseného používateľa.

Stránka Moje zásady tiež obsahuje prepojenia na Zásady administrátorov na strane 25 a Zásady bežných používateľov na strane 26.

Zálohovanie a obnovenie údajov

Odporúča sa, aby ste pravidelne zálohovali svoje údaje aplikácie HP Client Security. Frekvencia zálohovania závisí od toho, ako často meníte údaje. Ak napríklad pridávate denne nové prihlásenia, mali by ste zálohovať údaje každý deň.

Zálohy sa tiež dajú využiť pri migrácii z jedného počítača na druhý. Nazývame to tiež import a export.

POZNÁMKA: Touto funkciou je zálohovaný len Správca hesiel. Šifrovanie jednotky má nezávislý spôsob zálohovania. Device Access Manager a údaje o overovaní odtlačkom prsta nie sú zálohované.

Pred obnovením údajov zo súboru zálohy musí byť na počítači, na ktorý majú byť dodané údaje, nainštalovaná aplikácia HP Client Security.

Zálohovanie údajov:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na ikonu **ozubeného kolieska**.
2. Na stránke Advanced Settings (Rozšírené nastavenia) kliknite alebo klepnite na položku **Administrator Policies** (Zásady administrátorov).
3. Kliknite alebo klepnite na položku **Backup and Restore** (Zálohovať a obnoviť).
4. Kliknite alebo klepnite na položku **Backup** (Zálohovať) a potom overte svoju identitu.

5. Vyberte modul, ktorý chcete zahrnúť do zálohy, a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).
6. Zadajte názov uschovávaného súboru. Štandardne je súbor uložený do priečinka Dokumenty. Ak chcete určiť iné miesto, kliknite alebo klepnite na tlačidlo **Browse** (Prehľadávať).
7. Zadajte a potvrďte heslo na ochranu súboru.
8. Kliknite alebo klepnite na tlačidlo **Save** (Uložiť).

Obnovenie údajov:

1. Na úvodnej stránke aplikácie HP Client Security kliknite alebo klepnite na ikonu **ozubeného kolieska**.
2. Na stránke Advanced Settings (Rozšírené nastavenia) kliknite alebo klepnite na položku **Administrator Policies** (Zásady administrátorov).
3. Kliknite alebo klepnite na položku **Backup and Restore** (Zálohovať a obnoviť).
4. Vyberte možnosť **Restore** (Obnoviť) a potom overte svoju identitu.
5. Vyberte predtým vytvorený súbor zálohy. Do zobrazeného políčka zadajte cestu. Ak chcete určiť iné miesto, kliknite alebo klepnite na tlačidlo **Browse** (Prehľadávať).
6. Zadajte heslo použité na ochranu súboru a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).
7. Vyberte moduly, ktorých údaje chcete obnoviť.
8. Kliknite alebo klepnite na tlačidlo **Restore** (Obnoviť).

5 HP Drive Encryption (len vybrané modely)

Program HP Drive Encryption poskytuje komplexnú ochranu údajov šifrovaním počítačových údajov. Keď je aktivované Šifrovanie jednotky, je potrebné sa prihlásiť na prihlasovacej obrazovke funkcie Šifrovanie jednotky, ktorá je zobrazená pred spustením operačného systému Windows®.

Úvodná obrazovka aplikácie HP Client Security umožňuje administrátorom systému Windows aktivovať Šifrovanie jednotky, zálohovať šifrovací kľúč a vybrať alebo zrušiť výber oddielov na jednotkách, ktoré majú byť šifrované. Ďalšie informácie nájdete v Pomocníkovi k softvéru HP Client Security.

S funkciou Šifrovanie jednotky sa dajú vykonávať tieto úlohy:

- Výber nastavení funkcie Šifrovanie jednotky:
  - Šifrovanie alebo dešifrovanie jednotlivých jednotiek alebo oddielov pomocou softvérového šifrovania
  - Šifrovanie alebo dešifrovanie jednotlivých samošifrovacích jednotiek pomocou hardvérového šifrovania
  - Pridanie ďalšieho zabezpečenia vypnutím režimu spánku a pohotovostného režimu zaistí, že vždy je vyžadované overovanie funkciou Šifrovanie jednotky pri spustení

POZNÁMKA: Šifrovať je možné len interné SATA a externé eSATA pevné disky.

- Vytváranie záložných kľúčov
- Obnovenie prístupu k zašifrovanému počítaču pomocou záložných kľúčov a funkcie HP SpareKey
- Aktivovanie overenia funkciou Šifrovanie jednotky pri spúšťaní pomocou hesla, registrovaného odtlačku prsta alebo kódu PIN pre vybrané karty Smart

Otvorenie programu Šifrovanie jednotky

Administrátori majú prístup k programu Šifrovanie jednotky po otvorení aplikácie HP Client Security:

1. Na obrazovke Štart kliknite alebo klepnite na aplikáciu **HP Client Security** (Windows 8).

   – alebo –

   Na pracovnej ploche systému Windows dvakrát kliknite alebo dvakrát klepnite na ikonu aplikácie **HP Client Security** v oblasti oznámení na paneli úloh úplne vpravo.

2. Kliknite alebo klepnite na ikonu **Drive Encryption** (Šifrovanie jednotky).

Všeobecné úlohy

Aktivovanie funkcie Šifrovanie jednotky pre bežné pevné disky

Bežné pevné disky sú šifrované pomocou softvérového šifrovania. Pri šifrovaní jednotky alebo oddielu na disku postupujte takto:

1. Spustite **Drive Encryption** (Šifrovanie jednotky). Ďalšie informácie nájdete v časti Otvorenie programu Šifrovanie jednotky na strane 30.
2. Začiarknite políčko jednotky alebo oddielu, ktoré chcete zašifrovať, a potom kliknite alebo klepnite na položku **Záložný kľúč**.

POZNÁMKA: Pre lepšie zabezpečenie začiarknite možnosť **Disable sleep mode for increased security** (Vypnúť režim spánku pre zvýšenú bezpečnosť). Keď vypnete režim spánku, nie je vôbec žiadne riziko, že by boli poverenia použité na odomknutie jednotky uložené v pamäti.

3. Vyberte jednu alebo viac možností zálohovania a potom kliknite alebo klepnite na položku **Backup** (Zálohovať). Ďalšie informácie nájdete v časti Zálohovanie šifrovacích kľúčov na strane 34.
4. Počas zálohovania šifrovacieho kľúča môžete pokračovať v práci. Nereštartujte počítač.

POZNÁMKA: Objaví sa výzva na reštartovanie počítača. Po reštartovaní sa pred spustením systému Windows zobrazí obrazovka šifrovania jednotky pri spúšťaní vyžadujúca overenie.

Šifrovanie jednotky bolo aktivované. Zašifrovanie vybraných oddielov môže trvať niekoľko hodín, závisí to od počtu a veľkosti oddielov.

Ďalšie informácie nájdete v Pomocníkovi k softvéru HP Client Security.

Aktivovanie funkcie Šifrovanie jednotky pre samošifrovacie jednotky

Samošifrovacie jednotky spĺňajúce normu OPAL od Trusted Computing Group pre správu samošifrovacích jednotiek je možné zašifrovať pomocou softvérového alebo hardvérového šifrovania. Hardvérové šifrovanie je oveľa rýchlejšie než softvérové šifrovanie. Nie je však možné zvoliť, ktoré diskové oddiely majú byť šifrované. Zašifrovaný je celý disk vrátane všetkých diskových oddielov.

Ak chcete zašifrovať konkrétne oddiely, je potrebné použiť softvérové šifrovanie. Nezabudnite zrušiť začiarknutie políčka **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Povoliť len hardvérové šifrovanie pre samošifrovacie jednotky (SED)).

Šifrovanie jednotky pre samošifrovacie jednotky aktivujte podľa tohto postupu:

1. Spustite **Drive Encryption** (Šifrovanie jednotky). Ďalšie informácie nájdete v časti Otvorenie programu Šifrovanie jednotky na strane 30.
2. Začiarknite políčko jednotky, ktorú chcete zašifrovať, a potom kliknite alebo klepnite na položku **Backup Key** (Záložný kľúč).

POZNÁMKA: Pre lepšie zabezpečenie začiarknite políčko **Disable Sleep Mode for added security** (Vypnúť režim spánku pre zvýšenú bezpečnosť). Keď vypnete režim spánku, nie je vôbec žiadne riziko, že by boli poverenia použité na odomknutie jednotky uložené v pamäti.

3. Vyberte jednu alebo viac možností zálohovania a potom kliknite alebo klepnite na položku **Backup** (Zálohovať). Ďalšie informácie nájdete v časti Zálohovanie šifrovacích kľúčov na strane 34.

4. Počas zálohovania šifrovacieho kľúča môžete pokračovať v práci. Nereštartujte počítač.

POZNÁMKA: Pre samošifrovacie jednotky sa objaví výzva na vypnutie počítača.

Ďalšie informácie nájdete v Pomocníkovi k softvéru HP Client Security.

Deaktivovanie funkcie Šifrovanie jednotky

1. Spustite **Drive Encryption** (Šifrovanie jednotky). Ďalšie informácie nájdete v časti Otvorenie programu Šifrovanie jednotky na strane 30.

2. Zrušte začiarknutie políčka pri všetkých šifrovaných jednotkách a potom kliknite alebo klepnite na tlačidlo **Apply** (Použiť).

   Spustí sa deaktivovanie funkcie Šifrovanie jednotky.

POZNÁMKA: Ak bolo použité softvérové šifrovanie, spustí sa dešifrovanie. Môže to trvať niekoľko hodín, závisí to do veľkosti zašifrovaných oddielov na pevnom disku. Keď bude dešifrovanie dokončené, funkcia Šifrovanie jednotky je deaktivovaná.

Ak bolo použité hardvérové dešifrovanie, jednotka je dešifrovaná okamžite a po niekoľkých minútach je funkcia Šifrovanie jednotky deaktivovaná.

Keď je už funkcia Šifrovanie jednotky deaktivovaná, objaví sa výzva na vypnutie počítača, ak bolo šifrované hardvérovo. Ak bolo šifrované softvérovo, objaví sa výzva na reštartovanie počítača.

Prihlásenie po aktivovaní funkcie Šifrovanie jednotky

Keď po aktivovaní funkcie Šifrovanie jednotky a registrácii používateľského konta zapnete počítač, je potrebné sa prihlásiť na prihlasovacej obrazovke funkcie Šifrovanie jednotky:

POZNÁMKA: Keď sa počítač prebúdza z režimu spánku alebo pohotovostného režimu, overovanie funkciou Šifrovanie jednotky pri spúšťaní nie je pri softvérovom ani hardvérovom šifrovaní zobrazené. Hardvérové šifrovanie poskytuje možnosť **Disable sleep mode for increased security** (Vypnúť režim spánku pre lepšiu bezpečnosť), ktorá po aktivovaní zabraňuje v režime spánku alebo pohotovostnom režime.

Keď sa počítač prebúdza z režimu dlhodobého spánku, overovanie funkciou Šifrovanie jednotky pri spúšťaní je pri softvérovom aj hardvérovom šifrovaní zobrazené.

POZNÁMKA: Ak administrátor systému Windows aktivoval pre BIOS funkciu zabezpečenia na úrovni pri spúšťaní v aplikácii HP Client Security a je povolené prihlásenie v jednom kroku (predvolené), môžete sa prihlásiť na počítač okamžite po overení pri spúšťaní BIOS-u bez toho, aby bolo potrebné opätovné overenie na prihlasovacej obrazovke funkcie Šifrovanie jednotky.

Prihlásenie jedného používateľa:

- Na stránke **Logon** (Prihlásenie) zadajte svoje heslo do systému Windows, kód PIN pre kartu Smart alebo nasnímajte registrovaný prst.

Prihlásenie viacerých používateľov:

1. Na stránke **Select user to logon** (Vyberte používateľa na prihlásenie) vyberte v rozbaľovacom zozname používateľa na prihlásenie a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).
2. Na stránke **Logon** (Prihlásenie) zadajte svoje heslo do systému Windows, prípadne kód PIN pre kartu Smart alebo nasnímajte registrovaný prst.

POZNÁMKA: Podporované sú nasledujúce karty:

Podporované karty Smart

- Gemalto Cyberflex Access 64k V2c

POZNÁMKA: Ak je na prihlasovacej obrazovke funkcie Šifrovanie jednotky použitý kľúč obnovenia, na prístup k používateľským kontám sú pri prihlasovaní do systému Windows potrebné ďalšie poverenia.

Šifrovanie ďalších pevných diskov

Dôrazne odporúčame, aby ste na ochranu údajov zašifrovaním pevného disku použili program HP Drive Encryption. Po aktivovaní je možné zašifrovať všetky pridané pevné disky alebo vytvorené oddiely podľa tohto postupu:

1. Spustite **Drive Encryption** (Šifrovanie jednotky). Ďalšie informácie nájdete v časti Otvorenie programu Šifrovanie jednotky na strane 30.
2. Pri softvérovo šifrovaných jednotkách vyberte oddiely jednotky, ktoré majú byť zašifrované.

   POZNÁMKA: To sa týka tiež situácie so zmiešanými jednotkami, kde je jeden alebo viac pevných diskov a jedna alebo viac samošifrovacích jednotiek.

– alebo –

▲ Pri hardvérovo šifrovaných jednotkách vyberte oddiely jednotky, ktoré majú byť zašifrované.

Pokročilé úlohy

Spravovanie funkcie Šifrovanie jednotky (administrátorská úloha)

Administrátori môžu použiť Šifrovanie jednotky na prezeranie a zmenu stavu šifrovania (Nezašifrované alebo Zašifrované) pre všetky pevné disky v počítači.

- Ak je stav Aktivované, Šifrovanie jednotky bolo aktivované a nakonfigurované. Jednotka je v jednom z týchto stavov:

Softvérové šifrovanie

- Nezašifrované
- Zašifrované
- Šifrovanie
- Dešifrovanie

Hardvérové šifrovanie

- Zašifrované
- Nezašifrované (pre ďalšie jednotky)

Šifrovanie alebo dešifrovanie jednotlivých diskových oddielov (len softvérové šifrovanie)

Administrátori môžu použiť Šifrovanie jednotky na zašifrovanie jedného alebo viacerých oddielov na pevnom disku v počítači alebo dešifrovanie oddielov jednotky, ktoré už boli zašifrované.

1. Spustite **Drive Encryption** (Šifrovanie jednotky). Ďalšie informácie nájdete v časti Otvorenie programu Šifrovanie jednotky na strane 30.
2. V časti **Drive Status** (Stav jednotky) začiarknite alebo zrušte začiarknutie políčka vedľa jednotlivých oddielov pevného disku, ktoré chcete zašifrovať alebo dešifrovať, a potom kliknite alebo klepnite na tlačidlo **Apply** (Použiť).

POZNÁMKA: Keď sa oddiel šifruje alebo dešifruje, zobrazuje sa lišta priebehu s percentom šifrovania oddielu.

POZNÁMKA: Dynamické oddiely nie sú podporované. Ak sa jednotka zobrazuje ako dostupná, ale nedá sa po výbere zašifrovať, ide o dynamický oddiel. Dynamický oddiel vzniká pri vytváraní nového oddielu rozdelením oddielu vo funkcii Správa diskov.

Ak bude oddiel prevedený na dynamický, zobrazuje sa upozornenie.

Správa diskov

- **Nickname** (Prezývka) – pre ľahšiu identifikáciu môžete jednotky alebo oddiely pomenovať.
- **Disconnected drives** (Odpojené jednotky) – funkcia Šifrovanie jednotky môže sledovať disky, ktoré sú od počítača odpojené. Disk, ktorý je od počítača odpojený, sa automaticky presunie do zoznamu Odpojené. Ak sa disk vráti do systému, znova sa objaví v zozname Pripojené.
- Ak už nepotrebujete sledovať alebo spravovať odpojenú jednotku, môžete odpojenú jednotku odstrániť zo zoznamu Odpojené.
- Šifrovanie jednotky zostane aktivované, kým nie je zrušené začiarknutie všetkých pripojených jednotiek a zoznam Odpojené nie je prázdny.

Zálohovanie a obnovenie (administrátorská úloha)

Keď je aktivované Šifrovanie jednotky, administrátori môžu použiť stránku Zálohovanie šifrovacieho kľúča na zálohovanie šifrovacích kľúčov na vymeniteľné médium a vykonávanie obnovenia.

Zálohovanie šifrovacích kľúčov

Administrátori môžu zálohovať šifrovací kľúč pre zašifrovanú jednotku na vymeniteľné ukladacie zariadenie.

UPOZORNENIE: Nezabudnite uschovať ukladacie zariadenie obsahujúce záložný kľúč na bezpečnom mieste, pretože ak zabudnete heslo, stratíte kartu Smart alebo nemáte zaregistrovaný odtlačok prsta, zariadenie poskytuje jediný prístup k počítaču. Miesto uschovania musí tiež byť bezpečné, pretože ukladacie zariadenie umožňuje prístup do systému Windows.

1. Spustite **Drive Encryption** (Šifrovanie jednotky). Ďalšie informácie nájdete v časti Otvorenie programu Šifrovanie jednotky na strane 30.
2. Začiarknite políčko jednotky a potom kliknite alebo klepnite na tlačidlo **Backup Key** (Záložný kľúč).
3. V položke **Create HP Drive Encryption recovery key** (Vytvoriť kľúč obnovenia pre HP Drive Encryption) vyberte jednu alebo viaceré nasledujúce možnosti:
   - **Removable Storage** (Vymeniteľné ukladacie zariadenie) – začiarknite políčko a potom vyberte ukladacie zariadenie, na ktoré bude šifrovací kľúč uložený.
   - **SkyDrive** – začiarknite políčko. Je potrebné pripojenie na internet. Prihláste sa k službe Microsoft SkyDrive a potom kliknite alebo klepnite na tlačidlo **Yes** (Áno).

     POZNÁMKA: Ak chcete použiť záložný kľúč programu HP Drive Encryption, ktorý je uložený na službe SkyDrive, musíte ho prevziať zo služby SkyDrive na vymeniteľné ukladacie zariadenie a potom pripojiť ukladacie zariadenie k počítaču.
   - **TPM** (len vybrané modely) – umožňuje obnoviť údaje pomocou hesla TPM.

     UPOZORNENIE: Ak je TPM vymazané alebo je počítač poškodený, stratíte prístup k zálohe. Ak je vybraný tento spôsob, zvoliť sa dá tiež ďalší spôsob zálohovania.
4. Kliknite alebo klepnite na tlačidlo **Backup** (Zálohovať).

   Šifrovací kľúč bude uložený do vybraného ukladacieho zariadenia.

Obnovenie prístupu k aktivovanému počítaču pomocou záložných kľúčov

Administrátori môžu vykonávať obnovenie pomocou kľúča funkcie Šifrovanie jednotky, ktorý je zálohovaný na vymeniteľnom ukladacom zariadení pri aktivácii alebo zvolením možnosti **Backup Key** (Záložný kľúč) vo funkcii Šifrovanie jednotky.

1. Pripojte vymeniteľné ukladacie zariadenie obsahujúce záložný kľúč.
2. Zapnite počítač.
3. Keď sa otvorí prihlasovacie dialógové okno programu HP Drive Encryption, kliknite alebo klepnite na tlačidlo **Recovery** (Obnoviť).
4. Zadajte cestu k súboru alebo názov záložného kľúča a potom kliknite alebo klepnite na tlačidlo **Recovery** (Obnoviť).
5. Keď sa objaví dialógové okno potvrdenia, kliknite alebo klepnite na tlačidlo **OK**.

   Zobrazí sa obrazovka prihlásenia do systému Windows.

POZNÁMKA: Ak je na prihlasovacej obrazovke funkcie Šifrovanie jednotky použitý na prihlásenie kľúč obnovenia, na prístup k používateľským kontám pri prihlásení do systému Windows sú potrebné ďalšie poverenia. Po vykonaní obnovenia sa dôrazne odporúča vynulovať heslo.

Vykonanie obnovenia pomocou HP SpareKey

Obnovenie SpareKey v rámci overenia funkciou Šifrovanie jednotky pri spúšťaní vyžaduje, aby ste pred prístupom k počítaču správne odpovedali na bezpečnostné otázky. Ďalšie informácie o nastavení funkcie Obnovenie SpareKey nájdete v Pomocníkovi k softvéru HP Client Security.

Ako vykonať Obnovenie HP SpareKey v prípade zabudnutého hesla:

1. Zapnite počítač.
2. Keď sa zobrazí stránka aplikácie HP Drive Encryption, prejdite na obrazovku prihlásenia používateľa.
3. Kliknite na tlačidlo **SpareKey**.

   POZNÁMKA: Ak SpareKey nebol v aplikácii HP Client Security inicializovaný, tlačidlo **SpareKey** nie je k dispozícii.

4. Napíšte správne odpovede na zobrazené otázky a potom kliknite na tlačidlo **Logon** (Prihlásenie).

   Zobrazí sa obrazovka prihlásenia do systému Windows.

POZNÁMKA: Ak je na prihlasovacej obrazovke funkcie Šifrovanie jednotky použitý na prihlásenie SpareKey, na prístup k používateľským kontám pri prihlásení do systému Windows sú potrebné ďalšie poverenia. Po vykonaní obnovenia sa dôrazne odporúča vynulovať heslo.

6 HP File Sanitizer (len vybrané modely)

Aplikácia File Sanitizer umožňuje bezpečne skartovať aktíva (napríklad: osobné údaje alebo súbory, historické alebo webové údaje alebo iné údajové súčasti) na internom pevnom disku počítača a pravidelne dôkladne vyčistiť interný pevný disk počítača.

Program File Sanitizer nie je možné používať na vyčistenie alebo dôkladné vymazanie nasledujúcich typov jednotiek:

- jednotky Solid-state (SSD) vrátane zväzkov RAID zahŕňajúcich SSD zariadenie
- externé jednotky pripojené cez rozhranie USB, FireWire alebo eSATA

Ak je vykonaný pokus o skartovanie alebo dôkladné vyčistenie na jednotke SSD, zobrazí sa hlásenie s upozornením a úkon sa nevykoná.

Skartovanie

Skartovanie sa odlišuje od bežného úkonu odstránenia v systéme Windows®. Keď skartujete aktívum pomocou programu File Sanitizer, súbory sú prepísané bezvýznamnými údajmi, vďaka čomu je virtuálne nemožné získať pôvodnú položku. Jednoduchý úkon odstránenia v systéme Windows môže ponechať súbor (alebo aktívum) na pevnom disku neporušený, prípadne v stave, kedy je možné na jeho obnovenie použiť súdne spôsoby.

Môžete naplánovať čas skartovania do budúcnosti, prípadne môžete skartovanie aktivovať ručne pomocou ikony programu **File Sanitizer** na úvodnej obrazovke aplikácie HP Client Security, prípadne pomocou ikony **File Sanitizer** na pracovnej ploche systému Windows. Ďalšie informácie viď Nastavenie plánu skartovania na strane 39, Skartovanie pravým tlačidlom myši na strane 41 alebo Ručné spustenie úkonu skartovania na strane 42.

POZNÁMKA: Súbor vo formáte .dll je skartovaný a odstránený zo systému len vtedy, ak bol presunutý do Koša.

Dôkladné čistenie voľného miesta

Pri odstránení aktíva v systéme Windows nie je z pevného disku úplne odstránený obsah aktíva. Systém Windows odstráni len odkaz na aktívum, prípadne jeho umiestnenie na pevnom disku. Obsah aktíva stále zostáva na jednotke pevného disku, dokým iná položka neprepíše rovnakú oblasť na pevnom disku novými údajmi.

Čistenie voľného miesta vám umožňuje bezpečne zapísať náhodné údaje do odstránených aktív, čo zabráni používateľom prezerať pôvodný obsah odstráneného aktíva.

POZNÁMKA: Čistenie voľného miesta neposkytuje dodatočnú bezpečnosť skartovaným aktívam.

Čistenie voľného miesta môžete naplánovať do budúcnosti alebo môžete ručne aktivovať čistenie voľného miesta predtým skartovaných aktív pomocou ikony **File Sanitizer** na úvodnej stránke aplikácie HP Client Security, prípadne pomocou ikony **File Sanitizer** na pracovnej ploche systému Windows. Ďalšie informácie viď Nastavenie plánu dôkladného čistenia voľného miesta na strane 40, Ručné spustenie úkonu dôkladného čistenia voľného miesta na strane 42 alebo Používanie ikony programu File Sanitizer na strane 41.

Otvorenie programu File Sanitizer

1. Na obrazovke Štart kliknite alebo klepnite na aplikáciu **HP Client Security** (Windows 8).

   – alebo –

   Na pracovnej ploche systému Windows dvakrát kliknite alebo dvakrát klepnite na ikonu aplikácie **HP Client Security** v oblasti oznámení na paneli úloh úplne vpravo.

2. V časti **Data** (Údaje) kliknite alebo klepnite na položku **File Sanitizer**.

– alebo –

- Dvakrát kliknite alebo dvakrát klepnite na ikonu **File Sanitizer** na pracovnej ploche systému Windows.

– alebo –

- Kliknite pravým tlačidlom na ikonu programu **File Sanitizer** na pracovnej ploche systému Windows, prípadne na ňu klepnite a podržte, a potom vyberte položku **Open File Sanitizer** (Otvoriť File Sanitizer).

Postupy nastavenia

Shredding (Skartovanie) – program File Sanitizer bezpečne odstráni alebo skartuje vybrané kategórie aktív.

1. V časti **Skartovanie** začiarknite políčka jednotlivých typov súborov, ktoré majú byť skartované, prípadne zrušte začiarknutie políčka, ak tieto súbory nechcete skartovať.

   - **Recycle Bin** (Kôš) – skartujú sa všetky položky umiestnené v Koši.
   - **Temporary system files** (Dočasné systémové súbory) – skartujú sa všetky súbory nájdené v priečinku dočasných systémových súborov. Vyhľadávajú sa nasledujúce premenné prostredie v tomto poradí a prvá nájdená cesta sa považuje za systémový priečinok:
     - TMP
     - TEMP
   - **Temporary Internet files** (Dočasné internetové súbory) – skartujú sa kópie webových stránok, obrázkov a médií, ktoré sú v rámci rýchlejšieho zobrazovania ukladané webovými prehľadávačmi.
   - **Cookies** (Súbory cookie) – v počítači sa skartujú všetky súbory uložené webovými stránkami z dôvodu ukladania predvolieb, ako sú napríklad prihlasovacie údaje.

2. Ak chcete spustiť skartovanie, kliknite alebo klepnite na položku **Shred** (Skartovať).

Bleaching (Čistenie) – do voľného miesta sa zapisujú náhodné údaje a zabraňuje sa obnoveniu odstránených položiek.

- Ak chcete spustiť čistenie, kliknite alebo klepnite na položku **Bleach** (Vyčistiť).

File Sanitizer Options (Možnosti programu File Sanitizer) – začiarknutím políčka môžete aktivovať nasledujúce možnosti, prípadne zrušením začiarknutia voľbu deaktivujte:

- **Enable Desktop icon** (Povoliť ikonu na ploche) – zobrazuje ikonu programu File Sanitizer na pracovnej ploche systému Windows.
- **Enable right-click** (Povoliť kliknutie pravým tlačidlom) – umožňuje kliknúť pravým tlačidlom myši na aktívum (alebo na neho klepnúť a podržať) a potom vybrať položku **HP File Sanitizer – Shred** (HP File Sanitizer – Skartovať).
- **Ask for Windows password before manual shredding** (Vyžadovať heslo do systému Windows pred ručným skartovaním) – pred ručným skartovaním položky sa vyžaduje overenie heslom do systému Windows.
- **Shred Cookies and Temporary Internet Files on browser close** (Skartovať súbory cookie a dočasné internetové súbory pri zatvorení prehľadávača) – keď zatvoríte webový prehľadávač, skartujú sa všetky s webom súvisiace aktíva, ako je napríklad história URL adries.

Nastavenie plánu skartovania

Môžete naplánovať čas automatického skartovania, prípadne tiež môžete aktíva skartovať kedykoľvek ručne. Ďalšie informácie nájdete v časti Postupy nastavenia na strane 38.

1. Otvorte program File Sanitizer a potom kliknite alebo klepnite na položku **Settings** (Nastavenie).
2. Ak chcete naplánovať do budúcnosti skartovanie vybraných aktív, v časti **Shred Schedule** (Plán skartovania) vyberte položku **Never** (Nikdy), **Once** (Raz), **Daily** (Denne), **Weekly** (Týždenne) alebo **Monthly** (Mesačne) a potom vyberte deň a čas:
   a. Kliknite alebo klepnite na hodinu, minútu alebo políčko Dopoludnia/Popoludní.
   b. Listujte, kým sa požadovaná hodnota nezobrazí na rovnakej úrovni ako ostatné políčka.
   c. Kliknite alebo klepnite na biele miesto okolo políčok nastavenia času.
   d. Opakujte pri jednotlivých políčkach, kým nebude vybraný správny plán.
3. Uvedené sú nasledujúce štyri typy aktív:
   - **Recycle Bin** (Kôš) – skartujú sa všetky položky umiestnené v Koši.
   - **Temporary system files** (Dočasné systémové súbory) – skartujú sa všetky súbory nájdené v priečinku dočasných systémových súborov. Vyhľadávajú sa nasledujúce premenné prostredie v tomto poradí a prvá nájdená cesta sa považuje za systémový priečinok:
     - TMP
     - TEMP
   - **Temporary Internet files** (Dočasné internetové súbory) – skartujú sa kópie webových stránok, obrázkov a médií, ktoré sú v rámci rýchlejšieho zobrazovania ukladané webovými prehľadávačmi.
   - **Cookies** (Súbory cookie) – v počítači sa skartujú všetky súbory uložené webovými stránkami z dôvodu ukladania predvolieb, ako sú napríklad prihlasovacie údaje.

Ak je táto položka označená, v naplánovanom čase budú tieto aktíva skartované.

4. Ako vybrať ďalšie vlastné aktíva na skartovanie:

   a. V časti **Scheduled Shred List** (Zoznam plánovaného skartovania) kliknite alebo klepnite na položku **Add folder** (Pridať priečinok) a potom prejdite na súbor alebo priečinok.

   b. Kliknite alebo klepnite na tlačidlo **Open** (Otvoriť) a potom kliknite alebo klepnite na tlačidlo **OK**.

   Ak chcete odstrániť aktívum zo Zoznamu plánovaného skartovania, zrušte začiarknutie políčka aktíva.

Nastavenie plánu dôkladného čistenia voľného miesta

Čistenie voľného miesta neposkytuje dodatočnú bezpečnosť skartovaným aktívam.

1. Otvorte program File Sanitizer a potom kliknite alebo klepnite na položku **Settings** (Nastavenie).
2. Ak chcete do budúcnosti naplánovať čistenie pevného disku, v časti **Bleach Schedule** (Plán čistenia) vyberte položku **Never** (Nikdy), **Once** (Raz), **Daily** (Denne), **Weekly** (Týždenne) alebo **Monthly** (Mesačne) a potom vyberte deň a čas.

   a. Kliknite alebo klepnite na hodinu, minútu alebo políčko Dopoludnia/Popoludní.

   b. Listujte, kým sa požadovaný čas nezobrazí na rovnakej úrovni ako ostatné políčka.

   c. Kliknite alebo klepnite na biele miesto okolo políčok nastavenia času.

   d. Opakujte, kým nebude zvolený správny plán.

POZNÁMKA: Úkon dôkladného čistenia voľného miesta môže trvať veľmi dlho. Zaistite, aby bol počítač pripojený do elektrickej zásuvky. Hoci sa dôkladné čistenie voľného miesta vykonáva na pozadí, zvýšené zaťaženie procesora môže ovplyvniť výkon počítača. Dôkladné čistenie voľného miesta môže byť vykonávané po pracovnom čase, prípadne ak sa počítač nepoužíva.

Ochrana súborov pred skartovaním

Ako chrániť súbory alebo priečinky pred skartovaním:

1. Otvorte program File Sanitizer a potom kliknite alebo klepnite na položku **Settings** (Nastavenie).
2. V časti **Never Shred List** (Zoznam Nikdy neskartovať) kliknite alebo klepnite na položku **Add folder** (Pridať priečinok) a potom prejdite na súbor alebo priečinok.
3. Kliknite alebo klepnite na tlačidlo **Open** (Otvoriť) a potom kliknite alebo klepnite na tlačidlo **OK**.

POZNÁMKA: Súbory z tohto zoznamu sú chránené dovtedy, kým sa nachádzajú v zozname.

Ak chcete odstrániť aktívum zo zoznamu výnimiek, zrušte začiarknutie políčka aktíva.

Všeobecné úlohy

Program File Sanitizer použite na vykonávanie týchto úloh:

- **Use the File Sanitizer icon to initiate shredding** (Použiť ikonu programu File Sanitizer na spustenie skartovania) – potiahnite súbory na ikonu **File Sanitizer** na pracovnej ploche systému Windows. Podrobnosti viď Používanie ikony programu File Sanitizer na strane 41.
- **Manually shred a specific asset or all selected assets** (Ručne skartovať konkrétne aktívum alebo všetky vybrané aktíva) – skartovanie položiek kedykoľvek bez čakania na naplánovaný čas skartovania. Podrobnosti viď Skartovanie pravým tlačidlom myši na strane 41 alebo Ručné spustenie úkonu skartovania na strane 42.
- **Manually activate free space bleaching** (Ručne aktivovať dôkladné čistenie voľného miesta) – aktivovanie dôkladného čistenia voľného miesta kedykoľvek. Podrobnosti viď Ručné spustenie úkonu dôkladného čistenia voľného miesta na strane 42.
- **View the log files** (Zobraziť súbory denníka) – zobrazenie súborov denníka skartovania alebo dôkladného čistenia voľného miesta, ktoré obsahujú všetky chyby alebo zlyhania z posledného úkonu skartovania alebo dôkladného čistenia voľného miesta. Podrobnosti viď Prezeranie súborov denníka na strane 42.

POZNÁMKA: Úkon skartovania alebo dôkladného čistenia voľného miesta môže trvať veľmi dlho. Hoci sa skartovanie a dôkladné čistenie voľného miesta vykonáva na pozadí, zvýšené zaťaženie procesora môže ovplyvniť výkon počítača.

Používanie ikony programu File Sanitizer

UPOZORNENIE: Skartované aktíva sa nedajú obnoviť. Dôkladne zvážte, ktoré položky vyberáte na ručné skartovanie.

Keď spustíte ručne úkon skartovania, skartované budú položky z bežného zoznamu skartovania v zobrazení programu File Sanitizer (viď Postupy nastavenia na strane 38).

Úkon skartovania môžete spustiť ručne jedným z týchto spôsobov:

1. Otvorte program File Sanitizer (viď Otvorenie programu File Sanitizer na strane 38) a potom kliknite alebo klepnite na položku **Shred** (Skartovať).
2. Keď sa otvorí dialógové okno potvrdenia, uistite sa, či sú označené aktíva, ktoré chcete skartovať, a potom kliknite alebo klepnite na tlačidlo **OK**.

– alebo –

1. Kliknite pravým tlačidlom na ikonu programu **File Sanitizer** na pracovnej ploche systému Windows, prípadne na ňu klepnite a podržte, a potom kliknite alebo klepnite na položku **Shred Now** (Skartovať teraz).
2. Keď sa otvorí dialógové okno potvrdenia, uistite sa, či sú označené aktíva, ktoré chcete skartovať, a potom kliknite alebo klepnite na tlačidlo **Shred** (Skartovať).

Skartovanie pravým tlačidlom myši

UPOZORNENIE: Skartované aktíva sa nedajú obnoviť. Dôkladne zvážte, ktoré položky vyberáte na ručné skartovanie.

Ak bola v zobrazení programu File Sanitizer zvolená možnosť **Enable right-click shredding** (Povoliť skartovanie pravým tlačidlom myši), môžete skartovať aktívum takto:

1. Prejdite na dokument alebo priečinok, ktoré chcete skartovať.
2. Kliknite na súbor alebo priečinok pravým tlačidlom myši (prípadne na nich klepnite a podržte) a potom vyberte položku **HP File Sanitizer – Shred** (HP File Sanitizer – Skartovať).

Ručné spustenie úkonu skartovania

⚠ **UPOZORNENIE:** Skartované aktíva sa nedajú obnoviť. Dôkladne zvážte, ktoré položky vyberáte na ručné skartovanie.

Keď spustíte ručne úkon skartovania, skartované budú položky z bežného zoznamu skartovania v zobrazení programu File Sanitizer (viď Postupy nastavenia na strane 38).

Úkon skartovania môžete spustiť ručne jedným z týchto spôsobov:

1. Otvorte program File Sanitizer (viď Otvorenie programu File Sanitizer na strane 38) a potom kliknite alebo klepnite na položku **Shred** (Skartovať).
2. Keď sa otvorí dialógové okno potvrdenia, uistite sa, či sú označené aktíva, ktoré chcete skartovať, a potom kliknite alebo klepnite na tlačidlo **OK**.

– alebo –

1. Kliknite pravým tlačidlom na ikonu programu **File Sanitizer** na pracovnej ploche systému Windows, prípadne na ňu klepnite a podržte, a potom kliknite alebo klepnite na položku **Shred Now** (Skartovať teraz).
2. Keď sa otvorí dialógové okno potvrdenia, uistite sa, či sú označené aktíva, ktoré chcete skartovať, a potom kliknite alebo klepnite na tlačidlo **Shred** (Skartovať).

Ručné spustenie úkonu dôkladného čistenia voľného miesta

Keď spustíte ručne úkon čistenia, vyčistené budú položky z bežného zoznamu skartovania v zobrazení programu File Sanitizer (viď Postupy nastavenia na strane 38).

Úkon čistenia môžete spustiť ručne jedným z týchto spôsobov:

1. Otvorte program File Sanitizer (viď Otvorenie programu File Sanitizer na strane 38) a potom kliknite alebo klepnite na položku **Bleach** (Vyčistiť).
2. Keď sa objaví dialógové okno potvrdenia, kliknite alebo klepnite na tlačidlo **OK**.

– alebo –

1. Kliknite pravým tlačidlom na ikonu programu **File Sanitizer** na pracovnej ploche systému Windows, prípadne na ňu klepnite a podržte, a potom kliknite alebo klepnite na položku **Bleach Now** (Vyčistiť teraz).
2. Keď sa objaví dialógové okno potvrdenia, kliknite alebo klepnite na tlačidlo **Bleach** (Vyčistiť).

Prezeranie súborov denníka

Pri každom úkone skartovania alebo dôkladného čistenia voľného miesta sú vygenerované súbory denníka so všetkými chybami alebo zlyhaniami. Súbory denníka sú vždy aktualizované podľa najnovšieho úkonu skartovania alebo dôkladného čistenia voľného miesta.

POZNÁMKA: Súbory, ktoré boli úspešne skartované alebo dôkladne vyčistené, sa v súboroch denníka neobjavujú.

Jeden súbor denníka je vytvorený pre úkony skartovania a druhý súbor denníka je vytvorený pre úkony dôkladného čistenia voľného miesta. Obidva súbory denníka sú uložené na pevnom disku v týchto priečinkoch:

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

Pri 64-bitových systémoch sú súbory denníka uložené na pevnom disku v týchto priečinkoch:

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

7 HP Device Access Manager (len vybrané modely)

Program HP Device Access Manager ovláda prístup k údajom pomocou zakázania zariadení na prenos údajov.

POZNÁMKA: Niektoré zariadenia s ľudským rozhraním/vstupné zariadenia, ako je napríklad myš, klávesnica, TouchPad a čítačka odtlačkov prstov, nie sú programom Device Access Manager ovládané. Ďalšie informácie nájdete v časti Nespravované triedy zariadení na strane 47.

Administrátori systému Windows® používajú program HP Device Access Manager na ovládanie prístupu k zariadeniam v systéme a ochranu pred nepovoleným prístupom:

- Profily zariadení sú vytvárané pre jednotlivých používateľov a určujú, ktoré zariadenia majú povolené alebo zamietnuté oprávnenie na prístup.
- Just In Time Authentication (JITA) umožňuje vopred určeným používateľom overenie za účelom prístupu k zariadeniam, ktoré majú inak zakázané.
- Administrátori a dôveryhodní používatelia môžu byť vyňatí z obmedzení prístupu k zariadeniam ukladaných programom Device Access Manager po ich pridaní do skupiny Administrátori zariadenia. Členstvo v tejto skupine je spravované pomocou Rozšírených nastavení.
- Prístup k zariadeniu môže byť udelený alebo zamietnutý na základe členstva v skupine alebo pre jednotlivých používateľov.
- Pri triedach zariadení, ako sú napríklad jednotky CD-ROM a DVD jednotky môže byť prístup k čítaniu a zápisu povolený alebo zakázaný samostatne.

Program HP Device Access Manager je počas krokov Sprievodcu nastavením aplikácie HP Client Security automaticky nakonfigurovaný na tieto nastavenia:

- Just In Time Authentication (JITA) pre vymeniteľné zariadenia je povolené pre administrátorov a používateľov.
- Zásady zariadenia povoľujú plný prístup k ostatným zariadeniam.

Otvorenie programu Device Access Manager

1. Na obrazovke Štart kliknite alebo klepnite na aplikáciu **HP Client Security** (Windows 8).

   – alebo –

   Na pracovnej ploche systému Windows dvakrát kliknite alebo dvakrát klepnite na ikonu aplikácie **HP Client Security** v oblasti oznámení na paneli úloh úplne vpravo.

2. V časti **Device** (Zariadenie) kliknite alebo klepnite na položku **Device Permissions** (Povolenia zariadenia).

   - Bežní používatelia môžu vidieť svoj aktuálny prístup k zariadeniu (viď Používateľské zobrazenie na strane 45).
   - Administrátori môžu vidieť a robiť zmeny v prístupe k zariadeniu, ktoré sú momentálne na počítači nakonfigurované. Kliknite alebo klepnite na tlačidlo **Change** (Zmeniť) a potom zadajte svoje administrátorské heslo (viď Systémové zobrazenie na strane 45).

Používateľské zobrazenie

Keď je vybraná položka **Device Permission** (Oprávnenia zariadenia), objaví sa používateľské zobrazenie. V závislosti od zásad môžu bežní používatelia a administrátori prezerať svoj vlastný prístup k triedam zariadení alebo jednotlivým zariadeniam na tomto počítači.

- **Current user** (Aktuálny používateľ) – zobrazí sa meno používateľa, ktorý je práve prihlásený.
- **Device Class** (Trieda zariadenia) – zobrazené sú typy zariadení.
- **Access** (Prístup) – zobrazuje sa súčasný nakonfigurovaný prístup k typom zariadení alebo ku konkrétnym zariadeniam.
- **Duration** (Trvanie) – zobrazuje sa časový limit prístupu k jednotkám CD/DVD-ROM alebo vymeniteľným diskovým jednotkám.
- **Settings** (Nastavenia) – administrátori môžu zmeniť jednotky, ku ktorým je prístup ovládaný programom Device Access Manager.

Systémové zobrazenie

V systémovom zobrazení môžu administrátori povoliť alebo zamietnuť prístup k zariadeniam na tomto počítači pre skupinu používateľov alebo skupinu administrátorov.

▲ Administrátori môžu systémové zobrazenie otvoriť kliknutím alebo klepnutím na tlačidlo **Change** (Zmeniť), zadaním administrátorského hesla a potom môžu vybrať spomedzi týchto možností:

- **Device Access Manager** – zapnutie alebo vypnutie programu HP Device Access Manager s funkciou Just In Time Authentication. Kliknite alebo klepnite na tlačidlo **On** (Zapnúť) alebo **Off** (Vypnúť).
- **Users and groups on this PC** (Používatelia a skupiny na tomto PC) – zobrazuje skupinu používateľov alebo skupinu administrátorov, ktorí majú povolený alebo zakázaný prístup k vybraným triedam zariadení.
- **Device Class** (Trieda zariadenia) – zobrazuje triedy zariadení a zariadenia, ktoré sú v systéme nainštalované, prípadne boli v systéme nainštalované predtým. Ak chcete zoznam rozbaliť, kliknite na ikonu **+**. Zobrazené sú všetky zariadenia pripojené k počítaču a skupiny používateľov a administrátorov sú rozbalené a zobrazujú ich členstvo. Ak chcete obnoviť zoznam zariadení, kliknite na ikonu s kruhovou šípkou (obnoviť).
  - Ochrana je zvyčajne použitá pre triedu zariadení. Ak je prístup nastavený na možnosť **Allow** (Povoliť), vybraný používateľ alebo skupina majú prístup ku všetkým zariadeniam v triede zariadení.
  - Ochrana sa dá tiež použiť na konkrétne zariadenia.
  - Nakonfigurujte funkciu Just In Time authentication (JITA), ktorá umožňuje vybraným používateľom prístup k jednotkám DVD/CD-ROM alebo vymeniteľným diskovým jednotkám po ich overení. Ďalšie informácie nájdete v časti Konfigurácia funkcie JITA na strane 46.
  - Povoľte alebo zamietnite prístup k ďalším triedam zariadení, ako sú napríklad vymeniteľné médiá (napríklad USB flash jednotky), sériové a paralelné porty, zariadenia Bluetooth®, modemové zariadenia, karty PCMCIA/ExpressCard, zariadenia 1394, čítačka odtlačkov prstov a čítačka kariet Smart. Akú sú čítačka odtlačkov prstov a čítačka kariet Smart zamietnuté, môžu byť použité na overenie poverení, ale nemôžu byť použité na úrovni zásad relácie.

POZNÁMKA: Ak sú na overenie poverení používané zariadenia Bluetooth, prístup k zariadeniu Bluetooth nesmie byť zásadami programu Device Access Manager obmedzený.

- Keď vyberiete nastavenie na úrovni Skupina alebo Trieda zariadení, objaví sa výzva, či chcete použiť nastavenie na podriadené objekty:

  Yes (Áno) – nastavenie bude použité na podriadené objekty.

  No (Nie) – nastavenie nebude použité na podriadené objekty.

- Niektoré triedy zariadení, napríklad DVD a CD-ROM, môžu byť ďalej riadené povolením alebo zamietnutím prístupu osobitne pre úkony čítania a zápisu.

POZNÁMKA: Skupina administrátorov nemôže byť pridaná do zoznamu používateľov.

- **Access** (Prístup) – kliknite alebo klepnite na šípku nadol a potom vyberte jeden z nasledujúcich typov prístupu, čím povolíte alebo zamietnete prístup:
  - **Allow – Full Access** (Povoliť – úplný prístup)
  - **Allow – Read Only** (Povoliť – len na čítanie)
  - **Allow – JITA Required** (Povoliť – potrebné JITA), ďalšie informácie viď Konfigurácia funkcie JITA na strane 46.

    Ak je vybraný tento typ prístupu, v položke **Duration** (Trvanie) kliknutím alebo klepnutím na šípku nadol vyberte časový limit.
  - **Zamietnuť**
- **Duration** (Trvanie) – kliknutím alebo klepnutím na šípku nadol vyberte časový limit prístupu k jednotkám CD/DVD-ROM alebo vymeniteľným diskovým jednotkám (viď Konfigurácia funkcie JITA na strane 46).

Konfigurácia funkcie JITA

Konfigurácia funkcie JITA umožňuje administrátorovi prezerať a upravovať zoznamy používateľov a skupín, ktoré majú povolený prístup k zariadeniam pomocou funkcie Just In Time Authentication (JITA).

Používatelia s aktivovanou funkciou JITA budú mať prístup k niektorým zariadeniam, ku ktorým bol prístup zásadami vytvorenými v zobrazení **Device Class Configuration** (Konfigurácia triedy zariadení) obmedzený.

Časový limit funkcie JITA môže byť určený počtom minút alebo ako Neobmedzený. Neobmedzení používatelia majú prístup k zariadeniu od času, kedy boli overení, až po ich odhlásenie zo systému.

Ak má používateľ obmedzený časový limit JITA, minútu pred uplynutím časového limitu JITA sa používateľovi objaví výzva na predĺženie prístupu. Keď sa používateľ odhlási zo systému alebo sa prihlási iný používateľ, časový limit JITA uplynie. Pri ďalšom prihlásení a pokuse o prístup k zariadeniu s aktivovanou funkciou JITA sa zobrazí výzva na zadanie poverení.

Funkcia JITA je k dispozícii pre tieto triedy zariadení:

- Jednotky DVD/CD-ROM
- Vymeniteľné diskové jednotky

Vytvorenie zásad JITA pre používateľa alebo skupinu

Administrátori môžu povoliť používateľom alebo skupinám prístup k zariadeniam pomocou funkcie Just In Time Authentication (JITA).

1. Spustite program **Device Access Manager** a potom kliknite alebo klepnite na tlačidlo **Change** (Zmeniť).
2. Vyberte používateľa alebo skupinu a potom v položke **Access** (Prístup) pre **Removable Disk drives** (Vymeniteľné diskové jednotky) alebo **DVD/CD-ROM drives** (Jednotky DVD/CD-ROM) kliknite alebo klepnite na šípku nadol a vyberte možnosť **Allow – JITA Required** (Povoliť – potrebné JITA).
3. V položke **Duration** (Trvanie) kliknutím alebo klepnutím na šípku nadol vyberte časový limit pre prístup JITA.

Nové nastavenie JITA sa použije až po odhlásení a opätovnom prihlásení používateľa.

Deaktivovanie zásad JITA pre používateľa alebo skupinu

Administrátori môžu deaktivovať používateľom alebo skupinám prístup k zariadeniam pomocou funkcie Just In Time Authentication.

1. Spustite program **Device Access Manager** a potom kliknite alebo klepnite na tlačidlo **Change** (Zmeniť).
2. Vyberte používateľa alebo skupinu a potom v položke **Access** (Prístup) pre **Removable Disk drives** (Vymeniteľné diskové jednotky) alebo **DVD/CD-ROM drives** (Jednotky DVD/CD-ROM) kliknite alebo klepnite na šípku nadol a vyberte možnosť **Deny** (Zamietnuť).

Keď sa používateľ prihlási a pokúsi sa o prístup k zariadeniu, prístup bude zamietnutý.

Nastavenia

Zobrazenie **Settings** (Nastavenia) umožňuje administrátorom prezerať a meniť jednotky, ku ktorým je prístup ovládaný programom Device Access Manager.

POZNÁMKA: Keď sa konfiguruje zoznam písmen jednotiek, musí byť program Device Access Manager aktivovaný (viď Systémové zobrazenie na strane 45).

Nespravované triedy zariadení

Program HP Device Access Manager nespravuje tieto triedy zariadení:

- Vstupné/výstupné zariadenia
  - CD-ROM
  - Disková jednotka
  - Radič disketovej mechaniky (FDC)
  - Radič pevného disku (HDC)
  - Trieda zariadení s ľudským rozhraním (HID)
  - Infračervené zariadenia s ľudským rozhraním
  - Myš
  - Sériový viacnásobný port

- Klávesnica
- Tlačiarne Plug and play (PnP)
- Tlačiareň
- Inovácia tlačiarne

- napájanie
  - Podpora rozšírenej správy napájania (APM)
  - Batéria
- Rôzne
  - Počítač
  - Dekodér
  - Obrazovka
  - Jednotný ovládač obrazovky Intel®
  - Legacard
  - Ovládač médií
  - Menič médií
  - Pamäťová technológia
  - Monitor
  - Multifunkčné zariadenie
  - Klient siete
  - Služba siete
  - Net trans
  - Procesor
  - Adaptér SCSI
  - Zabezpečený urýchľovač
  - Bezpečnostné zariadenia
  - Systém
  - Neznáme
  - Zväzok
  - Snímka zväzku

8 HP Trust Circles

Program HP Trust Circles je aplikácia na zabezpečenie súborov a dokumentov, v ktorej sa spája šifrovanie priečinkov so súbormi s možnosťou praktického zdieľania dokumentov s dôveryhodným okruhom ľudí. Aplikácia šifruje súbory umiestnené v priečinkoch používateľa a chráni ich v rámci dôveryhodného okruhu. Chránené súbory je možné používať a zdieľať len s členmi dôveryhodného okruhu. Ak chránený súbor dostane nečlen, súbor zostáva zašifrovaný a nečlen nemá prístup k jeho obsahu.

Otvorenie programu Trust Circles

1. Na obrazovke Štart kliknite alebo klepnite na aplikáciu **HP Client Security**.

   – alebo –

   Na pracovnej ploche systému Windows dvakrát kliknite na ikonu aplikácie **HP Client Security** v oblasti oznámení umiestnenú na paneli úloh úplne vpravo.

2. V časti **Data** (Údaje) kliknite alebo klepnite na položku **Trust Circles**.

Úvodné informácie

Sú dva spôsoby, ako odoslať e-mailové pozvánky a odpovedať na ne:

- **Pomocou programu Microsoft® Outlook** – používanie programu Trust Circles v rámci aplikácie Microsoft Outlook automatizuje spracovávanie všetkých pozvánok programu Trust Circle a odpovede od ostatných používateľov programu Trust Circle.
- **Pomocou služieb Gmail, Yahoo, Outlook.com alebo iných e-mailových služieb (SMTP)** – keď zadáte svoje meno, e-mailovú adresu a heslo, program Trust Circles použije vašu e-mailovú službu a odošle e-mailové pozvánky členom, ktorých ste vybrali, aby sa pridali do dôveryhodného okruhu.

Nastavenie základného profilu:

1. Zadajte svoje meno a e-mailovú adresu a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).

   Meno vidia všetci členovia, ktorých ste pozvali, aby sa pridali do dôveryhodného okruhu. E-mailová adresa sa použije na odosielanie, prijímanie alebo odpovedanie na pozvánky.

2. Zadajte heslo pre e-mailové konto a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).

   Odošle sa testovací e-mail, aby sa zistilo, či sú nastavenia e-mailu správne.

   POZNÁMKA: Počítač musí byť pripojený k sieti.

3. Do políčka **Trust Circle Name** (Názov dôveryhodného okruhu) zadajte názov dôveryhodného okruhu a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej).

4. Pridajte členov a priečinky a potom kliknite alebo klepnite na tlačidlo **Next** (Ďalej). Dôveryhodný okruh je vytvorený so všetkými priečinkami, ktoré ste vybrali, a všetkým vybraným členom sa odošle e-mailová pozvánka. Ak z nejakého dôvodu nie je možné pozvánku odoslať, zobrazí sa upozornenie. Členov je možné kedykoľvek pozvať znova v zobrazení Dôveryhodné okruhy kliknutím na položku **Your Trust Circles** (dôveryhodné okruhy) a dvojitým kliknutím alebo

dvojitým klepnutím na dôveryhodný okruh. Ďalšie informácie nájdete v časti Dôveryhodné okruhy na strane 50.

Dôveryhodné okruhy

Dôveryhodný okruh môžete vytvoriť počas prvotného nastavenia po zadaní svojej e-mailovej adresy, prípadne v zobrazení Dôveryhodné okruhy:

▲ V zobrazení Dôveryhodné okruhy kliknite alebo klepnite na položku **Create Trust Circle** (Vytvoriť dôveryhodný okruh) a potom zadajte názov dôveryhodného okruhu.

- Ak chcete pridať členov do dôveryhodného okruhu, kliknite alebo klepnite na ikonu **M+** vedľa položky **Members** (Členovia) a potom postupujte podľa pokynov na obrazovke.
- Ak chcete do dôveryhodného okruhu pridať priečinky, kliknite alebo klepnite na ikonu **+** vedľa položky **Folders** (Priečinky) a potom postupujte podľa pokynov na obrazovke.

Pridanie priečinkov do dôveryhodného okruhu

Pridanie priečinkov do nového dôveryhodného okruhu:

- Počas vytvárania dôveryhodného okruhu môžete pridať priečinky kliknutím alebo klepnutím na ikonu **+** vedľa položky **Folders** (Priečinky) a potom postupujte podľa pokynov na obrazovke.

  – alebo –

- V programe Prieskumník Windows kliknite pravým tlačidlom myši (alebo klepnite a podržte) na priečinok, ktorý momentálne nie je časťou dôveryhodného okruhu, vyberte položku **Trust Circle** (Dôveryhodný okruh) a potom vyberte položku **Create Trust Circle from Folder** (Vytvoriť dôveryhodný okruh z priečinka).

TIP: Môžete pridať jeden alebo viac priečinkov.

Pridanie priečinkov do existujúceho dôveryhodného okruhu:

- V zobrazení Dôveryhodný okruh kliknite na položku **Your Trust Circles** (Vaše dôveryhodné okruhy), dvakrát kliknite alebo dvakrát klepnite na existujúci dôveryhodný okruh, čím zobrazíte aktuálne priečinky, kliknite alebo klepnite na ikonu **+** vedľa položky **Folders** (Priečinky) a potom postupujte podľa pokynov na obrazovke.

  – alebo –

- V programe Prieskumník Windows kliknite pravým tlačidlom myši (alebo klepnite a podržte) na priečinok, ktorý momentálne nie je časťou dôveryhodného okruhu, vyberte položku **Trust Circle** (Dôveryhodný okruh) a potom vyberte položku **Add to existing Trust Circle from Folder** (Pridať do existujúceho dôveryhodného okruhu z priečinka).

TIP: Môžete pridať jeden alebo viac priečinkov.

Keď sa priečinok pridá do dôveryhodného okruhu, program Trust Circles automaticky zašifruje priečinok a jeho obsah. Po zašifrovaní všetkých súborov sa zobrazí oznámenie. Okrem toho sa na ikonách všetkých zašifrovaných priečinkov a na ikonách súborov v priečinkoch zobrazí symbol zeleného zámku označujúci, že sú plne chránené.

Pridanie členov do dôveryhodného okruhu

Na pridanie členov do dôveryhodného okruhu sú potrebné tri kroky:

1. **Invite** (Pozvať) – najprv vlastník dôveryhodného okruhu pozve členov. Pozývací e-mail je možné poslať viacerým používateľom alebo distribučným zoznamom/skupinám.
2. **Accept** (Prijať) – pozvaný dostane pozvánku a vyberie, či ju prijíma alebo zamieta. Ak pozvaný prijme pozvánku, pozývajúcemu bude odoslaná e-mailová odpoveď. Ak bola pozvánka odoslaná skupine, každý člen dostane pozvánku a vyberie, či ju prijíma alebo zamieta.
3. **Enroll** (Registrovať) – pozývajúci má poslednú príležitosť rozhodnúť, či pridá člena do dôveryhodného okruhu. Ak sa pozývajúci rozhodne zaregistrovať člena, pozvanému je odoslaný e-mail s oznámením, že odpoveď bola zaevidovaná. Pozývajúci aj pozvaný majú voliteľnú možnosť overiť bezpečnosť procesu pozvania. Pozvanému sa zobrazuje overovací kód, ktorý musí pozývajúcemu prečítať do telefónu. Po overení kódu môže pozývajúci odoslať konečný registračný e-mail.

Pridanie členov do nového dôveryhodného okruhu:

▲ Počas vytvárania dôveryhodného okruhu môžete pridať členov kliknutím alebo klepnutím na ikonu **M+** vedľa položky **Members** (Členovia) a potom postupujte podľa pokynov na obrazovke.

- Ak používate program Outlook, vyberte kontakty z adresára programu Outlook a potom kliknite na tlačidlo **OK**.
- Ak používate inú e-mailovú službu, pridajte nové e-mailové adresy do dôveryhodného okruhu ručne, prípadne ich získajte z e-mailovej adresy zaregistrovanej v programe Trust Circle.

Pridanie členov do existujúceho dôveryhodného okruhu:

▲ V zobrazení Dôveryhodný okruh kliknite na položku **Your Trust Circles** (Vaše dôveryhodné okruhy), dvakrát kliknite alebo dvakrát klepnite na existujúci dôveryhodný okruh, čím zobrazíte aktuálnych členov, kliknite alebo klepnite na ikonu **M+** vedľa položky **Members** (Členovia) a potom postupujte podľa pokynov na obrazovke.

- Ak používate program Outlook, vyberte kontakty z adresára programu Outlook a potom kliknite na tlačidlo **OK**.
- Ak používate inú e-mailovú službu, pridajte nové e-mailové adresy do dôveryhodného okruhu ručne, prípadne ich získajte z e-mailovej adresy zaregistrovanej v programe Trust Circle.

Pridanie súborov do dôveryhodného okruhu

Súbory môžete do dôveryhodného okruhu pridať jedným z nasledujúcich spôsobov:

- Skopírujte alebo premiestnite súbor do existujúceho priečinka dôveryhodného okruhu.

  – alebo –

- V programe Prieskumník Windows kliknite pravým tlačidlom myši (alebo podržte a klepnite) na súbor, ktorý nie je momentálne zašifrovaný, vyberte položku **Trust Circle** (Dôveryhodný okruh) a potom vyberte položku **Encrypt** (Zašifrovať). Objaví sa výzva na výber dôveryhodného okruhu, do ktorého má byť súbor pridaný.

TIP: Môžete vybrať jeden alebo viac priečinkov.

Zašifrované priečinky

Všetci členovia dôveryhodného okruhu môžu prezerať a upravovať súbory prináležiace do daného dôveryhodného okruhu.

POZNÁMKA: Program Trust Circle Manager/Reader nesynchronizuje súbory medzi členmi.

Súbory musia byť zdieľané existujúcimi spôsobmi, napríklad e-mailom, cez FTP alebo cez poskytovateľov služieb Cloud. Súbory, ktoré sú skopírované a premiestnené do priečinka dôveryhodného okruhu, prípadne sú v ňom vytvorené, sú chránené okamžite.

Odstránenie priečinkov z dôveryhodného okruhu

Pri odstránení priečinka z dôveryhodného okruhu sa dešifruje priečinok a všetok jeho obsah a odstráni sa ochrana.

- V zobrazení Dôveryhodný okruh kliknite na položku **Your Trust Circles** (Vaše dôveryhodné okruhy), dvakrát kliknite alebo dvakrát klepnite na aktuálne priečinky a potom kliknite alebo klepnite na ikonu **koša** vedľa priečinka.

  – alebo –

- V programe Prieskumník Windows kliknite pravým tlačidlom myši (alebo klepnite a podržte) na priečinok, ktorý momentálne je časťou dôveryhodného okruhu, vyberte položku **Trust Circle** (Dôveryhodný okruh) a potom vyberte položku **Remove from trust circle** (Odstrániť z dôveryhodného okruhu).

TIP: Môžete pridať jeden alebo viac priečinkov.

Odstránenie súboru z dôveryhodného okruhu

Ak chcete odstrániť súbor z dôveryhodného okruhu, v programe Prieskumník Windows kliknite pravým tlačidlom myši (alebo klepnite a podržte) na súbor, ktorý je momentálne zašifrovaný, vyberte položku **Trust Circle** (Dôveryhodný okruh) a potom vyberte položku **Decrypt File** (Dešifrovať súbor).

Odstránenie členov z dôveryhodného okruhu

Člena, ktorý bol plne zaregistrovaný, nie je možné z dôveryhodného okruhu odstrániť. Alternatíva je vytvorenie nového dôveryhodného okruhu so všetkými ostatnými členmi, premiestnenie všetkých súborov a priečinkov do nového dôveryhodného okruhu a potom odstránenie starého dôveryhodného okruhu. Tým sa zaistí, že všetky nové súbory, ktoré člen dostane, nebudú prístupné, ale všetko, čo bolo predtým zdieľané, zostane prístupné členovi starého dôveryhodného okruhu.

Ak člen nie je plne zaregistrovaný (člen bol pozvaný na pridanie sa do dôveryhodného okruhu alebo neprijal pozvanie do dôveryhodného okruhu), môžete člena odstrániť z dôveryhodného okruhu jedným z nasledujúcich spôsobov:

- V zobrazení Dôveryhodný okruh kliknite alebo klepnite na položku **Your Trust Circles** (Vaše dôveryhodné okruhy) a dvojitým kliknutím alebo dvojitým klepnutím na dôveryhodný okruh zobrazte aktuálny zoznam členov. Kliknite alebo klepnite na ikonu **koša** vedľa mena člena, ktorého chcete odstrániť.
- V zobrazení Dôveryhodný okruh kliknite alebo klepnite na položku **Members** (Členovia) a dvojitým kliknutím alebo dvojitým klepnutím na člena zobrazte dôveryhodné okruhy, v ktorých sú členovia. Kliknite alebo klepnite na ikonu **koša** vedľa dôveryhodného okruhu, čím odstránite člena z daného dôveryhodného okruhu.

Odstránenie dôveryhodného okruhu

Ak chcete odstrániť dôveryhodný okruh, musíte byť jeho vlastník.

▲ V zobrazení Dôveryhodný okruh kliknite alebo klepnite na položku **Your Trust Circles** (Vaše dôveryhodné okruhy) a kliknite alebo klepnite na ikonu **koša** vedľa dôveryhodného okruhu, ktorý chcete odstrániť.

Tým odstránite dôveryhodný okruh zo stránky a všetkým členom dôveryhodného okruhu bude odoslaný e-mail s informáciou, že dôveryhodný okruh bol odstránený. Všetky súbory alebo priečinky, ktoré boli zahrnuté do dôveryhodného okruhu, sú dešifrované.

Nastavenie predvolieb

V zobrazení Dôveryhodný okruh kliknite alebo klepnite na položku **Preferences** (Predvoľby). Zobrazia sa tri karty.

- **Email Settings** (Nastavenia e-mailu)

Voľba	Popis
Username (Meno používateľa)	Zobrazuje sa momentálne používané meno používateľa. Ak ho chcete zmeniť, zadajte do textového políčka nové meno používateľa. Zmeny sa ukladajú automaticky.
Email Address (E-mailová adresa)	Zobrazuje sa momentálne používaná e-mailová adresa. Ak ju chcete zmeniť, kliknite alebo klepnite na položku **Change Email Settings** (Zmeniť nastavenia e-mailu) a potom postupujte podľa pokynov na obrazovke.
New Member Confirmation (Potvrdenie nového člena)	Vyberte spomedzi nasledujúcich možností: ◦ **Confirm Automatically** (Potvrdiť automaticky) – po prijatí súhlasu od pozvaného je bez ručného zadávania potvrdené prijatie do dôveryhodného okruhu a pozvanému je odoslaný potvrdzovací e-mail. ◦ **Confirm Manually** (Potvrdiť ručne) – po prijatí súhlasu od pozvaného je potrebné ručne zadať a zaregistrovať nových členov do dôveryhodného okruhu, potom je pozvanému odoslaný potvrdzovací e-mail. ◦ **Require Verification** (Vyžadovať overenie) – po prijatí súhlasu od pozvaného je na úplnú registráciu pozvaného potrebný overovací kód. Vlastník dôveryhodného okruhu musí kontaktovať pozvaného a vyžiadať si od neho overovací kód. Po zadaní správneho kódu bude odoslaný potvrdzovací e-mail.
Periodic Authentication (Pravidelné overovanie)	Pravidelné overovanie vyžaduje, aby po uplynutí určitého časového limitu (v minútach) a tiež počas vykonávania citlivých úkonov používateľ zadal heslo do systému Windows. Toto nastavenie umožňuje zapnúť alebo vypnúť overovanie používateľa.
Authentication Timeout (Časový limit overovania)	Vyberte časový limit (v minútach), po uplynutí ktorého má byť vykonané overenie.
Don't show confirmation message (Nezobrazovať potvrdenie)	Začiarknite toto políčko, ak chcete vypnúť zobrazovanie potvrdení, prípadne zrušte začiarknutie políčka, ak chcete potvrdenia zobrazovať.
I'd like to help improve the HP Trust Circle through anonymous usage tracking (Chcem pomôcť vylepšiť program HP Trust Circle anonymným zaznamenávaním využitia)	Začiarknite políčko, ak sa chcete zapojiť do programu, prípadne zrušte začiarknutie políčka, ak sa ho nechcete zúčastniť.

- **Backup/Restore** (Zálohovanie/Obnovenie)

Voľba	Popis
Zálohovanie	Skopírovanie údajov aplikácie Trust Circle Manager/Reader (nastavenia a dôveryhodné okruhy) do súboru zálohy. V prípade zlyhania alebo systémovej chyby môžete použiť tento súbor na obnovenie novej inštalácie programu Trust Circles do stavu uloženého v súbore. **POZNÁMKA:** Uložené sú len údaje aplikácie Trust Circle (dôveryhodné okruhy, nastavenia a členovia). Aktuálne súbory v priečinkoch dôveryhodného okruhu nie sú zálohované. Tieto súbory je potrebné zálohovať samostatne. Zálohovanie nastavení a používateľských údajov programu Trust Circle: **1.** Kliknite alebo klepnite na tlačidlo **Backup** (Zálohovať). **2.** Vyberte názov súboru a priečinok pre súbor zálohy a potom kliknite alebo klepnite na tlačidlo **Uložiť**. **3.** Zadajte heslo, potvrďte ho a potom kliknite alebo klepnite na tlačidlo **OK**. Toto heslo bude pri obnovení súboru požadované.
Obnovenie	Obnoví nastavenia a dôveryhodné okruhy so súboru zálohy, zvyčajne po zlyhaní systému alebo migrácii na iný počítač. Obnovenie nastavení a používateľských údajov programu Trust Circle Manager: **1.** Kliknite alebo klepnite na tlačidlo **Restore** (Obnoviť). **2.** Vyhľadajte priečinok a súbor so zálohou a potom kliknite alebo klepnite na tlačidlo **Open** (Otvoriť). **3.** Zadajte heslo, ktoré bolo nastavené počas vytvárania zálohy.

- **About** (Informácie) – zobrazuje sa verzia softvéru Trust Circle Manager/Reader. Zobrazujú sa prepojenia umožňujúce inováciu programu Trust Circle Manager na verziu Pro alebo sa zobrazuje vyhlásenie o ochrane súkromia od spoločnosti HP.

9 Obnovenie pri krádeži (len vybrané modely)

Služba Computrace (kupuje sa osobitne) vám umožňuje monitorovať, spravovať a sledovať váš počítač.

Po aktivovaní je služba Computrace nakonfigurovaná zo Zákazníckeho centra Absolute Software. Zo Zákazníckeho centra môže administrátor nakonfigurovať službu Computrace na monitorovanie alebo spravovanie počítača. Ak sa systém stratí alebo je odcudzený, Zákaznícke centrum môže pomôcť miestnym úradom vyhľadať a obnoviť počítač do výrobcom predvoleného stavu. Ak je služba Computrace nakonfigurovaná, dokáže fungovať naďalej aj v prípade, že je pevný disk vymazaný alebo vymenený.

Aktivovanie služby Computrace:

1. Pripojte na internet.
2. Otvorte aplikáciu HP Client Security. Ďalšie informácie nájdete v časti Otvorenie aplikácie HP Client Security na strane 9.
3. Kliknite na položku **Theft Recovery** (Obnovenie pri krádeži).
4. Ak chcete spustiť Sprievodcu aktivovaním služby Computrace, kliknite na položku **Get Started** (Úvodné informácie).
5. Zadajte kontaktné údaje a údaje k platbe kreditnou kartou, prípadne zadajte svoj vopred zakúpený produktový kód.

Sprievodca aktivovaním vás bezpečne prevedie procesom transakcie a nastaví vám používateľské konto na webovej stránke Zákazníckeho centra Absolute Software. Po dokončení dostanete potvrdzovací e-mail obsahujúci informácie o vašom konte v Zákazníckom centre.

Ak ste už predtým mali spusteného Sprievodcu aktivovaním služby Computrace a vaše konto v Zákazníckom centre už existuje, môžete si zakúpiť ďalšie licencie tak, že sa obrátite na zástupcu spoločnosti HP.

Prihlásenie do Zákazníckeho centra:

1. Prejdite na lokalitu https://cc.absolute.com/.
2. Do políčok **Login ID** (Prihlasovacie ID) a **Password** (Heslo) zadajte poverenia, ktoré ste dostali v potvrdzovacej e-mailovej správe, a potom kliknite na tlačidlo **Log in** (Prihlásiť sa).

Pomocou Zákazníckeho centra môžete robiť nasledovné:

- Monitorovať svoje počítače
- Chrániť na diaľku svoje údaje
- Nahlásiť krádež ktoréhokoľvek počítača chráneného službou Computrace

▲ Kliknite na tlačidlo **Learn More** (Ďalšie informácie), ak potrebujete ďalšie informácie o službe Computrace.

10 Výnimky lokalizovaného hesla

Na úrovni overovania pri zapnutí a na úrovni programu HP Drive Encryption je obmedzená podpora lokalizácie hesla. Ďalšie informácie nájdete v časti IME systému Windows nie je podporovaný na úrovni overovania pri zapnutí alebo na úrovni Šifrovanie jednotky na strane 56.

Čo robiť, keď je heslo odmietnuté

Heslá môžu byť odmietnuté z nasledujúcich dôvodov:

- Používateľ využíva IME, ktoré nie je podporované. Ide o bežný problém s dvojbajtovými jazykmi (kórejčina, japončina, čínština). Riešenie tohto problému:
  1. Pomocou položky **Control Panel** (Ovládací panel) pridajte podporované rozloženie klávesnice (pridajte klávesnice USA/angličtina k jazyku zadávania Čínština).
  2. Nastavte podporovanú klávesnicu na predvolené zadávanie.
  3. Spustite aplikáciu HP Client Security a potom zadajte heslo do systému Windows.
- Používateľ využíva nepodporovaný znak. Riešenie tohto problému:
  1. Zmeňte heslo do systému Windows tak, aby obsahovalo len podporované znaky. Ďalšie informácie o nepodporovaných znakoch nájdete v časti Narábanie so špeciálnymi klávesmi na strane 57.
  2. Spustite aplikáciu HP Client Security a potom zadajte heslo do systému Windows.

IME systému Windows nie je podporovaný na úrovni overovania pri zapnutí alebo na úrovni Šifrovanie jednotky

V systéme Windows môže používateľ zvoliť IME (input method editor – editor spôsobu zadávania) a pomocou štandardnej západnej klávesnice zadávať zložité znaky a symboly, ako sú napríklad japonské alebo čínske znaky.

IME nie sú podporované na úrovni overovania pri zapnutí alebo na úrovni Šifrovanie jednotky Heslo do systému Windows nie je možné zadať pomocou IME na prihlasovacej obrazovke overovania pri zapnutí alebo HP Drive Encryption a z toho dôvodu dochádza k zablokovaniu. V niektorých prípadoch systém Microsoft® Windows nezobrazuje IME, keď používateľ zadáva heslo.

Riešenie je prepnúť na jedno z nasledujúcich podporovaných rozložení klávesnice, ktoré prekladá do rozloženia klávesnice 00000411:

- Microsoft IME pre japončinu
- Japonské rozloženie klávesnice
- Office 2007 IME pre japončinu – ak spoločnosť Microsoft alebo iná strana používa výraz IME alebo „input method editor“, spôsob zadávania nemusí byť v skutočnosti IME. To môže spôsobiť zmätok, ale softvér číta hexadecimálnu reprezentáciu kódu. Ak teda IME mapuje na podporované rozloženie klávesnice, aplikácia HP Client Security môže podporovať konfiguráciu.

VAROVANIE! Keď je aplikácia HP Client Security nasadená, heslá zadávané pomocou IME systému Windows budú odmietnuté.

Zmeny hesla pomocou rozloženia klávesnice, ktoré je tiež podporované

Ak je heslo najprv nastavené pomocou jedného rozloženia klávesnice, napríklad Angličtina (USA) (409) a potom používateľ zmení heslo pomocou iného tiež podporovaného rozloženia klávesnice, napríklad Latinská Amerika (080A), zmena hesla bude fungovať na úrovni Šifrovanie jednotky, ale nebude fungovať v BIOS-e, ak používateľ využíva znaky, ktoré existujú neskôr, ale neexistovali predtým (napríklad ē).

POZNÁMKA: Administrátori môžu vyriešiť tento problém pomocou stránky Používatelia v aplikácii HP Client Security (otvára sa pomocou ikony **ozubeného kolieska** na úvodnej stránke) tak, že odstránia používateľa z aplikácie HP Client Security, vyberú v operačnom systéme požadované rozloženie klávesnice a potom pre toho istého používateľa znova spustia Sprievodcu nastavením aplikácie HP Client Security. BIOS uloží požadované rozloženie klávesnice a heslá, ktoré sa dajú zadávať touto klávesnicou, budú v BIOS-e správne nastavené.

Ďalší možný problém je používanie odlišných rozložení klávesnice, ktoré dokážu vytvárať rovnaké znaky. Napríklad medzinárodné rozloženie klávesnice (USA) (20409) a rozloženie klávesnice Latinská Amerika (080A) dokážu vytvoriť znak é, hoci môžu byť potrebné odlišné postupnosti stlačenia klávesov. Ak je heslo najprv nastavené s rozložením klávesnice Latinská Amerika, potom je v BIOS-e nastavené rozloženie klávesnice Latinská Amerika, hoci heslo je následne zmenené pomocou medzinárodného rozloženia klávesnice (USA).

Narábanie so špeciálnymi klávesmi

- Čínština, slovenčina, kanadská francúzština a čeština

  Keď používateľ zvolí jedno z nasledujúcich rozložení klávesnice a potom zadá heslo (napríklad abcdef), rovnaké heslo musí byť pri Overovaní pri spustení a funkcii HP Drive Encryption zadané pri súčasnom stlačení klávesu shift pre malé písmená a klávesov shift a caps lock pre veľké písmená. Číselné heslá musia byť zadávané pomocou číselnej klávesnice.

- Kórejčina

  Keď používateľ zvolí podporované rozloženie kórejskej klávesnice a potom zadá heslo, rovnaké heslo musí byť pri Overovaní pri spustení a funkcii HP Drive Encryption zadané pri súčasnom stlačení klávesu alt pre malé písmená a pravého klávesu alt a klávesu caps lock pre veľké písmená.

- Nepodporované znaky sú uvedené v nasledujúcej tabuľke:

Language (Jazyk)	Windows	Systém BIOS	Šifrovanie jednotky
Arabské	Klávesy ﻻ ,ﻷ a ﻹ vytvárajú dva znaky.	Klávesy ﻻ ,ﻷ a ﻹ vytvárajú jeden znak.	Klávesy ﻻ ,ﻷ a ﻹ vytvárajú jeden znak.
Francúzština (kanadská)	ç, è, à a é s klávesom caps lock sú Ç, È, À a É v systéme Windows.	ç, è, à a é s klávesom caps lock sú ç, è, à a é v Overovaní pri spustení.	ç, è, à a é s klávesom caps lock sú ç, è, à a é v aplikácii HP Drive Encryption.

Language (Jazyk)	Windows	Systém BIOS	Šifrovanie jednotky
Španielčina	40a nie je podporované. Nefunguje to však, pretože softvér to prevedie c0a. Pretože sú však medzi rozloženiami klávesnice nepatrné rozdiely, odporúča sa, aby španielsky hovoriaci používatelia zmenili svoje rozloženie klávesnice v systéme Windows na 1040a (španielsky variant) alebo 080a (Latinská Amerika).	n/a	n/a
Medzinárodná (USA)	◦ Klávesy ¡, ¤, ‘, ’, ¥ a × vo vrchnom riadku sú odmietnuté. ◦ Klávesy å, ® a Þ v druhom riadku sú odmietnuté. ◦ Klávesy á, ð a ø v treťom riadku sú odmietnuté. ◦ Kláves æ v spodnom riadku je odmietnutý.	n/a	n/a
čeština	◦ Kláves ğ je odmietnutý. ◦ Kláves į je odmietnutý. ◦ Kláves ų je odmietnutý. ◦ Klávesy ė, ı a ž sú odmietnuté. ◦ Klávesy ģ, ķ, ļ, ņ a ţ sú odmietnuté.	n/a	n/a
Slovenčina	Kláves ż je odmietnutý.	◦ Klávesy š, ś a ş sú pri písaní odmietnuté, ale prijaté, ak sa zadajú softvérovou klávesnicou. ◦ Mŕtvy kláves ţ vytvára dva znaky.	n/a
maďarčina	Kláves ż je odmietnutý.	Kláves ţ vytvára dva znaky.	n/a
Slovinčina	Kláves żŻ je odmietnutý v systéme Windows a kláves Alt vytvára mŕtvy kláves v BIOS-e.	Klávesy ú, Ú, ů, Ů, ş, Ş, ś, Ś, š a Š sú odmietnuté v BIOS-e.	n/a
Japončina	Ak je k dispozícii, je lepšie zvoliť Microsoft Office 2007 IME. Bez ohľadu na názov IME je to v skutočnosti rozloženie klávesnice 411, ktoré je podporované.	n/a	n/a

Glosár

administrátor systému Windows
Používateľ so všetkými právami na úpravu povolení a spravovanie ostatných používateľov.

aktivácia
Úloha, ktorá musí byť vykonaná pred tým, než budú funkcie Šifrovanie jednotky k dispozícii. Administrátori môžu aktivovať Šifrovanie jednotky pomocou Sprievodcu nastavením aplikácie HP Client Security Setup alebo v aplikácii HP Client Security. Proces aktivácie pozostáva z aktivácie softvéru, zašifrovania jednotky a vytvorenia prvotného záložného kľúča na vymeniteľnom ukladacom zariadení.

aktívum
Údajový komponent pozostávajúci z osobných údajov alebo súborov, historické alebo s webom súvisiace údaje a podobne, ktoré sú umiestnené na pevnom disku.

archív núdzového obnovenia
Chránený ukladací priestor, ktorý umožňuje znova zašifrovať základné používateľské kľúče od jedného vlastníka platformy druhému.

automatické skartovanie
Skartovanie, ktoré ste naplánovali v programe File Sanitizer.

bezkontaktná karta
Plastová karta obsahujúca počítačový čip, ktorá sa dá použiť na overenie.

Bluetooth
Technológia používajúca rádiové prenosy, ktorá na krátku vzdialenosť umožňuje bezdrôtovú komunikáciu medzi počítačmi podporujúcimi funkciu Bluetooth, tlačiarňami, myšou, mobilným telefónmi a ďalšími zariadeniami.

dešifrovanie
Postup používaný v kryptografii na prevod zašifrovaných údajov na obyčajný text.

doména
Skupina počítačov, ktoré sú časťou siete a zdieľajú databázu spoločného adresára. Domény majú jedinečný názov a každá z nich má nastavené spoločné pravidlá a postupy.

dôkladné čistenie voľného miesta
Zapisovanie náhodných údajov do odstránených aktív a nevyužitého miesta. Tento proces redukuje existenciu odstráneného aktíva, takže pôvodné aktívum je ťažšie obnoviť.

Dôveryhodný okruh
Poskytuje možnosť zamedzenia šírenia údajov len v rámci určenej skupiny dôveryhodných používateľov. Zabraňuje sa tak situácii, že sa nechtiac dostanú údaje do nesprávnych rúk. Zabezpečené pomocou technológie Zero Overhead Key Management od spoločnosti CryptoMill, údaje sú viazané na dôveryhodný okruh. Tým sa zabráni dešifrovaniu dokumentov alebo iných citlivých údajov mimo dôveryhodného okruhu.

DriveLock
Bezpečnostná funkcia, pri ktorej je pevný disk prepojený na používateľa a používateľ musí pri spustení počítača správne zadať heslo pre funkciu DriveLock.

Encryption File System (EFS)
Systém, pri ktorom sa šifrujú všetky súbory a podpriečinky v rámci vybraného priečinka.

hardvérové šifrovanie

Použitie samošifrovacích jednotiek spĺňajúcich normu OPAL od Trusted Computing Group na správu samošifrovacích jednotiek a vykonávanie okamžitého zašifrovania. Hardvérové šifrovanie je okamžité a môže trvať len niekoľko minút, ale softvérové šifrovanie môže trvať niekoľko hodín.

ID card (Karta SD)
Pomôcka na pracovnej ploche systému Windows, ktorá slúži na vizuálnu identifikáciu vašej pracovnej plochy menom používateľa a zvoleným obrázkom.

identita
V aplikácii HP Client Security je to skupina poverení a nastavení, s ktorými sa nakladá ako s kontom alebo profilom pre jednotlivého používateľa.

Jedno prihlásenie
Funkcia ukladajúca overovacie údaje a umožňujúca používať aplikáciu HP Client Security na prístup na internet a do aplikácií systému Windows, ktoré vyžadujú overovanie heslom.

Just In Time authentication
Pozrite Pomocníka k softvéru HP Device Access Manager.

karta Proximity
Plastová karta obsahujúca počítačový čip, ktorá sa pre doplnkovú bezpečnosť dá využívať na overovanie v spojení s ďalšími povereniami.

karta Smart Card
Hardvérové zariadenie, ktoré sa dá s kódom PIN využívať na overovanie.

metóda bezpečného prihlasovania
Metóda používaná na prihlásenie do počítača.

obnovenie
Proces, pri ktorom sa do tohto programu skopírujú údaje programu z predtým uloženého súboru zálohy.

Obnovenie HP SpareKey
Možnosť prístupu k počítaču správnym odpovedaním na bezpečnostné otázky.

odtlačok prsta
Digitálna extrakcia obrazu odtlačku prsta. Skutočný obraz odtlačku prsta nie je nikdy aplikáciou HP Client Security uložený.

overovanie
Proces overovania znamená, že osoba preukazuje, že je oprávnená. Robí to pomocou poverení, medzi ktoré patrí heslo do systému Windows, odtlačok prsta, karta Smart, bezkontaktná karta alebo karta Proximity.

overovanie funkciou Šifrovanie jednotky pri spúšťaní
Prihlasovacia obrazovka zobrazená pred spustením systému Windows. Používatelia musia zadať svoje meno používateľa a heslo alebo kód PIN pre kartu Smart, prípadne nasnímať registrovaný prst. Ak je vybraná možnosť prihlásenia v jednom kroku, zadanie správnych údajov na prihlasovacej obrazovke funkcie Šifrovanie jednotky umožňuje priamy prístup do systému Windows bez opätovného prihlásenia na prihlasovacej obrazovke systému Windows.

overovanie pri spustení
Bezpečnostná funkcia vyžadujúca určitú formu overenia pri zapnutí počítača, napríklad kartou Smart, bezpečnostným čipom alebo heslom.

PIN
Osobné identifikačné číslo pre zaregistrovaného používateľa využívané na overenie.

PKI
Norma infraštruktúry verejného kľúča (Public Key Infrastructure), ktorá určuje prostredia pre vytváranie, používanie a administráciu certifikátov a kryptografických kľúčov.

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

používateľské konto systému Windows
Používateľ, ktorý má oprávnenie prihlásiť sa do siete alebo k jednotlivým počítačom.

poverenie
Malá časť údajov alebo hardvérové zariadenie používané na overenie jednotlivých používateľov.

priečinok dôveryhodného okruhu
Akýkoľvek priečinok chránený dôveryhodným okruhom.

prihlásenie
Objekt v rámci aplikácie HP Client Security, ktorý sa skladá z mena používateľa a hesla (a prípadne ďalších vybraných údajov), ktorý môže byť použitý na prihlásenie na webové stránky alebo do iných programov.

prihlasovacia obrazovka funkcie Šifrovanie jednotky
Pozrite položku Overovanie funkciou Šifrovanie jednotky pri spúšťaní.

pripojené zariadenie
Hardvérové zariadenie, ktoré je pripojené k portu počítača.

reštartovanie
Proces reštartovania počítača.

ručné skartovanie
Okamžité skartovanie aktíva alebo vybraných aktív, ktorým sa obchádza plánované skartovanie.

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

skartovanie
Vykonanie algoritmu, ktorým sa bezvýznamnými údajmi prepisujú údaje obsiahnuté v aktíve.

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

softvérové šifrovanie
Použitie softvéru na zašifrovanie jednotlivých sektorov na pevnom disku. Tento proces je pomalší než hardvérové šifrovanie.

správca
Pozrite položku *Administrátor systému Windows*.

šifrovanie
Postup, ako je napríklad použitie algoritmu, využívaný v kryptografii na prevod obyčajného textu na šifrovaný text za účelom ochrany pred prečítaním daných údajov neoprávnenými príjemcami. Existuje veľa typov šifrovania údajov a predstavujú základ bezpečnosti v sieti. Medzi bežné typy patrí Data Encryption Standard (Norma šifrovania údajov) a šifrovanie verejným kľúčom.

Šifrovanie jednotky
Chráni vaše údaje prostredníctvom šifrovania pevných diskov, takže údaje si nemôžu prečítať neoprávnené osoby.

trieda zariadenia
Všetky zariadenia určitého typu, napríklad jednotky.

Trust Circle Manager/Reader

Trust Circle Reader môže len prijímať pozvánky odoslané používateľmi programu Trust Circle Manager. Trust Circle Manager však umožňuje vytváranie dôveryhodných okruhov. Medzi funkciami je e-mailové pozvanie do dôveryhodného okruhu a prijímanie pozvánok do dôveryhodného okruhu od ostatných. Keď je medzi partnermi nadviazaný dôveryhodný okruh, súbory chránené daným dôveryhodným okruhom je možné bezpečne zdieľať.

úvodná stránka
Centrálne miesto, kde máte prístup k funkciám a nastaveniam v aplikácii HP Client Security a môžete ich spravovať.

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

zabudovaný bezpečnostný čip Trusted Platform Module (TPM)
Modul TPM overuje počítač namiesto používateľa, ukladá informácie o konkrétnom hostiteľskom systéme, napríklad šifrovacie kľúče, digitálne certifikáty a heslá. Modul TPM minimalizuje riziko prezradenia informácií fyzickou krádežou alebo útokom externým hackerom.

zálohovanie
Pomocou funkcie zálohovania sa ukladá kópia dôležitých údajov programu na miesto mimo programu. Potom sa neskôr dá použiť na obnovenie údajov na rovnakom počítači alebo na inom.

zásady ovládania prístupu k zariadeniu
Zoznam zariadení, ku ktorým má používateľ povolený alebo zamietnutý prístup.

Register