HP ProtectTools

Začínáme

Bluetooth je ochranná známka příslušného vlastníka a je užívaná společností Hewlett-Packard Company v souladu s licencí. Intel je ochranná známka společnosti Intel Corporation v USA a dalších zemích a je užívána v souladu s licencí. Microsoft a Windows jsou registrované ochranné známky společnosti Microsoft Corporation v USA.

Informace uvedené v této příručce se mohou změnit bez předchozího upozornění. Jediné záruky na produkty a služby společnosti HP jsou výslovně uvedeny v prohlášení o záruce, které je každému z těchto produktů a služeb přiloženo. Žádná ze zde uvedených informací nezakládá další záruky. Společnost HP není zodpovědná za technické nebo redakční chyby ani za opomenutí vyskytující se v tomto dokumentu.

První vydání: srpen 2012

Číslo dokumentu: 702113-221

Obsah

1 Úvod k zabezpečení

Software HP ProtectTools Security Manager poskytuje funkce zabezpečení usnadňující ochranu proti neautorizovanému přístupu do počítače, sítě a k důležitým datům.

Aplikace	Funkce
Konzola pro správu nástroje HP ProtectTools Security Manager (pro správce)	• Možnost přístupu je podmíněna právy správce systému Microsoft Windows®. • Poskytuje přístup k modulům, jejichž konfiguraci obstarávají správci a které nejsou k dispozici uživatelům. • Umožňuje provést výchozí nastavení zabezpečení a konfiguraci možností nebo požadavků pro všechny uživatele.
Uživatelská konzola nástroje HP ProtectTools Security Manager (pro uživatele)	• Umožňuje uživatelům konfigurovat možnosti poskytované správcem. • Umožňuje správcům zajistit uživatelům omezený přístup k některým modulům nástroje HP ProtectTools.

Dostupnost softwarových modulů pro počítač je závislá na modelu počítače.

Softwarové moduly HP ProtectTools mohou být předinstalovány, předem zavedeny nebo k dispozici ke stažení na webu společnosti HP. Další informace naleznete na adrese http://www.hp.com.

POZNÁMKA: Pokyny v tomto průvodci jsou vytvořeny za předpokladu, že již máte nainstalovány příslušné softwarové moduly HP ProtectTools.

Vlastnosti aplikace HP ProtectTools

Následující tabulka obsahuje podrobnosti o hlavních vlastnostech modulů HP ProtectTools.

Modul	Hlavní vlastnosti
Konzola pro správu nástroje HP ProtectTools Security Manager	Správci mohou provádět následující funkce: • Použijte průvodce nastavením nástroje Security Manager k nastavení úrovní zabezpečení a metod zabezpečeného přihlašování. • Konfigurace možností nedostupných uživatelům. • Aktivujte modul Drive Encryption a konfigurujte uživatelský přístup. • Konfigurujte zásady Device Access Manager a uživatelský přístup. • Použijte nástroje správce k přidání a odebrání uživatelů a zobrazení stavu uživatelů aplikace HP ProtectTools.

Modul	Hlavní vlastnosti
Uživatelská konzola nástroje HP ProtectTools Security Manager	Obecní uživatelé mohou provádět následující funkce: • Nastavení zobrazení stavu šifrování a aplikace Device Access Manager. • Aktivace služby Computrace for HP ProtectTools. • Konfigurace předvoleb a možností zálohování a obnovení.
Credential Manager	Obecní uživatelé mohou provádět následující funkce: • Změnit uživatelská jména a hesla. • Konfigurace a změna údajů o uživateli, jako např. heslo systému Windows, otisk prstu, snímek tváře, čipová karta, karta s detekcí přiblížení nebo bezkontaktní karta.
Password Manager	Obecní uživatelé mohou provádět následující funkce: • Uspořádání a nastavení uživatelských jmen a hesel. • Vytváření silnějších hesel pro rozšířené zabezpečení účtu. Nástroj Password Manager umožňuje zadávat a odesílat informace automaticky. • Můžete zjednodušit přihlašování pomocí funkce jednotného přihlášení, která automaticky ukládá a používá údaje o uživateli.
Nástroj Drive Encryption for HP ProtectTools (pouze u vybraných modelů)	• Poskytuje kompletní šifrování celých oddílů pevných disků. • Vynucuje ověřování před spuštěním za účelem dešifrování a zajištění přístupu k datům. • Umožňuje aktivaci automatického šifrování jednotek (pouze u vybraných modelů).
Aplikace Device Access Manager for HP ProtectTools (pouze u vybraných modelů)	• Umožňuje správcům IT řídit přístup k zařízením podle uživatelských profilů. • Chrání před odstraněním dat neoprávněnými uživateli pomocí externích úložných médií a chrání před nakažením viry z externích médií. • Umožňuje správcům zamezit přístup jednotlivým uživatelům nebo jejich skupinám ke komunikačním zařízením.
Obnova po krádeži (služba Computrace for HP ProtectTools, prodává se samostatně)	• K aktivaci je zapotřebí samostatné zakoupení odběru služby sledování položek. • Poskytuje možnost zabezpečeného sledování položek. • Umožňuje sledovat aktivity uživatele stejně jako změny v hardwaru a softwaru. • Zůstává aktivní i po naformátování nebo výměně pevného disku.

Popis bezpečnostního produktu HP ProtectTools a příklady běžného využití

Většina bezpečnostních produktů HP ProtectTools umožňuje přístup uživatele s ověřením (nejčastěji pomocí hesla) i záložní přístup pro správce v případě ztráty, nedostupnosti nebo zapomenutí hesla nebo v případě potřeby přístupu bezpečnostním pracovníkem společnosti.

POZNÁMKA: Některé bezpečnostní produkty HP ProtectTools jsou navrženy tak, aby zabránily přístupu k datům. Pokud je citlivost dat natolik vysoká, že je před jejich zneužitím upřednostňována jejich ztráta, je vhodné je šifrovat. Doporučujeme všechna data zálohovat na bezpečném místě.

Password Manager

Modul Password Manager slouží k ukládání uživatelských jmen a hesel a je možné jej použít k následujícímu:

- Ukládání přihlašovacích jmen a hesel potřebných k přístupu na Internet nebo k e-mailu.
- Automatické přihlášení uživatele k webové stránce nebo e-mailu.
- Správa ověřování a uspořádání souvisejících dat.
- Výběr položky na webu nebo v síti a přímé otevření adresy v odkazu.
- Zobrazení jmen a hesel v případě potřeby.

Příklad 1: Pracovnice v oddělení nákupu pracující pro velkého výrobce provádí většinu transakcí po Internetu. Často také používá několik známých webových stránek vyžadujících přihlášení. Důsledně dodržuje vhodnou úroveň zabezpečení, a nepoužívá proto stejné heslo u všech účtů. Pracovnice v oddělení nákupu se rozhodla použít nástroj Password Manager k propojení odkazů na web s různými uživatelskými jmény a hesly. Pokud následně otevře webovou stránku a pokusí se o přihlášení, nástroj Password Manager automaticky poskytne potřebné přihlašovací údaje. Pokud si bude chtít prohlédnout uživatelská jména a hesla, nástroj Password Manager lze nastavit tak, aby je zobrazil.

Modul Password Manager je možné používat také ke správě ověřování a uspořádání souvisejících dat. Tento nástroj umožňuje uživateli výběr položky na webu nebo v síti a přímé otevření adresy v odkazu. Uživatel také může v případě potřeby zobrazit jména a hesla.

Příklad 2: Těžce pracující autorizovaný účetní byl povýšen a bude nyní spravovat celé účetní oddělení. Tým se musí přihlašovat k velkému počtu klientských webových účtů, z nichž každý využívá jiné přihlašovací údaje. Tyto přihlašovací údaje je třeba sdílet s ostatními pracovníky a zachování jejich důvěrnosti je tedy klíčové. Autorizovaný účetní se rozhodl pro uspořádání všech odkazů na web, uživatelských jmen a hesel v rámci nástroje Password Manager. Po dokončení účetní nasadí nástroj Password Manager k používání zaměstnancům, kteří tak mohou využívat webové účty bez jakýchkoli informací o používaných přihlašovacích údajích.

Nástroj Drive Encryption for HP ProtectTools (pouze u vybraných modelů)

Nástroj Drive Encryption je používán k omezení přístupu k datům na pevném disku počítače nebo na sekundárním pevném disku. Nástroj Drive Encryption je možné použít také ke správě jednotek s automatickým šifrováním.

Příklad 1: Doktor chce mít jistotu, že je jediný, kdo má přístup k datům na pevném disku počítače. Doktor aktivuje nástroj Drive Encryption, který vyžaduje před přihlášením do systému Windows provedení ověřování před spuštěním. Po dokončení nastavení nebude možné pevný disk používat bez zadání hesla před spuštěním operačního systému. Doktor může zabezpečení dále posílit šifrováním dat pomocí funkce automatického šifrování.

Nástroj Drive Encryption for HP ProtectTools neumožňuje přístup k šifrovaným datům ani v případě, kdy je disk odpojen, protože jsou vázané na původní základní desku.

Příklad 2: Správce v nemocnici si chce být jistý, že přístup k datům na místních počítačích budou mít pouze doktoři a pověření pracovníci, a to bez sdílení svých osobních hesel. Oddělení IT přidá správce, doktory a všechny pověřené pracovníky mezi uživatele nástroje Drive Encryption. Od této

chvíle budou moci spustit počítač nebo použít doménu za pomocí osobního uživatelského jména a hesla pouze dané pověřené osoby.

Aplikace Device Access Manager for HP ProtectTools (pouze u vybraných modelů)

Aplikace Device Access Manager for HP ProtectTools umožňuje správcům omezit a spravovat přístup k hardwaru. Aplikaci Device Access Manager for HP ProtectTools je možné používat k blokování neoprávněného přístupu k diskům USB flash, pomocí kterých mohou být kopírována data. Umožňuje také omezit přístup k diskům CD/DVD, spravovat zařízení USB, síťová připojení, atd. Vhodným příkladem by byla situace, ve které prodejci mimo pracoviště potřebují přístup k firemním počítačům, avšak bez možnosti kopírování dat na jednotku USB.

Příklad 1: Správce společnosti v oboru zásobování lékařským materiálem často pracuje spolu s firemními informacemi také s osobními lékařskými záznamy. Zaměstnanci potřebují mít k těmto datům přístup, je však nesmírně důležité, aby tato data pomocí jednotky USB nebo jiného externího úložiště nepřenášeli. Zabezpečení sítě je kvalitní, ale počítače jsou vybaveny mechanikami s možností zápisu na disky CD a porty USB, které umožňují kopírování nebo krádež dat. Správce použije aplikaci Device Access Manager k zablokování portů USB a vypalovaček disků CD tak, že jejich použití nebude možné. I když budou porty USB blokovány, funkce myši a klávesnice nebude nijak omezena.

Příklad 2: Pojišťovna si nepřeje, aby její zaměstnanci instalovali nebo používali osobní software nebo data přinesená z domu. Někteří zaměstnanci vyžadují přístup k portům USB na všech počítačích. Správce IT použije aplikaci Device Access Manager k povolení přístupu pouze některým zaměstnancům a zablokování externího přístupu všem ostatním.

Služba Computrace for HP ProtectTools (dříve pod názvem LoJack Pro) – k zakoupení samostatně

Služba Computrace for HP ProtectTools (prodává se samostatně) umožňuje vysledovat místo odcizeného počítače vždy, kdy se jeho uživatel připojí k Internetu. Služba Computrace for HP ProtectTools umožňuje také vzdáleně spravovat a sledovat polohu počítačů, monitorovat jejich využití a kontrolovat používané aplikace.

Příklad 1: Ředitel školy požádá oddělení IT o sledování všech počítačů ve škole. Po vytvoření soupisu počítačů oddělení IT všechny počítače zaregistruje ve službě Computrace, a umožní tak jejich sledování v případě krádeže. Po nějaké době se zjistí, že ve škole několik počítačů chybí a oddělení IT uvědomí odpovídající orgány a pracovníky služby Computrace. Počítače budou nalezeny a příslušnými úřady škole navráceny.

Příklad 2: Realitní společnost potřebuje řešení správy a aktualizace počítačů po celém světě. Rozhodnou se používat službu Computrace, a využít tak možnosti aktualizovat počítače bez nutnosti vysílat ke každému z nich pracovníka IT.

Dosažení hlavních cílů zabezpečení

Moduly HP ProtectTools mohou vzájemně řešit různé bezpečnostní otázky včetně následujících hlavních bezpečnostních cílů:

- ochrana před cílenou krádeží,
- omezení přístupu k citlivým datům,
- zabránění neoprávněnému přístupu z interních nebo externích míst,
- vytvoření zásad pro silná hesla.

Ochrana před cílenou krádeží

Příkladem cílené krádeže může být krádež počítače obsahujícího důvěrná data a informace o zákaznících u bezpečnostního kontrolního bodu na letišti. Proti cílené krádeži chrání následující funkce:

- Aktivací funkce ověřování před spuštěním zabráníte přístupu do operačního systému.
  - Nástroj Security Manager for HP ProtectTools – viz HP ProtectTools Security Manager na stránce 25.
  - Nástroj Drive Encryption for HP ProtectTools – viz Nástroj Drive Encryption for HP ProtectTools (pouze u vybraných modelů) na stránce 41.
- Šifrování chrání data před přístupem, i když je pevný disk odebraný a nainstalovaný do nezabezpečeného systému.
- Služba Computrace umožňuje sledovat polohu odcizeného počítače.
  - Služba Computrace for HP ProtectTools – viz Obnova po krádeži (pouze u vybraných modelů) na stránce 61.

Omezení přístupu k citlivým datům

Představte si například, že na pracovišti pracuje auditor smluvních vztahů, kterému byl umožněn přístup k počítači za účelem kontroly citlivých finančních údajů. Nepřejete si však, aby auditor mohl soubory vytisknout nebo je uložit na zapisovatelné médium, např. disk CD. Následující funkce napomáhají omezit přístup k datům:

- Modul Device Access Manager for HP ProtectTools umožňuje správcům IT omezit přístup ke komunikačním zařízením, aby citlivé informace nebylo možné kopírovat z pevného disku. Viz část Zobrazení Device Class Configuration (Konfigurace tříd zařízení) na stránce 52.

Zabránění neoprávněnému přístupu z interních nebo externích míst

Neoprávněný přístup k nezabezpečenému firemnímu počítači představuje velice reálné ohrožení prostředků podnikové sítě, jako např. dat finančních služeb, informace vedení nebo oddělení výzkumu a vývoje nebo soukromých dat (např. záznamy o pacientovi nebo osobní finanční údaje). Následující funkce pomáhají zabránit neoprávněnému přístupu:

- Aktivací funkce ověřování před spuštěním zabráníte přístupu do operačního systému:
  - Nástroj Security Manager for HP ProtectTools – viz HP ProtectTools Security Manager na stránce 25.
  - Nástroj Drive Encryption for HP ProtectTools – viz Nástroj Drive Encryption for HP ProtectTools (pouze u vybraných modelů) na stránce 41.
- Nástroj Security Manager brání neoprávněnému uživateli, aby získal hesla nebo přístup k aplikacím chráněným heslem. Viz část HP ProtectTools Security Manager na stránce 25.
- Modul Device Access Manager for HP ProtectTools umožňuje správcům IT omezit přístup k zařízením s možností zápisu, takže citlivé informace nelze kopírovat z pevného disku. Viz část Device Access Manager for HP ProtectTools (jen vybrané modely) na stránce 50.

Vytvoření zásad pro silná hesla

Když vstoupí v platnost nařízení společnosti, které vyžaduje použití silných zásad zabezpečení hesly pro desítky aplikací a databází pracujících v síti, aplikace Security Manager poskytuje chráněné

úložiště pro hesla a pohodlnou funkci Single Sign On (Jednotné přihlášení). Viz část HP ProtectTools Security Manager na stránce 25.

Další prvky zabezpečení

Přiřazení rolí zabezpečení

Při správě zabezpečení počítače (převážně u velkých organizací) hraje důležitou roli rozdělení odpovědností a práv mezi různé typy správců a uživatelů.

POZNÁMKA: U malých organizací a jednotlivých uživatelů mohou být všechny tyto role v rukou stejné osoby.

V případě nástrojů HP ProtectTools mohou být bezpečnostní funkce a oprávnění rozděleny do následujících rolí:

- Security officer (Správce zabezpečení) – určuje úroveň zabezpečení společnosti nebo sítě a určuje, jaké funkce zabezpečení se mají použít, například nástroj Drive Encryption.

  POZNÁMKA: Mnoho z funkcí nástrojů HP ProtectTools lze přizpůsobit správcem zabezpečení ve spolupráci se společností HP. Další informace naleznete na adrese http://www.hp.com.

- IT administrator (Správce IT) – aplikuje a spravuje funkce zabezpečení určené správcem zabezpečení. Může také aktivovat a deaktivovat některé funkce. Pokud se správce zabezpečení například rozhodne použít čipové karty, může správce IT aktivovat režim zabezpečení heslem i čipovými kartami.
- User (Uživatel) – používá funkce zabezpečení. Pokud například správce zabezpečení a správce IT v systému aktivovali použití čipových karet, může uživatel nastavit kód PIN čipové karty a používat ji pro ověřování.

UPOZORNĚNÍ: Správcům se doporučuje, aby se při omezování oprávnění a přístupu koncových uživatelů řídili “nejlepšími způsoby”.

Neoprávnění uživatelé by neměli mít oprávnění správce.

Správa hesel nástrojů HP ProtectTools

Většina funkcí nástroje HP ProtectTools Security Manager je zabezpečena hesly. Následující tabulka uvádí běžná hesla, softwarový modul, ve kterém je dané heslo použito, a funkce hesla.

V této tabulce jsou i hesla, která jsou nastavena a používána jen správci IT. Všechna ostatní hesla mohou být nastavena běžnými uživateli nebo správci.

Heslo nástrojů HP ProtectTools	Nastaveno v tomto modulu	Funkce
Heslo pro přihlášení do systému Windows	Ovládací panely systému Windows nebo nástroj HP ProtectTools Security Manager	Lze použít k ručnímu přihlášení nebo ověření přístupu k různým funkcím aplikace Security Manager.

Heslo nástrojů HP ProtectTools	Nastaveno v tomto modulu	Funkce
Heslo nástroje Security Manager Backup and Recovery	Security Manager, podle jednotlivých uživatelů	Chrání přístup k souboru nástroje Security Manager Backup and Recovery.
Kód PIN čipové karty	Credential Manager	Umožňuje použití ověřování pomocí několika faktorů. Umožňuje použití ověřování systému Windows. Ověřuje uživatele nástroje Drive Encryption, pokud je vybrána čipová karta.

Vytvoření bezpečného hesla

Při vytváření hesel je třeba postupovat podle pokynů daného programu. Obecně se řiďte následujícími pokyny, které vám pomohou vytvořit silné heslo a zabránit jeho zjištění:

- Používejte hesla obsahující více než 6 znaků, pokud možno více než 8 znaků.
- V rámci hesla používejte malá a velká písmena.
- Kdykoli je to možné, používejte společně alfanumerické znaky, zvláštní znaky a interpunkční znaménka.
- Nahraďte písmena hesla zvláštními znaky nebo číslicemi. Použijte například číslici 1 pro znak I nebo L.
- Použijte slova ze 2 či více jazyků.
- Rozdělte slovo nebo frázi uprostřed čísly nebo zvláštními znaky, příklad: “Mary2-2Cat45.”
- Nepoužívejte heslo, které je ve slovníku.
- Nepoužívejte jako heslo svoje jméno nebo jakékoli jiné osobní údaje jako datum narození, jména domácích mazlíčků nebo jméno matky za svobodna, ani napsané pozpátku.
- Heslo měňte pravidelně. Můžete jen přidat několik znaků.
- Pokud si heslo zapíšete, nedávejte je na běžné místo v blízkosti počítače.
- Neukládejte heslo do souboru v počítači, například do e-mailu.
- Nesdílejte účty ani nikomu heslo neříkejte.

Zálohování přihlašovacích údajů a nastavení

Přihlašovací údaje můžete zálohovat následujícími způsoby:

- Použijte nástroj Drive Encryption for HP ProtectTools k volbě a zálohování přihlašovacích údajů HP ProtectTools.
- Použijte nástroj Backup and Recovery aplikace HP ProtectTools Security Manager jako centrální místo pro zálohování a obnovu přihlašovacích údajů z některých nainstalovaných modulů HP ProtectTools.

2 Začínáme

Chcete-li zkonfigurovat nastavení pro nástroj HP ProtectTools, použijte Průvodce nastavením nástroje HP Client Security nebo Průvodce nastavením nástroje HP ProtectTools Security Manager.

Po dokončení Průvodce nastavením nástroje HP Client Security je stav aplikace zobrazen na nástrojového panelu nástroje HP Client Security.

Průvodce nastavením nástroje HP Client Security

POZNÁMKA: Správa nástroje HP ProtectTools vyžaduje oprávnění správce.

Průvodce nastavením nástroje HP Client Security vás provede nastavením nejčastěji používaných funkcí nástroje Security Manager. Pokud jste ještě nedokončili Průvodce nastavením nástroje HP Client Security, můžete jej spustit jedním z následujících způsobů:

▲ Na úvodní obrazovce klikněte nebo klepněte na aplikaci **HP Client Security**.

– nebo –

Z plochy systému Windows klikněte nebo klepněte na aplikaci **HP ProtectTools**.

Stránky jsou zobrazeny v následujícím pořadí:

1. **Heslo systému Windows** – zadejte heslo pro systém Windows.

   Tím se účet v systému Windows ochrání pomocí silného ověřování.

2. **SpareKey** – chcete-li zaregistrovat možnost SpareKey, vyberte tři bezpečnostní otázky.

3. **Zaregistrovat otisky prstů** – pokud je nainstalovaná čtečka otisků prstů a příslušný ovladač, můžete zaregistrovat otisky prstů. Musíte vybrat a zaregistrovat nejméně dva otisky prstů.

4. **Drive Encryption** – je-li nainstalován nástroj Drive Encryption for HP ProtectTools, můžete aktivovat zašifrování a primárním disku:

   - Softwarové šifrování pro tradiční pevný disk
   - Hardwarové šifrování, pokud je detekována jednotka s automatickým šifrováním.

   Před povolením šifrování musíte uložit šifrovací klíč na jedno nebo více následujících zařízení:

   POZNÁMKA: Pokud v tuto chvíli stornujete průvodce, nebudete schopni aktivovat ověřování systému Windows a Drive Encryption.

   - **Vyměnitelné médium**, jako je jednotka USB flash se souborovým formátem FAT 32.
     - Tato možnost je vybrána ve výchozím nastavení, pokud je detekováno jediné vyměnitelné zařízení před zobrazením stránky aplikace Drive Encryption.
     - Je-li detekováno dvě a více vyměnitelných zařízení, vyberte jednu ze zobrazených jednotek.
   - **SkyDrive** – tato možnost je k dispozici, je-li detekováno připojení k internetu.

Vyžaduje se účet Windows® Live ID. Zadejte své ID a heslo, nebo se zaregistrujte.

5. Stránka Dokončit zobrazí úspěšné oznámení a vyzve vás k restartování pro aktivaci funkce Drive Encryption.

Průvodce nastavením nástroje HP ProtectTools Security Manager

POZNÁMKA: Správa nástroje HP ProtectTools vyžaduje oprávnění správce.

Průvodce nastavením nástroje HP ProtectTools Security Manager vás provede nastavením funkcí nástroje Security Manager. Pomocí Konzoly pro správu lze nakonfigurovat nastavení, která se nacházejí v průvodci, a také mnohé další funkce zabezpečení. Tato nastavení platí pro daný počítač a všechny uživatele, kteří tento počítač sdílejí.

Postup spuštění Průvodce nastavením nástroje HP ProtectTools Security Manager:

▲ Klikněte na příkaz **Průvodce nastavení** v levém panelu Konzole pro správu a poté postupujte podle instrukcí na obrazovce do dokončení nastavení.

Správci mohou spustit Konzolu pro správu z Uživatelské konzoly nástroje HP ProtectTools Security Manager. Další informace naleznete v části Konzola pro správu nástroje HP ProtectTools Security Manager na stránce 14.

Nástroj Security Manager a jeho aplikace jsou dostupné všem uživatelům, kteří sdílejí tento počítač.

Nástrojový panel nástroje HP Client Security

Postup spuštění nástroje HP Client Security, pokud jste dříve dokončili Průvodce nastavením nástroje HP Client Security:

▲ Na úvodní obrazovce napište heslo `hp` a poté vyberte aplikaci **HP Client Security**.

Nástrojový panel zobrazuje rychlý přehled funkcí a příslušný stav každé aplikace.

▲ Klikněte nebo klepněte na řádek aplikace, abyste pro vybranou aplikaci zobrazili více informací:

- Tlačítko **Konfigurovat nyní** indikuje ještě nezkonfigurovanou aplikaci. Klikněte nebo klepněte na toto tlačítko, abyste otevřeli stránku aplikace a zkonfigurovali ji.
- Tlačítko **Nastavení** indikuje aplikaci se stavem OK. Klikněte nebo klepněte na toto tlačítko, abyste přistoupili na nastavení aplikace.
- Nástroj **Uživatelská konzola** se spouští pro uživatelskou konfiguraci.
- Nástroj **Konzola pro správu** se spouští pro konfiguraci vyžadující pověření správce.
- Nástroj **Stav nástrojového panelu** zůstává otevřený po spuštění Uživatelské konzoly nebo Konzoly pro správu a po zkonfigurování nastavení a zavření Konzoly je stav aktualizován.

3 Průvodce snadným nastavením pro malé firmy

Tato kapitola popisuje základní kroky pro aktivaci nejběžnějších a nejužitečnějších možností aplikace HP ProtectTools for Small Business. Tato aplikace nabízí řadu nástrojů a možností, které umožňují jemně doladit vaše předvolby a nastavit řízení přístupu. Tento průvodce snadným nastavením je zaměřen na to, aby každý modul mohl být spuštěn s minimálním úsilím a v co možná nejkratší době. Budete-li chtít získat další informace, vyberte modul, o který máte zájem, a klikněte na **?** nebo na tlačítko Nápověda v horním pravém rohu. Toto tlačítko vám poskytne informace o použití aktuálního zobrazeného okna.

Začínáme

1. Na ploše systému Windows spusťte nástroj HP ProtectTools Security Manager dvojitým kliknutím na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.
2. Zadejte heslo systému Windows nebo vytvořte heslo systému Windows.
3. Dokončete průvodce nastavením.

POZNÁMKA: Ve výchozím nastavení je nástroj HP ProtectTools Security Manager nastaven na zásady silného ověřování.

Toto nastavení zabraňuje neoprávněnému přístupu při přihlášení do systému Windows a doporučujeme je používat, pokud je požadováno vysoké zabezpečení nebo pokud jsou uživatelé během dne často pryč od počítače. Pokud toto nastavení chcete změnit, klikněte na kartu Zásady relace a proveďte volbu.

Chcete-li, aby nástroj HP ProtectTools Security Manager vyžadoval ověření pouze jednou během přihlášení do systému Windows, postupujte takto.

1. Na ploše systému Windows spusťte nástroj HP ProtectTools Security Manager dvojitým kliknutím na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.
2. V levém podokně klikněte na položku **Správa** a poté na položku **Konzola pro správu**.
3. V levém podokně vyberte v části **Systém** ze skupiny **Zabezpečení** položku **Ověření**.
4. Klikněte na kartu **Zásady relace** a poté vyberte požadavky kombinace přihlášení pro příslušnou relaci. Tyto volby stornujete kliknutím na možnost **Obnovit výchozí nastavení**.
5. Akci dokončete kliknutím na tlačítko **Použít**.

Password Manager

Hesla! Všichni jich máme docela velké množství – zvláště, pokud pravidelně přistupujete na webové stránky nebo používáte aplikace, které vyžadují přihlášení. Běžný uživatel používá stejná hesla pro každou aplikaci a webovou stránku, nebo se stává opravdu kreativní a okamžitě zapomene, jaké heslo patří ke které aplikaci.

Nástroj Password Manager si dokáže automaticky zapamatovat hesla nebo nabízí možnost rozlišit, které stránky si zapamatovat a které vynechat. Po přihlášení na počítači poskytne nástroj Password Manager hesla nebo přihlašovací údaje pro podílející se aplikace nebo webové stránky.

Při pokusu o přístup k aplikaci nebo na web, který vyžaduje přihlašovací údaje, nástroj Password Manager automaticky rozpozná danou aplikaci či web a zobrazí dotaz, zda si má údaje pamatovat. Pokud chcete, vyloučit některé weby, můžete žádost zamítnout.

Aktivace ukládání webů, uživatelských jmen a hesel:

1. Jako příklad přejděte na podílející se webovou stránku nebo aplikaci a poté klikněte na ikonu nástroje Password Manager v levém horním rohu webové stránky, abyste přidali webové ověření.
2. Pojmenujte odkaz (volitelné) a zadejte do nástroje Password Manager uživatelské jméno a heslo.

POZNÁMKA: Oblasti, které nástroj Password Manager použije nyní a pro další návštěvy, budou zvýrazněny.

3. Po skončení klikněte na tlačítko **OK**.
4. Nástroj Password Manager také umožňuje ukládání uživatelského jména a hesla pro síťové složky a namapované síťové jednotky.

Zobrazení a správa uložených přihlašovacích údajů v nástroji Password Manager

Nástroj Password Manager umožňuje zobrazit, spravovat, zálohovat a použít přihlašovací údaje z jediného místa. Nástroj Password Manager také podporuje otevírání uložených webů v systému Windows.

Nástroj Password Manager spusťte jedním z následujících způsobů:

- Pomocí kláves ctrl+Windows+h spusťte nástroj Password Manager a kliknutím na tlačítko **Otevřít** otevřete a ověřte uloženého zástupce.

  – nebo –

- Vyberte kartu **Správa** v nástroji Password Manager, abyste otevřeli nástroj HP ProtectTools Security Manager a mohli upravit přihlašovací údaje.

Možnost **Upravit** nástroje Password Manager umožňuje zobrazovat a upravovat jméno, přihlašovací jméno a dokonce i odhalovat hesla.

Nástroj HP ProtectTools for Small Business umožňuje zálohovat anebo zkopírovat všechny přihlašovací údaje a nastavení na jiný počítač.

Aplikace Device Access Manager for HP ProtectTools

Nástroj Device Access Manager lze použít k zakázání použití různých interních a externích úložišť, aby byla data vaší firmy maximálně zabezpečena. Můžete například povolit uživatelský přístup

k datům, ale blokovat jejich kopírování na disk, osobní přehrávač hudby nebo paměťové zařízení USB. Níže následujte snadný postup, jak toto zajistit.

1. Na ploše systému Windows spusťte uživatelskou konzolu nástroje HP ProtectTools Security Manager dvojitým kliknutím na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.
2. V levém podokně nástroje HP ProtectTools Security Manager klikněte na položku **Správa** a poté na položku **Konzola pro správu**.
3. Klikněte na položku **Device Access Manager** a poté na položku **Konfigurace tříd zařízení**.
4. Dalším krokem je volba uživatele, který bude mít i nadále přístup, zatímco každý jiný uživatel bude mít přístup blokován.
5. Vyberte hardwarová zařízení, která chcete zakázat, a proces dokončete kliknutím na tlačítko **Použít**.
6. Vyberte příkaz **Přidat**, klikněte na položku **Pokročilé** a poté na příkaz **Hledat nyní**.
7. Vyberte požadovaného uživatele a pak klikněte na příkaz **OK > OK > Použít**.

   Výběr se zobrazí v poli **Uživatelé/skupiny**.
8. Vyberte položku **Třída zařízení**, kterou bude uživatel používat, vyberte příkaz **Povolit** nebo **Zamítnout** a poté klikněte na příkaz **Použít**.

Aplikace Drive Encryption for HP ProtectTools

Nástroj Drive Encryption for HP ProtectTools slouží k ochraně dat šifrováním celého pevného disku. Data na pevném disku budou chráněna, i pokud bude počítač ukraden nebo bude z počítače odebrán pevný disk a nainstalován do jiného počítače.

Další bezpečností výhodou je, že nástroj Drive Encryption vyžaduje, abyste se před spuštěním operačního systému správně ověřili pomocí svého uživatelského jména a hesla. Tento proces se nazývá ověření před spuštěním.

Aby byl snadno proveditelný, řada softwarových modulů provádí synchronizaci hesel automaticky, včetně uživatelských účtů systému Windows, domén, nástroje Drive Encryption for HP ProtectTools, Password Manager a HP ProtectTools Security Manager.

Následující jednoduché kroky popisují aktivaci nástroje Drive Encryption for HP ProtectTools:

1. Na ploše systému Windows spusťte nástroj HP ProtectTools Security Manager dvojitým kliknutím na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.
2. V levém podokně klikněte na položku **Správa** a poté na položku **Konzola pro správu**.
3. V levém podokně klikněte na položku **Průvodce nastavením**.
4. Na uvítací stránce vyberte možnost **Další**.
5. Zadejte heslo systému Windows a spusťte průvodce aktivací, poté klikněte na tlačítko **Další**.
6. Vynechejte nástroj SpareKey, pokud není vyžadován.
7. Zaškrtněte políčko **Drive Encryption** a poté klikněte na tlačítko **Další**.
8. Zaškrtněte jednotku, kterou chcete šifrovat, a poté klikněte na tlačítko **Další**.
9. Konfigurační okno nástroje Drive Encryption vyžaduje jednotku USB flash nebo jiné externí zařízení, na které uloží obnovovací klíč zašifrování. Uchovávejte tento obnovovací klíč bezpečný

a zajištěný, protože se používá k obnovení dat nebo k přístupu na jednotku v případě ztráty nebo neúspěchu hesla před spuštěním.

10. Proces dokončete kliknutím na tlačítko **Další** a poté **Dokončit**. Vyjměte jednotku USB flash a poté restartujte počítač, jakmile budete připraveni.

11. Jakmile se systém spustí, nástroj Drive Encryption bude vyžadovat heslo systému Windows. Heslo zadejte a klikněte na tlačítko **OK**.

POZNÁMKA: V průběhu šifrování jednotky se může zdát, že počítač pracuje pomalu. Po úplném zašifrování se výkon počítače vrátí zpět do normálu. Data jsou během přístupu na jednotku šifrována nebo dešifrována podle potřeby správce.

Ověřování nástrojem Drive Encryption se “zřetězí” přes přihlášení do systému Windows přímo na plochu systému Windows, takže nebude nutné, abyste zadávali své heslo dvakrát.

4 Konzola pro správu nástroje HP ProtectTools Security Manager

Software HP ProtectTools Security Manager poskytuje funkce zabezpečení usnadňující ochranu proti neautorizovanému přístupu do počítače, sítě a k důležitým datům. Správa nástroje HP ProtectTools Security Manager se provádí prostřednictvím funkce Konzola pro správu.

Nástrojový panel aplikace Uživatelská konzola nástroje Security Manager nabízí další aplikace (pouze vybrané modely), které pomáhají s obnovením počítače v případě ztráty nebo odcizení.

Použití Konzoly pro správu umožňuje místnímu správci systému provádět následující úlohy:

- Povolení nebo zakázání funkcí zabezpečení
- Specifikace požadovaných přihlašovacích údajů pro ověření
- Správa uživatelů počítače
- Nastavování parametrů specifických pro zařízení
- Konfigurace instalovaných aplikací Security Manager

Začínáme

Chcete-li zkonfigurovat nastavení pro nástroj HP ProtectTools, použijte Průvodce nastavením nástroje HP Client Security nebo Průvodce nastavením nástroje HP ProtectTools Security Manager.

Po dokončení Průvodce nastavením nástroje HP Client Security je stav aplikace zobrazen na nástrojového panelu nástroje HP Client Security.

Průvodce nastavením nástroje HP Client Security

POZNÁMKA: Správa nástroje HP ProtectTools vyžaduje oprávnění správce.

Průvodce nastavením nástroje HP Client Security vás provede nastavením nejčastěji používaných funkcí nástroje Security Manager. Pokud jste ještě nedokončili Průvodce nastavením nástroje HP Client Security, můžete jej spustit jedním z následujících způsobů:

▲ Na úvodní obrazovce klikněte nebo klepněte na aplikaci **HP Client Security**.

– nebo –

Z plochy systému Windows klikněte nebo klepněte na aplikaci **HP ProtectTools**.

Stránky jsou zobrazeny v následujícím pořadí:

1. **Heslo systému Windows** – zadejte heslo pro systém Windows.

   Tím se účet v systému Windows ochrání pomocí silného ověřování.

2. **SpareKey** – chcete-li zaregistrovat možnost SpareKey, vyberte tři bezpečnostní otázky.
3. **Zaregistrovat otisky prstů** – pokud je nainstalovaná čtečka otisků prstů a příslušný ovladač, můžete zaregistrovat otisky prstů. Musíte vybrat a zaregistrovat nejméně dva otisky prstů.

4. **Drive Encryption** – je-li nainstalován nástroj Drive Encryption for HP ProtectTools, můžete aktivovat zašifrování a primárním disku:

   - Softwarové šifrování pro tradiční pevný disk
   - Hardwarové šifrování, pokud je detekována jednotka s automatickým šifrováním.

   Před povolením šifrování musíte uložit šifrovací klíč na jedno nebo více následujících zařízení:

   POZNÁMKA: Pokud v tuto chvíli stornujete průvodce, nebudete schopni aktivovat ověřování systému Windows a Drive Encryption.

   - **Vyměnitelné médium**, jako je jednotka USB flash se souborovým formátem FAT 32.
     - Tato možnost je vybrána ve výchozím nastavení, pokud je detekováno jediné vyměnitelné zařízení před zobrazením stránky aplikace Drive Encryption.
     - Je-li detekováno dvě a více vyměnitelných zařízení, vyberte jednu ze zobrazených jednotek.
   - **SkyDrive** – tato možnost je k dispozici, je-li detekováno připojení k internetu.

     Vyžaduje se účet Windows® Live ID. Zadejte své ID a heslo, nebo se zaregistrujte.

5. Stránka Dokončit zobrazí úspěšné oznámení a vyzve vás k restartování pro aktivaci funkce Drive Encryption.

Průvodce nastavením nástroje HP ProtectTools Security Manager

POZNÁMKA: Správa nástroje HP ProtectTools vyžaduje oprávnění správce.

Průvodce nastavením nástroje HP ProtectTools Security Manager vás provede nastavením funkcí nástroje Security Manager. Pomocí Konzoly pro správu lze nakonfigurovat nastavení, která se nacházejí v průvodci, a také mnohé další funkce zabezpečení. Tato nastavení platí pro daný počítač a všechny uživatele, kteří tento počítač sdílejí.

Postup spuštění Průvodce nastavením nástroje HP ProtectTools Security Manager:

▲ Klikněte na příkaz **Průvodce nastavení** v levém panelu Konzole pro správu a poté postupujte podle instrukcí na obrazovce do dokončení nastavení.

Správci mohou spustit Konzolu pro správu z Uživatelské konzoly nástroje HP ProtectTools Security Manager. Další informace naleznete v části Konzola pro správu nástroje HP ProtectTools Security Manager na stránce 14.

Nástroj Security Manager a jeho aplikace jsou dostupné všem uživatelům, kteří sdílejí tento počítač.

Nástrojový panel nástroje HP Client Security

Postup spuštění nástroje HP Client Security, pokud jste dříve dokončili Průvodce nastavením nástroje HP Client Security:

▲ Na úvodní obrazovce napište heslo `hp` a poté vyberte aplikaci **HP Client Security**.

Nástrojový panel zobrazuje rychlý přehled funkcí a příslušný stav každé aplikace.

▲ Klikněte nebo klepněte na řádek aplikace, abyste pro vybranou aplikaci zobrazili více informací:

- Tlačítko **Konfigurovat nyní** indikuje ještě nezkonfigurovanou aplikaci. Klikněte nebo klepněte na toto tlačítko, abyste otevřeli stránku aplikace a zkonfigurovali ji.
- Tlačítko **Nastavení** indikuje aplikaci se stavem OK. Klikněte nebo klepněte na toto tlačítko, abyste přistoupili na nastavení aplikace.
- Nástroj **Uživatelská konzola** se spouští pro uživatelskou konfiguraci.
- Nástroj **Konzola pro správu** se spouští pro konfiguraci vyžadující pověření správce.
- Nástroj **Stav nástrojového panelu** zůstává otevřený po spuštění Uživatelské konzoly nebo Konzoly pro správu a po zkonfigurování nastavení a zavření Konzoly je stav aktualizován.

Otevření konzoly pro správu nástroje HP ProtectTools

Konzolu pro správu nástroje HP ProtectTools použijte pro provádění správy, např.: nastavení zásad systému nebo konfiguraci softwaru. Přístup k Uživatelské konzole spuštěním aplikace HP ProtectTools Security Manager:

1. Na ploše systému Windows dvakrát klikněte na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.

   – nebo –

   v **Ovládacích panelech** vyberte **Systém a zabezpečení** a poté **HP ProtectTools Security Manager**.

2. V levém panelu Uživatelské konzoly nástroje Security Manager klikněte na položku **Správa** a poté na položku **Konzola pro správu**.

Použití Konzoly pro správu

Konzola pro správu nástroje HP ProtectTools je centrální místem pro správu funkcí a aplikací nástroje HP ProtectTools Security Manager.

1. Na ploše systému Windows dvakrát klikněte na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.

   – nebo –

   v **Ovládacích panelech** vyberte **Systém a zabezpečení** a poté **HP ProtectTools Security Manager**.

2. V levém panelu Uživatelské konzoly nástroje Security Manager klikněte na položku **Správa** a poté na položku **Konzola pro správu**.

Na levém panelu se v konzole pro správu v části Domů zobrazí následující volby:

- **Systém** – umožňuje konfigurovat následující funkce zabezpečení a ověřování pro uživatele a zařízení.
  - **Zabezpečení**
  - **Uživatelé**
  - **Přihlašovací údaje**
- **Aplikace** – umožňuje konfigurovat nastavení nástroje HP ProtectTools Security Manager a aplikací nástroje Security Manager.
- **Data** – umožňuje konfigurovat nastavení nástroje Drive Encryption (pouze vybrané modely).
- **Počítač** – umožňuje konfigurovat nastavení nástroje Device Access Manager.
- **Průvodce nastavením** – provede vás nastavením nástroje HP ProtectTools Security Manager.
- **O aplikaci** – slouží k zobrazení informací o nástroji HP ProtectTools Security Manager, jako je číslo verze a poznámka o autorských právech.
- **Hlavní oblast** – slouží k zobrazení specifických obrazovek aplikací.

  ? – zobrazuje nápovědu Konzoly pro správu. Tato ikona se nachází v pravém horním rohu okna vedle ikon pro minimalizaci a maximalizaci.

Konfigurace systému

Do skupiny **Systém** se přistupuje z panelu nabídky na levé straně Konzoly pro správu nástroje HP ProtectTools. Aplikace v této skupině můžete použít ke správě zásad a nastavení počítače, jeho uživatelů a zařízení.

Skupina **Systém** obsahuje následující aplikace:

- **Zabezpečení** – zajišťuje správu funkcí, ověřování a nastavení řídící interakce uživatelů s počítačem.
- **Uživatelé** – slouží k nastavení, správě a registraci uživatelů počítače.
- **Přihlašovací údaje** – slouží ke správě bezpečnostních zařízení vestavěných do počítače nebo k němu připojených a ke konfiguraci nastavení.

Nastavení ověřování v počítači

V aplikaci Ověřování můžete nastavit zásady, které řídí přístup k počítači. Můžete určit přihlašovací údaje vyžadované k ověření každé třídy uživatelů při přihlašování do systému Windows nebo při přihlašování k webovým stránkám a programům během relace uživatele.

Chcete-li v počítači nastavit ověřování, postupujte takto:

1. V levém panelu Konzoly pro správu klikněte na možnost **Zabezpečení** a poté na možnost **Ověřování**.
2. Chcete-li konfigurovat přihlašovací údaje pro ověřování, klikněte na kartu **Zásady přihlášení**, proveďte změny a poté klikněte na tlačítko **Použít**.
3. Chcete-li konfigurovat ověřování relace, klikněte na kartu **Zásady relace**, proveďte změny a poté klikněte na tlačítko **Použít**.

Zásady přihlášení

Definování zásad spravujících přihlašovací údaje požadované pro ověření uživatele při přihlašování do systému Windows:

1. V levém panelu Konzoly pro správu klikněte na možnost **Zabezpečení** a poté na možnost **Ověřování**.
2. Na kartě **Zásady přihlášení** klepněte na kategorii uživatele, jako jsou Správci nebo Standardní uživatelé.
3. Chcete-li zobrazit dialogové okno pro úpravu, klikněte na způsob ověření přihlašovacích údajů.
4. Chcete-li používat kombinaci dvou ověřovaných přihlašovacích údajů, kliknutím na šipku dolů vyberte požadovanou kombinaci a nakonec klikněte na tlačítko **OK**.
5. Pokud chcete přihlašovací údaje odebrat, klikněte na tlačítko **X** nebo klikněte pravým tlačítkem na přihlašovací údaje a poté na možnost **Odstranit**.
6. V dialogovém okně s konfigurací klikněte na tlačítko **Ano**.
7. Jestliže chcete potvrdit, zda jsou uživatelé oprávněni se přihlásit, klikněte na možnost **Ověřit, zda se uživatelé aplikace HP ProtectTools mohou přihlásit**.
8. Chcete-li nastavení vrátit do původního stavu, klikněte na možnost **Obnovit výchozí nastavení**.
9. Klikněte na tlačítko **Použít**.

Zásady relace

Definování zásad spravujících přihlašovací údaje požadované k provedení ověření během relace v systému Windows:

1. V levém panelu Konzoly pro správu klikněte na možnost **Zabezpečení** a poté na možnost **Ověřování**.
2. Na kartě **Zásady relace** klepněte na kategorii uživatele, jako jsou Správci nebo Standardní uživatelé.
3. Chcete-li zobrazit dialogové okno pro úpravu, klikněte na způsob ověření přihlašovacích údajů.
4. Chcete-li používat kombinaci dvou ověřovaných přihlašovacích údajů, kliknutím na šipku dolů vyberte požadovanou kombinaci a nakonec klikněte na tlačítko **OK**.
5. Pokud chcete přihlašovací údaje odebrat, klikněte na tlačítko **X** nebo klikněte pravým tlačítkem na přihlašovací údaje a poté na možnost **Odstranit**.
6. V dialogovém okně s konfigurací klikněte na tlačítko **Ano**.
7. Jestliže chcete potvrdit, zda jsou uživatelé oprávněni se přihlásit, klikněte na možnost **Ověřit, zda se uživatelé aplikace HP ProtectTools mohou přihlásit**.
8. Chcete-li nastavení vrátit do původního stavu, klikněte na možnost **Obnovit výchozí nastavení**.
9. Klikněte na tlačítko **Použít**.

Nastavení

Chcete-li povolit uživatelům počítače přeskočit přihlášení do systému Windows, pokud již bylo provedeno ověření v systému BIOS nebo na úrovni nástroje Drive Encryption, postupujte následovně:

1. V levém panelu Konzoly pro správu klikněte na možnost **Zabezpečení** a poté na možnost **Nastavení**.
2. **Povolit funkci One Step Logon** – zaškrtnutím pole povolíte funkci One Step Logon. Zrušením zaškrtnutí funkci zakážete.
3. Klikněte na tlačítko **Použít**.

Správa uživatelů

V aplikaci Uživatelé můžete sledovat a spravovat uživatele nástroje HP ProtectTools v tomto počítači.

Všichni uživatelé nástroje HP ProtectTools jsou uvedeni v seznamu a ověřeni podle zásad nastavených nástrojem Security Manager. Také je ověřeno, zda zaregistrovali nebo nezaregistrovali příslušné přihlašovací údaje, které jim umožňují vyhovět těmto zásadám.

Při správě uživatelů vybírejte z následujících nastavení:

- Další uživatele můžete přidat kliknutím na tlačítko **Přidat**.
- Chcete-li uživatele odstranit, klikněte na uživatele a poté na tlačítko **Odstranit**.
- Nastavení dalších přihlašovacích údajů pro uživatele provedete kliknutím na uživatele a poté kliknutím na tlačítko **Registrovat**.
- Chcete-li zobrazit zásady pro určitého uživatele, vyberte uživatele a poté zobrazte zásady v okně níže.

Přihlašovací údaje

V aplikaci Přihlašovací údaje můžete konfigurovat nastavení dostupná pro všechna vestavěná nebo připojená bezpečnostní zařízení rozpoznaná nástrojem HP ProtectTools Security Manager.

SpareKey

Můžete nastavit, zda má být při přihlašování k systému Windows povoleno ověřování pomocí hesla SpareKey, a spravovat bezpečnostní otázky, které se uživatelům zobrazí při přihlašování s heslem SpareKey.

1. Vyberte bezpečnostní otázky, které budou uživatelům zobrazeny při přihlašování s heslem SpareKey.

   Můžete zadat až tři otázky nebo můžete uživatelům umožnit, aby zadali své vlastní.
2. Pokud chcete povolit obnovení SpareKey při přihlášení k systému Windows, zaškrtněte políčko.
3. Klikněte na tlačítko **Použít**.

Otisky prstů

Pokud je v počítači nainstalována nebo je k němu připojena čtečka otisků prstů, stránka Otisky prstů zobrazí následující karty:

- **Registrace** – můžete zvolit minimální a maximální počet otisků prstů, které může uživatel zaregistrovat.

  Také můžete vymazat všechna data ze čtečky otisků prstů.

  ⚠ **UPOZORNĚNÍ:** Vymazáním všech dat ze čtečky otisků prstů se smažou všechny údaje o otiscích prstů pro všechny uživatele včetně správců. Pokud zásady přihlášení vyžadují pouze otisky prstů, může být všem uživatelům zabráněno v přihlášení k počítači.

- **Citlivost** – prostřednictvím posuvníku můžete nastavit citlivost snímání otisků prstů pomocí čtečky otisků prstů.

  Pokud není otisk prstu rozpoznáván konzistentně, může být zapotřebí nastavit nižší citlivost. Vyšší nastavení zvyšuje citlivost na odchylky v obrazech otisků prstů, a proto se snižuje možnost chybného přijetí. **Středně vysoké** nastavení poskytuje vhodnou kombinaci zabezpečení a pohodlí.

- **Upřesnit** – výběrem jedné z následujících funkcí můžete nakonfigurovat čtečku otisků prstů, aby šetřila energii a zlepšila svou vizuální odezvu:

  - **Optimalizováno** – čtečka otisků prstů se aktivuje, když je třeba. Při prvním použití čtečky se může vyskytnout kratší prodleva.
  - **Úsporný provoz** – čtečka otisků prstů reaguje o něco pomaleji, ale využívá mnohem méně energie.
  - **Plný provoz** – čtečka otisků prstů je vždy připravena k použití, ale využívá více energie.

Tvář

Pokud je v počítači nainstalována webová kamera nebo je k němu připojena a současně je nainstalován program Face Recognition, správce může nastavit úroveň zabezpečení pro program Face Recognition, aby byla vyvážena snadnost jeho použití a náročnost narušení zabezpečení počítače.

1. Klikněte na tlačítko **Přihlašovací údaje** a poté na tlačítko **Tvář**.
2. Přesunutím posuvníku doleva nastavíte pohodlnější používání, přesunutím doprava vyšší přesnost.
   - **Pohodlí** – chcete-li zaregistrovaným uživatelům usnadnit získání přístupu v okrajových situacích, kliknutím přesuňte pruh posuvníku do polohy **Pohodlí**.
   - **Vyvážení** – chcete-li zajistit dobrý kompromis mezi zabezpečením a využitelností nebo pokud máte v počítači citlivé informace, případně je umístěn v oblasti, kde může docházet k pokusům o neoprávněné přihlášení, kliknutím přesuňte posuvník do polohy **Vyvážení**.
   - **Přesnost** – chcete-li uživateli znesnadnit přístup v případě, že jsou zaregistrované scény nebo stávající světelné podmínky pod normálem a je méně pravděpodobné, že může dojít k falešnému přijetí, kliknutím přesuňte posuvník do polohy **Přesnost**.
3. Chcete-li nastavení vrátit na původní hodnoty, klikněte na možnost **Obnovit výchozí nastavení**.
4. Klikněte na tlačítko **Použít**.

Čipová karta

Předtím než bude možné čipovou kartu použít k ověřování, musí ji správce inicializovat. Systém Windows podporuje většinu standardních čipových karet CSP a PKCS11.

Inicializace čipové karty

Nástroj HP ProtectTools Security Manager podporuje různé čipové karty. Počet a typ znaků použitých v kódech PIN se může lišit. Výrobce čipové karty by měl poskytovat nástroje pro instalaci bezpečnostního certifikátu a kód PIN pro správu, které aplikace HP ProtectTools použije ve svém algoritmu zabezpečení.

POZNÁMKA: Musí být nainstalován middleware čipové karty.

1. Získejte a nainstalujte middleware používané čipové karty (např. middleware ActivClient 6.x pro čipovou kartu ActivIdentity).
2. Vložte čipovou kartu do čtečky.
3. Inicializujte (naformátujte) čipovou kartu.
   a. Spusťte nástroj k inicializaci čipové karty, který se může také zobrazit po vložení čipové karty do čtečky.
   b. Podle instrukcí na obrazovce nastavte kód PIN.
   c. Pro budoucí potřebu si poznamenejte kód k odblokování.
4. Vytvořte pár klíčů a certifikát.
   a. Spusťte **Konzolu pro správu nástroje HP ProtectTools**.
   b. Klikněte na možnost **Přihlašovací údaje**, **Čipová karta** a poté na kartu **Správa**.
   c. Ujistěte se, že je vybrána možnost **Inicializovat čipovou kartu**.
   d. Zadejte kód PIN, klikněte na tlačítko **Použít** a poté postupujte podle pokynů na obrazovce.

   Jakmile čipovou kartu úspěšně inicializujete, je třeba ji zaregistrovat.

Registrace čipové karty

Jakmile je čipová karta inicializována, správci ji mohou zaregistrovat jako metodu ověřování v Konzole pro správu nástroje HP ProtectTools:

1. Klikněte na tlačítko **Průvodce nastavením**.
2. Na stránce **Vítejte!** klikněte na tlačítko **Další**.
3. Zadejte a potvrďte heslo pro systém Windows a pak klikněte na tlačítko **Další**.
4. Na stránce **SpareKey** klikněte na možnost **Přeskočit nastavení funkce SpareKey** (pokud nechcete aktualizovat informace ve funkci SpareKey) a poté na tlačítko **Další**.
5. Na stránce **Povolit funkce zabezpečení** klikněte na tlačítko **Další**.
6. Na stránce **Vybrat přihlašovací údaje** zkontrolujte, zda je vybrána možnost **Čipová karta**, a klikněte na možnost **Další**.
7. Na stránce **Čipová karta** zadejte kód PIN a poté klikněte na tlačítko **Další**.
8. Klikněte na tlačítko **Dokončit**.

Uživatelé mohou čipovou kartu také zaregistrovat v Uživatelské konzole nástroje Security Manager. Další informace získáte v nápovědě softwaru HP ProtectTools Security Manager kliknutím na modrou ikonu **?** v pravé horní části stránky Čipová karta.

Konfigurace čipové karty

Pokud je v počítači nainstalována nebo je k němu připojena čtečka čipových karet, stránka Čipová karta zobrazí dvě karty:

- **Nastavení** – zaškrtnutím pole **Uzamknout počítač po vyjmutí čipové karty** nastavíte počítač tak, že se po odebrání čipové karty počítač automaticky uzamkne. Následně klikněte na tlačítko **Použít**.

POZNÁMKA: Počítač se uzamkne pouze tehdy, byla-li čipová karta použita k ověření přihlašovacích údajů při přihlášení do systému Windows. Vyjmutí čipové karty, která nebyla použita pro přihlášení do systému Windows, počítač neuzamkne.

- **Správa** – můžete si vybrat z následujících možností:
  - **Inicializovat čipovou kartu** – připraví čipovou kartu pro použití s nástrojem HP ProtectTools. Jestliže byla čipová karta inicializována již dříve mimo nástroj HP ProtectTools (obsahuje asymetrický pár klíčů a související certifikát), nepotřebuje být inicializována znovu, pokud není požadována inicializace se specifickým certifikátem.
  - **Změnit kód PIN čipové karty** – umožňuje změnit kód PIN používaný čipovou kartou.
  - **Smazat pouze data nástroje HP ProtectTools** – smaže pouze certifikát nástroje HP ProtectTools vytvořený během inicializace karty. Z karty nejsou odstraněna žádná jiná data.
  - **Smazat všechna data na čipové kartě** – smaže všechna data na uvedené čipové kartě. Kartu již nebude možné použít s nástrojem HP ProtectTools nebo jinými aplikacemi.

POZNÁMKA: Funkce, které nejsou čipovou kartou nebo přidruženým middleware podporovány, nejsou dostupné.

▲ Klikněte na tlačítko **Použít**.

Bezkontaktní karta

Bezkontaktní karta je malá plastová karta obsahující elektronický čip. Pokud je k počítači připojena čtečka bezkontaktních karet, jsou nainstalovány potřebné ovladače výrobce a byla-li vybrána bezkontaktní karta jako způsob ověření přihlašovacích údajů, kartu můžete začít používat pro ověřování. Software HP ProtectTools podporuje následující typy bezkontaktních karet:

- Paměťové karty Contactless HID iCLASS
- Paměťové bezkontaktní karty MiFare Classic 1k, 4k a mini

▲ Bezkontaktní kartu nastavíte tak, že ji umístíte do těsné blízkosti čtečky, budete postupovat podle pokynů na obrazovce a nakonec kliknete na tlačítko **Použít**.

Karta s detekcí přiblížení

Karta s detekcí přiblížení je malá plastová karta obsahující elektronický čip. Pokud je k počítači připojena čtečka karet s detekcí přiblížení, jsou nainstalovány potřebné ovladače výrobce a byla-li vybrána karta s detekcí přiblížení jako způsob ověření přihlašovacích údajů, můžete začít používat kartu s detekcí přiblížení jako doplněk ostatních přihlašovacích údajů ke zvýšení zabezpečení.

▲ Chcete-li nastavit kartu s detekcí přiblížení, umístěte ji do těsné blízkosti čtečky a klikněte na tlačítko **Použít**.

Bluetooth

Pokud je počítač vybaven rozhraním Bluetooth® , bylo-li rozhraní Bluetooth vybráno jako způsob ověření přihlašovacích údajů a je-li s počítačem spárován telefon s rozhraním Bluetooth, můžete toto rozhraní začít používat jako doplněk ostatních přihlašovacích údajů ke zvýšení zabezpečení. Zadejte nastavení rozhraní Bluetooth:

▲ Jestliže chcete povolit bezobslužné ověřování, zaškrtněte odpovídající políčko a klikněte na tlačítko **Použít**.

Kód PIN

Pokud byl kód PIN vybrán jako způsob ověření přihlašovacích údajů, můžete jej začít používat jako doplněk ostatních přihlašovacích údajů ke zvýšení zabezpečení. Zadejte nastavení kódu PIN:

1. Klikněte na šipku nahoru nebo dolů a určete tak minimální délku kódu PIN.

   Maximální povolený počet čísel je 8.

2. Klikněte na tlačítko **Použít**.

Aplikace

Stránka Nastavení v části Aplikace na levém panelu konzoly pro správu nabízí dvě karty sloužící k přizpůsobení chování nainstalovaných aplikací HP ProtectTools Security Manager.

▲ V levém panelu Konzoly pro správu v části **Aplikace** klikněte na možnost **Nastavení**.

Karta Obecné

Na kartě **Obecné** jsou dostupná následující nastavení:

- **Nespouštět automaticky průvodce nastavením pro správce** – výběrem této možnosti zabráníte automatickému otevření průvodce po přihlášení.
- **Nespouštět automaticky průvodce Začínáme pro uživatele** – výběrem této možnosti zabráníte automatickému otevření uživatelského nastavení po přihlášení.

1. Zaškrtněte pole vedle specifického nastavení, abyste je povolili. Zrušením zaškrtnutí dané nastavení zakážete.
2. Klikněte na tlačítko **Použít**.

Karta Aplikace

Správci mohou povolit nebo zakázat následující aplikace:

- **Stav** – zaškrtnutím pole povolíte všechny aplikace. Zrušením zaškrtnutí všechny aplikace zakážete.
- **Password Manager** – povoluje aplikaci Password Manager pro všechny uživatele počítače.

1. Zaškrtněte pole vedle specifického nastavení, abyste je povolili. Zrušením zaškrtnutí dané nastavení zakážete.
2. Klikněte na tlačítko **Použít**.

Chcete-li obnovit výchozí nastavení všech aplikací, klikněte na tlačítko **Obnovit výchozí nastavení**.

Data

Část Data na levém panelu konzoly pro správu nabízí prostředky k úpravě nastavení následující aplikace:

- **Drive Encryption** – konfigurace nastavení a zobrazení stavu jednotky. Další informace získáte v nápovědě softwaru Drive Encryption kliknutím na modrou ikonu **?** v pravé horní části stránky Drive Encryption.

Počítač

Část Počítač na levém panelu konzoly pro správu nabízí prostředky k úpravě nastavení aplikace Device Access Manager:

- Zobrazení Simple Configuration (Jednoduchá konfigurace)
- Zobrazení Device Class Configuration (Konfigurace tříd zařízení)
- Konfigurace ověřování v reálném čase (JITA)
- Upřesnit nastavení

Další informace získáte v nápovědě k softwaru Device Access Manager kliknutím na modrou ikonu **?** v pravé horní části stránky Device Access Manager.

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager vám umožňuje značně zvýšit zabezpečení vašeho počítače.

Můžete použít předinstalované aplikace nástroje a také další aplikace, které jsou k dispozici k okamžitému stažení z webu:

- Správa přihlášení a hesel.
- Snadná změna hesla operačního systému Windows®.
- Nastavení předvoleb programů.
- Použití otisků prstů ke zvýšení zabezpečení a pohodlí.
- Registrace jedné nebo více scén pro ověření.
- Nastavení čipové karty pro ověřování.
- Zálohování a obnova dat programů.
- Přidání dalších aplikací.

Spuštění nástroje Security Manager

Nástroj Security Manager můžete spustit jedním z následujících způsobů:

▲ Na ploše systému Windows dvakrát klikněte na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.

– nebo –

v **Ovládacích panelech** vyberte **Systém a zabezpečení** a poté **HP ProtectTools Security Manager**.

Použití Uživatelské konzoly nástroje Security Manager

Uživatelská konzole nástroje Security Manager zajišťuje snadný přístup k funkcím, aplikacím a nastavením nástroje Security Manager. Uživatelská konzole zobrazuje následující komponenty:

- **Identifikační karta** – zobrazuje jméno uživatele v systému Windows a ikonu identifikující účet právě přihlášeného uživatele.
- **Bezpečnostní aplikace** – slouží k zobrazení nabídky odkazů pro konfiguraci následujících typů zabezpečení:
  - **Domov** – správa hesel, nastavení přihlašovacích údajů pro ověřování a kontrola stavu bezpečnostních aplikací.
  - **Obnova po krádeži** – služba Computrace for HP ProtectTools (prodává se samostatně).
- **Mé přihlašovací údaje** – správa přihlašovacích údajů pro ověřování nástrojů Password Manager a Credential Manager.
- **Moje data** – správa zabezpečení dat s nástroji Drive Encryption a File Sanitizer.

POZNÁMKA: Tato položka se nezobrazuje, pokud není aplikace nainstalována.

- **Tento počítač** – správa zabezpečení počítače s aplikací Device Access Manager.

POZNÁMKA: Tato položka se nezobrazuje, pokud není aplikace nainstalována.

- **Správa** – umožňuje správcům přistupovat na **Konzolu pro správy** a spravovat zabezpečení a uživatele.
- **Upřesnit** – zobrazuje příkazy pro přístup k dalším funkcím, mezi které patří:
  - **Předvolby** – umožňuje upravit nastavení nástroje Security Manager.
  - **Zálohování a obnova** – umožňuje zálohovat nebo obnovit data.
  - **O aplikaci** – slouží k zobrazení informací o nástroji HP ProtectTools Security Manager, jako je číslo verze a poznámka o autorských právech.
- **Hlavní oblast** – slouží k zobrazení specifických obrazovek aplikací.
- **?** – zobrazuje nápovědu Uživatelské konzoly nástroje Security Manager. Tato ikona se nachází v pravém horním rohu okna vedle ikon pro minimalizaci a maximalizaci.

Osobní identifikační karta

Identifikační karta vás jednoznačně identifikuje jako vlastníka tohoto účtu systému Windows. Obsahuje vaše jméno a obrázek podle vašeho vlastního výběru. Tato karta je nápadně zobrazena v levém horním rohu stránek nástroje Security Manager.

Způsob zobrazení svého jména můžete změnit. Ve výchozím nastavení se zobrazí vaše plné uživatelské jméno systému Windows a obrázek vybraný při instalaci systému Windows.

Chcete-li změnit zobrazované jméno, postupujte takto:

1. Otevřete Uživatelskou konzolu nástroje Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
2. Klikněte na tlačítko identifikační karty v levém horním rohu Uživatelské konzoly.
3. Klikněte na pole uvádějící uživatelské jméno daného účtu v systému Windows, zadejte nové jméno a klikněte na možnost **Uložit**.

Má přihlášení

Aplikace zahrnuté do této skupiny pomáhají při správě různých aspektů digitální identity.

- **Password Manager** – vytváří a spravuje rychlé odkazy, které umožňují spouštět programy a přihlašovat se k webovým stránkám na základě ověření pomocí hesla pro systém Windows, otisku prstu, vaší tváře, čipové karty, karty s detekcí přiblížení, bezkontaktní karty, telefonu s rozhraním Bluetooth nebo kódu PIN.
- **Credential Manager** – nabízí snadný způsob změny hesla pro systém Windows, registrace otisku prstu, registrace tváře či nastavení čipové karty, bezkontaktní karty, karty s detekcí přiblížení, telefonu s rozhraním Bluetooth nebo kódu PIN.

Správci mohou využívat informace o dalších dostupných bezpečnostních aplikacích kliknutím na možnost **Správa** a následným kliknutím na možnost **Centrální správa** v levém dolním rohu nástrojového panelu.

Správce hesel

Použití nástroje Password Manager usnadňuje přihlášení k systému Windows, webovým stránkám a aplikacím. Můžete jej využít k vytvoření silnějších hesel, která si nemusíte zapisovat ani pamatovat, a pak se snadno a rychle přihlašovat pomocí otisku prstu, tváře, čipové karty, bezkontaktní karty, kódu PIN nebo hesla pro systém Windows.

Správce hesel nabízí následující možnosti:

Karta Správa

- Umožňuje přidávat, upravovat a odstraňovat přihlášení.
- Rychlé odkazy umožňují spustit výchozí prohlížeč a přihlásit se k libovolnému webu nebo programu, který byl nastaven.
- Přetažením pomocí myši lze jednotlivé rychlé odkazy uspořádat do kategorií.
- Je možné rychle zkontrolovat, zda je některé z použitých hesel ohroženo.

Karta Síla hesla

- Umožňuje kontrolovat sílu jednotlivých hesel použitých na webových stránkách a aplikacích nebo zkontrolovat celkovou sílu hesla.
- Síla hesla je vyznačena červeným, žlutým nebo zeleným stavovým ukazatelem.

Ikona **Password Manager** je zobrazena v levém horním rohu webové stránky nebo přihlašovací obrazovky aplikace. Pokud dosud nebyly zadány přihlašovací údaje pro webové stránky nebo aplikaci, na ikoně se zobrazí symbol plus.

▲ Kliknutím na ikonu **Password Manager** zobrazíte kontextovou nabídku, která nabízí následující možnosti:

- Přidat [doména.com] do aplikace Password Manager
- Spustit aplikaci Password Manager
- Nastavení ikon
- Nápověda

Webové stránky a programy, pro které dosud nebylo vytvořeno přihlášení

V kontextové nabídce jsou zobrazeny následující možnosti:

- **Přidat [somedomain.com] do nástroje Password Manager** – umožňuje přidat přihlášení pro aktuální přihlašovací obrazovku.
- **Spustit Password Manager** – spustí nástroj Password Manager.
- **Nastavení ikony** – umožňuje určit podmínky, za nichž se zobrazí ikona **Password Manager**.
- **Nápověda** – zobrazuje nápovědu aplikace Security Manager.

Webové stránky a programy, pro které již bylo vytvořeno přihlášení

V kontextové nabídce jsou zobrazeny následující možnosti:

- **Zadat přihlašovací data** – obsahuje stránku Ověřte identitu. Po úspěšném ověření se vaše přihlašovací údaje automaticky zadají do přihlašovacích polí a stránka se odešle (pokud při vytvoření nebo poslední úpravě přihlášení bylo určeno odeslání).
- **Upravit přihlášení** – umožňuje upravit přihlašovací údaje pro danou webovou stránku.
- **Přidat přihlášení** – umožňuje přidat účet do aplikace Password Manager.
- **Spustit Password Manager** – spustí aplikaci Password Manager.
- **Nápověda** – zobrazuje nápovědu aplikace Security Manager.

POZNÁMKA: Je možné, že správce tohoto počítače nastavil nástroj Security Manager tak, aby při ověřování identity vyžadoval více přihlašovacích údajů.

Přidání přihlášení

Přihlášení k webu nebo programu lze snadno přidat zadáním přihlašovacích informací. Od tohoto okamžiku již bude nástroj Password Manager zadávat tyto informace za vás. Tato přihlášení můžete využít při otevření webové stránky nebo programu. Také můžete kliknout na přihlášení v nabídce **Rychlé odkazy nástroje Password Manager**. Nástroj Password Manager poté otevře příslušný web nebo program a přihlásí vás.

Chcete-li přidat přihlášení, postupujte takto:

1. Otevřete přihlašovací obrazovku pro daný web nebo program.
2. Klikněte na šipku na ikoně **Správce hesel** a v závislosti na tom, zda se jedná o přihlášení k webu nebo programu, poté klikněte na jednu z následujících položek:
   - V případě webu klikněte na položku **Přidat [název domény] do Správce hesel**.
   - V případě programu klikněte na položku **Přidat tuto přihlašovací obrazovku do Správce hesel**.
3. Zadejte přihlašovací údaje. Přihlašovací pole na obrazovce a odpovídající pole v dialogovém okně jsou označena výrazným oranžovým okrajem. Toto dialogové okno můžete rovněž zobrazit kliknutím na položku **Přidat přihlášení** na kartě **Správa nástroje Password Manager** pomocí kláves ctrl + logo Windows + h nebo naskenováním otisku prstu.
   a. Chcete-li přihlašovací pole vyplnit pomocí některé z předem nastavených možností, klikněte na šipku vpravo od pole.
   b. Chcete-li zobrazit heslo pro toto přihlášení, klikněte na položku **Zobrazit heslo**.
   c. Chcete-li, aby přihlašovací pole byla vyplněna, ale nikoli odeslána, zrušte zaškrtnutí políčka **Automaticky odeslat přihlašovací údaje**.

d. Kliknutím na tlačítko **OK** vyberte požadovanou metodu ověření (otisky prstů, tvář, čipová karta, karta s detekcí přiblížení, bezkontaktní karta, telefon s rozhraním Bluetooth, kód PIN nebo heslo) a poté se přihlaste pomocí vybrané metody ověřování.

   Z ikony **Správce hesel** je odebrán symbol plus, což znamená, že přihlášení bylo vytvořeno.

e. Pokud nástroj Správce hesel nezjistí pole pro přihlášení, klikněte na možnost **Další pole**.

   - Zaškrtněte políčko u každého pole požadovaného pro přihlášení nebo zrušte zaškrtnutí políček u polí, která požadována nejsou.
   - Klikněte na tlačítko **Zavřít**.

Při každém přístupu k tomuto webu nebo spuštění tohoto programu se zobrazí v levém horním rohu jejich okna ikona **Správce hesel**, která indikuje, že k přihlášení lze použít zaregistrované přihlašovací údaje.

Úprava přihlášení

Chcete-li upravit přihlášení, postupujte takto:

1. Otevřete přihlašovací obrazovku pro daný web nebo program.
2. Chcete-li zobrazit dialogové okno umožňující upravit přihlašovací informace, klikněte na šipku na ikoně **Password Manager** a poté na položku **Upravit přihlášení**. Přihlašovací pole na obrazovce a odpovídající pole v dialogovém okně jsou označena výrazným oranžovým okrajem.

   Toto dialogové okno můžete rovněž zobrazit kliknutím na položku **Upravit pro požadované přihlášení** na kartě **Správa Správce hesel**.
3. Upravte přihlašovací informace.
   - Chcete-li vyplnit přihlašovací pole **Uživatelské jméno** pomocí některé z předem nastavených možností, klikněte na šipku dolů vpravo od pole.
   - Chcete-li vyplnit přihlašovací pole **Heslo** pomocí některé z předem nastavených možností, klikněte na šipku dolů vpravo od pole.
   - Chcete-li k přihlášení přidat další pole z obrazovky, klikněte na položku **Další pole**.
   - Chcete-li zobrazit heslo pro toto přihlášení, klikněte na položku **Zobrazit heslo**.
   - Chcete-li, aby přihlašovací pole byla vyplněna, ale nikoli odeslána, zrušte zaškrtnutí políčka **Automaticky odeslat přihlašovací údaje**.
4. Klikněte na tlačítko **OK**.

Použití nabídky rychlých odkazů v nástroji Password Manager

Nástroj Password Manager nabízí rychlý a snadný způsob spouštění webů a programů, pro které jste vytvořili přihlášení. Dvakrát klikněte na přihlášení k webu nebo programu v nabídce **Rychlé odkazy nástroje Password Manager** nebo na kartě **Správa** nástroje Password Manager. Otevře se přihlašovací obrazovka a budou vyplněny přihlašovací údaje.

Přihlášení je po vytvoření automaticky přidáno do nabídky **Rychlé odkazy** nástroje Password Manager.

Chcete-li zobrazit nabídku **Rychlé odkazy**, postupujte následovně:

1. Stiskněte klávesovou zkratku pro nástroj **Password Manager**. Výchozí nastavení z výroby je (ctrl+logo Windows+h). Chcete-li změnit klávesovou zkratku, na Uživatelské konzole nástroje Security Manager dvakrát klikněte na možnost **Password Manager** a poté na možnost **Nastavení**.
2. Naskenujte otisk prstu (u počítačů s integrovanou nebo připojenou čtečkou otisků prstů) nebo zadejte heslo k systému Windows.

Uspořádání přihlášení do kategorií

Chcete-li uspořádat přihlašovací údaje, vytvořte pro ně jednu nebo více kategorií. Potom jednotlivá přihlášení přetáhněte pomocí myši do požadovaných kategorií.

Chcete-li přidat kategorii, postupujte takto:

1. Na Uživatelské konzole nástroje Security Manager klepněte na položku **Password Manager**.
2. Klikněte na kartu **Správa** a poté na položku **Přidat kategorii**.
3. Zadejte název kategorie.
4. Klikněte na tlačítko **OK**.

Chcete-li přidat přihlášení do kategorie, postupujte takto:

1. Nastavte ukazatel myši na požadované přihlášení.
2. Stiskněte a podržte levé tlačítko myši.
3. Přetáhněte přihlášení do seznamu kategorií. Při pohybu myši budou zvýrazňovány jednotlivé kategorie.
4. Jakmile je zvýrazněna požadovaná kategorie, uvolněte tlačítko myši.

Přihlášení nebude do dané kategorie přesunuto, ale pouze zkopírováno. Přihlášení lze přidat do několika kategorií. Chcete-li zobrazit všechna přihlášení, klikněte na položku **Vše**.

Správa přihlášení

Správce hesel usnadňuje správu přihlašovacích informací pro uživatelská jména, hesla a účty pro vícenásobné přihlášení z jednoho centrálního místa.

Přihlášení jsou uvedena na kartě **Správa**. Pokud bylo pro stejný web vytvořeno několik přihlašovacích údajů, jsou jednotlivá přihlášení v seznamu uvedena pod názvem webu a odsazena.

Chcete-li provádět správu přihlášení, postupujte takto:

▲ Na Uživatelské konzole nástroje Security Manager klikněte na položku **Password Manager** a pak klikněte na kartu **Správa**.

- **Přidání přihlášení** – klikněte na položku **Přidat přihlášení** a postupujte podle pokynů na obrazovce.
- **Přihlášení** – klikněte na existující přihlašovací údaje, vyberte jednu z následujících možností a poté postupujte dle pokynů na obrazovce:
  - **Otevřít** – otevře webovou stránku nebo program, pro které máte přihlašovací údaje.
  - **Přidat** – přidání přihlašovacích údajů. Další informace naleznete v části Přidání přihlášení na stránce 28.

- **Upravit** – úprava přihlášení. Další informace naleznete v části Úprava přihlášení na stránce 29.
- **Odstranit** – odstraní webovou stránku nebo program, pro které máte přihlašovací údaje.

- **Přidat kategorii** – klikněte na možnost **Přidat kategorii** a poté postupujte dle pokynů na obrazovce. Další informace naleznete v části Uspořádání přihlášení do kategorií na stránce 30.

Chcete-li pro určitý web nebo program přidat další přihlášení, postupujte takto:

1. Otevřete přihlašovací obrazovku pro požadovaný web nebo program.
2. Kliknutím na ikonu **Správce hesel** zobrazte místní nabídku.
3. Klikněte na položku **Přidat přihlášení** a poté postupujte podle pokynů na obrazovce.

Vyhodnocení síly hesla

Použití silných hesel při přihlašování k webům a programům představuje důležitý aspekt ochrany identity.

Správce hesel usnadňuje monitorování a zvyšování zabezpečení díky okamžité automatizované analýze síly jednotlivých hesel použitých k přihlášení k webům a programům.

Na kartě **Síla hesla** je pomocí červeného, žlutého nebo zeleného stavového ukazatele uvedena síla jednotlivých hesel použitých na webových stránkách a aplikacích a celková síla hesla.

Nastavení ikony Správce hesel

Správce hesel se pokouší identifikovat přihlašovací obrazovky webů a programů. Jakmile detekuje přihlašovací obrazovku, pro kterou jste dosud nevytvořili přihlášení, vyzve vás k přidání přihlášení pro tuto obrazovku, a to zobrazením ikony **Správce hesel** se symbolem plus.

1. Chcete-li určit, jak má nástroj Password Manager pracovat s webovými stránkami obsahujícími přihlášení, klikněte na ikonu a poté vyberte možnost **Nastavení ikony**.
   - **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky** – zaškrtněte toto políčko, chcete-li, aby nástroj Password Manager zobrazoval výzvu k přidání přihlášení vždy, když se zobrazí přihlašovací obrazovka, pro niž dosud nebylo vytvořeno přihlášení.
   - **Nezahrnovat tuto obrazovku** – toto políčko zaškrtněte, chcete-li, aby nástroj Password Manager již nezobrazoval výzvu k přidání přihlášení pro tuto přihlašovací obrazovku.

     Postup přidání přihlašovacích údajů pro obrazovku, která byla dříve vyloučena:

     - Zobrazte dříve vyloučené přihlášení k webové stránce nebo stránku programu, otevřete Uživatelskou konzolu nástroje Security Manager a poté klikněte na možnost **Password Manager**.
     - Klikněte na tlačítko **Přidat přihlášení**.

       Dialogové okno Přidat přihlášení se otevře s přihlašovací stránkou webu nebo programu uvedenou v poli **Aktuální obrazovka**.
     - Klikněte na tlačítko **Pokračovat**.

       Zobrazí se obrazovka Přidat přihlášení do Správce hesel.

- Řiďte se instrukcemi na obrazovce. Další informace naleznete v části Přidání přihlášení na stránce 28.
- Ikona **Správce hesel** se zobrazí při každém otevření této přihlašovací obrazovky webu nebo aplikace.

Nezobrazovat výzvu k přidání přihlašovacích údajů pro přihlašovací obrazovky – vyberte přepínač.

2. Chcete-li zobrazit další nastavení nástroje Password Manager, klikněte na položku **Password Manager** a pak v Uživatelské konzole nástroje Security Manager klikněte na položku **Nastavení**.

Nastavení

Podle potřeby můžete přizpůsobit nastavení nástroje Password Manager:

1. **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky** – ikona nástroje **Password Manager** se symbolem plus se zobrazí vždy, když je detekována přihlašovací obrazovka webové stránky nebo programu, a indikuje, že je možné do trezoru hesel přidat přihlášení k této obrazovce do nabídky **Přihlašovací údaje**. Chcete-li tuto funkci zakázat, zrušte zaškrtnutí pole u možnosti **Zobrazit výzvu k přidání přihlašovacích údajů pro přihlašovací obrazovky**.
2. **Spustit Password Manager pomocí ctrl+win+h** – výchozí klávesová zkratka, která otevře nabídku **Rychlé odkazy nástroje Password Manager** je ctrl+logo Windows+h. Chcete-li tuto kombinaci kláves změnit, klikněte na tuto položku a stiskněte novou kombinaci kláves. Kombinace kláves mohou obsahovat jeden nebo více následujících prvků: ctrl, alt nebo shift a libovolná alfanumerická klávesa.
3. Změny uložíte kliknutím na tlačítko **Použít**.

Credential Manager

Přihlašovací údaje nástroje Security Manager slouží k ověření vaší identity. Správce tohoto počítače může nastavit, které přihlašovací údaje lze použít k ověření vaší identity při přihlášení k účtu systému Windows, webovým stránkám nebo programům.

Dostupné přihlašovací údaje se mohou lišit v závislosti na bezpečnostních zařízeních, která jsou vestavěna nebo připojena k tomuto počítači. Podporované přihlašovací údaje, požadavky a aktuální stav jsou zobrazeny po kliknutí na možnost **Credential Manager** v části **Má přihlášení** a mohou zahrnovat následující:

- Heslo
- SpareKey
- Otisky prstů
- Tvář
- Čipová karta
- Bezkontaktní karta
- Karta s detekcí přiblížení
- Bluetooth
- Kód PIN

Chcete-li zaregistrovat nebo změnit přihlašovací údaje, klikněte na odkaz a postupujte podle pokynů na obrazovce.

Změna hesla pro systém Windows

Nástroj Security Manager usnadňuje a zrychluje změnu hesla pro systém Windows (ve srovnání s použitím ovládacího panelu systému Windows).

Chcete-li změnit hesla pro systému Windows, postupujte takto:

1. V Uživatelské konzole nástroje Security Manager klikněte postupně na položky **Credential Manager** a **Heslo**.
2. Do textového pole **Aktuální heslo pro systém Windows** zadejte aktuální heslo.
3. Do textového pole **Nové heslo pro systém Windows** zadejte nové heslo a pak je zadejte znovu do pole **Potvrzení nového hesla**.
4. Kliknutím na tlačítko **Změnit** okamžitě nastavíte nově zadané heslo jako aktuální.

Nastavení hesla SpareKey

Heslo SpareKey umožňuje získat přístup k počítači (u podporovaných platforem) odpovědí na tři bezpečnostní otázky ze seznamu, který byl dříve definován správcem.

Nástroj HP ProtectTools Security Manager váš požádá o nastavení osobního hesla SpareKey během úvodního nastavení v průvodci nastavením nástroje HP ProtectTools Security Manager.

Nastavení hesla SpareKey:

1. V průvodci na stránce SpareKey vyberte tři bezpečnostní otázky a pro každou z nich zadejte odpověď.
2. Klikněte na možnost **Vytvořit**.

Na stránce SpareKey v nástroji **Credential Manager** můžete vybrat různé otázky nebo změnit odpovědi.

Poté co heslo SpareKey nastavíte, budete moci získat přístup k počítači z přihlašovací obrazovky před startem nebo z uvítací obrazovky systému Windows.

Registrace otisků prstů

Pokud správce na obrazovce **Vybrat přihlašovací údaje** vybere možnost Otisky prstů a počítač je vybaven čtečkou otisků prstů nebo je k ní připojen, průvodce nastavením nástroje HP ProtectTools Security Manager vás provede procesem nastavení nebo „registrace“ otisků prstů. Otisky prstů můžete také zaregistrovat na stránce Otisk prstu v nástroji **Credential Manager** v Uživatelské konzole nástroje Security Manager.

1. V průvodci jsou na stránce Otisky prstů zobrazeny obrysy dvou rukou. Prsty, které již jsou registrované, jsou zvýrazněné. Klikněte na prst na obrysu.

POZNÁMKA: Pokud chcete odstranit dříve zaregistrovaný otisk prstu, klikněte na příslušný prst.

2. Budete vyzváni k sejmutí otisku prstu, dokud jeho otisk nebude úspěšně zaregistrován. Zaregistrovaný prst se na obrysu zvýrazní.
3. Musíte zaregistrovat minimálně dva prsty; nejvhodnější jsou ukazováčky nebo prostředníčky. Opakujte kroky 1 a 2 pro další prst.
4. Postupujte podle pokynů na obrazovce a poté klikněte na tlačítko **Další**.

UPOZORNĚNÍ: Pokud registrujete otisky prstů podle pokynů průvodce, informace o otiscích prstů se neuloží, dokud nekliknete na tlačítko **Další**. Pokud necháte počítač chvíli neaktivní nebo zavřete program, provedené změny se **neuloží**.

Registrace scén pro přihlášení pomocí tváře

Pokud zvolíte přihlašování pomocí tváře a počítač disponuje vestavěnou nebo připojenou kamerou, průvodce nastavením nástroje HP ProtectTools Security Manager vás vyzve k registraci scén. Scény můžete také zaregistrovat na stránce Přihlášení pomocí tváře v nástroji **Credential Manager** v Uživatelské konzole nástroje Security Manager.

Chcete-li používat přihlášení pomocí tváře, je nutné zaregistrovat jednu nebo více scén. Po úspěšné registraci můžete novou scénu zaregistrovat také v případě, že během přihlašování došlo k potížím způsobeným změnou jedné nebo více následujících podmínek:

- Od posledního přihlášení se značně změnil vzhled vaší tváře.
- Od některého z předchozích přihlášení se změnilo osvětlení.
- Při posledním přihlášení jste měli (nebo naopak neměli) nasazené brýle.

POZNÁMKA: Máte-li problémy s registrací scén, zkuste se přemístit blíže k webové kameře.

K registraci scény z Průvodce nastavením nástroje HP ProtectTools Security Manager použijte následující postup:

1. V průvodci na stránce Přihlášení pomocí tváře klikněte na možnost **Upřesnit** a poté nakonfigurujte další možnosti. Další informace naleznete v části Pokročilá uživatelská nastavení na stránce 36.
2. Klikněte na tlačítko **OK**.
3. Klikněte na možnost **Spustit**. Pokud jste již dříve scény registrovali, klikněte na možnost **Zaregistrovat novou scénu**.
4. Během registrace scény můžete po kliknutí na tlačítko **Přehrát video** sledovat ukázku.

   Jedná-li se o první registraci, zobrazí se dialogové okno s dotazem, zda chcete spustit ukázkové video. Klikněte na tlačítko **Ano** nebo **Ne**.
5. Při slabém osvětlení dokáže software automaticky zesvětlit obrazovku nebo změnit nastavení protisvětla, klikněte na ikonu **Žárovka**.
6. Klikněte na ikonu **fotoaparátu** a poté postupujte dle pokynů na obrazovce, abyste zaregistrovali scénu.

   POZNÁMKA: Během zachycování scén se dívejte na svůj obraz a odpovídajícím způsobem natočte hlavu.
7. Klikněte na tlačítko **Další**.

Scény můžete také zaregistrovat z Uživatelské konzoly nástroje Security Manager:

1. Otevřete Uživatelskou konzolu nástroje Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
2. V části **Má přihlášení** klikněte na položky **Credential Manager** a **Tvář**.
3. Chcete-li nakonfigurovat další možnosti, klikněte na volbu **Upřesnit**. Další informace naleznete v části Pokročilá uživatelská nastavení na stránce 36.
4. Klikněte na tlačítko **OK**.

5. Klikněte na možnost **Spustit**. Pokud jste již dříve scény registrovali, klikněte na možnost **Zaregistrovat novou scénu**.
6. Pokud budete požádáni o zadání hesla pro systém Windows, zadejte je a pak klikněte na tlačítko **Další**.
7. Během registrace scény můžete po kliknutí na tlačítko **Přehrát video** sledovat ukázku.

   Jedná-li se o první registraci, zobrazí se dialogové okno s dotazem, zda chcete spustit ukázkové video. Klikněte na tlačítko **Ano** nebo **Ne**.
8. Při slabém osvětlení dokáže software automaticky zesvětlit obrazovku nebo změnit nastavení protisvětla, klikněte na ikonu **Žárovka**.
9. Klikněte na ikonu **fotoaparátu** a poté postupujte dle pokynů na obrazovce, abyste zaregistrovali scénu.

POZNÁMKA: Během zachycování scén se dívejte na svůj obraz a odpovídajícím způsobem natočte hlavu.

Další informace získáte v nápovědě softwaru Face Recognition kliknutím na modrou ikonu **?** v pravé horní části stránky Registrace tváře.

Ověřování

Po zaregistrování jedné či více scén můžete použít svou tvář k ověření při přihlašování k počítači nebo zahajování nové relace v systému Windows.

1. Jakmile se zobrazí obrazovka pro ověření a kamera nalezne vaši tvář, máte 5 sekund k zahájení procesu přihlášení. Pokud bude vaše tvář úspěšně ověřena, získáte přístup k počítači.
2. Pokud dojde k vypršení časového limitu přihlášení pomocí tváře, aplikace Face Recognition bude pozastavena. Kliknutím na ikonu **fotoaparátu** obnovíte proces ověřování.

POZNÁMKA: Pokud je osvětlení nedostatečné a nelze se pomocí aplikace Face Recognition přihlásit, můžete zadat heslo systému Windows, abyste se přihlásili k počítači.

3. Pokud se po přihlášení k počítači aplikace Face Recognition zeptá, zda chcete přidat další scénu, aby se do budoucna při přihlášení zlepšila schopnost vašeho rozpoznání, klikněte na možnost **Ano**.

Tmavý režim

Pokud je při přihlašování pomocí tváře příliš málo světla, barva pozadí obrazovky přihlašování pomocí tváře se automaticky přepne na bílou, aby byla vaše tvář lépe osvětlena.

Chcete-li ručně přepnout barvu pozadí obrazovky přihlašování pomocí tváře, klikněte na ikonu **žárovky**.

Výuka

Bylo-li přihlášení pomocí tváře neúspěšné, ale zadali jste správné heslo, můžete být požádáni o uložení série snímků, aby se do budoucna zvýšila šance na úspěšné přihlášení pomocí tváře.

Odstranění scény

Odstranění aktuálně zaregistrované scény:

1. Otevřete Uživatelskou konzolu nástroje Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
2. V části **Má přihlášení** klikněte na možnost **Credential Manager** a poté klikněte na možnost **Tvář**.
3. Klikněte na scénu, kterou chcete odstranit, a poté na ikonu **koše**.
4. V dialogovém okně s potvrzením klikněte na tlačítko **OK**.

Pokročilá uživatelská nastavení

1. Otevřete Uživatelskou konzolu nástroje Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
2. V části **Má přihlášení** klikněte na položky **Credential Manager** a **Tvář**.
3. Kliknutím na možnost **Upřesnit** můžete nakonfigurovat následující možnosti:

   Karta **Další nastavení** – zaškrtnutím polí můžete vybrat jednu nebo více možností. Zrušením jejich zaškrtnutí můžete dané možnosti zakázat. Tato nastavení platí pouze pro aktuálního uživatele.

   - **Přehrávání zvuků při událostech rozpoznání tváře** – přehraje zvuk při úspěchu či neúspěchu přihlášení pomocí tváře.
   - **Vyzvat k aktualizaci scén při nezdařeném pokusu o přihlášení** – v případě neúspěšného přihlášení pomocí tváře, ale úspěšného zadání hesla, můžete být vyzváni k uložení série zachycených snímků, aby se do budoucna zvýšila šance úspěšného přihlášení pomocí tváře.
   - **Vyzvat k zaregistrování nové scény při nezdařeném pokusu o přihlášení** – v případě neúspěšného přihlášení pomocí tváře, ale úspěšného zadání hesla, můžete být vyzváni k registraci nové scény, aby se do budoucna zvýšila šance úspěšného přihlášení pomocí tváře.
4. Chcete-li nastavení vrátit na původní hodnoty, klikněte na možnost **Obnovit výchozí nastavení**.
5. Klikněte na tlačítko **OK**.

Instalace čipové karty

Pokud je čtečka čipových karet vestavěna v počítači nebo je k němu připojena, správce povolil čipovou kartu jako způsob ověření přihlašovacích údajů a provedl kroky popsané v nápovědě ke Konzole pro správu nástroje HP ProtectTools, průvodce nastavením nástroje HP ProtectTools Security Manager vás vyzve k vložení a nastavení čipové karty. Čipovou kartu můžete také zaregistrovat na stránce Čipová karta v nástroji **Credential Manager** v Uživatelské konzole nástroje Security Manager.

POZNÁMKA: Před tím, než bude možné čipovou kartu použít, musí ji správce inicializovat.

Inicializace čipové karty

Nástroj HP ProtectTools Security Manager podporuje různé čipové karty. Počet a typ znaků použitých v kódech PIN se může lišit. Výrobce čipové karty by měl poskytovat nástroje pro instalaci bezpečnostního certifikátu a správu kódu PIN, které aplikace HP ProtectTools použije ve svém algoritmu zabezpečení.

Správci mohou čipovou kartu inicializovat buď prostřednictvím softwaru od výrobce, nebo Konzoly pro správu nástroje HP ProtectTools. Další informace naleznete v nápovědě ke Konzole pro správu nástroje HP ProtectTools.

Registrace čipové karty

Jakmile uživatelé čipovou kartu inicializují, mohou ji zaregistrovat v aplikaci Security Manager:

1. Otevřete Uživatelskou konzolu nástroje Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
2. Klikněte na možnost **Credential Manager** a poté na možnost **Čipová karta**.
3. Ujistěte se, že je vybrána možnost **Nastavit**.
4. Zadejte heslo pro systém Windows a kód PIN a pak klikněte na tlačítko **Uložit**.

Správci mohou k registraci čipové karty použít také Konzolu pro správu nástroje HP ProtectTools. Další informace naleznete v nápovědě ke Konzole pro správu nástroje HP ProtectTools.

Změna kódu PIN čipové karty

Změna kódu PIN čipové karty:

1. Vložte čipovou kartu, která byla dříve naformátována a inicializována.
2. Vyberte možnost **Změnit kód PIN čipové karty**.
3. Zadejte starý kód PIN a poté zadejte a potvrďte nový.

Bezkontaktní karta

Bezkontaktní karta je malá plastová karta obsahující elektronický čip. Pokud je k počítači připojena čtečka bezkontaktních karet, správce nainstaloval potřebné ovladače výrobce a vybral bezkontaktní kartu jako způsob ověření přihlašovacích údajů, kartu můžete začít používat k ověření. Software HP ProtectTools podporuje následující typy bezkontaktních karet:

- Paměťové karty Contactless HID iCLASS
- Paměťové bezkontaktní karty MiFare Classic 1k, 4k a mini

▲ Bezkontaktní kartu nastavíte tak, že ji umístíte do těsné blízkosti čtečky, budete postupovat podle pokynů na obrazovce a nakonec kliknete na tlačítko **Použít**.

Karta s detekcí přiblížení

Karta s detekcí přiblížení je malá plastová karta obsahující elektronický čip. Pokud je k počítači připojena čtečka karet s detekcí přiblížení, správce nainstaloval potřebné ovladače výrobce a vybral kartu s detekcí přiblížení jako způsob ověření přihlašovacích údajů, kartu můžete začít používat jako doplněk ostatních přihlašovacích údajů ke zvýšení zabezpečení.

▲ Kartu s detekcí přiblížení nastavíte tak, že ji umístíte do těsné blízkosti čtečky, budete postupovat podle pokynů na obrazovce a nakonec kliknete na tlačítko **Použít**.

Bluetooth

Pokud správce vybral rozhraní Bluetooth jako způsob ověření přihlašovacích údajů, můžete začít používat telefon s rozhraním Bluetooth jako doplněk ostatních přihlašovacích údajů ke zvýšení zabezpečení.

POZNÁMKA: Podporovány jsou pouze telefony s rozhraním Bluetooth.

1. Ujistěte se, že je rozhraní Bluetooth v počítači povoleno a v telefonu je aktivní režim vyhledávání. V rámci připojení telefonu může být zapotřebí zadat do zařízení s rozhraním Bluetooth automaticky vytvořený kód. V závislosti na konfiguraci zařízení s rozhraním Bluetooth může být nutné zadat párovací kód počítače s telefonem.
2. Telefon zaregistrujete tak, že jej vyberete a kliknete na možnost **Zaregistrovat**.
3. V dialogovém okně s potvrzením klikněte na tlačítko **OK**.

Kód PIN

Pokud správce vybral kód PIN jako způsob ověření přihlašovacích údajů, můžete tento kód začít používat jako doplněk ostatních přihlašovacích údajů ke zvýšení zabezpečení.

▲ Nový kód PIN vytvoříte tak, že jej zadáte a opakovaným zadáním jej potvrdíte.

Správa

Správci mohou přistoupit na Konzolu pro správu a možnost Centrální správa kliknutím na položku **Správa** a poté výběrem položky **Konzola pro správu** v levém dolním panelu Uživatelské konzoly nástroje HP ProtectTools Security Manager.

Další informace naleznete v nápovědě ke Konzole pro správu nástroje HP ProtectTools.

Rozšířené

Kliknutím na možnost **Upřesnit** v levé dolní části Uživatelské konzoly získáte přístup k následujícím možnostem:

- **Předvolby** – umožňuje upravit nastavení nástroje Security Manager.
- **Zálohování a obnova** – umožňuje zálohovat a obnovit data aplikace Security Manager.
- **O aplikaci** – zobrazí informace o verzi nástroje Security Manager.

Nastavení předvoleb

Je možné upravit nastavení nástroje HP ProtectTools Security Manager. V Uživatelské konzole nástroje Security Manager klikněte na položku **Upřesnit** a pak na položku **Předvolby**. Dostupná nastavení jsou zobrazena na dvou kartách, **Obecné** a **Otisk prstu**.

Karta Obecné

Vzhled – zobrazit ikonu v oznamovací oblasti lišty

- Chcete-li povolit zobrazení ikony na liště, zaškrtněte toto políčko.
- Chcete-li zakázat zobrazení ikony na liště, zrušte zaškrtnutí tohoto políčka.

Karta Otisk prstu

POZNÁMKA: Karta **Otisk prstu** je dostupná pouze v případě, že je počítač vybaven čtečkou otisků prstů a je v něm nainstalován správný ovladač.

- **Rychlé akce** – pomocí funkce Rychlé akce lze vybrat úkol nástroje Security Manager, který bude proveden, pokud při skenování otisku prstu stisknete určenou klávesu.

  Chcete-li přiřadit rychlou akci k jedné z uvedených kláves, klikněte na položku **(Klávesa) + Otisk prstu** a pak vyberte jeden z dostupných úkolů v nabídce.

- **Odezva při skenování otisku prstu** – tato možnost se zobrazí pouze v případě, že je k dispozici čtečka otisků prstů. Pomocí tohoto nastavení můžete upravit odezvu, která bude použita při skenování otisku prstu.

  - **Povolit zvukovou odezvu** – nástroj Security Manager při skenování otisku prstu poskytne zvukovou odezvu. Pro jednotlivé události jsou přehrávány různé zvuky. Nové zvuky lze těmto událostem rovněž přiřadit pomocí karty **Zvuky** v části s nastavením zvuku na ovládacím panelu systému Windows. Chcete-li zvukovou odezvu zakázat, zrušte zaškrtnutí této položky.

  - **Zobrazit zpětnou vazbu ke kvalitě skenování**

    Chcete-li zobrazit všechny naskenované položky bez ohledu na kvalitu, zaškrtněte toto políčko.

    Chcete-li zobrazit pouze kvalitní naskenované položky, zaškrtnutí políčka zrušte.

Zálohování a obnova dat

Doporučuje se pravidelně zálohovat data nástroje Security Manager. Četnost zálohování závisí na tom, jak často se tato data mění. Pokud například denně přidáváte nová přihlášení, měli byste pravděpodobně zálohovat data každý den.

Zálohy lze rovněž použít k migraci dat mezi počítači (pro tuto operaci je rovněž používán termín import a export).

POZNÁMKA: Tato funkce umožňuje zálohování pouze informací z nástrojů Password Manager a Face Recognition. Nástroje Drive Encryption má nezávislou metodu zálohování. Nástroj Device Access Manager a informace o ověřování otiskem prstu zálohování neumožňují.

V počítači, do něhož jsou přenesena zálohovaná data, musí být nainstalován nástroj HP ProtectTools Security Manager, jinak nebude možné data za zálohy obnovit.

Chcete-li zálohovat data, postupujte takto:

1. Otevřete Uživatelskou konzolu nástroje Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
2. V levé části Uživatelské konzoly klikněte na položku **Upřesnit** a poté klikněte na položku **Zálohování a obnova**.
3. Klikněte na tlačítko **Zálohovat data**.
4. Vyberte moduly, které chcete zahrnout do zálohování. Ve většině případů vyberete všechny moduly.
5. Ověřte identitu.
6. Zadejte název souboru se zálohou. Ve výchozím nastavení bude tento soubor uložen do složky Dokumenty. Kliknutím na tlačítko **Procházet** můžete určit jiné umístění.
7. Zadejte heslo, chcete-li zálohu zašifrovat.
8. Klikněte na tlačítko **Dokončit**.

Chcete-li obnovit data, postupujte takto:

1. Otevřete Uživatelskou konzolu nástroje Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
2. V levé části Uživatelské konzoly klikněte na položku **Upřesnit** a poté klikněte na položku **Zálohování a obnova**.
3. Klikněte na tlačítko **Obnovit data**.
4. Vyberte dříve vytvořený soubor se zálohou. Zadejte cestu do příslušného pole nebo klikněte na tlačítko **Procházet**.
5. Zadejte heslo, kterým jste zálohu zašifrovali.
6. Vyberte moduly, pro které chcete obnovit data. Ve většině případů vyberete všechny uvedené moduly.
7. Ověřte heslo pro systém Windows.
8. Klikněte na tlačítko **Dokončit**.

6 Nástroj Drive Encryption for HP ProtectTools (pouze u vybraných modelů)

Nástroj Drive Encryption for HP ProtectTools poskytuje prostřednictvím šifrování dat v počítači jejich kompletní ochranu. Je-li aplikace Drive Encryption aktivována, je třeba se přihlásit na přihlašovací obrazovce aplikace Drive Encryption, která se zobrazí před spuštěním operačního systému Windows®.

Nástroj HP ProtectTools Security Manager (Průvodce nastavením nástroje HP Client Security, Pokročilý průvodce nastavením nebo Konzola pro správu) umožňuje správcům systému Windows aktivovat nástroj Drive Encryption, zálohovat šifrovací klíč a přidat či odebrat jednotky nebo oddíly určené k šifrování. Další informace naleznete v nápovědě k nástroji HP ProtectTools Security Manager.

Aplikace Drive Encryption umožňuje provádět následující úlohy:

- Výběr nastavení aplikace Drive Encryption:
  - Aktivace hesla chráněného modulem TPM
  - Šifrování a dešifrování jednotlivých jednotek a oddílů pomocí softwarového šifrování
  - Šifrování a dešifrování jednotlivých samošifrujících jednotek pomocí hardwarového šifrování
  - Rozšíření zabezpečení zakázáním režimu spánku a úsporného režimu, aby bylo vždy vyžadováno předbootovací ověření aplikace Drive Encryption

POZNÁMKA: Šifrovat lze pouze interní pevné disky SATA a externí pevné disky eSATA.

- Vytvoření záložních klíčů
- Obnovení přístupu k šifrovanému počítači pomocí záložních klíčů a nástroje HP SpareKey
- Povolení ověřování před spuštěním v rámci nástroje Drive Encryption pomocí hesla, registrovaného otisku prstu nebo kódu PIN pro vybrané čipové karty

Spuštění aplikace Drive Encryption

Správci mohou k aplikaci Drive Encryption přistupovat spuštěním Uživatelské konzoly nástroje HP ProtectTools Security Manager.

1. Na ploše systému Windows dvakrát klikněte na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.

   – nebo –

   v **Ovládacích panelech** vyberte **Systém a zabezpečení** a poté **HP ProtectTools Security Manager**.

2. V levém panelu Uživatelské konzoly nástroje HP ProtectTools Security Manager vyberte položku **Správa** a poté **Konzola pro správu**.

3. Na levém panelu Konzoly pro správu nástroje HP ProtectTools vyberte možnost **Drive Encryption**.

Všeobecné úlohy

Aktivace aplikace Drive Encryption pro standardní pevné disky

Standardní pevné disky jsou šifrovány pomocí softwarového šifrování. Aktivaci aplikace Drive Encryption lze provést následovně:

1. Spusťte **Konzolu pro správu nástroje HP ProtectTools**. Další informace naleznete v části Otevření konzoly pro správu nástroje HP ProtectTools na stránce 16.

2. V levém panelu klikněte na položku **Průvodce nastavením**.

3. Zaškrtněte políčko **Drive Encryption** a pak klikněte na tlačítko **Další**.

4. Chcete-li vytvořit zálohu šifrovacího klíče, připojte externí zařízení pro záznam tohoto klíče. Tento klíč musí být použit k přístupu na data, pokud ostatní metody selžou.

5. V části **Zálohovat klíče aplikace Drive Encryption** zaškrtněte políčko u paměťového zařízení, do něhož má být uložen šifrovací klíč.

6. Klikněte na tlačítko **Další**.

POZNÁMKA: Budete vyzváni k restartu počítače. Po restartu se před spuštěním systému Windows zobrazí nástroj Drive Encryption, který vyžaduje přihlášení.

Nástroj Drive Encryption byl aktivován. Zašifrování vybraných oddílů jednotky může v závislosti na jejich počtu a velikosti trvat až několik hodin.

Další informace naleznete v nápovědě k nástroji HP ProtectTools Security Manager.

Aktivace aplikace Drive Encryption pro samošifrující jednotky

Samošifrující jednotky splňující specifikaci OPAL organizace Trusted Computing Group pro správu samošifrujících jednotek lze šifrovat prostřednictvím softwarového nebo hardwarového šifrování. Chcete-li aktivovat aplikaci Drive Encryption pro samošifrující jednotky, postupujte dle následujících kroků:

POZNÁMKA: Hardwarové šifrování je k dispozici pouze v případě, že všechny jednotky v počítači jsou jednotky s automatickým šifrováním splňující normy OPAL organizace Trusted Computing Group pro správu jednotek s automatickým šifrováním. V takovém případě je k dispozici možnost **Použít hardwarové šifrování jednotky** a lze použít šifrování hardwarové i softwarové.

Pokud je váš počítač vybaven kombinací jednotek s automatickým šifrováním a standardních pevných disků, možnost **Použít hardwarové šifrování jednotky** není k dispozici a lze použít pouze šifrování softwarové. Další informace naleznete v části Aktivace aplikace Drive Encryption pro standardní pevné disky na stránce 42.

- ▲ Aktivujte aplikaci Drive Encryption pomocí Průvodce nastavením nástroje HP ProtectTools Security Manager.

– nebo –

Softwarové šifrování

1. Spusťte **Konzolu pro správu nástroje HP ProtectTools**. Další informace naleznete v části Otevření konzoly pro správu nástroje HP ProtectTools na stránce 16.
2. V levém panelu klikněte na položku **Průvodce nastavením**.
3. Zaškrtněte políčko **Drive Encryption** a pak klikněte na tlačítko **Další**.

   POZNÁMKA: Je-li ve spodní části obrazovky uvedena možnost **Použít hardwarové šifrování jednotky**, zrušte zaškrtnutí jejího políčka.

4. V části **Jednotky, které mají být zašifrovány** zaškrtněte políčko u pevného disku, který chcete šifrovat, a poté klikněte na možnost **Další**.
5. Chcete-li vytvořit zálohu šifrovacího klíče, připojte úložné zařízení k odpovídající zásuvce.
6. V části **Zálohovat klíče aplikace Drive Encryption** zaškrtněte políčko u paměťového zařízení, do něhož má být uložen šifrovací klíč.
7. Klikněte na tlačítko **Použít**.

   POZNÁMKA: Počítač se restartuje.

   Aplikace Drive Encryption byla aktivována. Šifrování jednotky může v závislosti na její velikosti trvat i několik hodin.

Hardwarové šifrování

1. Spusťte **Konzolu pro správu nástroje HP ProtectTools**. Další informace naleznete v části Otevření konzoly pro správu nástroje HP ProtectTools na stránce 16.
2. V levém panelu klikněte na položku **Průvodce nastavením**.
3. Zaškrtněte políčko **Drive Encryption** a pak klikněte na tlačítko **Další**.
4. Pokud je ve spodní části obrazovky k dispozici políčko **Použít hardwarové šifrování jednotky**, zaškrtněte je.

   Jestliže políčko není zaškrtnuto nebo není k dispozici, je použito softwarové šifrování. Další informace naleznete v části Aktivace aplikace Drive Encryption pro standardní pevné disky na stránce 42.

5. V části **Jednotky, které mají být zašifrovány** zaškrtněte políčko u pevného disku, který chcete šifrovat, a poté klikněte na možnost **Další**.

POZNÁMKA: Pokud je v seznamu uvedena jediná jednotka, pole pro výběr jednotky je automaticky zaškrtnuto a nebude dostupné.

Je-li uvedena pouze jedna jednotka, automaticky se vybere disk 0, pole nebude dostupné, ale možnost výběru dalších pevných disků určených k hardwarovému šifrování bude k dispozici.

Dokud neoznačíte alespoň jednu jednotku, na tlačítko **Další** nebude možné kliknout.

6. Chcete-li vytvořit zálohu šifrovacího klíče, připojte úložné zařízení k odpovídající zásuvce.
7. V části **Zálohovat klíče aplikace Drive Encryption** zaškrtněte políčko u paměťového zařízení, do něhož má být uložen šifrovací klíč.
8. Klikněte na tlačítko **Použít**.

POZNÁMKA: Budete vyzváni k restartu počítače. Před spuštěním systému Windows se zobrazí nástroj Drive Encryption vyžadující vaše přihlášení.

Aplikace Drive Encryption byla aktivována. Šifrování jednotky může trvat několik minut.

Další informace naleznete v nápovědě k nástroji HP ProtectTools Security Manager.

Deaktivace aplikace Drive Encryption

K deaktivaci aplikace Drive Encryption mohou správci použít Průvodce nastavením nástroje HP ProtectTools Security Manager. Další informace naleznete v nápovědě k nástroji HP ProtectTools Security Manager.

1. Spusťte **Konzolu pro správu nástroje HP ProtectTools**. Další informace naleznete v části Otevření konzoly pro správu nástroje HP ProtectTools na stránce 16.
2. V levém panelu klikněte na položku **Průvodce nastavením**.
3. Zrušte zaškrtnutí pole **Drive Encryption** a pak klikněte na tlačítko **Další**.

Bude zahájena deaktivace aplikace Drive Encryption.

POZNÁMKA: V případě, že bylo použito softwarové šifrování, bude zahájeno dešifrování. V závislosti na velikosti zašifrovaných oddílů na jednotce může proces trvat až několik hodin. Po dokončení dešifrování se nástroj Drive Encryption deaktivuje.

Bylo-li použito hardwarové šifrování, jednotka bude okamžitě dešifrována a po několika minutách bude nástroj Drive Encryption deaktivován.

Po deaktivaci šifrování jednotky budete vyzváni k vypnutí počítače (v případě hardwarového šifrování) nebo jeho restartu (v případě softwarového šifrování).

Přihlášení po aktivaci aplikace Drive Encryption

Zapnete-li počítač po aktivaci aplikace Drive Encryption a uživatelský účet je zahrnut, je třeba se přihlásit na přihlašovací obrazovce aplikace Drive Encryption:

POZNÁMKA: Během přechodu z úsporného režimu / režimu spánku do běžného provozu se obrazovka pro ověřování před spuštěním v rámci nástroje Drive Encryption v případě softwarového nebo hardwarového šifrování nezobrazí. Při hardwarovém šifrování máte k dispozici možnost **Zakažte režim spánku (vyšší úroveň zabezpečení)**, jejíž aktivace nepovolí přechod do režimu spánku nebo úsporného režimu.

Během přechodu z hibernace do běžného provozu se obrazovka pro ověřování před spuštěním v rámci nástroje Drive Encryption v případě softwarového ani hardwarového šifrování nezobrazí.

POZNÁMKA: Pokud správce systému Windows aktivoval funkci Zabezpečení před spuštěním v systému BIOS nástroje HP ProtectTools Security Manager a je povolena funkce One-Step Logon (výchozí nastavení), můžete se po ověření totožnosti v rámci Zabezpečení před spuštěním v systému BIOS okamžitě přihlašovat k počítači bez opětovného ověřování na přihlašovací obrazovce nástroje Drive Encryption.

Přihlášení jednoho uživatele:

- ▲ Na stránce **Přihlášení** zadejte heslo systému Windows, kód PIN čipové karty, SpareKey, tvář nebo přiložte zaregistrovaný prst.

Přihlášení více uživatelů:

1. Na stránce **Vyberte uživatele k přihlášení** vyberte z rozevíracího seznamu uživatele, pod kterým se chcete přihlásit, a poté klikněte na tlačítko **Další**.
2. Na stránce **Přihlášení** zadejte heslo systému Windows nebo kód PIN čipové karty nebo přiložte zaregistrovaný prst.

POZNÁMKA: Podporovány jsou následující čipové karty:

Podporované čipové karty

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

POZNÁMKA: Použijete-li k přihlášení na přihlašovací obrazovce Drive Encryption klíč obnovy, bude třeba před získáním přístupu k uživatelskému účtu zadat na přihlašovací stránce systému Windows další přihlašovací údaje.

Ochrana dat zašifrováním pevného disku

Důrazně doporučujeme k ochraně dat pomocí šifrování pevného disku používat Průvodce nastavením nástroje HP ProtectTools Security Manager. Po aktivaci můžete následujícím postupem šifrovat všechny přidané pevné disky nebo vytvořené oddíly:

1. Klikněte na ikonu **+** na levém panelu vlevo od položky **Drive Encryption**, abyste zobrazili dostupné možnosti.
2. Klikněte na tlačítko **Nastavení**.
3. U softwarově šifrovaných jednotek vyberte oddíly, které chcete zašifrovat.

POZNÁMKA: To samé také platí pro případ, kdy je přítomna jedna nebo více standardních jednotek a jedna nebo více samošifrujících jednotek.

– nebo –

- ▲ V případě hardwarově šifrovaných jednotek vyberte další jednotky, které mají být zašifrovány.

Pokročilé operace

Správa Drive Encryption (Šifrování jednotek) (úloha správce)

Správci mohou v rámci stránky Nastavení v nástroji Drive Encryption prohlížet a měnit stav nástroje Drive Encryption (povolen, zakázán nebo aktivace hardwarového šifrování) a prohlížet stav šifrování všech pevných disků v počítači.

POZNÁMKA: Na stránce s nastavením nástroje Drive Encryption můžete pouze vybrat nebo odebrat další pevné disky určené k hardwarovému šifrování.

- Je-li nastaven stav Zakázáno, nástroj Drive Encryption dosud nebyl správcem systému Windows aktivován a pevný disk není chráněn. Aktivujte aplikaci Drive Encryption pomocí Průvodce nastavením nástroje HP ProtectTools Security Manager.
- Je-li nastaven stav Povoleno, aplikace Drive Encryption byla aktivována a nakonfigurována. Jednotka je v některém z následujících stavů:

Softwarové šifrování

- Nešifrováno
- Šifrováno
- Šifrování
- Dešifrování

Hardwarové šifrování

- Šifrováno
- Nešifrováno (další jednotky)

Použití funkce Zvýšit zabezpečení pomocí TPM (pouze vybrané modely)

Pokud je aktivována funkce TPM (Trusted Platform Module) a vybrána funkce Zvýšit zabezpečení pomocí TPM v nástroji Drive Encryption, začne být heslo nástroje Drive Encryption chráněno pomocí bezpečnostního čipu TPM. Při odebrání a instalaci pevného disku v jiném počítači bude disk nepřístupný.

UPOZORNĚNÍ: Vlastnictví modulu TPM nelze sdílet s nástrojem Windows TPM.msc.

POZNÁMKA: Vzhledem k tomu, že heslo je chráněno pomocí bezpečnostního čipu TPM, nelze po přesunutí pevného disku do jiného počítače získat přístup k datům, nejsou-li do tohoto počítače současně také přenesena nastavení TPM.

POZNÁMKA: V nastavení systému BIOS musí být povolena možnost TPM.

Šifrování nebo dešifrování jednotlivých oddílů jednotky (pouze pomocí softwarového šifrování)

Správci mohou v rámci stránky s nastavením modulu Drive Encryption zašifrovat jeden nebo více oddílů jednotky v počítači nebo dešifrovat libovolné oddíly jednotky, které již byly zašifrovány.

1. Spusťte **Konzolu pro správu nástroje HP ProtectTools**. Další informace naleznete v části Otevření konzoly pro správu nástroje HP ProtectTools na stránce 16.
2. Klikněte na ikonu **+** na levém panelu vlevo od položky **Drive Encryption**, abyste zobrazili dostupné možnosti.

3. Klikněte na tlačítko **Nastavení**.
4. V části **Stav jednotky** zaškrtněte políčka u pevných disků, které chcete zašifrovat, nebo zrušte jejich zaškrtnutí u pevných disků, které chcete dešifrovat, a pak klikněte na tlačítko **Použít**.

POZNÁMKA: Je-li oddíl šifrován nebo dešifrován, indikátor průběhu zobrazí procento zašifrování oddílu a čas zbývající k dokončení procesu.

POZNÁMKA: Dynamické oddíly nejsou podporovány. Pokud je oddíl zobrazen jako dostupný, ale po výběru jej nelze zašifrovat, jedná se o dynamický oddíl. Dynamický oddíl vzniká zmenšováním oddílu za účelem vytvoření nového pomocí Správy disku.

Pokud má být oddíl převeden na dynamický, zobrazí se varování.

Záloha a obnova (úloha pro správce)

Pokud je aplikace Drive Encryption aktivována, správci mohou použít stránku Záloha šifrovacího klíče k zálohování šifrovacích klíčů na vyjímatelná média pro potřeby obnovení.

Zálohování šifrovacích klíčů

Správci mohou zálohovat šifrovací klíč pro šifrovanou jednotku na vyjímatelné paměťové zařízení.

UPOZORNĚNÍ: Nezapomeňte uložit paměťové zařízení obsahující záložní klíč na bezpečném místě. Zapomenete-li heslo, ztratíte-li čipovou kartu nebo nemáte-li zaregistrovaný prst, bude toto zařízení poskytovat jediný přístup k počítači. Dbejte také na bezpečnost úložiště, protože toto paměťové zařízení umožňuje přístup do systému Windows.

POZNÁMKA: Chcete-li uložit šifrovací klíč, je nutné použít paměťové zařízení USB s formátem FAT32 nebo FAT16. K zálohování lze použít paměťový modul USB, paměťovou kartu (SD) nebo kartu MMC.

1. Spusťte **Konzolu pro správu nástroje HP ProtectTools**. Další informace naleznete v části Otevření konzoly pro správu nástroje HP ProtectTools na stránce 16.
2. Klikněte na ikonu **+** na levém panelu vlevo od položky **Drive Encryption**, abyste zobrazili dostupné možnosti.
3. Klikněte na možnost **Zálohování šifrovacích klíčů**.
4. Připojte úložné zařízení, na kterém chcete vytvořit zálohu šifrovacího klíče.

   POZNÁMKA: Chcete-li uložit šifrovací klíč, je nutné použít paměťové zařízení USB s formátem FAT32. K zálohování lze použít paměťový modul USB, paměťovou kartu (SD) nebo kartu MMC. V některých případech lze použít funkci SkyDrive.
5. V části **Jednotka** zaškrtněte políčko u paměťového zařízení, v němž má být zálohován šifrovací klíč.
6. Klikněte na položku **Záložní klíče**.
7. Přečtěte si informace na zobrazené stránce a klikněte na tlačítko **OK**. Šifrovací klíč bude uložen do vybraného paměťového zařízení.

Obnovení přístupu k aktivovanému počítači pomocí záložních klíčů

Správci mohou provést obnovení pomocí klíče nástroje Drive Encryption zálohovaného na vyjímatelné paměťové zařízení nebo kliknutím na možnost **Zálohování šifrovacího klíče paměťové jednotky** v nástroji Security Manager.

1. Vložte vyjímatelné paměťové zařízení obsahující záložní klíč.
2. Zapněte počítač.
3. Jakmile se zobrazí přihlašovací dialogové okno nástroje Drive Encryption for HP ProtectTools, klikněte na tlačítko **Možnosti**.
4. Klikněte na možnost **Obnova**.
5. Zadejte umístění nebo název souboru obsahující záložní klíč a klikněte na tlačítko **Obnovit**.

   – nebo –

   Kliknutím na tlačítko **Procházet** požadovaný soubor se zálohou vyhledejte, klikněte na tlačítko **OK** a poté na možnost **Obnovit**.
6. Jakmile se zobrazí dialogové okno s potvrzením, klikněte na tlačítko **OK**.

   Zobrazí se přihlašovací obrazovka systému Windows.

POZNÁMKA: Použijete-li k přihlášení na přihlašovací obrazovce Drive Encryption klíč obnovy, bude třeba před získáním přístupu k uživatelskému účtu zadat na přihlašovací stránce systému Windows další přihlašovací údaje. Důrazně doporučujeme, abyste po provedení obnovy resetovali heslo.

Provedení obnovení HP SpareKey

Funkce obnovení SpareKey v rámci ověřování Drive Encryption před spuštěním systému vyžaduje zodpovězení bezpečnostních otázek. Další informace o nastavení funkce obnovení SpareKey naleznete v nápovědě k softwaru Security Manager.

Zapomenete-li heslo a chcete-li provést obnovení HP SpareKey, postupujte takto:

1. Zapněte počítač.
2. Jakmile se zobrazí stránka nástroje Drive Encryption for HP ProtectTools, přejděte na stránku pro přihlášení uživatelů.
3. Klikněte na možnost **SpareKey**.

POZNÁMKA: Jestliže nebylo ověřování SpareKey v nástroji Security Manager aktivováno, tlačítko **SpareKey** nebude dostupné.

4. Zadejte správné odpovědi na uvedené otázky a klikněte na tlačítko **Přihlásit**.

   Zobrazí se přihlašovací obrazovka systému Windows.

POZNÁMKA: Použijete-li k přihlášení na přihlašovací obrazovce Drive Encryption funkci SpareKey, bude třeba před získáním přístupu k uživatelskému účtu zadat na přihlašovací stránce systému Windows další přihlašovací údaje. Důrazně doporučujeme, abyste po provedení obnovy resetovali heslo.

Zobrazení stavu šifrování

K zobrazení stavu šifrování lze použít nástroj HP ProtectTools Security Manager.

POZNÁMKA: Správci mohou změnit stav aplikace Drive Encryption pomocí Konzoly pro správu nástroje HP ProtectTools.

1. Spusťte **Uživatelskou konzolu HP ProtectTools**. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
2. V části **Moje data** klikněte na položku **Drive Encryption**.

   V případě softwarového nebo hardwarového šifrování se zobrazí jeden z následujících stavů šifrování disku:

   - Povoleno
   - Zakázáno

   V případě softwarového šifrování se u každého pevného disku nebo oddílu jednotky zobrazí jeden z následujících stavů šifrování disku:

   - Nešifrováno
   - Zašifrováno
   - Šifrování
   - Dešifrování

   V případě hardwarového šifrování se zobrazí jeden z následujících stavů šifrování disku:

   - Nešifrováno
   - Zašifrováno

   Je-li pevný disk právě šifrován nebo dešifrován, indikátor průběhu zobrazí procento dokončení a čas zbývající k dokončení šifrování nebo dešifrování.

7 Device Access Manager for HP ProtectTools (jen vybrané modely)

Aplikace HP ProtectTools Device Access Manager řídí přístup k datům tím, že zakazuje zařízení pro přenos dat.

POZNÁMKA: Některá člověkem ovládaná nebo vstupní zařízení, jako je myš, klávesnice, zařízení TouchPad a čtečka otisků prstů, nejsou aplikací Device Access Manager řízena. Další informace naleznete v části Třídy nespravovaných zařízení na stránce 59.

Správci operačního systému Windows® používají aplikaci HP ProtectTools Device Access Manager při řízení přístupu k zařízením v systému a k ochraně před neoprávněným přístupem:

- Pro každého uživatele jsou vytvořeny profily zařízení s cílem definovat zařízení, k nimž má či nemá umožněn přístup.
- Funkce ověřování v reálném čase (JITA) umožňuje ověření předdefinovaných uživatelů, aby měli přístup k zařízením, která jsou jinak zakázána.
- Správce a důvěryhodné uživatele lze vyloučit z omezení přístupu vynucovaných aplikací Device Access Manager, a to tak, že je přidáte do skupiny Správci zařízení. Členství v této skupině můžete nastavit pomocí nabídky Rozšířená nastavení.
- Přístup k zařízení může být přidělen nebo odmítnut na základě členství jednotlivých uživatelů ve skupině.
- U tříd zařízení, jako jsou jednotky CD-ROM a DVD, lze přístup pro čtení a přístup pro zápis povolit či odmítnout jednotlivě.

Spuštění aplikace Device Access Manager

1. Přihlaste se jako správce.
2. Spusťte nástroj **HP ProtectTools Security Manager** z **nástrojového panelu nástroje HP Client Security**.

   – nebo –

   Na ploše systému Windows dvakrát klikněte na ikonu **HP ProtectTools** v oznamovací oblasti umístěné na pravé straně hlavního panelu.

   – nebo –

   v **Ovládacích panelech** vyberte **Systém a zabezpečení** a poté **HP ProtectTools Security Manager**.
3. V levém panelu Uživatelské konzoly nástroje HP ProtectTools Security Manager klikněte na položku **Správa** a poté vyberte položku **Konzola pro správu**.
4. V levém panelu nástroje Konzola pro správu klepněte na položku **Device Access Manager**.

Standardní uživatel může zobrazovat zásady aplikace HP ProtectTools Device Access Manager pomocí aplikace HP ProtectTools Security Manager. Tato konzola zobrazuje pouze informace ke čtení.

Postupy nastavení

Konfigurace přístupu zařízení

Aplikace HP ProtectTools Device Access Manager nabízí čtyři zobrazení:

- **Jednoduchá konfigurace** – umožňuje povolit nebo odmítnout přístup k třídám zařízení na základě členství ve skupině Správci zařízení.
- **Konfigurace tříd zařízení** – umožňuje povolit nebo odmítnout přístup k typům zařízení či specifickým zařízením pro jednotlivé uživatele nebo skupiny.
- **Konfigurace JITA** – slouží ke konfiguraci funkce ověřování v reálném čase (JITA) a umožňuje vybraným uživatelům přístup k jednotkám DVD/CD-ROM a vyměnitelným médiím prostřednictvím vlastního ověření.
- **Rozšířená nastavení** – slouží ke konfiguraci seznamu písmen jednotek, ke kterým aplikace Device Access Manager nebude omezovat přístup, jako je jednotka C nebo systémová jednotka. Z tohoto zobrazení lze také spravovat členství ve skupině Správci zařízení.

Jednoduchá konfigurace

Správci mohou využít zobrazení **Jednoduchá konfigurace** k povolení nebo zakázání přístupu k následujícím třídám zařízení pro všechny uživatele, kteří nejsou členy skupiny Device Administrators:

- Všechna vyjímatelná média (diskety, jednotky USB Flash atd.)
- Všechny jednotky DVD/CD-ROM
- Všechny sériové a paralelní porty
- Všechna zařízení Bluetooth

POZNÁMKA: Pokud používáte zařízení Bluetooth k ověřování, neměli byste je v zásadách aplikace Device Access Manager zakazovat.

- Všechna modemová zařízení
- Všechna zařízení PCMCIA/ExpressCard
- Všechna zařízení 1394

Chcete-li povolit nebo odmítnout přístup ke třídě zařízení pro všechny uživatele, kteří nejsou členy skupiny Device Administrators, postupujte takto:

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak na položku **Jednoduchá konfigurace**.
2. Chcete-li odmítnout přístup, zaškrtněte v pravém podokně políčko pro specifické zařízení nebo třídu zařízení. Chcete-li pro specifické zařízení nebo třídu zařízení povolit přístup, zrušte zaškrtnutí příslušného políčka.

   Pokud je zaškrtávací políčko zobrazeno šedě, byly hodnoty ovlivňující scénář přístupu změněny v rámci zobrazení **Konfigurace tříd zařízení**. Chcete-li obnovit konfigurační nastavení výrobce, klikněte v zobrazení **Konfigurace třídy zařízení** na možnost **Obnovit**.
3. Klikněte na tlačítko **Použít**.

POZNÁMKA: Pokud služba na pozadí není spuštěna, zobrazí se dialogové okno s dotazem, zda ji chcete spustit. Klikněte na tlačítko **Ano**.

4. Klikněte na tlačítko **OK**.

Spuštění služby na pozadí

Při prvním definování a použití nových zásad se automaticky spustí služba na pozadí HP ProtectTools Device Locking/Auditing a nastaví se, aby se spouštěla automaticky při každém startu systému.

POZNÁMKA: Před zobrazením výzvy služby na pozadí musí být definován profil zařízení.

Správci rovněž mohou tuto službu spustit nebo ukončit.

Ukončení služby Device Locking/Auditing neznamená ukončení uzamčení zařízení. Zamykání zařízení vynucují dvě komponenty:

- Služba Device Locking/Auditing
- Ovladač DAMDrv.sys

Spuštění služby znamená spuštění ovladače, ale ukončení služby neznamená ukončení ovladače.

Chcete-li určit, zda je spuštěna služba na pozadí, otevřete okno příkazového řádku a zadejte příkaz `sc query flcdlock`.

Chcete-li určit, zda je spuštěn ovladač zařízení, otevřete okno příkazového řádku a zadejte příkaz `sc query damdrv`.

Zobrazení Device Class Configuration (Konfigurace tříd zařízení)

Správci mohou zobrazovat a upravovat seznamy uživatelů a skupin, jimž je uděleno nebo odmítnuto oprávnění k přístupu k třídám zařízení nebo specifickým zařízením.

Zobrazení **Konfigurace tříd zařízení** obsahuje následující části:

- **Seznam zařízení** – zobrazuje všechny třídy zařízení a zařízení, která jsou v systému nainstalována nebo která byla v systému nainstalována dříve.
  - Ochrana je zpravidla použita pro třídu zařízení. Vybraný uživatel nebo skupina bude mít přístup k libovolnému zařízení v rámci třídy zařízení.
  - Ochrana může být rovněž použita pro specifická zařízení.
- **Seznam uživatelů** – zobrazuje všechny uživatele a skupiny, jimž je udělen nebo odmítnut přístup k vybrané třídě zařízení nebo specifickému zařízení.
  - Položka v seznamu uživatelů může odpovídat specifickému uživateli nebo skupině, jíž je tento uživatel členem.
  - Je-li položka uživatele nebo skupiny v seznamu User List (Seznam uživatelů) nedostupná, bylo toto nastavení zděděno ze třídy zařízení v seznamu Device List (Seznam zařízení) nebo ze složky Class.
  - Některé třídy zařízení, jako jsou například jednotky CD-ROM a DVD, mohou být dále řízeny povolením nebo odmítnutím přístupu pro operace čtení a pro operace zápisu.

    U ostatních tříd a zařízení mohou být práva čtení a zápisu zděděna. Například přístup pro čtení může být zděděn z vyšší třídy, ale přístup pro zápis může být pro uživatele nebo skupinu specificky odmítnut.

    POZNÁMKA: Je-li zaškrtávací políčko **Čtení** prázdné, nemá položka řízení přístupu žádný vliv na přístup pro čtení k danému zařízení, ale přístup pro čtení není odmítnut.

    POZNÁMKA: Skupinu správci nelze přidat do seznamu uživatelů. Místo toho použijte skupinu Správci zařízení.

Příklad 1 – je-li uživateli nebo skupině odmítnut přístup pro zápis pro určité zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny lze udělit přístup pro zápis nebo přístup pro čtení a zápis pouze pro zařízení, které je v hierarchii zařízení umístěno pod tímto zařízením.

Příklad 2 – je-li uživateli nebo skupině povolen přístup pro zápis pro určité zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny lze odmítnout přístup pro zápis nebo přístup pro čtení a zápis pouze pro stejné zařízení nebo pro zařízení, které je v hierarchii zařízení umístěno pod tímto zařízením.

Příklad 3 – je-li uživateli nebo skupině povolen přístup pro čtení pro určité zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny lze odmítnout přístup pro čtení nebo přístup pro čtení a zápis pouze pro stejné zařízení nebo pro zařízení, které je v hierarchii zařízení umístěno pod tímto zařízením.

Příklad 4 – je-li uživateli nebo skupině odmítnut přístup pro čtení pro určité zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny lze udělit přístup pro zápis nebo přístup pro čtení a zápis pouze pro zařízení, které je v hierarchii zařízení umístěno pod tímto zařízením.

Příklad 5 – je-li uživateli nebo skupině povolen přístup pro čtení a zápis pro určité zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny lze odmítnout přístup pro zápis nebo přístup pro čtení a zápis pouze pro stejné zařízení nebo pro zařízení, které je v hierarchii zařízení umístěno pod tímto zařízením.

Příklad 6 – je-li uživateli nebo skupině odmítnut přístup pro čtení a zápis pro určité zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny lze udělit přístup pro čtení nebo přístup pro čtení a zápis pouze pro zařízení, které je v hierarchii zařízení umístěno pod tímto zařízením.

Odmítnutí přístupu uživateli nebo skupině

Chcete-li uživateli nebo skupině zabránit v přístupu k zařízení nebo třídě zařízení, postupujte takto:

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klikněte na třídu zařízení, kterou chcete konfigurovat.
   - **Třída zařízení**
   - **Všechna zařízení**
   - **Jednotlivé zařízení**
3. V části **Uživatel/skupiny** vyberte skupinu, pro niž chcete odmítnout přístup, a pak klikněte na tlačítko **Odmítnout**.
4. Klikněte na tlačítko **Použít**.

POZNÁMKA: Jsou-li na stejné úrovni zařízení pro uživatele použita nastavení pro povolení a odmítnutí, odmítnutí přístupu má přednost před povolením.

Povolení přístupu uživateli nebo skupině

Chcete-li uživateli nebo skupině udělit oprávnění pro přístup k zařízení nebo třídě zařízení, postupujte takto:

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klikněte na jednu z následujících položek:
   - **Třída zařízení**
   - **Všechna zařízení**
   - **Jednotlivé zařízení**
3. Klikněte na tlačítko **Add** (Přidat).

   Otevře se dialogové okno **Select Users or Groups** (Vybrat uživatele nebo skupiny).
4. Klikněte na položku **Advanced** (Upřesnit) a pak kliknutím na tlačítko **Find Now** (Hledat nyní) vyhledejte uživatele nebo skupiny, které chcete přidat.
5. Klikněte na uživatele nebo skupinu, které chcete přidat do seznamu dostupných uživatelů a skupin, a pak klikněte na tlačítko **OK**.
6. Znovu klikněte na tlačítko **OK**.
7. Kliknutím na položku **Allow** (Povolit) udělte tomuto uživateli přístup.
8. Klikněte na tlačítko **Použít**.

Povolení přístupu ke třídě zařízení pro jednoho uživatele nebo skupinu

Chcete-li uživateli umožnit přístup ke třídě zařízení a všem ostatním členům skupiny tohoto uživatele odmítnout přístup, postupujte takto:

1. V levém podokně okna **Konzola pro správu nástroje HP ProtectTools** klikněte na položku **Device Access Manager** a pak na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klikněte na třídu zařízení, kterou chcete konfigurovat.
   - **Třída zařízení**
   - **Všechna zařízení**
   - **Jednotlivé zařízení**
3. V části **User/Groups** (Uživatel/skupiny) vyberte skupinu, pro niž chcete odmítnout přístup, a pak klikněte na tlačítko **Deny** (Odmítnout).
4. Přejděte ke složce pod složkou požadované třídy a pak přidejte konkrétního uživatele.
5. Kliknutím na položku **Allow** (Povolit) udělte tomuto uživateli přístup.
6. Klikněte na tlačítko **Použít**.

Povolení přístupu ke specifickému zařízení pro jednoho uživatele nebo skupinu

Správci mohou povolit přístup k určitému zařízení a současně všem ostatním členům skupiny tohoto uživatele odmítnout přístup ke všem zařízením v příslušné třídě:

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klikněte na třídu zařízení, kterou chcete konfigurovat, a pak přejděte ke složce pod ní.
3. V části **User/Groups** (Uživatel/skupiny) klikněte na tlačítko **Allow** (Povolit) vedle skupiny, jíž chcete udělit přístup.
4. Klikněte na tlačítko **Deny** (Odmítnout) vedle skupiny, jíž chcete odmítnout přístup.
5. V seznamu zařízení přejděte ke specifickému zařízení, k němuž chcete uživateli povolit přístup.
6. Klikněte na tlačítko **Add** (Přidat).

   Otevře se dialogové okno **Select Users or Groups** (Vybrat uživatele nebo skupiny).
7. Klikněte na položku **Advanced** (Upřesnit) a pak kliknutím na tlačítko **Find Now** (Hledat nyní) vyhledejte uživatele nebo skupiny, které chcete přidat.
8. Klikněte na uživatele, kterému má být povolen přístup, a pak klikněte na tlačítko **OK**.
9. Kliknutím na položku **Allow** (Povolit) udělte tomuto uživateli přístup.
10. Klikněte na tlačítko **Použít**.

Odebrání nastavení uživatele nebo skupiny

Chcete-li uživateli nebo skupině odebrat oprávnění pro přístup k zařízení nebo třídě zařízení, postupujte takto:

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klikněte na třídu zařízení, kterou chcete konfigurovat.
   - **Třída zařízení**
   - **Všechna zařízení**
   - **Jednotlivé zařízení**
3. V části **User/Groups** (Uživatel/skupiny) klikněte na uživatele nebo skupinu, která má být odebrána, a pak klikněte na tlačítko **Remove** (Odebrat).
4. Klikněte na tlačítko **Použít**.

Obnovení konfigurace

UPOZORNĚNÍ: Obnovení konfigurace způsobí odstranění všech změn konfigurace, které byly provedeny, a u všech nastavení obnoví hodnoty nastavené výrobcem.

POZNÁMKA: Stránka Rozšířená nastavení resetována nebude.

Chcete-li obnovit konfigurační nastavení výrobce, postupujte takto:

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak na položku **Konfigurace tříd zařízení**.
2. Klikněte na možnost **Obnovit**.
3. V žádosti o potvrzení klikněte na možnost **Ano**.
4. Klikněte na tlačítko **Použít**.

Konfigurace JITA

Zobrazení Konfigurace JITA umožňuje správcům zobrazovat a upravovat seznamy uživatelů a skupin, jimž je udělen přístup k zařízením prostřednictvím funkce ověřování v reálném čase (JITA).

Uživatelé s povolenou funkcí JITA budou moci přistupovat k některým zařízením, pro která byly omezeny zásady vytvořené v zobrazeních **Konfigurace tříd zařízení** nebo **Jednoduchá konfigurace**.

- **Scénář** – zásady zobrazení Jednoduchá konfigurace jsou nastaveny tak, aby všem nesprávcům zakazovaly přístup k jednotce DVD/CD-ROM.
- **Výsledek** – uživatel s povolenou funkcí JITA, který se pokusí o přístup k jednotce DVD/CD-ROM, obdrží stejnou zprávu “Přístup zamítnut”, jako uživatel bez povolené funkce JITA. Poté se zobrazí bublina se zprávou, zda uživatel chce použít přístup pomocí funkce JITA. Po kliknutí na bublinu se zobrazí dialogové okno ověření uživatele. Pokud uživatel úspěšně zadá přihlašovací údaje, bude mu udělen přístup k jednotce DVD/CD-ROM.

Dobu použití funkce JITA lze povolit na stanovený počet minut nebo 0 minut. Doba použití funkce JITA o hodnotě 0 minut nikdy nevyprší. Uživatelé budou mít přístup k zařízení od chvíle ověření až do odhlášení ze systému.

Dobu použití funkce JITA lze také prodloužit, bylo-li tak nakonfigurováno. V tomto scénáři mohou uživatelé 1 minutu před vypršením doby použití funkce JITA kliknout na výzvu a prodloužit přístup bez nutnosti opětovného ověření.

Bez ohledu na to, zda je uživateli udělena omezená či neomezená doba použití funkce JITA, jakmile se uživatel odhlásí ze systému nebo se přihlásí jiný uživatel, doba použití funkce JITA vyprší. Při příštím přihlášení uživatele a pokusu o přístup k zařízení, pro něž je povolena funkce JITA, se zobrazí výzva k zadání přihlašovacích údajů.

Funkce JITA je dostupná pro následující třídy za řízení:

- Jednotky DVD/CD-ROM
- Vyměnitelná média

Vytvoření funkce JITA pro uživatele nebo skupinu

Správci mohou uživatelům nebo skupinám povolit přístup k zařízením prostřednictvím ověřování v reálném čase.

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak klikněte na položku **Konfigurace JITA**.
2. V rozevírací nabídce zařízení vyberte možnost **Vyměnitelná média** nebo **Jednotky DVD/CD-ROM**.
3. Kliknutím na položku **+** přidáte uživatele nebo skupinu do konfigurace funkce JITA.
4. Zaškrtněte políčko **Povoleno**.

5. Nastavte dobu použití funkce JITA na požadovaný čas.
6. Klikněte na tlačítko **Použít**.

Při použití nového nastavení funkce JITA se musí uživatel odhlásit a poté znovu přihlásit.

Vytvoření rozšiřitelné funkce JITA pro uživatele nebo skupinu

Správci mohou uživatelům nebo skupinám povolit přístup k zařízením prostřednictvím ověření v reálném čase, které může uživatel před vypršením prodloužit.

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak klikněte na položku **Konfigurace JITA**.
2. V rozevírací nabídce zařízení vyberte možnost **Vyměnitelná média** nebo **Jednotky DVD/CD-ROM**.
3. Kliknutím na položku **+** přidáte uživatele nebo skupinu do konfigurace funkce JITA.
4. Zaškrtněte políčko **Povoleno**.
5. Nastavte dobu použití funkce JITA na požadovaný čas.
6. Zaškrtněte políčko **Prodloužitelné**.
7. Klikněte na tlačítko **Použít**.

Při použití nového nastavení funkce JITA se musí uživatel odhlásit a poté znovu přihlásit.

Zakázání funkce JITA pro uživatele nebo skupinu

Správci mohou uživatelům nebo skupinám zakázat přístup k zařízením prostřednictvím ověření v reálném čase.

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klikněte na položku **Device Access Manager** a pak klikněte na položku **Konfigurace JITA**.
2. V rozevírací nabídce zařízení vyberte možnost **Vyměnitelná média** nebo **Jednotky DVD/CD-ROM**.
3. Vyberte uživatele nebo skupinu, kterým chcete zakázat použití funkce JITA.
4. Zrušte zaškrtnutí políčka **Povoleno**.
5. Klikněte na tlačítko **Použít**.

Pokud se uživatel přihlásí a pokusí o přístup k zařízení, přístup mu bude zakázán.

Rozšířená nastavení

Rozšířená nastavení poskytují následující funkce:

- Správa skupiny Správci zařízení
- Správa písmen jednotek, pro které aplikace Device Access Manager nikdy nezakazuje přístup.

Skupina Správci zařízení slouží k vyloučení důvěryhodných uživatelů (důvěryhodných, co se týče přístupu k zařízení) z omezení přístupu vynucovaných zásadami aplikace Device Access Manager. Důvěryhodní uživatelé obvykle zahrnují správce systému. Další informace naleznete v části Skupina Správci zařízení na stránce 58.

Zobrazení **Rozšířená nastavení** také umožňuje správci nakonfigurovat seznam písmen jednotek, k nimž nebude aplikace Device Access Manager omezovat přístup pro žádného uživatele.

POZNÁMKA: Služby na pozadí aplikace Device Access Manager musí být při konfiguraci písmen jednotek spuštěny.

Postup spuštění těchto služeb:

1. Použijte zásady zobrazení Jednoduchá konfigurace, aby například všem nesprávcům zařízení zakazovaly přístup k vyměnitelným médiím.

   – nebo –

   Otevřete okno příkazového řádku s oprávněními správce, a poté zadejte:

   ```
   sc start flcdlock
   ```

   Stiskněte klávesu enter.

2. Po spuštění služeb můžete upravit seznam jednotek. Zadejte písmena jednotek, k nimž nechcete řídit přístup pomocí aplikace Device Access Manager.

   Písmena jednotek jsou zobrazena pro fyzické pevné disky a oddíly.

POZNÁMKA: Ať už se v seznamu nachází systémová jednotka či nikoli (obvykle jednotka C), přístup k ní nebude nikdy žádnému uživateli zakázán.

Skupina Správci zařízení

Při instalaci aplikace Device Access Manager je vytvořena skupina Device Administrators (Správci zařízení).

Skupina Správci zařízení slouží k vyloučení důvěryhodných uživatelů (důvěryhodných, co se týče přístupu k zařízení) z omezení přístupu vynucovaných zásadami aplikace Device Access Manager. Důvěryhodní uživatelé obvykle zahrnují správce systému.

POZNÁMKA: Přidání do skupiny Device Administrators (Správci zařízení) neumožňuje automaticky uživateli přístup k zařízením. Pokud je skupině uživatelů v zobrazení **Konfigurace tříd zařízení** zakázán přístup k zařízení, skupině Správci zařízení musí být udělen přístup, aby její členové mohli přistupovat k zařízení. Zobrazení **Jednoduchá konfigurace** lze ale použít k zakázání přístupu k třídám zařízení pro všechny uživatele, kteří nejsou členy skupiny Správci zařízení.

Postup přidání uživatelů do skupiny Správci zařízení:

1. V zobrazení **Rozšířená nastavení** klikněte na možnost **+**.
2. Zadejte uživatelské jméno důvěryhodného uživatele.
3. Klikněte na tlačítko **OK**.
4. Klikněte na tlačítko **Použít**.

Podpora zařízení eSATA

Aby mohla aplikace Device Access Manager řídit přístup k zařízením eSATA, musí být nakonfigurováno následující:

1. Jednotka musí být při spuštění počítače připojena.
2. V zobrazení **Rozšířená nastavení** se ujistěte, že písmeno jednotky eSATA není uvedeno v seznamu jednotek, ke kterým nebude aplikace Device Access Manager zakazovat přístup. Pokud je písmeno jednotky eSATA v seznamu uvedeno, odstraňte je a poté klikněte na možnost **Použít**.
3. Přístup k zařízení lze řídit prostřednictvím třídy Vyměnitelná zařízení pomocí zobrazení **Jednoduchá konfigurace** nebo **Konfigurace tříd zařízení**.

Třídy nespravovaných zařízení

Aplikace HP ProtectTools Device Access Manager nespravuje následující třídy zařízení:

- Vstupně-výstupní zařízení
  - Biometrická zařízení
  - Myš
  - Klávesnice
  - Tiskárna
  - Tiskárny podporující technologii Plug and play (PnP)
  - Upgrade tiskárny
  - Zařízení infračerveného lidského rozhraní
  - Čtečka čipových karet
  - Víceportové sériově připojené zařízení
  - Disková jednotka
  - Řadič disketové jednotky (FDC)
  - Řadič pevného disku (HDC)
  - Třída zařízení lidského rozhraní (HID)
- Napájení
  - Baterie
  - Podpora pokročilé správy napájení (APM)
- Různé
  - Počítač
  - Dekodér
  - Displej
  - Procesor
  - Systém
  - Neznámé

- Svazek
- Snímek objemu
- Bezpečnostní zařízení
- Bezpečnostní urychlovač
- Jednotný ovladač zobrazení Intel®
- Ovladač médií
- Měnič médií
- Multifunkční
- Karta s právními informacemi
- Síťový klient
- Síťová služba
- Síťový přenos
- Adaptér SCSI

8 Obnova po krádeži (pouze u vybraných modelů)

Služba Computrace for HP ProtectTools (prodávaná samostatně) umožňuje vzdáleně sledovat, spravovat a monitorovat polohu počítačů.

Po aktivaci bude služba Computrace for HP ProtectTools konfigurována na stránkách zákaznického centra společnosti Absolute Software. V rámci zákaznického centra může správce konfigurovat službu Computrace for HP ProtectTools tak, aby počítač sledovala nebo spravovala. V případě ztráty nebo krádeže počítače může zákaznické centrum pomoci odpovídajícím úřadům počítač vyhledat a získat zpět. Po konfiguraci bude služba Computrace fungovat i v případě vymazání nebo výměny pevného disku.

Aktivace služby Computrace for HP ProtectTools:

1. Připojte se k Internetu.
2. Otevřete Uživatelskou konzolu nástroje Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 25.
3. V levém podokně nástroje Security Manager klikněte na položku **Obnova po krádeži**.
4. Chcete-li spustit Průvodce aktivací služby Computrace, klikněte na tlačítko **Začněte**.
5. Zadejte kontaktní údaje spolu s údaji pro platbu platební kartou, nebo vložte předem zakoupený klíč produktu.

Průvodce aktivací bezpečně zpracuje transakci a vytvoří uživatelský účet na stránkách zákaznického centra společnosti Absolute Software. Po dokončení obdržíte e-mail s potvrzením, který obsahuje informace o účtu v zákaznickém centru.

Jestliže jste již dříve Průvodce aktivací služby Computrace spustili a máte účet v zákaznickém středisku, můžete si zakoupit další licence, pokud se obrátíte na zástupce společnosti HP.

Přihlášení k zákaznickému centru:

1. Přejděte na adresu https://cc.absolute.com/.
2. Do polí **ID přihlášení** a **Heslo** zadejte přihlašovací údaje, které jste obdrželi v e-mailu s potvrzením, a poté klikněte na tlačítko **Přihlásit**.

Pomocí účtu v zákaznickém centru můžete následující:

- sledovat počítače,
- chránit data na dálku,
- hlásit krádeže počítačů chráněných službou Computrace.

▲ Další informace o službě Computrace for HP ProtectTools naleznete po kliknutí na tlačítko **Další informace**.

9 Výjimky při lokalizaci hesel

Na úrovni funkce Zabezpečení před spuštěním a aplikace HP Drive Encryption je podpora lokalizace hesel omezena.

Jak postupovat, pokud bylo heslo odmítnuto

Heslo může být odmítnuto z následujících důvodů:

- Uživatel používá editor IME, který není podporován. Jedná se o běžný problém s dvoubajtovými jazyky (korejštinou, japonštinou, čínštinou atd.). Řešení:

  1. Pomocí nástroje **Ovládací panely** přidejte podporované rozvržení klávesnice (v části Čínština přidejte americké rozvržení klávesnice).
  2. Podporovanou klávesnici nastavte na výchozí zadávání.
  3. Restartujte nástroj HP ProtectTools a zadejte heslo znovu.

- Uživatel používá znak, který není podporován. Řešení:

  1. Změňte heslo systému Windows tak, aby obsahovalo jen podporované znaky. Další informace o nepodporovaných znacích naleznete v nápovědě ke Konzole pro správu nástroje HP ProtectTools.
  2. Spusťte průvodce nastavením nástroje HP ProtectTools Security Manager a zadejte nové heslo systému Windows.

Na úrovni funkce Zabezpečení před spuštěním a aplikace HP Drive Encryption nejsou podporovány editory IME systému Windows

V systému Windows lze pomocí editoru IME a standardní klávesnice zadávat složité znaky a symboly jazyků, jako jsou např. japonština a čínština.

Na úrovni funkce Zabezpečení před spuštěním a aplikace HP Drive Encryption nejsou editory IME podporovány. Na přihlašovací obrazovce funkce Zabezpečení před spuštěním nebo aplikace HP Drive Encryption nelze zadat heslo pomocí editoru IME, jelikož by mohlo dojít k blokaci. V některých případech systém Microsoft® Windows při zadávání hesla editor IME nezobrazí.

Řešením je přepnout na jedno z následujících podporovaných rozvržení klávesnice, které překládá na rozvržení klávesnice 00000411:

- editor Microsoft IME pro japonštinu,
- japonské rozvržení klávesnice,
- editor Office 2007 IME pro japonštinu. Pokud společnost Microsoft nebo třetí strana použijí termín „editor IME“ nebo „editor metody zadávání znaků“, nemusí se ve skutečnosti o editor IME jednat. Tato skutečnost působí zmatek, jelikož daný software může umět hexadecimální kód číst. Takže pokud editor IME provádí mapování na rozvržení klávesnice, může nástroj HP ProtectTools danou konfiguraci podporovat.

VAROVÁNÍ! Pokud bude použit nástroj HP ProtectTools, budou hesla zadaná pomocí editoru Windows IME odmítnuta.

Změna hesla pomocí rozvržení klávesnice, které je rovněž podporováno

Pokud bylo heslo původně nastaveno pomocí jednoho rozvržení klávesnice, např. Anglické (Spojené státy) (409), a uživatel poté heslo změní pomocí jiného rozvržení klávesnice, které je rovněž podporováno, např. Latinskoamerické (080A), bude nové heslo fungovat v aplikaci HP Drive Encryption. Co se týče systému BIOS, zde bude heslo fungovat rovněž, avšak jedině v případě, pokud nebudou použity znaky, které v původním rozvržení neexistují (např. ē).

POZNÁMKA: Tento problém mohou správci vyřešit pomocí možnosti Správa uživatelů nástroje HP ProtectTools. Pomocí této možnosti je třeba uživatele z nástroje HP ProtectTools odstranit, poté je třeba v operačním systému vybrat požadované rozvržení klávesnice a nakonec znovu pro stejného uživatele spustit průvodce nastavením nástroje Security Manager. V systému BIOS dojde k uložení požadovaného rozvržení klávesnice a hesla zadaná pomocí tohoto rozvržení budou v systému BIOS nastavena správně.

Další možný problém spočívá v zadávání stejných znaků pomocí různých rozvržení klávesnice. Například pomocí rozvržení klávesnice Mezinárodní (USA) (20409) a Latinskoamerické (080A) lze (i když stisknutím různých kláves) vytvořit stejný znak „é“. Pokud však bylo heslo původně zadáno pomocí rozvržení klávesnice Latinskoamerické, bude toto rozvržení nastaveno v systému BIOS, a to i přesto, že bylo heslo později změněno pomocí rozvržení klávesnice Mezinárodní (USA).

Práce se speciálními klávesami

- Čínština, slovenština, kanadská francouzština a čeština

  Pokud bylo uživatelem vybráno jedno z těchto rozvržení klávesnice a poté bylo zadáno heslo (např. abcdef), je třeba ve funkci Zabezpečení před spuštěním systému BIOS nebo aplikaci HP Drive Encryption zadat stejné heslo stisknutím klávesy shift pro malá písmena a kláves shift a caps lock pro velká písmena. Hesla složená z čísel je třeba zadat pomocí numerické klávesnice.

- Korejština

  Pokud bylo uživatelem vybráno podporované rozvržení klávesnice Korejština a poté bylo zadáno heslo, je třeba ve funkci Zabezpečení před spuštěním systému BIOS nebo aplikaci HP Drive Encryption zadat stejné heslo stisknutím klávesy pravý alt pro malá písmena a kláves pravý alt a caps lock pro velká písmena.

- V následující tabulce jsou uvedeny nepodporované znaky:

Jazyk	Windows	BIOS	Drive Encryption
Arabština	Stisknutím klávesy ﻯ ,ﻱ nebo ﻱ dojde k vytvoření dvou znaků.	Stisknutím klávesy ﻯ ,ﻱ nebo ﻱ dojde k vytvoření jednoho znaku.	Stisknutím klávesy ﻯ ,ﻱ nebo ﻱ dojde k vytvoření jednoho znaku.
Kanadská francouzština	Stisknutím klávesy ç, è, à nebo é spolu s klávesou caps lock dojde v systému Windows k vytvoření znaku Ç, È, À resp. É.	Stisknutím klávesy ç, è, à nebo é spolu s klávesou caps lock dojde v rámci funkce Zabezpečení před spuštěním systému BIOS k vytvoření znaku ç, è, à resp. é.	Stisknutím klávesy ç, è, à nebo é spolu s klávesou caps lock dojde v nástroji HP Drive Encryption k vytvoření znaku ç, è, à resp. é.

Jazyk	Windows	BIOS	Drive Encryption
Španělština	Rozvržení klávesnice 40a není podporováno. I přesto toto rozvržení funguje, protože je softwarem převedeno na rozvržení c0a. Avšak z důvodu velkých rozdílů mezi těmito rozvrženími klávesnice je španělsky mluvícím uživatelům doporučeno změnit rozvržení klávesnice systému Windows na 1040a (Španělské - variace) nebo 080a (Latinskoamerické).	Není k dispozici	Není k dispozici
Mezinárodní (Spojené státy)	◦ Nelze použít klávesy ¡, ¤, ‘, ’, ¥ a × v horní řadě. ◦ Nelze použít klávesy å, ® a Þ v druhé řadě. ◦ Nelze použít klávesy á, ð a ø v třetí řadě. ◦ Nelze použít klávesu æ v dolní řadě.	Není k dispozici	Není k dispozici
Čeština	◦ Nelze použít klávesu ğ. ◦ Nelze použít klávesu į. ◦ Nelze použít klávesu ų. ◦ Nelze použít klávesy ė, ı a ż ◦ Nelze použít klávesy ģ, ķ, ļ, ņ a ţ	Není k dispozici	Není k dispozici
Slovenština	Nelze použít klávesu ż.	◦ Klávesy š, ś a ş lze použít pouze na softwarové klávesnici. ◦ Stisknutím znaménkové klávesy ţ dojde k vytvoření dvou znaků.	Není k dispozici
Maďarština	Nelze použít klávesu ż.	Stisknutím klávesy ţ dojde k vytvoření dvou znaků.	Není k dispozici

Jazyk	Windows	BIOS	Drive Encryption
Slovinština	Klávesu žŽ nelze použít v systému Windows a klávesa alt v systému BIOS představuje znaménkovou klávesu.	V systému BIOS nelze použít klávesy ú, Ú, ů, Ů, ş, Ş, ś, Ś, š a Š.	Není k dispozici
Japonština	Pokud je to možné, je lépe používat editor IME Microsoft Office 2007. Navzdory názvu se v tomto případě vlastně jedná o podporované rozvržení klávesnice 411.	Není k dispozici	Není k dispozici

Slovníček

aktivace
Úkol musí být dokončen, aby byly přístupné jakékoliv funkce Drive Encryption (Šifrování jednotky). Funkce Drive Enryption (Šifrování jednotek) je aktivována pomocí průvodce nastavením HP ProtectTools. Funkci Drive Encryption (Šifrování jednotek) může aktivovat pouze správce. Proces aktivace se skládá z aktivace softwaru, šifrování jednotky, tvorby uživatelského účtu a tvorby počátečního záložního šifrovacího klíče na odnímatelném úložném zařízení.

archiv pro nouzovou obnovu
Chráněné úložiště, které umožňuje opětovné šifrování základních uživatelských klíčů z jednoho klíče vlastníka platformy na jiný.

biometrická
Způsob ověřování uživatele, který pro identifikaci uživatele používá například otisk prstu.

certifikát pravosti (CA)
Služba, která vydává certifikáty vyžadované pro funkci infrastruktury používající veřejné klíče.

čipová karta
Malé hardwarové zařízení, velikostí a tvarem podobné kreditní kartě, které uchovává identifikační informace týkající se majitele. Používá se k ověření vlastníka pro práci s počítačem.

dešifrování
Postup používaný k šifrování, který má za úkol převést šifrovaná data na nešifrovaný text.

doména
Skupina počítačů v rámci jedné sítě, které sdílí společnou adresářovou databázi. Domény jsou jednoznačně pojmenovány a každá obsahuje sadu společných pravidel a procedur.

Drive Encryption (Šifrování jednotky)
Chrání vaše data šifrováním vašeho pevného disku(ů), čímž budou informace bez řádné autorizace nečitelné.

DriveLock
Bezpečnostní funkce, která přiřazuje pevný disk jednotlivým uživatelům a vyžaduje od uživatele, aby při spuštění počítače zadal správné heslo zámku jednotek DriveLock.

Identifikační karta
Miniaplikace na pracovní ploše systému Windows, která slouží k vizuální identifikaci pracovní plochy pomocí jména uživatele a zvoleného obrázku.

identita
Skupina ověření a nastavení v aplikaci HP ProtectTools Security Manager, která je zpracovávána stejně jako účet nebo profil určitého uživatele.

Jednotné přihlášení
Funkce, která uchovává ověřovací údaje a umožňuje uživateli použít aplikaci Security Manager pro přístup k síti Internet a k aplikacím systému Windows, které vyžadují ověření pomocí hesla.

JITA
Ověřování v reálném čase.

Kód PIN
Osobní identifikační číslo.

Konzola pro správu

Centrální místo, v němž lze přistupovat k funkcím a nastavením tohoto programu a spravovat je v konzole pro správu nástroje HP ProtectTools.

metoda zabezpečeného přihlašování
Způsob použitý pro přihlášení se k počítači.

obnovení HP SpareKey
Možnost přístupu k počítači správnou odpovědí na bezpečnostní otázky.

obnovit
Proces, který zkopíruje informace o programu z dříve uloženého záložního souboru do tohoto programu.

odvolání hesla
Heslo, které je vytvořeno při žádosti uživatele o digitální certifikát. Heslo je požadováno, když chce uživatel odvolat svůj digitální certifikát. Tím se zajistí, že odvolat certifikát může pouze uživatel.

otisk prstu
Digitální extrakce obrázku vašeho otisku prstu. Security Manager nikdy neukládá aktuální obrázek vašeho otisku prstu.

ověření při spuštění
Bezpečnostní funkce, která vyžaduje při spuštění počítače určitou formu ověření, například pomocí čipové karty, bezpečnostního čipu nebo hesla.

ověřování
Proces, při kterém se ověřuje, zda je uživatel oprávněn provádět určitou operaci, například použití počítače, úpravu nastavení určitého programu nebo zobrazení zabezpečených dat.

PKI
Standard infrastruktury veřejného klíče, který definuje rozhraní pro vytváření, používání a spravování certifikátů a šifrovacích klíčů.

poskytovatel kryptografických služeb (CSP)
Poskytovatel nebo knihovna šifrovacích algoritmů, které lze použít v řádně definovaném rozhraní, aby prováděly určité funkce šifrování.

prostředek
Datová komponenta sestávající z osobních údajů nebo souborů, historických dat, dat z webu nebo jiných dat, která jsou umístěna na pevném disku.

přihlášení
Objekt v nástroji Security Manager, který obsahuje jméno a heslo uživatele (a případně další zvolené informace) a který lze použít pro přihlášení k webovým stránkám nebo k jiným programům.

Přihlašovací obrazovka Drive Encryption (Šifrování jednotky)
Přihlašovací obrazovka, která se zobrazí před spuštěním systému Windows. Uživatel musí zadat své uživatelské jméno a heslo systému Windows nebo kód PIN čipové karty. Zadání správných informací na přihlašovací obrazovce aplikace Drive Encryption ve většině případů umožní přímý přístup do systému Windows, aniž by bylo nutné se znovu přihlašovat na přihlašovací obrazovce systému Windows.

přihlašovací údaje
Postup, při kterém uživatel prokazuje způsobilost k provádění určité operace během procesu ověřování.

restart
Proces restartování počítače.

režim zařízení SATA
Režim přenosu dat mezi počítačem a velkokapacitním úložným zařízením, jako např. pevný disk, nebo optická jednotka.

scéna

Fotografie zaregistrovaného uživatele pro použití k ověřování.

síťový účet
Účet uživatele nebo správce systému Windows na místním počítači, v pracovní skupině nebo v doméně.

skupina
Skupina uživatelů, kteří mají stejnou úroveň přístupu nebo odepření přístupu ke třídě zařízení nebo jednotlivým zařízením.

služba na pozadí
služba HP ProtectTools Device Locking/Auditing běžící na pozadí, která musí být spuštěna, aby mohly být použity zásady řízení přístupu k zařízením. Lze ji zobrazit pomocí části Služby v ovládacím panelu Nástroje pro správu. Pokud tato služba není spuštěna, nástroj HP ProtectTools Security Manager se ji pokusí spustit při použití zásad řízení přístupu k zařízením.

správce
Viz *Správce systému Windows*.

Správce Windows
Uživatel s úplnými právy upravovat povolení a spravovat ostatní uživatele.

šifrování
Způsob kódování a dekódování dat, kdy je lze dekódovat pouze pověřenými osobami.

šifrování
Kryptografický proces, během kterého je běžný text převeden do šifry za použití algoritmu, za účelem ochrany dat před neautorizovaným přístupem. Způsobů šifrování je mnoho a jsou základem zabezpečení na síti. Běžné způsoby zahrnují symetrickou šifru DES a dvouklíčové šifrování Public-key.

Šifrovaný souborový systém (Encryption File System - EFS)
Systém, který šifruje všechny soubory a vnořené složky v rámci zvolené složky.

třída zařízení
Všechna zařízení určitého typu, např. jednotky.

TXT
Trusted Execution Technology.

Účet uživatele systému Windows
Profil jednotlivce, který má oprávnění pro přihlášení k síti nebo k určitému počítači.

uživatel
Kdokoliv registrovaný v Drive Encryption. Uživatelé bez správcovských oprávnění mají omezená práva v Drive Encryption. Mohou se jen registrovat (se souhlasem správce) a přihlásit.

Vestavěný bezpečnostní čip TPM (Trusted Platform Module)
Obecný výraz pro čip HP ProtectTools Embedded Security. Čip TPM spíše než k ověření uživatele slouží k ověření počítače. K tomu používá uložené informace definující hostitelský systém, jako např. šifrovací klíče, digitální certifikáty a hesla. Čip TPM slouží ke snížení rizika situace, kdy by byla informace v počítači vyzrazena fyzickou krádeží nebo prostřednictvím vzdáleného útoku hackerem.

Zabezpečení přihlášení do systému Windows
Chrání váš účet(účty) systému Windows tak, že pro přihlášení vyžaduje použití specifických pověření.

zálohování
Pomocí funkce zálohování se uloží kopie důležitých informací o programu na místo mimo program. Může se později využít k obnově informací na stejný nebo jiný počítač.

zásady řízení přístupu k zařízení
Seznam zařízení, ke kterým je uživateli povolen nebo odepřen přístup.

Rejstřík

V

Z