HP ProtectTools

Začínáme

První vydání: Leden 2011

Číslo dokumentu: 638391-221

Obsah

1 Úvod do 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 (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.
Nástroj HP ProtectTools Security Manager (pro uživatele)	• Umožňuje uživatelům konfigurovat možnosti poskytované správcem. • Umožňuje správcům zajistit uživatelům omezený přístup k některým modulům nástroje HP ProtectTools.

Obsah nabídky dostupných softwarových modulů je závislý na modelu počítače.

Softwarové moduly HP ProtectTools mohou být předinstalovány, přednahrány do počítače nebo k dispozici pro stažení z internetových stránek společnosti HP. Další informace naleznete na webu http://www.hp.com.

POZNÁMKA: Pokyny v této příručce předpokládají, že jsou již nainstalovány odpovídající moduly softwaru HP ProtectTools.

Funkce nástroje HP ProtectTools

V následující tabulce najdete podrobnosti o nejdůležitějších funkcích modulů HP ProtectTools.

Modul	Klíčové funkce
Konzola pro správu nástroje HP ProtectTools (pro správce)	• Nastavení a konfigurace úrovní zabezpečení a způsobů bezpečného přihlášení pomocí Průvodce nastavením funkce Security Manager. • Konfigurace možností nedostupných uživatelům. • Konfigurace nastavení a uživatelského přístupu pro Device Access Manager. • Přidávání a odstraňování uživatelů HP ProtectTools a prohlížení stavu uživatele pomocí nástrojů správce.
Nástroj HP ProtectTools Security Manager (pro uživatele)	• Uspořádání, nastavení a změna hesel. • Konfigurace a změna údajů o uživateli, jako např. změna hesla systému Windows, otisku prstu a čipové karty. • Konfigurace a změna nastavení funkcí ničení, čištění aj. v aplikaci File Sanitizer. • Nastavení zobrazení pro Device Access Manager. • Konfigurace služby Computrace for HP ProtectTools. • Konfigurace předvoleb a možností zálohování a obnovení.
Credential Manager pro HP ProtectTools (nástroj Password manager)	• Ukládání, uspořádání a ochrana uživatelských jmen a hesel. • Nastavování přihlašovacích obrazovek na webových stránkách a programů pro rychlý a bezpečný přístup. • Ukládání uživatelských jmen a hesel pro webové stránky jejich zadáním do nástroje Password Manager. Při příští návštěvě dané stránky nástroj Password Manager automaticky vyplní a odešle příslušné údaje. • Vytváření silnějších hesel pro rozšířené zabezpečení účtu. Nástroj Password Manager umožňuje zadávat a odesílat informace automaticky.
Drive Encryption (Šifrování jednotek) pro HP ProtectTools (jen vybrané modely)	• Poskytuje kompletní šifrování celých oddílů pevných disků. • Vynucuje ověřování před spuštěním za účelem dešifrování a zajištění přístupu k datům.
File Sanitizer for HP ProtectTools	• Zajišťuje bezpečné ničení cenných digitálních položek (např. souborů aplikací, webových dat a dat spojených s historií nebo dalších důvěrných dat) ve vašem počítači a pravidelné čištění položek na pevném disku.
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 k zařízením s možností zápisu.

Modul	Klíčové funkce
Privacy Manager (Správce utajení) pro HP ProtectTools (jen vybrané modely)	• Slouží k získání certifikátů pravosti, které ověřují zdroj, integritu a zabezpečení komunikace při používání e-mailů a dokumentů aplikace Microsoft Office.
Služba Computrace for HP ProtectTools (prodává se samostatně)	• 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. • K aktivaci je zapotřebí samostatné zakoupení odběru služby sledování položek.
Nástroj Embedded Security for HP ProtectTools (pouze u vybraných modelů)	• Využívá vestavěný bezpečnostní čip TPM (Trusted Platform Module) k ochraně před neoprávněným přístupem k uživatelským datům a přihlašovacím údajům uloženým v počítači. • Umožňuje vytvářet osobní zabezpečené disky (PSD), které jsou užitečné při ochraně informací o uživatelských souborech a složkách. • Podporuje provádění operací chráněných digitálním certifikátem pomocí aplikací třetích stran (např. Microsoft Outlook a Internet Explorer).

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.

Nástroj Credential Manager for HP ProtectTools

Modul Credential Manager (součást nástroje Security 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 modul Credential Manager k propojení odkazů na web s různými uživatelskými jmény a hesly. Pokud následně otevře webovou stránku a pokusí se o přihlášení, modul Credential Manager ji automaticky poskytne potřebné přihlašovací údaje. Pokud si bude chtít prohlédnout uživatelská jména a hesla, modul Credential Manager lze nastavit tak, aby jي to umožňoval.

Modul Credential 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 aplikace Credential Manager for HP ProtectTools. Po dokončení účetní aplikaci Credential Manager předloží k používání zaměstnancům, kteří tak mohou využívat webové účty bez jakýchkoli informací o používaných přihlašovacích údajích.

Aplikace Drive Encryption for HP ProtectTools

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 vyžadující 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 SED (jednotka s automatickým šifrováním - Self-Encrypting Drive).

Nástroj Embedded Security for HP ProtectTools spolu s nástrojem Drive Encryption for HP ProtectTools neumožňují 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.

File Sanitizer for HP ProtectTools

Aplikace File Sanitizer for HP ProtectTools slouží k trvalému mazání dat, včetně informací o aktivitě prohlížeče Internetu, dočasných souborů, dříve odstraněných dat a dalších libovolných údajů. Aplikaci File Sanitizer je možné konfigurovat tak, že bude spuštěna buď ručně, nebo automaticky podle uživatelem definovaného rozvrhu.

Příklad 1: Právní zástupce často pracuje s citlivými informacemi o klientovi a chce se ujistit, že odstraněné soubory nebude možné obnovit. Právní zástupce použije aplikaci File Sanitizer k „zničení“ odstraněných souborů takovým způsobem, že jejich obnovení bude téměř nemožné.

Pokud v systému Windows odstraníte soubory běžným způsobem, data z pevného disku nebudou skutečně smazána. Namísto toho budou sektory pevného disku označeny za dostupné pro další použití. Dokud nebudou data přepsána, bude možné je snadno obnovit pomocí běžných nástrojů dostupných na Internetu. Aplikace File Sanitizer slouží k přepsání sektorů pomocí náhodných dat (podle potřeby i několikrát), čímž nebude možné odstraněná data přečíst ani obnovit.

Příklad 2: Vědecká pracovnice chce zničit odstraněná data, dočasné soubory, informace o aktivitě prohlížeče, atd. automaticky při jejím odhlášení. Používá aplikaci File Sanitizer k naplánování „ničení“ dat takovým způsobem, aby mohla vybrat běžné nebo vlastní soubory, které budou automaticky trvale odstraněny.

Device Access Manager for HP ProtectTools

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. Správce může také naplánovat způsob a čas, po který bude přístup k diskům povolen. Vhodným příkladem by byla situace, ve které prodejci mimo pracoviště potřebují přístup k firemním počítačům, avšak bez možnosti kopírování dat na jednotku USB. Aplikace Device Access Manager for HP ProtectTools umožňuje správcům omezit a spravovat přístup k hardwaru.

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.

Aplikace Privacy Manager for HP ProtectTools

Aplikace Privacy Manager for HP ProtectTools je vhodným řešením situace, ve které je třeba zajistit zabezpečení komunikace po Internetu prostřednictvím e-mailu. Uživatel bude moci vytvářet a odesílat pouze takové e-maily, které bude moci otevřít pouze ověřený příjemce. Díky aplikaci Privacy Manager nemůže podvodník informace zneužít nebo vysledovat.

Příklad 1: Burzovní makléř chce mít jistotu, že jeho e-maily jsou doručovány pouze daným klientům, jeho e-mailový účet nelze zfalšovat a odeslané e-maily vysledovat. Makléř přihlásí sebe a své klienty k aplikaci Privacy Manager. Aplikace Privacy Manager každému uživateli přiřadí certifikát pravosti (Certificate of Authentication - CA). V případě použití tohoto nástroje musí burzovní makléř i jeho klienti podstoupit před přenosem e-mailu ověření.

Aplikace Privacy Manager for HP ProtectTools umožňuje po ověření příjemce snadné odesílání i příjem e-mailů. Tuto e-mailovou službu je možné také zašifrovat. Postup šifrování je podobný jako v případě běžných nákupů na Internetu s využitím kreditních karet.

Příklad 2: Výkonný ředitel chce mít jistotu, že informace zaslané v e-mailu budou moci prohlížet pouze členové představenstva. Výkonný ředitel využije možnosti šifrování e-mailů, které jsou představenstvu odesílány a které jsou od nich přijímány. Certifikát pravosti aplikace Privacy Manager umožňuje výkonnému řediteli a představenstvu vlastnit kopii šifrovacího klíče, díky kterému budou jediní, kteří budou moci důvěrný e-mail dešifrovat.

Služba Computrace for HP ProtectTools (dříve pod názvem LoJack Pro)

Služba Computrace for HP ProtectTools (prodávaná samostatně) umožňuje vysledovat místo odcizeného počítače pokaždé, když se jeho uživatel připojí k Internetu.

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.

Služba Computrace for HP ProtectTools umožňuje také vzdáleně spravovat a sledovat polohu počítačů, monitorovat jejich využití a kontrolovat používané aplikace.

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.

Nástroj Embedded Security for HP ProtectTools (pouze u vybraných modelů)

Nástroj Embedded Security for HP ProtectTools umožňuje vytvořit osobní zabezpečený disk. Uživatel tak může v počítači vytvořit virtuální oddíl jednotky, který je až do jeho využití zcela neviditelný. Aplikaci Embedded Security je možné použít vždy, když je zapotřebí chránit data jejich skrytím a ponechat ostatní data nešifrovaná.

Příklad 1: Správce skladu využívá počítač, který během dne nepravidelně používá několik pracovníků. Správce chce zašifrovat a skrýt důvěrná data o skladu uložená v počítači. Chce zajistit takovou úroveň zabezpečení, že v případě odcizení pevného disku nebude možné data dešifrovat nebo přečíst. Správce skladu se rozhodne aktivovat aplikaci Embedded Security a přesune důvěrná

data na osobní zabezpečený disk. Správce poté může zadat heslo a využívat důvěrná data stejně, jako by to byl další pevný disk. Po odhlášení nebo restartu nebude osobní zabezpečený disk viditelný, ani jej nebude možné bez odpovídajícího hesla otevřít. Pracovníci během používání počítače důvěrná data vůbec neuvidí.

Nástroj Embedded Security uchovává šifrovací klíč na hardwarovém čipu TPM (Trusted Platform Module), který se nachází na základní desce. Jedná se o jediný šifrovací nástroj, který splňuje minimální požadavky na odolání pokusu o prolomení hesla, bude-li se někdo pokoušet heslo pro dešifrování uhodnout. Nástroj Embedded Security umožňuje také šifrování celých jednotek nebo e-mailů.

Příklad 2: Burzovní makléřka plánuje přenést velice důvěrná data do jiného počítače s využitím přenosné jednotky. Chce mít jistotu, že i při prozrazení hesla budou existovat pouze dva počítače, ve kterých bude možné jednotku použít. Makléřka využije možnosti přenosu pomocí technologie Embedded Security TPM, díky čemuž bude mít druhý počítač nezbytné šifrovací klíče potřebné k dešifrování dat. Během přenosu budou bez ohledu na heslo existovat pouze dva fyzické počítače, které budou moci data dešifrovat.

Dosažení klíčových cílů zabezpečení

Moduly HP ProtectTools mohou vzájemně spolupracovat, a poskytovat tak řešení pro různé problémy zabezpečení, včetně následujících klíčových cílů zabezpečení:

- Ochrana před cílenou krádeží
- Omezení přístupu k citlivým datům
- Zabránění neoprávněnému přístupu z interních či externích umístění
- Vytvoření silných zásad zabezpečení hesly

Ochrana proti cílené krádeži

Příkladem cílené krádeže může být krádež počítače obsahujícího důvěrné údaje a informace o zákaznících na kontrolním stanovišti na letišti. Následující funkce pomáhají ochránit proti cílené krádeži:

- Aktivací funkce ověřování před spuštěním zabráníte přístupu do operačního systému. Další informace naleznete v následujících kapitolách:
  - Aplikace Security Manager for HP ProtectTools
  - Nástroj Embedded Security for HP ProtectTools
  - Aplikace Drive Encryption for HP ProtectTools
- Funkce Osobní zabezpečený disk poskytovaná v rámci modulu Embedded Security for HP ProtectTools umožňuje šifrovat důvěrná data, a pomáhá tak zajistit, aby data nebylo možné bez ověření používat. Další informace naleznete v následující kapitole:
  - Nástroj Embedded Security for HP ProtectTools
- Služba Computrace umožňuje sledovat polohu odcizeného počítače. Další informace naleznete v následující kapitole:
  - Computrace for HP ProtectTools

Omezení přístupu k citlivým údajům

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 k zařízením s možností zápisu, takže citlivé informace nelze tisknout ani kopírovat z pevného disku na vyjímatelná média.

Zabránění neoprávněnému přístupu z interních či externích umístění

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. Další informace naleznete v následujících kapitolách:
  - Nástroj Password Manager for HP ProtectTools
  - Nástroj Embedded Security for HP ProtectTools
  - Nástroj Drive Encryption for HP ProtectTools
- Správce hesel pomáhá zajistit, že neoprávněný uživatel nemůže získat heslo pro přístup k aplikacím chráněným heslem.
- 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.
- Aplikace File Sanitizer umožňuje bezpečně mazat data pomocí ničení důležitých souborů a složek a čištění odstraněných položek na pevném disku (přepsáním dat, která byla odstraněna, ale která je i nadále možné obnovit).
- Aplikace Privacy Manager umožňuje získat certifikáty pravosti vhodné při používání e-mailů a dokumentů aplikace Microsoft Office. Odesílání a ukládání důležitých informací tak bude naprosto bezpečné.

Vytvoření přísných zásad ohledně hesel

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).

Další prvky zabezpečení

Přidělení bezpečnostních rolí

Při správě zabezpečení počítačů (zvláště u velkých organizací) je jedním z důležitých kroků rozdělení odpovědností a práv mezi různé druhy správců a uživatelů.

POZNÁMKA: V malých organizacích nebo při soukromém použití, může tyto role zastávat jedna a tatáž osoba.

U nástroje HP ProtectTools jsou 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 nástroje Drive Encryption nebo Embedded Security.

  POZNÁMKA: Mnohé funkce HP ProtectTools mohou být upraveny pracovníkem odpovědným za bezpečnost ve spolupráci s HP. Další informace naleznete na internetových stránkách společnosti HP 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 je doporučováno při omezení práv koncových uživatelů a omezení uživatelského přístupu postupovat podle „nejlepších postupů“.

Neoprávněným uživatelům by neměla být udělována správcovská oprávnění.

Správa hesel nástroje HP ProtectTools

Většina funkcí nástroje HP ProtectTools Security Manager je zabezpečena pomocí hesla. V následující tabulce je uveden seznam běžně používaných hesel, softwarových modulů, v nichž se tato hesla nastavují, a funkcí těchto hesel.

V tabulce jsou současně vyznačena hesla, která mohou nastavovat a používat pouze správci IT. Všechna ostatní hesla mohou nastavit jak běžní uživatelé, tak správci.

Heslo nástroje HP ProtectTools	Nastaven v tomto modulu	Funkce
Heslo přihlášení Windows	Ovládací panel Windows® nebo HP ProtectTools Security Manager	Může být použito pro manuální přihlášení se a ověření přístupu k různým funkcím Security Manager.
Heslo nástroje Security Manager Backup and Recovery	Security Manager, individuálním uživatelem	Chrání přístup k souboru zálohování a obnovení Security Manager.

Heslo nástroje HP ProtectTools	Nastaven v tomto modulu	Funkce
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 známka čipové karty.
Heslo známky nouzové obnovy	Modul Embedded Security, správce IT	Chrání přístup ke známce nouzové obnovy, což je soubor zálohy vestavěného bezpečnostního čipu.
Heslo vlastníka	Modul Embedded Security, správce IT	Chrání systém a čip TPM před neoprávněným přístupem ke všem funkcím majitele modulu Embedded Security.
Heslo správce systému BIOS	Nástroj Computer Setup, správce IT	Chrání přístup k nástroji Computer Setup.

Vytvoření bezpečného hesla

Při vytváření hesel musíte nejprve přihlédnout k požadavkům programu. V každém případě je však třeba zvážit následující pravidla, která vám pomohou vytvořit silně zabezpečené heslo a sníží riziko prolomení hesla:

- Používejte hesla s alespoň 6 znaky a pokud možno s více než 8 znaky.
- V hesle používejte zároveň znaky s velkým i malým písmenem.
- Pokud je to možné, používejte zároveň písmena i čísla a speciální znaky a znaménka interpunkce.
- V klíčovém slově nahraďte písmena čísly nebo speciálními znaky. Například můžete číslem 1 nahradit písmena I nebo L.
- Kombinujte slova ze 2 a více jazyků.
- Rozdělte slova nebo fráze uprostřed pomocí čísel nebo speciálních znaků, například „Mary2-2Cat45“.
- Nepoužívejte jako heslo slovo, které lze najít 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.
- Hesla pravidelně měňte. Stačí vždy změnit pouze několik znaků.
- Pokud si zapíšete heslo, neskladujte jej na běžně přístupném místě v blízkosti počítače.
- Neukládejte heslo do souboru na počítači, například do zprávy elektronické pošty.
- Nesdílejte s nikým uživatelské účty ani nikomu neprozrazujte hesla.

Zálohování a obnovování přihlašovacích údajů aplikace HP ProtectTools

Funkci zálohování a obnovení nástroje HP ProtectTools můžete použít k výběru a zálohování přihlašovacích údajů a nastavení HP ProtectTools.

2 Průvodce Začínáme s nastavením

Průvodce nastavením nástroje Security Manager vás provede procesem povolení dostupných funkcí zabezpečení, které se vztahují na všechny uživatele počítače. Tyto funkce můžete také spravovat na stránce Bezpečnostní funkce v Konzole pro správu.

Postup nastavení funkcí zabezpečení prostřednictvím průvodce nastavením nástroje Security Manager:

1. Pomocí ikony miniaplikace HP ProtectTools na ploše nebo pomocí ikony panelu nástrojů v oznamovací oblasti na pravé straně hlavního panelu spusťte nástroj HP ProtectTools Security Manager.

Barva proužku v rámci miniaplikace HP ProtectTools na ploše informuje o jednom z následujících stavů:

- Červená – Nástroj HP ProtectTools není instalován, nebo některý z jeho modulů je v chybovém stavu.
- žlutá – Ověřte na stránce Applications Status (Stav aplikací) modulu Security Manager, zda není nutné provést nějaké změny nastavení.
- Modrá – Nástroj HP ProtectTools je nainstalován a funguje správně.

Ve spodní části ikony miniaplikace se zobrazí zpráva oznamující jeden z následujících stavů:

- **Nastavit nyní** — Správce musí kliknout na ikonu miniaplikace, aby spustil Průvodce nastavením aplikace Security Manager, kde může konfigurovat přihlašovací údaje pro ověřování v počítači.

  Průvodce nastavením je nezávislá aplikace.

- **Registrovat nyní** — Uživatel musí kliknout na ikonu miniaplikace, aby spustil průvodce Začínáme v aplikaci Security Manager, kde může zaregistrovat přihlašovací údaje pro ověřování v počítači.

  Průvodce Začínáme se zobrazuje na nástrojovém panelu aplikace Security Manager.

- **Zkontrolovat nyní** — Kliknutím na ikonu miniaplikace zobrazíte další podrobnosti na stránce Stav bezpečnostních aplikací.

POZNÁMKA: Ikona miniaplikace HP ProtectTools na ploše není v systému Windows XP k dispozici.

– nebo –

Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**. V levém podokně klikněte na položku **Průvodce nastavením**.

2. Přečtěte si text na uvítací obrazovce a poté klikněte na tlačítko **Další**.

3. Zadáním hesla systému Windows ověřte svou identitu a klikněte na tlačítko **Další**.

   Pokud jste dosud nevytvořili heslo Windows, budete k tomu vyzváni. Heslo Windows je požadováno za účelem ochrany vašeho účtu Windows před přístupem neoprávněných osob a kvůli použití funkcí HP ProtectTools Security Manager.

4. Na stránce SpareKey vyberte tři bezpečnostní otázky a pro každou z nich zadejte odpověď. Poté klikněte na možnost **Další**.

   Na stránce SpareKey v nástroji **Credential Manager** na nástrojovém panelu aplikace Security Manager můžete vybrat různé otázky nebo změnit odpovědi.

POZNÁMKA: Nastavení hesla SpareKey mohou provádět pouze správci.

5. Povolte funkce zabezpečení zaškrtnutím jejich polí a poté klikněte na možnost **Další**.

   Čím více funkcí zvolíte, tím lépe bude počítač zabezpečen.

POZNÁMKA: Tato nastavení platí pro všechny uživatele. Pokud žádná pole nezaškrtnete, průvodce nastavením nebude uživatelům zobrazovat výzvu k registraci přihlašovacích údajů.

- **Zabezpečení přihlášení do systému Windows** – Chrání účty systému Windows, neboť pro přístup požaduje použití specifických přihlašovacích údajů.

- **Drive Encryption** – Chrání data zašifrováním pevných disků, takže pro osoby bez řádné autorizace budou informace nečitelné.

- **Zabezpečení před spuštěním** - Chrání počítač ještě před spuštěním systému Windows zákazem přístupu neautorizovaným osobám.

POZNÁMKA: Funkce Zabezpečení před spuštěním nebude k dispozici, pokud ji systém BIOS nepodporuje.

6. Průvodce nastavením vás vyzve k registraci přihlašovacích údajů.

   Pokud není k dispozici čtečka otisků prstů, čipová karta ani webová kamera, budete vyzváni k zadání hesla pro systém Windows. Poté budete moci zaregistrované přihlašovací údaje použít k ověření vaší identity, kdykoli to bude potřeba.

POZNÁMKA: Registraci těchto přihlašovacích údajů mohou provádět pouze správci.

7. Na poslední stránce průvodce klepněte na **Dokončit**.

   Zobrazí se domovská stránka panelu nástrojů nástroje Security Manager.

3 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 Security Manager nabízí další aplikace (pouze vybrané modely), které pomáhají s obnovením počítače v případě ztráty nebo odcizení.

Použití konzoly 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
- Přidávání dalších aplikací Security Manager

Otevření konzoly pro správu nástroje HP ProtectTools

Při provádění správy, jako je nastavení zásad systému nebo konfigurace softwaru, spusťte konzolu následujícím způsobem:

- Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.

  – nebo –

  V levém panelu 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.

▲ Chcete-li spustit Konzolu pro správu nástroje HP ProtectTools, klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.

nebo

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

Konzola se skládá z následujících komponent:

- **Domů** – Umožňuje nakonfigurovat následující možnosti zabezpečení:
  - **Zvýšit zabezpečení systému**
  - **Vyžadovat silné ověřování**
  - **Spravovat uživatele nástroje HP ProtectTools**
  - **Zjistit, jak lze centrálně spravovat nástroj HP ProtectTools**
- **Systém** – Umožňuje konfigurovat následující funkce zabezpečení a ověřování pro uživatele a zařízení:
  - **Zabezpečení**
  - **Používatelia**
  - **Přihlašovací údaje**
- **Aplikace** – Umožňuje konfigurovat nastavení nástroje HP ProtectTools Security Manager a aplikací nástroje Security Manager.
- **Data** – Poskytuje rozbalovací nabídku odkazů na aplikace Security Manager, které chrání vaše data.
- **Centrální správa** – Zobrazuje karty pro přístup k dalším řešením, aktualizacím produktů a zprávám.
- **Průvodce nastavením** – Provede vás nastavením nástroje HP ProtectTools Security Manager.
- **Podrobnosti** – 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 softwarovou 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 nastavení bezpečnostních zařízení vestavěných do počítače nebo k němu připojených.

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 přihlašování

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** klikněte na šipku dolů a poté vyberte kategorii uživatele:
   - **Pro správce tohoto počítače**
   - **Pro uživatele, kteří nejsou správci**
3. Určete ověřované přihlašovací údaje, které jsou požadované pro zvolenou kategorii uživatelů.
4. Vyberte, zda bude k ověření uživatele požadován JEDEN z blíže určených přihlašovacích údajů, nebo VŠECHNY.
5. Klikněte na tlačítko **Použít**.

Zásady relace

Definování zásad spravujících přihlašovací údaje požadované pro přístup k aplikacím HP ProtectTools 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** klikněte na šipku dolů a poté vyberte kategorii uživatele:
   - **Pro správce tohoto počítače**
   - **Pro uživatele, kteří nejsou správci**
3. Klikněte na šipku dolů a poté vyberte přihlašovací údaje pro ověřování požadované pro vybranou kategorii uživatele:
   - **Vyžadovat jeden z požadovaných přihlašovacích údajů**

     POZNÁMKA: Zrušením zaškrtnutí všech polí pro všechny přihlašovací údaje má stejný efekt jako výběr položky **Nevyžadovat ověřování**.
   - **Vyžadovat všechny zadané přihlašovací údaje**
   - **Nevyžadovat ověřování** — Výběrem této možnosti odstraníte všechny přihlašovací údaje uvedené v okně.
4. Klikněte na tlačítko **Použít**.

Nastavení

1. Zaškrtnutím pole povolíte následující nastavení a zrušením zaškrtnutí pole toto nastavení zakážete:

   Povolit přihlášení v jednom kroku – Umožňuje uživateli počítače přeskočit přihlášení do systému Windows, pokud bylo provedeno ověření v systému BIOS nebo na úrovni šifrovaného disku.
2. 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 specifikovat 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. Zaškrtnutím nebo zrušením zaškrtnutí pole můžete povolit či zakázat ověřování pomocí hesla SpareKey při přihlášení k systému Windows.
2. 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.
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.

čipová karta,

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

- **Nastavení** – Můžete nakonfigurovat počítač, aby se automaticky uzamkl, pokud je vyjmuta čipová karta.

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 Protect Tools. 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 podporovány, nejsou dostupné.

▲ Klikněte na tlačítko **Použít**.

tvář.

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

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. Klikněte na tlačítko **Přihlašovací údaje** a poté na tlačítko **Tvář**.
3. 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**.

4. Klikněte na možnost **Upřesnit** a poté nakonfigurujte další zabezpečení. Další informace naleznete v části Pokročilá uživatelská nastavení na stránce 40.

5. Klikněte na tlačítko **Použít**.

Konfigurace aplikací

Pro přizpůsobení chování aktuálně nainstalovaných aplikací HP ProtectTools Security Manager můžete použít nabídku Nastavení.

Chcete-li upravit nastavení aplikací, postupujte takto:

1. V levém panelu Konzoly pro správu v části **Aplikace** klikněte na možnost **Nastavení**.
2. Zaškrtněte pole vedle specifického nastavení, abyste je povolili. Zrušením zaškrtnutí dané nastavení zakážete.
3. Klikněte na tlačítko **Použít**.

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.

Karta Aplikace

Nastavení, která se zde zobrazují, je možné změnit při přidání nových aplikací do nástroje Security Manager. Minimální nastavení zobrazená ve výchozím nastavení jsou následující:

- **Stav aplikací** – Umožňuje zobrazení stavu u všech aplikací.
- **Password Manager** – Povoluje nástroj Password Manager pro všechny uživatele počítače.
- **Privacy Manager** – Povoluje aplikaci Privacy Manager pro všechny uživatele počítače.
- **Povolit odkaz Centrální správa** – Umožňuje všem uživatelům tohoto počítače přidávat aplikace do nástroje HP ProtectTools Security Manager kliknutím na odkaz **Centrální správa**.

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

Centrální správa

Do nástroje Security Manager lze přidat nové nástroje pro správu zpřístupňující další aplikace. Správce počítače může tuto funkci zakázat na stránce Nastavení. Stránka Centrální správa obsahuje dvě karty:

- **Řešení pro podniky** — Pokud je dostupné připojení k Internetu, můžete navštívit webové stránky společnosti DigitalPersona (http://www.digitalpersona.com/) a zkontrolovat, zda jsou dostupné nové aplikace.
- **Aktualizace a zprávy**
  - Pokud chcete být informováni o nových aplikacích a aktualizacích, zaškrtněte políčko **Informujte mě o nových aplikacích a aktualizacích**.
  - Pokud chcete vytvořit plán automatických aktualizací, zadejte počet dní.
  - Pokud chcete aktualizace zkontrolovat, klikněte na tlačítko **Zkontrolovat nyní**.

4 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 libovolným z následujících způsobů:

- Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, potom na položku **HP** a nakonec na položku **HP ProtectTools Security Manager**.
- Poklepejte na ikonu **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu.
- Klikněte pravým tlačítkem myši na ikonu **HP ProtectTools** a pak klikněte na příkaz **Spustit nástroj HP ProtectTools Security Manager**.
- Klikněte na ikonu miniaplikace **HP ProtectTools** na ploše.
- Stisknutím kombinace kláves ctrl+logo Windows+h otevřete nabídku **Rychlé odkazy nástroje Security Manager**.

  Informace o změně kombinace kláves naleznete v části Nastavení na stránce 35.

Použití nástrojového panelu nástroje Security Manager

Nástrojový panel nástroje Security Manager zajišťuje snadný přístup k funkcím, aplikacím a nastavením nástroje Security Manager.

▲ Chcete-li otevřít nástrojový panel nástroje Security Manager, klikněte na tlačítko **Start**, poté na položku **Všechny programy**, **HP** a položku **HP ProtectTools Security Manager**.

Nástrojový panel zobrazuje následující komponenty:

- **Identifikační karta** — zobrazuje jméno uživatele v systému Windows a obrázek přiřazený k účtu právě přihlášeného uživatele.
- **Bezpečnostní aplikace** — Slouží k zobrazení nabídky odkazů pro konfiguraci následujících typů zabezpečení:
  - **Domů** — Správa hesel, nastavení přihlašovacích údajů pro ověřování a kontrola stavu bezpečnostních aplikací.
  - **Stav** — Kontrola stavu bezpečnostních aplikací HP ProtectTools.

POZNÁMKA: Aplikace, které nejsou v počítači nainstalovány, nejsou v následujícím seznamu uvedeny.

- **Má přihlášení** — Správa přihlašovacích údajů pro ověřování Správce hesel, Credential Manager, hesla, SpareKey, karty Smart Card, tváře a otisky prstů.
- **Moje data** — Správa zabezpečení dat s nástroji Drive Encryption a File Sanitizer.
- **Tento počítač** — Správa zabezpečení počítače s aplikací Device Access Manager.
- **Komunikace** — Správa zabezpečení komunikace s aplikací Privacy Manager.
- **Správa** – Umožňuje správcům přístup k následujícím možnostem:
  - **Konzola pro správu** — Umožňuje správcům spravovat zabezpečení a uživatele.
  - **Centrální správa** — Poskytuje správcům přístup k dalším řešením, aktualizacím produktů a zprávám.
- **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.
  - **Podrobnosti** – 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 softwarovou nápovědu aplikace Security Manager. Tato ikona se nachází v pravém horním rohu okna vedle ikon pro minimalizaci a maximalizaci.

Stav bezpečnostních aplikací

Stav nainstalovaných bezpečnostních aplikací lze zobrazit na dvou místech:

- **Miniaplikace HP ProtectTools na pracovní ploše**

  Barva proužku v horní části ikony miniaplikace HP ProtectTools se mění podle celkového stavu nainstalovaných bezpečnostních aplikací.

  - **Červená** — Varování
  - **Žlutá** — Upozornění: není konfigurováno
  - **Modrá** — OK

  Ve spodní části ikony miniaplikace se zobrazí zpráva oznamující jeden z následujících stavů:

  - **Nastavit nyní** — Správce musí kliknout na ikonu miniaplikace, aby spustil Průvodce nastavením aplikace Security Manager, kde může konfigurovat přihlašovací údaje pro ověřování v počítači.

    Průvodce nastavením je nezávislá aplikace.

  - **Registrovat nyní** — Uživatel musí kliknout na ikonu miniaplikace, aby spustil průvodce Začínáme v aplikaci Security Manager, kde může zaregistrovat přihlašovací údaje pro ověřování v počítači.

    Průvodce Začínáme se zobrazuje na nástrojovém panelu aplikace Security Manager.

  - **Zkontrolovat nyní** — Kliknutím na ikonu miniaplikace zobrazíte další podrobnosti na stránce Stav bezpečnostních aplikací.

- **Stránka Stav bezpečnostních aplikací** — Kliknutím na možnost **Stav** na nástrojovém panelu aplikace Security Manager zobrazíte celkový stav nainstalovaných bezpečnostních aplikací a specifický stav jednotlivých aplikací.

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 webům na základě ověření pomocí hesla pro systém Windows, otisku prstu nebo čipové karty.
- **Credential Manager** – Nabízí snadný způsob změny hesla pro systém Windows, registrace otisků prstů či nastavení čipové karty.

Správci mohou přidávat další aplikace kliknutím na možnost **Správa** a následným kliknutím na možnost **Centrální správa** v levém dolním rohu nástrojového panelu.

Správce hesel

Použití Správce hesel 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, čipové karty 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, a automaticky vytvářet komplexní silná hesla pro nové weby.

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

▲ Kliknutím na ikonu **Správce hesel** zobrazíte kontextovou nabídku, která nabízí následující možnosti.

Webové stránky a programy, pro které dosud nebylo vytvořeno přihlášení

V kontextové nabídce jsou zobrazeny následující možnosti:

- **Přidat [doména.com] do Správce hesel** – Umožňuje přidat přihlášení pro aktuální přihlašovací obrazovku.
- **Spustit Správce hesel** – Spustí Správce hesel.
- **Nastavení ikony** – Umožňuje určit podmínky, za nichž se zobrazí ikona **Správce hesel**.
- **Nápověda** – Zobrazuje softwarovou nápovědu aplikace Security Manager.

Webové stránky a programy, pro které již bylo vytvořeno přihlášení

V kontextové nabídce jsou zobrazeny následující možnosti:

- **Vyplnit přihlašovací údaje** – Vloží přihlašovací údaje do přihlašovacích polí a pak stránku odešle (pokud při vytvoření nebo poslední úpravě přihlášení bylo určeno odeslání).
- **Upravit přihlášení** – Umožňuje upravit přihlašovací údaje pro daný web.
- **Přidat přihlášení** – Umožňuje přidat k přihlášení nový účet.
- **Spustit Správce hesel** – Spustí Správce hesel.
- **Nápověda** – Zobrazuje softwarovou 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 Správce hesel zadávat tyto informace za vás. Tato přihlášení můžete využít při otevření webové stránky nebo programu. Také můžete kliknout na přihlášení v nabídce **Přihlášení**. Správce hesel pak otevře příslušný web nebo program a přihlásí vás.

Chcete-li přidat přihlášení, postupujte takto:

1. Otevřete přihlašovací obrazovku pro požadovaný web nebo program.
2. Klikněte na šipku na ikoně **Správce hesel** a pak v závislosti na tom, zda se jedná o přihlášení k webu nebo programu, 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 Správce hesel**. Některé možnosti závisejí na bezpečnostních zařízeních, která jsou připojena k počítači, například použití klávesové zkratky ctrl+logo Windows+h, skenování otisku prstu či vložení čipové karty.
   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. Chcete-li povolit zabezpečení VeriSign VIP, vyberte zaškrtávací políčko **Chci na těchto stránkách použít zabezpečení VIP**.

      Tato možnost se zobrazuje pouze u stránek, pro které je zabezpečení VeriSign Identity Protection (VIP) dostupné. Pokud je danými stránkami podporováno, můžete také vedle běžné metody ověření vybrat možnost automatického vyplnění bezpečnostního kódu VIP.

e. Klikněte na tlačítko **OK**, klikněte na požadovanou metodu ověření (otisky prstů, heslo nebo tvář) a poté se přihlaste pomocí vybrané metody ověřování.

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

f. 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.
   - Pokud Správce hesel nemůže zjistit všechna přihlašovací pole, zobrazí se zpráva s dotazem, zda chcete pokračovat. Klikněte na tlačítko **Ano**.
   - Zobrazí se dialogové okno s vyplněnými přihlašovacími poli. Klikněte na ikonu u každého pole a přetáhněte ji do odpovídajícího přihlašovacího pole. Pak se kliknutím na tlačítko přihlaste na web.

     POZNÁMKA: Po zadání přihlašovacích údajů pro web pomocí ručního režimu je nutné pokračovat v této metodě při budoucím přihlášení na stejný web.

     POZNÁMKA: Ruční režim zadání přihlašovacích údajů nabízí pouze aplikace Internet Explorer 8.

   - 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 požadovaný web nebo program.
2. Chcete-li zobrazit dialogové okno umožňující upravit přihlašovací informace, klikněte na šipku na ikoně **Správce hesel** a pak klikněte 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 povolit zabezpečení VeriSign VIP, vyberte zaškrtávací políčko **Chci na těchto stránkách použít zabezpečení VIP**.

     Tato možnost se zobrazuje pouze u stránek, pro které je zabezpečení VeriSign VIP dostupné. Pokud je danými stránkami podporováno, můžete také vedle běžné metody ověření vybrat možnost automatického vyplnění bezpečnostního kódu VIP.

   - 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 přihlášení

Správce hesel nabízí rychlý a snadný způsob spouštění webů a programů, pro něž jste vytvořili přihlášení. Dvakrát klikněte na přihlášení k webu nebo programu v nabídce **Přihlášení** nebo na kartě **Správa** nástroje Správce hesel. Otevře se přihlašovací obrazovka a budou vyplněny přihlašovací údaje.

Přihlášení je po vytvoření automaticky přidáno do nabídky **Přihlášení** Správce hesel.

Chcete-li zobrazit nabídku **Přihlášení**, postupujte takto:

1. Stiskněte klávesovou zkratku pro nástroj **Password Manager**. Výchozí nastavení z výroby je ctrl +logo Windows+h. Chcete-li změnit klávesovou zkratku, na nástrojovém panelu aplikace Security Manager 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 nástrojovém panelu nástroje Security Manager klikněte na položku **Správce hesel**.
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 přihlášení, jsou jednotlivá přihlášení v seznamu uvedena pod názvem webu a odsazena.

Chcete-li provádět správu přihlášení, postupujte takto:

▲ Na nástrojovém panelu nástroje Security Manager klikněte na položku **Správce hesel** 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 webové stránky nebo program, pro které máte přihlašovací údaje.
  - **Přidat** — Přidání přihlašovacích údajů. Další informace naleznete v části Přidání přihlášení na stránce 30.
  - **Upravit** — Úprava přihlášení. Další informace naleznete v části Úprava přihlášení na stránce 31.
  - **Odstranit** — Odstraní webové stránky 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 32.

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.

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 Správce hesel pracovat s webovými stránkami obsahujícími přihlášení, klikněte na šipku u ikony a poté vyberte možnost **Nastavení ikony**.

   - **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky** – Zaškrtněte toto políčko, chcete-li, aby Správce hesel 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 Správce hesel 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 nástrojový panel aplikace Security Manager a poté klikněte na možnost **Správce hesel**.

     ◦ 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 30.

     ◦ Ikona **Správce hesel** se zobrazí při každém otevření této přihlašovací obrazovky webu nebo aplikace.

2. Chcete-li zakázat možnost zobrazení výzvy k přidání přihlašovacích údajů pro přihlašovací obrazovky, zaškrtněte pole.

3. Chcete-li zobrazit další nastavení nástroje Správce hesel, klikněte na položku **Správce hesel** a pak na nástrojovém panelu nástroje Security Manager klikněte na položku **Nastavení**.

VeriSign Identity Protection (VIP)

Pro přístup k webovým stránkám podporujícím zabezpečení VeriSign VIP můžete vytvořit přístupové tokeny VeriSign VIP. Tyto tokeny jsou používány nástrojem Správce hesel pro vytváření automatických přihlášení, která zahrnují použití tokenů přetažených na přihlašovací obrazovky podporující zabezpečení VeriSign nebo ručně zadaných do uvedených polí.

Povolit zabezpečení VeriSign VIP a vytvořit token můžete na nástrojovém panelu aplikace Security Manager nebo na kterýchkoli stránkách podporujících zabezpečení VeriSign VIP. Token je třeba zaregistrovat na všech webových stránkách, kde jej hodláte použít.

Po zaregistrování a prvním použití tokenu může (volitelně) dojít k jeho připojení k běžným přihlašovacím údajům a odeslání s nimi. V případě stránek nepovolujících připojení tokenu můžete provést přetažení nebo ruční zadání informací tokenu.

Povolení zabezpečení VeriSign VIP a vytvoření tokenu VeriSign VIP z nástrojového panelu aplikace Security Manager:

1. Otevřete nástrojový panel aplikace Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 26.
2. Klikněte na možnost **Správce hesel** a poté na možnost **VIP**.
3. Klikněte na tlačítko **Získat VIP**.

   Vytvoří se token zabezpečení VeriSign VIP, který se zobrazí na stránce VeriSign VIP. Token bude od této doby zobrazován při každé návštěvě této stránky.

Povolení zabezpečení VeriSign VIP a vytvoření tokenu VeriSign VIP na webových stránkách:

1. Nástroj Správce hesel zobrazí upozornění při každé návštěvě webových stránek podporujících zabezpečení VeriSign VIP.
2. Vytvořte přihlášení k dané obrazovce. Další informace naleznete v části Přidání přihlášení na stránce 30.
3. V dialogovém okně Vytvořit přihlášení vyberte možnost **Chci další ochranu účtu se zabezpečením VIP**.

Zaregistrování tokenu VeriSign VIP pro webové stránky:

1. Přihlaste se k webovým stránkám podporujícím zabezpečení VeriSign VIP ručně nebo pomocí nástroje Správce hesel.
2. Kliknutím na zobrazenou bublinu zabezpečení VeriSign VIP vytvořte přihlášení k daným stránkám.
3. V dialogovém okně Přidat přihlášení do Správce hesel vyberte možnost **Chci na těchto stránkách použít zabezpečení VIP**.

   Tato možnost se zobrazuje pouze u stránek, pro které je zabezpečení VeriSign VIP dostupné. Pokud je danými stránkami podporováno, můžete také vedle běžné metody ověření vybrat možnost automatického vyplnění bezpečnostního kódu VIP.

Nastavení

Je možné upravit nastavení nástroje HP ProtectTools Security Manager:

1. **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky** — Ikona **Správce hesel** se symbolem plus se zobrazí vždy, když je detekována přihlašovací obrazovka webu nebo programu, a indikuje, že je možné do trezoru hesel přidat přihlášení pro tuto obrazovku. Chcete-li tuto funkci zakázat, zrušte v dialogovém okně Nastavení ikony zaškrtnutí políčka **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky**.
2. **Spustit nástroj 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, zda se skutečně jedná o vás. Správce tohoto počítače může nastavit, které přihlašovací údaje lze použít k ověření vaší identity při přihlášení k účtu systému Windows, webům 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,
- čipová karta,
- tvář.

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. Na nástrojovém panelu 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 Začínáme.

Nastavení hesla SpareKey:

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

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 počítač disponuje vestavěnou nebo připojenou čtečkou otisků prstů, nástroj HP ProtectTools Security Manager vás při úvodním nastavení v průvodci Začínáme vyzve k nastavení nebo registraci otisků prstů. Otisky prstů můžete také zaregistrovat na stránce Otisk prstu v nástroji **Credential Manager** na nástrojovém panelu aplikace Security Manager.

1. Zobrazí se obrysy dvou rukou. Prsty, které již jsou registrované, jsou zvýrazněny zeleně. Klikněte na prst na obrysu.

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

2. Po výběru prstu pro registraci budete vyzváni k naskenování prstu, dokud jeho otisk nebude úspěšně zaregistrován. Zaregistrovaný prst se na obrysu zvýrazní zeleně.

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 postupu v části Začínáme, informace o otiscích prstů se neuloží, dokud nekliknete na tlačítko **Další**. Pokud necháte počítač chvíli neaktivní nebo zavřete program, provedené změny se **neuloží**.

Instalace čipové karty

Předtím, než bude možné čipovou kartu použít k ověřování, musí být inicializována a zaregistrována správcem.

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 software ActivIdentity.

1. Vložte kartu do čtečky.

2. Klikněte na tlačítko **Start**, poté na položku **Všechny programy** a poté na položku **ActivClient PIN Initialization Tool**.

3. Zadejte a potvrďte kód PIN.

4. Klikněte na tlačítko **Další**.

   Software čipové karty vám poskytne klíč pro odemčení. Většina čipových karet se po pěti neúspěšných pokusech o zadání kódu PIN zamkne. K odemčení karty slouží klíč.

5. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.

6. Klikněte na možnost **Přihlašovací údaje** a poté klikněte na možnost **Čipová karta**.

7. Klikněte na kartu **Správa**.
8. Ujistěte se, že je vybrána možnost **Nastavit čipovou kartu**.
9. Zadejte kód PIN, klikněte na tlačítko **Použít** a poté postupujte podle pokynů na obrazovce.
10. Jakmile čipovou kartu úspěšně inicializujete, bude ji třeba zaregistrovat.

Registrace čipové karty

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

1. V části **Centrální správa** klikněte na možnost **Průvodce nastavením**.
2. Na stránce Vítejte klikněte na tlačítko **Další** a poté zadejte heslo systému Windows.
3. Na stránce SpareKey klikněte na možnost **Přeskočit nastavení funkce SpareKey** (pokud nechcete aktualizovat informace ve funkci SpareKey).
4. Na stránce Povolit funkce zabezpečení klikněte na tlačítko **Další**.
5. Na stránce Vybrat přihlašovací údaje zkontrolujte, zda je vybrána možnost **Nastavit čipovou kartu**, a poté klikněte na možnost **Další**.
6. Na stránce Čipová karta zadejte kód PIN a poté klikněte na tlačítko **Další**.
7. Klikněte na tlačítko **Dokončit**.

Uživatelé mohou čipovou kartu také zaregistrovat v aplikaci Security Manager. Další informace naleznete v nápovědě k softwaru Security Manager for HP ProtectTools.

Konfigurace čipové karty

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

- **Nastavení** – Můžete nakonfigurovat počítač, aby se automaticky uzamkl, pokud je vyjmuta čipová karta.

  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 Protect Tools. 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 podporovány, nejsou dostupné.

▲ Klikněte na tlačítko **Použít**.

Registrace scén pro přihlášení pomocí tváře

Pokud počítač disponuje vestavěnou nebo připojenou webovou kamerou, nástroj HP ProtectTools Security Manager vás při úvodním nastavení v průvodci Začínáme vyzve k nastavení nebo registraci scén. Scény můžete také zaregistrovat na stránce Přihlášení pomocí tváře v nástroji **Credential Manager** na nástrojovém panelu aplikace 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.

Registrace scény v průvodci Začínáme:

1. V průvodci na stránce Tvář klikněte na možnost **Upřesnit** a poté nakonfigurujte další zabezpečení. Další informace naleznete v části Pokročilá uživatelská nastavení na stránce 40.
2. Klikněte na tlačítko **OK**.
3. Klikněte na možnost **Spustit**. Pokud jste již dříve scény registrovali, klikněte na možnost **Zaregistrovat novou scénu**.
4. Pokud jste nevybrali žádné další možnosti zabezpečení, budete vyzváni k výběru možnosti dodatečného zabezpečení. Postupujte podle pokynů na obrazovce a poté klikněte na možnost **Další**. Další informace naleznete v části Pokročilá uživatelská nastavení na stránce 40.
5. Klikněte na ikonu **fotoaparátu** a poté postupujte dle pokynů na obrazovce, abyste zaregistrovali scénu.

   Postupujte dle pokynů na obrazovce a při zachycování scén se nezapomeňte podívat na svůj snímek.
6. Klikněte na tlačítko **Další**.
7. Klikněte na tlačítko **Dokončit**.

Scény můžete také zaregistrovat z nástrojového panelu aplikace Security Manager:

1. Otevřete nástrojový panel aplikace Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 26.
2. V části **Má přihlášení** klikněte na položky **Credential Manager** a **Tvář**.
3. Klikněte na možnost **Upřesnit** a poté nakonfigurujte další zabezpečení. Další informace naleznete v části Pokročilá uživatelská nastavení na stránce 40.
4. Klikněte na tlačítko **OK**.

5. Klikněte na možnost **Spustit**. Pokud jste již dříve scény registrovali, klikněte na možnost **Zaregistrovat novou scénu**.

6. Pokud jste nevybrali žádné další možnosti zabezpečení, budete vyzváni k výběru možnosti dodatečného zabezpečení. Postupujte podle pokynů na obrazovce a poté klikněte na možnost **Další**. Další informace naleznete v části Pokročilá uživatelská nastavení na stránce 40.

7. Klikněte na ikonu **fotoaparátu** a poté postupujte dle pokynů na obrazovce, abyste zaregistrovali scénu.

   Postupujte dle pokynů na obrazovce a při zachycování scén se nezapomeňte podívat na svůj snímek.

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

Pokročilá uživatelská nastavení

Pokud nebylo vybráno žádné další zabezpečení, jsou tyto možnosti zobrazeny také na stránce Dodatečné zabezpečení.

1. Otevřete nástrojový panel aplikace Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 26.

2. V části **Má přihlášení** klikněte na položky **Credential Manager** a **Tvář**.

3. Kliknutím na možnost **Upřesnit** můžete nakonfigurovat následující možnosti zabezpečení:

   a. Karta **Zabezpečení** — Vyberte jednu z následujících možností:

   - **Žádné další zabezpečení** — Tuto možnost vyberte, pokud pro přihlašování pomocí tváře nevyžadujete žádné další zabezpečení.
   - **Použít kód PIN pro další zabezpečení** — Pokud vyberete tuto možnost, bude při přihlašování pomocí tváře vyžadováno zadání uživatelského kódu PIN.
     - Klikněte na možnost **Vytvořit kód PIN**.
     - Zadejte heslo pro systém Windows.
     - Zadejte nový kód PIN a poté jej potvrďte opětovným zadáním.

       Po vytvoření kódu PIN si můžete vybrat z následujících možností: **Změnit**, **Resetovat** nebo **Odebrat kód PIN**.
   - **Použít rozhraní Bluetooth pro další zabezpečení** — Vyberte tuto možnost, abyste spárovali telefon podporující technologii Bluetooth s aplikací Face Recognition. Při přihlašování k systému Windows provede aplikace Face Recognition po ověření tváře také kontrolu přítomnosti spárovaného telefonu s rozhraním Bluetooth. Pokud je

telefon přítomen (a má zapnuté rozhraní Bluetooth), bude vám umožněno se přihlásit k systému Windows.

- Ujistěte se, že je rozhraní Bluetooth povoleno v počítači i v telefonu.

  Pokud telefon s rozhraním Bluetooth není přítomen, budete vyzváni k povolení rozhraní Bluetooth ve spárovaném telefonu a k restartu procesu přihlašování. Po uplynutí 30 sekund se činnost přihlašovacího okna aplikace Face Recognition pozastaví. Chcete-li proces přihlašování zahájit, klikněte na ikonu **fotoaparátu**. Pokud telefon s rozhraním Bluetooth není přítomen, můžete použít k přihlášení normální heslo systému Windows.

- Klikněte na tlačítko **Přidat**.

- Pokud je zařízení Bluetooth zobrazeno, vyberte je a klikněte na možnost **Další**.

Klikněte na tlačítko **OK**.

b. 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 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.

Klikněte na tlačítko **OK**.

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.

Můžete změnit obrázek a také způsob zobrazení jména. Ve výchozím nastavení se zobrazí vaše plné uživatelské jméno systému Windows a obrázek, který jste vybrali při instalaci systému Windows.

Chcete-li změnit zobrazované jméno, postupujte takto:

1. Otevřete nástrojový panel aplikace Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 26.
2. Klikněte na tlačítko Office v levém horním rohu obrazovky.
3. Klikněte na pole uvádějící uživatelské jméno daného účtu v systému Windows, zadejte nové jméno a klikněte na možnost **Uložit**.

Chcete-li změnit zobrazovaný obrázek, postupujte takto:

1. Otevřete nástrojový panel aplikace Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 26.
2. Klikněte na tlačítko Office v levém horním rohu obrazovky.
3. Klikněte na tlačítko **Vybrat obrázek**, vyberte obrázek a poté klikněte na tlačítko **Uložit**.

Nastavení předvoleb

Je možné upravit nastavení nástroje HP ProtectTools Security Manager. Na nástrojovém panelu nástroje Security Manager klikněte na položku **Upřesnit** a pak klikněte 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 přehrány různé zvuky. Nové zvuky lze těmto událostem rovněž přiřadit pomocí karty **Zvuky** 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 otisky bez ohledu na kvalitu, zaškrtněte toto políčko.

    Chcete-li zobrazit pouze kvalitní naskenované otisky, 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: Prostřednictvím této funkce jsou zálohována pouze data.

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 nástrojový panel aplikace Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 26.
2. V levé části nástrojového panelu 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 nástrojový panel aplikace Security Manager. Další informace naleznete v části Spuštění nástroje Security Manager na stránce 26.
2. V levé části nástrojového panelu 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**.

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

Nástroj Drive Encryption for HP ProtectTools poskytuje prostřednictvím šifrování pevného disku kompletní ochranu dat. Je-li nástroj Drive Encryption aktivován, je třeba se přihlásit na přihlašovací obrazovce nástroje Drive Encryption, která se zobrazí před spuštěním operačního systému Windows®.

Průvodce nastavením nástroje HP ProtectTools Security Manager umožňuje správcům systému Windows aktivovat nástroj Drive Encryption, zálohovat šifrovací klíč nebo přidat či odebrat jednotky. Další informace naleznete v softwarové nápovědě k aplikaci HP ProtectTools Security Manager.

Aplikace Drive Encryption umožňuje provádět následující úlohy:

- Úprava nastavení nástroje Drive Encryption:
  - Aktivace hesla chráněného modulem TPM
  - Šifrování nebo dešifrování jednotlivých jednotek nebo oddílů pomocí softwarového šifrování
  - Šifrování nebo dešifrování jednotlivých jednotek s automatickým šifrováním pomocí hardwarového šifrování
  - Posílení zabezpečení deaktivací úsporného režimu/režimu spánku, díky čemuž bude ověřování před spuštěním v rámci nástroje Drive Encryption vždy vyžadováno

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

- Vytvoření záložních klíčů
- Obnovení klíče nástroje Drive Encryption
- Povolení ověřování před spuštěním v rámci nástroje Drive Encryption pomocí hesla, registrovaného otisku prstu nebo kódu PIN čipové karty

Spuštění aplikace Drive Encryption

Správci mohou nástroj Drive Encryption spustit prostřednictvím Konzoly pro správu nástroje HP ProtectTools.

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně klepněte na položku **Drive Encryption**.

Všeobecné úlohy

Aktivace nástroje Drive Encryption u standardních pevných disků

Standardní pevné disky jsou šifrovány prostřednictvím softwarového šifrování. Nástroj Drive Encryption aktivujete pomocí následujícího postupu:

1. K aktivaci nástroje Drive Encryption použijte Průvodce nastavením aplikace HP ProtectTools Security Manager.
2. Postupujte podle pokynů na obrazovce, dokud se nezobrazí stránka **Povolit funkce zabezpečení**. Následně postupujte podle kroku 4 uvedeného níže.

nebo

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. Kliknutím na ikonu **+** v levém podokně nalevo od položky **Zabezpečení** zobrazíte dostupné možnosti.
3. Klikněte na možnost **Funkce**.
4. Zaškrtněte políčko **Drive Encryption** a pak klepněte na tlačítko **Další**.

POZNÁMKA: Pokud nebyla vybrána žádná jednotka coby cíl šifrování, ověřování před spuštěním pomocí nástroje Drive Encryption bude povoleno, ale žádné jednotky nebudou zašifrovány.

5. V části **Jednotky, které mají být zašifrovány** zaškrtněte políčko u pevného disku, který chcete šifrovat, a klikněte na tlačítko **Další**.
6. Chcete-li šifrovací klíč zálohovat, vložte do vhodné zásuvky úložné zařízení.

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

7. V části **Zálohování klíče nástroje Drive Encryption** zaškrtněte políčko u paměťového zařízení, na kterém má být šifrovací klíč uložen.
8. Klikněte na tlačítko **Další**.

POZNÁMKA: Počítač se restartuje.

Nástroj Drive Encryption byl aktivován. Zašifrování jednotky může v závislosti na její velikosti trvat až několik hodin.

Další informace naleznete v softwarové nápovědě k aplikaci HP ProtectTools Security Manager.

Aktivace nástroje Drive Encryption u jednotek s automatickým šifrováním

Jednotky s automatickým šifrováním splňující normy OPAL organizace Trusted Computing Group pro správu jednotek s automatickým šifrováním je možné šifrovat softwarově nebo hardwarově. Pomocí následujících kroků můžete aktivovat nástroj Drive Encryption u jednotek s automatickým šifrováním:

1. K aktivaci nástroje Drive Encryption použijte Průvodce nastavením aplikace HP ProtectTools Security Manager.
2. Postupujte podle pokynů na obrazovce, dokud se nezobrazí stránka **Povolit funkce zabezpečení**. Následně postupujte podle kroku 4 uvedeného v části „Softwarové šifrování“ nebo „Hardwarové šifrování“ níže.

POZNÁMKA: Pokud váš počítač není vybaven jednotkou s automatickým šifrováním splňující normy OPAL organizace Trusted Computing Group pro správu jednotek s automatickým šifrováním, hardwarové šifrování není k dispozici a je třeba použít šifrování softwarové.

Pokud je váš počítač vybaven kombinací jednotek s automatickým šifrováním a standardních pevných disků, hardwarové šifrování není k dispozici a je třeba použít šifrování softwarové.

nebo

Softwarové šifrování

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. Kliknutím na ikonu **+** v levém podokně nalevo od položky **Zabezpečení** zobrazíte dostupné možnosti.
3. Klikněte na možnost **Funkce**.
4. Zaškrtněte políčko **Drive Encryption** a pak klepněte na tlačítko **Další**.
5. V části **Jednotky, které mají být zašifrovány** zaškrtněte políčko u pevného disku, který chcete šifrovat, a klikněte na tlačítko **Další**.
6. Chcete-li šifrovací klíč zálohovat, vložte do vhodné zásuvky úložné zařízení.

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

7. V části **Zálohování klíče nástroje Drive Encryption** zaškrtněte políčko u paměťového zařízení, na kterém má být šifrovací klíč uložen.
8. Klikněte na tlačítko **Použít**.

POZNÁMKA: Počítač se restartuje.

Nástroj Drive Encryption byl aktivován. Zašifrování jednotky může v závislosti na její velikosti trvat až několik hodin.

Hardwarové šifrování

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. Kliknutím na ikonu **+** v levém podokně nalevo od položky **Zabezpečení** zobrazíte dostupné možnosti.
3. Klikněte na možnost **Funkce**.
4. Zaškrtněte políčko **Drive Encryption** a pak klepněte na tlačítko **Další**.

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

Pokud je v seznamu uvedeno jednotek více, pole pro výběr jednotky jsou automaticky zaškrtnuta, ale nebudou dostupná.

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

5. Ujistěte se, že je zaškrtnuto pole **Použít hardwarové šifrování** ve spodní části obrazovky.
6. V části **Jednotky, které mají být zašifrovány** zaškrtněte políčko u pevného disku, který chcete šifrovat, a klikněte na tlačítko **Další**.
7. Chcete-li šifrovací klíč zálohovat, vložte do vhodné zásuvky úložné zařízení.

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

8. V části **Zálohování klíče nástroje Drive Encryption** zaškrtněte políčko u paměťového zařízení, na kterém má být šifrovací klíč uložen.
9. Klikněte na tlačítko **Použít**.

POZNÁMKA: Počítač je třeba restartovat.

Nástroj Drive Encryption byl aktivován. Zašifrování jednotky může trvat několik minut.

Další informace naleznete v softwarové nápovědě k aplikaci HP ProtectTools Security Manager.

Deaktivace aplikace Drive Encryption

Správci mohou k deaktivaci aplikace Drive Encryption použít Průvodce nastavením nástroje HP ProtectTools Security Manager. Další informace naleznete v softwarové nápovědě k aplikaci HP ProtectTools Security Manager.

▲ Postupujte podle pokynů na obrazovce, dokud se nezobrazí stránka **Povolit funkce zabezpečení**. Následně postupujte podle kroku 4 uvedeného níže.

– nebo –

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. Kliknutím na ikonu **+** v levém podokně nalevo od položky **Zabezpečení** zobrazíte dostupné možnosti.

3. Klikněte na možnost **Funkce**.

4. Zrušte zaškrtnutí políčka **Drive Encryption** a poté klikněte na tlačítko **Další**.

   Bude zahájena deaktivace nástroje Drive Encryption.

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

   Bylo-li použito hardwarové šifrování, jednotka bude okamžitě dešifrována (tento proces může trvat několik minut) a nástroj Drive Encryption bude deaktivován.

   Po deaktivaci šifrování jednotky je třeba počítač restartovat.

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: V případě hardwarového šifrování se ujistěte, že je počítač vypnutý. Pokud počítač nebude vypnut a následně restartován, obrazovka ověřování před spuštěním v rámci nástroje Drive Encryption se nezobrazí.

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 (pokud není deaktivováno) nezobrazí.

Při přechodu do běžného provozu z režimu hibernace se obrazovka pro ověřování po spuštění v rámci nástroje Drive Encryption zobrazí.

POZNÁMKA: Pokud správce systému Windows aktivoval funkci Zabezpečení před spuštěním nástroje HP ProtectTools Security Manager, můžete se po zapnutí počítače okamžitě přihlašovat k počítači a přihlašovací obrazovka nástroje Drive Encryption se nezobrazí.

1. Klikněte na své uživatelské jméno a poté zadejte heslo systému Windows nebo kód PIN čipové karty, nebo přiložte zaregistrovaný prst.

   POZNÁMKA: Podporovány jsou následující čipové karty:

Čipové karty

- Čipová karta ActivIdentity 64K V2C
- ActivIdentity SIM 48010-B DEC06
- USB zařízení ActivIdentity V3.0 ZFG-48001-A

Čtečky PCMCIA

- Interní čtečka karet Express Card 54 SCR3340
- SCR 201
- SCR 243 (také výrobky HP)
- ActivCard

- Omnikey 4040
- Cisco

Čtečky USB

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- Terminál čtečky karet Smart Card

2. Klepněte na tlačítko **OK**.

POZNÁMKA: Použijete-li k přihlášení na přihlašovací obrazovce Drive Encryption klíč obnovy, budete vyzváni k ověření na přihlašovací obrazovce systému Windows pomocí hesla, kódu PIN čipové karty nebo registrovaným prstem.

Ochrana dat zašifrováním pevného disku

Důrazně doporučujeme k ochraně dat pomocí šifrování pevného disku používat Průvodce nastavením nástroje HP ProtectTools Security Manager:

1. Kliknutím na ikonu **+** v levém podokně nalevo od položky **Drive Encryption** zobrazíte dostupné možnosti.
2. Klikněte na tlačítko **Nastavení**.
3. V případě softwarově šifrovaných jednotek vyberte ty oddíly jednotky, které mají být zašifrovány.

POZNÁMKA: Tento krok je platný také v případě kombinace jednoho či více standardních pevných disků a jedné či více jednotek s automatickým šifrováním.

nebo

▲ V případě hardwarově šifrovaných jednotek vyberte jednotky, které mají být zašifrovány. Je třeba vybrat alespoň jednu jednotku.

Zobrazení stavu šifrování

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

POZNÁMKA: Správci mohou ke změně stavu nástroje Drive Encryption použít nástroj Konzola pro správu nástroje HP ProtectTools.

1. Otevřete nástroj HP ProtectTools Security Manager.
2. V části **Moje data** klikněte na položku **Drive Encryption**.

V případě softwarového šifrování se v části **Stav jednotky** zobrazí jeden z následujících stavových kódů:

- Povoleno
- Zakázáno
- Nešifrováno
- Šifrováno
- Šifrování
- Dešifrování

V případě hardwarového šifrování se v části **Stav jednotky** zobrazí následující stavový kód:

- Šifrováno

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

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, neaktivní nebo aktivace hardwarového šifrování) a prohlížet stav šifrování všech pevných disků v počítači.

POZNÁMKA: Hardwarové šifrování nelze na stránce Nastavení měnit.

- Je-li nastaven stav Zakázáno, nástroj Drive Encryption dosud nebyl správcem systému Windows aktivován a pevný disk není chráněn. K aktivaci nástroje Drive Encryption použijte Průvodce nastavením aplikace HP ProtectTools Security Manager.
- Je-li nastaven stav Povoleno, nástroj Drive Encryption byl aktivován a konfigurován. Jednotka je v některém z následujících stavů:

Softwarové šifrování

- Nešifrováno
- Šifrováno
- Šifrování
- Dešifrování

Hardwarové šifrování

- Šifrováno

Šifrování nebo dešifrování jednotlivých jednotek (pouze pomocí softwarového šifrování)

Správci mohou v rámci stránky Nastavení zašifrovat jeden nebo více pevných disků v počítači nebo dešifrovat jednotku, která již byla zašifrována.

1. Otevřete Konzolu pro správu nástroje HP ProtectTools.
2. Kliknutím na ikonu **+** v levém podokně nalevo od položky **Drive Encryption** zobrazíte dostupné možnosti.
3. Klikněte na tlačítko **Nastavení**.
4. V části **Stav jednotky** zaškrtněte políčka u jednotek, které chcete zašifrovat, nebo zrušte jejich zaškrtnutí u jednotek, které chcete dešifrovat, a poté klikněte na tlačítko **Použít**.

POZNÁMKA: Při šifrování nebo dešifrování jednotky se v indikátoru průběhu zobrazuje čas zbývající k dokončení procesu v rámci aktuální relace.

Pokud je počítač v průběhu šifrování vypnut nebo byl aktivován úsporný režim/režim spánku či hibernace a poté je znovu restartován, je indikátor zbývajícího času nastaven na začátek, ale vlastní šifrování bude pokračovat od místa, kde bylo zastaveno. Indikátor průběhu s hodnotami v procentech a zbývající čas se bude měnit rychleji a bude odrážet předchozí průběh.

POZNÁMKA: Dynamické oddíly nejsou podporovány. Pokud je oddíl uveden v seznamu dostupných oddílů, ale po jeho výběru nedojde k jeho zašifrování, jedná se o dynamický oddíl. Dynamický oddíl je výsledkem redukce velikosti oddílu v nástroji Správa disků za účelem vytvoření oddílu nového.

Pokud má dojít k převodu na dynamický oddíl, zobrazí se upozornění.

Záloha a obnova (úloha pro správce)

Po aktivaci nástroje Drive Encryption mohou správci použít stránku Záloha šifrovacího klíče k zálohování šifrovacích klíčů na vyjímatelná média a provedení jejich obnovení.

Zálohování šifrovacích klíčů

Správci mohou šifrovací klíč pro šifrovanou jednotku zálohovat 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 pevnému disku.

1. Otevřete Konzolu pro správu nástroje HP ProtectTools.
2. Kliknutím na ikonu **+** v levém podokně nalevo od položky **Drive Encryption** zobrazíte dostupné možnosti.
3. Klikněte na možnost **Zálohování šifrovacího klíče**.
4. Vložte úložné zařízení použité k zálohování šifrovacího klíče.
5. V části **Jednotka** zaškrtněte políčko u paměťového zařízení, na kterém má být šifrovací klíč uložen.
6. Klepněte na položku **Záložní klíče**.
7. Přečtěte si informace na zobrazené stránce a klikněte na tlačítko **Další**. Šifrovací klíč bude uložen do vybraného paměťového zařízení.

Obnovení šifrovacích klíčů

Správci mohou šifrovací klíč obnovit z vyjímatelného paměťového zařízení, na které byl dříve uložen:

1. Zapněte počítač.
2. Vložte vyjímatelné paměťové zařízení obsahující záložní klíč.
3. Jakmile se zobrazí přihlašovací dialogové okno nástroje Drive Encryption for HP ProtectTools, klikněte na tlačítko **Možnosti**.
4. Klikněte na možnost **Obnova**.
5. Vyberte soubor obsahující záložní klíč nebo klepněte na tlačítko **Procházet** a vyhledejte jej a poté klepněte na tlačítko **Další**.
6. Jakmile se zobrazí dialogové okno s potvrzením, klepněte na tlačítko **OK**.

   Počítač se spustí.

POZNÁMKA: Důrazně doporučujeme, abyste po provedení obnovy resetovali heslo.

6 Privacy Manager (Správce utajení) pro HP ProtectTools (jen vybrané modely)

Nástroj Privacy Manager for HP ProtectTools poskytuje pokročilé bezpečnostní postupy při přihlašování, které ověřují zdroj, integritu a zabezpečení komunikace při přijímání a odesílání pošty nebo otevírání dokumentů Microsoft® Office.

Nástroj Privacy Manager využívá strukturu zabezpečení aplikace HP ProtectTools Security Manager, která zahrnuje následující způsoby zabezpečeného přihlašování:

- ověřování otiskem prstu,
- heslo pro systém Windows®,
- Čipová karta
- Face Recognition

V nástroji Privacy Manager je možné využít jakýkoli výše zmíněný způsob zabezpečeného přihlašování.

Spuštění nástroje Privacy Manager

Spustit nástroj Privacy Manager lze následujícím způsobem:

- Chcete-li použít funkce specifické pro aplikaci Microsoft Outlook, klikněte na možnost **Bezpečně odeslat** ve skupině **Soukromí** na kartě **Zpráva**.
- Chcete-li využít většinu funkcí v dokumentech sady Microsoft Office, klikněte na tlačítko **Podepsat a šifrovat** ve skupině **Soukromí** na kartě **Domů**.
- Další funkce získáte na nástrojovém panelu aplikace HP ProtectTools Security Manager.
  - Klikněte na nabídku **Start**, **Všechny programy**, **HP**, **HP ProtectTools Security Manager** a **Privacy Manager**.

    nebo

  - Klikněte na ikonu miniaplikace **HP ProtectTools** na ploše.

    nebo

  - Klikněte pravým tlačítkem na ikonu **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu, klikněte na položku **Privacy Manager** a pak klikněte na položku **Konfigurace**.

Instalační postupy

Správa certifikátů Privacy Manager

Certifikáty nástroje Privacy Manager využívají pro ochranu dat a zpráv šifrovací technologii zvanou struktura veřejného klíče (PKI). Technologie PKI vyžaduje po uživateli šifrovací klíč a certifikát nástroje Privacy Manager vydaný odpovídající společností (CA). Na rozdíl od většiny softwaru pro šifrování a ověřování totožnosti, který vyžaduje pouze pravidelné ověřování, nástroj Privacy Manager vyžaduje po uživateli ověření při každém užití šifrovacího klíče k podepsání e-mailové zprávy či dokumentu Microsoft Office. Ukládání a odesílání důležitých informací je s použitím nástroje Privacy Manager naprosto bezpečné.

Správce certifikátů umožňuje provádět následující úlohy:

Zažádání o certifikát nástroje Privacy Manager

Před získáním přístupu k funkcím nástroje Privacy Manager je nutné zažádat a nainstalovat certifikát nástroje Privacy Manager (začleněná funkce) použitím platné e-mailové adresy. Je zapotřebí, aby byla uvedena stejná e-mailová adresa, která byla na daném počítači použita při vytváření účtu v aplikaci Microsoft Outlook.

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Certifikáty**.
2. Klikněte na tlačítko **Zažádat o certifikát nástroje Privacy Manager**.
3. Přečtěte si text úvodní stránky a poté klikněte na tlačítko **Další**.
4. Na stránce Licenční smlouva si pročtěte licenční smlouvu.
5. Ujistěte se, že jste zaškrtli pole vedle položky **Souhlasím s podmínkami uvedenými v licenční smlouvě**, a klepněte na tlačítko **Další**.
6. Na stránce Podrobnosti o certifikátu zadejte požadované informace a klikněte na tlačítko **Další**.
7. Na stránce Žádost o certifikát přijata klikněte na tlačítko **Dokončit**.

V aplikaci Microsoft Outlook obdržíte e-mail s připojeným certifikátem nástroje Privacy Manager.

Získání předem přiděleného podnikového certifikátu nástroje Privacy Manager

1. V aplikaci Outlook otevřete e-mailovou zprávu informující o tom, že vám byl předem přidělen podnikový certifikát.
2. Klepněte na položku **Získat**.

V aplikaci Microsoft Outlook obdržíte e-mail s připojeným certifikátem nástroje Privacy Manager.

Informace o instalaci tohoto certifikátu naleznete v části Nastavení certifikátu pro nástroj Privacy Manager na stránce 59.

Nastavení certifikátu pro nástroj Privacy Manager

1. Jakmile obdržíte e-mailovou zprávu s připojeným certifikátem nástroje Privacy Manager, otevřete ji a poté klikněte na tlačítko **Nastavení** v pravém dolním rohu zprávy (Outlook 2007 nebo Outlook 2010) nebo v levém horním rohu zprávy (Outlook 2003).
2. Pomocí zvolené metody bezpečného přihlášení proveďte ověření.
3. Na stránce Certifikát nainstalován klikněte na tlačítko **Další**.
4. Na stránce Zálohování certifikátu zadejte umístění a název souboru zálohy, nebo klikněte na tlačítko **Procházet** a vyhledejte požadované umístění.

   UPOZORNĚNÍ: Soubor se zálohou je vhodné uložit jinam než na pevný disk a uschovat na bezpečném místě. K tomuto souboru, který je potřebný k obnově certifikátu nástroje Privacy Manager a přidružených klíčů, by nikdo neměl mít přístup.
5. Zadejte a potvrďte heslo a pak klepněte na tlačítko **Další**.
6. Pomocí zvolené metody bezpečného přihlášení proveďte ověření.
7. Chcete-li zahájit proces pozvánky do důvěryhodných kontaktů, pokračujte podle pokynů na obrazovce počínaje krokem 2 tématu Přidání důvěryhodných kontaktů pomocí kontaktů aplikace Microsoft Outlook na stránce 63.

   nebo

   Klepnete-li na tlačítko **Storno**, naleznete potřebné informace o přidávání důvěryhodných kontaktů později v části Správce důvěryhodných kontaktů na stránce 62.

Import certifikátů vydaných třetí stranou

Certifikát vydaný třetí stranou lze importovat do aplikace Privacy Manager prostřednictvím Průvodce importem certifikátu.

Chcete-li tuto funkci použít, v Konzole pro správu aplikace HP ProtectTools musí být na stránce Nastavení v nástroji **Privacy Manager** povolena možnost **Povolit užití certifikátů vydaných třetí stranou**.

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Certifikáty**.
2. Vyberte kartu **Správce certifikátů** a poté klikněte na možnost **Importovat certifikáty**.

   Toto tlačítko se nezobrazuje, pokud není import certifikátů povolen.

3. Vyberte, zda chcete importovat certifikát, který je již v tomto počítači nainstalován, nebo certifikát uložený jako soubor PFX (Personal Information Exchange/PKCS#12) a poté klikněte na možnost **Další**.

   - Chcete-li importovat certifikát, který je nainstalován v tomto počítači, vyberte jej a poté klikněte na možnost **Další**.
   - Chcete-li vybrat certifikát PFX, klikněte na tlačítko **Procházet**, vyhledejte umístění souboru PFX a poté klikněte na tlačítko **Další**. Zadejte heslo souboru PFX a poté klikněte na tlačítko **Další**.

4. Po dokončení importu klikněte na možnost **Další**.
5. Budete mít k dispozici možnost zálohovat importovaný certifikát.

   Doporučujeme certifikát zálohovat na jiném místě, než je pevný disk počítače.

Zobrazení podrobností o certifikátu nástroje Privacy Manager

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Certifikáty**.
2. Klikněte na tlačítko Certifikát nástroje Privacy Manager.
3. Klikněte na položku **Podrobnosti o certifikátu**.
4. Po prohlédnutí podrobností klikněte na tlačítko **OK**.

Prodloužení platnosti certifikátu nástroje Privacy Manager

Když se přiblíží termín vypršení platnosti certifikátu, budete upozorněni na nutnost jeho prodloužení:

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Certifikáty**.
2. Klikněte na položku **Obnovit certifikát**.
3. Podle pokynů na obrazovce získejte nový certifikát pro nástroj Privacy Manager.

POZNÁMKA: Nově zakoupený certifikát nenahrazuje certifikát původní. K získání a instalaci certifikátu nástroje Privacy Manager je třeba podstoupit stejné kroky jako v části Zažádání o certifikát nástroje Privacy Manager na stránce 58.

V případě podnikových certifikátů vydaných vaší společností prostřednictvím cerfitikační autority společnosti Microsoft musí správce CA obnovit certifikát pomocí stejného soukromého klíče jako předchozí certifikát nebo musí pomocí toho klíče vydat nový certifikát.

Nastavení výchozího certifikátu pro nástroj Privacy Manager

Nástroj Privacy Manager zobrazuje pouze certifikáty pro něj určené a to i v případě, že jsou v počítači nainstalovány certifikáty od jiných společností.

Pokud jste vlastníkem více než jednoho certifikátu pro nástroj Privacy Manager, který je v počítači nainstalován, je možné určit, který certifikát bude používán jako výchozí:

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Certifikáty**.
2. Klikněte na certifikát nástroje Privacy Manager, který má být označen jako výchozí, a klikněte na tlačítko **Nastavit jako výchozí**.
3. Klikněte na tlačítko **OK**.

POZNÁMKA: Zároveň však lze používat i ostatní certifikáty nástroje Privacy Manager. Použitím různých funkcí nástroje Privacy Manager je možné vybrat a použít kterýkoli jiný certifikát.

Odstranění certifikátu nástroje Privacy Manager

Po odstranění certifikátu nástroje Privacy Manager nebude možné otevřít žádný soubor či používat data, která byla tímto certifikátem šifrována. Pokud byl certifikát pro nástroj Privacy Manager omylem smazán, lze jej obnovit za pomoci zálohovacího souboru vytvořeného během instalace certifikátu. Další informace naleznete na stránce Obnovení certifikátu nástroje Privacy Manager na stránce 61.

Odstranit certifikát nástroje nástroj Privacy Manager lze následujícím způsobem:

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Certifikáty**.
2. Klikněte na certifikát nástroje Privacy Manager, který má být odstraněn, a klikněte na tlačítko **Upřesnit**.
3. Klikněte na tlačítko **Odstranit**.
4. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.
5. Klikněte na tlačítko **Zavřít** a poté na tlačítko **Použít**.

Obnovení certifikátu nástroje Privacy Manager

V průběhu instalace certifikátu nástroje Privacy Manager je třeba vytvořit záložní kopii tohoto certifikátu. K vytvoření záložní kopie můžete rovněž použít stránku Migrace. Tuto záložní kopii lze využít při migraci do jiného počítače nebo k obnově certifikátu v původním počítači.

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Migrace**.
2. Klikněte na tlačítko **Obnovit**.
3. Na stránce Migrační soubor klikněte na tlačítko **Procházet** a vyhledejte soubor s příponou .dppsm, který byl vytvořen během procesu zálohování, a poté klikněte na tlačítko **Další**.
4. Zadejte heslo použité při vytvoření zálohy a pak klikněte na tlačítko **Další**.
5. Klikněte na tlačítko **Dokončit**.

Další informace naleznete v části Nastavení certifikátu pro nástroj Privacy Manager na stránce 59 nebo Zálohování certifikátů Privacy Manager a důvěryhodných kontaktů na stránce 71.

Stornování certifikátu nástroje Privacy Manager

Pokud máte pocit, že bezpečnost vašeho certifikátu nástroje Privacy Manager byla ohrožena, lze tento certifikát stornovat následujícím způsobem:

POZNÁMKA: Stornovaný certifikát není úplně odstraněn. Nadále jej lze používat k prohlížení souborů, které byly jeho pomocí zašifrovány.

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Certifikáty**.
2. Klikněte na tlačítko **Upřesnit**.
3. Klikněte na certifikát nástroje Privacy Manager, který má být stornován, a poté klikněte na tlačítko **Stornovat**.

4. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.
5. Pomocí zvolené metody bezpečného přihlášení proveďte ověření.
6. Řiďte se instrukcemi na obrazovce.

Správce důvěryhodných kontaktů

Důvěryhodné kontakty jsou seznam uživatelů, se kterými sdílíte certifikát nástroje Privacy Manager, což oběma stranám umožňuje zabezpečenou komunikaci.

Správce důvěryhodných kontaktů umožňuje provádět následující úlohy:

- zobrazit podrobnosti u důvěryhodných kontaktů,
- odstranit důvěryhodné kontakty,
- zkontrolovat, zda certifikát nebyl stornován (pokročilé nastavení).

Přidání důvěryhodných kontaktů

Postup přidání důvěryhodných kontaktů lze rozdělit na 3 kroky:

1. Zaslání pozvánky e-mailem budoucímu důvěryhodnému kontaktu.
2. Příjemce vám odpoví na e-mail.
3. Po přijetí odpovědi od příjemce důvěryhodného kontaktu klikněte na tlačítko **Přijmout**.

E-mailovou pozvánku do důvěryhodných kontaktů lze zaslat jednotlivým osobám nebo všem kontaktům v adresáři aplikace Microsoft Outlook.

Více informací naleznete v odpovídajících oddílech.

POZNÁMKA: Odpovědět na pozvánku do důvěryhodných kontaktů je možné, pouze pokud má příjemce nainstalován nástroj Privacy Manager či jiný vhodný software pro šifrování. Více informací o vhodném softwaru naleznete na webové stránce společnosti DigitalPersona http://digitalpersona.com/privacymanager/download.

Přidání důvěryhodného kontaktu

1. Otevřete nástroj Privacy Manager a klikněte na položku **Správce důvěryhodných kontaktů** a poté na tlačítko **Pozvat kontakt**.

   – nebo –

   V panelu nástrojů v aplikaci Microsoft Outlook rozviňte nabídku kliknutím na šipku vedle položky **Šifrovat** a poté klikněte na tlačítko **Pozvat kontakt**.
2. Pokud se otevře dialogové okno „Vyberte certifikát“, zvolte certifikát nástroje Privacy Manager, který chcete používat, a klikněte na tlačítko **OK**.
3. Pokud se otevře dialogové okno „Pozvat důvěryhodný kontakt“, přečtěte si text a klikněte na tlačítko **OK**.

   E-mail bude vytvořen automaticky.
4. Zadejte e-mailové adresy příjemců, které chcete přidat do důvěryhodných kontaktů.

5. Je možné upravit text zprávy a vložit podpis (nepovinné).

6. Klikněte na tlačítko **Odeslat**.

POZNÁMKA: Pokud jste nezískali certifikát nástroje Privacy Manager, zobrazí se informace, že k odeslání žádosti o přidání do důvěryhodných kontaktů je třeba mít tento certifikát k dispozici. Průvodce žádostí o certifikát spustíte kliknutím na tlačítko **OK**. Další informace naleznete na stránce Zažádání o certifikát nástroje Privacy Manager na stránce 58.

7. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.

POZNÁMKA: Jakmile příjemce důvěryhodného kontaktu obdrží tento e-mail, musí jej otevřít a kliknout na tlačítko **Přijmout** v pravém spodním rohu. V potvrzovacím dialogovém okně pak musí kliknout na tlačítko **OK**.

8. Po obdržení e-mailu s odpovědí od příjemce pozvánky do důvěryhodných kontaktů klikněte na tlačítko v pravém spodním rohu zprávy **Přijmout**.

   Objeví se dialogové okno potvrzující úspěšné přidání osoby do seznamu důvěryhodných kontaktů.

9. Klikněte na tlačítko **OK**.

Přidání důvěryhodných kontaktů pomocí kontaktů aplikace Microsoft Outlook

1. Otevřete nástroj Privacy Manager a klikněte na položku **Správce důvěryhodných kontaktů** a poté na tlačítko **Pozvat kontakty**.

   – nebo –

   Na panelu nástrojů aplikace Microsoft Outlook klikněte na šipku vedle položky **Bezpečně odeslat** a poté klikněte na tlačítko **Pozvat mé kontakty aplikace Outlook**.

2. Jakmile se otevře stránka Pozvánka do důvěryhodných kontaktů, zadejte e-mailové adresy všech osob, které chcete přidat jako důvěryhodné kontakty, a klikněte na tlačítko **Další**.

3. Na stránce Odesílání pozvání klikněte na tlačítko **Dokončit**.

   Automaticky se vytvoří e-mail se seznamem vybraných e-mailových adres aplikace Microsoft Outlook.

4. Je možné upravit text zprávy a vložit podpis (nepovinné).

5. Klikněte na tlačítko **Odeslat**.

POZNÁMKA: Pokud jste nezískali certifikát nástroje Privacy Manager, zobrazí se informace, že k odeslání žádosti o přidání do důvěryhodných kontaktů je třeba mít tento certifikát k dispozici. Průvodce žádostí o certifikát spustíte kliknutím na tlačítko **OK**. Další informace naleznete na stránce Zažádání o certifikát nástroje Privacy Manager na stránce 58.

6. Pomocí zvolené metody bezpečného přihlášení proveďte ověření.

POZNÁMKA: Jakmile příjemce důvěryhodného kontaktu obdrží tento e-mail, musí jej otevřít a kliknout na tlačítko **Přijmout** v pravém spodním rohu. V potvrzovacím dialogovém okně pak musí kliknout na tlačítko **OK**.

7. Po obdržení e-mailu s odpovědí od příjemce pozvánky do důvěryhodných kontaktů klikněte na tlačítko **Přijmout** v pravém dolním rohu.

Zobrazí se dialogové okno potvrzující úspěšné přidání příjemce do seznamu důvěryhodných kontaktů.

8. Klikněte na tlačítko **OK**.

Zobrazení podrobností o důvěryhodných kontaktech

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Důvěryhodné kontakty**.
2. Klikněte na položku Důvěryhodné kontakty.
3. Klikněte na tlačítko **Podrobnosti o kontaktech**.
4. Po prohlédnutí podrobností klikněte na tlačítko **OK**.

Odstranění důvěryhodného kontaktu

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Důvěryhodné kontakty**.
2. Klikněte na důvěryhodný kontakt, který chcete odstranit.
3. Klikněte na tlačítko **Odstranit kontakt**.
4. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

Kontrola, zda certifikát důvěryhodného kontaktu nebyl stornován

Zkontrolovat, zda certifikát důvěryhodného kontaktu nebyl stornován, lze následujícím způsobem:

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Důvěryhodné kontakty**.
2. Klikněte na položku Důvěryhodné kontakty.
3. Klikněte na tlačítko **Upřesnit**.

   Otevře se dialogové okno s pokročilým nastavením pro důvěryhodné kontakty.
4. Klikněte na tlačítko **Ověřit stornování**.
5. Klikněte na tlačítko **Zavřít**.

Obecné úlohy

Nástroj Privacy Manager je možné používat s následujícími produkty Microsoft:

- Microsoft Outlook
- Microsoft Office

Použití modulu Privacy Manager v Microsoft Outlook

Po nainstalování nástroje Privacy Manager se zpřístupní dvě nová tlačítka: v panelu nástrojů aplikace Microsoft Outlook tlačítko Důvěrné a v panelu nástrojů e-mailové zprávy tlačítko Šifrovat. Po rozbalení nabídky kliknutím na šipku vedle tlačítka **Důvěrné** nebo **Šifrovat** si budete moci vybrat z následujících možností:

- **Podepsat a odeslat zprávu** (pouze tlačítko Bezpečně odeslat) – Tato možnost přiřadí k e-mailu digitální podpis a po ověření totožnosti vámi zvoleným způsobem zabezpečeného přihlašování ji odešle.
- **Šifrovat pro důvěryhodný kontakt a odeslat zprávu** (pouze tlačítko Bezpečně odeslat) – Tato možnost přiřadí k e-mailu digitální podpis a po ověření totožnosti vámi zvoleným způsobem zabezpečeného přihlašování jej zašifruje a odešle.
- **Pozvat kontakty** – Tato možnost je určena pro zasílání pozvánky do důvěryhodných kontaktů. Další informace naleznete na stránce Přidání důvěryhodného kontaktu na stránce 62.
- **Pozvat kontakty aplikace Outlook** – Tato možnost je určena pro zaslání pozvánky do důvěryhodných kontaktů všem osobám v adresáři aplikace Microsoft Outlook. Další informace naleznete na stránce Přidání důvěryhodných kontaktů pomocí kontaktů aplikace Microsoft Outlook na stránce 63.
- **Spustit nástroj Privacy Manager** – Možnosti Certifikáty, Důvěryhodné kontakty a Nastavení umožňují spustit nástroj Privacy Manager a využít jej pro přidání, zobrazení či úpravu aktuálního nastavení. Další informace naleznete v části Správa certifikátů Privacy Manager na stránce 58, Správce důvěryhodných kontaktů na stránce 62 nebo Nastavení nástroje Privacy Manager pro aplikaci Microsoft Outlook na stránce 65.

Nastavení nástroje Privacy Manager pro aplikaci Microsoft Outlook

1. Otevřete nástroj Privacy Manager a klikněte na položku **Nastavení** a poté na ikonu **E-mail**.

   – nebo –

   Na hlavním panelu nástrojů aplikace Microsoft Outlook klikněte na šipku vedle položky **Bezpečně odeslat** (**Osobní údaje** v aplikaci Outlook 2003) a poté klikněte na tlačítko **Nastavení**.

   – nebo –

   V panelu nástrojů e-mailové zprávy rozviňte nabídku kliknutím na šipku vedle položky **Šifrovat** a poté klikněte na tlačítko **Nastavení**.

2. Vyberte akci, která se má vykonat při odesílání zabezpečeného e-mailu, a klikněte na tlačítko **OK**.

Podepsání a odeslání e-mailové zprávy

1. V aplikaci Microsoft Outlook klikněte na tlačítko **Nová zpráva** nebo na tlačítko **Odpovědět**.
2. Napište e-mailovou zprávu.
3. Klikněte na šipku vedle položky **Bezpečně odeslat** (**Osobní údaje** v aplikaci Outlook 2003) a poté klikněte na tlačítko **Podepsat a odeslat**.
4. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.

Zapečetění a odeslání e-mailové zprávy

Zapečetěnou e-mailovou zprávu, která byla digitálně podepsána a zašifrována, mohou přečíst pouze osoby z vašeho seznamu důvěryhodných kontaktů.

Zapečetit a odeslat e-mailovou zprávu důvěryhodnému kontaktu lze následujícím způsobem:

1. V aplikaci Microsoft Outlook klikněte na tlačítko **Nová zpráva** nebo **Odpovědět**.
2. Napište e-mailovou zprávu.
3. Klikněte na šipku vedle položky **Bezpečně odeslat** (**Osobní údaje** v aplikaci Outlook 2003) a poté klikněte na tlačítko **Zapečetit pro důvěryhodné kontakty a odeslat**.
4. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.

Prohlížení zapečetěné e-mailové zprávy

Otevřená šifrovaná e-mailová zpráva obsahuje v záhlaví označení zabezpečení. Toto označení poskytuje následující informace:

- Pověření použité k určení totožnosti osoby, která podepsala e-mailovou zprávu.
- Nástroj použitý ke kontrole ověření osoby, která podepsala e-mailovou zprávu.

Použití Privacy Manager v dokumentu Microsoft Office 2007

Po nainstalování certifikátu nástroje Privacy Manager bude dostupné nové tlačítko Podepsat a zašifrovat na pravé straně panelu nástrojů v dokumentech MS Word, MS Excel a MS PowerPoint. Po rozvinutí nabídky kliknutím na šipku vedle tlačítka **Podepsat a zašifrovat** si budete moci vybrat z následujících možností:

- **Podepsat dokument** – Tato možnost připojí k dokumentu váš digitální podpis.
- **Přidat podpisovou linku před podepsáním** (pouze aplikace MS Word a MS Excel) – Podle výchozího nastavení je linka pro podpis přidána až po podepsání a zašifrování dokumentu MS Word či MS Excel. Nastavení lze změnit kliknutím na tlačítko **Přidat podpisovou linku** a odškrtnutím pole.
- **Zašifrovat dokument** – Tato možnost připojí k dokumentu váš digitální podpis a šifrování.
- **Odstranit šifrování** – Tato možnost odstraní šifrování z dokumentu.
- **Spustit nástroj Privacy Manager** – Možnosti Certifikáty, Důvěryhodné kontakty a Nastavení umožňují spustit nástroj Privacy Manager a využít jej pro přidání, zobrazení či úpravu aktuálního nastavení. Další informace naleznete v části Správa certifikátů Privacy Manager na stránce 58, Správce důvěryhodných kontaktů na stránce 62 nebo Nastavení nástroje Privacy Manager pro aplikaci Microsoft Office na stránce 67.

Nastavení nástroje Privacy Manager pro aplikaci Microsoft Office

1. Otevřete nástroj Privacy Manager a klikněte na položku **Nastavení** a poté na ikonu **Dokumenty**.

   – nebo –

   V panelu nástrojů dokumentu Microsoft Office rozviňte nabídku kliknutím na šipku vedle položky **Podepsat a šifrovat** a poté klikněte na tlačítko **Nastavení**.

2. Vyberte akci, kterou chcete upravit, a klikněte na tlačítko **OK**.

Podepsání dokumentu Microsoft Office

1. Vytvořte a uložte dokument v aplikaci MS Word, MS Excel či MS PowerPoint.
2. Rozviňte nabídku kliknutím na šipku vedle položky **Podepsat a šifrovat** a poté klikněte na tlačítko **Podepsat dokument**.
3. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.
4. V otevřeném dialogovém okně si přečtěte text a klikněte na tlačítko **OK**.

V případě pozdější úpravy dokumentu je třeba dodržet následující kroky:

1. Klikněte na tlačítko **Office** v levém horním rohu obrazovky.
2. Klikněte na tlačítko **Připravit** a poté na tlačítko **Označit jako finální**.
3. V otevřeném dialogovém okně klikněte na tlačítko **Ano** a pokračujte v práci.
4. Po dokončení úprav opět podepište dokument.

Přidání podpisové linky při podepisování dokumentu MS Word nebo MS Excel

Nástroj Privacy Manager umožňuje přidání podpisové linky při podepisování dokumentu MS Word nebo MS Excel:

1. Vytvořte a uložte dokument v aplikaci MS Word nebo MS Excel.
2. Klikněte na nabídku **Domů**.
3. Rozviňte nabídku kliknutím na šipku vedle položky **Podepsat a šifrovat** a poté klikněte na tlačítko **Přidat podpisovou linku před podepsáním**.

   POZNÁMKA: Políčko vedle položky Přidání podpisové linky před podepsáním bude nyní zaškrtnuté. Při výchozím nastavení je tato možnost již aktivována.

4. Rozviňte nabídku kliknutím na šipku vedle položky **Podepsat a šifrovat** a poté klikněte na tlačítko **Podepsat dokument**.
5. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.

Přidání podpisové linky pro další signatáře v dokumentu MS Word nebo MS Excel

Je možné v dokumentu přidat více než jednu podpisovou linku určením dalších signatářů. Takový signatář je uživatel určený majitelem dokumentu MS Word nebo MS Excel, po kterém je vyžadováno dokument podepsat. Může se jednat o vás či jakoukoli jinou osobu, která má dokument podepsat. Pokud je například připravován dokument, který má být podepsán všemi členy vašeho oddělení, je

možné pro tyto uživatele na konec finálního dokumentu vložit podpisové linky s instrukcemi stanovujícími datum podpisu.

Přidat podpisovou linku pro dalšího signatáře v dokumentu MS Word nebo MS Excel lze následujícím způsobem:

1. Vytvořte a uložte dokument v aplikaci MS Word nebo MS Excel.
2. Klikněte na nabídku **Vložit**.
3. V části pro **Text** v panelu nástrojů rozviňte nabídku kliknutím na šipku vedle položky **Podpisová linka** a poté klikněte na tlačítko **Poskytovatel podpisu pro nástroj Privacy Manager**.

   Otevře se dialogové okno pro nastavení podpisu.
4. Do pole pod položkou **Další signatář** vložte jméno dalšího signatáře.
5. Do pole pod položkou **Instrukce pro signatáře** vložte vhodný text.

POZNÁMKA: Tato zpráva bude zobrazena na místě určeném pro podpis a po podepsání dokumentu bude smazána či přepsána jménem signatáře.

6. Pro zobrazení data podpisu zaškrtněte políčko vedle položky **Zobrazit datum podpisu na podpisové lince**.
7. Pro zobrazení titulu signatáře na podpisové lince zaškrtněte políčko vedle položky **Zobrazit titul signatáře na podpisové lince**.

POZNÁMKA: Vlastník přiděluje svému dokumentu další signatáře. Pole **Zobrazit datum podpisu na podpisové lince** a/nebo **Zobrazit titul signatáře na podpisové lince** musí být zaškrtnuta, aby další signatář mohl v podpisové lince zobrazit datum a/nebo titul.

8. Klikněte na tlačítko **OK**.

Přidání podpisové linky pro další signatáře

Pokud po otevření dokumentu spatří signatář svoje jméno v závorkách, znamená to, že je po něm vyžadován podpis dokumentu.

Podepsání dokumentu:

1. Poklepejte na příslušnou podpisovou linku.
2. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.

   Podpisová linka bude zobrazena podle specifikací majitele dokumentu.

Šifrování dokumentu Microsoft Office

Je možné zašifrovat dokumenty Microsoft Office pro vás a vaše důvěryhodné kontakty. Po zašifrování a zavření dokumentu je před jeho opětovným otevřením nutné ověření totožnosti.

Zašifrovat dokument Microsoft Office lze následujícím způsobem:

1. Vytvořte a uložte dokument v aplikaci MS Word, MS Excel či MS PowerPoint.
2. Klikněte na nabídku **Domů**.
3. Klikněte na šipku dolů vedle položky **Podepsat a šifrovat** a poté klikněte na možnost **Zašifrovat dokument**.

Otevře se dialogové okno se seznamem důvěryhodných kontaktů.

4. Klikněte na kontakt, který bude moci otevřít dokument a přečíst si jeho obsah.

POZNÁMKA: Výběr více jmen provedete podržením klávesy ctrl a následným kliknutím na jednotlivá jména.

5. Klikněte na tlačítko **OK**.

V případě pozdější úpravy dokumentu je třeba dodržet tento postup - Dešifrování dokumentu Microsoft Office na stránce 69. Po odstranění šifry z dokumentu je možné jej upravovat. Opětné zašifrování dokumentu lze provést způsobem popsaným v tomto oddílu nápovědy.

Dešifrování dokumentu Microsoft Office

Po dešifrování dokumentu Microsoft Office již není zapotřebí pro otevření dokumentu ověřovat totožnost vás ani vašich důvěryhodných kontaktů.

Dešifrování dokumentu Microsoft Office lze provést následujícím způsobem:

1. Otevřete zašifrovaný dokument MS Word, MS Excel či MS PowerPoint.
2. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.
3. Klikněte na nabídku **Domů**.
4. Klikněte na šipku dolů vedle položky **Podepsat a šifrovat** a poté klikněte na možnost **Dešifrovat**.

Odesílání zašifrovaného dokumentu Microsoft Office

Je možné připojit zašifrovaný dokument k e-mailové zprávě, aniž by samotná zpráva byla šifrována či digitálně podepsána. To lze provést vytvořením a odesláním běžného nechráněného e-mailu s digitálně podepsaným či zašifrovaným dokumentem v příloze.

Pro větší bezpečnost je nicméně vhodné zašifrovat i samotný e-mail.

Odeslání šifrovaného e-mailu s přiloženým zašifrovaným či digitálně podepsaným dokumentem Microsoft Office lze provést následujícím způsobem:

1. V aplikaci Microsoft Outlook klikněte na tlačítko **Nová zpráva** nebo na tlačítko **Odpovědět**.
2. Napište e-mailovou zprávu.
3. Připojte dokument Microsoft Office.
4. Více informací naleznete v části Zapečetění a odeslání e-mailové zprávy na stránce 66.

Prohlížení šifrovaného dokumentu Microsoft Office

POZNÁMKA: Pro prohlédnutí zašifrovaného dokumentu Microsoft Office není nutné vlastnit certifikát nástroje Privacy Manager.

Jakmile je otevřen podepsaný dokument Microsoft Office, zobrazí se ve stavovém řádku ve spodní části okna dokumentu ikona Digitální podpisy.

1. Kliknutím na ikonu **Digitální podpisy** můžete přepnout zobrazení dialogového okna Podpisy, v němž se zobrazují jména všech uživatelů, kteří tento dokument podepsali, a také datum jejich podpisu.

2. Chcete-li zobrazit další informace o jednotlivých podpisech, klikněte pravým tlačítkem na jméno v dialogovém okně Podpisy a poté vyberte příkaz **Podrobnosti o podpisu**.

Prohlížení zašifrovaného dokumentu Microsoft Office

K zobrazení zašifrovaného dokumentu Microsoft Office z jiného počítače je nutné, aby byl v počítači nainstalován nástroj Privacy Manager. Navíc je nutné obnovit certifikát nástroje Privacy Manager, který byl použit k zašifrování tohoto souboru.

Pokud jste přišli o certifikát a chcete zobrazit zašifrovaný dokument sady Microsoft Office, musíte obnovit certifikát aplikace Privacy Manager, který byl použit k zašifrování souboru.

Důvěryhodný kontakt, který si chce prohlédnout šifrovaný dokument Microsoft Office, musí mít certifikát Privacy Manager a modul Privacy Manager musí být instalován na jeho počítači. Navíc musí být Důvěryhodný kontakt vybrán majitelem šifrovaného dokumentu Microsoft Office.

Pokročilé úlohy

Migrace certifikátu Privacy Manager a Důvěryhodných kontaktů na jiný počítač

Je možné bezpečně přenést certifikáty nástroje Privacy Manager a důvěryhodné kontakty do jiného počítače nebo zálohovat data pro zvýšení bezpečnosti. V takovém případě je třeba vytvořit zálohu dat v souboru chráněném heslem na umístění v síti nebo ve vyjímatelném paměťovém zařízení a pak obnovit soubor do nového počítače.

Zálohování certifikátů Privacy Manager a důvěryhodných kontaktů

Zálohování certifikátů nástroje Privacy Manager a důvěryhodných kontaktů do souboru chráněného heslem lze provést následujícím způsobem:

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Migrace**.
2. Klikněte na položku **Záloha**.
3. Na stránce Výběr dat vyberte migrační soubor a klikněte na tlačítko **Další**.
4. Na stránce Migrační soubor zadejte umístění a jméno souboru nebo klikněte na tlačítko **Procházet** a umístění vyhledejte a poté klikněte na tlačítko **Další**.
5. Zadejte a potvrďte heslo. Poté klikněte na tlačítko **Další**.

POZNÁMKA: Toto heslo uložte na bezpečném místě. Budete je potřebovat při obnově migračního souboru.

6. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.
7. Na stránce Migrační soubor byl uložen klikněte na tlačítko **Dokončit**.

Obnovení certifikátů Privacy Manager a důvěryhodných kontaktů

Obnovu certifikátů nástroje Privacy Manager a důvěryhodných kontaktů v jiném počítači v rámci procesu migrace nebo ve stejném počítači lze provést následujícím způsobem:

1. Otevřete nástroj Privacy Manager a poté klikněte na položku **Migrace**.
2. Klikněte na tlačítko **Obnovit**.
3. Na stránce Migrační soubor klikněte na tlačítko **Procházet**, soubor vyhledejte a poté klikněte na tlačítko **Další**.
4. Zadejte heslo použité při vytvoření souboru zálohy a pak klikněte na tlačítko **Další**.
5. Na stránce Migrační soubor klikněte na tlačítko **Dokončit**.

Centrální správa nástroje Privacy Manager

Je možné, že tato instalace nástroje Privacy Manager je součástí centralizované instalace, která byla správcem přizpůsobena. Je možné, že jedna nebo více následujících funkcí budou povoleny nebo zakázány:

- **Zásady používání certifikátů** – Je možné, že budete omezeni na používání certifikátů nástroje Privacy Manager vydaných společností Comodo, nebo může být povoleno i používání digitálních certifikátů vydaných jinými certifikačními úřady.
- **Zásady šifrování** – Možnosti šifrování mohou být jednotlivě povoleny nebo zakázány v rámci sady Microsoft Office či aplikace Microsoft Outlook.

7 File Sanitizer (bezpečné odstranění souborů) pro HP ProtectTools

Nástroj File Sanitizer umožňuje bezpečné ničení cenných položek (např.: osobních informací či souborů, webových dat a dat spojených s historií a dalších datových součástí) ve vašem počítači a pravidelné čištění odstraněných položek z pevného disku.

POZNÁMKA: Tato verze aplikace File Sanitizer pracuje pouze s pevným diskem v počítači.

Bezpečné odstranění

Proces ničení se liší od standardního odstranění v systému Windows®, které je v aplikaci File Sanitizer nazýváno jednoduchým odstraněním. Při ničení dat pomocí aplikace File Sanitizer dojde k přepsání souborů nesmyslnými daty, čímž je prakticky znemožněno získání původních informací. Jednoduché odstranění systémem Windows může soubor (položku) ponechat v pořádku na pevném disku nebo ve stavu, kdy data lze obnovit vyšetřovacími metodami.

Při výběru profilu ničení (**Vysoké zabezpečení**, **Střední zabezpečení** či **Nízké zabezpečení**) je pro ničení automaticky vybrán předdefinovaný seznam položek a metoda odstranění. Můžete si také přizpůsobit profil ničení zadáním počtu cyklů ničení, zadáním položek, které mají být do ničení zahrnuty, před ničením kterých položek má být vyžadováno potvrzení a které položky mají být z ničení vyjmuty. Další informace naleznete v části Výběr a vytváření profilu ničení na stránce 78.

Můžete nastavit plán automatického ničení, nebo můžete ničení ručně aktivovat pomocí ikony **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu. Další informace naleznete v části Nastavení plánu ničení na stránce 77, Ruční zničení položky na stránce 82 nebo Ruční zničení všech vybraných položek na stránce 82.

POZNÁMKA: Soubor formátu DLL bude zničen a odstraněn ze systému jen tehdy, pokud byl přesunut do koše.

Čištění volného prostoru

Odstranění položky v systému Windows obsah položky z pevného disku zcela neodstraní. Systém Windows pouze smaže odkaz na položku. Obsah položky na pevném disku nadále zůstává, dokud není jeho prostor na pevném disku přepsán novými informacemi jiné položky.

Čištění volného prostoru umožňuje bezpečně přepisovat odstraněné položky nahodilými daty, což znemožňuje uživatelům zobrazovat původní obsah odstraněné položky.

POZNÁMKA: Čištění volného prostoru lze provádět příležitostně u položek odstraněných výběrem možnosti **Nastavení jednoduchého odstranění** v aplikaci File Sanitizer, přesunutím do koše systému Windows nebo ručním odstraněním. Čištění volného prostoru neposkytuje žádné další zabezpečení zničených položek.

Můžete nastavit plán automatického čištění volného prostoru, nebo můžete čištění ručně aktivovat pomocí ikony **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu. Další informace naleznete v části Nastavení plánu čištění volného prostoru na stránce 77 nebo Manuální spuštění čištění volného prostoru na stránce 83.

Spuštění aplikace File Sanitizer

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, poté na položku **HP** a nakonec na položku **HP ProtectTools Security Manager**.
2. Klikněte na položku **File Sanitizer**.

nebo

- Dvakrát klikněte na ikonu **File Sanitizer** umístěnou na pracovní ploše.

nebo

- Klikněte pravým tlačítkem na ikonu **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu, klikněte na položku **File Sanitizer** a poté na položku **Spustit aplikaci File Sanitizer**.

Instalační postupy

Nastavení plánu ničení

Můžete použít předdefinovaný profil ničení nebo si vytvořit vlastní profil ničení. Další informace naleznete v části Výběr a vytváření profilu ničení na stránce 78. Položky můžete také kdykoli zničit ručně. Další informace najdete v části Zahájení ničení sekvencí kláves na stránce 81.

POZNÁMKA: Naplánovaná úloha je spuštěna ve specifickou dobu. Pokud je systém v naplánované době vypnutý nebo v úsporném režimu/režimu spánku, aplikace File Sanitizer se nepokusí provést úlohu znovu později.

1. Spusťte aplikaci File Sanitizer a klikněte na tlačítko **Ničení**.
2. Vyberte jednu nebo více možností ničení:
   - **Vypnutí systému Windows** – Zničí všechny vybrané položky při vypínání systému Windows.

     POZNÁMKA: Při vypínání se otevře dialogové okno s dotazem, zda chcete pokračovat zničením souborů, nebo chcete proceduru přeskočit.

     Kliknutím na tlačítko **Ano** proceduru ničení přeskočíte, kliknutím na tlačítko **Ne** pokračujete v ničení.
   - **Spuštění webového prohlížeče** – Zničí všechny vybrané webové položky, jako například historii adres URL webového prohlížeče, při spuštění webového prohlížeče.
   - **Ukončení webového prohlížeče** – Zničí všechny vybrané webové položky, jako například historii adres URL webového prohlížeče, při zavření webového prohlížeče.
   - **Zadání sekvence kláves** – Umožňuje zahájit ničení sekvencí nastavených kláves. Podrobnosti naleznete v kapitole Zahájení ničení sekvencí kláves na stránce 81.

   POZNÁMKA: Soubor formátu DLL bude zničen a odstraněn ze systému jen tehdy, pokud byl přesunut do koše.
3. Pokud chcete do budoucna naplánovat ničení vybraných položek, vyberte pole **Aktivovat plánovač**, zadejte heslo systému Windows a poté vyberte datum a čas.
4. Klikněte na tlačítko **Použít**.

Nastavení plánu čištění volného prostoru

Čištění volného prostoru lze provádět příležitostně u položek odstraněných výběrem možnosti **Nastavení jednoduchého odstranění** v aplikaci File Sanitizer, přesunutím do koše systému Windows nebo ručním odstraněním. Čištění volného prostoru neposkytuje žádné další zabezpečení zničených položek.

POZNÁMKA: Naplánovaná úloha je spuštěna ve specifickou dobu. Pokud je systém v naplánované době vypnutý nebo v úsporném režimu/režimu spánku, aplikace File Sanitizer se nepokusí provést úlohu znovu později.

1. Spusťte aplikaci File Sanitizer a klikněte na tlačítko **Čištění**.
2. Pokud chcete do budoucna naplánovat čištění odstraněných položek na pevném disku, vyberte pole **Aktivovat plánovač**, zadejte heslo systému Windows a poté vyberte datum a čas.
3. Klikněte na tlačítko **Použít**.

POZNÁMKA: Operace čištění volného prostoru může být časově náročná. Ačkoli je čištění prováděno na pozadí, počítač může fungovat pomaleji z důvodu zvýšeného využití procesoru.

Výběr a vytváření profilu ničení

Můžete určit metodu mazání a vybrat položky ke zničení volbou předdefinovaného profilu, nebo vytvořením vlastního profilu.

Volba předdefinovaného profilu ničení

Při výběru předdefinovaného profilu ničení je automaticky vybrána předdefinovaná metoda mazání a seznam položek. Také můžete zobrazit předdefinovaný seznam položek vybraných pro zničení.

1. Spusťte aplikaci File Sanitizer a poté klikněte na tlačítko **Nastavení**.
2. Klikněte na předdefinovaný profil ničení:
   - **Vysoké zabezpečení**
   - **Střední zabezpečení**
   - **Nízké zabezpečení**
3. Kliknutím na tlačítko **Zobrazit podrobnosti** zobrazíte položky vybrané pro zničení.
   a. **Vybrané položky budou po potvrzení zobrazené zprávy zničeny. Nevybrané položky budou zničeny bez zobrazení zprávy k potvrzení.** — Chcete-li zničení položky potvrdit, zaškrtněte příslušné políčko. Zrušením zaškrtnutí položku zničíte bez zobrazení potvrzovací zprávy.

      POZNÁMKA: Položka bude zničena i v případě, že zrušíte zaškrtnutí pole.

   b. Klikněte na tlačítko **Použít**.
4. Klikněte na tlačítko **Použít**.

Přizpůsobení profilu ničení

Při vytváření profilu ničení, můžete zadat počet cyklů ničení, které položky mají být do ničení zahrnuty, před ničením kterých položek má být vyžadováno potvrzení a které položky mají být z ničení vyjmuty:

1. Spusťte aplikaci File Sanitizer, klikněte na tlačítko **Nastavení**, dále na možnost **Rozšířené nastavení zabezpečení** a poté na položku **Zobrazit podrobnosti**.
2. Vyberte počet cyklů ničení.

POZNÁMKA: S každou položkou bude proveden zadaný počet cyklů ničení. Pokud například zvolíte 3 cykly ničení, algoritmus překrývající data bude proveden nezávisle třikrát. Pokud zvolíte vyšší počet cyklů bezpečnostního ničení, může ničení trvat podstatnou dobu. Čím vyšší počet cyklů ničení však použijete, tím méně pravděpodobná bude možnost obnovení dat.

3. Výběr položek ke zničení:
   a. V části **Dostupné možnosti ničení** klikněte na položku a poté na možnost **Přidat**.
   b. Chcete-li přidat vlastní položku, klikněte na možnost **Přidat vlastní možnost** a vyhledejte nebo zadejte cestu k souboru nebo ke složce.
   c. Klikněte na tlačítko **Otevřít** a poté na tlačítko **OK**.
   d. V části **Dostupné možnosti ničení** klikněte na vlastní položku a poté na možnost **Přidat**.

   Položku lze z dostupných možností ničení odebrat kliknutím na položku a poté na možnost **Odstranit**.
4. **Vybrané položky budou po potvrzení zobrazené zprávy zničeny. Nevybrané položky budou zničeny bez zobrazení zprávy k potvrzení.** — Chcete-li zničení položky potvrdit, zaškrtněte příslušné políčko. Zrušením zaškrtnutí položku zničíte bez zobrazení potvrzovací zprávy.

POZNÁMKA: Položka bude zničena i v případě, že zrušíte zaškrtnutí pole.

   Položku vyjmete ze seznamu ničení kliknutím na položku a poté na možnost **Vyjmout**.
5. Ochrana složek nebo souborů před automatickým ničením:
   a. V části **Neničit následující** klikněte na možnost **Přidat** a vyhledejte nebo zadejte cestu k souboru nebo ke složce.
   b. Klikněte na tlačítko **Otevřít** a poté na tlačítko **OK**.

   Položku odstraníte ze seznamu výjimek kliknutím na položku a poté na možnost **Odstranit**.
6. Klikněte na tlačítko **Použít**.

Přizpůsobení profilu jednoduchého odstranění

Profil jednoduchého odstranění provede standardní odstranění položky bez jejího ničení. Profil jednoduchého odstranění si můžete přizpůsobit, pokud zadáte, které položky mají být zahrnuty, které položky vyžadují před odstraněním potvrzení a které položky mají být vyloučeny.

POZNÁMKA: Pokud vyberete možnost **Nastavení jednoduchého odstranění**, čištění volného prostoru lze občas provádět u položek, které byly odstraněny ručně nebo prostřednictvím koše systému Windows.

1. Spusťte aplikaci File Sanitizer, klikněte na tlačítko **Nastavení**, dále na možnost **Nastavení jednoduchého odstranění** a poté na položku **Zobrazit podrobnosti**.
2. Vyberte položky, které chcete odstranit:
   a. V části **Dostupné možnosti odstranění** klikněte na položku a poté na možnost **Přidat**.
   b. Chcete-li přidat vlastní položku, klikněte na možnost **Přidat vlastní možnost**, vyhledejte nebo zadejte cestu k souboru nebo ke složce a poté klikněte na možnost **OK**.
   c. Klikněte na vlastní položku a poté na tlačítko **Přidat**.

   Z dostupných možností odstranění položku odstraníte kliknutím na položku a poté na možnost **Odstranit**.
3. **Vybrané položky budou po potvrzení zobrazené zprávy zničeny. Nevybrané položky budou zničeny bez zobrazení zprávy k potvrzení.** — Chcete-li zničení položky potvrdit, zaškrtněte příslušné políčko. Zrušením zaškrtnutí položku zničíte bez zobrazení potvrzovací zprávy.

   POZNÁMKA: Položka bude zničena i v případě, že zrušíte zaškrtnutí pole.

   Položku vyjmete ze seznamu odstranění kliknutím na položku a poté na možnost **Vyjmout**.
4. Ochrana položek před automatickým odstraněním:
   a. V části **Neodstraňovat následující** klikněte na možnost **Přidat** a vyhledejte nebo zadejte cestu k souboru nebo ke složce.
   b. Klikněte na tlačítko **Otevřít** a poté na tlačítko **OK**.

   Položku odstraníte ze seznamu výjimek kliknutím na položku a poté na možnost **Odstranit**.
5. Klikněte na tlačítko **Použít**.

Obecné úlohy

File Sanitizer můžete použít k provedení následujících úkolů:

- Použít kombinaci kláves pro zahájení bezpečného odstranění - Tato funkce vám umožňuje vytvořit kombinaci kláves (například ctrl+alt+s) pro zahájení bezpečného odstranění. Podrobné informace naleznete v Zahájení ničení sekvencí kláves na stránce 81.
- Použití ikony File Sanitizer pro zahájení bezpečného odstranění - Tato funkce je podobná funkci potáhnout a pustit systému Windows. Podrobné informace naleznete v Použití ikony File Sanitizer na stránce 82.
- Ručně bezpečně odstranit specifický prostředek nebo všechny vybrané prostředky - Tyto funkce vám umožňují ruční bezpečné odstranění bez čekání na zahájení pravidelného naplánovaného bezpečného odstranění. Podrobné informace naleznete v Ruční zničení položky na stránce 82 nebo Ruční zničení všech vybraných položek na stránce 82.
- Ručně aktivovat čištění volného prostoru - Tato funkce vám umožňuje ručně aktivovat čištění volného prostoru. Podrobné informace naleznete v Manuální spuštění čištění volného prostoru na stránce 83.
- Zrušit operace bezpečného odstranění nebo čištění volného prostoru - Tato funkce vám umožní zastavit operace bezpečného odstranění nebo čištění volného prostoru. Podrobné informace naleznete v Zrušení operace ničení a čištění volného prostoru na stránce 83.
- Zobrazení souboru protokolů - Tato funkce vám umožňuje zobrazit soubor protokolů bezpečného odstranění a čištění volného prostoru, který obsahuje jakékoliv chyby nebo selhání z poslední operace bezpečného odstraňování nebo čištění volného prostoru. Podrobné informace naleznete v Zobrazování protokolů na stránce 83.

POZNÁMKA: Operace bezpečného odstranění nebo čištění volného prostoru může trvat značně dlouhou dobu. Protože v pozadí probíhá bezpečné odstraňování a čištění volného prostoru, počítač může fungovat pomaleji kvůli zvýšeným nárokům na procesor.

Zahájení ničení sekvencí kláves

1. Spusťte aplikaci File Sanitizer a klikněte na tlačítko **Ničení**.
2. Zaškrtněte políčko **Sekvence kláves**.
3. Zadejte znak do poskytnutého pole.
4. Vyberte políčko **CTRL** nebo **ALT** a pak vyberte políčko **SHIFT**.

   Pokud například chcete zahájit automatické ničení klávesami s a ctrl+shift, zadejte do pole s a poté zvolte možnosti **CTRL** a **SHIFT**.

POZNÁMKA: Zadejte sekvenci kláves odlišnou od ostatních, které jste již konfigurovali.

Zahájení ničení sekvencí kláves:

1. Podržte klávesy shift a ctrl nebo alt (nebo jakoukoli určenou kombinaci) a zároveň stiskněte zvolený znak.
2. Zobrazí-li se dialogové okno s potvrzením, klikněte na možnost **Ano**.

Použití ikony File Sanitizer

UPOZORNĚNÍ: Zničené položky nelze obnovit. Pečlivě zvažte, které položky chcete vybrat pro ruční ničení.

1. Přejděte do umístění dokumentu nebo složky, kterou chcete zničit.
2. Přetáhněte položku na ikonu **File Sanitizer** na pracovní ploše.
3. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

Ruční zničení položky

UPOZORNĚNÍ: Zničené položky nelze obnovit. Pečlivě zvažte, které položky chcete vybrat pro ruční ničení.

1. Klikněte pravým tlačítkem na ikonu **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu, klikněte na položku **File Sanitizer** a poté **Zničit jeden**.
2. Když se otevře dialogové okno Procházet, vyhledejte položku, kterou chcete zničit, a klikněte na tlačítko **OK**.

   POZNÁMKA: Zvolená položka může být jednotlivý soubor nebo složka.

3. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

– nebo –

1. Klikněte pravým tlačítkem na ikonu **File Sanitizer** na ploše a poté kliknete na možnost **Zničit jeden**.
2. Když se otevře dialogové okno Procházet, vyhledejte položku, kterou chcete zničit, a klikněte na tlačítko **OK**.
3. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

– nebo –

1. Spusťte aplikaci File Sanitizer a klikněte na tlačítko **Ničení**.
2. Klikněte na tlačítko **Procházet**.
3. Když se otevře dialogové okno Procházet, vyhledejte položku, kterou chcete zničit, a klikněte na tlačítko **OK**.
4. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

Ruční zničení všech vybraných položek

1. Klikněte pravým tlačítkem na ikonu **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu, klikněte na položku **File Sanitizer** a poté **Zničit nyní**.
2. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

– nebo –

1. Klikněte pravým tlačítkem na ikonu **File Sanitizer** na ploše a poté kliknete na možnost **Zničit nyní**.
2. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

– nebo –

1. Spusťte aplikaci File Sanitizer a klikněte na tlačítko **Ničení**.
2. Klikněte na tlačítko **Zničit nyní**.
3. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

Manuální spuštění čištění volného prostoru

1. Klikněte pravým tlačítkem na ikonu **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu, klikněte na položku **File Sanitizer** a poté **Vyčistit nyní**.
2. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

– nebo –

1. Spusťte aplikaci File Sanitizer a poté klikněte na tlačítko **Čištění volného prostoru**.
2. Klikněte na položku **Vyčistit nyní**.
3. V otevřeném dialogovém okně klikněte na tlačítko **Ano**.

Zrušení operace ničení a čištění volného prostoru

Když probíhá ničení nebo čištění volného prostoru, zobrazí se zpráva nad ikonou HP ProtectTools Security Manager v oznamovací oblasti na pravém konci panelu úloh. Zpráva podává informace o průběhu ničení nebo čištění volného prostoru (procentuální dokončení) a nabízí možnost zrušení operace.

▲ Operaci zrušíte kliknutím na zprávu a poté na možnost **Zastavit**.

Zobrazování protokolů

Kdykoli je prováděno ničení nebo čištění volného prostoru, jsou generovány protokoly o případných chybách. Protokoly jsou vždy aktualizovány podle posledních operací ničení a čištění volného prostoru.

POZNÁMKA: Úspěšně zničené nebo vyčištěné soubory se v protokolech nezobrazují.

Jeden soubor protokolu je vytvořen pro operace ničení a jeden pro operace čištění volného prostoru. Oba soubory protokolu jsou umístěny na pevném disku v umístění:

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

U 64bitových systémů jsou oba soubory protokolu umístěny na pevném disku v umístění:

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

8 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 95.

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. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
3. V levém podokně klepněte na položku **Device Access Manager**.

Uživatelé mohou 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.

Zobrazení Simple Configuration (Jednoduchá konfigurace)

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

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

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klepněte na položku **Device Access Manager** a pak klepněte 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. Klepněte 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. Klepněte 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 spustit nebo ukončit tuto službu:

1. V systému Windows 7 klikněte na tlačítko **Start**, poté na tlačítko **Ovládací panely** a nakonec na tlačítko **Systém a zabezpečení**.

   nebo

   V systému Windows Vista® klikněte na tlačítko **Start**, poté na tlačítko **Ovládací panely** a nakonec na tlačítko **Systém a údržba**.

   nebo

   V systému Windows XP klikněte na tlačítko **Start**, poté na tlačítko **Ovládací panely** a dále na možnost **Výkon a údržba**.

2. Klepněte na položku **Nástroje pro správu** a poté klepněte na položku **Služby**.
3. Vyhledejte službu **HP ProtectTools Device Locking/Auditing**.
4. Chcete-li službu spustit, klikněte na možnost **Spustit**.

   nebo

   Chcete-li běžící službu zastavit, klikněte na možnost **Zastavit**.

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 uživatelů nedostupná, bylo toto nastavení zděděno ze třídy zařízení v seznamu 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 klepněte na položku **Device Access Manager** a pak klepněte na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klepněte 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 klepněte na tlačítko **Odmítnout**.
4. Klepněte 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 klepněte na položku **Device Access Manager** a pak klepněte na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klepněte na jednu z následujících položek:
   - **Třída zařízení**
   - **Všechna zařízení**
   - **Jednotlivé zařízení**
3. Klepněte na tlačítko **Přidat**.

   Otevře se dialogové okno Vybrat uživatele nebo skupiny.
4. Klepněte na položku **Upřesnit** a pak klepnutím na tlačítko **Hledat nyní** vyhledejte uživatele nebo skupiny, které chcete přidat.

5. Klepněte na uživatele nebo skupinu, které chcete přidat do seznamu dostupných uživatelů a skupin, a pak klepněte na tlačítko **OK**.
6. Znovu klepněte na tlačítko **OK**.
7. Klepnutím na položku **Povolit** udělte tomuto uživateli přístup.
8. Klepněte 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 klepněte na položku **Device Access Manager** a pak klepněte na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klepněte 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 klepněte na tlačítko **Odmítnout**.
4. Přejděte ke složce pod složkou požadované třídy a pak přidejte konkrétního uživatele.
5. Klepnutím na položku **Povolit** udělte tomuto uživateli přístup.
6. Klepněte 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 klepněte na položku **Device Access Manager** a pak klepněte na položku **Konfigurace tříd zařízení**.
2. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat, a pak přejděte ke složce pod ní.
3. V části **Uživatel/skupiny** klepněte na tlačítko **Povolit** vedle skupiny, jíž chcete udělit přístup.
4. Klepněte na tlačítko **Odmítnout** vedle skupiny, jíž chcete odmítnout přístup.
5. V seznamu zařízení přejděte ke specifickému zařízení, k němuž chcete uživateli povolit přístup.
6. Klepněte na tlačítko **Přidat**.

   Otevře se dialogové okno Select Users or Groups (Vybrat uživatele nebo skupiny).
7. Klepněte na položku **Upřesnit** a pak klepnutím na tlačítko **Hledat nyní** vyhledejte uživatele nebo skupiny, které chcete přidat.
8. Klepněte na uživatele, kterému má být povolen přístup, a pak klepněte na tlačítko **OK**.

9. Klepnutím na položku **Povolit** udělte tomuto uživateli přístup.

10. Klepněte 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 klepněte na položku **Device Access Manager** a pak klepněte na položku **Konfigurace tříd zařízení**.

2. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat.

   - **Třída zařízení**
   - **Všechna zařízení**
   - **Jednotlivé zařízení**

3. V části **Uživatel/skupiny** klepněte na uživatele nebo skupinu, která má být odebrána, a pak klepněte na tlačítko **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.

Chcete-li obnovit konfigurační nastavení výrobce, postupujte takto:

1. V levém podokně okna Konzola pro správu nástroje HP ProtectTools klepněte na položku **Device Access Manager** a pak klepněte 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 otevře dialogové okno pro 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 klepněte na položku **Device Access Manager** a pak klepněte 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 klepněte na položku **Device Access Manager** a pak klepněte 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 klepněte na položku **Device Access Manager** a pak klepněte 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 na stránce Skupina Správci zařízení na stránce 94.

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**.

Alternativní metody pro správu členství v této skupině zahrnují:

- V systémech Windows 7 Professional a Windows Vista lze uživatele do této skupiny přidávat pomocí standardního modulu snap-in „Místní uživatelé a skupiny“ konzoly Microsoft Management Console (MMC).
- U verze Home systémů Windows 7, Windows Vista a Windows XP použijte účet správce a do příkazového řádku zadejte následující příkaz:

  ```
  net localgroup “Device Administrators” username /add
  ```

  V tomto příkaze představuje parametr „username“ uživatelské jméno uživatele, kterého chcete do této skupiny přidat.

Podpora rozhraní 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

9 Obnova po krádeži

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. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, potom na položku **HP** a nakonec na položku **HP ProtectTools Security Manager**.
3. V levém podokně nástroje Security Manager klikněte na položku **Obnova po krádeži**.
4. Chcete-li spustit Průvodce aktivací služby Computrace, klikněte na tlačítko **Aktivovat nyní**.
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**.

10 Nástroj HP ProtectTools Embedded Security Manager (pouze vybrané modely)

POZNÁMKA: Pokud chcete používat modul Embedded Security pro ProtectTools, musí být v počítači nainstalován čip integrovaného zabezpečení TPM (Trusted Platform Module).

Modul Embedded Security for HP ProtectTools zajišťuje ochranu před neoprávněným přístupem k datům nebo přihlašovacím údajům uživatele. Tento softwarový modul poskytuje následující bezpečnostní funkce:

- rozšířený šifrovaný souborový systém Microsoft® Encryption File System (EFS) pro šifrování souborů a složek,
- vytvoření osobního zabezpečeného disku (PSD) pro ochranu uživatelských dat,
- funkce pro správu dat, například zálohování a obnovení hierarchie klíčů,
- podpora operací s chráněnými digitálními certifikáty při použití nástroje Embedded Security u aplikací jiných dodavatelů (například aplikace Microsoft Outlook a Internet Explorer).

Vestavěný bezpečnostní čip TPM nabízí zvýšenou a rozšířenou nabídku funkcí aplikace HP ProtectTools Security Manager. Aplikace Credential Manager for HP ProtectTools může například použít vestavěný čip pro potřeby ověřování během přihlašování do systému Windows.

Nastavení

⚠ **UPOZORNĚNÍ:** V rámci snížení bezpečnostního rizika důrazně doporučujeme, aby váš správce IT vestavěný bezpečnostní čip co nejdříve inicializoval. Pokud nebude vestavěný bezpečnostní čip inicializován, může dojít k tomu, že k počítači získá přístup neoprávněný uživatel nebo počítačový virus, který ovládne procesy majitele (například správu archivu pro nouzovou obnovu), nebo bude provádět změny přístupových práv uživatelů.

Podle kroků v následujících dvou částech aktivujte a inicializujte vestavěný bezpečnostní čip.

Aktivace vestavěného bezpečnostního čipu v nástroji Computer Setup

Vestavěný bezpečnostní čip musí být aktivován v Průvodci rychlou inicializací, nebo v nástroji Computer Setup.

Aktivace vestavěného bezpečnostního čipu v nástroji Computer Setup:

1. Spusťte nástroj Computer Setup zapnutím nebo restartováním počítače a stisknutím klávesy f10 v okamžiku, kdy je v dolním levém rohu obrazovky zobrazena zpráva ”F10 = ROM Based Setup” (F10 = konfigurační nástroj v paměti ROM).
2. Pokud jste nenastavili heslo správce, pomocí kláves se šipkami vyberte **Security** (Zabezpečení), poté **Setup password** (Nastavení hesla) a poté stiskněte enter.
3. Zadejte heslo do polí **New password** (Nové heslo) a **Verify new password** (Potvrdit nové heslo) a stiskněte klávesu f10.
4. V nabídce **Security** (Zabezpečení) pomocí kláves se šipkami vyberte položku **TPM Embedded Security** (Integrované zabezpečení TPM) a stiskněte klávesu enter.
5. U položky **Embedded Security** (Integrované zabezpečení) v případě, že je zařízení skryté, vyberte volbu **Available** (Dostupné).
6. Vyberte možnost **Stav zařízení Embedded Security** a změňte nastavení na hodnotu **Povolit**.
7. Stisknutím klávesy f10 přijmete změny v konfiguraci integrovaného zabezpečení.
8. Pokud chcete předvolby uložit a ukončit nástroj Computer Setup, pomocí kláves se šipkami vyberte položku **Soubor**, vyberte možnost **Uložit změny a ukončit** a postupujte podle pokynů na obrazovce.

Inicializace vestavěného bezpečnostního čipu

Během inicializace funkce Embedded Security je třeba provést tyto akce:

- nastavit heslo vlastníka integrovaného bezpečnostního čipu, které chrání před přístupem ke všem funkcím vlastníka integrovaného bezpečnostního čipu,
- nastavit archív pro nouzovou obnovu, což je chráněné úložiště, které umožňuje opětovné šifrování základních uživatelských klíčů všech uživatelů.

Inicializace integrovaného bezpečnostního čipu:

1. Klikněte pravým tlačítkem na ikonu **HP ProtectTools Security Manager** v oznamovací oblasti na pravé straně hlavního panelu a vyberte položku **Inicializace funkce Embedded Security**.

   Spustí se průvodce HP ProtectTools Embedded Security Initialization Wizard.

2. Postupujte podle pokynů na obrazovce.

Vytvoření základního uživatelského účtu

Vytvoření základního uživatelského účtu v modulu Embedded Security zahrnuje tyto akce:

- Vytváří základní uživatelský klíč, který chrání šifrované informace a nastavuje heslo základního uživatelského klíče, které chrání základní uživatelský klíč.
- Vytváří osobní zabezpečený disk (PSD) pro ukládání šifrovaných souborů a složek.

⚠ **UPOZORNĚNÍ:** Heslo základního uživatelského klíče bezpečně uschovejte. K šifrovaným informacím nelze přistupovat ani je nelze obnovit v případě ztráty tohoto hesla.

Vytvoření základního uživatelského účtu a aktivace uživatelských bezpečnostních funkcí:

1. Pokud není průvodce Embedded Security User Initialization Wizard spuštěn, klikněte na tlačítko **Start**, poté na položku **Všechny programy**, **HP** a položku **HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Embedded Security** a potom vyberte položku **Uživatelská nastavení**.
3. V pravém podokně u položky **Funkce integrovaného zabezpečení** klepněte na volbu **Konfigurovat**.

   Spustí se průvodce Embedded Security User Initialization Wizard.
4. Postupujte podle pokynů na obrazovce.

POZNÁMKA: Pro použití el. pošty musíte nejprve konfigurovat klienta el. pošty, aby bylo možné používat digitální certifikát, který je vytvořen v rámci intergrovaného zabezpečení. Pokud není digitální certifikát k dispozici, musíte jej získat od certifikačního úřadu. Pokyny ke konfiguraci vaší el. pošty a získání digitálního certifikátu viz Nápověda k softwaru klienta el. pošty.

Obecné úlohy

Jakmile vytvoříte základní uživatelský účet, můžete provádět následující operace:

- Šifrování souborů a složek
- Odesílání a přijímání šifrované elektronické pošty

Používání osobního zabezpečeného disku

Jakmile vytvoříte disk PSD, budete při příštím přihlášení vyzváni k zadání hesla základního uživatelského klíče. Pokud správně zadáte heslo základního uživatelského klíče, můžete přistupovat k disku PSD přímo z aplikace Windows Explorer.

Šifrování souborů a složek

Při práci se šifrovanými soubory v systému vezměte v úvahu následující pravidla:

- Šifrovat lze pouze soubory a složky v oddílech NTFS. Nelze šifrovat soubory a složky v oddílech FAT.
- Soubory systému a komprimované soubory nelze šifrovat a šifrované soubory nelze komprimovat.
- Dočasné složky by měly být šifrovány, protože jsou potencionálním cílem hackerů.
- Při prvním zašifrování souboru nebo složky jsou automaticky nastaveny zásady pro obnovu. Tyto zásady zajistí, že v případě ztráty šifrovacích certifikátů a soukromých klíčů bude program pro obnovu schopen dešifrovat uložené informace.

Šifrování souborů a složek:

1. Klepněte pravým tlačítkem myši na soubor nebo složku, které chcete zašifrovat.
2. Klepněte na tlačítko **Encrypt**.
3. Vyberte jednu z následujících možností:
   - **Použít změny pouze u této složky.**
   - **Použít změny u této složky, vnořených složek a souborů.**
4. Klepněte na tlačítko **OK**.

Odesílání a přijímání šifrované elektronické pošty

Integrované zabezpečení umožňuje odesílání a přijímání šifrovaných zpráv el. pošty, ale postup se liší v závislosti na programu, který pro el. poštu používáte. Více informací viz Nápověda softwaru integrovaného zabezpečení a programu el. pošty.

Změna hesla základního uživatelského klíče

Změna hesla základního uživatelského klíče:

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, potom na položku **HP** a nakonec na položku **HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Embedded Security** a potom vyberte položku **Uživatelská nastavení**.
3. V pravém podokně klikněte v části **Základní uživatelské heslo** na položku **Změnit**.
4. Zadejte staré heslo a potom nastavte a potvrďte nové heslo.
5. Klepněte na tlačítko **OK**.

Pokročilé operace

Správci mohou v nástroji Embedded Security provádět následující úlohy:

- Zálohování a obnova přihlašovacích údajů nástroje Embedded Security, úprava nastavení nástroje Embedded Security a správa osobního zabezpečeného disku
- Změna hesla vlastníka
- Změna uživatelského hesla
- Zabezpečený přenos uživatelských bezpečnostních přihlašovacích údajů ze zdrojové platformy na cílovou

Zálohování a obnova

Funkce zálohování Embedded Security vytváří archív, který obsahuje certifikační údaje, které lze obnovit v případě nouze.

Vytvoření souboru zálohy

Vytvoření souboru zálohy:

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně klepněte na možnost **Embedded Security** a poté klepněte na položku **Zálohování**.
3. V pravém podokně klikněte na možnost **Konfigurovat**. Spustí se Průvodce zálohováním nástroje HP Embedded Security for ProtectTools.
4. Postupujte podle pokynů na obrazovce.

Obnovení certifikačních údajů ze souboru zálohy

Obnovení dat se souboru zálohy:

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně klepněte na možnost **Embedded Security** a poté klepněte na položku **Zálohování**.
3. V pravém podokně klikněte na možnost **Obnovit vše**. Spustí se Průvodce zálohováním nástroje HP Embedded Security for ProtectTools.
4. Postupujte podle pokynů na obrazovce.

Změna hesla vlastníka

Správci mohou měnit heslo vlastníka:

1. Klikněte na tlačítko **Start**, poté na položku **Všechny programy**, na položku **HP** a nakonec na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně klepněte na možnost **Embedded Security** a potom klepněte na položku **Pokročilé**.
3. V pravém podokně klepněte u možnosti **Heslo vlastníka** na položku **Změnit**.
4. Zadejte staré heslo vlastníka a potom nastavte a potvrďte nové heslo vlastníka.
5. Klepněte na tlačítko **OK**.

Resetování hesla uživatele

Správce může uživateli pomoci resetovat zapomenuté heslo. Další informace naleznete v Nápovědě softwaru.

Migrace klíčů pomocí průvodce Migration Wizard

Migrace je pokročilá procedura, která umožňuje správu, obnovu a převod klíčů a certifikátů.

Podrobnosti o migraci viz Nápověda softwaru integrovaného zabezpečení.

11 Výjimky při lokalizaci hesel

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

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, jakými 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.

Například v některých japonských verzích systému Windows XP se výchozí editor IME nazývá Microsoft IME Standard 2002 pro japonštinu a tento editor překládá dle rozvržení klávesnice E0010411. Jedná se však o rozvržení pro editor IME a ne o běžné rozvržení klávesnice. (Kódovací schéma rozvržení klávesnice je rezervováno společností Microsoft pro editor IME nad rámec běžného rozvržení klávesnice.) Jelikož se jedná o rozvržení klávesnice, které nelze vyjádřit v prostředí pro psaní hesla v rámci funkce Zabezpečení před spuštěním systému BIOS nebo aplikace HP Drive Encryption, bude jakékoli heslo napsané pomocí editoru IME odmítnuto nástrojem HP ProtectTools. Editor Microsoft IME Standard 2002 pro japonštinu se rovněž liší od „běžného názvu“ v systému Microsoft Windows Vista®. Systém Windows mapuje některé editory IME na rozvržení klávesnice. V takovém případě je editor IME nástrojem HP ProtectTools podporován, jelikož je použita výchozí definice rozvržení klávesnice (hexadecimální kód).

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 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 původní 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 pomocí tohoto rozvržení zadaná budou v systému BIOS nastavena správně.

Další možný problém spočívá v užití stejných znaků pomocí různých rozvržení klávesnice. Například při 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, přestože 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 ﻯ dojde k vytvoření dvou znaků.	Stisknutím klávesy ﻯ ,ﻱ nebo ﻯ dojde k vytvoření jednoho znaku.	Stisknutím klávesy ﻯ ,ﻱ nebo ﻯ 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 rámci aplikace HP Drive Encryption k vytvoření znaku ç, è, à resp. é.
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)	◦ Klávesy ¡, ¤, ‘, ’, ¥, a × v horní řadě nelze použít. ◦ Nelze použít klávesy å, ® a Þ v druhé řadě. ◦ Nelze použít klávesy á, ð a ø ve třetí řadě. ◦ Nelze použít klávesu æ v dolní řadě.	Není k dispozici	Není k dispozici

Jazyk	Windows	BIOS	Drive Encryption
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 ŗ.	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
Slovinština	Klávesu żŻ nelze použít v systému Windows a klávesa alt v systému BIOS představuje znaménkovou klávesu.	Nelze použít klávesy ú, Ú, ů, Ů, ş, Ş, ś, Ś, š a Š.	Není k dispozici
Japonština	V systému Windows XP je plně podporováno standardní japonské rozvržení klávesnice (411). Editor Microsoft Standard IME 2002, který je v systému Windows XP běžně přítomen, by za normálních okolností podporován nebyl. Bylo však ověřeno, že tento editor IME je při psaní jednoduchých znaků téměř totožný s rozvržením klávesnice 411. Při používání lokalizovaných japonských hesel v systému BIOS a aplikaci HP Drive Encryption proto software tento editor IME přepíná na rozvržení klávesnice 411. Pokud je to možné, je lepší používat editor IME Microsoft Office 2007. Navzdory názvu se v tomto případě jedná vlastně o podporované rozvržení klávesnice 411.	Není k dispozici	Není k dispozici

Jak postupovat v případě, že 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. Klikněte na tlačítko **Start**, poté na tlačítko **Ovládací panely** a poté na tlačítko **Místní a jazykové nastavení**.
  2. Klikněte na kartu **Jazyky**.
  3. Klikněte na tlačítko **Podrobnosti**.
  4. Na kartě **Nastavení** kliknutím na tlačítko **Přidat** přidejte podporovanou klávesnici (např. v části Čínština přidejte americké rozvržení klávesnice).
  5. Podporovanou klávesnici nastavte na výchozí zadávání.
  6. 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. Nepodporované znaky jsou uvedeny v následující tabulce Práce se speciálními klávesami na stránce 111.
  2. Spusťte průvodce nastavením nástroje Security Manager a zadejte nové heslo systému Windows.

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.

ATM
Automatic Technology Manager (ATM) umožňuje síťovým správcům dálkovou správu systémů na úrovni BIOS.

automatické bezpečné odstranění
Naplánované bezpečné odstranění, které uživatel nastavil v modulu File Sanitizer.

bezpečné odstranění
Vyvolání algoritmu, který chrání data obsažená v prostředku.

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.

Certifikát Správce soukromí
Digitální certifikát, který vyžaduje ověření pokaždé, když jej používáte pro kryptografické operace, jako např. podepsání a šifrování zpráv el. pošty a dokumentů Microsoft Office.

cyklus bezpečného odstranění
Počet opakování algoritmu bezpečného odstranění, který je vyvolán pro každý prostředek. Čím více cyklů určíte, tím více zabezpečený počítač je.

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.

čištění volného místa
Bezpečné zapisování náhodných dat přes odstraněné prostředky pro zničení obsahů odstraněných prostředků.

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

digitální certifikát

Elektronická pověření, která potvrzují identitu jednotlivce nebo společnosti spojením identity majitele digitálního certifikátu s párem elektronických klíčů, které jsou používány pro podepisování digitálních informací.

digitální podpis
Data odeslaná se souborem, který ověřuje odesílatele materiálu a že soubor nebyl před podpisem upravován.

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.

důvěryhodná zpráva
Relace komunikace, během které jsou odesílány důvěryhodné zprávy mezi důvěryhodným odesílatelem a Důvěryhodným kontaktem.

Důvěryhodný kontakt
Osoba, která přijala pozvání Důvěryhodného kontaktu.

důvěryhodný odesílatel
Důvěryhodný kontakt, který odešle podepsané a/nebo šifrované zprávy el. pošty a dokumenty Microsoft Office.

HP SpareKey
Záložní kopie klíče nástroje Drive Encryption.

Identifikační karta
Miniaplikace na pracovní ploše systému Windows, která slouží k vizuální identifikaci pracovní plochy pomocí jména uživatele a zvoleného obrázku. Klepnutím na identifikační kartu spustíte Konzolu pro správu nástroje HP ProtectTools.

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

jednoduché odstranění
Odstranění reference Windows k prostředku. Obsah prostředku zůstane na pevném disku, dokud nebude přepsán pomocí čištění volného místa.

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

kombinace kláves
Kombinace specifických kláves, která při stisknutí zahájí automatické bezpečné odstranění, např. ctrl+alt+s.

konzola
Ústřední místo, odkud můžete zpřístupnit a spravovat funkce a nastavení v konzole správce HP ProtectTools.

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

manuální bezpečné odstranění
Okamžité bezpečné odstranění vybraného prostředku nebo prostředků, kterým se obejde naplánované automatické bezpečné odstranění.

metoda zabezpečeného přihlašování
Způsob použitý pro přihlášení se k počítači.

migrace
Úkol, který umožňuje správu, obnovu a přesun certifikátů a důvěryhodných kontaktů Privacy Manager.

navrhovaný podepisující
Uživatel, který je navržen majitelem dokumentu Microsoft Word nebo Excel pro přidání řádku s podpisem do dokumentu.

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.

paměť
Viz *metoda zabezpečeného přihlašování*.

Paměť USB
Bezpečnostní zařízení, které uchovává informace identifikující uživatele. Podobně jako čtečka čipových karet nebo čtečka biometrických údajů se používá pro ověření vlastníka pro práci s počítačem.

panel nástrojů
Ústřední místo, odkud můžete zpřístupnit a spravovat funkce a nastavení v Security Manager pro HP ProtectTools.

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.

Pozvání Důvěryhodného kontaktu
Zpráva el. pošty, která je odeslána osobě, která žádá o to, aby se stala Důvěryhodným kontaktem.

profil bezpečného odstraňování

Specifikovaný způsob odstranění a seznam prostředků.

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 rámci Security Manager, který se skládá z uživatelského jména a hesla (a případně dalších vybraných informací), který může být použit k přihlášení se na webové stránky nebo jiné programy.

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.

Příjemce Důvěryhodného kontaktu
Osoba, která obdrží pozvání k tomu, aby se stala Důvěryhodným kontaktem.

PSD
Osobní bezpečná jednotka, která poskytuje chráněné úložiště pro citlivé informace.

restart
Proces restartování počítače.

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

řádek s podpisem
Rámeček pro zobrazení digitálního podpisu. Když je dokument podepsán, zobrazí se jméno a způsob ověření podepisujícího. Může být zobrazeno i datum a titul podepisujícího.

scéna
Fotografie registrovaného uživatele, která se použije při ověření.

Seznam Důvěryhodných kontaktů
Seznam Důvěryhodných kontaktů.

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
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.

tlačítko Podepsat a šifrovat
Toto tlačítko se nachází na panelu nástrojů aplikace Microsoft Office. Kliknutím na něj zpřístupníte možnost podepsat, zašifrovat či dešifrovat dokument Microsoft Office.

tlačítko pro bezpečné odeslání
Softwarové tlačítko, které se zobrazí na liště zpráv el. pošty Microsoft Outlook. Klepnutím na toto tlačítko umožníte podepsání a/nebo šifrování zprávy el. pošty Microsoft Outlook.

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.

virtuální paměť
Bezpečnostní funkce, která funguje podobným způsobem jako čipová karta se čtečkou. Známka se ukládá buď na pevný disk počítače, nebo do registru systému Windows. Při přihlášení pomocí virtuální známky je uživatel v rámci dokončení procesu ověření vyzván k zadání kódu PIN.

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.

zapečetění zprávy pro důvěryhodný kontakt
Přidává digitální podpis, šifruje el. poštu a odesílá ji po vašem ověření pomocí zvoleného způsobu bezpečného přihlášení.

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

Rejstřík