Zabezpečovací software nástroje HP ProtectTools pro malé podniky, verze 5.10

Uživatelská příručka

Uživatelská příručka zabezpečovacího softwaru nástroje HP ProtectTools pro malé podniky, verze 5.10

HP Business PC

Třetí vydání: Červenec 2010

Číslo dokumentace: 610663-223

Informace o této knize

Tato uživatelská příručka poskytuje informace o zabezpečovacím softwaru nástroje HP ProtectTools pro malé podniky.

⚠ **VAROVÁNÍ!** Text zvýrazněný tímto způsobem označuje, že nedodržení pokynů by mohlo vést ke zranění nebo smrti.

△ **UPOZORNĚNÍ:** Text zvýrazněný tímto způsobem označuje, že nedodržení pokynů by mohlo vést k poškození zařízení či ztrátě informací.

POZNÁMKA: Text zvýrazněný tímto způsobem poskytuje důležité doplňkové informace.

Obsah

1 Úvod do zabezpečení

Společnost HP si uvědomuje, že váš čas je cenný a že se potřebujete soustředit na řízení své společnosti – nikoli na vhodný zabezpečovací software chránící váš počítač, data a podnik.

Měli byste se vážně zamyslet nad nákupem zabezpečovacího řešení, které bude jednoduché, ale účinně ochrání váš podnikový majetek. Zabezpečení není v dnešní době jen módní záležitost – je to naprostá nutnost!

Společnost HP nabízí zabezpečovací řešení, která se snadno implementuje i používá. Jde o nástroj HP ProtectTools, který byl navržen speciálně pro malé podniky.

Zabezpečovací software nástroje HP ProtectTools pro malé podniky je vybaven funkcemi, díky nimž se riziko neoprávněného přístupu k počítači a důležitým datům snižuje na minimum. Rozšířené funkce zabezpečení poskytuje několik softwarových modulů HP ProtectTools.

Nástroj HP ProtectTools pro malé podniky zahrnuje dvě verze: konzolu pro správu nástroje HP ProtectTools Security Manager a nástroj HP ProtectTools Security Manager (pro běžné uživatele). Uživatelská verze i verze pro správce jsou dostupné prostřednictvím nabídky **Start** > **Všechny programy**.

Modul	Funkce
Konzola pro správu nástroje HP ProtectTools Security Manager	• Vyžaduje pro přístup oprávnění správce systému Microsoft Windows. • Přístup k modulům musí konfigurovat správce, není k dispozici pro obecné uživatele. • Umožňuje počáteční nastavení zabezpečení a konfiguruje možnosti nebo požadavky pro všechny uživatele.
HP ProtectTools Security Manager (pro běžné uživatele)	• Umožňuje uživatelům konfigurovat možnosti poskytnuté správcem. • Je možné omezit přístup a umožnit uživateli pouze omezenou kontrolu nad některými moduly nástroje HP ProtectTools.

Softwarové moduly nástroje HP ProtectTools mohou být předem nainstalovány, zavedeny nebo k dispozici jako konfigurovatelné možnosti či jako volitelné produkty. Další informace naleznete na webu http://www.hp.com.

Funkce nástroje HP ProtectTools

V následující tabulce je uveden podrobný přehled klíčových funkcí modulů nástroje HP ProtectTools pro malé podniky:

Modul	Klíčové funkce
Konzola pro správu nástroje HP ProtectTools Security Manager	• Průvodce nastavením nástroje Security Manager využívají správci k nastavení a konfiguraci úrovní zabezpečení a metod přihlašování. • Umožňuje konfigurovat možnosti, které jsou běžným uživatelům skryty. • Umožňuje konfigurovat přístup uživatelů a nastavení pro nástroj Device Access Manager. • Nástroje pro správce slouží k přidávání a odebírání uživatelů nástroje HP ProtectTools a zobrazení stavu uživatelů.
HP ProtectTools Security Manager (pro běžné uživatele)	• Umožňuje uspořádat, nastavit a změnit uživatelská jména a hesla. • Umožňuje konfigurovat a měnit přihlašovací údaje uživatelů, například hesla systému Windows a čipové karty. • Umožňuje konfigurovat a měnit nastavení, skartaci a čištění nástroje File Sanitizer. • Zobrazit nastavení modulu Device Access Manager. • Umožňuje konfigurovat předvolby a možnosti zálohování a obnovení.
Modul Credential Manager pro nástroj HP ProtectTools (Password Manager)	• Je určen k ukládání, organizování a ochraně vašich uživatelských jmen a hesel. • Umožňuje nastavení přihlašovacích obrazovek webových stránek a programů pro rychlý a zabezpečený přístup. • Chcete-li uložit uživatelská jména a hesla při přístupu na různé webové stránky, zadejte je do aplikace Password Manager, abyste si je nemuseli pamatovat. Při příští návštěvě stránek aplikace Password Manager údaje automaticky vyplní a data odešle. • Umožňuje vytvářet silnější hesla, která si nemusíte zapisovat ani pamatovat, a přitom zvyšuje zabezpečení vašich účtů.
Drive Encryption for HP ProtectTools	• Poskytuje kompletní šifrování celého obsahu pevného disku. • Vynucuje ověřování před spuštěním s cílem dešifrovat data na pevném disku a získat k nim přístup. • Pomáhá s dodržováním právních a technologických předpisů vztahujících se k ochraně osobních a citlivých dat. • Data chrání před neautorizovaným přístupem šifrováním celého pevného disku. V případě krádeže počítače nebo vyjmutí disku z původního systému a umístění do nového systému tak nebude utajení dat ohroženo.

Modul	Klíčové funkce
File Sanitizer for HP ProtectTools	• Odstraníte-li data v systému Windows, z pevného disku se obsah zcela neodstraní. Systém Windows pouze odstraní odkazy na tato data. Data zůstanou na pevném disku, dokud nedojde k přepsání jiným souborem. S nástrojem File Sanitizer můžete úplně odstranit dokumenty, historii procházení webu, dočasné soubory, atd. • Nástroj umožňuje bezpečné vymazání (nebo ničení) důležitých souborů a složek (osobní informace nebo soubory, data týkající se historie nebo webu a další data) z vašeho počítače a pravidelné čištění pevného disku (přepsání dříve smazaných dat).
Device Access Manager nástroje HP ProtectTools	• Lze jej použít k řízení přístupu k jednotkám médií, USB a dalším hardwarovým zařízením na základě uživatelských profilů. • Umožňuje vám omezit schopnost uživatele ukládat klíčová data. • Brání uživatelům v používání externích úložných zařízení, jako jsou osobní hudební přehrávače, a v kopírování dat z počítače nebo ze sítě. • Brání uživatelům v přenesení virů do systému z externích médií. • Umožňuje zakázat určitou skupinu zařízení (např. přenosná zařízení USB, zapisovatelná zařízení, osobní hudební přehrávače) podle uživatele nebo skupiny uživatelů. Osoba s heslem správce se může přihlásit a zkopírovat informace z počítače, ostatní uživatelé však nikoli.

Popis bezpečnostních produktů HP ProtectTools a příklady jejich běžného využití

Většina bezpečnostních produktů HP ProtectTools je vybavena prostředky ověřování uživatelů (obvykle se jedná o heslo) a zálohou pro správu, která umožňuje získat přístup při ztrátě, zapomenutí či nedostupnosti hesla a nebo kdykoli, když to vyžaduje podnikové zabezpečení.

POZNÁMKA: Některé bezpečnostní produkty HP ProtectTools byly navrženy tak, aby omezovaly přístup k datům. Pokud jsou data pro uživatele příliš důležitá a raději by o ně přišel, než aby byla kompromitována, měla by být zašifrována. Doporučujeme vytvořit zálohu veškerých dat na bezpečném umístění.

Modul Credential Manager (Správce hesel) pro nástroj HP ProtectTools

Credential Manager (součást nástroje Security Manager) je úložiště pro uživatelská jména a hesla. Nejčastěji slouží k ukládání přihlašovacích jmen a hesel pro přístup k Internetu nebo k e-mailové schránce. Nástroj Credential Manager umožňuje automatické přihlášení uživatele k webovým stránkám nebo k e-mailové schránce.

Příklad 1: Jednatelka malé výrobní společnosti uskutečňuje většinu svých podnikových transakcí přes Internet. Také často navštěvuje populární webové stránky, které vyžadují zadání přihlašovacích údajů. Je si dobře vědoma bezpečnostních rizik, a proto nepoužívá ke každému svému účtu stejné heslo. Jednatelka se rozhodla, že bude k zadávání uživatelských jmen a hesel na různých stránkách používat nástroj Credential Manager. Jakmile otevře stránku požadující zadání přihlašovacích údajů, nástroj Credential Manager je zadá automaticky za ni. Svá uživatelská jména a hesla si může v nástroji Credential Manager kdykoli zobrazit.

Nástroj Credential Manager lze také použít ke správě přihlášení. Tento nástroj umožňuje uživateli vybírat jednotlivé webové nebo síťové položky a přímo k nim přistupovat prostřednictvím odkazu. V případě nutnosti si zde uživatel může také prohlížet uživatelská jména a jejich hesla.

Příklad 2: Pracovitý certifikovaný auditor z malé účetní firmy dostal na starosti správu způsobu přihlašování zákazníků k zabezpečeným webovým stránkám, kde zadávají aktuální informace. Certifikovaný účetní chce řídit přístup ke stránkám a sdílet aktuální přihlašovací údaje. Auditor se rozhodne spravovat všechny webové odkazy a s nimi související uživatelská jména a hesla v nástroji Credential Manager for HP ProtectTools. Jakmile auditor zadá všechny potřebné údaje, nasadí nástroj Credential Manager v počítačích zákazníků, aby mohli používat webové účty a nemuseli si pamatovat používané přihlašovací údaje.

Modul Drive Encryption pro nástroj HP ProtectTools

Modul Drive Encryption se nejčastěji používá k omezení přístupu k datům na celém pevném disku počítače nebo na sekundárním pevném disku.

Příklad 1: Lékař si chce být jistý, že pouze on může přistupovat k datům na svém pevném disku. Lékař tedy aktivuje modul Drive Encryption, který umožňuje ověřování před spuštěním nebo vyžaduje ověření před přihlášením k systému Windows. Po nastavení nebude možné pevný disk bez zadání hesla otevřít, a to dokonce ještě před spuštěním operačního systému.

Pokud dojde k odpojení disku, nástroj Drive Encryption for HP ProtectTools nepovolí přístup k šifrovaným datům, která jsou na něm uložena, protože je disk vázán na původní základní desku.

Příklad 2: Správce malé kliniky chce zajistit, aby měli přístup k datům v jejich místním počítači pouze doktoři a oprávnění pracovníci a to bez nutnosti sdílení osobních hesel. Oddělení pro informační technologie přidá správce, doktory a všechny oprávněné pracovníky jako uživatele nástroje Drive Encryption. Od této chvíle se budou moci k počítači přihlašovat pouze oprávnění pracovníci, a to pomocí svého uživatelského jména a hesla.

Modul File Sanitizer pro nástroj HP ProtectTools

Modul File Sanitizer pro nástroj HP ProtectTools slouží k trvalému odstraňování dat, včetně činnosti prohlížeče Internetu, dočasných souborů, dříve odstraněných dat a jiných informací. Modul File Sanitizer lze nakonfigurovat, aby se spouštěl ručně nebo automaticky na základě uživatelem stanoveného plánu.

Příklad 1: Advokát často přichází do styku s citlivými informacemi od svých klientů a chce si být jistý, že data v odstraněných souborech nebude možné obnovit. Advokát použije modul File Sanitizer k bezpečnému odstranění smazaných souborů, a jejich obnovení tak bude téměř nemožné.

Pokud v systému Windows smažete data běžným způsobem, k jejich skutečnému odstranění z pevného disku nedojde. Sektory na pevném disku s těmito daty se pouze označí jako dostupné pro další využití. Dokud nedojde k přepsání dat, jejich obnovení pomocí běžných nástrojů dostupných na Internetu je snadné. Modul File Sanitizer přepíše sektory náhodnými daty (v případě potřeby i několikrát) a učiní tak data nečitelná a neobnovitelná.

Příklad 2: Vědecká pracovnice chce bezpečně odstranit smazaná data, dočasné soubory a činnost prohlížečů automaticky při svém odhlášení. Používá modul File Sanitizer umožňující bezpečné odstranění, takže může vybrat běžné soubory nebo kterékoli vlastní soubory, aby byly trvale odstraňovány automaticky.

Modul Device Access Manager pro nástroj HP ProtectTools

Modul Device Access Manager pro nástroj HP ProtectTools lze použít k blokování neoprávněného přístupu k jednotkám USB flash, odkud by mohlo dojít ke zkopírování dat. Příkladem využití modulu může být situace, kdy externí dodavatelé potřebují přístup k podnikovým počítačům, ale chcete jim zabránit v kopírování dat na jednotku USB. Modul Device Access Manager pro nástroj HP ProtectTools umožňuje správci omezit a spravovat přístup k hardwaru. Pomocí něj lze také omezit přístup k jednotkám CD/DVD a řídit přístup k zařízením USB nebo používání síťového připojení.

Příklad 1: Manažer malé firmy dodávající zdravotnické potřeby často zároveň pracuje s lékařskými záznamy a s informacemi o své společnosti. Zaměstnanci potřebují mít k těmto datům přístup, ale nesmí je z počítače vynášet pomocí jednotky USB nebo jiných externích úložných médií. Síť je sice zabezpečená, ale počítače jsou vybaveny vypalovacími mechanikami disků CD a porty USB, které mohou být zneužity ke zkopírování nebo krádeži dat. Manažer použije nástroj Device Access Manager k zakázání portů USB a vypalovacích mechanik disků CD, aby je zaměstnanci nemohli používat. Přestože budou porty USB blokovány, k nim připojené myši a klávesnice budou i nadále fungovat.

Příklad 2: Malá pojišťovna nechce, aby její zaměstnanci instalovali do počítačů osobní software nebo aby do nich nahrávali data z domova. Někteří zaměstnanci potřebují přístup k portům USB na všech počítačích. Správce informačních technologií použije nástroj Device Access Manager k povolení přístupu pro některé ze zaměstnanců, zatímco ostatním bude externí přístup i nadále zablokován.

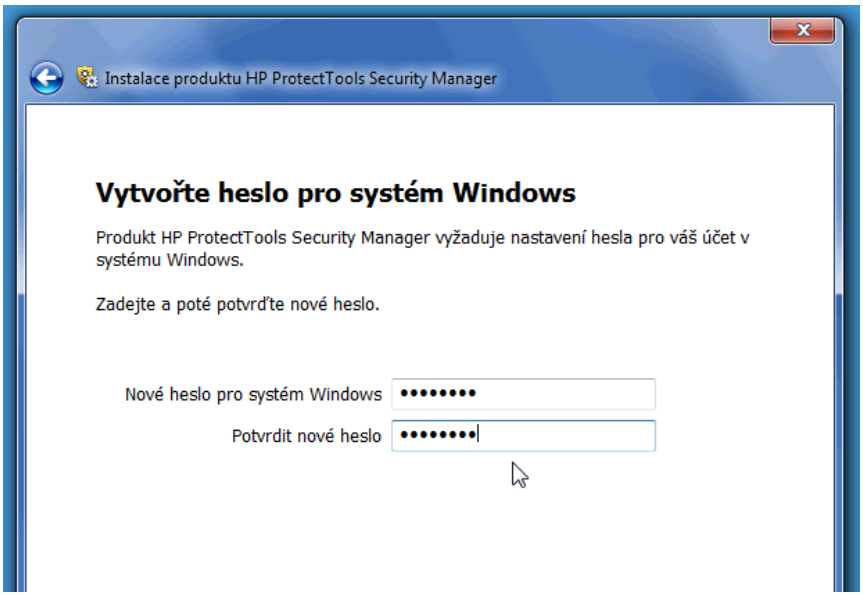
2 Příručka jednoduchého nastavení nejužitečnějších možností

Tato příručka jednoduchého nastavení vás provede základními kroky, které se týkají aktivace nejběžnějších a nejužitečnějších možností v nástroji HP ProtectTools pro malé podniky. V tomto softwaru je k dispozici řada nástrojů a možností, které vám umožní zvolit ty nejvhodnější funkce a nastavit řízení přístupu. V příručce jednoduchého nastavení najdete postupy, díky kterým spustíte každý modul v té nejkratší možné době, a to s minimálním úsilím. Máte-li zájem o další informace, vyberte konkrétní modul a klepněte na symbol „?“ nebo na tlačítko Nápověda v pravém horním rohu. Získáte informace, které vám pomohou s aktuálně zobrazeným oknem.

Začínáme

1. Nástroj HP ProtectTools Security Manager otevřete pomocí ikony miniaplikace, ikony v panelu nástrojů (zlatý štít) nebo klepnutím na položky **Start** > **Všechny programy** > **HP**.

2. Zadejte své heslo pro systém Windows nebo si heslo vytvořte.

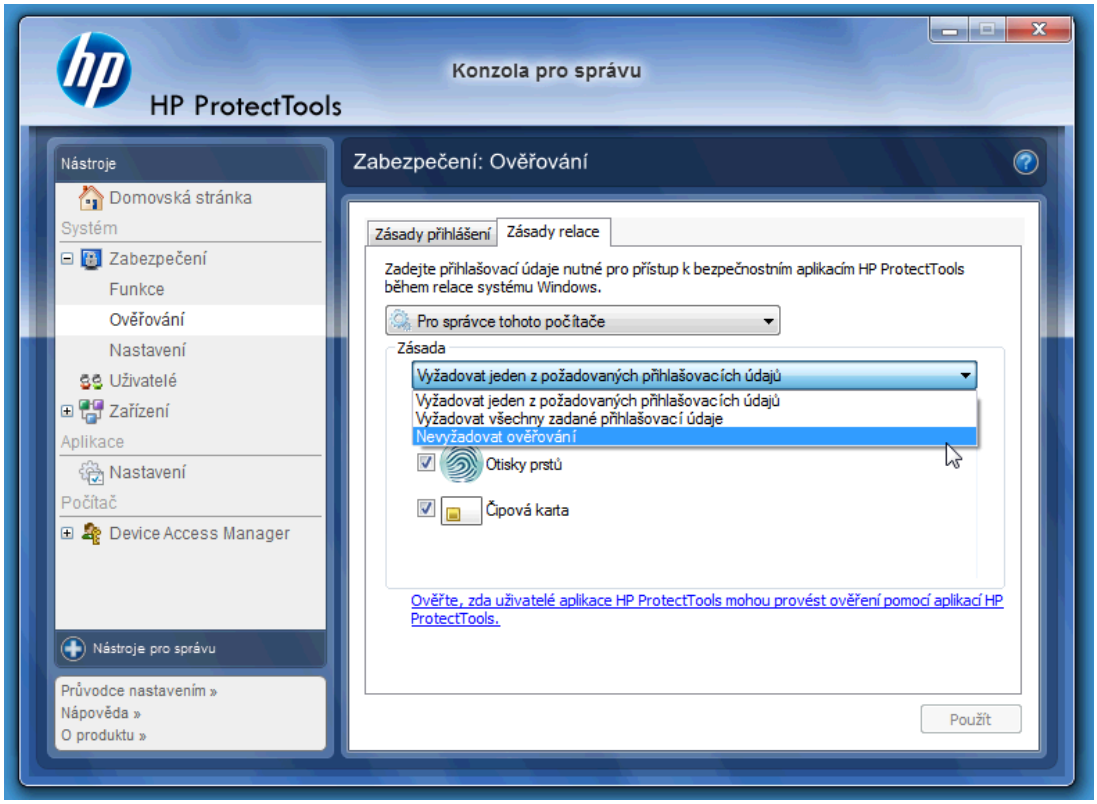


3. Dokončete průvodce nastavením.

POZNÁMKA: Ve výchozím nastavení je v nástroji HP ProtectTools Security Manager nastavena zásada silného ověřování.

Toto nastavení brání neoprávněnému přístupu, když jste přihlášeni k systému Windows, a velmi dobře se osvědčuje v situacích, kdy je nezbytné vysoké zabezpečení, nebo pokud uživatelé odcházejí během dne často od systému. Chcete-li toto nastavení změnit, klepněte na kartu Zásady relace a nastavení změňte.

Chcete-li nastavit nástroj HP ProtectTools Security Manager tak, aby používal pouze úvodní přihlášení systému Windows pro celou relaci, změňte následující nastavení.



Nastavení nástroje HP ProtectTools Security Manager, aby provedl pouze jedno ověření během přihlášení k systému Windows:

1. Klepněte na položky **Start** > **Všechny programy** > **HP** > **Konzola pro správu nástroje HP ProtectTools**.
2. V levém panelu **Nástroje** vyberte možnost **Ověřování** ze skupiny **Zabezpečení**.
3. Klepněte na kartu **Zásady relace** a vyberte možnost **Nevyžadovat ověřování** z rozevírací nabídky v části **Zásady**.
4. Po dokončení klepněte na tlačítko **Použít**.

Modul Credential Manager pro nástroj HP ProtectTools (Password Manager)

Hesla! Všichni jich používáme poměrně dost – především v případě, že pravidelně navštěvujeme některé webové stránky nebo používáme aplikace, které vyžadují přihlášení. Běžný uživatel buď používá pro všechny aplikace a webové stránky stejné heslo, nebo popustí uzdu fantazii a následně rychle zapomene, ke které aplikaci které heslo patří.

Nebylo by hezké, kdyby si software automaticky pamatoval vaše hesla k webům, které nejsou výjimečně důležité, nebo vám umožnil určit, které weby si pamatovat a které nikoliv? Modul Credential Manager pro nástroj HP ProtectTools je přesně to, potřebujete. Modul Credential Manager je správce hesel, který vám tyto možnosti nabízí. Jakmile se přihlásíte k počítači, modul Credential Manager vám poskytne vaše hesla a přihlašovací údaje, které potřebujete.

Pokud přejdete k aplikaci nebo webu, který vyžaduje přihlašovací údaje, modul Credential Manager web automaticky rozpozná a zeptá se vás, zda chcete, aby si vaše údaje pamatoval. Pokud budete

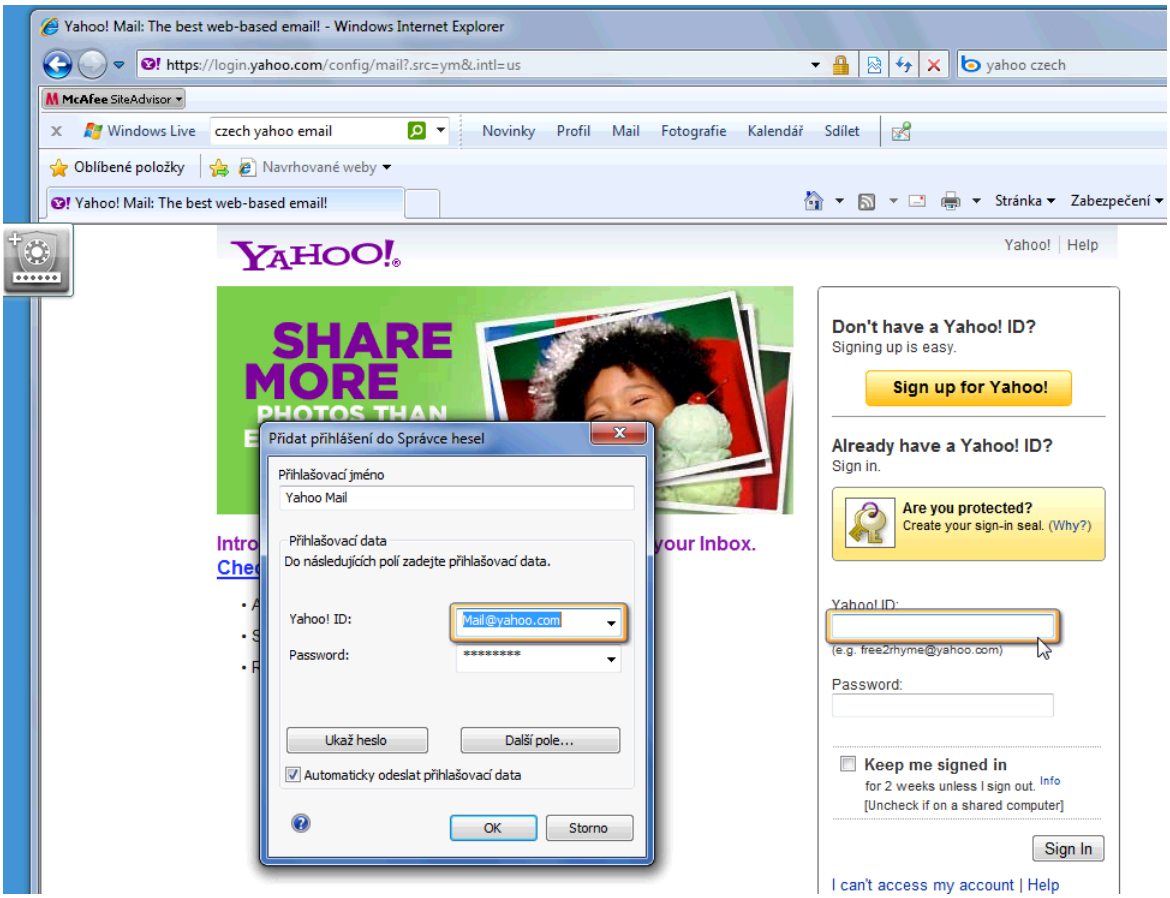
souhlasit, nebudete si již heslo muset pamatovat. Požadavek na zapamatování informací můžete odmítnout, pokud chcete některé weby vyloučit.

Zahájení ukládání webových umístění, uživatelských jmen a hesel:

1. Přejděte například ke svému webovému poštovnímu účtu a přikažte modulu Credential Manager (klepněte na jeho ikonu), aby si web přidal.

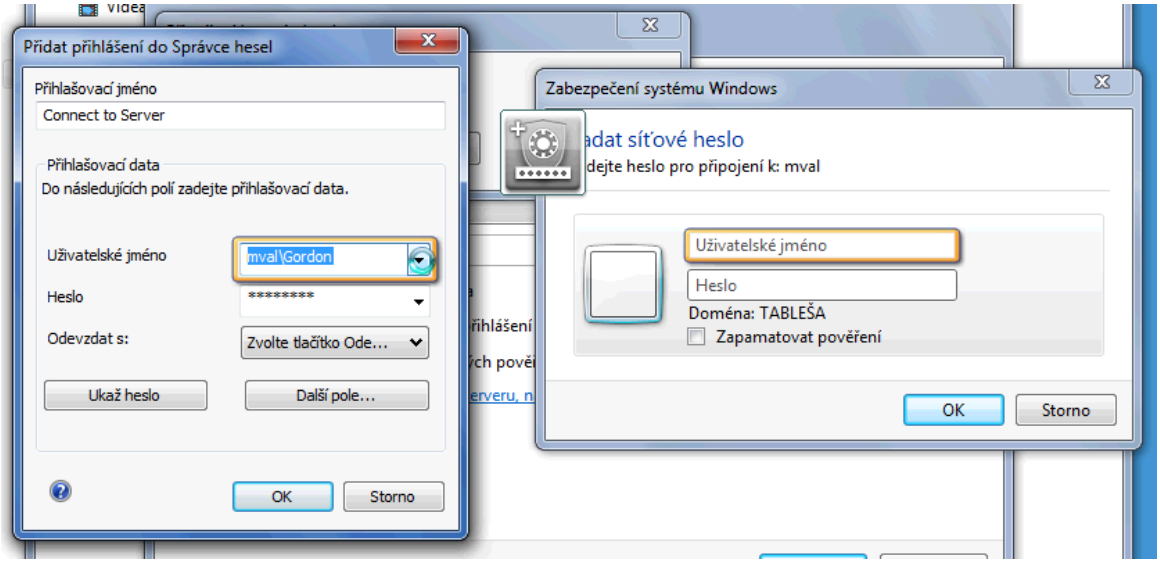
2. Odkaz pojmenujte (volitelné) a do modulu Credential Manager zadejte uživatelské jméno a heslo.

POZNÁMKA: Webová stránka zvýrazní oblasti, které modul Credential Manager použije pro aktuální a následující návštěvy.



3. Po dokončení klepněte na tlačítko **OK**.

4. Modul Credential Manager může také uložit vaše uživatelská jména a hesla pro sdílená místa v síti nebo pro mapování síťových jednotek.



Zobrazení a správa uloženého ověřování v modulu Credential Manager

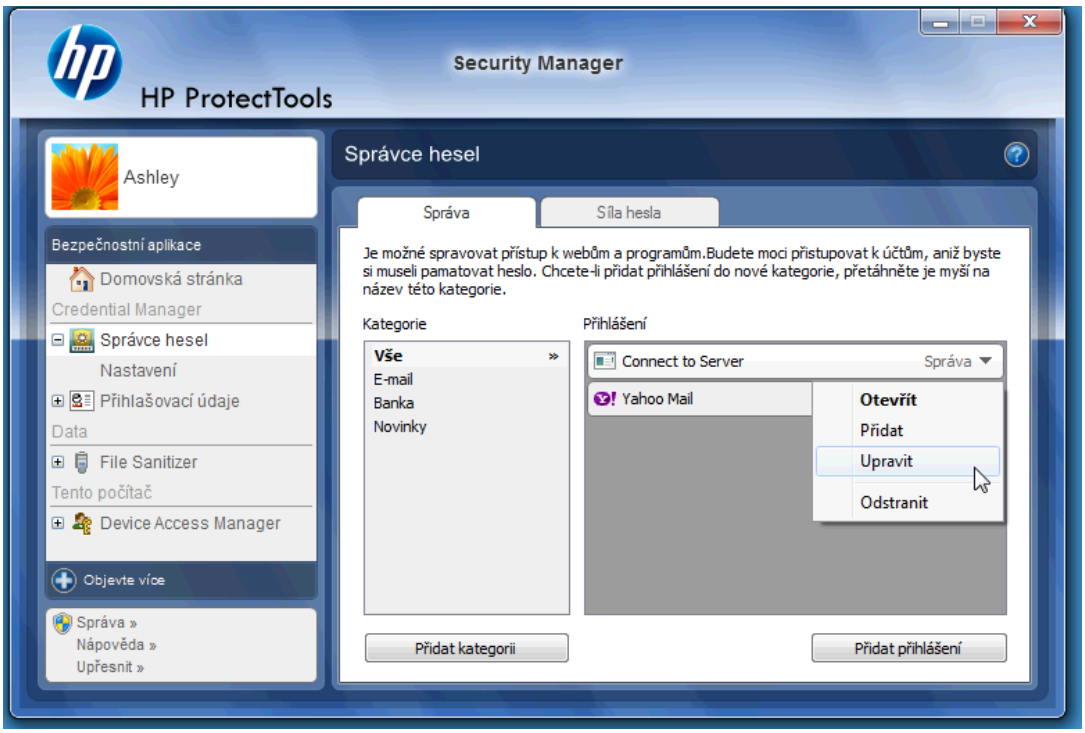
Mezi výhody modulu Credential Manager patří možnost zobrazit, spravovat, zálohovat a spouštět ověřování z centrálního umístění. Modul Credential Manager podporuje také spouštění uložených stránek ze systému Windows.

Chcete-li otevřít aplikaci Password Manager, použijte jeden ze dvou následujících způsobů:

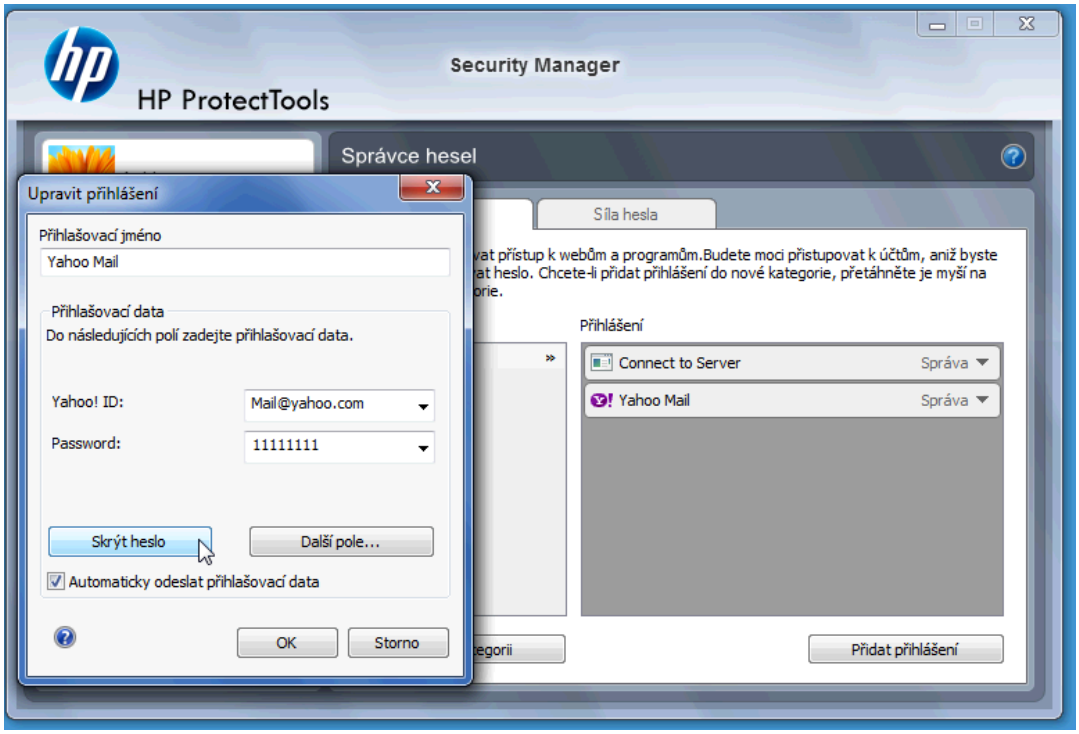
- Pomocí kombinace kláves Ctrl + Windows + H otevřete aplikaci Password Manager. Vybráním možnosti **Otevřít** provedete spuštění a ověření uloženého zástupce.

NEBO

- Vyberte kartu **Správa** v aplikaci Password Manager a otevřete nástroj HP ProtectTools Security Manager, kde můžete přihlašovací údaje upravit.



Možnost **Upravit** modulu Credential manager vám umožní zobrazit a upravit název, přihlašovací jméno, a dokonce i zjistit hesla.



Nástroj HP ProtectTools pro malé podniky umožní zálohování a kopírování přihlašovacích údajů do jiného počítače.


HP ProtectTools
Security Manager
Ashley
Bezpečnostní aplikace
Domovská stránka
Credential Manager
Správce hesel
Nastavení
Přihlašovací údaje
Data
File Sanitizer
Tento počítač
Device Access Manager
Objevte více
Správa »
Nápověda »
Upřesnit »
Předvolby »
Zálohování a obnovení dat »
O produktu »
Zálohování a obnovení dat
Průvodce zálohováním a obnovou HP ProtectTools vám pomůže v bezpečném zálohování dat spravovaných aplikacemi HP ProtectTools. Tato data lze obnovit na kterémkoli počítači s nainstalovaným softwarem HP ProtectTools.
Přihlašovací údaje, například otisky prstů, se nezálohují.
Vyberte požadovanou akci.
Zálohovat data
Obnovit data
Zobrazit protokol zálohování a obnovy

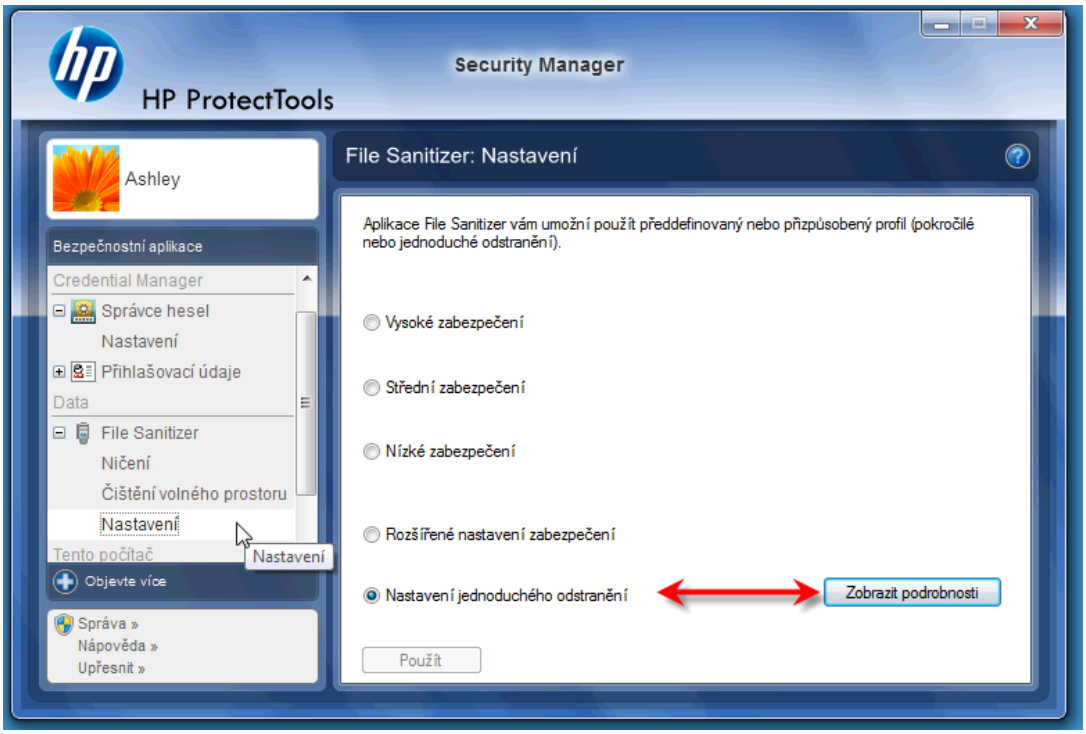
File Sanitizer for HP ProtectTools

Nástroj File Sanitizer zajišťuje, aby obnovení vámi odstraněných dat bylo pro neoprávněné osoby minimálně velmi obtížné. K dispozici máte několik možností pro ruční smazání nebo nastavení pravidelného mazání vybraných souborů a složek, včetně historie prohlížeče.

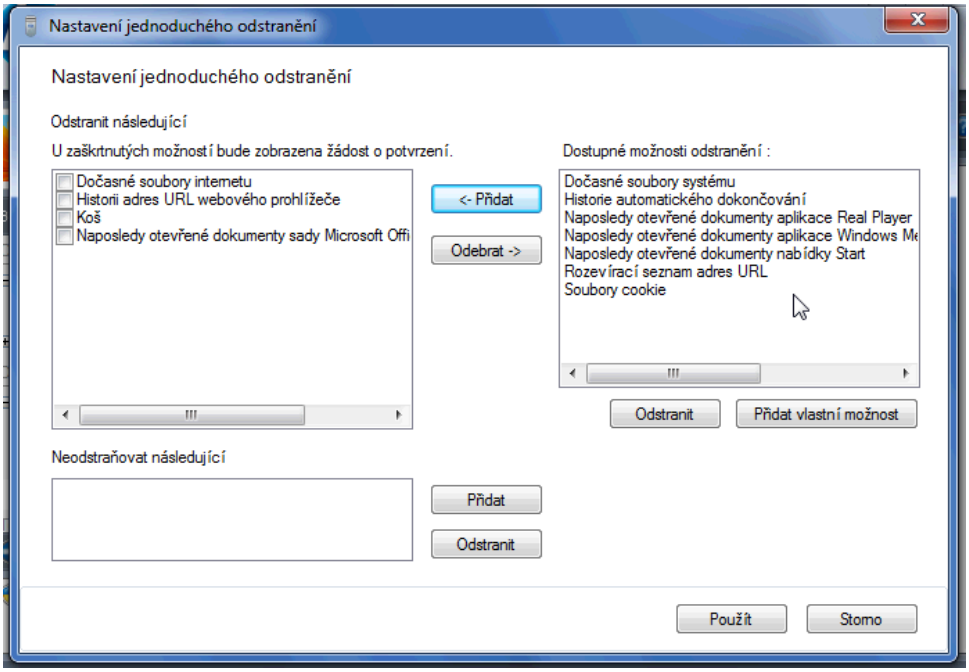
Níže je uvedeno několik jednoduchých konfigurací.

Chcete-li začít trvale mazat odstraněná data, vyberte soubor nebo složky, které již nepotřebujete.

1. Přejděte do části **Security Manager** > **File Sanitizer** > **Nastavení**. Vyberte možnost **Nastavení jednoduchého odstranění** a klepněte na tlačítko **Zobrazit podrobnosti**.



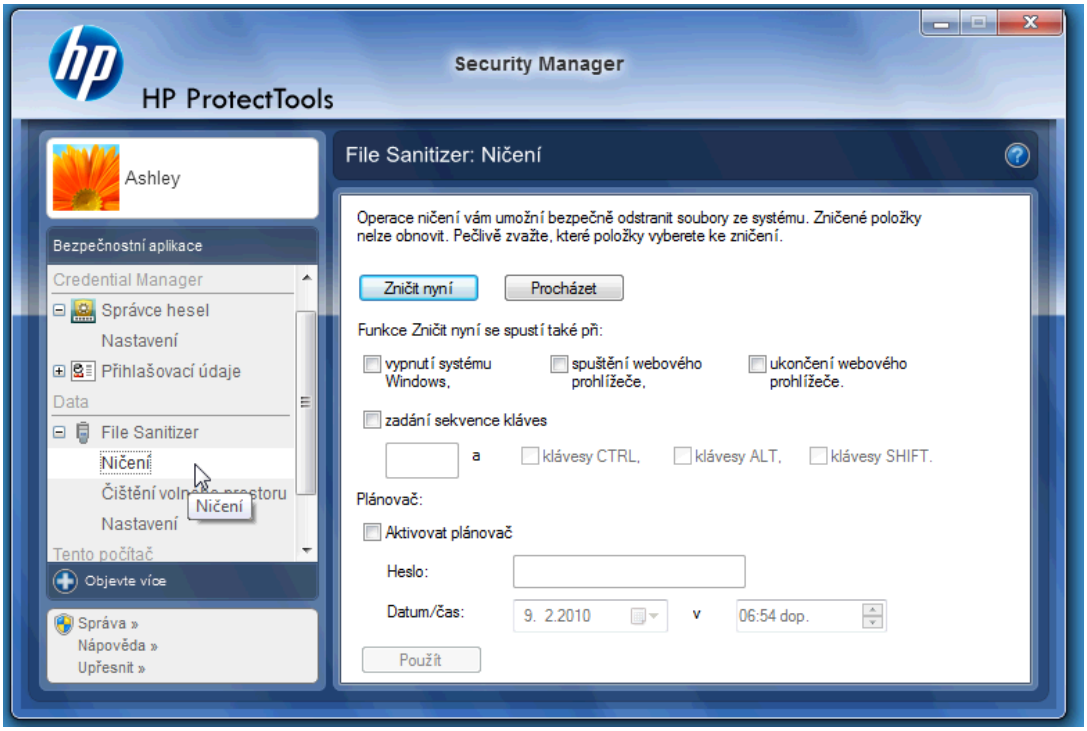
2. V pravé části okna Nastavení jednoduchého odstranění vyberte položky, které chcete pravidelně trvale odstraňovat, a klepněte na tlačítko **<-Přidat**, čímž vybrané položky přesunete do části Odstranit.



3. Nejprve vyberte položku Koš a pak přidávejte další položky, které chcete smazat nebo zničit.

4. Jakmile vyberete vše, co chcete trvale odstraňovat, klepněte na tlačítko **Použít**.

5. Přejděte k možnosti **Ničení** a nastavte, kdy se má akce provést. Tlačítko **Zničit nyní** okamžitě smaže položky vybrané v okně Nastavení jednoduchého odstranění, které jste právě potvrdili.



6. V panelu nástrojů se při každém spuštění a dokončení Ničení zobrazí malá bublina.

Device Access Manager nástroje HP ProtectTools

Nástroj Device Access Manager lze použít k omezení použití různých interních a externích úložných zařízení, aby vaše data zůstala v bezpečí pevného disku a nemohla být vynesena z vašeho podniku. Můžete například umožnit přístup k datům, ale zablokovat jejich kopírování na disky CD, osobní hudební přehrávače nebo paměťová zařízení USB. Níže naleznete jednoduchý postup, jak tuto funkci nastavit.

1. Klepněte na položky **Start** > **Všechny programy** > **HP** > **Konzola pro správu** > **Device Access Manager** > **Jednoduchá konfigurace**.

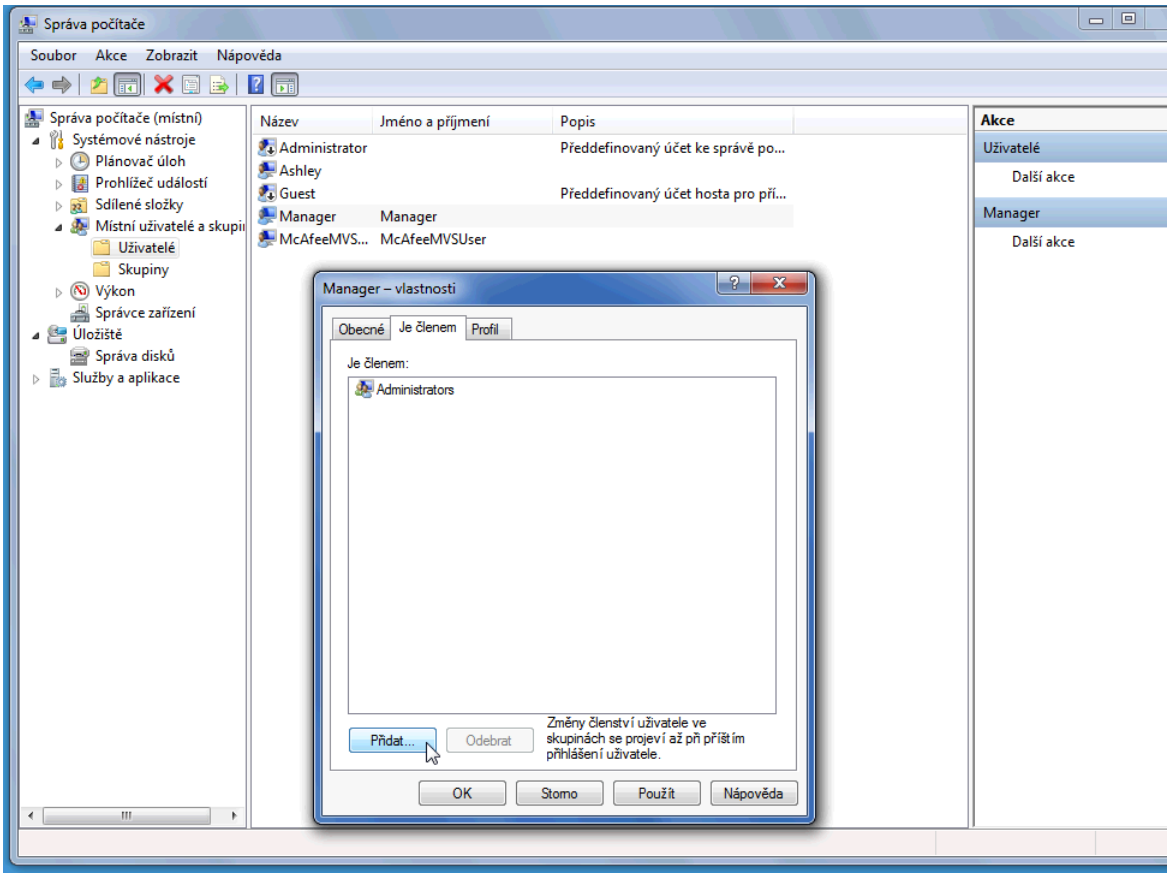
2. Vyberte hardwarová zařízení, která chcete omezit, a klepnutím na tlačítko **Použít** proces dokončete.

3. Prostřednictvím dalšího níže uvedeného kroku můžete vybrat, komu bude i nadále přístup povolen, zatímco ostatní budou zablokováni.

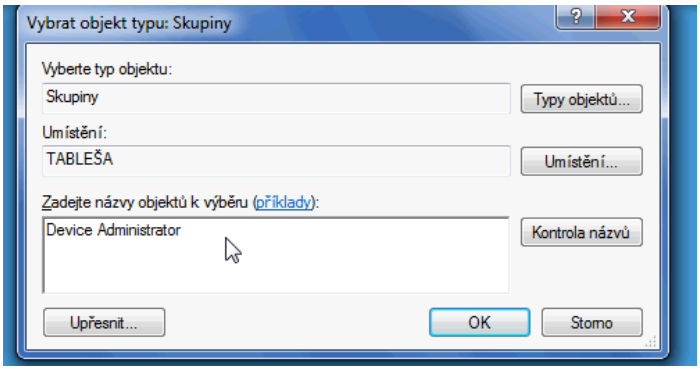
4. Přejděte do části **Tento počítač**, klepněte pravým tlačítkem myši a vyberte možnost **Spravovat** > **Správa počítače** > **Systémové nástroje** > **Místní uživatelé a skupiny** > **Uživatelé**.

5. Klepněte na uživatele (v tomto příkladě na možnost „Manager“), kterým chcete ponechat přístup k blokovanému hardwaru.

6. Na kartě **Je členem** klepněte na tlačítko **Přidat**.



7. V okně **Vybrat objekt typu: Skupiny** můžete použít možnost **Upřesnit** nebo zadat skupinu „Device Administrator“. Klepnutím na tlačítko **OK** okna zavřete. Abyste získali oprávnění, musíte se odhlásit a znovu přihlásit.



Nyní budou interní a externí úložná zařízení, včetně disků CD, USB, osobních hudebních přehrávačů atd. funkční pouze pro osobu (osoby) patřící do skupiny „Device Administrator“.

Nástroj Drive Encryption for HP ProtectTools

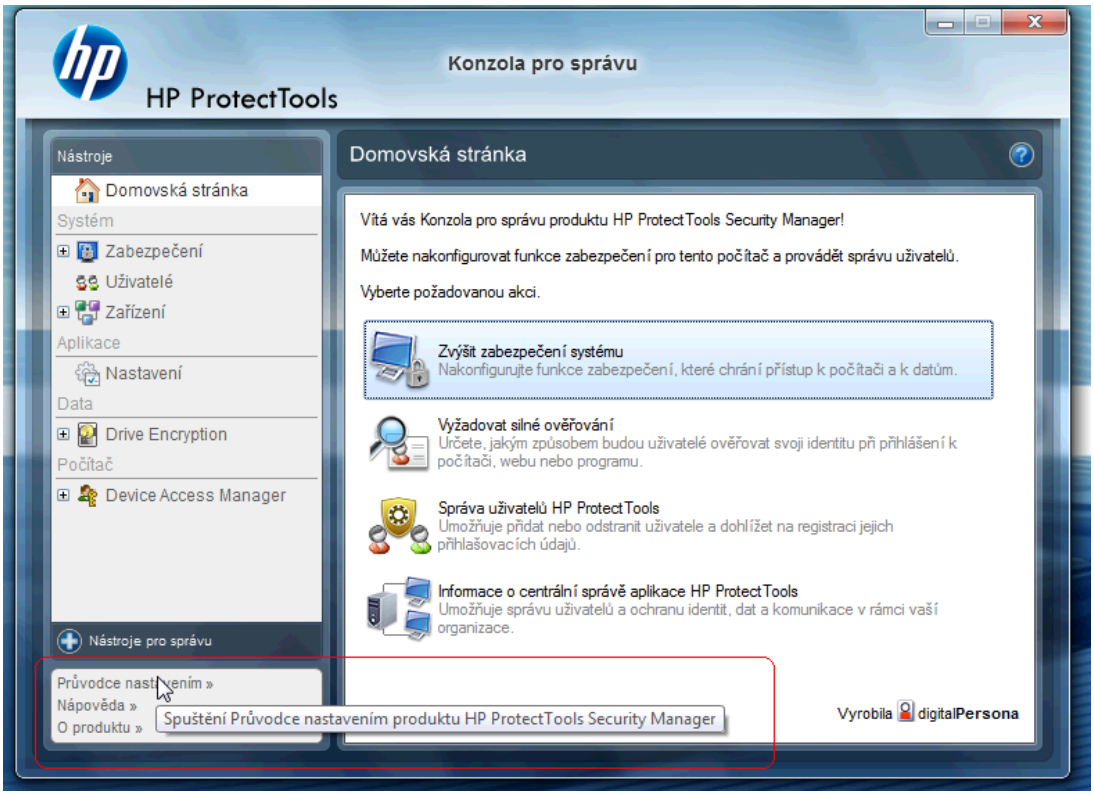
Nástroj Drive Encryption for HP ProtectTools je software chránící data šifrováním celého pevného disku. Data na pevném disku budou chráněna i v případě krádeže počítače nebo vyjmutí disku z původního systému a umístění do nového systému.

Další bezpečnostní výhodou softwaru Drive Encryption je vyžadování zadání přihlašovacího jména a hesla při spouštění systému. Tento postup se nazývá Ověření před spuštěním.

Uživatelé systému Windows mají situaci snadnější – domény, nástroj Credential Manager for HP ProtectTools a HP ProtectTools Security Manager komunikují se softwarem Drive Encryption a umožňují synchronizaci hesel.

Pokud chcete aktivovat nástroj Drive Encryption for HP ProtectTools, postupujte podle těchto pokynů.

1. Klepněte na nabídku **Start** > **Všechny programy** > **HP** > **HP ProtectTools Administrative Console** > **Management Tools** > **Setup Wizard**. Zobrazí se tato informace:



2. Na úvodní obrazovce vyberte možnost **Další**.

3. Aktivace průvodce vyžaduje zadání hesla pro systém Windows. Poté klepněte na možnost **Další**.

4. Zaškrtněte políčko **Drive Encryption** a vyberte možnost **Další**.

5. V konfiguračním okně softwaru Drive Encryption se zobrazí dostupné disky, které lze zašifrovat. K uložení dešifrovacího klíče je nutné připojit jednotku USB. Tento dešifrovací klíč uchovávejte na bezpečném místě, protože slouží k obnovení dat a přístupu k disku v případě, že ztratíte heslo.

6. Vyberte možnost **Další**, dokončete postup a vyberte možnost **Dokončit**. Po výzvě odpojte jednotku USB a restartujte systém.

7. Až se systém na pevném disku spustí, software Drive Encryption bude vyžadovat zadání hesla pro systém Windows. Zadejte heslo a klepněte na tlačítko **OK**.

POZNÁMKA: Během šifrování se může zdát, že počítač běží pomalu. Jakmile bude šifrování dokončeno, systém se vrátí do běžného provozu. Při přístupu k datům na disku budou data automaticky šifrována a dešifrována.

Nezapomeňte, že autorizace k nástroji Drive Encryption je automaticky převzata Správcem Pověření systému Windows. Nemusíte tedy své heslo zadávat dvakrát.

3 Výhody nástroje HP ProtectTools pro malé podniky

Přístup k zabezpečovacímu softwaru nástroje HP ProtectTools pro malé podniky

Chcete-li získat přístup k nástroji HP ProtectTools Security Manager pomocí nabídky Start systému Windows, postupujte takto:

▲ V systému Windows klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP ProtectTools Security Manager**.

Chcete-li získat přístup ke Konzole pro správu nástroje HP ProtectTools Security Manager pomocí nabídky Start systému Windows, postupujte takto:

▲ V systému Windows klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.

Dosažení hlavních cílů zabezpečení

Moduly HP ProtectTools mohou vzájemně spolupracovat a poskytovat tak řešení pro celou řadu problémů se zabezpečením, včetně následujících hlavních cílů zabezpečení:

- Omezení přístupu k citlivým datům
- Prevence neoprávněného přístupu z interních a externích míst
- Zásady vytváření silných hesel

Omezení přístupu k citlivým datům

Předpokládejme, že na pracovišti působí externí auditor, který má přístup k počítačům za účelem kontroly citlivých finančních dat. Chcete však zamezit tomu, aby si auditor mohl tisknout soubory nebo je ukládat na zapisovatelná zařízení, například na CD. Následující funkce pomáhá omezit přístup k datům:

Modul Device Access Manager for HP ProtectTools umožňuje správcům omezit přístup k zapisovatelným zařízením, takže není možné tisknout citlivé informace nebo je kopírovat z pevného disku na vyměnitelná média. Viz Konfigurace tříd zařízení (pokročilá funkce) na stránce 52.

Prevence neoprávněného přístupu z interních a externích míst

Neoprávněný přístup k nezabezpečeným kancelářským počítačům představuje velmi reálné riziko pro kritická data, jako jsou informace z finančního oddělení, od vedoucího nebo od týmu pro výzkum a vývoj, a pro soukromé informace, například záznamy pacientů nebo osobní finanční záznamy. Následující funkce pomáhají neoprávněnému přístupu k datům zabránit:

- Je-li aktivována funkce ověřování před spuštěním, pomáhá zabránit v přístupu k operačnímu systému. Viz následující kapitoly:
  - Modul Credential Manager pro nástroj HP ProtectTools (Password Manager) na stránce 39
  - Drive Encryption for HP ProtectTools na stránce 36
- Modul Credential Manager for HP ProtectTools pomáhá zabránit neoprávněným uživatelům v přístupu k heslům či k aplikacím chráněným heslem. Viz následující kapitola:
  - Modul Credential Manager pro nástroj HP ProtectTools (Password Manager) na stránce 39
- Modul Device Access Manager for HP ProtectTools umožňuje správcům omezit přístup k zapisovatelným zařízením, takže není možné kopírovat citlivé informace z pevného disku. Viz následující kapitola:
  - Device Access Manager for HP ProtectTools na stránce 51
- Nástroj File Sanitizer umožňuje bezpečné odstraňování dat prostřednictvím zničení kritických souborů a složek nebo vyčištění volného prostoru na pevném disku (přepsání dat, která již byla odstraněna, avšak jsou na pevném disku stále přítomna, aby se ztížilo jejich případné obnovení). Viz následující kapitola:
  - File Sanitizer for HP ProtectTools na stránce 44

Zásady vytváření silných hesel

Je-li vyžadováno použití zásad pro vytváření silných hesel (komplikované heslo, které nelze jednoduše odhalit) pro přístup k webovým aplikacím a databázím, modul Credential Manager for HP ProtectTools poskytuje chráněné úložiště hesel a funkci Jednotné přihlášení. Viz následující kapitola:

- Modul Credential Manager pro nástroj HP ProtectTools (Password Manager) na stránce 39

Další prvky zabezpečení

Přiřazení rolí zabezpečení

Jeden z důležitých postupů správné ochrany dat spočívá v rozdělení odpovědností a práv mezi různé typy správců a uživatelů.

POZNÁMKA: V malé organizaci nebo při soukromém použití může všechny tyto role zastávat jedna osoba.

V případě produktu HP ProtectTools pro malé podniky lze práva a povinnosti související se zabezpečením rozdělit do následujících rolí:

- Správce – zavádí a spravuje prvky zabezpečení. Může také povolit nebo zakázat některé funkce.
- Uživatel – používá prvky zabezpečení.

Správa hesel produktu HP ProtectTools

Většina funkcí nástroje HP ProtectTools Security Manager je chráněna hesly. V následující tabulce jsou uvedena běžně používaná hesla, softwarové moduly, ve kterých jsou daná hesla nastavena, a funkce těchto hesel.

V této tabulce jsou uvedena i hesla, která mohou nastavit a používat pouze správci. Všechna ostatní hesla mohou nastavovat běžní uživatelé.

Heslo nástroje HP ProtectTools	Nastaveno v tomto modulu nástroje HP ProtectTools	Funkce
Přihlašovací heslo pro nástroj Správce hesel	Správce hesel	Toto heslo nabízí dvě možnosti: • Po přihlášení k systému Windows může být použito k samostatném přihlášení do nástroje Správce hesel. • Může nahradit proces přihlášení k systému Windows, takže zajistí přístup k systému Windows a současně i k nástroji Správce hesel.
Heslo pro nástroj Computer Setup **POZNÁMKA:** Také se označuje jako heslo správce systému BIOS, nástroje F10 Setup nebo nastavení zabezpečení.	Systém BIOS, zajišťují správci	Chrání přístup k nástroji Computer Setup.
Heslo po zapnutí	BIOS	Chrání přístup k obsahu počítače po zapnutí a restartování počítače nebo návratu počítače z režimu hibernace.
Přihlašovací heslo systému Windows	Ovládací panely systému Windows	Lze použít pro ruční přihlášení.

Vytvoření silného hesla

Při vytváření hesel je v první řadě třeba řídit se specifikacemi stanovenými příslušným programem. Následující obecné pokyny vám pomohou vytvořit silné heslo a snížit riziko prozrazení hesla:

- Použijte heslo delší než 6 znaků, v ideálním případě delší než 8 znaků.
- V rámci hesla střídejte velká a malá písmena.
- Pokud je to možné, střídejte alfanumerické znaky a použijte v hesle zvláštní znaky a interpunkční znaménka.

- Některá písmena v klíčovém slově nahraďte zvláštními znaky nebo čísly. Můžete například nahradit písmena I nebo L číslicí 1.
- Kombinujte slova ze dvou či více jazyků.
- Rozdělte slovo nebo slovní spojení čísly či zvláštními znaky, například: „Mary2-2Cat45“.
- Nepoužívejte hesla, která by se mohla samostatně objevit ve slovníku.
- Nepoužívejte v hesle své jméno ani žádné osobní informace, jako je datum narození, jména domácích mazlíčků nebo rodné jméno matky, a to ani pozadu.
- Hesla pravidelně obměňujte. Můžete změnit pouze některé znaky.
- Pokud si heslo zapíšete, neukládejte je na dobře viditelné místo v blízkosti počítače.
- Neukládejte heslo do souboru v počítači, například do e-mailu.
- Nesdílejte účty a své heslo nikomu nesdělujte.

Zálohování přihlašovacích údajů a nastavení

Použijte nástroj zálohování a obnovy v aplikaci HP ProtectTools Security Manager jako centrální úložiště, ze kterého můžete zálohovat a obnovit přihlašovací údaje zabezpečení z nainstalovaných modulů softwaru HP ProtectTools.

4 Konzola pro správu nástroje HP ProtectTools Security Manager

O Konzole pro správu nástroje HP ProtectTools

Konzola pro správu zajišťuje správu nástroje HP ProtectTools Security Manager.

Pomocí konzoly může místní správce provádět tyto úkony:

- Povolovat nebo zakazovat funkce zabezpečení
- Spravovat uživatele počítače
- Upravovat parametry jednotlivých zařízení
- Konfigurovat aplikace nástroje Security Manager
- Přidávat do nástroje Security Manager další aplikace

Používání Konzoly pro správu

Konzola pro správu nástroje Security Manager představuje centrální umístění pro správu nástroje HP ProtectTools Security Manager.

Otevření konzoly:

- Klikněte na položky **Start** > **Všechny programy** > **Konzola pro správu nástroje HP ProtectTools**, nebo:
- Klikněte na odkaz **Správa** v levém dolním rohu konzoly Security Manager.

Konzola pro správu se skládá ze dvou podoken – z levého a pravého podokna. Levé podokno obsahuje nástroje pro správu. Pravé podokno obsahuje pracovní oblast umožňující konfiguraci těchto nástrojů.

Levé podokno Konzoly pro správu obsahuje tyto položky:

- **Domovská stránka** – poskytuje rychlý přístup k často používaným úkonům, včetně aktivace funkcí zabezpečení, určení přihlašovacích údajů a správy uživatelů.
- **Systém** – umožňuje správu konfigurace celosystémových funkcí zabezpečení, uživatelů a ověřovacích zařízení, jako jsou čtečky čipových karet.
- **Aplikace** – obsahuje nástroje pro konfiguraci chování nástroje Security Manager a jeho aplikací.
- **Data** – nabízí nástroje pro zálohování a obnovení šifrovacích klíčů.

- **Počítač** – poskytuje rozšířené volby zabezpečení umožňující deaktivaci jednotlivých typů zařízení, která by mohla ohrozit zabezpečení počítače, a stanovení přístupových práv pro různé uživatele a skupiny.
- **Nástroje pro správu** – otevře ve výchozím prohlížeči webovou stránku obsahující další aplikace a nástroje pro správu, které rozšiřují funkce nástroje Security Manager. Stránka nabízí také upozorňování na nové aplikace a aktualizace, které jsou k dispozici.
- **Odkazy** – obsahuje následující možnosti:
  - **Průvodce nastavením** – spustí Průvodce nastavením, který vás provede úvodní konfigurací nástroje Security Manager.
  - **Nápověda** – otevře soubor nápovědy, který obsahuje informace o nástroji Security Manager a jeho aplikacích.
  - **O produktu** – zobrazí informace o produktu Security Manager, včetně čísla verze a informací o autorských právech.

Začínáme s průvodcem nastavením

Pro správu nástroje HP ProtectTools Security Manager je třeba mít k dispozici oprávnění správce.

Průvodce nastavením nástroje HP ProtectTools Security Manager vás provede nastavením funkcí zabezpečení. Konzola nástroje HP ProtectTools Security Manager však nabízí celou řadu dalších funkcí. Nastavení v průvodci a další bezpečnostní funkce lze konfigurovat prostřednictvím konzoly, kterou je možné spustit z nabídky Start systému Windows nebo pomocí odkazu v Konzole pro správu Tato nastavení budou použita pro počítač a všechny uživatele, kteří počítač sdílejí.

Při prvním přihlášení k systému Windows budete vyzváni k nastavení nástroje HP ProtectTools Security Manager. Kliknutím na tlačítko **OK** spustíte Průvodce nastavením nástroje Security Manager, který vás provede základními kroky při konfiguraci programu.

POZNÁMKA: Průvodce zabezpečením můžete spustit také kliknutím na položku **Průvodce zabezpečením** v dolní části levého podokna Konzoly pro správu.

Podle pokynů na obrazovkách Průvodce nastavením dokončete nastavení.

Pokud nastavení pomocí průvodce nedokončíte, průvodce se bude automaticky spouštět do té doby, než kliknete na možnost **Tohoto průvodce již příště nezobrazovat**.

Chcete-li používat aplikace nástroje HP ProtectTools Security Manager, spusťte nástroj HP ProtectTools Security Manager z nabídky **Start** nebo kliknutím pravým tlačítkem myši na ikonu **Security Manager** v oznamovací oblasti hlavního panelu. Nástroj Security Manager a jeho aplikace jsou k dispozici všem uživatelům, kteří sdílejí tento počítač.

Konfigurace systému

Skupinu aplikací **Systém** otevřete pomocí nabídky **Nástroje** v levé části Konzoly pro správu.

Pomocí aplikací z této skupiny můžete konfigurovat a spravovat zásady a nastavení pro tento počítač, jeho uživatele a zařízení.

Skupina Systém zahrnuje následující aplikace:

- **Zabezpečení** – spravuje funkce zabezpečení, zásady ověřování a další nastavení ovlivňující způsob ověřování uživatelů při přihlášení k počítači nebo aplikacím nástroje HP ProtectTools.
- **Uživatelé** – umožňuje nastavení, správu a registraci uživatelů tohoto počítače.
- **Zařízení** – spravuje zařízení pro bezpečnostní zařízení, která jsou v počítači vestavěna nebo jsou k němu připojena.

Aktivace funkcí zabezpečení

Funkce zabezpečení, které zde aktivujete, se vztahují na všechny uživatele tohoto počítače.

1. V levém podokně Konzoly pro správu rozbalte nabídku **Zabezpečení** a klikněte na možnost **Funkce**.
2. Chcete-li aktivovat některou funkci zabezpečení, u možnosti **Zabezpečení přihlášení do systému Windows** či **Drive Encryption** zaškrtněte příslušné políčko.
   - **Zabezpečení přihlášení do systému Windows** – chrání účty systému Windows tím, že vyžaduje přístup pomocí určitých přihlašovacích údajů.
   - **Drive Encryption** – chrání data pomocí šifrování pevných disků, takže jsou informace pro uživatele bez patřičného oprávnění nečitelné.
3. Klikněte na tlačítko **Další**.
4. Klikněte na tlačítko **Použít**.

Definování zásad ověřování nástroje Security Manager

Zásady ověřování nástroje Security Manager pro tento počítač se určují na dvou kartách (Přihlášení a Relace), které obsahují přihlašovací údaje nezbytné pro ověření všech tříd uživatelů při získávání přístupu k počítači a aplikacím nástroje HP ProtectTools při relaci uživatele.

Karta Přihlášení

Zadání přihlašovacích údajů nutných pro přístup k počítači, dešifrování pevného disku a přihlášení k systému Windows:

1. V levém podokně Konzoly pro správu rozbalte nabídku **Zabezpečení** a klikněte na možnost **Ověřování**.
2. Na kartě **Přihlášení** vyberte z rozevíracího seznamu kategorii uživatele.
3. V části **Zásady** určete přihlašovací údaje pro ověření, které jsou pro vybranou kategorii uživatelů vyžadovány, zaškrtnutím políček u uvedených přihlašovacích údajů. Je třeba určit alespoň jeden přihlašovací údaj.
4. V rozevíracím seznamu v části **Zásady** určete, zda je pro ověření uživatele vyžadován některý (pouze JEDEN) z vybraných přihlašovacích údajů, nebo VŠECHNY vybrané přihlašovací údaje.
5. Klikněte na tlačítko **Použít**.

Karta Relace

Definování zásad určujících přihlašovací údaje nezbytné pro ověření uživatele při přihlášení k aplikacím nástroje HP ProtectTools v průběhu relace systému Windows:

1. V levém podokně Konzoly pro správu rozbalte nabídku **Zabezpečení** a klikněte na možnost **Ověřování**.
2. Na kartě **Relace** vyberte z rozevíracího seznamu kategorii uživatele.
3. V části **Zásady** určete přihlašovací údaje pro ověření, které jsou pro vybranou kategorii uživatelů vyžadovány, zaškrtnutím políček u uvedených přihlašovacích údajů. Je třeba určit alespoň jeden přihlašovací údaj.
4. V rozevíracím seznamu v části **Zásady** určete, zda je pro ověření uživatele vyžadován některý(pouze JEDEN) z vybraných přihlašovacích údajů, nebo VŠECHNY vybrané přihlašovací údaje.
5. Klikněte na tlačítko **Použít**.

Definování nastavení

Můžete určit, která rozšířená nastavení zabezpečení budou povolena. Úprava nastavení:

1. V levém podokně Konzoly pro správu rozbalte nabídku **Zabezpečení** a klikněte na možnost **Nastavení**.
2. Zaškrtnutím příslušného políčka můžete dané nastavení povolit nebo zakázat.
3. Změny uložte kliknutím na tlačítko **Použít**.

POZNÁMKA: Nastavení **Povolit přihlášení v jednom kroku** umožňuje uživatelům tohoto počítače přeskočit přihlášení k systému Windows, pokud již bylo ověření provedeno na úrovni systému BIOS.

Správa uživatelů

V rámci aplikace Uživatelé může správce systému Windows spravovat uživatele tohoto počítače a zásady, které ovlivňují jejich práci. Chcete-li v Konzole pro správu otevřít aplikaci Uživatelé, klikněte na položku **Uživatelé**.

Uživatelé nástroje HP ProtectTools jsou uvedeni v seznamu a jsou ověřováni na základě zásad ověřování nastavených pomocí nástroje Security Manager a přihlašovacích údajů, které jsou těmito zásadami vyžadovány.

Chcete-li zobrazit zásady platné pro určitého uživatele, vyberte uživatele ze seznamu a klikněte na tlačítko **Zobrazit zásady**.

Chcete-li na některého uživatele dohlížet při registraci přihlašovacích údajů, vyberte uživatele ze seznamu a klikněte na tlačítko **Registrovat**.

Přidání uživatele

Tento proces přidá uživatele do seznamu přihlášení. Než přidáte uživatele, musí mít již tento uživatel v počítači nastaven účet uživatele systému Windows a musí být při následující proceduře přítomen, aby mohl zadat heslo.

Přidání uživatele do seznamu uživatelů:

1. Klikněte na položky **Start** a **Všechny programy** a pak na **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně Konzoly pro správu klikněte na **Uživatel**.
3. Klikněte na tlačítko **Přidat**. Otevře se dialogové okno **Vyberte uživatele**.
4. Kliknutím na tlačítko **Upřesnit** a poté na tlačítko **Najít** vyhledejte uživatele, které chcete přidat.
5. Klikněte na uživatele, kterého chcete přidat do seznamu, a klikněte na tlačítko **OK**.
6. Klikněte na tlačítko **OK** v dialogovém okně **Vyberte uživatele**.
7. Zadejte heslo systému Windows pro vybraný účet a klikněte na tlačítko **Dokončit**.

POZNÁMKA: Musíte použít existující účet systému Windows a zadat přesné heslo. Pomocí tohoto dialogového okna nelze upravovat nebo přidávat uživatelské účty systému Windows.

Odebrání uživatele

POZNÁMKA: Tato procedura nemá za následek odstranění uživatelského účtu systému Windows. Dojde pouze k odebrání daného účtu z nástroje Security Manager. Chcete-li příslušného uživatele úplně odstranit, musíte jej odebrat z nástroje Security Manager i ze systému Windows.

1. Klikněte na položky **Start** a **Všechny programy** a pak na **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně Konzoly pro správu klikněte na **Uživatel**.
3. Klikněte na uživatelské jméno u účtu, který chcete odebrat, a poté klikněte na možnost **Odstranit**.
4. V dialogovém okně pro potvrzení klikněte na možnost **Ano**.

Kontrola stavu uživatele

Aktuální stav každého uživatele je uveden v části Uživatel Konzoly pro správu:

- **Zelený symbol zaškrtnutí** – udává, že uživatel již nakonfiguroval požadované metody zabezpečeného přihlášení.
- **Červené X** – udává, že uživatel ještě nenakonfiguroval požadovanou metodu zabezpečeného přihlášení a počítač pro něj bude uzamčen, až se pokusí přihlásit. Uživatel musí spustit průvodce nastavením a nakonfigurovat požadované metody přihlášení.
- **Prázdné** – udává, že není vyžadována žádná metoda zabezpečeného přihlášení.

Konfigurace nastavení aplikací

Okno Nastavení obsahuje nástroje pro konfiguraci chování nástroje Security Manager a jeho aplikací. Úprava nastavení:

1. Klikněte na položky **Start** a **Všechny programy** a pak na **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně Konzoly pro správu klikněte na **Nastavení**.

3. Na kartě **Obecné** zvolte obecné nastavení nástroje HP ProtectTools Security Manager a klikněte na tlačítko **Použít**.

4. Na kartě **Aplikace** vyberte aplikace, které chcete povolit nebo zakázat, a poté klikněte na tlačítko **Použít**.

POZNÁMKA: Povolení nebo zakázání aplikace se může projevit až po restartování počítače.

Šifrování jednotek

Nástroj Drive Encryption for HP ProtectTools umožňuje šifrování pevných disků počítače, díky čemuž bude pevný disk nečitelný a nepřístupný pro neoprávněné osoby, které by se mohly pokusit o přístup, a to i po vyjmutí jednotky z počítače nebo odeslání dat do služby obnovení dat.

Chcete-li nástroj Drive Encryption povolit nebo zakázat, klikněte na položku Průvodce nastavením v Konzole pro správu.

△ **UPOZORNĚNÍ:** Je důležité provést zálohu šifrovacího klíče na jednotku USB a uložit ji na bezpečné místo. Pokud zapomenete heslo, jedinou možnost přístupu k pevnému disku představuje toto zařízení.

Další informace o používání aplikace Drive Encryption for HP ProtectTools naleznete v kapitole Drive Encryption for HP ProtectTools na stránce 36.

Správa přístupu zařízení

Nástroj Device Access Manager for HP ProtectTools poskytuje rozšířené volby zabezpečení umožňující zákaz některých typů zařízení, které by mohly ohrozit zabezpečení vašeho počítače. Další informace o používání nástroje Device Access Manager for HP ProtectTools naleznete v kapitole Device Access Manager for HP ProtectTools na stránce 51.

5 HP ProtectTools Security Manager

Nástroj HP ProtectTools Security Manager umožňuje značné zvýšení úrovně zabezpečení počítače. Pomocí aplikací nástroje Security Manager lze provádět následující úkony:

- Spravovat přihlašovací jméno a hesla
- Snadno změnit heslo systému Windows
- Nastavit přihlašovací údaje pro ověření, včetně čipové karty
- Zničit data na pevném disku nebo disk vyčistit
- Zobrazit stav šifrování jednotky
- Zobrazit nastavení přístupu zařízení
- Zálohovat a obnovit data nástroje Security Manager

Správa hesel

Přihlašovací jména a hesla jsou vytvářena a spravována nástrojem Credential Manager produktu HP ProtectTools (Password Manager). Tento nástroj umožňuje otevírání a spouštění webových stránek a programů pomocí zaregistrovaných přihlašovacích údajů.

Další informace o správě hesel naleznete v kapitole Modul Credential Manager pro nástroj HP ProtectTools (Password Manager) na stránce 39.

Nastavení přihlašovacích údajů

Přihlašovací údaje nástroje Security Manager slouží k ověření, zda se opravdu jedná o daného uživatele. Správce tohoto počítače může stanovit, které přihlašovací údaje budou použity k prokázání vaší totožnosti při přihlašování k vašemu účtu v systému Windows, webovým stránkám nebo programům.

Dostupné přihlašovací údaje se mohou lišit v závislosti na bezpečnostním zařízení, které je v počítači vestavěno nebo je k němu připojeno. Každému podporovanému přihlašovacímu údaji bude odpovídat položka ve skupině Přihlašovací údaje.

Změna hesla systému Windows

Pomocí nástroje Security Manager můžete své heslo do systému Windows změnit snáze a rychleji než prostřednictvím Ovládacích panelů systému Windows.

Změna hesla systému Windows:

1. V levém podokně nástroje HP ProtectTools Security Manager klikněte na položku **Přihlašovací údaje**.
2. Klikněte na položku **Heslo pro systém Windows**.
3. Zadejte stávající heslo do pole **Aktuální heslo pro systém Windows**.
4. Do polí **Nové heslo pro systém Windows** a **Potvrzení nového hesla** zadejte nové heslo.
5. Klikněte na možnost **Změnit**.

Ničení a čištění souborů

Nástroj File Sanitizer for HP ProtectTools odstraňuje soubory tak, že je přepíše nic neznamenajícími daty. Tento proces, označovaný jako „ničení“, značně zvyšuje zabezpečení informací, takto odstraněné soubory se totiž velmi obtížně obnovují. Nástroj File Sanitizer dále zlepšuje zabezpečení informací přepsáním používaného prostoru na pevném disku pomocí procesu označovaného jako „čištění“. Soubory odstraněné pomocí nástroje File Sanitizer nelze obnovit za použití operačního systému nebo běžně dostupného softwaru pro obnovení dat.

Další informace o používání nástroje File Sanitizer for HP ProtectTools naleznete v kapitole File Sanitizer for HP ProtectTools na stránce 44.

Zobrazení stavu šifrování jednotky

Šifrování jednotky zajišťuje nástroj Drive Encryption, který nastavuje správce systému Windows pomocí Konzoly pro správu. Uživatelé mohou zobrazit stav šifrování pomocí nástroje Security Manager.

Zobrazení stavu šifrování jednotky:

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP ProtectTools Security Manager**.
2. V levém podokně aplikace Security Manager klikněte na položku **Stav šifrování**. Na stránce Stav šifrování je uvedeno, zda je šifrování jednotky aktivní či neaktivní a které jednotky jsou nebo nejsou zašifrovány.

Zobrazení přístupu zařízení

Přístup zařízení nastavuje správce systému Windows pomocí Konzoly pro správu. Uživatelé mohou zobrazit své nastavení přístupu zařízení pomocí nástroje Security Manager.

Zobrazení nastavení přístupu zařízení:

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP ProtectTools Security Manager**.
2. V levém podokně aplikace Security Manager rozbalte nabídku **Device Access Manager**.
3. Chcete-li zjistit, kterým zařízením je odepřen přístup, klikněte na položku **Jednoduchá konfigurace**. Zařízením označeným symbolem zaškrtnutí je odepřen přístup.

4. Chcete-li zjistit, kterým uživatelům či skupinám je odepřen přístup, klikněte na položku **Konfigurace tříd zařízení**.

5. Kliknutím na zařízení zjistíte, kterým uživatelům či skupinám je přístup k danému zařízení odepřen nebo povolen.

Přidávání aplikací

K dispozici mohou být další aplikace, které přidají k tomuto programu další funkce.

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP ProtectTools Security Manager**.

2. V levém podokně aplikace Security Manager klikněte na položku **Objevte více**.

POZNÁMKA: Není-li odkaz **Objevte více** k dispozici, znamená to, že byl správcem vašeho počítače zakázán.

3. Na kartě **Přidat aplikace** můžete vyhledat další aplikace.

4. Na kartě **Aktualizace a zprávy** můžete získat informace o nových aplikacích a aktualizacích zaškrtnutím políčka **Informujte mne o nových aplikacích a aktualizacích** a zadáním intervalu pro hledání aktualizací nebo můžete aktualizace vyhledat okamžitě kliknutím na tlačítko **Zkontrolovat nyní**.

Nastavení předvoleb

Stránka předvoleb umožňuje zaškrtnutí políčka **Zobrazit ikonu na hlavním panelu**. Ikona nástroje Security Manager pak bude zobrazena v oznamovací oblasti hlavního panelu.

Otevření stránky předvoleb:

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP ProtectTools Security Manager**.

2. V levém podokně aplikace Security Manager klikněte na položku **Upřesnit** a poté na položku **Předvolby**.

3. Zaškrtněte políčko **Zobrazit ikonu na hlavním panelu** nebo zrušte jeho zaškrtnutí a klikněte na možnost **Použít**.

Zálohování a obnovení

Data nástroje Security Manager se vyplatí pravidelně zálohovat. Frekvence záloh závisí na tom, jak často se data mění. Pokud například každý den přidáváte nová přihlášení, je dobré provádět každodenní zálohování dat.

Zálohy lze také využít při migraci dat z jednoho počítače do druhého, tedy při importu a exportu dat. Mějte však na paměti, že tato funkce zajišťuje pouze zálohování dat.

Pokud obnovíte soubor zálohy v jiném počítači nebo ve stejném počítači po přeinstalování operačního systému, musí již být v systému nainstalován nástroj HP ProtectTools Security Manager, aby bylo možné ze souboru zálohy obnovit data.

Zálohování dat

Při zálohování dat dochází k uložení přihlášení a přihlašovacích údajů do šifrovaného souboru chráněného heslem, které zadáte.

Postup zálohování dat:

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP ProtectTools Security Manager**.
2. V levém podokně aplikace Security Manager klikněte na položku **Upřesnit** a poté na položku **Zálohování a obnovení**.
3. Klikněte na možnost **Zálohovat data**.
4. Vyberte moduly, které chcete do zálohy zahrnout. Ve většině případů se provádí zálohování všech modulů. Klikněte na tlačítko **Další**.
5. Zadejte své heslo pro ověření totožnosti a poté klikněte na tlačítko se šipkou.
6. Zadejte název souboru úložiště a cestu k němu. Ve výchozím nastavení bude soubor uložen do složky Dokumenty. Chcete-li zadat jiné umístění, klikněte na možnost **Procházet**. Klikněte na tlačítko **Další**.
7. Zadejte a potvrďte heslo, kterým bude soubor chráněn.
8. Klikněte na tlačítko **Dokončit**.

Obnovení dat

Data můžete obnovit ze zašifrovaného souboru chráněného heslem, který jste předtím vytvořili pomocí funkce obnovení a zálohy nástroje Security Manager.

Postup obnovení dat:

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP ProtectTools Security Manager**.
2. V levém podokně aplikace Security Manager klikněte na položku **Upřesnit** a poté na položku **Zálohování a obnovení**.
3. Klikněte na možnost **Obnovit data**.
4. Zadejte název souboru úložiště a cestu k němu nebo klikněte na možnost **Procházet** a vyberte požadovaný soubor.
5. Zadejte heslo, kterým je soubor chráněn, a klikněte na položku **Další**.
6. Vyberte moduly, jejichž data chcete obnovit. Ve většině případů se jedná o všechny uvedené moduly. Klikněte na tlačítko **Další**.
7. Klikněte na tlačítko **Dokončit**.

Změna jména a obrázku uživatele systému Windows

Your Windows user name and a picture are displayed in the upper left corner of Security Manager.

Postup při změně jména či obrázku uživatele:

1. Klikněte do pravého horního rohu nástroje Security Manager, kde je uvedeno vaše jméno uživatele a obrázek.
2. Chcete-li změnit jméno uživatele, zadejte vybrané jméno do pole **Jméno uživatele systému Windows**.
3. Chcete-li změnit obrázek, klikněte na tlačítko **Vybrat obrázek** a vyhledejte požadovaný obrázek.
4. Změny uložte kliknutím na tlačítko **Uložit**.

6 Drive Encryption for HP ProtectTools

POZNÁMKA: Nástroj Drive Encryption for HP ProtectTools je k dispozici pouze pro některé modely.

V dnešní době může snadno dojít ke krádeži počítače patřícího vám nebo některému z vašich zaměstnanců a k prozrazení kritických informací o vaší společnosti. Pokud však všechna data na pevném disku počítače zašifrujete, bude pevný disk nečitelný a nepřístupný pro neoprávněné osoby, které by se mohly pokusit o přístup, a to i po vyjmutí jednotky z počítače nebo odeslání dat do služby obnovení dat.

Nástroj Drive Encryption for HP ProtectTools poskytuje kompletní ochranu dat šifrováním pevného disku. Pokud je nástroj Drive Encryption aktivní, je nutné se ještě před spuštěním systému Windows přihlásit prostřednictvím přihlašovací obrazovky nástroje Drive Encryption.

Nástroj Drive Encryption nezabraňuje neautorizovanému přístupu v rámci jedné relace systému Windows. Po spuštění počítače a zadání jména a hesla jsou data na pevném disku stále šifrována, ale jsou dostupná všem uživatelům systému. Zajistěte, aby relaci systému Windows po dobu vaší nepřítomnosti chránilo heslo.

POZNÁMKA: Nástroj Drive Encryption for HP ProtectTools můžete aktivovat pouze v Průvodci nastavením Konzoly pro správu nástroje HP ProtectTools.

POZNÁMKA: Nástroj Drive Encryption není podporován v 64bitových operačních systémech při konfiguraci s diskovým polem RAID v systémech používajících procesor AMD.

POZNÁMKA: Nástroj Drive Encryption nepodporuje obranu proti slovníkovému útoku.

Nástroj Drive Encryption:

- Umožňuje zašifrování všech dat na vestavěných pevných discích
- Poskytuje snadný přístup pomocí hesla a ověřování před spuštěním
- Podporuje systémy Microsoft Windows XP, Windows Vista a Windows 7

Aplikace Drive Encryption for HP ProtectTools umožňuje provádění různých úkonů:

- Správa šifrování jednotky
  - Šifrování nebo dešifrování jednotlivých disků
- Zálohování a obnovení
  - Vytváření záložních klíčů
  - Provedení obnovení

△ **UPOZORNĚNÍ:** Je důležité provést zálohu šifrovacího klíče na jednotku USB a uložit ji na bezpečné místo. Pokud zapomenete heslo, jedinou možnost přístupu k pevnému disku představuje toto zařízení.

UPOZORNĚNÍ: Pokud se rozhodnete modul Drive Encryption odinstalovat nebo pokud používáte řešení zálohování a obnovení, je nutné nejdříve všechny zašifrované jednotky dešifrovat. Pokud tak neučiníte, nebudete mít přístup k datům na zašifrovaném disku. Přístup k zašifrovaným diskům nelze obnovit opětovnou instalací modulu Drive Encryption.

Postupy nastavení

Spuštění nástroje Drive Encryption

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.
2. Klikněte na možnost **Drive Encryption**.

Obecné úlohy

Aktivace nástroje Drive Encryption

Modul Drive Encryption můžete aktivovat pomocí Průvodce nastavením v Konzole pro správu nástroje HP ProtectTools.

Deaktivace nástroje Drive Encryption

Modul Drive Encryption můžete deaktivovat pomocí Průvodce nastavením v Konzole pro správu nástroje HP ProtectTools.

Přihlášení po aktivaci modulu Drive Encryption

Pokud zapnete počítač po aktivaci nástroje Drive Encryption a váš uživatelský účet je zaregistrován, musíte se přihlásit prostřednictvím přihlašovací obrazovky modulu Drive Encryption:

POZNÁMKA: Pokud správce systému Windows povolil v Konzole pro správu nástroje HP ProtectTools zabezpečení před spuštěním, budete se k počítači přihlašovat ihned po zapnutí počítače, nikoli prostřednictvím přihlašovací obrazovky nástroje Drive Encryption.

POZNÁMKA: Pokud k přihlášení pomocí přihlašovací obrazovky nástroje Drive Encryption použijete klíč obnovení, budete také vyzváni k vybrání svého jména uživatele systému Windows a zadání hesla na přihlašovací obrazovce systému Windows.

Pokročilé operace

Správa modulu Drive Encryption (úloha správce)

Okno nástroje Drive Encryption umožňuje správcům systému Windows zobrazení a změnu stavu modulu Drive Encryption (aktivní nebo neaktivní) a zobrazení stavu šifrování všech pevných disků v počítači.

Šifrování nebo dešifrování jednotlivých disků

1. V levém podokně Konzoly pro správu rozbalte nabídku **Drive Encryption** a klikněte na možnost **Správa šifrování**.
2. Klikněte na tlačítko **Změnit šifrování**.
3. V dialogovém okně Změnit šifrování zaškrtněte políčko vedle pevného disku, který chcete zašifrovat, nebo zrušte zaškrtnutí políčka vedle pevného disku, který chcete dešifrovat, a klikněte na možnost **OK**.

POZNÁMKA: V průběhu šifrování nebo dešifrování jednotky udává ukazatel průběhu čas zbývající do dokončení procesu v aktuální relaci. Pokud dojde v průběhu procesu šifrování k vypnutí počítače nebo k přechodu do režimu spánku či hibernace a poté k restartování, vrátí se zobrazený zbývající čas na začátek, šifrování však ve skutečnosti započne od místa, kde bylo přerušeno. Zbývající čas a průběh budou ubíhat rychleji, aby se zohlednil předchozí průběh.

Zálohování a obnova (úloha správce)

Okno Zálohování a obnova v modulu Drive Encryption umožňuje správcům systému Windows zálohování a obnovu šifrovacích klíčů.

Vytváření záložních klíčů

UPOZORNĚNÍ: Úložné zařízení obsahující záložní klíč uložte na bezpečné místo, protože toto zařízení představuje jediný způsob přístupu k pevnému disku v případě, že zapomenete heslo.

1. V levém podokně Konzoly pro správu rozbalte nabídku **Drive Encryption** a klikněte na možnost **Zálohování a obnova**.
2. Klikněte na tlačítko **Záložní klíče**.
3. Na stránce Vybrat zálohovací disk klikněte na název zařízení, na které chcete šifrovací klíč zálohovat, a klikněte na možnost **Další**.
4. Přečtěte si informace na další zobrazené stránce a klikněte na položku **Další**.

   Šifrovací klíč bude uložen na vybrané úložné zařízení.
5. V dialogovém okně pro potvrzení klikněte na tlačítko **OK**.

POZNÁMKA: Informace o správě a provedení obnovení naleznete v souboru nápovědy pro modul Drive Encryption for HP ProtectTools.

7 Modul Credential Manager pro nástroj HP ProtectTools (Password Manager)

S nástrojem Password Manager je přihlašování k systému Windows, webovým stránkám a programům snazší a bezpečnější.

Správce hesel umožňuje nastavení přihlašovacích obrazovek webových stránek a programů pro rychlý a zabezpečený přístup. Správce hesel nejdříve zjistí vaše přihlašovací údaje a data, která zadáváte do polí na každé přihlašovací obrazovce. Když se pak otevře přihlašovací stránka, Správce hesel po ověření vaší totožnosti provede automatické zadání a odeslání údajů.

Chcete-li získat ještě rychlejší přístup, můžete zobrazit nabídku přihlášení pomocí jednoduché klávesové zkratky, kterou si můžete sami nastavit (výchozí zkratka je Ctrl+Windows+H). V nabídce jednoduše vyberete přihlášení a nástroj Password Manager spustí webovou stránku či program, otevře přihlašovací obrazovku a automaticky vás přihlásí.

K ověření totožnosti budete používat přihlašovací údaje produktu HP ProtectTools pro malé podniky, například heslo systému Windows. To znamená, že budete k přihlášení na všech přihlašovacích obrazovkách, které jste nastavili, používat stejné přihlašovací údaje. Můžete tak vytvářet silnější hesla, která si nemusíte zapisovat či pamatovat, a přitom zvýšit zabezpečení svých účtů.

Díky Správci hesel rychle zjistíte, zda některé z vašich hesel představuje bezpečnostní riziko, a můžete automaticky vygenerovat silné komplexní heslo pro nové stránky.

Nástroj Password Manager také umožňuje zobrazení vašich přihlašovacích údajů a hesel a jejich okamžitou úpravu. Mnohé funkce Správce hesel jsou také k dispozici prostřednictvím ikony Správce hesel, která se zobrazí vždy, když je aktivní přihlašovací obrazovka nastaveného programu nebo přihlašovací obrazovka libovolné webové stránky. Kliknutím na tuto ikonu zobrazíte kontextovou nabídku, ve které si můžete vybrat z následujících možností.

Webové stránky nebo programy, u nichž ještě nebylo vytvořeno přihlášení:

V kontextové nabídce se zobrazí následující volby.

- Přidat [doména.com] do Správce hesel: Slouží k přidání přihlášení pro aktuální přihlašovací obrazovku.
- Spustit Správce hesel: Spustí nástroj Security Manager na stránce Správce hesel.
- Nastavení ikon Správce hesel: Umožňuje určení podmínek, za kterých se zobrazí ikona Správce hesel.
- Nápověda: Zobrazí nápovědu online pro aplikaci Správce hesel.

Webové stránky nebo programy, u nichž již bylo vytvořeno přihlášení:

V kontextové nabídce se zobrazí následující volby.

- Zadat přihlašovací data: Umístí přihlašovací údaje do přihlašovacích polí a poté stránku odešle (pokud bylo při vytváření nebo poslední úpravě přihlášení nastaveno odeslání).
- Upravit přihlášení: Umožňuje úpravu přihlašovacích údajů pro tuto stránku.
- Přidat přihlášení: Slouží k přidání dalšího přihlášení pro stejnou webovou stránku nebo program.
- Spustit Správce hesel: Spustí panel nástrojů modulu Security Manager na stránce Správce hesel.
- Nápověda: Zobrazí nápovědu online pro aplikaci Správce hesel.

Přidání přihlášení

Postup pro přidání přihlášení:

1. Otevřete přihlašovací obrazovku webové stránky nebo programu.
2. Klikněte na šipku na ikoně Správce hesel a vyberte některou z následujících možností podle toho, zda se jedná o přihlašovací obrazovku webové stránky nebo programu.
   - Webová stránka – vyberte možnost **Přidat [název domény] do Správce hesel**.
   - Program – vyberte možnost **Přidat tuto přihlašovací obrazovku do Správce hesel**.
3. Zadejte přihlašovací údaje. Přihlašovací pole na obrazovce a odpovídající pole v dialogovém okně jsou označena silným oranžovým okrajem. Jsou k dispozici i další možnosti zobrazení tohoto dialogového okna, můžete například vybrat volbu Přidat přihlášení na kartě **Správa** ve Správci hesel. Některé možnosti závisí na bezpečnostních zařízeních, která jsou k počítači připojena, například použití klávesové zkratky Ctrl+H nebo vložení čipové karty.
   - Kliknutím na šipky vpravo vedle přihlašovacího pole zadáte do pole jednu z několika předformátovaných možností.
   - Kliknutím na položku **Vybrat další pole** můžete také ke svému přihlášení přidat další pole z obrazovky.
   - Zrušte zaškrtnutí políčka **Odeslat přihlašovací údaje**, pokud chcete zadávat údaje do přihlašovacích polí, avšak tyto údaje neodesílat.
   - Chcete-li zobrazit heslo pro toto přihlášení, klikněte na možnost **Zobrazit heslo**.
4. Klikněte na tlačítko **OK**. Z ikony Správce hesel zmizí znaménko plus. To znamená, že bylo vytvořeno přihlášení.

Při každém dalším otevření dané webové stránky nebo spuštění daného programu se zobrazí ikona Správce hesel, která značí, že můžete k přihlášení použít zaregistrované přihlašovací údaje.

Úprava přihlášení

Postup pro úpravu přihlášení:

1. Otevřete přihlašovací obrazovku webové stránky nebo programu.
2. Klikněte na šipku na ikoně Správce hesel a volbou položky **Upravit přihlášení** zobrazte dialogové okno, ve kterém můžete upravit své přihlašovací informace. Přihlašovací pole na obrazovce a odpovídající pole v dialogovém okně jsou označena silným oranžovým okrajem.
3. Upravte své přihlašovací informace.
   - Kliknutím na šipky vpravo vedle přihlašovacího pole zadáte do pole jednu z několika předformátovaných možností.
   - Kliknutím na položku **Vybrat další pole** můžete také ke svému přihlášení přidat další pole z obrazovky.
   - Zrušte zaškrtnutí políčka **Odeslat údaje účtu**, pokud chcete zadávat údaje do přihlašovacích polí, avšak tyto údaje neodesílat.
   - Chcete-li zobrazit heslo pro toto přihlášení, klikněte na možnost Zobrazit heslo.
4. Klikněte na tlačítko **OK**.

Používání nabídky přihlášení

Správce hesel poskytuje snadný a rychlý způsob otevírání webových stránek a spouštění programů, pro které jste vytvořili přihlášení. Pokud dvakrát kliknete na přihlášení k programu nebo webové stránce v nabídce přihlášení nebo na kartě **Správa** ve Správci hesel, otevře se příslušná přihlašovací obrazovka a automaticky se zadají přihlašovací údaje. Ve výchozím nastavení se tyto údaje také okamžitě odešlou na webovou stránku, tuto funkci však můžete deaktivovat zrušením zaškrtnutí políčka **Odeslat údaje účtu** při úvodním nastavení nebo úpravě daného přihlášení.

Když vytvoříte přihlášení, je automaticky přidáno do nabídky přihlášení Správce hesel.

Chcete-li zobrazit nabídku přihlášení, stiskněte klávesovou zkratku Správce hesel. Výchozí klávesovou zkratkou je Ctrl+H, zkratku však můžete změnit na obrazovce **Správce hesel** > **Nastavení**.

Uspořádání přihlášení do kategorií

Kategorie umožňují přehledné uspořádání přihlášení. Stačí pouze vytvořit jednu či více kategorií a přetáhnout do nich příslušná přihlášení.

Postup pro přidání kategorie:

1. V levém podokně aplikace Security Manager vyberte možnost **Správce hesel**.
2. Vyberte kartu **Správa** a klikněte na možnost **Přidat kategorii**.
3. Zadejte název kategorie.
4. Klikněte na tlačítko **OK**.

Postup pro přidání přihlášení do kategorie:

1. Přesuňte ukazatel myši na požadované přihlášení.
2. Stiskněte a podržte levé tlačítko myši.
3. Přetáhněte přihlášení do seznamu kategorií. Kategorie, na které se právě nachází ukazatel myši, bude zvýrazněna.
4. Až bude zvýrazněna požadovaná kategorie, uvolněte tlačítko myši.

Přihlášení se do vybrané kategorie nepřesunou, ale pouze zkopírují. To znamená, že jedno přihlášení můžete přidat do více kategorií. Kdykoli můžete zobrazit všechna přihlášení kliknutím na možnost **Vše**.

Správa přihlášení

Správce hesel umožňuje snadnou a intuitivní správu přihlašovacích údajů (uživatelských jmen, hesel a různých přihlašovacích účtů) z jednoho místa.

Vaše přihlášení jsou uvedena na kartě **Správa**. Pokud pro stejnou webovou stránku vytvoříte více přihlášení, budou tato přihlášení v seznamu uvedena pod názvem webové stránky a odsazena od okraje.

Postup při správě přihlášení:

V levém podokně aplikace Security Manager vyberte možnost **Správce hesel** a klikněte na kartu **Správa**.

- Přidání přihlášení – klikněte na možnost **Přidat přihlášení** a postupujte podle pokynů na obrazovce.
- Úprava přihlášení – vyberte přihlášení a klikněte na položku **Upravit**. Pak proveďte změnu přihlašovacích údajů.
- Odstranění přihlášení – vyberte přihlášení a klikněte na položku **Odstranit**.

Přidání dalšího přihlášení pro webovou stránku nebo program:

1. Zobrazte přihlašovací obrazovku webové stránky nebo programu.
2. Kliknutím na ikonu Správce hesel zobrazte nabídku zkratek.
3. Vyberte možnost **Přidat další přihlášení** a postupujte podle pokynů na obrazovce.

Hodnocení síly hesla

Používání silných hesel pro přihlašování k webovým stránkám a programům představuje důležitou součást ochrany vaší totožnosti.

Správce hesel zjednodušuje monitorování a zlepšování zabezpečení prostřednictvím rychlé, automatické analýzy síly všech hesel, která při přihlašování k webovým stránkám a programům používáte. Sílu hesel, která používáte, můžete ověřit na kartě **Síla hesla** ve Správci hesel.

Nastavení ikony Správce hesel

Správce hesel provádí pokusy o rozpoznání přihlašovacích obrazovek k webovým stránkám a programům. Pokud Správce hesel nalezne přihlašovací obrazovku, pro kterou jste ještě nevytvořili přihlášení, vyzve vás k přidání přihlášení pro danou obrazovku zobrazením znaménka „+“ na ikoně Správce hesel.

Lze konfigurovat následující nastavení:

- Vždy zobrazit výzvu – tuto volbu vyberte v případě, že chcete, aby Správce hesel zobrazoval výzvu k přidání přihlášení při každém zobrazení přihlašovací stránky, pro kterou ještě není nastaveno přihlášení.
- Nezobrazovat výzvu pro tuto obrazovku – vyberete-li tuto volbu, Správce hesel již nebude pro danou přihlašovací obrazovku zobrazovat výzvu k přidání přihlášení.
- Nikdy nezobrazovat výzvu – vyberete-li tuto volbu, Správce hesel nebude zobrazovat žádné výzvy k přidání přihlášení pro přihlašovací obrazovky, které ještě nebyly nastaveny.

8 File Sanitizer for HP ProtectTools

Aplikace File Sanitizer je nástroj, který umožňuje bezpečné vymazání kritických souborů a složek (osobní informace nebo soubory, data týkající se historie nebo webu a další data) z vašeho počítače a pravidelné čištění pevného disku.

POZNÁMKA: V současné době lze aplikaci File Sanitizer použít pouze pro pevný disk.

Ničení obsahu

Odstraníte-li soubory a/nebo složky v systému Windows, z pevného disku se obsah zcela neodstraní. Systém Windows odstraní pouze odkazy na ně. Obsah zůstane na pevném disku, dokud nedojde k přepsání jiným souborem.

Operace ničení obsahu se liší od standardního odstranění v systému Windows (které je v aplikaci File Sanitizer označováno jako jednoduché smazání), protože jakmile data zničíte, je téměř nemožné je obnovit.

Když zvolíte profil ničení (Vysoké zabezpečení, Střední zabezpečení nebo Nízké zabezpečení), automaticky tím vyberete předdefinovaný seznam souborů a/nebo složek a metodu mazání. Můžete také některý profil ničení upravit. Budete moci určit počet mazacích cyklů, soubory, které chcete mazat, soubory, jejichž smazání chcete nejprve potvrdit, a soubory, které mazat nechcete.

Můžete také nastavit plán automatického ničení obsahu a mimo něj kdykoli provést ničení souborů a/nebo složek ručně.

Čištění volného prostoru

Čištění volného prostoru umožňuje bezpečné přepsání odstraněných souborů náhodnými daty, takže uživatelé nebudou moci zobrazit původní obsah odstraněného souboru.

POZNÁMKA: Čištění volného prostoru je určeno pro soubory vymazané pomocí Koše systému Windows nebo pro ručně odstraněné soubory. Čištění volného prostoru neposkytuje žádné další zabezpečení vymazaných souborů.

Můžete nastavit plán automatického čištění volného prostoru nebo můžete čištění volného prostoru kdykoli aktivovat ručně prostřednictvím ikony produktu HP ProtectTools v oznamovací oblasti v pravé části hlavního panelu.

Postupy nastavení

Spuštění aplikace File Sanitizer

Postup spuštění aplikace File Sanitizer

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **HP ProtectTools Security Manager**.
2. V levém podokně aplikace Security Manager klikněte na položku **File Sanitizer**.

   – nebo –

- Dvakrát klikněte na ikonu **File Sanitizer**.

  – nebo –

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

Nastavení plánu čištění volného prostoru

Postup nastavení plánu čištění volného prostoru:

1. V levém podokně aplikace Security Manager rozbalte podstrom **File Sanitizer** a klikněte na položku **Čištění**.
2. Zaškrtněte políčko **Aktivovat plánovač**, zadejte heslo systému Windows a poté určete den a dobu, kdy chcete pevný disk vyčistit.
3. Klikněte na ikonu **Uložit**.

POZNÁMKA: Operace čištění volného prostoru může trvat poměrně dlouho. Přestože se tato operace provádí na pozadí, může se počítač zpomalit kvůli vytížení procesoru a disku.

Nastavení plánu ničení

1. V levém podokně aplikace Security Manager rozbalte podstrom **File Sanitizer** a klikněte na položku **Ničení**.
2. Vyberte požadovanou možnost:
   - **Vypnutí systému Windows** – Vyberte, chcete-li zničit všechny vybrané soubory při vypnutí systému Windows.

     POZNÁMKA: Je-li vybrána tato možnost, zobrazí se při vypnutí systému dialogové okno s dotazem, zda chcete pokračovat ve zničení vybraných souborů, nebo zda chcete operaci přeskočit. Kliknutím na tlačítko Ano operaci přeskočíte, kliknutím na tlačítko Ne provedete zničení položek. Tlačítko Ano nebo Ne je třeba stisknout rychle, neboť systém Windows v rámci přípravy na vypnutí software ukončí s chybovou zprávou. Pokud budete kliknutím na tlačítko Ne pokračovat ve zničení vybraných položek, systém Windows může zobrazit chybovou zprávu informující o tom, že program File Sanitizer neodpovídá. Nechte aplikaci File Sanitizer dokončit ničení a poté systém znovu vypněte.
   - **Spuštění webového prohlížeče** – Vyberte, chcete-li v okamžiku spuštění webového prohlížeče zničit všechny soubory související s webem, jako je například historie adres URL.
   - **Ukončení webového prohlížeče** – Vyberte, chcete-li v okamžiku ukončení webového prohlížeče zničit všechny soubory související s webem, jako je například historie adres URL.
   - **Zadání sekvence kláves** – Výběrem této možnosti můžete ničení vybraných položek zahájit stisknutím určené kombinace kláves.
   - **Plánovač** – Zaškrtněte políčko Aktivovat plánovač, zadejte heslo systému Windows a poté určete den a dobu, kdy chcete zničit vybrané soubory.
3. Klikněte na ikonu **Uložit**.

Výběr nebo vytvoření profilu ničení

Výběrem předdefinovaného profilu nebo vytvořením vlastního můžete zvolit metodu mazání a vybrat soubory a/nebo složky, které chcete ničit.

Výběr předdefinovaného profilu ničení

Když zvolíte předdefinovaný profil ničení (Vysoké zabezpečení, Střední zabezpečení nebo Nízké zabezpečení), vyberete tím současně metodu mazání i seznam souborů. Kliknutím na tlačítko Zobrazit podrobnosti si můžete prohlédnout předdefinovaný seznam souborů určených ke zničení.

Výběr předdefinovaného profilu ničení:

1. V levém podokně aplikace Security Manager rozbalte podstrom **File Sanitizer** a klikněte na položku **Nastavení**.
2. Klikněte na některý předdefinovaný profil ničení.
3. Klepnutím na tlačítko **Zobrazit podrobnosti** si můžete prohlédnout předdefinovaný seznam souborů určených ke zničení.

4. Ve skupině **Zničit následující** zaškrtněte políčko vedle každého souboru, jehož zničení chcete před provedením potvrdit.

5. Klikněte na tlačítko **Použít**.

Přizpůsobení rozšířeného zabezpečení profilu ničení

Když vytváříte profil ničení, určujete počet mazacích cyklů, soubory, které chcete mazat, soubory, jejichž smazání chcete nejprve potvrdit, a soubory, které mazat nechcete:

1. V levém podokně aplikace Security Manager rozbalte podstrom **File Sanitizer**, klikněte na položku **Nastavení**, vyberte **Rozšířené nastavení zabezpečení** a poté klikněte na tlačítko **Zobrazit podrobnosti**.

2. Určete počet mazacích cyklů.

POZNÁMKA: Každý soubor bude smazán nastaveným počtem mazacích cyklů. Pokud například zvolíte 3 mazací cykly, bude algoritmus mazající původní data proveden třikrát. Pokud zvolíte více mazacích cyklů, může ničení trvat výrazně déle, vymazání dat však bude bezpečnější.

3. Vyberte položky, které chcete ničit:

   a. V části **Dostupné možnosti ničení** klepněte na soubor a poté klepněte na tlačítko **Přidat**.

   b. Chcete-li přidat vlastní soubor, klepněte na možnost **Přidat vlastní možnost**, zadejte celý název souboru či složky nebo soubor či složku vyberte procházením a klepněte na tlačítko **OK**. Klepněte na vlastní soubor a poté na tlačítko **Přidat**.

   POZNÁMKA: Chcete-li odstranit soubor ze seznamu dostupných položek, klepněte na něj a poté klepněte na tlačítko **Odstranit**.

4. Ve skupině **Zničit následující** zaškrtněte políčko vedle každého souboru, jehož zničení chcete před provedením potvrdit.

POZNÁMKA: Chcete-li soubor odstranit ze seznamu položek ke zničení, klepněte na něj a poté klepněte na tlačítko **Odebrat**.

5. Ve skupině **Neničit následující** klepněte na tlačítko **Přidat** a vyberte specifické soubory, které nechcete do ničení zahrnout.

6. Až dokončíte konfiguraci profilu ničení, klikněte na tlačítko **Použít**.

Přizpůsobení profilu jednoduchého odstranění

Profil jednoduchého odstranění provádí běžné vymazání souboru, aniž by provedl jeho bezpečné zničení. Když přizpůsobujete profil jednoduchého odstranění, určujete soubory, které chcete odstranit, soubory, jejichž odstranění chcete nejprve potvrdit, a soubory, které odstraňovat nechcete:

POZNÁMKA: Pokud používáte metodu jednoduchého odstranění, důrazně se doporučuje pravidelně používat čištění volného prostoru.

1. V levém podokně aplikace Security Manager rozbalte podstrom **File Sanitizer**, klikněte na položku **Nastavení**, vyberte **Nastavení jednoduchého odstranění** a poté klikněte na tlačítko **Zobrazit podrobnosti**.
2. Vyberte soubory, které chcete odstranit:
   a. V části **Dostupné možnosti odstranění** klepněte na soubor a poté klepněte na tlačítko **Přidat**.
   b. Chcete-li přidat vlastní soubor, klepněte na možnost **Přidat vlastní možnost**, zadejte celý název souboru či složky nebo soubor či složku vyberte procházením a klepněte na tlačítko **OK**. Klepněte na vlastní soubor a poté na tlačítko **Přidat**.

   POZNÁMKA: Chcete-li odstranit soubor ze seznamu dostupných položek, klepněte na něj a poté klepněte na tlačítko **Odstranit**.
3. Ve skupině **Odstranit následující** zaškrtněte políčko vedle každého souboru, jehož odstranění chcete před provedením potvrdit.

POZNÁMKA: Chcete-li soubor odstranit ze seznamu položek k odstranění, klepněte na něj a poté klepněte na tlačítko **Odebrat**.

4. Ve skupině **Nemazat následující** klepněte na tlačítko **Přidat** a vyberte specifické soubory, které nechcete zahrnout do ničení.
5. Až dokončíte konfiguraci profilu jednoduchého odstranění, klikněte na tlačítko **Použít**.

Obecné úlohy

Použití sekvence kláves ke spuštění ničení

Při zadávání sekvence kláves postupujte takto:

1. V levém podokně aplikace Security Manager rozbalte podstrom **File Sanitizer** a klikněte na položku **Ničení**.
2. Zaškrtněte políčko **Zadání sekvence kláves**.
3. Do příslušného pole zadejte znak požadované klávesy a poté zaškrtněte libovolná z políček **CTRL**, **ALT** a **SHIFT**.

   Chcete-li například zahájit automatické ničení pomocí klávesové zkratky Ctrl+Shift+S, zadejte do pole písmeno S a zaškrtněte políčka **CTRL** a **SHIFT**.

POZNÁMKA: Ujistěte se, že nastavená sekvence kláves není používána k jinému účelu.

Spuštění ničení pomocí sekvence kláves:

1. Podržte klávesy Ctrl, Alt nebo Shift (podle nastavené kombinace) a stiskněte zvolený znak.
2. Pokud se zobrazí dialogové okno pro potvrzení, klikněte na tlačítko **Ano**.

Použití ikony File Sanitizer

△ **UPOZORNĚNÍ:** Zničené soubory nelze žádným způsobem obnovit. Pečlivě zvažte, pro které položky použijete ruční ničení.

1. Přejděte k dokumentu nebo složce, kterou chcete zničit.
2. Přetáhněte soubor na ikonu File Sanitizer na ploše.
3. V dialogovém okně pro potvrzení klikněte na tlačítko **Ano**.

Ruční zničení jedné položky

△ **UPOZORNĚNÍ:** Zničené soubory nelze žádným způsobem obnovit. Pečlivě zvažte, pro které položky použijete ruční ničení.

1. Klikněte pravým tlačítkem myši na ikonu **HP ProtectTools** v oznamovací oblasti v pravé části hlavního panelu, zvýrazněte položku **File Sanitizer** a klikněte na příkaz **Zničit jeden**.
2. Po otevření okna Procházet vyhledejte soubor, který chcete zničit, a klepněte na tlačítko **Otevřít**.

POZNÁMKA: Můžete vybrat jeden soubor nebo celou složku.

3. V dialogovém okně pro potvrzení klikněte na tlačítko **Ano**.

– nebo –

1. Klikněte pravým tlačítkem myši na ikonu **File Sanitizer** na ploše a vyberte příkaz **Zničit jeden**.
2. Po otevření okna Procházet vyhledejte soubor, který chcete zničit, a klepněte na tlačítko **OK**.
3. V dialogovém okně pro potvrzení klikněte na tlačítko **Ano**.

– nebo –

1. V levém podokně aplikace Security Manager rozbalte podstrom **File Sanitizer** a klikněte na položku **Ničení**.
2. Klikněte na tlačítko **Procházet**.
3. Po otevření okna Procházet vyhledejte soubor, který chcete zničit, a klepněte na tlačítko **Otevřít**.
4. V dialogovém okně pro potvrzení klikněte na tlačítko **Ano**.

Ruční zničení všech vybraných položek

1. Klikněte pravým tlačítkem myši na ikonu **HP ProtectTools** v oznamovací oblasti v pravé části hlavního panelu, zvýrazněte položku **File Sanitizer** a klikněte na příkaz **Zničit nyní**.
2. V dialogovém okně pro potvrzení klikněte na tlačítko **Ano**.

– nebo –

1. Klikněte pravým tlačítkem myši na ikonu **File Sanitizer** na ploše a vyberte příkaz **Zničit nyní**.
2. V dialogovém okně pro potvrzení klikněte na tlačítko **Ano**.

Ruční zahájení čištění volného prostoru

1. Klikněte pravým tlačítkem myši na ikonu **HP ProtectTools** v oznamovací oblasti v pravé části hlavního panelu, zvýrazněte položku **File Sanitizer** a klikněte na příkaz **Vyčistit nyní**.
2. Objeví se bublina informující o zahájení čištění volného prostoru.

– nebo –

1. V levém podokně aplikace Security Manager rozbalte podstrom **File Sanitizer** a klikněte na položku **Čištění**.
2. Klikněte na tlačítko **Vyčistit nyní**.
3. Objeví se bublina informující o zahájení čištění volného prostoru.

Přerušení operace ničení nebo čištění volného prostoru

V průběhu operace ničení nebo čištění volného prostoru se nad ikonou aplikace HP ProtectTools Security Manager v oznamovací oblasti zobrazuje zpráva. Zpráva obsahuje podrobnosti o procesu ničení nebo čištění volného prostoru (průběh v procentech) a poskytuje také možnost přerušení operace.

Postup přerušení operace:

▲ Klikněte na zprávu a poté přerušte operaci kliknutím na příkaz **Zastavit**.

Prohlížení souborů s protokolem

Při každém provedení operace ničení nebo čištění volného prostoru jsou vytvořeny soubory s protokolem o případných chybách nebo selháních. Soubory protokolu jsou vždy aktualizovány podle poslední operace ničení nebo čištění volného prostoru.

POZNÁMKA: Soubory úspěšně zničené nebo vyčištěné se v souborech protokolu neobjeví.

Jeden soubor protokolu se vytvoří pro operace ničení a jeden pro operace čištění volného prostoru. Oba soubory protokolu jsou umístěny na pevném disku:

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

9 Device Access Manager for HP ProtectTools

Tento nástroj zabezpečení je k dispozici pouze správcům. Modul Device Access Manager for HP ProtectTools poskytuje následující funkce zabezpečení, které chrání před neoprávněným přístupem k zařízením připojeným k počítači.

- Pro každého uživatele jsou vytvořeny profily zařízení definující oprávnění k přístupu k zařízením.
- Přístup k zařízením může být povolen nebo zakázán na základě členství ve skupinách.

POZNÁMKA: Modul Device Access Manager používá při řízení přístupu funkci systému Windows Místní uživatelé a skupiny. Systémy Windows Home nepodporují funkci Místní uživatelé a skupiny, modul Device Access Manager proto v těchto verzích systému nebude pracovat správně. Modul Device Access Manager však bude pracovat v systému Microsoft Windows Vista Home, pokud k nastavení uživatelů použijete příkazový řádek. Pokyny naleznete v nápovědě k modulu Device Access Manager.

Spuštění služby na pozadí

Aby bylo možné používat profily zařízení, musí být na pozadí spuštěna služba HP ProtectTools Device Locking/Auditing. Když poprvé použijete profily zařízení, konzola pro správu nástroje HP ProtectTools zobrazí dialogové okno s otázkou, zda chcete spustit službu na pozadí. Kliknutím na tlačítko **Ano** službu spustíte a nastavíte její automatické spuštění při každém startu systému.

Jednoduchá konfigurace

Modul Device Access Manager vytvoří během inicializace novou skupinu uživatelů nazvanou Device Administrators (Správci zařízení), jejíž členové mohou zařízení používat a prozkoumávat jako správci. Do této skupiny zařaďte ty uživatele, kteří mají mít plný přístup k zařízením spravovaným v rámci jednoduché konfigurace modulu Device Access Manager.

Tato funkce umožňuje odmítnout přístup k následujícím třídám zařízení:

- Jednotky USB pro všechny uživatele, kteří nejsou správci zařízení
- Všechna výměnná média (diskety, hudební přehrávače, jednotky Flash atd.) pro všechny uživatele, kteří nejsou správci zařízení
- Všechny jednotky DVD/CD-ROM pro všechny uživatele, kteří nejsou správci zařízení
- Všechna sériová a paralelní rozhraní pro všechny uživatele, kteří nejsou správci zařízení

Postup při odmítnutí přístupu k zařízením pro všechny uživatele, kteří nejsou správci zařízení:

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně aplikace klikněte na položku **Device Access Manager** a poté na položku **Jednoduchá konfigurace**.
3. V pravém podokně zaškrtněte políčko u zařízení, ke kterému chcete odmítnout přístup.
4. Klikněte na ikonu **Uložit**.

POZNÁMKA: Pokud není spuštěna služba na pozadí, program se pokusí ji nyní spustit. Povolte spuštění kliknutím na tlačítko **Ano**.

5. Klikněte na tlačítko **OK**.

Konfigurace tříd zařízení (pokročilá funkce)

K dispozici jsou další možnosti, pomocí kterých lze určitým uživatelům nebo skupinám uživatelů povolit nebo zakázat přístup k jednotlivým typům zařízení.

Přidání uživatele nebo skupiny

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně aplikace rozbalte podstrom **Device Access Manager** a poté klikněte na položku **Konfigurace tříd zařízení**.
3. V seznamu zařízení vyberte třídu zařízení, kterou chcete konfigurovat.
4. Klikněte na tlačítko **Přidat**. Otevře se dialogové okno **Vyberte uživatele nebo skupiny**.
5. Kliknutím na tlačítko **Upřesnit** a poté na tlačítko **Najít nyní** vyhledejte uživatele nebo skupiny, které chcete přidat.
6. V seznamu dostupných položek klikněte na uživatele nebo skupiny, které chcete přidat, a klikněte na tlačítko **OK**.
7. Klikněte na tlačítko **OK**.

Odebrání uživatele nebo skupiny

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně aplikace rozbalte podstrom **Device Access Manager** a poté klikněte na položku **Konfigurace tříd zařízení**.
3. V seznamu zařízení vyberte třídu zařízení, kterou chcete konfigurovat.
4. Klikněte na uživatele nebo skupiny, které chcete odebrat, a poté klikněte na možnost **Odebrat**.

Odmítnutí nebo povolení přístupu uživateli nebo skupině

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně aplikace rozbalte podstrom **Device Access Manager** a poté klikněte na položku **Konfigurace tříd zařízení**.
3. V seznamu zařízení vyberte třídu zařízení, kterou chcete konfigurovat.
4. V seznamu **Uživatelé/skupiny** klikněte na uživatele nebo skupiny, kterým chcete zakázat přístup.
5. Klikněte na tlačítko **Odmítnout** vedle uživatele nebo skupiny, kterým chcete zakázat přístup.
6. Klikněte na ikonu **Uložit** a poté na tlačítko **OK**.

Nastavení přístupu uživatelů (pokročilá funkce)

Funkce nastavení řízení přístupu umožňuje správcům určit, kteří uživatelé a skupiny mohou používat zobrazení Jednoduchá konfigurace a konfigurace tříd zařízení.

Aby uživatel nebo skupina mohl prohlížet informace v zobrazení Jednoduchá konfigurace a konfigurace tříd zařízení, musí mu být udělen přístup **Zobrazit nastavení konfigurace (jen pro čtení)**.

Aby uživatel nebo skupina mohl měnit informace v zobrazení Jednoduchá konfigurace a konfigurace tříd zařízení, musí mu být udělen přístup **Změnit nastavení konfigurace**.

Aby uživatel nebo skupina mohl upravovat nastavení v zobrazení Jednoduchá konfigurace a konfigurace tříd zařízení, musí mu být udělen přístup **Plná práva správce uživatelů**.

Přidání uživatele nebo skupiny

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně aplikace rozbalte podstrom **Device Access Manager** a poté klikněte na položku **Nastavení přístupu uživatelů**.
3. Klikněte na tlačítko **Přidat**. Otevře se dialogové okno **Vyberte uživatele nebo skupiny**.
4. Kliknutím na tlačítko **Upřesnit** a poté na tlačítko **Najít nyní** vyhledejte uživatele nebo skupiny, které chcete přidat.
5. V seznamu dostupných položek klikněte na uživatele nebo skupiny, které chcete přidat, a klikněte na tlačítko **OK**.
6. Klikněte na tlačítko **OK**.
7. Klikněte na ikonu **Uložit**.

Odebrání uživatele nebo skupiny

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně aplikace rozbalte podstrom **Device Access Manager** a poté klikněte na položku **Nastavení přístupu uživatelů**.
3. Klikněte na uživatele nebo skupiny, které chcete odebrat, a poté klikněte na možnost **Odebrat**.
4. Klikněte na ikonu **Uložit**.

Povolení nebo odmítnutí přístupu

1. Klikněte na položky **Start** a **Všechny programy** a pak klikněte na položku **Konzola pro správu nástroje HP ProtectTools**.
2. V levém podokně aplikace rozbalte podstrom **Device Access Manager** a poté klikněte na položku **Nastavení přístupu uživatelů**.
3. V poli **Jména skupin nebo uživatelů** vyberte uživatele nebo skupiny.

4. V poli **Oprávnění** zaškrtněte políčko **Povolit** nebo **Odmítnout**.
5. Klikněte na ikonu **Uložit**.

Slovníček

automatické ničení.
Ničení, které uživatel naplánuje pomocí modulu File Sanitizer for HP ProtectTools.

Automatický správce technologie (ATM).
Umožňuje správcům sítě vzdálenou správu počítačů na úrovni systému BIOS.

Čištění.
viz **čištění volného prostoru**.

čištění volného prostoru.
Bezpečné přepsání volného místa na pevném disku náhodnými daty, čímž se výrazně omezí možnost obnovení smazaných dat.

doména.
Skupina počítačů, které jsou součástí jedné sítě a sdílejí společnou adresářovou databázi. Domény mají jedinečné názvy a každá má sadu společných pravidel a postupů.

jednoduché odstranění.
Bezpečně odstraní citlivé informace včetně souborů, historie, obsahu souvisejícího s weby a dalších důvěrných dat.

klávesová zkratka.
Kombinace určitých kláves, jejichž současným stisknutím se zahájí automatické ničení, např. Ctrl+Alt+S.

mazací cyklus.
Jedno přepsání položky náhodnými daty v rámci ničení. Čím vyšší počet mazacích cyklů zvolíte, tím bude zničení bezpečnější.

metoda ověřování.
Metoda používaná pro ověření identity uživatele přihlášeného k počítači.

Ničení.
Provedení algoritmu, který několikrát přepíše danou položku náhodnými daty.

ověřování.
Proces kontroly, zda je uživatel oprávněn provádět určité úlohy, jako je použití počítače, úprava nastavení některého programu nebo prohlížení zabezpečených dat.

ověřování po zapnutí.
Bezpečnostní funkce, která po zapnutí počítače vyžaduje některou formu ověření, např. heslo.

položka.
Určitá data, například osobní údaje nebo soubory, historická data nebo historie prohlížeče atd., umístěná na pevném disku.

profil ničení.
Určená metoda ničení a seznam položek, které se mají ničit.

přihlašovací údaje.
Metoda, kterou uživatel prokazuje oprávnění provést určitou úlohu v procesu ověřování, např. uživatelské jméno a heslo.

restart.
Proces opětovného spuštění počítače.

ruční ničení.
Okamžité zničení položky nebo vybraných položek mimo rámec plánu automatického ničení.

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

správce.
Viz správce systému Windows.

správce systému Windows.
Uživatel s plnými možnostmi měnit oprávnění jiných uživatelů a provádět jejich správu.

uživatelský účet systému Windows.
Profil pro určitého oprávněného uživatele, který umožňuje přihlášení k jednotlivému počítači nebo k síti.

Rejstřík