HP ProtectTools
Uživatelská příručka

První vydání: Říjen 2009

Číslo dílu dokumentace: 572661-221

Obsah

1 Úvod do zabezpečení

Software HP ProtectTools Security Manager poskytuje funkce zabezpečení, které chrání před neoprávněným přístupem k počítačům, sítím a důležitým datům. Administrace softwaru HP ProtectTools Security Manager je zajišťována prostřednictvím funkce Konzola pro správu.

Použití konzoly umožňuje místnímu správci systému provádět následující úlohy:

- Povolit nebo zakázat funkce zabezpečení
- Zahrnout otisky prstů pro uživatele tohoto počítače
- Instalovat čipové karty
- Specifikovat požadované přihlašovací údaje pro ověření
- Spravovat uživatele počítače
- Nastavovat parametry specifické pro zařízení
- Konfigurovat instalované aplikace Security Manager
- Přidávat další aplikace Security Manager

Obsah nabídky dostupných softwarových modulů je závislý na modelu počítače.

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

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

Funkce nástroje HP ProtectTools

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

Modul	Klíčové funkce
Nástroj HP ProtectTools - modul Credential Manager	• Správce hesla funguje jako osobní trezor na heslo, zjednodušující proces jednotného přihlášení, který si automaticky pamatuje a používá přihlašovací údaje uživatele. • Jednotné přihlášení také nabízí zvýšenou ochranu tím, že vyžaduje kombinaci různých bezpečnostních technologií jako jsou Java™ Card a biometrické údaje pro autentikaci uživatele. • Úložiště hesla je chráněno softwarovým šifrováním a může být zdokonaleno použitím ověření pomocí bezpečnostního zařízení (!), například pomocí technologie Java Card nebo pomocí biometriky. **POZNÁMKA:** Funkci Credential Manager najdete v nástroji HP ProtectTools Security Manager pod možností Správce hesla.
Drive Encryption (Šifrování jednotek) pro HP ProtectTools (jen vybrané modely)	• Modul Drive Encryption poskytuje úplné šifrování celého obsahu pevného disku. • Aby mohla být data dešifrována a přístupná, modul Drive Encryption vyžaduje autentikaci před zavedením systému.
Privacy Manager (Správce utajení) pro HP ProtectTools (jen vybrané modely)	• Modul Privacy Manager používá pokročilých přihlašovacích postupů k ověření zdroje, integrity a bezpečnosti komunikace při používání el. pošty, dokumentů sady Microsoft® Office nebo rychlých zpráv (IM).
File Sanitizer (bezpečné odstranění souborů) pro HP ProtectTools	• Modul File Sanitizer umožňuje bezpečné vymazání digitálních informací (citlivých informací včetně souborů aplikací, historického nebo k internetu se vztahujícímu obsahu nebo jiná důvěrná data) na vašem počítači a pravidelné vyčištění pevného disku.
Device Access Manager for HP ProtectTools (jen vybrané modely)	• Modul Device Access Manager umožňuje správcům IT kontrolovat přístup k zařízením založeným na uživatelských profilech. • Modul Device Access Manager brání neoprávněným uživatelům v odstraňování dat pomocí externích paměťových médií a v pronikání virů z externích médií do systému. • Správce může zakázat přístup k zapisovatelným zařízením pro konkrétní jednotlivce nebo skupiny uživatelů.

Dosažení klíčových cílů zabezpečení

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

- Ochrana před cílenou krádeží
- Omezení přístupu k citlivým datům
- Zabránění neoprávněnému přístupu z interních či externích umístění
- Vytvoření silných zásad zabezpečení hesly
- Vyhovění regulatorním požadavkům na bezpečnost.

Ochrana proti cílené krádeži

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

- Funkce ověření před zavedením, je-li povolena, pomáhá zamezit přístup k operačnímu systému. Další informace naleznete v tématech:
  - Security Manager
  - Drive Encryption (Šifrování jednotky)

Omezení přístupu k citlivým údajům

Předpokládejme, že na pracovišti pracuje externí auditor, kterému byl poskytnut počítačový přístup ke kontrole citlivých finančních údajů. Nechcete, aby si mohl tisknout nebo ukládat soubory na zapisovatelná zařízení, např. na disk CD. Následující funkce pomůže omezit přístup k údajům:

- Aplikace Device Access Manager for HP ProtectTools umožňuje IT manažerům omezit přístup na zapisovatelná zařízení, takže citlivé informace nemohou být kopírovány z pevného disku.

Zabránění neoprávněnému přístupu z interních či externích umístění

Neautorizovaný přístup k nezabezpečenému podnikovému PC představuje velmi konkrétní riziko pro zdroje firmy na síti, jako jsou finanční informace, materiály vedení nebo výzkumu a vývoje a důvěrné informace, jako jsou dokumentace pacientů a informace o osobních financích. Následující moduly pomáhají zabránit neautorizovanému přístupu:

- Funkce ověření před zavedením, je-li povolena, pomáhá zamezit přístup k operačnímu systému. Další informace naleznete v tématech:
  - Správce hesel
  - Drive Encryption (Šifrování jednotky)
- Správce hesel pomáhá zajistit, že neoprávněný uživatel nemůže získat heslo pro přístup k aplikacím chráněným heslem.

- Aplikace Device Access Manager for HP ProtectTools umožňuje IT manažerům omezit přístup na zapisovatelná zařízení, takže citlivé informace nemohou být vytištěny nebo kopírovány z pevného disku.
- DriveLock zajišťuje, že na disk nelze přistupovat i v případě, že je pevný disk vyňat a instalován do nezabezpečeného systému.

Vytvoření přísných zásad ohledně hesel

Pokud je zavedeno nařízení, které vyžaduje přísné zásady ohledně hesel pro tucty aplikací a databází založených na webu, Security Manager poskytuje chráněné úložiště pro hesla a pohodlné Jednotné přihlášení.

Další prvky zabezpečení

Přidělení bezpečnostních rolí

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

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

U nástroje HP ProtectTools jsou bezpečnostní funkce a oprávnění rozděleny do následujících rolí:

- Security officer (Správce zabezpečení) – Určuje úroveň zabezpečení společnosti nebo sítě a určuje, jaké funkce zabezpečení se mají použít, například karty Java™ Card, čtečky otisků prstů nebo klíče USB.

  POZNÁMKA: Mnohé funkce HP ProtectTools mohou být upraveny pracovníkem odpovědným za bezpečnost ve spolupráci s HP. Další informace naleznete na internetových stránkách společnosti HP http://www.hp.com.

- IT administrator (Správce IT) – Aplikuje a spravuje funkce zabezpečení určené správcem zabezpečení. Může současně aktivovat a deaktivovat některé funkce. Pokud se správce zabezpečení například rozhodne použít karty Java Cards, může správce IT aktivovat režim zabezpečení kartami Java Card systému BIOS.

- User (Uživatel) – Používá funkce zabezpečení. Pokud například správce zabezpečení a správce IT aktivovali v systému použití karet Java Card, může uživatel nastavit kód PIN karty Java Card a používat ji pro ověřování.

UPOZORNĚNÍ: Správcům je doporučováno při omezení práv koncových uživatelů a omezení uživatelského přístupu postupovat podle „nejlepších postupů“.

Neoprávněným uživatelům by neměla být udělována správcovská oprávnění.

Správa hesel nástroje HP ProtectTools

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

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

Heslo nástroje HP ProtectTools	Nastavuje se v tomto modulu nástroje HP ProtectTools	Funkce
Heslo pro přihlášení do nástroje Security Manager	Security Manager	Heslo nabízí 2 možnosti použití: • Lze je použít k přihlášení k nástroji Security Manager po přihlášení k systému Windows. • Může být použito k umožnění přístupu do systému Windows i nástroje Security Manager současně.

Heslo nástroje HP ProtectTools	Nastavuje se v tomto modulu nástroje HP ProtectTools	Funkce
Heslo souboru obnovení nástroje Security Manager	Modul Security Manager, správce IT	Chrání přístup k souboru pro obnovení nástroje Security Manager.
Kód PIN karty Java™ Card	Zabezpečení karty Java Card	Chrání přístup k obsahu karty Java Card a ověřuje uživatele karty Java Card. Při použití pro ověřování při spuštění omezuje kód PIN karty Java Card současně přístup k nástroji Computer Setup a k obsahu počítače. Ověřuje uživatele modulu Drive Encryption, pokud je vybrána známka karty Java Card.
Heslo pro přihlášení do systému Windows	Ovládací panely systému Windows®	Lze jej použít k ručnímu přihlášení nebo jej lze uložit na kartu Java Card.

Vytvoření bezpečného hesla

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

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

Zálohování a obnova pověření HP ProtectTools

K výběru a zálohování pověření nástrojů HP ProtectTools můžete použít aplikaci Drive Encryption (Šifrování jednotek).

2 Začínáme

POZNÁMKA: Správa nástroje HP ProtectTools vyžaduje oprávnění správce.

Průvodce instalací HP ProtectTools vás provede nastavením nejčastěji používaných funkcí Security Manager. Avšak prostřednictvím Konzoly pro správu nástroje HP ProtectTools je k dispozici velké množství dalších funkcí. Stejné nastavení, jaké najdete v průvodci, stejně jako další bezpečnostní funkce, mohou být konfigurovány prostřednictvím konzoly, kterou otevřete z nabídky Start systému Windows®. Tato nastavení se použijí na počítač a všechny uživatele, kteří jej sdílejí.

1. Na úvodní stránce lze deaktivovat další zobrazování průvodce, a to výběrem jedné z uvedených možností.

2. Po týdnu nastavování počítače, nebo když uživatel se správcovskými právy poprvé přejede prstem přes čtečku otisků prstů, se Průvodce instalací HP ProtectTools automaticky spustí a provede vás základními kroky konfigurace programu. Automaticky se spustí výukové video o nastavení vašeho počítače.

3. Postupujte podle pokynů na obrazovce, dokud nebude nastavení dokončeno.

Pokud nedokončíte průvodce, automaticky se spustí ještě dvakrát. Poté můžete k průvodci přistupovat z bubliny s upozorněním, která se zobrazí v blízkosti oznamovací oblasti hlavního panelu (pokud jste jej nezakázali, jak je popsáno v kroku 2), dokud nebude nastavení dokončeno.

Chcete-li použít aplikace HP ProtectTools Security Manager, spusťte nástroj HP ProtectTools Security Manager z nabídky Start nebo klepněte pravým tlačítkem na ikonu Security Manager v oznamovací oblasti na pravé straně hlavního panelu. Konzola pro správu nástroje HP ProtectTools a její aplikace jsou dostupné všem uživatelům, kteří sdílejí tento počítač.

Spuštění Konzoly pro správu nástroje HP ProtectTools

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

- Klepněte na **Start**, poté na **Všechny programy** a poté klepněte na **HP** a poté na **Konzola pro správu nástroje ProtectTools**.

  nebo

  Na levém panelu nástroje Security Manager klepněte na položku **Správa**.

Pro účely uživatelských úkolů, např. registraci otisků prstů nebo použití Security Manager, spusťte konzolu dle následujícího postupu:

- Klepněte na **Start**, poté na **Všechny programy** a poté klepněte na **HP** a poté na **HP ProtectTools Security Manager**.

  nebo

  Poklepejte na ikonu **HP ProtectTools Security Manager** v oznamovací oblasti na pravé straně hlavního panelu.

Povolení funkce zabezpečení

Průvodce instalací vás požádá o ověření identity.

1. Přečtěte si text na uvítací obrazovce a poté klepněte na tlačítko **Další**.
2. Ověřte svou identitu buď zadáním hesla pro přístup k systému Windows, pokud dosud nemáte zaregistrované žádné otisky prstů, nebo naskenováním otisku prstu pomocí čtečky otisků prstů. Klepněte na tlačítko **Další**.

   Pokud je pole pro heslo pro systém Windows prázdné, budete vyzváni, abyste heslo vytvořili. Heslo pro systém Windows je vyžadováno z důvodu ochrany vašeho účtu v systému Windows před přístupem neautorizovaných osob a kvůli využití funkcí nástroje HP ProtectTools Security Manager.

Průvodce instalací vás provede procesem aktivace bezpečnostních funkcí, které se použijí na všechny uživatele počítače:

- Zabezpečení přihlášení do systému Windows chrání účty systému Windows, neboť požaduje použití specifických přihlašovacích údajů pro přístup.
- Funkce šifrování jednotky ochrání data uložená na pevném disku pomocí šifrování, takže pro osoby bez řádné autorizace budou informace nečitelné.
- Předbootovací zabezpečení ochrání počítač ještě před spuštěním systému Windows zákazem přístupu neautorizovaným osobám.

Chcete-li povolit funkce zabezpečení, zaškrtněte odpovídající políčko. Čím více funkcí zvolíte, tím lépe bude počítač zabezpečen.

POZNÁMKA: Předbootovací zabezpečení nebude dostupné, pokud je systém BIOS nepodporuje.

Registrace otisků prstů

Pokud jste vybrali položku Otisk prstu a počítač je vybaven čtečkou otisků prstů nebo je k ní připojen, budete provedeni postupem nastavení nebo „registrace“ otisků prstů:

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

   POZNÁMKA: Pokud chcete odstranit dříve zaregistrovaný otisk prstu, klepněte na odpovídající prst.

2. Po výběru prstu pro registraci budete vyzýváni k naskenování otisku prstu, dokud neproběhne jeho úspěšná registrace. Zaregistrovaný prst se na obrysu zvýrazní zeleně.

3. Musíte zaregistrovat minimálně dva prsty; vhodnější jsou ukazováčky nebo prostředníčky. Opakujte kroky 1 až 3 pro další prst.

4. Klepněte na tlačítko **Další**.

POZNÁMKA: Pokud registrujete otisky prstů podle postupu v části Začínáme, informace o otiscích prstů se neuloží, dokud neklepnete na tlačítko **Další**. Pokud necháte počítač chvíli neaktivní nebo zavřete panel nástrojů, provedené změny se **neuloží**.

Instalace čipové karty

Pokud jste zvolili „Smart card“ a čtečka čipových karet je zabudovaná nebo připojená k počítači, vyzve vás Průvodce instalací HP ProtectTools k nastavení kódu PIN (osobní identifikační číslo) čipové karty.

Chcete-li nastavit kód PIN čipové karty, postupujte takto:

1. Na stránce Instalace čipové karty zadejte a potvrďte kód PIN.

   Také můžete změnit kód PIN. Zadejte starý kód PIN a poté zvolte nový.

2. Pokračujte klepnutím na tlačítko **Další**.

Použití Konzoly pro správu

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

Konzola se skládá z následujících komponent:

- **Nástroje** – Slouží k zobrazení následujících kategorií pro konfiguraci zabezpečení ve vašem počítači:
  - **Domů** – Umožňuje vybírat úlohy zabezpečení, které mají být prováděny:
  - **Systém** – Umožňuje konfigurovat funkce zabezpečení a ověřování pro uživatele a zařízení.
  - **Aplikace** – Slouží k zobrazení obecných nastavení nástroje HP ProtectTools Security Manager a aplikací Security Manager.
  - **Data** – Poskytuje rozbalovací nabídku odkazů na aplikace Security Manager, které chrání vaše data.
- **Nástroje pro správu** – Poskytují informace o dalších nástrojích. Na příslušném panelu jsou zobrazeny následující volby:
  - **Průvodce instalací HP ProtectTools**–Provede vás nastavením HP ProtectTools Security Manager.
  - **Nápověda**–Zobrazí soubor Nápovědy, který poskytne informace o Security Manager jeho předinstalovaných aplikacích. Nápovědy pro aplikace, které můžete přidat, najdete v těchto aplikacích.
  - **Podrobnosti** – Slouží k zobrazení informací o nástroji HP ProtectTools Security Manager, jako je číslo verze a poznámka o autorských právech.
- **Hlavní oblast** – Slouží k zobrazení specifických obrazovek aplikací.

Konzolu pro správu HP ProtectTools spustíte klepnutím na **Start**, **Všechny programy**, poté na **HP** a poté klepněte na **Konzola pro správu HP ProtectTools**.

3 Konfigurace vašeho systému

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

Systémová skupina obsahuje následující aplikace:

- **Zabezpečení** – Zajišťuje správu funkcí, ověřování a nastavení řídící interakce uživatelů s počítačem.
- **Uživatelé** – Slouží k nastavení, správě a registraci uživatelů počítače.
- **Zařízení** – Slouží ke správě nastavení bezpečnostních zařízení vestavěných do počítače nebo k němu připojených.

Nastavení ověřování v počítači

V aplikaci Ověřování můžete vybrat, která funkce zabezpečení by se měla implementovat do počítače, nastavit zásady regulující přístup do počítače a konfigurovat další rozšířená nastavení. Můžete určit přihlašovací údaje vyžadované k ověření každé třídy uživatelů při přihlašování do systému Windows nebo při přihlašování k webovým stránkám a programům během relace uživatele.

Chcete-li v počítači nastavit ověřování, postupujte takto:

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

Zásady přihlášení

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

1. V nabídce Nástroje klepněte na možnost **Zabezpečení** a poté klepněte na možnost **Ověřování**.
2. Na kartě **Zásady přihlášení** klepněte na kategorii uživatele.
3. Určete ověřované přihlašovací údaje, které jsou požadované pro zvolenou kategorii uživatelů. Musíte určit alespoň jeden přihlašovací údaj.
4. Vyberte, zda má být k ověření uživatele vybrán NĚKTERÝ (pouze jeden) ze specifikovaných pověření nebo VŠECHNY specifikované přihlašovací údaje. Můžete také jakémukoliv uživateli zabránit v přístupu k počítači.
5. Klepněte na tlačítko **Použít**.

Zásady relace

Definování zásad spravujících přihlašovací údaje požadované pro přístup k aplikacím HP ProtectTools během relace v systému Windows:

1. V nabídce Nástroje klepněte na možnost **Zabezpečení** a poté klepněte na možnost **Ověřování**.
2. Na kartě **Zásady relace** klepněte na kategorii uživatele.
3. Určete ověřované přihlašovací údaje, které jsou požadované pro zvolenou kategorii uživatelů.
4. Vyberte, zda má být k ověření uživatele vybrán NĚKTERÝ (pouze jeden) ze specifikovaných pověření nebo VŠECHNY specifikované přihlašovací údaje. Pro přístup k softwaru HP ProtectTools také nemusíte požadovat žádné ověření.
5. Klepněte na tlačítko **Použít**.

Nastavení

Můžete povolit nejméně jedno z následujících nastavení zabezpečení:

- **Povolit přihlášení v jednom kroku** – Umožňuje uživateli počítače přeskočit přihlášení do systému Windows, pokud bylo provedeno ověření v systému BIOS nebo na úrovni šifrovaného disku.
- **Povolit ověření funkcí HP SpareKey pro přihlášení do systému Windows** – Umožňuje uživateli počítače použít funkci HP SpareKey pro přihlášení do systému Windows nehledě na jakékoli další zásady ověřování požadované nástrojem Security Manager.

Chcete-li upravit nastavení, postupujte takto:

1. Klepnutím na možnost povolte nebo zakažte určité nastavení.
2. Klepnutím na možnost **Použít** uložíte provedené změny.

Správa uživatelů

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

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

Další uživatele můžete přidat klepnutím na tlačítko **Přidat**.

Chcete-li uživatele odstranit, klepněte na uživatele a poté na tlačítko **Odstranit**.

Zaregistrování otisků prstů nebo nastavení dalších přihlašovacích údajů pro uživatele provedete klepnutím na uživatele a poté klepnutím na tlačítko **Registrovat**.

Chcete-li zobrazit zásady pro určitého uživatele, vyberte uživatele a poté klepněte na možnost **Zobrazit zásady**.

Specifikace nastavení zařízení

V aplikaci Zařízení můžete specifikovat nastavení dostupná pro všechna vestavěná nebo připojená bezpečnostní zařízení rozpoznaná nástrojem HP ProtectTools Security Manager.

Otisky prstů

Stránka Otisky prstů má tři karty: Registrace, Citlivost a Upřesnit.

Registrace

Můžete zvolit minimální a maximální počet otisků prstů, které může uživatel zaregistrovat.

Také můžete vymazat všechna data ze čtečky otisků prstů.

⚠ **VAROVÁNÍ!** Budou vymazána všechna data otisků prstů pro všechny uživatele, včetně správců. Pokud zásady přihlášení vyžadují pouze otisky prstů, může být všem uživatelům zabráněno v přihlášení k počítači.

Citlivost

Citlivost čtečky otisků prstů při skenování otisků prstů se nastavuje pomocí posuvníku.

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

Upřesnit

Můžete nastavit úsporný provoz čtečky otisků prstů v době, kdy je počítač napájen z baterie.

Čipová karta

Můžete nakonfigurovat počítač, aby se automaticky uzamkl, pokud je vyjmuta čipová karta. Počítač se však uzamkne pouze tehdy, pokud byla čipová karta použita pro ověření přihlašovacích údajů při přihlášení do systému Windows. Vyjmutí čipové karty, která nebyla použita pro přihlášení do systému Windows, neuzamkne počítač.

▲ Zaškrtněte odpovídající políčko pro povolení nebo zakázání uzamčení počítače při vyjmutí čipové karty.

4 Konfigurace vašich aplikací

Do skupiny Aplikace se přistupuje z panelu nabídky Aplikace zabezpečení na levé straně Konzoly pro správu nástroje HP ProtectTools. Pro přizpůsobení chování aktuálně nainstalovaných aplikací HP ProtectTools Security Manager můžete použít nabídku Nastavení.

Chcete-li upravit nastavení aplikací, postupujte takto:

1. V nabídce Nástroje, ve skupině **Aplikace** klepněte na možnost **Nastavení**.
2. Klepněte na možnost povolit nebo zakázat určité nastavení.
3. Klepnutím na možnost **Použít** uložte provedené změny.

Karta Obecné

Na kartě Obecné jsou dostupná následující nastavení:

- **Automaticky nespouštět Průvodce instalací pro správce** – Tuto možnost vyberte, abyste zabránili průvodci v automatickém spuštění při přihlášení.
- **Nespouštět automaticky průvodce Začínáme pro uživatele** – Výběrem této možnosti zabráníte automatickému otevření uživatelského nastavení po přihlášení.

Záložka Aplikace

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

- **Security Manager** – Zpřístupní aplikaci Security Manager všem uživatelům počítače.
- **Povolit tlačítko Objevit více** – Umožňuje všem uživatelům tohoto počítače přidávat aplikace do nástroje HP ProtectTools Security Manager klepnutím na tlačítko **[+] Objevit více**.

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

5 Přidání nástrojů pro správu

Do nástroje Security Manager lze přidat nové nástroje pro správu zpřístupňující další aplikace. Správce daného počítače může zakázat tuto funkci pomocí aplikace Nastavení.

Chcete-li přidat další nástroje pro správu, klepněte na položku **[+] Nástroje pro správu**.

Můžete využít přístup k webovým stránkám společnosti DigitalPersona a ověřit, zda jsou k dispozici nové aplikace, nebo můžete vytvořit plán pro automatické aktualizace.

6 HP ProtectTools Security Manager

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

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

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

Postupy nastavení

Začínáme

Průvodce instalací HP ProtectTools se automaticky zobrazí jako výchozí stránka v HP ProtectTools Security Manager, jakmile se instalace dokončí.

Chcete-li nastavit nástroj Security Manager, postupujte takto:

POZNÁMKA: Pokud není k dispozici čtečka otisků prstů ani čipová karta, proveďte pouze kroky 1, 5 a 6.

1. Na úvodní stránce klepněte na tlačítko **Další**.
2. Na následující stránce se zobrazí seznam způsobů ověřování, které jsou v tomto počítači k dispozici. Pokračujte klepnutím na tlačítko **Další**.
3. Na stránce pro ověření identity zadejte heslo pro systém Windows a pak klepněte na tlačítko **Další**.
4. V závislosti na konfiguraci počítače si přečtěte jedno nebo více následujících témat.
   - Pokud je k dispozici čtečka otisků prstů, viz Zahrnutí vašich otisků prstů na stránce 24.
   - Pokud je k dispozici čipová karta, viz Instalace čipové karty na stránce 25.
5. Pokud není k dispozici čtečka otisků prstů ani čipová karta, budete vyzváni k zadání hesla pro systém Windows. Toto heslo musíte v budoucnu použít, kdykoli bude požadováno ověření.
6. Na poslední stránce průvodce klepněte na tlačítko **Dokončit**.

   Zobrazí se nástrojový panel nástroje Security Manager.

Registrace pověření

Pomocí stránky „Má identita“ můžete registrovat různé způsoby ověření nebo pověření. Po jejich registraci můžete tyto způsoby použít k přihlášení k Security Manager.

Zahrnutí vašich otisků prstů

Pokud je váš počítač vybaven nebo připojen ke čtečce otisků prstů, provede vás Průvodce instalací HP ProtectTools procesem nastavení nebo „zahrnutí“ vašich otisků prstů.

1. Přečtěte si text na uvítací obrazovce a poté klepněte na tlačítko **Další**.
2. Ověřte svou identitu buď zadáním hesla pro přístup k systému Windows, pokud dosud nemáte zaregistrované žádné otisky prstů, nebo naskenováním otisku prstu pomocí čtečky otisků prstů. Klepněte na tlačítko **Další**.

   Pokud je pole pro heslo pro systém Windows prázdné, budete vyzváni, abyste heslo vytvořili. Heslo pro systém Windows je vyžadováno z důvodu ochrany vašeho účtu v systému Windows před přístupem neautorizovaných osob a kvůli využití funkcí nástroje HP ProtectTools Security Manager.
3. Zobrazí se obrysy dvou rukou. Prsty, které již jsou registrované, jsou zvýrazněny zeleně. Klepněte na prst na obrysu.

POZNÁMKA: Pokud chcete odstranit dříve zaregistrovaný otisk prstu, klepněte na něj.

4. Po výběru prstu pro registraci budete vyzváni k naskenování otisku prstu, dokud neproběhne jeho úspěšná registrace. Zaregistrovaný prst se na obrysu zvýrazní zeleně.

5. Musíte zaregistrovat minimálně dva prsty; vhodnější jsou ukazováčky nebo prostředníčky. Opakujte kroky 3 a 4 pro další prst.

6. Klepněte na tlačítko **Další**.

POZNÁMKA: Pokud registrujete otisky prstů podle postupu v části Začínáme, informace o otiscích prstů se neuloží, dokud neklepnete na tlačítko **Další**. Pokud necháte počítač chvíli neaktivní nebo zavřete nástrojový panel, provedené změny se **neuloží**.

Změna hesla systému Windows

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

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

1. Na nástrojovém panelu nástroje Security Manager klepněte postupně na položky **Identita**, **Přihlašovací údaje** a **Heslo**.

2. Do textového pole **Aktuální heslo pro systém Windows** zadejte aktuální heslo.

3. Do textového pole **Nové heslo pro systém Windows** zadejte nové heslo a pak je zadejte znovu do pole **Potvrzení nového hesla**.

4. Klepnutím na tlačítko **Změnit** okamžitě nastavíte nově zadané heslo jako aktuální.

Instalace čipové karty

Pokud je čtečka čipových karet vestavěna v počítači nebo je k němu připojena, nástroj Security Manager vás vyzve k nastavení kódu PIN (Personal Identification Number) čipové karty.

- Chcete-li nastavit kód PIN čipové karty, zadejte a potvrďte jej na stránce Instalace čipové karty.
- Chcete-li kód PIN změnit, zadejte nejprve starý kód PIN a poté zvolte nový.

Použití nástrojového panelu nástroje Security Manager

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

Nástrojový panel se skládá z následujících komponent:

- **Identifikační karta** – zobrazuje jméno uživatele v systému Windows a obrázek přiřazený k účtu právě přihlášeného uživatele.
- **Bezpečnostní aplikace** – Slouží k zobrazení nabídky odkazů pro konfiguraci následujících typů zabezpečení:
  - **Identita**
  - **Data**
  - **Tento počítač**
- **Objevit více** – Otevře stránku, kde naleznete další aplikace umožňující zvýšit zabezpečení identity, dat a komunikací.

- **Hlavní oblast** – Slouží k zobrazení specifických obrazovek aplikací.
- **Správa** – Otevře nástroj Konzola pro správu nástroje HP ProtectTools.
- **Tlačítko Nápověda** – Zobrazí informace o aktuální obrazovce.
- **Upřesnit** – Umožňuje přístup k následujícím možnostem:
  - **Předvolby** – Umožňuje upravit nastavení nástroje Security Manager.
  - **Zálohování a obnova** – Umožňuje zálohovat nebo obnovit data.
  - **O aplikaci** – Zobrazí informace o verzi nástroje Security Manager.

Spuštění nástrojového panelu Security Manager provedete klepnutím na **Start**, **Všechny programy**, **HP** a poté klepněte na **HP ProtectTools Security Manager**.

Spuštění HP ProtectTools Security Manager

HP ProtectTools Security Manager můžete spustit jakýmkoliv z následujících způsobů:

- Klepněte na **Start**, poté na **Všechny programy** a poté klepněte na **HP** a poté na **HP ProtectTools Security Manager**.
- Poklepejte na ikonu **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu.
- Klepněte pravým tlačítkem myši na ikonu **HP ProtectTools** a pak klepněte na příkaz **Spustit nástroj HP ProtectTools Security Manager**.
- Klepněte na miniaplikaci **Security Manager ID Card** na postranním panelu Windows.
- Stisknutím kombinace kláves ctrl+alt+h otevřete nabídku rychlých odkazů nástroje Security Manager.

Obecné úlohy

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

- **Security Manager** – Vytvoří a spravuje Rychlé odkazy, které umožňují spustit a přihlásit se na webové stránky a programy ověřením pomocí vašeho hesla systému Windows, vašich otisků prstů nebo karty Smart.
- **Přihlašovací údaje** – Nabízí snadný způsob změny hesla pro systém Windows, registrace otisku prstu či nastavení čipové karty.

Chcete-li přidat další aplikace, klepněte na tlačítko [+] **Objevte více** v levém dolním rohu nástrojového panelu. Toto tlačítko však může být zakázáno správcem.

Správce hesel

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

Správce hesel nabízí následující možnosti:

- Karta Správa umožňuje přidávat, upravovat a odstraňovat přihlášení.
- Rychlé odkazy umožňují spustit výchozí prohlížeč a přihlásit se k libovolnému webu nebo programu, který byl nastaven.
- Přetažením pomocí myši lze jednotlivé Rychlé odkazy uspořádat do kategorií.
- Je možné rychle zkontrolovat, zda je některé z použitých hesel ohroženo, a automaticky vytvářet komplexní silná hesla pro nové weby.

Celá řada funkcí Správce hesel je k dispozici rovněž prostřednictvím ikony Správce hesel, která se zobrazí v případě, že je fokus nastaven na přihlašovací obrazovce programu nebo webové stránky. Klepnutím na ikonu zobrazíte kontextovou nabídku, která nabízí následující možnosti.

Webové stránky a programy, pro něž dosud nebylo vytvořeno přihlášení

V kontextové nabídce jsou zobrazeny následující možnosti:

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

Webové stránky a programy, pro něž již bylo vytvořeno přihlášení

V kontextové nabídce jsou zobrazeny následující možnosti:

- **Vyplnit přihlašovací údaje** – Vloží přihlašovací údaje do přihlašovacích polí a pak stránku odešle (pokud při vytvoření nebo poslední úpravě přihlášení bylo určeno odeslání).
- **Upravit přihlášení** – Umožňuje upravit přihlašovací údaje pro daný web.

- **Přidat nový účet** – Umožňuje přidat k přihlášení nový účet.
- **Spustit Správce hesel** – Spustí aplikaci Správce hesel.
- **Nápověda** – Zobrazí nápovědu k softwaru Správce hesel.

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

Přidání přihlášení

Přihlášení k webu nebo programu lze snadno přidat zadáním přihlašovacích informací. Od tohoto okamžiku již bude Správce hesel zadávat tyto informace za vás. Toto přihlášení můžete využít pro přechod k dané stránce nebo programu nebo můžete klepnout na přihlášení v nabídce **Přihlášení**. Správce hesel pak otevře příslušný web nebo program a přihlásí vás.

Chcete-li přidat přihlášení, postupujte takto:

1. Otevřete přihlašovací obrazovku pro požadovaný web nebo program.
2. Klepněte na šipku na ikoně **Správce hesel** a pak v závislosti na tom, zda se jedná o přihlášení k webu nebo programu, klepněte na jednu z následujících položek:
   - V případě webu klepněte na položku **Přidat [název domény] do Správce hesel**.
   - V případě programu klepněte na položku **Přidat tuto přihlašovací obrazovku do Správce hesel**.
3. Zadejte přihlašovací údaje. Přihlašovací pole na obrazovce a odpovídající pole v dialogovém okně jsou označena výrazným oranžovým okrajem. Toto dialogové okno můžete rovněž zobrazit klepnutím na položku **Přidat přihlášení** na kartě **Správa Správce hesel**. Některé možnosti závisejí na bezpečnostních zařízeních, která jsou připojena k počítači, například použití klávesové zkratky ctrl+alt+H, skenování otisku prstu či vložení čipové karty.
   - Chcete-li přihlašovací pole vyplnit pomocí některé z předem nastavených možností, klepněte na šipku vpravo od pole.
   - Chcete-li k přihlášení přidat další pole z obrazovky, klepněte na položku **Zvolit další pole**.
   - Chcete-li, aby přihlašovací pole byla vyplněna, ale nikoli odeslána, zrušte zaškrtnutí políčka **Odeslat přihlašovací údaje**.
   - Chcete-li zobrazit heslo pro toto přihlášení, klepněte na položku **Zobrazit heslo**.
4. Klepněte na tlačítko **OK**.

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

Při každém přístupu k tomuto webu nebo spuštění tohoto programu se zobrazí ikona Správce hesel, která indikuje, že k přihlášení lze použít zaregistrované přihlašovací údaje.

Úprava přihlášení

Chcete-li upravit přihlášení, postupujte takto:

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

   Toto dialogové okno můžete rovněž zobrazit klepnutím na položku **Upravit pro požadované přihlášení** na kartě **Správa Správce hesel**.
3. Upravte přihlašovací informace.
   - Chcete-li přihlašovací pole vyplnit pomocí některé z předem nastavených možností, klepněte na šipku vpravo od pole.
   - Chcete-li k přihlášení přidat další pole z obrazovky, klepněte na položku **Zvolit další pole**.
   - Chcete-li, aby přihlašovací pole byla vyplněna, ale nikoli odeslána, zrušte zaškrtnutí políčka **Odeslat přihlašovací údaje**.
   - Chcete-li zobrazit heslo pro toto přihlášení, klepněte na položku **Zobrazit heslo**.
4. Klepněte na tlačítko **OK**.

Použití nabídky přihlášení

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

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

Chcete-li zobrazit nabídku Přihlášení, postupujte takto:

1. Stiskněte kombinaci kláves **Správce hesel**. Nastavení výrobce je ctrl+alt+h. Chcete-li tuto kombinaci kláves změnit, klepněte na položku **Správce hesel** a pak klepněte na položku **Nastavení**.
2. Naskenujte otisk prstu (u počítačů s integrovanou nebo připojenou čtečkou otisků prstů).

Uspořádání přihlášení do kategorií

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

Chcete-li přidat kategorii, postupujte takto:

1. Na nástrojovém panelu nástroje Security Manager klepněte na položku **Správce hesel**.
2. Klepněte na kartu **Správa** a poté na položku **Přidat kategorii**.
3. Zadejte název kategorie.
4. Klepněte na tlačítko **OK**.

Chcete-li přidat přihlášení do kategorie, postupujte takto:

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

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

Správa přihlášení

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

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

Chcete-li provádět správu přihlášení, postupujte takto:

Na nástrojovém panelu nástroje Security Manager klepněte na položku **Správce hesel** a pak klepněte na kartu **Správa**.

- **Přidání přihlášení** – Klepněte na položku **Přidat přihlášení** a postupujte podle pokynů na obrazovce.
- **Úprava přihlášení** – Klepněte na požadované přihlášení, klepněte na položku **Upravit** a pak změňte přihlašovací údaje.
- **Odstranění přihlášení** – Klepněte na požadované přihlášení a pak klepněte na položku **Odstranit**.

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

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

Hodnocení bezpečnosti vašeho hesla

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

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

Nastavení ikony Správce hesel

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

Chcete-li určit, jak má **Správce hesel** pracovat s webovými stránkami obsahujícími přihlášení, klepněte na šipku u ikony a poté vyberte možnost **Nastavení ikony**.

- **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky** – Zaškrtněte toto políčko, chcete-li, aby Správce hesel zobrazoval výzvu k přidání přihlášení vždy, když se zobrazí přihlašovací obrazovka, pro niž dosud nebylo vytvořeno přihlášení.
- **Nezahrnovat tuto obrazovku** – Toto políčko zaškrtněte, chcete-li, aby Správce hesel již nezobrazoval výzvu k přidání přihlášení pro tuto přihlašovací obrazovku.

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

Nastavení

Je možné upravit nastavení nástroje HP ProtectTools Security Manager:

1. **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky** – Ikona Správce hesel se symbolem plus se zobrazí vždy, když je detekována přihlašovací obrazovka webu nebo programu, a indikuje, že je možné do trezoru hesel přidat přihlášení pro tuto obrazovku. Chcete-li tuto funkci zakázat, zrušte v dialogovém okně **Nastavení ikony** zaškrtnutí políčka **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky**.
2. **Spustit Správce hesel pomocí ctrl+alt+H** – Výchozí kombinací kláves pro zobrazení nabídky rychlých odkazů nástroje Správce hesel je ctrl+alt+H. Chcete-li tuto kombinaci kláves změnit, klepněte na tuto položku a stiskněte novou kombinaci kláves. Kombinace kláves mohou obsahovat jeden nebo více následujících prvků: ctrl, alt nebo shift a libovolná alfanumerická klávesa.
3. Změny uložíte klepnutím na tlačítko **Použít**.

Přihlašovací údaje

Přihlašovací údaje nástroje Security Manager slouží k ověření, zda se skutečně jedná o vás. Místní správce tohoto počítače může nastavit, které přihlašovací údaje lze použít k ověření vaší identity při přihlášení k účtu systému Windows, webům nebo programům.

Dostupné přihlašovací údaje se mohou lišit v závislosti na bezpečnostních zařízeních, která jsou vestavěna nebo připojena k tomuto počítači. Pro každý podporovaný přihlašovací údaj existuje položka ve skupině **Identita, Přihlašovací údaje**.

Jsou zde uvedeny přihlašovací údaje, požadavky a aktuální stav a mohou zde být rovněž uvedeny následující prvky:

- Otisky prstů
- Heslo
- Čipová karta

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

Osobní identifikační karta

Identifikační karta vás jednoznačně identifikuje jako vlastníka tohoto účtu systému Windows. Na této kartě se zobrazuje vaše jméno a obrázek podle vašeho výběru. Je nápadně zobrazena v levém horním rohu stránek nástroje Security Manager a také ve formě miniaplikace na postranním panelu Windows.

Klepnutí na identifikační kartu na postranním panelu Windows představuje jeden z mnoha způsobů, jak získat rychle přístup k nástroji Security Manager.

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

Chcete-li změnit zobrazované jméno, postupujte takto:

1. Na nástrojovém panelu nástroje Security Manager klepněte na položku **Identifikační karta** v levém horním rohu.
2. Klepněte na pole se jménem, které jste zadali pro váš účet v systému Windows. Systém zobrazí uživatelské jméno, které je s tímto účtem systému Windows spojené.
3. Chcete-li toto jméno změnit, zadejte nové jméno a klepněte na tlačítko **Uložit**.

Chcete-li změnit zobrazovaný obrázek, postupujte takto:

1. Na nástrojovém panelu nástroje Security Manager klepněte na položku **Identita** a pak klepněte na položku **Identifikační karta** v levém horním rohu.
2. Klepněte na tlačítko **Vybrat obrázek**, vyberte obrázek a poté klepněte na tlačítko **Uložit**.

Nastavení předvoleb

Je možné upravit nastavení nástroje HP ProtectTools Security Manager. Na nástrojovém panelu nástroje Security Manager klepněte na položku **Upřesnit** a pak klepněte na položku **Předvolby**. Dostupná nastavení jsou zobrazena na dvou kartách, Obecné a Otisk prstu.

Obecné

Na kartě Obecné jsou dostupná následující nastavení:

Vzhled – **Zobrazit ikonu na nástrojovém panelu**

Chcete-li povolit zobrazení ikony na nástrojovém panelu, zaškrtněte toto políčko.

Chcete-li zakázat zobrazení ikony na nástrojovém panelu, zrušte zaškrtnutí tohoto políčka.

Otisk prstu

Na kartě Otisk prstu jsou dostupná následující nastavení:

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

Chcete-li přiřadit rychlou akci jedné z uvedených kláves, postupujte takto:

- Klepněte na položku **(Klávesa)+Otisk prstu** a pak klepněte na jeden z dostupných úkolů v nabídce.

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

- **Povolit zvukovou odezvu** – Nástroj Security Manager při naskenování otisku prstu poskytne zvukovou odezvu. Pro jednotlivé události jsou přehrány různé zvuky. Nové zvuky lze těmto událostem rovněž přiřadit pomocí ovládacího panelu Zvuky systému Windows. Chcete-li zvukovou odezvu zakázat, zrušte zaškrtnutí této položky.
- **Zobrazit odezvu kvality skenování** – Ve výchozím nastavení nástroj Security Manager zobrazí obrázek otisku prstu s otazníkem, pokud kvalita naskenovaného otisku prstu neumožňuje ověření. Zobrazení tohoto obrázku lze zakázat zrušením zaškrtnutí tohoto políčka.

Zálohování a obnova vašich dat

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

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

POZNÁMKA: Prostřednictvím této funkce jsou zálohována pouze data.

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

Chcete-li zálohovat data, postupujte takto:

1. Na levém panelu klepněte na položku **Upřesnit** a pak klepněte na položku **Zálohování a obnova**.
2. Klepněte na tlačítko **Zálohovat data**.
3. Vyberte moduly, které chcete zahrnout do zálohování. Ve většině případů pravděpodobně budete chtít zahrnout všechny.
4. Zadejte název souboru se zálohou. Ve výchozím nastavení bude tento soubor uložen do složky Dokumenty. Klepnutím na tlačítko **Procházet** můžete určit jiné umístění.
5. Zadejte heslo, chcete-li zálohu zašifrovat.
6. Ověřte svoji identitu.
7. Klepněte na tlačítko **Dokončit**.

Chcete-li obnovit data, postupujte takto:

1. Na levém panelu klepněte na položku **Upřesnit** a pak klepněte na položku **Zálohování a obnova**.
2. Klepněte na tlačítko **Obnovit data**.
3. Vyberte dříve vytvořený soubor se zálohou. Můžete zadat cestu do příslušného pole, nebo klepnout na tlačítko **Upravit**.
4. Zadejte heslo, kterým jste zálohu zašifrovali.

5. Vyberte moduly, které chcete obnovit. Ve většině případů půjde o všechny zálohované moduly.
6. Klepněte na tlačítko **Dokončit**.

Přidání aplikací

Je možné, že jsou k dispozici další aplikace poskytující nové funkce pro tento program.

Na nástrojovém panelu nástroje Security Manager klepněte na položku **[+] Objevit více**.

POZNÁMKA: Pokud v levém dolním rohu nástrojového panelu není zobrazen odkaz **[+] Objevit více**, byl zablokován správcem tohoto počítače.

Stav bezpečnostních aplikací

Na stránce stavu aplikací nástroje Security Manager se zobrazuje celkový stav všech nainstalovaných bezpečnostních aplikací. Jsou zde uvedeny aplikace, které jsou nainstalovány, a jejich stav. Tento přehled se zobrazí automaticky při otevření nástrojového panelu nástroje Security Manager nebo po klepnutí na položku **Bezpečnostní aplikace**.

7 Drive Encryption (Šifrování jednotek) pro HP ProtectTools (jen vybrané modely)

△ **UPOZORNĚNÍ:** Pokud se rozhodnete odinstalovat modul Drive Encryption (Šifrování jednotky), musíte nejprve dešifrovat veškeré šifrované jednotky. Pokud tak neučiníte, nebudete mít přístup k datům na zašifrovaných jednotkách, pokud jste se nezaregistrovali u služby Drive Encryption recovery (Obnovení šifrování jednotky). Přeinstalování modulu Drive Encryption (Šifrování jednotky) vám neumožní přístup k zašifrovaným jednotkám.

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

Průvodce instalací HP ProtectTools umožňuje správcům systému Windows aktivovat Drive Encryption (Šifrování jednotek), zálohovat šifrovací klíč, přidávat a odstraňovat uživatele a deaktivovat Drive Encryption (Šifrování jednotek). Více informací viz Nápověda softwaru HP ProtectTools Security Manager.

Aplikace Drive Encryption umožňuje provádět následující úlohy:

- Správa šifrování
  - Šifrování nebo dešifrování jednotlivých jednotek

    POZNÁMKA: Šifrovat lze pouze interní pevné disky.
- Obnova
  - Vytvoření záložních klíčů
  - Provedení obnovy

Instalační postupy

Spuštění Drive Encryption (Šifrování jednotky)

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

Všeobecné úlohy

Aktivace Drive Encryption (Šifrování jednotky)

Pomocí Průvodce instalací HP ProtectTools aktivujte Drive Encryption (Šifrování jednotky).

POZNÁMKA: Tohoto průvodce lze rovněž využít k přidání a odebrání uživatelů.

– nebo –

1. Klepněte na **Start**, poté na **Všechny programy** a poté klepněte na **HP** a poté na **Konzola pro správu nástroje ProtectTools**.
2. V levém podokně klepněte na položku **Zabezpečení** a pak klepněte na položku **Funkce**.
3. Zaškrtněte políčko **Drive Encryption** a pak klepněte na tlačítko **Další**.
4. V části **Jednotky, které mají být zašifrovány,** zaškrtněte políčko u pevného disku, který chcete šifrovat.
5. Vložte paměťové zařízení do příslušného slotu.

   POZNÁMKA: Chcete-li uložit šifrovací klíč, je nutné použít paměťové zařízení USB s formátem FAT32.

6. V části **Externí paměťové zařízení pro uložení šifrovacího klíče** zaškrtněte políčko u paměťového zařízení, do něhož má být uložen šifrovací klíč.
7. Klepněte na tlačítko **Použít**.

   Bude zahájeno šifrování jednotky.

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

Deaktivace aplikace Drive Encryption

Pomocí Průvodce instalací HP ProtectTools deaktivujte Drive Encryption (Šifrování jednotky). Více informací viz Nápověda softwaru HP ProtectTools Security Manager.

– nebo –

1. Klepněte na **Start**, poté na **Všechny programy** a poté klepněte na **HP** a poté na **Konzola pro správu nástroje ProtectTools**.
2. V levém podokně klepněte na položku **Zabezpečení** a pak klepněte na položku **Funkce**.
3. Zrušte zaškrtnutí políčka **Drive Encryption** a pak klepněte na tlačítko **Použít**.

   Bude zahájeno dešifrování jednotky.

Přihlášení po aktivaci aplikace Drive Encryption

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

POZNÁMKA: Pokud správce systému Windows aktivoval funkci Prebootovací zabezpečení nástroje HP ProtectTools Security Manager, budete se po zapnutí počítače okamžitě přihlašovat k počítači a nezobrazí se přihlašovací obrazovka aplikace Drive Encryption.

1. Klepněte na své uživatelské jméno a pak zadejte heslo systému Windows nebo kód PIN karty Java™ nebo přiložte zaregistrovaný prst.
2. Klepněte na tlačítko **OK**.

POZNÁMKA: Použijete-li k přihlášení na přihlašovací obrazovce Drive Encryption klíč obnovy, budete rovněž vyzváni k výběru přihlašovacího jména systému Windows a k zadání hesla na přihlašovací obrazovce systému Windows.

Chraňte vaše data zašifrováním pevného disku

Pomocí Průvodce instalací HP ProtectTools chraňte vaše data šifrováním pevného disku:

1. V nástroji Security Manager klepněte na tlačítko **Začínáme** a poté na ikonu **Nastavení nástroje Security Manager**. Je spuštěna ukázka popisující funkce nástroje Security Manager. (Nástroj Security Manager lze rovněž spustit ze stránky Drive Encryption.)
2. V levém podokně klepněte na položku **Drive Encryption** a pak klepněte na položku **Správa šifrování**.
3. Klepněte na tlačítko **Změnit šifrování**.
4. Vyberte jednotky, které mají být zašifrovány.

POZNÁMKA: Důrazně se doporučuje zašifrovat pevný disk.

Zobrazení stavu šifrování

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

POZNÁMKA: Ke změně stavu šifrování je nutné použít nástroj Konzola pro správu nástroje HP ProtectTools.

1. Otevřete nástroj **HP ProtectTools Security Manager**.
2. V části **Moje data** klepněte na položku **Stav šifrování**.

   Je-li aplikace Drive Encryption aktivní, zobrazí se jako stav jednotky jeden z následujících stavových kódů:

   - Aktivní
   - Neaktivní
   - Nešifrováno
   - Šifrováno
   - Šifrování
   - Dešifrování

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

Pokročilé operace

Správa Drive Encryption (Šifrování jednotek) (úloha správce)

Průvodce nastavením nástroje HP ProtectTools Security Manager umožňuje správcům systému Windows aktivovat aplikaci Drive Encryption, zálohovat šifrovací klíč, přidat či odebrat uživatele a deaktivovat aplikaci Drive Encryption.

- Pokud je stav Neaktivní, nebylo šifrování jednotky v HP ProtectTools Security Manager aktivováno správcem Windows a nechrání pevný disk. Pomocí Průvodce instalací HP ProtectTools Security Manager aktivujte Drive Encryption (Šifrování jednotky).
- Je-li nastaven stav Aktivní, aplikace Drive Encryption byla aktivována a nakonfigurována. Jednotka je v některém z následujících stavů:
  - Nešifrováno
  - Šifrováno
  - Šifrování
  - Dešifrování

Šifrování nebo dešifrování individuálních jednotek

Chcete-li zašifrovat jednu nebo více jednotek v počítači nebo dešifrovat jednotku, která již byla zašifrována, použijte funkci Změnit šifrování:

1. Spusťte nástroj **Konzola pro správu nástroje HP ProtectTools**, klepněte na položku **Drive Encryption** a pak klepněte na položku **Správa šifrování**.
2. Klepněte na tlačítko **Změnit šifrování**.
3. V dialogovém okně Změnit šifrování zaškrtněte políčka u jednotek, které chcete zašifrovat, nebo zrušte jejich zaškrtnutí u jednotek, které chcete dešifrovat, a pak klepněte na tlačítko **OK**.

POZNÁMKA: Při šifrování nebo dešifrování jednotky se v indikátoru průběhu zobrazuje čas zbývající k dokončení procesu v rámci aktuální relace. Pokud je počítač v průběhu šifrování vypnut nebo aktivuje režim spánku nebo hibernace a pak je znovu restartován, je indikátor zbývajícího času nastaven na začátek, ale vlastní šifrování bude pokračovat od místa, kde bylo zastaveno. Zobrazení průběhu a zbývajícího času se bude měnit rychleji a bude odrážet předchozí průběh.

Záloha a obnova (úloha pro správce)

Stránka Obnova umožňuje uživatelům zálohování a obnovu šifrovacích klíčů.

Záloha šifrovacího klíče místní jednotky – Umožňuje při aktivaci aplikace Drive Encryption zálohovat šifrovací klíče na vyjímatelná média.

Tvorba zálohovacích klíčů

Šifrovací klíč pro šifrovanou jednotku lze zálohovat na vyjímatelné paměťové zařízení:

△ **UPOZORNĚNÍ:** Nezapomeňte uložit paměťové zařízení obsahující záložní klíč na bezpečném místě. Zapomenete-li heslo nebo ztratíte-li kartu Java, bude toto zařízení poskytovat jediný přístup k pevnému disku.

1. Spusťte nástroj **Konzola pro správu nástroje HP ProtectTools**, klepněte na položku **Drive Encryption** a pak klepněte na položku **Obnova**.
2. Klepněte na položku **Záložní klíče**.
3. Na stránce Vybrat zálohovací disk zaškrtněte políčko vedle zařízení, do něhož chcete zálohovat záložní klíč, a pak klepněte na tlačítko **Další**.
4. Přečtěte si informace zobrazené na následující stránce a pak klepněte na tlačítko **Další**. Šifrovací klíč bude uložen do vybraného paměťového zařízení.
5. Jakmile se zobrazí dialogové okno s potvrzením, klepněte na tlačítko **Dokončit**.

Provedení obnovy

Zapomenete-li heslo a chcete-li provést obnovu, postupujte takto:

1. Zapněte počítač.
2. Vložte vyjímatelné paměťové zařízení obsahující záložní klíč.
3. Jakmile se zobrazí přihlašovací dialogové okno Drive Encryption for HP ProtectTools, klepněte na tlačítko **Storno**.
4. V levém dolním rohu obrazovky klepněte na položku **Možnosti** a pak klepněte na položku **Obnova**.
5. Vyberte soubor obsahující záložní klíč nebo klepněte na tlačítko **Procházet** a vyhledejte jej a poté klepněte na tlačítko **Další**.
6. Jakmile se zobrazí dialogové okno s potvrzením, klepněte na tlačítko **OK**.

   Počítač se spustí.

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

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

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

Privacy Manager zlepšuje bezpečnostní infrastrukturu nástroje HP ProtectTools Security Manager, který zahrnuje následující bezpečné způsoby přihlašování:

- ověřování otiskem prstu,
- heslo pro systém Windows®,
- karta HP ProtectTools Java™.

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

Privacy Manager vyžaduje následující:

- HP ProtectTools Security Manager 5.00 nebo vyšší
- Operační systém Windows® 7, Windows Vista® nebo Windows XP
- Microsoft Outlook 2007 nebo Microsoft Outlook 2003
- Platný e-mailový účet

POZNÁMKA: Certifikát Privacy Manager (digitální certifikát) musí být vyžádán a instalován prostřednictvím Privacy Manager dříve, než budete mít přístup k bezpečnostním funkcím. Informace o vyžádání certifikátu Privacy Manager viz Požadavek a instalace certifikátu Privacy Manager na stránce 42.

Instalační postupy

Spouštění Privacy Manager

Spuštění Privacy Manager:

1. Klepněte na **Start**, poté na **Všechny programy** a poté klepněte na **HP** a poté na **HP ProtectTools Security Manager**.
2. Klepněte na **Privacy Manager**.

– nebo –

Klepněte pravým tlačítkem na ikonu **HP ProtectTools** v oznamovací oblasti v pravé části hlavního panelu, klepněte na **Privacy Manager** a poté na **Konfigurace**.

– nebo –

Na liště zpráva el. pošty Microsoft Outlook klepněte na šipku dolů vedle **Odeslat bezpečně** a poté klepněte na **Certifikáty** nebo **Důvěryhodné kontakty**.

– nebo –

Na liště zpráva dokumentu Microsoft Office klepněte na šipku dolů vedle **Podepsat a šifrovat** a poté klepněte na **Certifikáty** nebo **Důvěryhodné kontakty**.

Správa certifikátů Privacy Manager

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

Můžete provádět následující úlohy:

- zažádat či nainstalovat certifikát nástroje Privacy Manager,
- zobrazit podrobnosti o certifikátech nástroje Privacy Manager,
- prodloužit platnost certifikátu nástroje Privacy Manager,
- při více dostupných certifikátech nastavit výchozí certifikát nástroje Privacy Manager,
- odstranit či stornovat certifikát nástroje Privacy Manager (pokročilé nastavení).

Požadavek a instalace certifikátu Privacy Manager

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

Zažádání o certifikát nástroje Privacy Manager

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

Do aplikace Microsoft Outlook vám přijde e-mail s připojeným certifikátem nástroje Privacy Manager.

Získání předdefinovaného korporátního certifikátu Privacy Manager

1. V aplikaci Outlook otevřete e-mailovou zprávu informující o tom, že vám byl předem přidělen podnikový certifikát.
2. Klepněte na položku **Získat**.
3. V aplikaci Microsoft Outlook obdržíte e-mail s připojeným certifikátem nástroje Privacy Manager.
4. Instalace certifikátu viz Instalace certifikátu nástroje Privacy Manager na stránce 43

Instalace certifikátu nástroje Privacy Manager

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

△ **UPOZORNĚNÍ:** Soubor se zálohou je vhodné uložit jinam než na pevný disk a uschovat na bezpečném místě. K tomuto souboru, který je potřebný k obnově certifikátu nástroje Privacy Manager a přidružených klíčů, by nikdo neměl mít přístup.

5. Zadejte a potvrďte heslo a pak klepněte na tlačítko **Další**.
6. Pomocí zvolené metody bezpečného přihlášení proveďte ověření.
7. Pokud zvolíte spuštění procesu pozvání Důvěryhodného kontaktu, postupujte podle pokynů na obrazovce a začněte krokem 2 tématu Přidání důvěryhodných kontaktů pomocí kontaktů aplikace Microsoft Outlook na stránce 47.

– nebo –

Pokud klepnete na **Storno**, více informací o pozdějším přidání Důvěryhodného kontaktu najdete v Přidání Důvěryhodného kontaktu na stránce 46.

Zobrazení podrobností o certifikátu nástroje Privacy Manager

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

Prodloužení platnosti certifikátu nástroje Privacy Manager

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

1. Otevřete nástroj Privacy Manager a klepněte na položku **Certifikáty**.
2. Klepněte na položku **Obnovit certifikát**.
3. Podle pokynů na obrazovce proveďte nákup nového certifikátu pro nástroj Privacy Manager.

POZNÁMKA: Proces prodloužení certifikátu Privacy Manager nenahrazuje váš starý certifikát Privacy Manager. Budete muset zakoupit nový certifikát Privacy Manager a instalovat jej stejným způsobem jako v Požadavek a instalace certifikátu Privacy Manager na stránce 42.

Nastavení výchozího certifikátu pro nástroj Privacy Manager

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

Pokud jste vlastníkem více než jednoho certifikátu pro nástroj Privacy Manager, který byl na váš počítač nainstalován, je možné určit, který certifikát bude používán jako výchozí:

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

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

Odstranění certifikátu nástroje Privacy Manager

Pokud odstraníte certifikát Privacy Manager, nemůžete otevřít jakýkoliv soubor nebo zobrazit jakákoliv data, která jste pomocí tohoto certifikátu zašifrovali. Pokud jste omylem odstranili certifikát Privacy Manager, můžete jej obnovit pomocí záložního souboru, který jste vytvořili, když jste certifikát instalovali. Další informace naleznete v Obnovení certifikátu nástroje Privacy Manager na stránce 45.

Odstranit certifikát nástroje nástroj Privacy Manager lze následujícím způsobem:

1. Otevřete nástroj Privacy Manager a klepněte na položku **Certifikáty**.
2. Klepněte na certifikát nástroje Privacy Manager, který má být odstraněn, a klepněte na tlačítko **Upřesnit**.

3. Klepněte na tlačítko **Odstranit**.
4. V otevřeném dialogovém okně klepněte na tlačítko **Ano**.
5. Klepněte na tlačítko **Zavřít** a poté na tlačítko **Použít**.

Obnovení certifikátu nástroje Privacy Manager

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

1. Otevřete nástroj Privacy Manager a klepněte na položku **Přesun**.
2. Klepněte na tlačítko **Obnovit**.
3. Na stránce „Migrační soubor“ klepněte na tlačítko **Procházet** a vyhledejte soubor s příponou .dppsm, který byl vytvořen během procesu zálohování, a pak klepněte na tlačítko **Další**.
4. Zadejte heslo použité při vytvoření zálohy a pak klepněte na tlačítko **Další**.
5. Klepněte na tlačítko **Dokončit**.
6. Klepněte na tlačítko **OK**.

Viz Instalace certifikátu nástroje Privacy Manager na stránce 43 nebo Zálohování certifikátů Privacy Manager a Důvěryhodných kontaktů na stránce 60, kde najdete další informace.

Stornování certifikátu nástroje Privacy Manager

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

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

1. Otevřete nástroj Privacy Manager a klepněte na položku **Certifikáty**.
2. Klepněte na tlačítko **Upřesnit**.
3. Klepněte na certifikát nástroje Privacy Manager, který má být stornován, a poté klepněte na tlačítko **Stornovat**.
4. V otevřeném dialogovém okně klepněte na tlačítko **Ano**.
5. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.
6. Řiďte se instrukcemi na obrazovce.

Správa Důvěryhodných kontaktů

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

Správce důvěryhodných kontaktů umožňuje provádět následující úlohy:

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

Přidání důvěryhodných kontaktů

Postup přidání důvěryhodných kontaktů lze rozdělit na 3 kroky:

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

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

Více informací naleznete v odpovídajících oddílech.

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

Přidání Důvěryhodného kontaktu

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

   – nebo –

   V panelu nástrojů v aplikaci Microsoft Outlook rozviňte nabídku klepnutím na šipku vedle položky **Šifrovat** a poté klepněte na tlačítko **Pozvat kontakt**.

2. Pokud se otevře dialogové okno „Vyberte certifikát“, zvolte certifikát nástroje Privacy Manager, který chcete používat, a klepněte na tlačítko **OK**.
3. Pokud se otevře dialogové okno „Pozvat důvěryhodný kontakt“, přečtěte si text a klepněte na tlačítko **OK**.

   E-mail bude vytvořen automaticky.

4. Zadejte e-mailové adresy všech osob v seznamu, které chcete přidat do důvěryhodných kontaktů.
5. Je možné upravit text zprávy a vložit podpis (nepovinné).
6. Klepněte na tlačítko **Odeslat**.

   POZNÁMKA: Pokud jste nezískali certifikát Privacy Manager, zobrazí se informující zpráva, že musíte mít certifikát Privacy Manager, aby bylo možné odeslat požadavek na Důvěryhodný kontakt. Klepněte na **OK** pro spuštění průvodce požadavkem na certifikát. Další informace naleznete v Požadavek a instalace certifikátu Privacy Manager na stránce 42.

7. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.

POZNÁMKA: Po zaslání pozvánky do důvěryhodných kontaktů je nutné, aby příjemce otevřel email a klepnul na tlačítko **Přijmout** v spodním pravém rohu dopisu a poté v nově otevřeném dialogovém okně klepnul na tlačítko **OK**.

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

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

9. Klepněte na tlačítko **OK**.

Přidání důvěryhodných kontaktů pomocí kontaktů aplikace Microsoft Outlook

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

   – nebo –

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

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

3. Na stránce „Odesílání pozvání“ klepněte na tlačítko **Dokončit**.

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

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

5. Klepněte na tlačítko **Odeslat**.

POZNÁMKA: Pokud jste nezískali certifikát Privacy Manager, zobrazí se informující zpráva, že musíte mít certifikát Privacy Manager, aby bylo možné odeslat požadavek na Důvěryhodný kontakt. Klepněte na **OK** pro spuštění průvodce požadavkem na certifikát. Další informace naleznete v Požadavek a instalace certifikátu Privacy Manager na stránce 42.

6. Pomocí zvolené metody bezpečného přihlášení proveďte ověření.

POZNÁMKA: Jakmile příjemce obdrží tento e-mail, musí jej otevřít a klepnout na tlačítko **Přijmout** v pravém dolním rohu. V dialogu s potvrzením pak musí klepnout na tlačítko **OK**.

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

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

8. Klepněte na tlačítko **OK**.

Zobrazení podrobností o důvěryhodných kontaktech

1. Otevřete nástroj Privacy Manager a klepněte na položku **Důvěryhodné kontakty**.

2. Klepněte na položku Důvěryhodné kontakty.

3. Klepněte na tlačítko **Podrobnosti o kontaktech**.
4. Po prohlédnutí podrobností klepněte na tlačítko **OK**.

Odstranění důvěryhodného kontaktu

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

Kontrola, zda certifikát důvěryhodného kontaktu nebyl stornován

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

1. Otevřete nástroj Privacy Manager a klepněte na položku **Důvěryhodné kontakty**.
2. Klepněte na položku Důvěryhodné kontakty.
3. Klepněte na tlačítko **Upřesnit**.

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

Obecné úlohy

Nástroj Privacy Manager je možné používat s následujícími produkty Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Použití modulu Privacy Manager v Microsoft Outlook

Když je instalován modul Privacy Manager, je na liště Microsoft Outlook zobrazeno tlačítko Privacy a na liště každé zprávy el. pošty Microsoft Outlook je zobrazeno tlačítko Odeslat bezpečně. Pokud klepnete na šipku dolů vedle **Privacy** nebo **Odeslat bezpečně**, můžete si vybrat z následujících možností:

- Podepsat a odeslat (Pouze tlačítko Odeslat bezpečně) - Tato možnost přidá ke zprávě el. pošty digitální podpis a odešle ji, jakmile provedete ověření pomocí vámi zvoleného způsobu bezpečného přihlášení.
- Podepsat pro důvěryhodné kontakty a odeslat (Pouze tlačítko Odeslat bezpečně) - Tato možnost přidá ke zprávě el. pošty digitální podpis a odešle ji, jakmile provedete ověření pomocí vámi zvoleného způsobu bezpečného přihlášení.
- Pozvat kontakty - Tato možnost vám umožní odeslat pozvání Důvěryhodnému kontaktu. Další informace naleznete v Přidání Důvěryhodného kontaktu na stránce 46.
- Pozvat kontakty z Outlooku - Tato možnost vám umožní odeslat pozvání Důvěryhodnému kontaktu všem kontaktům ve vašem adresáři Microsoft Outlook. Další informace naleznete v Přidání důvěryhodných kontaktů pomocí kontaktů aplikace Microsoft Outlook na stránce 47.
- Spustit software Privacy Manager - Možnosti Certifikáty, Důvěryhodné kontakty a Nastavení vám umožní spustit software Privacy Manager pro přidání, zobrazení nebo změnu aktuálních nastavení. Další informace naleznete v Konfigurace Privacy Manager pro Microsoft Outlook na stránce 49.

Konfigurace Privacy Manager pro Microsoft Outlook

1. Spusťte Privacy Manager, klepněte na **Nastavení** a potom na kartu **E-mail**.

   – nebo –

   Na hlavní liště Microsoft Outlook klepněte na šipku dolů vedle **Odeslat bezpečně** (**Privacy** v Outlook 2003) a poté klepněte na **Nastavení**.

   – nebo –

   Na liště el. zprávy Microsoft klepněte na šipku dolů vedle **Odeslat bezpečně** a poté klepněte na **Nastavení**.

2. Zvolte činnosti, které chcete provést při odesílání zabezpečené zprávy el. pošty a poté klepněte na **OK**.

Podepsání a odeslání zprávy el. pošty

1. V Microsoft Outlook klepněte na **Nový** nebo **Odpovědět**.
2. Napište zprávu el. pošty.
3. Klepněte na šipku dolů vedle **Odeslat bezpečně** (**Privacy** v Outlook 2003) a poté klepněte na **Podepsat a odeslat**.
4. Proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.

Zapečetí a odeslání zprávy el. pošty

Zabezpečené zprávy el. pošty, které jsou digitálně podepsány a zabezpečeny (šifrovány) mohou zobrazit pouze lidé, které jste vybrali ze seznamu vašich Důvěryhodných kontaktů.

Zabezpečení a odeslání zprávy el. pošty Důvěryhodnému kontaktu:

1. V Microsoft Outlook klepněte na **Nový** nebo **Odpovědět**.
2. Napište zprávu el. pošty.
3. Klepněte na šipku dolů vedle **Odeslat bezpečně** (**Privacy** v Outlook 2003) a poté klepněte na **Zabezpečit pro Důvěryhodný kontakt a odeslat**.
4. Proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.

Zobrazení zabezpečené zprávy el. pošty

Když otevřete zabezpečenou zprávu el. pošty, v hlavičce se zobrazí bezpečnostní štítek. Bezpečnostní štítek poskytuje následující informace:

- Které pověření byly použity při ověření identity osoby, která podepsala tuto zprávu el. pošty
- Produkt, který byl použit pro ověření pověření osoby, která podepsala zprávu el. pošty

Použití Privacy Manager v dokumentu Microsoft Office 2007

POZNÁMKA: Privacy Manager může být použit pouze s dokumenty Microsoft Office 2007.

Po instalaci certifikátu Privacy Manager se na pravé straně lišty všech dokumentů Microsoft Word, Excel a PowerPoint zobrazí tlačítko Podepsat a šifrovat. Pokud klepnete na šipku dolů vedle **Podepsat a šifrovat**, můžete si vybrat z následujících možností:

- Podepsat dokument - Tato možnost přidá k dokumentu váš digitální podpis.
- Přidat řádek s podpisem před podepsáním (pouze Microsoft Word a Microsoft Excel) - Ve výchozím nastavení je při podpisu nebo šifrování dokumentu Microsoft Word nebo Microsoft Excel přidán řádek s podpisem. Pro vypnutí této možnosti klepnutím na **Přidat řádek s podpisem** odstraňte znaménko zaškrtnutí.
- Šifrovat dokument - Tato možnost přidá k dokumentu váš digitální podpis a zašifruje ho.
- Odstranit šifrování - Tato možnost z dokumentu odstraní šifrování.
- Spustit software Privacy Manager - Možnosti Certifikáty, Důvěryhodné kontakty a Nastavení vám umožní spustit software Privacy Manager pro přidání, zobrazení nebo změnu aktuálních nastavení. Viz Správa certifikátů Privacy Manager na stránce 42, Správa Důvěryhodných kontaktů

na stránce 45, nebo Konfigurace Privacy Manager pro Microsoft Office na stránce 51, kde najdete další informace.

Konfigurace Privacy Manager pro Microsoft Office

1. Spusťte Privacy Manager, klepněte na **Nastavení** a potom na kartu **Dokumenty**.

   – nebo –

   Na liště dokumentu Microsoft Office klepněte na šipku dolů vedle **Podepsat a šifrovat** a poté klepněte na **Nastavení**.

2. Vyberte činnosti, které chcete konfigurovat a klepněte na **OK**.

Podepsání dokumentu Microsoft Office

1. Vytvořte a uložte dokument v Microsoft Word, Excel nebo PowerPoint.
2. Klepněte na šipku dolů vedle **Podepsat a šifrovat** a poté klepněte na **Podepsat dokument**.
3. Proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.
4. Když se zobrazí potvrzující dialogové okno, přečtěte si text a poté klepněte na **OK**.

Pokud se později rozhodnete pro úpravu dokumentu, postupujte dle těchto kroků:

1. Klepněte na tlačítko **Office** v horním levém rohu obrazovky.
2. Klepněte na **Připravit** a poté na **Označit jako konečné**.
3. Po otevření dialogového okna s potvrzením klepněte na **Ano** a pokračujte v práci.
4. Když jste dokončili úpravu dokumentu, podepište jej znovu.

Přidání řádku s podpisem při podepisování dokumentu Microsoft Word nebo Excel

Modul Privacy Manager vám umožňuje přidat při podepisování dokumentu Microsoft Word nebo Excel řádek s podpisem:

1. Vytvořte a uložte dokument v Microsoft Word nebo Excel.
2. Klepněte na nabídku **Domů**.
3. Klepněte na šipku dolů vedle **Podepsat a šifrovat** a poté klepněte na **Přidat řádek s podpisem před podepsáním**.

   POZNÁMKA: Pokud je možnost vybrána, zobrazí se vedle Přidat řádek s podpisem před podepsáním zaškrtávací značka. Ve výchozím nastavení je tato možnost zapnuta.

4. Klepněte na šipku dolů vedle **Podepsat a šifrovat** a poté klepněte na **Podepsat dokument**.
5. Proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.

Přidání navrhovaných podepisujících do dokumentu Microsoft Word nebo Excel

Do dokumentu můžete přidat více než jeden řádek s podpisem určením navrhovaných podepisujících. Navrhovaný podepisující je uživatel, který je navržen majitelem dokumentu Microsoft Word nebo Excel pro přidání řádku s podpisem do dokumentu. Navrhovaný podepisující můžete být buď vy nebo jiná osoba, která chce dokument podepsat. Pokud například připravíte dokument, který musí být podepsán

všemi pracovníky vašeho oddělení, můžete do dokumentu na poslední stránku zahrnout řádky pro podpis těchto uživatelů s pokyny, jak dokument podepsat podle specifického data.

Přidání navrhovaných podepisujících do dokumentu Microsoft Word nebo Excel:

1. Vytvořte a uložte dokument v Microsoft Word nebo Excel.
2. Klepněte na nabídku **Vložit**.
3. Ve skupině **Text** na liště klepněte na šipku vedle **Řádek pro podpis** a poté klepněte na **Poskytovatel podpisu Privacy Manager**.

   Otevře se dialogové okno pro nastavení podpisu.
4. V poli pod **Navrhovaný podepisující** zadejte jméno podepisujícího.
5. V poli pod **Pokyny pro podepisujícího** zadejte zprávu pro podepisujícího.

POZNÁMKA: Tato zpráva se zobrazí na místě titulu a bude buď odstraněna nebo nahrazena titulem uživatele při podpisu dokumentu.

6. Označte zaškrtávací pole **Na řádku s podpisem zobrazit datum** pro zobrazení data.
7. Označte zaškrtávací pole **Na řádku s podpisem zobrazit titul** pro zobrazení titulu.

POZNÁMKA: Protože majitel dokumentu přiděluje navrhované podepisující do svého dokumentu, pokud nejsou zaškrtnuta políčka **Na řádku s podpisem zobrazit datum** a/nebo **Na řádku s podpisem zobrazit titul**, nebude navrhovaný podepisující moci zobrazit datum a/nebo titul na řádku s podpisem ani v případě, že je tak v nastavení dokumentu uvedeno.

8. Klepněte na tlačítko **OK**.

Přidání řádku s podpisem pro navrhovaného podepisujícího

Když navrhovaný podepisující otevře dokument, uvidí své jméno v závorkách, což označuje, že se musí podepsat.

Podepsání dokumentu:

1. Poklepejte na příslušnou řádku pro podpis.
2. Proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.

   Řádka pro podpis se zobrazí dle nastavení provedených majitelem dokumentu.

Šifrování dokumentu Microsoft Office

Dokument Microsoft Office můžete šifrovat pro vás a vaše Důvěryhodné kontakty. Když zašifrovaný dokument zavřete, musíte vy a vámi vybraný(é) Důvěryhodný(é) kontakt(y) ze seznamu provést před jeho otevřením ověření.

Šifrování dokumentu Microsoft Office:

1. Vytvořte a uložte dokument v Microsoft Word, Excel nebo PowerPoint.
2. Klepněte na nabídku **Domů**.
3. Klepněte na šipku dolů vedle **Podepsat a šifrovat** a poté klepněte na **Šifrovat dokument**.

   Otevře se dialogové okno Výběr důvěryhodného kontaktu.

4. Klepněte na jméno Důvěryhodného kontaktu, který bude schopen otevřít dokument a zobrazit jeho obsah.

POZNÁMKA: Pro vybrání více jmen Důvěryhodných kontaktů, podržte klávesu ctrl a klepněte na individuální jména.

5. Klepněte na tlačítko **OK**.

Pokud se později rozhodnete pro úpravu dokumentu, postupujte dle kroků v Odebrání šifrování z dokumentu Microsoft Office na stránce 53: Po odstranění šifrování můžete dokument upravovat. Pro opětovné šifrování dokumentu postupujte dle kroků v této části.

Odebrání šifrování z dokumentu Microsoft Office

Pokud odstraníte šifrování z dokumentu Microsoft Office, nebude již pro vás ani vaše Důvěryhodné kontakty vyžadováno, aby prováděli ověření při otevírání a prohlížení dokumentu.

Odstranění šifrování z dokumentu Microsoft Office:

1. Otevřete šifrovaný dokument Microsoft Word, Excel nebo PowerPoint.
2. Proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.
3. Klepněte na nabídku **Domů**.
4. Klepněte na šipku dolů vedle **Podepsat a šifrovat** a poté klepněte na **Odstranit šifrování**.

Odesílání šifrovaného dokumentu Microsoft Office

Do zprávy el. pošty můžete přikládat šifrovaný dokument Microsoft Office, aniž byste museli podepsat nebo šifrovat samotnou zprávu el. pošty. Vytvořte a odešlete zprávu el. pošty s podepsaným nebo šifrovaným dokumentem naprosto stejně jako s jinou přílohou.

Avšak pro optimální zabezpečení doporučujeme, abyste šifrovali zprávu el. pošty, pokud přikládáte podepsaný nebo šifrovaný dokument Microsoft Office.

Pro odeslání zabezpečené zprávy el. pošty s přiloženým podepsaným a/nebo šifrovaným dokumentem Microsoft Office postupujte dle těchto kroků:

1. V Microsoft Outlook klepněte na **Nový** nebo **Odpovědět**.
2. Napište zprávu el. pošty.
3. Přiložte dokument Microsoft Office.
4. Další pokyny viz Zapečetí a odeslání zprávy el. pošty na stránce 50.

Zobrazení podepsaného dokumentu Microsoft Office

POZNÁMKA: Abyste mohli zobrazit podepsaný dokument Microsoft Office, nemusíte mít certifikát Privacy Manager.

Při otevření podepsaného dokumentu Microsoft Office se na stavové liště ve spodní části okna dokumentu zobrazí ikona Digitálního podpisu.

1. Klepněte na ikonu **Digitální podpisy** pro přepnutí zobrazení dialogového okna Podpisy, které zobrazuje jména všech uživatelů, kteří dokument podepsali a datum podpisu.

2. Klepnutím pravým tlačítkem myši na jméno v dialogovém okně Podpisy a vybráním Podrobnosti podpisu zobrazíte další podrobnosti každého podpisu.

Zobrazení šifrovaného dokumentu Microsoft Office

Pro zobrazení šifrovaného dokumentu Microsoft Office z jiného počítače musíte mít instalován modul Privacy Manager. Navíc musíte obnovit certifikát Privacy Manager, který byl použit pro šifrování souboru.

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

Použití Privacy Manager ve Windows Live Messenger

Privacy Manager přidá následující funkce zabezpečené komunikace do Windows Live Messenger:

- **Zabezpečený chat** - Zprávy jsou přenášeny pomocí SSL/TLS (Secure Sockets Layer/Transport Layer Security) prostřednictvím protokolu XML, což je stejná technologie, která zajišťuje zabezpečené transakce elektronického obchodního styku.
- **Identifikace příjemce** - Můžete ověřit přítomnost a identitu osoby dříve, než odešlete zprávu.
- **Podepsané zprávy** - Můžete elektronicky podepsat vaše zprávy. Po obdržení zprávy příjemcem, pokud bude změněna, bude označena jako neplatná.
- **Funkce Skrýt/zobrazit** - Můžete skrýt jakékoliv nebo všechny zprávy v okně chatu Privacy Manager. Můžete též odeslat zprávu se skrytým obsahem. Před zobrazením zprávy je vyžadováno ověření.
- **Zabezpečit historii chatu** - Protokoly o vašich chatových relacích jsou před uložením šifrovány a před zobrazením vyžadují ověření.
- **Automatické zamknutí/odemknutí** - Okno chatu Privacy Manager můžete zamknout a odemknout nebo nastavit automatické zamknutí po určité době nečinnosti.

Spuštění chatové relace Privacy Manager

POZNÁMKA: Aby bylo možné používat chat Privacy Manager, musí mít obě strany instalován tento modul a certifikát Privacy Manager. Podrobnosti o instalaci certifikátu Privacy Manager viz Požadavek a instalace certifikátu Privacy Manager na stránce 42.

1. Pro spuštění chatu Privacy Manager ve Windows Live Messenger proveďte jeden z následujících postupů:

   a. Klepněte pravým tlačítkem na online kontakt v Live Messenger a potom vyberte **Spustit**.

   b. Klepněte na **Spustit chat**.

– nebo –

a. Poklepejte na online kontakt v Live Messenger a potom klepněte na nabídku **Zobrazit seznam aktivit**.

b. Klepněte na **Činnost** a poté na **Spustit chat**.

– nebo –

a. Klepněte pravým tlačítkem na ikonu ProtectTools v oznamovací oblasti, klepněte na **Privacy Manager pro HP ProtectTools** a poté vyberte **Spustit chat**.

b. V Live Messenger klepněte na **Činnosti: Spusťte Činnost** a poté vyberte **Chat Privacy Manager**.

POZNÁMKA: Každý uživatel musí být online v Live Messenger a uživatelé musí být navzájem zobrazeni online ve svých oknech Live Messenger. Klepnutím vyberte uživatele online.

Privacy Manager odešle pozvání kontaktu pro spuštění chatu Privacy Manager. Když kontakt pozvání přijme, otevře se okno chatu Privacy Manager. Pokud pozvaný kontakt nemá Privacy Manager, bude vyzván k jeho stáhnutí.

2. Klepněte na **Start** pro spuštění zabezpečeného chatu.

Konfigurace Privacy Manager pro Windows Live Messenger

1. V chatu Privacy Manager klepněte na tlačítko **Nastavení**.

   – nebo –

   V Privacy Manager, klepněte na **Nastavení** a potom na kartu **Chat**.

   – nebo –

   V zobrazení historie Privacy Manager Live Messenger klepněte na tlačítko **Nastavení**.

2. Chcete-li specifikovat dobu, kterou Privacy Manager Chat čeká před uzamknutím relace, vyberte číslo z pole **Uzamknout po _ minutách nečinnosti**.

3. Pro specifikaci složky historie pro vaše relace chatu klepněte na **Procházet** pro vyhledání složky a poté klepněte na **OK**.

4. Pro automatické šifrování a uložení vašich relací po jejich uzavření označte zaškrtávací pole **Automaticky uložit zabezpečenou historii chatu**.

5. Klepněte na tlačítko **OK**.

Chatování v okně chatu Privacy Manager

Po spuštění chatu Privacy Manager se otevře okno chatu Privacy Manager ve Windows Live Messenger. Použití chatu Privacy Manager je podobné jako používání základního Windows Live Messenger kromě toho, že následující dodatečné funkce jsou dostupné v okně chatu Privacy Manager:

- **Uložit** – Klepněte na toto tlačítko pro uložení relace chatu do složky specifikované ve vašem nastavení. Můžete také nastavit chat Privacy Manager tak, aby automaticky uložil každou relaci po jejím zavření.
- **Skrýt vše** a **Zobrazit vše** – Klepněte na příslušné tlačítko pro rozbalení nebo skrytí zprávy zobrazené v okně Zabezpečené komunikace. Můžete také skrýt nebo zobrazit individuální zprávy klepnutím na hlavičku zprávy.
- **Jsi tam?** – Klepněte na toto tlačítko pro vyžádání ověření od vašeho kontaktu.
- **Uzamknout** – Klepněte na toto tlačítko pro zavření okna chatu Privacy Manager a pro návrat na okno Vstup na chat. Pro opětovné zobrazení okna Zabezpečená komunikace klepněte na **Pokračovat v relaci** a poté proveďte ověření pomocí vašeho zvoleného způsobu zabezpečení.
- **Odeslat** – Klepněte na toto tlačítko pro odeslání šifrované zprávy vašemu kontaktu.
- **Odeslat podepsané zprávy** – Označte toto zaškrtávací políčko pro elektronické podepsání a šifrování vašich zpráv. Po obdržení zprávy příjemcem, pokud bude změněna, bude označena jako neplatná. Ověření musíte provést pokaždé, když odesíláte podepsanou zprávu.
- **Odeslat skryté** – Označte toto zaškrtávací políčko pro šifrování a odeslání zprávy, kde se bude zobrazovat pouze hlavička zprávy. Váš kontakt musí provést ověření, aby bylo možné přečíst obsah zprávy.

Zobrazení historie chatu

Privacy Manager Chat: V zobrazení historie Live Messenger jsou šifrované soubory relací chatu Privacy Manager. Relace mohou být uložené klepnutím na **Uložit** v okně chatu Privacy Manager nebo konfigurací automatického uložení na kartě chat v Privacy Manager. V prohlížeči se u každé relace zobrazí (šifrovaně) obrazovka se jménem kontaktu a datum a čas započetí a ukončení relace. Ve výchozím stavu jsou zobrazené relace pro všechny účty el. pošty, které jste nastavili. Můžete použít nabídku **Zobrazit historii pro** pro zvolení pouze specifických účtů k zobrazení.

Prohlížeč vám umožňuje provádění následujících operací:

- Odhalit všechny relace na stránce 57
- Odhalit relace pro specifický účet na stránce 57
- Zobrazení ID relace na stránce 57
- Zobrazení relace na stránce 57
- Vyhledat v relacích specifický text na stránce 58
- Odstranit relaci na stránce 58
- Přidat nebo odebrat sloupce na stránce 58
- Filtrování zobrazených relací na stránce 59

Spuštění prohlížeče historie Live Messenger:

- Klepněte pravým tlačítkem na ikonu **HP ProtectTools** v oznamovací oblasti v pravé části hlavního panelu, klepněte na **Privacy Manager: pro HP ProtectTools** a poté klepněte na **prohlížeč historie Live Messenger**.

– nebo –

- V relaci chatu klepněte na **Prohlížeč historie** nebo **Historie**.

Odhalit všechny relace

Odhalením všech relací zobrazíte dešifrovanou obrazovku se jménem kontaktu pro aktuálně vybranou relaci(e) a všechny relace se stejným účtem.

Odhalení všech vašich uložených relací historie chatu:

1. V prohlížeči historie Live Messenger klepněte pravým tlačítkem na relaci a poté vyberte **Odhalit všechny relace**.
2. Proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.

   Obrazovka s názvy kontaktů je dešifrována.
3. Poklepejte na jakoukoliv relaci pro zobrazení tohoto obsahu.

Odhalit relace pro specifický účet

Odhalením relací zobrazíte dešifrovanou obrazovku se jménem kontaktu pro aktuálně vybrané relace.

Odhalení určité relace historie chatu:

1. V prohlížeči historie Live Messenger klepněte pravým tlačítkem na relaci a poté vyberte **Odhalit relaci**.
2. Proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.

   Obrazovka s názvy kontaktu je dešifrována.
3. Poklepáním na zobrazenou relaci zobrazíte její obsah.

POZNÁMKA: Další relace šifrované se stejným certifikátem zobrazí nezajištěné ikony, které označují, že je můžete zobrazit poklepáním na jakoukoliv z těchto relací bez dalšího ověřování. Relace šifrované pomocí různých certifikátů zobrazí zajištěnou ikonu, která označuje, že je zapotřebí další ověření pro tyto relace před zobrazením obrazovky se jménem kontaktu nebo obsahu.

Zobrazení ID relace

Zobrazení ID relace:

- V prohlížeči historie Live Messenger klepněte pravým tlačítkem na jakoukoliv odhalenou relaci a vyberte **Zobrazit ID relace**.

Zobrazení relace

Zobrazením relace otevřete soubor pro prohlížení. Pokud již nebyla relace odhalena (zobrazením dešifrované obrazovky se jménem kontaktu), současně se odhalí.

Zobrazení historie relace Live Messenger:

1. V prohlížeči historie Live Messenger klepněte pravým tlačítkem na relaci a poté vyberte **Zobrazit**.
2. Pokud budete vyzváni, proveďte ověření pomocí vybraného zabezpečeného způsobu přihlášení.

   Obsah relace je dešifrován.

Vyhledat v relacích specifický text

Vyhledávat můžete pouze text v odhalených (dešifrovaných) relacích, které jsou zobrazeny v okně prohlížeče. Jde o relace, kde je obrazovka se jménem kontaktu zobrazena jako prostý text.

Vyhledání textu v historii relací chatu:

1. V prohlížeči historie Live Messenger klepněte na tlačítko **Hledat**.
2. Zadejte hledaný text, nastavte jakékoliv požadované parametry pro vyhledávání a poté klepněte na **OK**.

   Relace, které obsahují text, jsou zvýrazněny v okně prohlížeče.

Odstranit relaci

1. Vyberte relaci z historie chatu.
2. Klepněte na tlačítko **Odstranit**.

Přidat nebo odebrat sloupce

Ve výchozím nastavení jsou v prohlížeči historie Live Messenger zobrazeny 3 nejpoužívanější sloupce. Můžete přidat další sloupce, nebo je naopak odstranit.

Přidání sloupců k zobrazení:

1. Klepněte pravým tlačítkem na hlavičku jakéhokoliv sloupce a poté vyberte **Přidat/odstranit sloupce**.
2. Vyberte hlavičku sloupce v levém panelu a poté klepněte na **Přidat** pro jeho přesun do pravého panelu.

Odstranění sloupců k zobrazení:

1. Klepněte pravým tlačítkem na hlavičku jakéhokoliv sloupce a poté vyberte **Přidat/odstranit sloupce**.
2. Vyberte hlavičku sloupce v pravém panelu a poté klepněte na **Odstranit** pro jeho přesun do levého panelu.

Filtrování zobrazených relací

Seznam relací pro všechny vaše účty je zobrazen v prohlížeči historie Live Messenger. Zobrazené relace též můžete filtrovat dle následujících kritérií:

- Specifické účty. Podrobné informace naleznete v Zobrazení relací pro specifický účet na stránce 59.
- Rozpětí dat. Podrobné informace naleznete v Zobrazení relací pro rozpětí dat na stránce 59.
- Různé složky. Podrobné informace naleznete v Zobrazení relací, které jsou uloženy ve složce jiné, než je výchozí na stránce 59.

Zobrazení relací pro specifický účet

▲ V prohlížeči historie Live Messenger vyberte účet z nabídky **Zobrazit historii pro**.

Zobrazení relací pro rozpětí dat

1. V prohlížeči historie Live Messenger klepněte na ikonu **Pokročilý filtr**.

   Otevře se dialogové okno Pokročilý filtr.

2. Označte zaškrtávací políčko **Zobrazit pouze relace v rámci specifikovaného rozpětí dat**.
3. Do polí **Datum od** a **Datum do** zadejte den, měsíc a/nebo rok nebo klepněte na šipku vedle kalendáře pro vybrání dat.
4. Klepněte na tlačítko **OK**.

Zobrazení relací, které jsou uloženy ve složce jiné, než je výchozí

1. V prohlížeči historie Live Messenger klepněte na ikonu **Pokročilý filtr**.
2. Označte zaškrtávací políčko **Použití alternativní složky historie**.
3. Zadejte umístění složky nebo klepněte na **Procházet** pro vyhledání složky.
4. Klepněte na tlačítko **OK**.

Pokročilé úlohy

Migrace certifikátu Privacy Manager a Důvěryhodných kontaktů na jiný počítač

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

Zálohování certifikátů Privacy Manager a Důvěryhodných kontaktů

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

1. Otevřete nástroj Privacy Manager a klepněte na položku **Přesun**.
2. Klepněte na položku **Záloha**.
3. Na stránce „Vybrat data“ vyberte soubor, který má být přesouván, a klepněte na tlačítko **Další**.
4. Na stránce „Přesouvaný soubor“ zadejte umístění a jméno souboru nebo klepněte na tlačítko **Procházet** a umístění vyhledejte a poté klepněte na tlačítko **Další**.
5. Zadejte a potvrďte heslo. Poté klepněte na tlačítko **Další**.

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

6. Ověřte totožnost vámi zvoleným způsobem zabezpečeného přihlašování.
7. Na stránce „Přesouvaný soubor byl uložen“ klepněte na tlačítko **Dokončit**.

Obnovení certifikátů Privacy Manager a Důvěryhodných kontaktů

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

1. Otevřete nástroj Privacy Manager a klepněte na položku **Přesun**.
2. Klepněte na tlačítko **Obnovit**.
3. Na stránce „Přesouvaný soubor“ klepněte na tlačítko **Procházet**, soubor vyhledejte a poté klepněte na tlačítko **Další**.
4. Zadejte heslo použité při vytvoření souboru zálohy a pak klepněte na tlačítko **Další**.
5. Na stránce „Migrační soubor“ klepněte na tlačítko **Dokončit**.

Centrální správa nástroje Privacy Manager

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

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

9 File Sanitizer (bezpečné odstranění souborů) pro HP ProtectTools

File Sanitizer je nástroj umožňující bezpečné ničení cenných položek (osobní údaje či soubory, webová data a data spojená s historií a další datové součásti) ve vašem počítači a pravidelné vyčištění pevného disku.

POZNÁMKA: Tato verze aplikace File Sanitizer pracuje pouze se systémovým pevným diskem.

Bezpečné odstranění

Ničení se liší od standardního odstranění v systému Windows® (v aplikaci File Sanitizer nazývané také jako jednoduché odstranění) tak, že když položku zničíte pomocí aplikace File Sanitizer, je uplatněn algoritmus, který zakryje data tak, že obnovení původní položky prakticky znemožní. Jednoduché odstranění systémem Windows může soubor (položku) ponechat v pořádku na pevném disku nebo ve stavu, kdy soubor (položku) lze obnovit vyšetřovacími metodami.

Při výběru profilu ničení (Vysoké zabezpečení, Střední zabezpečení či Nízké zabezpečení) je pro ničení automaticky vybrán předdefinovaný seznam položek a metoda odstranění. Můžete si také přizpůsobit profil ničení, což umožňuje zadat počet cyklů ničení, které položky mají být do ničení zahrnuty, před ničením kterých položek má být vyžadováno potvrzení a které položky mají být z ničení vyjmuty. Další informace naleznete v části Výběr nebo tvorba profilu pro bezpečné odstraňování na stránce 66.

Můžete nastavit plán automatického ničení a také můžete položky ničit ručně, kdy je třeba. Další informace naleznete v části Nastavení rozvrhu bezpečného odstraňování na stránce 65, Ruční bezpečné odstranění jednoho prostředku na stránce 70 nebo Ruční bezpečné odstranění všech vybraných položek na stránce 70.

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

Čištění volného prostoru

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

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

POZNÁMKA: Čištění volného prostoru se týká položek odstraněných pomocí koše systému Windows, nebo při ručním odstranění položky. Čištění volného prostoru neposkytuje žádné další zabezpečení zničených položek.

Můžete nastavit plán automatického čištění volného prostoru, nebo můžete čištění ručně aktivovat pomocí ikony **HP ProtectTools** v oznamovací oblasti na pravé straně hlavního panelu. Další informace naleznete v části Nastavení rozvrhu pro čištění volného prostoru na stránce 66 nebo Ručně aktivovat čištění volného místa na stránce 71.

Instalační postupy

Spouštění File Sanitizer

Spuštění aplikace File Sanitizer:

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

– nebo –

▲ Poklikejte na ikonu **File Sanitizer** umístěnou na pracovní ploše.

– nebo –

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

Nastavení rozvrhu bezpečného odstraňování

POZNÁMKA: Informace o volbě předdefinovaného profilu ničení či vytvoření profilu ničení najdete v části Výběr nebo tvorba profilu pro bezpečné odstraňování na stránce 66.

POZNÁMKA: Informace o ručním bezpečném odstraňování prostředků viz část Ruční bezpečné odstranění jednoho prostředku na stránce 70.

1. Spusťte aplikaci File Sanitizer a klikněte na tlačítko **Ničení**.
2. Vyberte možnost ničení:
   - **Vypnutí Windows** – Zvolte tuto možnost, pokud chcete zničit všechny vybrané položky při vypínání systému Windows.

     POZNÁMKA: Když je vybrána tato možnost, zobrazí se při vypínání dialogové okno s dotazem, zda chcete pokračovat zničením souborů, nebo chcete proceduru přeskočit. Kliknutím na tlačítko **Ano** proceduru ničení přeskočíte, kliknutím na tlačítko **Ne** pokračujete v ničení.

   - **Spuštění webového prohlížeče** – Tuto možnost zvolte, pokud chcete zničit všechny vybrané webové položky, jako například historii adres URL webového prohlížeče, při spuštění webového prohlížeče.
   - **Ukončení webového prohlížeče** – Tuto možnost zvolte, pokud chcete zničit všechny vybrané webové položky, jako například historii adres URL webového prohlížeče, při zavření webového prohlížeče.
   - **Sekvence kláves** – Tuto možnost zvolte, pokud chcete zahájit ničení sekvencí kláves.
   - **Plánovač** – Zaškrtněte políčko **Aktivovat plánovač**, zadejte heslo systému Windows a poté zadejte den a čas zničení vybraných položek.

   POZNÁMKA: Soubor formátu DLL bude zničen a odstraněn ze systému jen tehdy, pokud byl přesunut do koše.
3. Klikněte na tlačítko **Použít** a potom na tlačítko **OK**.

Nastavení rozvrhu pro čištění volného prostoru

POZNÁMKA: Čištění volného prostoru se týká položek odstraněných pomocí koše systému Windows, nebo ručně odstraněné položky. Čištění volného prostoru neposkytuje žádné další zabezpečení zničených položek.

Nastavení plánu čištění volného prostoru:

1. Spusťte aplikaci File Sanitizer a klikněte na tlačítko **Čištění volného prostoru**.
2. Zaškrtněte políčko **Aktivovat plánovač**, zadejte heslo systému Windows a poté zadejte den a čas vyčištění pevného disku.
3. Klikněte na tlačítko **Použít** a potom na tlačítko **OK**.

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

Výběr nebo tvorba profilu pro bezpečné odstraňování

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

Výběr předem definovaného profilu bezpečného odstraňování

Při výběru předdefinovaného profilu ničení (Vysoké zabezpečení, Střední zabezpečení či Nízké zabezpečení) je automaticky vybrána předdefinovaná metoda mazání a seznam položek. Kliknutím na tlačítko **Zobrazit podrobnosti** můžete zobrazit předdefinovaný seznam položek vybraných pro zničení.

Volba předdefinovaného profilu ničení:

1. Spusťte aplikaci File Sanitizer a klikněte na tlačítko **Nastavení**.
2. Klikněte na předdefinovaný profil ničení.
3. Kliknutím na tlačítko **Zobrazit podrobnosti** zobrazte seznam položek vybraných pro zničení.
4. V části **Zničit následující** vyberte zaškrtávací políčko vedle každé položky, kterou chcete před zničením potvrdit.
5. Klikněte na tlačítko **Použít** a potom na tlačítko **OK**.

Přizpůsobení profilu bezpečného odstraňování

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

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

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

3. Vyberte položky, které chcete zničit:

   a. V části **Dostupné možnosti ničení** klikněte na položku a poté na možnost **Přidat**.

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

POZNÁMKA: Položku lze z dostupných možností ničení odebrat kliknutím na položku a poté na možnost **Odstranit**.

4. Pod **Bezpečně odstranit následující** zaškrtněte políčko vedle prostředku, který chcete potvrdit před bezpečným odstraněním.

POZNÁMKA: Ze seznamu ničení vyjmete položku kliknutím na ni a poté na možnost **Vyjmout**.

5. Chcete-li soubory nebo složky před automatickým zničením ochránit, klikněte v části **Neničit následující** na možnost **Přidat** a vyhledejte nebo zadejte cestu k názvu souboru nebo ke složce. Klikněte na tlačítko **Otevřít** a poté na tlačítko **OK**.

POZNÁMKA: Ze seznamu výjimek odstraníte položku kliknutím na ni a poté na možnost **Odstranit**.

6. Po dokončení konfigurace profilu ničení klikněte na tlačítko **Použít** a poté na tlačítko **OK**.

Přizpůsobení profilu pro jednoduché odstranění

Profil jednoduchého odstranění provede standardní odstranění položky bez jejího ničení. Při přizpůsobování profilu jednoduchého odstranění, můžete zadat, které položky do jednoduchého odstranění zahrnout, před jednoduchým odstraněním kterých položek má být vyžadováno potvrzení a které položky mají být z odstranění vyjmuty.

POZNÁMKA: Pokud používáte možnost jednoduchého odstranění, lze občas provést čištění volného prostoru nad položkami, které byly odstraněny ručně nebo pomocí koše systému Windows.

Přizpůsobení profilu jednoduchého odstranění:

1. Spusťte aplikaci File Sanitizer, klikněte na tlačítko **Nastavení**, dále **Nastavení jednoduchého odstranění** a poté na položku **Zobrazit podrobnosti**.

2. Vyberte položky, které chcete odstranit:

   a. V části **Dostupné možnosti odstranění** klikněte na položku a poté na možnost **Přidat**.

   b. Vlastní položku přidáte kliknutím na možnost **Přidat vlastní možnost**, zadáním názvu souboru nebo složky a kliknutím na tlačítko **OK**. Klikněte na vlastní položku a potom na tlačítko **Přidat**.

POZNÁMKA: Z dostupných možností odstranění odstraníte položku kliknutím na ni a poté na možnost **Odstranit**.

3. Pod **Odstranit následující** zaškrtněte políčko vedle prostředku, který chcete potvrdit před odstraněním.

POZNÁMKA: Ze seznamu odstranění vyjmete položku kliknutím na ni a poté na možnost **Vyjmout**.

4. V **Neodstraňovat následující** klepněte na **Přidat** pro vybrání určitého prostředku, který chcete z bezpečného odstranění vyjmout.

POZNÁMKA: Ze seznamu výjimek odstraníte položku kliknutím na ni a poté na možnost **Odstranit**.

5. Po dokončení konfigurace profilu jednoduchého odstranění klikněte na tlačítko **Použít** a poté na tlačítko **OK**.

Obecné úlohy

File Sanitizer můžete použít k provedení následujících úkolů:

- Použít kombinaci kláves pro zahájení bezpečného odstranění - Tato funkce vám umožňuje vytvořit kombinaci kláves (například ctrl+alt+s) pro zahájení bezpečného odstranění. Podrobné informace naleznete v Zahájení ničení sekvencí kláves na stránce 69.
- Použití ikony File Sanitizer pro zahájení bezpečného odstranění - Tato funkce je podobná funkci potáhnout a pustit systému Windows. Podrobné informace naleznete v Použití ikony File Sanitizer na stránce 70.
- Ručně bezpečně odstranit specifický prostředek nebo všechny vybrané prostředky - Tyto funkce vám umožňují ruční bezpečné odstranění bez čekání na zahájení pravidelného naplánovaného bezpečného odstranění. Podrobné informace naleznete v Ruční bezpečné odstranění jednoho prostředku na stránce 70 nebo Ruční bezpečné odstranění všech vybraných položek na stránce 70.
- Ručně aktivovat čištění volného prostoru - Tato funkce vám umožňuje ručně aktivovat čištění volného prostoru. Podrobné informace naleznete v Ručně aktivovat čištění volného místa na stránce 71.
- Zrušit operace bezpečného odstranění nebo čištění volného prostoru - Tato funkce vám umožní zastavit operace bezpečného odstranění nebo čištění volného prostoru. Podrobné informace naleznete v Zrušení operace ničení a čištění volného prostoru na stránce 71.
- Zobrazení souboru protokolů - Tato funkce vám umožňuje zobrazit soubor protokolů bezpečného odstranění a čištění volného prostoru, který obsahuje jakékoliv chyby nebo selhání z poslední operace bezpečného odstraňování nebo čištění volného prostoru. Podrobné informace naleznete v Zobrazení souborů protokolů na stránce 71.

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

Zahájení ničení sekvencí kláves

Zadání sekvence kláves:

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

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

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

Zahájení ničení sekvencí kláves:

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

Použití ikony File Sanitizer

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

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

Ruční bezpečné odstranění jednoho prostředku

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

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

   POZNÁMKA: Zvolená položka může být jednotlivý soubor nebo složka.

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

– nebo –

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

– nebo –

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

Ruční bezpečné odstranění všech vybraných položek

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

– nebo –

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

– nebo –

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

Ručně aktivovat čištění volného místa

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

– nebo –

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

Zrušení operace ničení a čištění volného prostoru

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

Zrušení operace:

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

Zobrazení souborů protokolů

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

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

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

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

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

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

- Pro každého uživatele jsou vytvořeny profily zařízení, které definují ta zařízení, ke kterým má nebo nemá povolení přístupu.
- Uživatelé jsou také organizováni do skupin, například jako předem definovaní správci systému. Skupiny je možno nadefinovat také prostřednictvím volby Správa počítače v části Nástroje pro správu v Ovládacích panelech.
- Přístup k zařízením je možno udělovat nebo odepírat na základě členství ve skupinách.
- U zařízení typů jednotky CD-ROM nebo DVD mohou být práva čtení a zápisu udělena nebo odepřena odděleně.

Uživatelům s omezenými oprávněními lze rovněž udělit oprávnění ke čtení a úpravám zásad řízení přístupu k zařízení.

Postupy nastavení

Spuštění aplikace Device Access Manager

Pro spuštění aplikace Device Access Manager postupujte dle těchto kroků:

1. Klepněte na **Start**, poté na **Všechny programy** a poté klepněte na **HP** a poté na **Konzola pro správu nástroje ProtectTools**.
2. V levém panelu klepněte na **Device Access Manager**.

Konfigurace přístupu zařízení

Device Access Manager for HP ProtectTools nabízí tři pohledy:

- Jednoduchá konfigurace se používá k udělení nebo odebrání přístupu třídám zařízení pro členy skupiny Správci zařízení.
- Konfigurace třídy zařízení se používá k udělení a odebrání přístupu typům zařízení nebo specifickým zařízením pro specifické uživatele nebo skupiny.
- Nastavení přístupu uživatelů se používá pro specifikaci toho, kteří uživatelé mohou zobrazit nebo upravit informace Jednoduché konfigurace nebo Konfigurace třídy zařízení.

Skupina Správci zařízení

Pokud je instalována aplikace Device Access Manager, je vytvořena skupina Správci zařízení.

Správce systému může implementovat jednoduché zásady řízení přístupu k zařízením odmítnutím přístupu k sadě tříd zařízení, pokud uživatel není důvěryhodný (co se týká přístupu zařízení). Doporučeným způsobem jak odlišit uživatele „důvěryhodného“ od „nedůvěryhodného“, co se zařízení týká, je učinit všechny „důvěryhodné“ uživatele členy skupiny Správci zařízení. Pokud udělíte členům skupiny Správci zařízení přístup k zařízením pomocí Jednoduché konfigurace nebo Konfigurace třídy zařízení, zajistíte, že „důvěryhodní“ uživatelé budou mít plný přístup ke specifikované sadě tříd zařízení.

POZNÁMKA: Přidání uživatele do skupiny Správci zařízení mu automaticky neumožní přístup k zařízení. Avšak Jednoduchá konfigurace může být použita k udělení přístupu požadované sadě tříd zařízení pro „důvěryhodné" uživatele.

Přidání uživatelů do skupiny Správci zařízení provedete takto:

- U Windows 7, Vista, nebo XP Professional použijte MMC standardní modul snap-in „Místní uživatelé a skupiny“.
- U domácích verzí Windows 7, Vista®, nebo XP zadejte z oprávněného účtu do okna s příkazovým řádkem následující:

```
c:\> net localgroup “Device Administrators” username /ADD
```

Jednoduchá konfigurace

Správci a oprávnění uživatelé mohou Jednoduchou konfiguraci použít pro úpravu přístupu k následujícím třídám zařízení pro všechny nečleny skupiny Správci zařízení.

POZNÁMKA: Aby mohla být tato možnost použita pro čtení informací o přístupu zařízení, musí být uživateli nebo skupině uděleno oprávnění „číst“ pomocí **Nastavení přístupu uživatelů**. Aby mohla být tato možnost použita pro úpravu informací o přístupu zařízení, musí být uživateli nebo skupině uděleno oprávnění „měnit“ pomocí **Nastavení přístupu uživatelů**.

- Všechna vyjímatelná média (diskety, USB disky, atd.)
- Všechny jednotky DVD/CD-ROM
- Všechny sériové a paralelní porty
- Všechna zařízení Bluetooth®
- Všechna infračervená zařízení
- Všechna zařízení modemu
- Všechna zařízení PCMCIA
- Všechna zařízení 1394

Umožnění nebo odepření přístupu ke třídě zařízení všem uživatelům, kteří nejsou správci zařízení, provedete následujícím způsobem:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Jednoduchá konfigurace**.
2. V pravém panelu odmítnete přístup tak, že zaškrtnete políčko pro třídu zařízení nebo specifické zařízení. Pro umožnění přístupu k této třídě zařízení nebo specifickému zařízení zrušte označení políčka.

   Pokud je zaškrtávací políčko šedé, byly hodnoty, které mají vliv na scénář přístupu, změněny v rámci Konfigurace třídy zařízení. Hodnoty resetujete zpět na jednoduché nastavení tak, že zaškrtávací políčko klepnutím označíte nebo nastavíte a poté klepnutím na **Ano** potvrdíte.
3. Klepněte na ikonu **Uložit**.

   POZNÁMKA: Pokud služby v pozadí neběží, otevře se dialogové okno s otázkou, zda je chcete spustit. Klepněte na **Ano**.
4. Klepněte na tlačítko **OK**.

Spouštění služeb na pozadí

Než budou použity profily zařízení, otevře HP ProtectTools Security Manager dialogové okno s otázkou, zda chcete spustit služby na pozadí HP ProtectTools Device Locking/Auditing. Klepněte na **Ano**. Služby na pozadí se spustí a budou se spouštět automaticky, kdykoliv bude zaveden operační systém.

POZNÁMKA: Dříve než se zobrazí výzva pro služby na pozadí, musí být definován profil zařízení.

Správci mohou spustit nebo zastavit tyto služby:

1. Klepněte na tlačítko **Start** a poté na tlačítko **Ovládací panely**.
2. Klepněte na **Nástroje pro správu** a poté klepněte na **Služby**.
3. Vyhledejte službu **HP ProtectTools Device Locking/Auditing**.

Vypnutí služby Device Locking/Auditing nezastaví uzamykání zařízení. Zamykání zařízení podporují dvě komponenty:

- Služba Device Locking/Auditing
- Ovladač DAMDrv.sys

Spuštění služby spustí ovladač zařízení, ale vypnutí služby nezastaví ovladač.

Abyste zjistili, zda služby na pozadí běží, otevřete okno pro zadání příkazu a zadejte sc query flcdlock.

Abyste zjistili, zda ovladač zařízení běží, otevřete okno pro zadání příkazu a zadejte sc query damdrv.

Konfigurace třídy zařízení

Správci a pověření uživatelé mohou zobrazovat a měnit seznam uživatelů a skupin, které mají povolený nebo zakázaný přístup ke třídám zařízení, nebo jednotlivým zařízením.

POZNÁMKA: Aby mohla být tato možnost použita pro čtení informací o přístupu zařízení, musí být uživateli nebo skupině uděleno oprávnění „číst“ pomocí **Nastavení přístupu uživatelů**. Aby mohla být tato možnost použita pro úpravu informací o přístupu zařízení, musí být uživateli nebo skupině uděleno oprávnění „měnit“ pomocí **Nastavení přístupu uživatelů**.

Náhled Konfigurace třídy zařízení má následující části:

- **Seznam zařízení** – Zobrazuje všechny třídy a zařízení, která jsou instalována v systému nebo byla instalována dříve.
  - Pro třídu zařízení je obvykle použita ochrana. Uživatel, nebo vybraná skupina, budou mít přístup k jakémukoliv zařízení ve třídě.
  - Ochrana může být nastavena pro jednotlivá zařízení.
- **Seznam uživatelů** – Zobrazuje všechny uživatele a skupiny, které mají nebo nemají přístup k vybrané třídě zařízení nebo jednotlivému zařízení.
  - Záznam v Seznamu uživatelů může představovat jednotlivého uživatele nebo skupinu, jejíž členem je uživatel.
  - Pokud je záznam uživatele nebo skupiny uživatelů nedostupný, nastavení bylo převzato z třídy zařízení nebo Seznamu zařízení nebo ze složky Tříd.
  - Některé třídy zařízení, např. DVD a CD-ROM, mohou být dále ovládány udělením nebo odepřením přístupu zvlášť pro čtení a zapisování.

    Stejně jako u jiných zařízení a tříd mohou být práva čtení a zapisování převzata. Například přístup ke čtení může být převzat z vyšší třídy, ale přístup k zapisování může být specificky odepřen uživateli nebo skupině.

    POZNÁMKA: Pokud je zaškrtávací pole Čtení prázdné, nemá položka řízení přístupu žádný efekt na přístup ke čtení zařízení. Neuděluje ani neodepírá přístup ke čtení zařízení.

    Příklad 1 - Pokud je uživateli nebo skupině odepřen přístup k zápisu pro zařízení nebo třídu zařízení:

    Stejnému uživateli, stejné skupině nebo členu stejné skupiny může být udělen přístup k zapisování nebo čtení + zapisování pouze pro zařízení, která jsou v hierarchii podřízena tomuto zařízení.

Příklad 2 - Pokud je uživateli nebo skupině udělen přístup k zápisu pro zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny může být odepřen přístup k zapisování nebo čtení + zapisování pouze pro stejné zařízení nebo zařízení, která jsou v hierarchii podřízena tomuto zařízení.

Příklad 3 - Pokud je uživateli nebo skupině udělen přístup pro čtení pro zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny může být odepřen přístup k čtení nebo čtení + zapisování pouze pro stejné zařízení nebo zařízení, která jsou v hierarchii podřízena tomuto zařízení.

Příklad 4 - Pokud je uživateli nebo skupině odepřen přístup k čtení pro zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny může být udělen přístup ke čtení nebo přístup ke čtení + zapisování pouze pro zařízení, která jsou v hierarchii podřízena tomuto zařízení.

Příklad 5 - Pokud je uživateli nebo skupině udělen přístup ke čtení + zápisu pro zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny může být odepřen přístup k zapisování nebo čtení + zapisování pouze pro stejné zařízení nebo zařízení, která jsou v hierarchii podřízena tomuto zařízení.

Příklad 6 - Pokud je uživateli nebo skupině odepřen přístup k čtení + zapisování pro zařízení nebo třídu zařízení:

Stejnému uživateli, stejné skupině nebo členu stejné skupiny může být udělen přístup ke čtení nebo čtení + zapisování pouze pro zařízení, která jsou v hierarchii podřízena tomuto zařízení.

Odepření přístupu uživateli nebo skupině

Pomocí následujících kroků zabráníte uživateli nebo skupině v přístupu k zařízení nebo třídě zařízení:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Konfigurace třídy zařízení**.
2. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat.
   - Třída zařízení
   - Všechna zařízení
   - Jednotlivé zařízení
3. V seznamu **Uživatel/skupiny** klepněte na uživatele nebo skupinu, kterým chcete odepřít přístup.
4. Klepněte na **Odepřít** vedle uživatele nebo skupiny.
5. Klepněte na ikonu **Uložit**.

POZNÁMKA: Pokud uživateli nastavíte odepření nebo povolení na stejné úrovni zařízení, má odepření přednost před povolením přístupu.

Povolení přístupu uživateli nebo skupině

Pomocí následujících kroků povolíte uživateli nebo skupině přístup k zařízení nebo třídě zařízení:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Konfigurace třídy zařízení**.
2. V seznamu zařízení klepněte na jednu z následujících položek:
   - Třída zařízení
   - Všechna zařízení
   - Jednotlivé zařízení
3. Klepněte na tlačítko **Přidat**.

   Otevře se dialogové okno **Vyberte uživatele nebo skupiny**.
4. Klepněte na **Rozšířené** a poté klepněte na **Vyhledat nyní** pro hledání uživatelů nebo skupin pro přidání.
5. Klepnutím na uživatele nebo skupinu je přidáte do seznamu dostupných uživatelů nebo skupin, poté klepněte na **OK**.
6. Klepněte ještě jednou na tlačítko **OK**.
7. Klepnutím na **Povolit** udělíte tomuto uživateli nebo skupině přístup.
8. Klepněte na ikonu **Uložit**.

Odebrání přístupu uživateli nebo skupině

Pomocí následujících kroků odeberete uživateli nebo skupině přístup k zařízení nebo třídě zařízení:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Konfigurace třídy zařízení**.
2. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat.
   - Třída zařízení
   - Všechna zařízení
   - Jednotlivé zařízení
3. Pod **Uživatel/Skupiny** klepněte na uživatele nebo skupinu, kterou chcete odebrat a poté klepněte na **Odebrat**.
4. Klepněte na ikonu **Uložit**.

Povolení přístupu ke třídě zařízení jednomu uživateli ze skupiny

Pomocí následujících kroků povolíte uživateli přístup ke třídě zařízení, zatímco odmítnete přístup ostatním členům skupiny uživatelů:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Konfigurace třídy zařízení**.
2. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat.
   - Třída zařízení
   - Všechna zařízení
   - Jednotlivé zařízení
3. V seznamu **Uživatel/Skupiny** vyberte skupinu, které chcete odepřít přístup a poté klepněte na **Odepřít**.
4. Přejděte do níže uvedené složky požadované třídy a poté přidejte konkrétního uživatele.
5. Klepnutím na tlačítko **Povolit** udělíte tomuto uživateli přístup.
6. Klepněte na ikonu **Uložit**.

Povolení přístupu ke konkrétnímu zařízení jednomu uživateli ze skupiny

Správci mohou povolit přístup uživateli ke konkrétnímu zařízení, zatímco všem ostatním členům skupiny, do které tento uživatel patří, bude odepřen přístup ke všem zařízením ve třídě.

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Konfigurace třídy zařízení**.
2. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat, a poté přejděte do složky pod touto třídou.
3. Klepněte na tlačítko **Přidat**. Otevře se dialogové okno **Vyberte uživatele nebo skupiny**.
4. Klepněte na **Rozšířené** a poté na **Nalézt nyní** pro vyhledání skupiny uživatele, které má být odepřen přístup ke všem zařízením ve třídě.
5. Klepněte na skupinu a potom na tlačítko **OK**.
6. Přejděte na specifické zařízení v rámci třídy zařízení, ke které má být uživateli povolen přístup.
7. Klepněte na tlačítko **Přidat**. Otevře se dialogové okno **Vyberte uživatele nebo skupiny**.
8. Klepněte na **Rozšířené** a poté klepněte na **Vyhledat nyní** pro hledání uživatelů nebo skupin pro přidání.
9. Klepněte na uživatele, kterému chcete povolit přístup, a poté klepněte na tlačítko **OK**.
10. Klepnutím na tlačítko **Povolit** udělíte tomuto uživateli přístup.
11. Klepněte na ikonu **Uložit**.

Resetování konfigurace

△ **UPOZORNĚNÍ:** Resetováním konfigurace zrušíte veškeré změny konfigurace zařízení, které jste zavedli a veškerá nastavení se vrátí na hodnoty nastavené při výrobě.

Pomocí následujících kroků resetujete nastavení konfigurace na hodnoty nastavené výrobcem:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Konfigurace třídy zařízení**.
2. Klepněte na tlačítko **Obnovit**.
3. Pro potvrzení klepněte na **Ano**.
4. Klepněte na ikonu **Uložit**.

Pokročilé operace

Ovládání přístupu k nastavení konfigurace

V **Nastavení přístupu uživatelů** správci určí skupiny nebo uživatele, kterým je umožněno používat stránky Jednoduchá konfigurace a Konfigurace třídy zařízení.

POZNÁMKA: Uživatel nebo skupina musí být „Úplná uživatelská správcovská práva“, aby mohli upravovat Nastavení přístupu uživatelů.

- Uživateli nebo skupině musí být udělen přístup „Zobrazit (pouze pro čtení) nastavení konfigurace“ v Nastavení přístupu uživatelů, aby mohli zobrazit informace o Jednoduché konfiguraci a Konfiguraci třídy zařízení.
- Uživateli nebo skupině musí být udělen přístup „Změnit nastavení konfigurace“ v Nastavení přístupu uživatelů, aby mohli změnit informace o Jednoduché konfiguraci a Konfiguraci třídy zařízení.

POZNÁMKA: I členům skupiny Správci musí být udělen přístup ke „čtení“ pro zobrazení Jednoduché konfigurace nebo Konfigurace třídy zařízení a přístup ke „změně“ pro změnu dat pomocí Jednoduché konfigurace a Konfigurace třídy zařízení.

POZNÁMKA: Po vyhodnocení úrovní přístupu všech uživatelů a skupin je uživateli odepřen přístup k určité úrovni, pokud nemá pro příslušnou úroveň zvoleno buď Povolit nebo Odepřít.

Udělení přístupu existující skupině nebo uživateli

Pomocí následujících kroků udělíte přístup existující skupině nebo uživateli pro zobrazení nebo změnu nastavení konfigurace:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Nastavení přístupu uživatele**.
2. Klepněte na skupinu nebo uživatele, kterému chcete povolit přístup.
3. V **Povolení** klepněte na **Povolit** pro každý typ povolení, které má být uděleno vybrané skupině nebo uživateli.

   POZNÁMKA: Udělená povolení se kumulují. Například uživateli, kterému je uděleno povolení „Změnit nastavení konfigurace“, je automaticky uděleno i povolení „Zobrazit (pouze pro čtení) nastavení konfigurace“. Uživateli, kterému je uděleno povolení „Úplná uživatelská správcovská práva“, jsou udělena i povolení „Změnit nastavení konfigurace“ a „Zobrazit (pouze pro čtení) nastavení konfigurace“.

   - Úplná uživatelská správcovská práva
   - Změnit nastavení konfigurace
   - Zobrazit (pouze pro čtení) nastavení konfigurace
4. Klepněte na ikonu **Uložit**.

Odepření přístupu existující skupině nebo uživateli

Pomocí následujících kroků odepřete přístup existující skupině nebo uživateli pro zobrazení nebo změnu nastavení konfigurace:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Nastavení přístupu uživatele**.
2. Klepněte na skupinu nebo uživatele, kterému chcete odepřít přístup.
3. V **Povolení** klepněte na **Odepřít** pro každý typ povolení, které má být odepřeno vybrané skupině nebo uživateli.
   - Úplná uživatelská správcovská práva
   - Změnit nastavení konfigurace
   - Zobrazit (pouze pro čtení) nastavení konfigurace
4. Klepněte na ikonu **Uložit**.

Přidání nové skupiny nebo uživatele

Pomocí následujících kroků udělíte přístup nové skupině nebo uživateli pro zobrazení nebo změnu nastavení konfigurace:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Nastavení přístupu uživatele**.
2. Klepněte na tlačítko **Přidat**. Otevře se dialogové okno **Vyberte uživatele nebo skupiny**.
3. Klepněte na **Rozšířené** a poté klepněte na **Vyhledat nyní** pro hledání uživatelů nebo skupin pro přidání.
4. Klepněte na skupinu nebo uživatele, poté na **OK** a poté opět na **OK**.
5. Klepnutím na tlačítko **Povolit** udělíte tomuto uživateli přístup.
6. Klepněte na ikonu **Uložit**.

Odebrání přístupu skupině nebo uživateli

Pomocí následujících kroků odeberete přístup skupině nebo uživateli pro zobrazení nebo změnu nastavení konfigurace:

1. V levém panelu **Konzoly pro správu HP ProtectTools** klepněte na možnost **Device Access Manager** a poté klepněte na položku **Nastavení přístupu uživatele**.
2. Klepněte na skupinu nebo uživatele a poté klepněte na **Odebrat**.
3. Klepněte na ikonu **Uložit**.

Související dokumentace

Device Access Manager for HP ProtectTools je kompatibilní s firemním produktem HP ProtectTools Enterprise Device Access Manager. Při práci s firemním produktem umožní Device Access Manager for HP ProtectTools pouze přístup čtení vlastních funkcí.

Více informací o Device Access Manager for HP ProtectTools je k dispozici na webové stránce http://www.hp.com/hps/security/products.

11 LoJack Pro pro HP ProtectTools

Computrace LoJack Pro od Absolute Software (nutno zakoupit zvlášť) se zaměřuje na rostoucí problém zcizení nebo ztráty počítačů.

Aktivace tohoto softwaru zapne agenta Computrace, který ve vašem počítači zůstane aktivním i když je pevný disk zformátován nebo vyměněn.

LoJack Pro povoluje vzdálené monitorování, správu a sledování vašeho počítače. Pokud by došlo ke ztrátě nebo zcizení vašeho počítače, tým Absolute vám pomůže s jeho opětovným získáním.*

POZNÁMKA: *Tato funkce závisí na zeměpisném umístění. Další podrobnosti viz smlouva o poskytování služeb Absolute Software.

12 Řešení potíží

HP ProtectTools Security Manager

Stručný popis	Podrobnosti	Řešení
Karty Smart a tokeny USB nejsou v Security Manager k dispozici, pokud byly instalovány až po něm.	Aby bylo možné používat karty Smart nebo tokeny USB v Security Manager, musí být instalován podpůrný software (ovladače, poskytovatelé PKCS#11, atd.) dříve než Security Manager. Pokud již máte Security Manager instalován, proveďte následující kroky po instalaci podpůrného softwaru karty Smart nebo tokenu:	Přihlaste se ke Správci hesel. V HP ProtectTools Security Manager klepněte na **Správce hesel**, klepněte na **Pověření** a poté klepněte na **Čipová karta** Budete-li vyzváni k restartu počítače, proveďte restart.
Některé webové stránky aplikace vytvářejí chyby, které brání uživateli v provedení nebo dokončení úloh.	Některé webové aplikace ukončí činnost a hlásí chyby z důvodu deaktivace funkčního schématu funkce Single Sign On (Jednotné přihlášení). V aplikaci Internet Explorer se například zobrazí znak **!** ve žlutém trojúhelníku, který oznamuje, že došlo k chybě.	Funkce Jednotné přihlášení Security Manager nepodporuje všechna softwarová rozhraní webu. Deaktivujte tuto funkci pro specifickou webovou stránku vypnutím podpory funkce Jednotné přihlášení. Podívejte se do kompletní dokumentace k funkci Jednotné přihlášení, která je k dispozici v souborech Nápovědy Security Manager. Nelze-li u dané aplikace deaktivovat konkrétní funkci Single Sign On (Jednotné přihlášení), obraťte se na technickou podporu HP a požádejte o podporu třetí úrovně prostřednictvím servisního kontaktu HP.
Možnost **Browse for Virtual Token** (Vyhledat virtuální paměť) se během přihlášení nezobrazuje.	Uživatel nemůže přesunout umístění registrovaného virtuálního tokenu ve Správci hesel, protože možnost procházení byla odstraněna kvůli snížení bezpečnostních rizik.	Možnost procházení byla odstraněna, protože umožňovala neoprávněným uživatelům odstraňovat a přejmenovávat soubory a ovládat systém Windows.
Správci domén nemohou měnit hesla systému Windows ani po ověření.	Stane se to poté, co se přihlásí správce domény a zaregistruje její identitu u Správce hesel pomocí účtu se správcovskými právy k doméně a místnímu PC. Pokud se správce domény pokusí změnit heslo systému Windows ze Správce hesel, správci se zobrazí chyba při přihlašování. **Omezení uživatelského účtu**.	Správce hesel nemůže změnit heslo k účtu uživatele domény prostřednictvím **Změna hesla Windows**. Security Manager může měnit pouze hesla k účtům místního PC. Uživatel domény může měnit jeho/její heslo pomocí možnosti **Změnit heslo** na **Zabezpečení systému Windows**, ale protože uživatel domény nemá fyzický účet na místním PC, Správce hesel může změnit pouze heslo používané při přihlášení.
Správce hesel může být nekompatibilní s Corel WordPerfect 12 heslo GINA.	Pokud se uživatel přihlásí ke Správci hesel, vytvoří dokument v WordPerfect a uloží jej s ochranou heslem, Správce hesel nerozpozná (ručně ani automaticky) heslo GINA.	Společnost HP pracuje na řešení budoucích rozšíření produktů.

Stručný popis	Podrobnosti	Řešení
Správce hesel nerozpozná tlačítko **Připojit** na obrazovce.	Pokud jsou přihlašovací údaje funkce Single Sign On (Jednotné přihlášení) pro připojení RDP (Remote Desktop Connection) nastaveny na možnost **Connect** (Připojit), při novém spuštění funkce Single Sign On (Jednotné přihlášení) se spustí příkaz **Save As** (Uložit jako), nikoli **Connect** (Připojit).	Společnost HP pracuje na řešení budoucích rozšíření produktů.
Uživatel se nemůže přihlásit ke Správci hesel po přepnutí z režimu spánku do hibernace pouze u Windows XP Service Pack 1.	Po umožnění systému, aby se přepnul do režimu hibernace a spánku, se nemůže správce ani uživatel přihlásit ke Správci hesel a přihlašovací obrazovka systému Windows zůstane zobrazena, ať jsou vybrány jakékoliv přihlašovací údaje (heslo, otisky prstů nebo karta Java).	Aktualizace Windows na Service Pack 2 pomocí Windows Update. Více informací o příčině problému viz databáze znalostí Microsoft článek 813301 na http://www.microsoft.com. Aby bylo přihlášení možné, musí uživatel vybrat Správce hesel a přihlásit se. Po přihlášení se ke Správci hesel je uživatel vyzván k přihlášení se do systému Windows (uživatel může vybrat možnost přihlášení se do systému Windows), čímž se dokončí proces přihlášení. Pokud se uživatel přihlásí nejprve do systému Windows, musí se ručně přihlásit ke Správci hesel.
Proces zabezpečení **Restore Identity** (Obnovit identitu) ztrácí přiřazení virtuální paměti.	Pokud uživatel obnoví identitu, může Správce hesel ztratit propojení s umístěním virtuálního tokenu na přihlašovací obrazovce. I když má Správce hesel registrovaný virtuální token, musí jej uživatel znovu registrovat, čímž obnoví propojení.	Aktuálně se jedná o správnou funkci. Pokud se Security Manager odinstaluje bez zachování identit, systémová (serverová) část tokenu je zničena, takže token nelze dále používat pro přihlašování, ani pokud je jeho klientská část obnova pomocí obnovení identity. Společnost HP zkoumá možnosti řešení z dlouhodobého hlediska.

Device Access Manager for HP ProtectTools

Uživatelům byl v rámci aplikace Device Access Manager odmítnut přístup, ale zařízení jsou i nadále přístupná.

- **Vysvětlení** – Zobrazení Simple Configuration (Jednoduchá konfigurace) a/nebo Device Class Configuration (Konfigurace tříd zařízení) bylo v rámci aplikace Device Access Manager použito k odmítnutí přístupu k zařízením. Přestože je přístup odmítnut, uživatelé mají k zařízením i nadále přístup.
- **Řešení:**
  - Ověřte, zda byla spuštěna služba HP ProtectTools Device Locking/Auditing.
  - Jako uživatel s oprávněním správce klepněte na položku **Ovládací panely** a pak na položku **Systém a údržba**. V okně Nástroje pro správu klepněte na položku **Služby** a pak vyhledejte službu **HP ProtectTools Device Locking/Auditing**. Ověřte, zda je tato služba spuštěna a zda je jako typ spuštění uvedena možnost **Automatické**

Uživatel má neočekávaně přístup k zařízení nebo mu byl neočekávaně odmítnut přístup k zařízení.

- **Vysvětlení** – Aplikace Device Access Manager byla použita k odmítnutí přístupu k některým zařízením a k povolení přístupu k jiným zařízením. Uživatel má přístup k zařízením, která podle něj byla pomocí aplikace Device Access Manager odmítnuta, a nemá přístup k zařízením, která by aplikace Device Access Manager měla povolit.
- **Řešení:**
  - Pomocí zobrazení Device Class Configuration (Konfigurace tříd zařízení) ověřte nastavení uživatele v rámci aplikace Device Access Manager.
  - Klepněte na položku **Security Manager**, pak na položku **Device Access Manager** a nakonec klepněte na položku **Device Class Configuration** (Konfigurace tříd zařízení). Rozbalte úrovně ve stromu tříd zařízení a ověřte nastavení platná pro tohoto uživatele. Zkontrolujte všechna oprávnění Deny (Odmítnout), která jsou nastavena pro tohoto uživatele nebo pro libovolnou skupinu Windows, které může být členem, například skupinu Users či Administrators.

Povolení nebo odmítnutí, co má přednost?

- **Vysvětlení** – V rámci zobrazení Device Class Configuration (Konfigurace tříd zařízení) byla nastavena následující konfigurace.
  - Oprávnění Allow (Povolit) bylo uděleno skupině systému Windows (např. BUILTIN \Administrators) a oprávnění Deny (Odmítnout) bylo uděleno jiné skupině systému Windows (např. BUILTIN\Users) na stejné úrovni hierarchie tříd zařízení (např. jednotky DVD/CD-ROM).
  - Je-li uživatel členem obou těchto skupin, které nastavení má přednost?
- **Řešení:**
  - Uživateli je odmítnut přístup k zařízení. Nastavení Deny (Odmítnout) má přednost před nastavením Allow (Povolit).
  - Důvodem odmítnutí přístupu je způsob, jímž systém Windows zjišťuje platná oprávnění pro dané zařízení. Jedné skupině je přístup odmítnut a druhé skupině je přístup povolen, ale uživatel je členem obou těchto skupin. Uživateli je odmítnut přístup, protože odmítnutí přístupu má přednost před povolením přístupu.
  - Jedním z možných řešení je odmítnout přístup skupině Users na úrovni jednotek DVD/CD-ROM a povolit přístup skupině Administrators na úrovni pod úrovní jednotek DVD/CD-ROM.
  - Dalším možným řešením je vytvoření specifických skupin systému Windows, jedné pro povolení přístupu k jednotkám DVD/CD a druhé pro odmítnutí přístupu k těmto jednotkám. Jednotliví uživatelé pak budou přidáni do příslušné skupiny.

Zobrazení Simple Configuration (Jednoduchá konfigurace) bylo použito k definování zásad řízení přístupu k zařízením, ale uživatelé s oprávněním správce nemají přístup k zařízením.

- **Vysvětlení** – Zobrazení Simple Configuration (Jednoduchá konfigurace) odmítá přístup pro skupiny Users (Uživatelé) a Guests (Hosté) a umožňuje přístup skupině Device Administrators (Správci zařízení).
- **Řešení:** Přidejte uživatele s oprávněním správce do skupiny Device Administrators (Správci zařízení).

Různé

Ovlivněný software – stručný popis	Podrobnosti	Řešení
Security Manager – varovné hlášení: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (Bezpečnostní aplikaci nelze nainstalovat, dokud nebude nainstalován modul HP Protect Tools Security Manager).	Všechny bezpečnostní aplikace, jako např. Java Card Security a biometrika jsou rozšiřitelnými moduly plug-in pro rozhraní Security Manager. Security Manager musí být instalován před bezpečnostním modulem plug-in povoleným společností HP.	Software Security Manager musí být nainstalován před instalací jakýchkoli bezpečnostních modulů plug-in.
Modul HP ProtectTools Security Manager – Přerušovaně se zobrazuje chyba při zavírání rozhraní modulu Security Manager.	Přerušovaně (jednou z dvanácti případů) dochází k chybě při použití tlačítka pro uzavření v pravém horním rohu obrazovky k ukončení modulu Security Manager před dokončením načítání všech aplikací plug-in.	Jedná se o časovou závislost doby zavádění služeb plug-in při ukončení a novém spuštění modulu Security Manager. Jelikož program PTHOST.exe je shell pro ostatní aplikace (moduly plug-in), závisí na schopnosti modulu plug-in, zda dokončí dobu zavádění (služby). Uzavřením shellu předtím, než dojde k dokončení zavádění modulu plug-in, je hlavní příčina. Ponechte modulu Security Manager čas k dokončení zprávy o zavádění služeb (v horní části okna Security Manager) a všech modulů plug-in uvedených v levém sloupci. Aby nedošlo k selhání, ponechte dostatečný čas k zavedení těchto modulů.
HP ProtectTools – Neomezený přístup nebo neřízená oprávnění správce znamenají bezpečnostní riziko.	Při neomezeném přístupu ke klientskému počítači existuje mnoho rizik, mezi jinými tato: • odstranění disku PSD, • úmyslná změna uživatelských nastavení, • deaktivace zásad a funkcí zabezpečení.	Správcům je doporučováno při omezení práv koncových uživatelů a omezení uživatelského přístupu postupovat podle „nejlepších postupů“. Neoprávněným uživatelům by neměla být udělována správcovská oprávnění.

Slovníček

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

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

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

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

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

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

certifikační úřad Služba, která vydává certifikáty vyžadované pro funkci infrastruktury používající veřejné klíče.

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

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

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

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

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

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

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

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

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

DriveLock Funkce zabezpečení, která spojí pevný disk s uživatelem a vyžaduje správné zadání hesla DriveLock při spuštění počítače.

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

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

Důvěryhodný kontakt Osoba, která přijala pozvání Důvěryhodného kontaktu.

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

HP SpareKey Záložní kopie šifrovacího klíče jednotky.

Identifikační karta Miniaplikace postranního panelu systému Windows, která vizuálně identifikuje vaší plochu s vaším jménem a vybraným obrázkem. Klepnutím na Identifikační kartu otevřete Konzolu pro správu nástroje HP ProtectTools.

identita Skupina pověření a nastavení v modulu HP ProtectTools Security Manager, se kterou se zachází stejně jako s účtem nebo profilem určitého uživatele.

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

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

Karta Java Vyjímatelná karta, která je vložena do počítače. Obsahuje identifikační informace pro přihlášení. Přihlášení s kartou Java na přihlašovací obrazovce Drive Encryption vyžaduje, abyste vložili kartu Java a zadali vaše uživatelské jméno a PIN k této kartě.

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

konzola Centrální umístění, kde najdete a můžete spravovat funkce a nastavení tohoto programu.

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

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

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

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

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

odhalení Úkol, který umožňuje uživateli dešifrovat jednu nebo více historií relací chatu, zobrazuje obrazovku se jménem kontaktu jako prostý text a umožní zobrazení relace.

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

oprávněný uživatel Uživatel, kterému bylo uděleno povolení v Nastavení přístupu uživatele pro zobrazení nebo úpravu nastavení konfigurace u Jednoduché konfigurace nebo Konfigurace třídy zařízení.

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

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

ověřování Proces ověření toho, zda je uživatel autorizován pro provádění úloh typu přístupu k počítači, úpravě nastavení pro příslušný program nebo zobrazení zabezpečených dat.

paměť Viz způsob bezpečného přihlášení.

Paměť USB Bezpečnostní zařízení, které ukládá identifikační informace o uživateli. Stejně jako karta Java nebo biometrická čtečka je používán k ověření majitele počítače.

panel nástrojů Centrální umístění, kde najdete a můžete spravovat funkce a nastavení tohoto programu.

PKI Standard PKI (Public Key Infrastructure) definuje rozhraní pro vytváření, používání a spravování certifikátů a šifrovacích klíčů.

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

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

profil bezpečného odstraňování Specifikovaný způsob odstranění a seznam prostředků.

Prohlížeč historie aplikace Live Messenger Komponenta chatu Privacy Manager umožňuje vyhledat a zobrazit šifrovanou historii relací chatu.

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

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

Přihlašovací obrazovka Drive Encryption (Šifrování jednotky) Přihlašovací obrazovka, která se zobrazí před spuštěním Windows. Uživatelé musí zadat uživatelská jména Windows a heslo nebo PIN ke kartě Java. Za většiny okolností zadání správných informací na přihlašovací obrazovce umožní přímý přístup do Windows bez nutnosti znovu se přihlašovat na přihlašovací obrazovce Windows.

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

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

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

relace historie chatu Šifrovaný soubor, který obsahuje záznam obou stran konverzace relace chatu.

restart Proces restartování počítače.

režim zařízení SATA Režim transferu dat mezi počítačem a hromadným úložným zařízením, jako je např. pevný disk nebo optický disk.

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

Seznam Důvěryhodných kontaktů Seznam Důvěryhodných kontaktů.

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

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

služba na pozadí Služba na pozadí HP ProtectTools Device Locking/Auditing, která musí být spuštěna, aby se mohly použít zásady řízení přístupu k zařízení. Lze ji zobrazit z aplikace Služby pod možností Nástroje pro správu v Ovládacím panelu. Pokud neběží, pokusí se HP ProtectTools Security Manager o její spuštění, když jsou použity zásady řízení přístupu k zařízení.

správce *Viz* správce Windows.

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

šifrování Procedura, jako například použití algoritmu, která se v šifrování používá k převodu prostého textu na šifrovaný text, aby se neoprávněným osobám zabránilo v přístupu k datům. Způsobů šifrování dat je celá řada a šifrování dat tvoří základ síťového zabezpečení. Mezi běžné způsoby šifrování patří norma pro kódování dat Data Encryption Standard (DES) a šifrování za pomoci veřejného klíče.

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

tlačítko Podepsat a šifrovat Softwarové tlačítko, které se zobrazí na liště aplikací Microsoft Office. Klepnutím na tlačítko umožníte podepsání, šifrování nebo odstranění šifrování u dokumentu Microsoft Office.

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

třída zařízení Všechna zařízení určitého typu, např. jednotky.

TXT Trusted Execution Technology.

Účet uživatele systému Windows Profil osoby, která je oprávněna se přihlašovat k síti nebo k určitému počítači.

uživatel Kdokoliv, kdo se účastní Drive Encryption (Šifrování jednotky) – Uživatelé, kteří nejsou správci, mají omezená práva. Mohou se pouze účastnit (se souhlasem správce) a přihlásit se.

virtuální paměť Bezpečnostní funkce, která funguje podobně jako karta Java nebo čtečka karty. Paměť je uložena buď na pevném disku počítače nebo v registru Windows. Když se přihlásíte pomocí virtuálního paměti, budete požádáni o PIN uživatele pro dokončení ověření.

zabezpečení pro důvěryhodné kontakty Přidává digitální podpis, šifruje el. poštu a odesílá ji po vašem ověření pomocí zvoleného způsobu bezpečného přihlášení.

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

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

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

způsob bezpečného přihlášení Způsob používaný pro přihlášení se do počítače.

Rejstřík