# HP Client Security

## Začínáme

První vydání: srpen 2013

Číslo dokumentu: 735339-221

# Obsah

# 1 Úvod do aplikace HP Client Security Manager

Aplikace HP Client Security umožňuje chránit data, zařízení a identitu a tím pádem zvyšuje zabezpečení počítače.

Dostupnost softwarových modulů pro počítač je závislá na modelu počítače.

Softwarové moduly HP Client Security 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 jsou napsány s předpokladem, že jste již nainstalovali příslušné softwarové moduly nástroje HP Client Security.

## Vlastnosti produktu HP Client Security

V následující tabulce jsou uvedeny podrobnosti o nejdůležitějších funkcích modulů HP Client Security.

| Modul | Hlavní vlastnosti |
|---|---|
| HP Client Security Manager | Správci mohou provádět následující funkce:<br>• Ochránit počítač již před spuštěním systému Windows®<br>• Ochránit účet v systému Windows pomocí silného ověřování<br>• Spravovat přihlašovací údaje a hesla pro webové stránky a aplikace<br>• Snadno změnit heslo pro operační systém Windows®<br>• Použít otisky prstů pro další zabezpečení a pohodlí<br>• Nastavit čipovou kartu, bezkontaktní kartu nebo kartu s detekcí přiblížení pro ověření<br>• Použít telefon Bluetooth jako metodu identifikace<br>• Nastavit kód PIN k rozšíření možností ověření<br>• Zkonfigurovat zásady přihlášení a relace<br>• Provést zálohu a obnovení programových dat<br>• Přidat další aplikace, jako HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager a HP Computrace<br>Obecní uživatelé mohou provádět následující funkce:<br>• Zobrazit nastavení pro nástroje Encryption Status a Device Access Manager.<br>• Aktivovat službu Computrace.<br>• Zkonfigurovat možnosti předvoleb, a zálohy a obnovení. |

| Modul | Hlavní vlastnosti |
|---|---|
| Password Manager | Obecní uživatelé mohou provádět následující funkce:<br>• Uspořádání a nastavení uživatelských jmen a hesel.<br>• Vytvořit silnější hesla pro pokročilé zabezpečení účtu pro e-mailové a webové účty. Nástroj Password Manager umožňuje zadávat a odesílat informace automaticky.<br>• Můžete zjednodušit přihlašování pomocí funkce jednotného přihlášení, která automaticky ukládá a používá údaje o uživateli.<br>• Označit účet za prozrazený, abyste byli upozorněni na další účty s podobnými přihlašovacími údaji.<br>• Naimportovat přihlašovací údaje z podporovaného prohlížeče. |
| HP Drive Encryption (pouze vybrané modely) | • Poskytuje kompletní šifrování celých oddílů pevných disků.<br>• Vynucuje ověřování před spuštěním za účelem dešifrování a zajištění přístupu k datům.<br>• Umožňuje aktivaci automatického šifrování jednotek (pouze u vybraných modelů). |
| HP Device Access Manager | • Umožňuje správcům IT řídit přístup k zařízením podle uživatelských profilů.<br>• Chrání před odstraněním dat neoprávněnými uživateli pomocí externích úložných médií a chrání před nakažením viry z externích médií.<br>• Umožňuje správcům zamezit přístup jednotlivým uživatelům nebo jejich skupinám ke komunikačním zařízením. |
| HP Trust Circles | • Poskytuje zabezpečení souborů a dokumentů.<br>• Šifruje soubory umístěné do složek určených uživatelem a chrání je v rámci skupiny Trust Circle.<br>• Umožňuje, aby soubory byly používány a sdíleny pouze členy v rámci skupiny Trust Circle. |
| Theft Recovery (Computrace, nutné zakoupit zvlášť) | • K aktivaci je zapotřebí samostatné zakoupení odběru služby sledování položek.<br>• Poskytuje možnost zabezpečeného sledování položek.<br>• Umožňuje sledovat aktivity uživatele stejně jako změny v hardwaru a softwaru.<br>• Zůstává aktivní i po naformátování nebo výměně pevného disku. |

# Popis produktu HP Client Security a příklady použití

Většina produktů HP Client Security používá ověření uživatele (obvykle pomocí hesla) a nějakou administrativní zálohu pro případ ztráty hesla, jeho zapomenutí či nedostupnosti či jiných situací, kdy je z důvodu bezpečnosti vyžadováno zajištění přístupu.

**POZNÁMKA:** Některé produkty HP Client Security jsou navrženy tak, aby omezovaly přístup k datům. Důležitá data, která by uživatel raději ztratil, než aby došlo k jejich vyzrazení, by měla být zašifrována. Doporučuje se zálohovat všechna data na bezpečném umístění.

## Password Manager

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

- Ukládání přihlašovacích jmen a hesel potřebných k přístupu na Internet nebo k e-mailu.
- Automatické přihlášení uživatele k webové stránce nebo e-mailu.
- Správa ověřování a uspořádání souvisejících dat.
- Výběr položky na webu nebo v síti a přímé otevření adresy v odkazu.
- Zobrazení jmen a hesel v případě potřeby.
- K označení účtu za prozrazený, abyste byli upozorněni na další účty s podobnými přihlašovacími údaji.
- Naimportování přihlašovacích údajů z podporovaného prohlížeče.

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

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

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

## HP Drive Encryption (pouze vybrané modely)

Nástroj HP Drive Encryption slouží k omezení přístupu k datům na celém pevném disku počítače či na sekundární jednotce. Nástroj Drive Encryption může také spravovat disky s vnitřním šifrováním.

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

**Příklad 2:** Správce v nemocnici si chce být jistý, že přístup k datům na místních počítačích budou mít pouze doktoři a pověření pracovníci, a to bez sdílení svých osobních hesel. Oddělení IT přidá správce, doktory a všechny pověřené pracovníky mezi uživatele nástroje Drive Encryption. Od této chvíle budou moci spustit počítač nebo použít doménu za pomocí osobního uživatelského jména a hesla pouze dané pověřené osoby.

## HP Device Access Manager (pouze vybrané modely)

Nástroj HP Device Access Manager umožňuje správci omezit a spravovat přístup k hardwaru. Nástroj Device Access Manager lze použít k zablokování nepovoleného přístupu k diskům USB, kam by jinak bylo možné kopírovat data. Může také omezit přístup k jednotkám CD/DVD, ovládat zařízení USB, síťová připojení a další. Příkladem je situace, kdy externí prodejci potřebují přístup k firemním počítačům, ale neměli by mít možnost kopírovat si data na disky USB.

**Příklad 1:** Vedoucí společnosti dodávající lékařský materiál často vedle firemních informací pracuje také s osobními zdravotními záznamy. Zaměstnanci potřebují mít přístup k těmto datům, ale je velmi krajně důležité, aby nedošlo k vyjmutí dat z počítače pomocí jednotky USB či jiného externího úložného zařízení. Síť je zabezpečená, ale počítače mají vypalovací jednotky CD-ROM a port USB, které umožňují kopírování či odcizení dat. Vedoucí použije nástroj Device Access Manager a deaktivuje porty USB a vypalovací jednotky CD-ROM, takže je nelze použít. I přes zablokování USB portů ostatní zařízení jako myš a klávesnice i nadále fungují.

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

## Computrace (nutno zakoupit zvlášť)

Služba Computrace (nutno zakoupit zvlášť) dokáže lokalizovat odcizený počítač ve chvíli, kdy se neoprávněný uživatel připojí k síti Internet. Software Computrace také pomáhá se vzdálenou správou a lokalizací počítačů i se sledováním využití počítačů a aplikací.

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

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

# Dosažení hlavních cílů zabezpečení

Moduly HP Client Security mohou spolupracovat a nabídnout řešení celé řady bezpečnostních rizik, včetně následujících klíčových cílů zabezpečení:

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

## Ochrana před cílenou krádeží

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

- Aktivací funkce ověřování před spuštěním zabráníte přístupu do operačního systému.
  - HP Client Security—Viz HP Client Security na stránce 12.
  - HP Drive Encryption—Viz HP Drive Encryption (pouze vybrané modely) na stránce 29.
- Šifrování chrání data před přístupem, i když je pevný disk odebraný a nainstalovaný do nezabezpečeného systému.
- Služba Computrace umožňuje sledovat polohu odcizeného počítače.
  - Computrace—Viz Obnova po krádeži (pouze u vybraných modelů) na stránce 53.

## Omezení přístupu k citlivým datům

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 HP Device Access Manager umožňuje IT manažerům omezit přístup na komunikační zařízení, takže citlivé informace nemohou být kopírovány z pevného disku. Viz Systémové zobrazení na stránce 43.

## Zabránění neoprávněnému přístupu z interních nebo externích míst

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

- Aktivací funkce ověřování před spuštěním zabráníte přístupu do operačního systému. (viz HP Drive Encryption (pouze vybrané modely) na stránce 29.
- Aplikace HP Client Security pomáhá zajistit, aby neoprávněný uživatel nemohl získat hesla nebo přístup k aplikacím chráněným heslem. Viz HP Client Security na stránce 12.
- Aplikace HP Device Access Manager umožňuje IT manažerům omezit přístup na zapisovatelná zařízení, takže citlivé informace nemohou kopírovány z pevného disku. Viz HP Device Access Manager (pouze vybrané modely) na stránce 42.

## Vytvoření zásad pro silná hesla

Když vstoupí v platnost nařízení společnosti, které vyžaduje použití silných zásad zabezpečení hesly pro desítky aplikací a databází pracujících v síti, aplikace Password Manager poskytuje chráněné úložiště pro hesla a pohodlnou funkci Single Sign On (Jednotné přihlášení). Viz Password Manager na stránce 18.

# Další prvky zabezpečení

## Přiřazení rolí zabezpečení

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

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

Pro nástroj HP Client Security lze bezpečnostní nároky a oprávnění rozdělit mezi následující role:

- Správce zabezpečení—Definuje úroveň zabezpečení pro společnost či síť a určuje, jaké budou implementovány bezpečnostní funkce, jako je například Drive Encryption.

  **POZNÁMKA:** Celou řadu funkcí nástroje HP Client Security může správce zabezpečení ve spolupráci se společností HP přizpůsobit podle vlastních potřeb. Další informace naleznete v části http://www.hp.com.

- Správce IT – Aplikuje a spravuje funkce zabezpečení určené správcem zabezpečení. Může zároveň aktivovat a deaktivovat některé funkce. Pokud se správce zabezpečení například rozhodne zavést čipové karty, může správce IT aktivovat režim hesla i čipových karet.
- Uživatel – Používá funkce zabezpečení. Pokud například správce zabezpečení a správce IT v systému zavedli čipové karty, uživatel může nastavit kód PIN karty a používat kartu k ověřování.

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

Neoprávnění uživatelé by neměli mít oprávnění správce.

## Správa hesel HP Client Security

Většina funkcí zabezpečení HP Client Security je zajištěna pomocí hesla. Následující tabulky obsahují přehled běžně používaných hesel, softwarových modulů, kde jsou hesla vytvořena, a popis jejich funkcí.

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

| Heslo HP Client Security | Nastaveno v tomto modulu | Funkce |
|---|---|---|
| Heslo pro přihlášení do systému Windows | Ovládací panely systému Windows nebo aplikace HP Client Security | Lze použít k manuálnímu přihlášení a ověření přístupu k různým funkcím aplikace HP Client Security. |
| Heslo pro zálohování a obnovu aplikace HP Client Security | HP Client Security, podle jednotlivého uživatele | Chrání přístup k souboru zálohování a obnovy aplikace HP Client Security. |
| Kód PIN čipové karty | Credential Manager | Umožňuje použití ověřování pomocí několika faktorů.<br>Umožňuje použití ověřování systému Windows.<br>Ověřuje uživatele nástroje Drive Encryption, pokud je vybrána čipová karta. |

## Vytvoření bezpečného hesla

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

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

## Zálohování přihlašovacích údajů a nastavení

Nástroj Zálohování a obnova v aplikaci HP Client Security lze použít jako centrální umístění, ze kterého můžete zálohovat a obnovit zabezpečovací přihlašovací údaje z některého z instalovaných modulů aplikace HP Client Security.

# 2 Začínáme

Chcete-li konfigurovat aplikaci HP Client Security pro použití se svými přihlašovacími údaji, spusťte aplikaci HP Client Security jedním z následujících způsobů. Jakmile byl průvodce jednou dokončen, stejný uživatel jej již nemůže znovu spustit.

1. Na obrazovce Start nebo Aplikace klikněte nebo klepněte na aplikaci **HP Client Security** (Windows 8).

   – nebo –

   Na ploše systému Windows klikněte nebo klepněte na aplikaci **HP Client Security Gadget** (Windows 7).

   – nebo –

   Na ploše systému Windows dvakrát klikněte nebo dvakrát klepněte na ikonu **HP Client Security** v oznamovací oblasti umístěné na pravé straně hlavního panelu

   – nebo –

   Na ploše systému Windows klikněte nebo klepněte na ikonu **HP Client Security** v oznamovací oblasti a poté vyberte možnost **Otevřít aplikaci HP Client Security**.

2. Spustí se Průvodce nastavením aplikace HP Client Security se zobrazenou uvítací stránkou.

3. Přečtěte si uvítací obrazovku, zadáním hesla systému Windows ověřte svou identitu a klikněte nebo klepněte na tlačítko **Další**.

   Pokud jste dosud nevytvořili heslo pro systém Windows, budete vyzváni k jeho vytvoření. Heslo pro systém Windows je vyžadováno z důvodu ochrany vašeho účtu v systému Windows před přístupem neautorizovaných osob a také, aby bylo možné využívat funkce aplikace HP Client Security.

4. Na stránce HP SpareKey vyberte tři bezpečnostní otázky. Zadejte odpovědi na jednotlivé otázky a poté klikněte na tlačítko **Další**. Je také možné zadat vlastní otázky. Další informace naleznete v části HP SpareKey – obnovení hesla na stránce 14.

5. Na stránce Otisky prstů zaregistrujte alespoň minimální počet požadovaných otisků prstů a poté klikněte nebo klepněte na tlačítko **Další**. Další informace naleznete v části Otisky prstů na stránce 12.

6. Na stránce Drive Encryption aktivujte šifrování, zálohujte šifrovací klíč a klikněte nebo klepněte na tlačítko **Další**. Další informace naleznete v nápovědě softwaru HP Drive Encryption.

   **POZNÁMKA:** Toto platí pro scénář, kde uživatel je správce a Průvodce nastavením aplikace HP Client Security ještě nebyl zkonfigurován správcem.

7. Na poslední stránce průvodce klikněte nebo klepněte na tlačítko **Dokončit**.

   Tato stránka obsahuje údaje o stavu funkcí a přihlašovacích údajů.

8. Průvodce nastavením aplikace HP Client Security zajišťuje aktivaci funkcí JITA (Just In Time Authentication) a File Sanitizer. Další informace najdete v nápovědě softwaru HP Device Access Manager a HP File Sanitizer.

   **POZNÁMKA:** Toto platí pro scénář, kde uživatel je správce a Průvodce nastavením aplikace HP Client Security ještě nebyl zkonfigurován správcem.

# Spuštění aplikace HP Client Security

Aplikaci HP Client Security lze spustit jedním z následujících způsobů:

**POZNÁMKA:** Před spuštěním aplikace HP Client Security musí být dokončen Průvodce nastavením aplikace HP Client Security.

- Na obrazovce Start nebo Aplikace klikněte na aplikaci **HP Client Security**.

  – nebo –

  Na ploše systému Windows klikněte nebo klepněte na aplikaci **HP Client Security** Gadget (Windows 7).

  – nebo –

  Na ploše systému Windows dvakrát klikněte nebo dvakrát klepněte na ikonu **HP Client Security** v oznamovací oblasti umístěné na pravé straně hlavního panelu

  – nebo –

  Na ploše systému Windows klikněte nebo klepněte na ikonu **HP Client Security** v oznamovací oblasti a poté vyberte možnost **Otevřít aplikaci HP Client Security**.

# 3 Průvodce snadným nastavením pro malé firmy

Tato kapitola má za cíl předvést základní kroky při aktivaci nejčastěji používaných a užitečných možností nástroje HP Client Security for Small Business. Celá řada nástrojů a možností v tomto softwaru vám umožní vyladit nastavení přesně podle vašich požadavků a nastavit vaše řízení přístupu. Tento Průvodce snadným nastavením se vynasnaží aktivovat každý modul s co nejmenšími nároky a v nejkratším čase. Chcete-li získat další, vyberte požadovaný modul a klikněte na tlačítko **?** nebo tlačítko Nápověda v pravém horním rohu okna. Toto tlačítko automaticky zobrazí informace, které vám poradí s obsahem právě zobrazeného okna.

## Začínáme

1. Na pracovní ploše Windows otevřete nástroj HP Client Security dvojím kliknutím na ikonu **HP Client Security** v oznamovací oblasti v krajní pravé pozici hlavního panelu.
2. Zadejte heslo systému Windows nebo vytvořte heslo systému Windows.
3. Dokončete nastavení nástroje HP Client Security.

Chcete-li, aby aplikace HP Client Security vyžadovala ověření pouze jednou během přihlášení k systému Windows, přečtěte si Bezpečnostní funkce na stránce 26.

## Password Manager

Každý používá celou řadu hesel – zvláště pokud pravidelně navštěvujete webové stránky či používáte aplikace, které vyžadují přihlášení. Běžný uživatel buď používá stejné heslo pro všechny aplikace a stránky, nebo popustí uzdu své kreativitě a rychle zapomene, které z různých hesel platí pro konkrétní aplikace.

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

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

Aktivace ukládání webů, uživatelských jmen a hesel:

1. Jako příklad přejděte na podílející se webovou stránku nebo aplikaci a poté klikněte na ikonu nástroje Password Manager v levém horním rohu webové stránky, abyste přidali webové ověření.
2. Pojmenujte odkaz (volitelné) a zadejte do nástroje Password Manager uživatelské jméno a heslo.
3. Po skončení klikněte na tlačítko **OK**.
4. Nástroj Password Manager také umožňuje ukládání uživatelského jména a hesla pro síťové složky a namapované síťové jednotky.

## Zobrazení a správa uložených přihlašovacích údajů v nástroji Password Manager

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

Ke spuštění nástroje Správce hesel použijte na klávesnici kombinaci kláves Ctrl+klávesa Windows+h a poté klikněte na příkaz **Přihlásit**, aby se spustil a ověřil uložený zástupce.

Možnost **Upravit** nástroje Password Manager vám umožní zobrazit, a změnit jméno, přihlašovací jméno a dokonce i odkrýt hesla.

Nástroj HP Client Security for Small Business umožňuje zazálohování všech ověřovacích údajů a nastavení či jejich zkopírování do jiného počítače.

# HP Device Access Manager

Aplikaci Device Access Manager lze použít k omezení přístupu k různým interním a externím úložným zařízením, takže vaše data budou v bezpečí na pevném disku a neopustí vaši kancelář. Příkladem je povolení uživatelského přístupu k datům, ovšem se zablokováním možnosti kopírování na disky CD, přenosné přehrávače hudby či paměťová zařízení USB.

1. Spusťte aplikaci **Device Access Manager** (viz Spuštění aplikace Device Access Manager na stránce 42).

   Zobrazen je přístup k aktuálnímu uživateli.

2. Chcete-li změnit přístup pro uživatele, skupiny nebo zařízení, klikněte nebo klepněte na tlačítko **Změnit**. Další informace naleznete v části Systémové zobrazení na stránce 43.

# HP Drive Encryption

Aplikace HP Drive Encryption chrání vaše data šifrováním celého pevného disku. Data na vašem pevném disku zůstanou chráněna i v případě krádeže vašeho počítače nebo při vyjmutí pevného disku z počítače a jeho umístění do jiného počítače.

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

Pro snadné ovládání si různé softwarové moduly automaticky synchronizují hesla, včetně uživatelských účtů Windows, domén pro ověřování a aplikací HP Drive Encryption, Password Manager a HP Client Security.

Chcete-li během prvního nastavení pomocí Průvodce nastavením aplikace HP Client Security nastavit aplikaci HP Drive Encryption, přečtěte si Začínáme na stránce 8.

# 4 HP Client Security

Domovská stránka aplikace HP Client Security je centrální umístění, které zajišťuje snadný přístup k funkcím, aplikacím a nastavením aplikace HP Client Security. Domovská stránka je rozdělena na tři oddíly:

- **DATA** – poskytuje přístup k aplikacím používaným ke správě zabezpečení dat.
- **ZAŘÍZENÍ** – poskytuje přístup k aplikacím používaným ke správě zabezpečení zařízení.
- **IDENTITA** – slouží k registraci a správě pověření pro ověření.

Chcete-li zobrazit popis aplikace, přesuňte kurzor nad dlaždici aplikace.

Aplikace HP Client Security může v dolní části stránky obsahovat odkazy na nastavení pro uživatele a správce. Aplikace HP Client Security umožňuje přístup do části Rozšířená nastavení kliknutím nebo klepnutím na ikonu ozubeného kola **Nastavení**.

## Aplikace, nastavení a funkce pro ověření identity

Aplikace, nastavení a funkce pro ověření identity v aplikaci HP Client Security vám pomohou spravovat různé aspekty vaší digitální identity. Klikněte nebo klepněte na jednu z následujících dlaždic na domovské stránce aplikace HP Client Security a poté zadejte své heslo systému Windows:

- **Otisky prstů** – slouží k registraci a správě pověření otisku prstu.
- **SpareKey** – slouží k nastavení a správě pověření nástroje HP SpareKey, které lze použít k přihlášení k počítači v případě, že ostatní pověření byla ztracena nebo založena na špatné místo. Umožňuje také resetovat zapomenuté heslo.
- **Heslo systému Windows** – poskytuje snadný přístup ke změně hesla pro systém Windows.
- **Zařízení Bluetooth** – umožňuje zaregistrovat a spravovat zařízení Bluetooth.
- **Karty** – umožňuje zaregistrovat a spravovat čipové karty, bezkontaktní karty a karty s detekcí přiblížení.
- **PIN** – umožňuje zaregistrovat a spravovat přihlašovací údaj kódu PIN.
- **RSA SecurID** – umožňuje zaregistrovat a spravovat přihlašovací údaj aplikace RSA SecurID (je-li na místě náležité nastavení).
- **Password Manager** – umožňuje spravovat hesla pro online účty a aplikace.

### Otisky prstů

Průvodce nastavením aplikace HP Client Security vás provede procesem nastavení (registrace) otisků prstů.

Otisky prstů můžete také zaregistrovat nebo odstranit na stránce Otisky prstů, na kterou lze přistoupit kliknutím nebo klepnutím na ikonu **Otisky prstů** na domovské stránce aplikace HP Client Security.

1. Na stránce Otisky prstů přejeďte prstem přes čtečku, až dojde k jeho úspěšné registraci.

   Na stránce je také uveden počet prstů potřebných k registraci. Doporučuje se použít ukazovák nebo prostředník.

2. Chcete-li odstranit dříve zaregistrované otisky prstů, klikněte nebo klepněte na možnost **Odstranit**.

3. Chcete-li registrovat další prsty, klikněte nebo klepněte na tlačítko **Zaregistrovat další otisk prstu**.

4. Před opuštěním stránky klikněte nebo klepněte na tlačítko **Uložit**.

⚠ **UPOZORNĚNÍ:** Pokud registrujete otisky prstů podle pokynů průvodce, informace o otiscích prstů se neuloží, dokud nekliknete na tlačítko **Další**. Pokud ponecháte počítač po nějakou dobu neaktivní nebo program zavřete, vámi provedené změny se **neuloží**.

- ▲ Chcete-li otevřít okno Nastavení pro správu otisků prstů, kde mohou správci určit registraci, přesnost a další nastavení, klikněte nebo klepněte na možnost **Nastavení pro správu** (vyžaduje oprávnění správce).
- ▲ Chcete-li otevřít okno Uživatelská nastavení otisků prstů, kde můžete určit nastavení řídící vzhled a chování funkce rozpoznávání otisků prstů, klikněte nebo klepněte na možnost **Uživatelská nastavení**.

## Nastavení pro správu otisků prstů

Správci mohou pro čtečku otisků prstů určit registraci, přesnost a další nastavení. K tomuto kroku jsou vyžadována oprávnění správce.

- ▲ Chcete-li otevřít okno Nastavení pro správu pro pověření využívající otisky prstu, na stránce Otisky prstů klikněte nebo klepněte na možnost **Nastavení pro správu**.

- **Registrace uživatele** – zvolte minimální a maximální počet otisků prstů, které může uživatel zaregistrovat.
- **Rozpoznání** – pomocí posuvníku upravte citlivost používanou čtečkou otisků prstů při načítání otisku.

  Pokud není otisk prstu rozpoznáván konzistentně, může být zapotřebí nastavit nižší citlivost rozpoznání. 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.

### Uživatelská nastavení otisků prstů

Na stránce Uživatelská nastavení otisků prstů můžete určit nastavení ovládající vzhled a chování procesu rozpoznávání otisků prstů.

▲ Chcete-li otevřít okno Uživatelská nastavení otisků prstů, na stránce Otisky prstů klikněte nebo klepněte na možnost **Uživatelská nastavení**.

- **Povolit zvukovou zpětnou vazbu** – ve výchozím nastavení poskytuje aplikace HP Client Security při skenování otisku prstu zvukovou zpětnou vazbu. Pro jednotlivé události jsou přehrány různé zvuky. Těmto událostem můžete rovněž přiřadit nové zvuky pomocí karty Zvuky v části s nastavením zvuku v ovládacích panelech systému Windows. Chcete-li zvukovou odezvu zakázat, zrušte zaškrtnutí této položky.
- **Zobrazit zpětnou vazbu ke kvalitě naskenovaného otisku** – chcete-li zobrazit všechny naskenované otisky bez ohledu na kvalitu, zaškrtněte toto políčko. Chcete-li zobrazit pouze kvalitní naskenované otisky, zaškrtnutí políčka zrušte.

## HP SpareKey – obnovení hesla

Funkce HP SpareKey umožňuje získat přístup k počítači (u podporovaných platforem) pomocí odpovědí na tři bezpečnostní otázky ze seznamu.

Aplikace HP Client Security váš požádá o nastavení osobního hesla SpareKey během úvodního nastavení v Průvodci nastavením nástroje HP Client Security.

Nastavení hesla HP SpareKey:

1. V průvodci na stránce HP SpareKey vyberte tři bezpečnostní otázky a pro každou z nich zadejte odpověď.

   Můžete vybrat otázky z předdefinovaného seznamu nebo zadat své vlastní otázky.

2. Klikněte nebo klepněte na tlačítko **Registrovat**.

Postup odstranění hesla HP SpareKey:

▲ Klikněte nebo klepněte na tlačítko **Odstranit funkci SpareKey**.

Po nastavení funkce SpareKey můžete přistoupit do počítače pomocí hesla SpareKey z přihlašovací obrazovky Ověřování po zapnutí nebo uvítací obrazovky Windows.

Na stránce funkce SpareKey, na kterou se přistupuje z dlaždice Obnovení hesla na domovské stránce aplikace HP Client Security, můžete vybrat různé otázky nebo změnit své odpovědi.

Chcete-li otevřít stránku Nastavení funkce HP SpareKey, kde správci mohou určit nastavení související s pověřením HP SpareKey, klepněte na možnost **Nastavení** (vyžaduje oprávnění správce).

### Nastavení funkce HP SpareKey

Na stránce Nastavení funkce HP SpareKey můžete určit nastavení řídící vzhled a způsob použití pověření HP SpareKey.

▲ Stránku Nastavení funkce HP SpareKey otevřete kliknutím nebo klepnutím na možnost **Nastavení** na stránce HP SpareKey (vyžaduje oprávnění správce).

Správci mohou vybrat následující nastavení:

- Určit otázky, které budou předloženy každému uživateli během nastavení funkce HP SpareKey.
- Přidat až tři vlastní bezpečnostní otázky, které budou přidány na seznam otázek dostupných pro uživatele.
- Zvolit, zda uživatelé mohou zadávat své vlastní bezpečnostní otázky.
- Určit, která ověřovací prostředí (Windows nebo ověření při zapnutí) umožní použití funkce HP SpareKey pro obnovení hesla.

## Heslo systému Windows

Aplikace HP Client Security usnadňuje a zrychluje změnu hesla pro systém Windows (ve srovnání s použitím ovládacích panelů systému Windows).

Postup změny hesla systému Windows:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na tlačítko **Heslo systému Windows**.
2. Své současné heslo zadejte do textového pole **Aktuální heslo pro systém Windows**.
3. Do textového pole **Nové heslo pro systém Windows** napište nové heslo a poté jej znovu napište do textového pole **Potvrzení nového hesla**.
4. Kliknutím či klepnutím na tlačítko **Změnit** okamžitě nastavíte nově zadané heslo jako aktuální.

## Zařízení Bluetooth

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

**POZNÁMKA:** Jako zařízení jsou podporovány pouze telefony s rozhraním Bluetooth.

1. Ujistěte se, že je rozhraní Bluetooth v počítači povoleno a v telefonu je aktivní režim vyhledávání. V rámci připojení telefonu může být zapotřebí zadat do zařízení s rozhraním Bluetooth automaticky vytvořený kód. V závislosti na nastaveních konfigurace zařízení Bluetooth může být vyžadováno porovnání párovacích kódů mezi počítačem a telefonem.
2. Chcete-li mobilní telefon zaregistrovat, vyberte jej a poté klikněte nebo klepněte na tlačítko **Registrovat**.

Přístup na stránku Nastavení zařízení Bluetooth na stránce 15, kde může správce stanovit nastavení pro zařízení Bluetooth, získáte kliknutím na tlačítko **Nastavení** (vyžaduje oprávnění správce).

### Nastavení zařízení Bluetooth

Správci mohou určit následující nastavení, která upravují chování a způsob použití pověření pomocí zařízení Bluetooth:

#### Tiché ověřování

- **Automaticky použít připojené zaregistrované zařízení Bluetooth během ověřování identity** – toto políčko zaškrtněte, pokud chcete uživatelům povolit používat pověření Bluetooth k ověření bez další vyžadované akce ze strany uživatele. V opačném případě tuto možnost zakažte zrušením zaškrtnutí políčka.

### Detekce přiblížení rozhraní Bluetooth

- **Uzamknout počítač, když se registrované zařízení Bluetooth dostane z dosahu počítače** – toto políčko zaškrtněte, pokud se má uzamknout počítač, když se zařízení připojené při přihlášení vzdálí z dosahu. V opačném případě tuto možnost zakažte zrušením zaškrtnutí políčka.

**POZNÁMKA:** Aby bylo možné tuto funkci použít, musí modul Bluetooth počítače tuto funkci podporovat.

## Karty

Aplikace HP Client Security může podporovat celou řadu různých typů identifikačních karet, což jsou malé plastové karty obsahující počítačový čip. Mezi ně patří čipové karty, bezkontaktní karty a karty s detekcí přiblížení. Pokud je předložena karta a k počítači je připojena příslušná čtečka karet, správce nainstaloval potřebné ovladače výrobce a povolil kartu jako způsob ověření přihlašovacích údajů, můžete kartu použít k ověření.

Pro čipové karty by měl výrobce poskytovat nástroje pro instalaci bezpečnostního certifikátu a správu kódu PIN, které aplikace HP Client Security použije ve svém algoritmu zabezpečení. Počet a typ znaků použitých v kódech PIN se může lišit. Před tím, než bude možné čipovou kartu použít, musí ji správce inicializovat.

Aplikace HP Client Security podporuje následující formáty čipových karet:

- CSP
- PKCS11

Nástroj HP Client Security podporuje následující typy bezkontaktních karet:

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

Aplikace HP Client Security podporuje následující formáty karet s detekcí přiblížení:

- HID Proximity Cards

Postup zaregistrování čipové karty:

1. Vložte kartu do připojené čtečky čipových karet.
2. Po rozpoznání karty zadejte kód PIN karty a poté klikněte nebo klepněte na možnost **Zaregistrovat**.

Změna kódu PIN čipové karty:

1. Vložte kartu do připojené čtečky čipových karet.
2. Po rozpoznání karty zadejte kód PIN karty a poté klikněte nebo klepněte na možnost **Ověřit**.
3. Klikněte nebo klepněte na možnost **Změnit kód PIN** a zadejte nový kód PIN.

Potup při zaregistrování bezkontaktní karty či karty s detekcí přiblížení:

1. Umístěte kartu do těsné blízkosti příslušné čtečky.
2. Po rozpoznání karty klikněte nebo klepněte na možnost **Zaregistrovat**.

Postup při odstranění zaregistrované karty:

1. Přiložte kartu ke čtečce.
2. Pro čipové karty po rozpoznání karty zadejte přiřazený kód PIN karty a poté klikněte nebo klepněte na možnost **Ověřit**.
3. Klikněte nebo klepněte na možnost **Odstranit**.

Po zaregistrování karty jsou podrobnosti o kartě zobrazeny v části **Zaregistrované karty**. Po odstranění je karta odebrána ze seznamu.

Chcete-li otevřít nastavení čipové karty, bezkontaktní karty a karty s detekcí přiblížení, kde může správce určit nastavení týkající se pověření příslušejících ke kartě, klikněte nebo klepněte na možnost **Nastavení** (vyžaduje oprávnění správce).

### Nastavení pro čipové karty, bezkontaktní karty a karty s detekcí přiblížení

Chcete-li otevřít nastavení pro nějakou kartu, klikněte nebo klepněte na kartu v seznamu karet a poté klikněte nebo klepněte na zobrazenou šipku.

Změna kódu PIN čipové karty:

1. Přiložte kartu ke čtečce.
2. Zadejte přiřazený kód PIN karty a poté klikněte nebo klepněte na možnost **Pokračovat**.
3. Zadejte a potvrďte nový kód PIN karty a poté klikněte nebo klepněte na možnost **Pokračovat**.

Inicializace kódu PIN čipové karty:

1. Přiložte kartu ke čtečce.
2. Zadejte přiřazený kód PIN karty a poté klikněte nebo klepněte na možnost **Pokračovat**.
3. Zadejte a potvrďte nový kód PIN karty a poté klikněte nebo klepněte na možnost **Pokračovat**.
4. Klikněte nebo klepněte na možnost **Ano**, čímž potvrdíte inicializaci.

Postup při vymazání dat karty:

1. Přiložte kartu ke čtečce.
2. Zadejte přiřazený kód PIN karty (pouze pro čipové karty) a poté klikněte nebo klepněte na možnost **Pokračovat**.
3. Klikněte nebo klepněte na možnost **Ano**, čímž potvrdíte odstranění.

## Kód PIN

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

Postup při nastavení nového kódu PIN:

- Zadejte kód PIN, poté jej zadejte znovu na potvrzení a klikněte nebo klepněte na možnost **Použít**.

Odstranění kódu PIN:

- Klikněte nebo klepněte na možnost **Odstranit** a pak pro potvrzení klikněte nebo klepněte na možnost **Ano**.

Chcete-li otevřít nastavení kódu PIN, kde může správce určit nastavení týkající se pověření příslušejících ke kódu PIN, klikněte nebo klepněte na možnost **Nastavení** (vyžaduje oprávnění správce).

### Nastavení systému PIN

Na stránce Nastavení kódu PIN můžete určit minimální a maximální přípustnou délku pro pověření PIN.

## RSA SecurID

Pokud správce pro ověřování povolil přihlašovací údaj RSA a jsou splněny následující podmínky, můžete zaregistrovat nebo odstranit pověření RSA SecurID.

**POZNÁMKA:** Je vyžadováno příslušné nastavení.

- Uživatel musí být vytvořen na serveru RSA.
- Token RSA SecurID přiřazený uživateli a počítači musí být uveden v rámci domény serveru RSA.
- Na počítači je nainstalován software SecurID.
- Je k dispozici připojení k správně konfigurovanému serveru RSA.

Postup při zaregistrování pověření RSA SecurID:

▲ zadejte své uživatelské jméno a přístupový kód RSA SecurID (kód tokenu RSA SecurID nebo kód PIN+kód tokenu, v závislosti na vašem prostředí) a klikněte nebo klepněte na možnost **Použít**.

Při úspěšném zaregistrování se zobrazí zpráva o úspěšném zaregistrování pověření RSA SecurID a bude zpřístupněno tlačítko Odstranit.

Postup při odstranění pověření RSA SecurID:

▲ Klikněte na tlačítko **Odstranit** a v zobrazeném dialogovém okně s dotazem, zda chcete opravdu odstranit své pověření RSA SecurID, vyberte možnost **Ano**”

## Password Manager

Použití nástroje Password Manager usnadňuje a zvyšuje bezpečnost přihlášení k 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, karty s detekcí přiblížení, bezkontaktní karty, telefonu Bluetooth, kódu PIN, pověření RSA nebo hesla pro systém Windows.

**POZNÁMKA:** Kvůli průběžně se měnící struktuře přihlašovacích obrazovek webů nemusí nástroj Password Manager být vždy schopen podporovat všechny weby.

Nástroj Password Manager nabízí následující možnosti:

### Stránka nástroje Password Manager

- Kliknutím nebo klepnutím na účet automaticky spustíte webovou stránku či aplikaci a přihlásíte se.
- Účty můžete organizovat pomocí kategorií.

### Síla hesla

- Je možné rychle zkontrolovat, zda je některé z použitých hesel ohroženo.
- Při přidávání údajů přihlášení probíhá kontrola síly jednotlivých hesel použitých pro webové stránky a aplikace.
- Síla hesla je vyznačena červeným, žlutým nebo zeleným stavovým ukazatelem.

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

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

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

## Webové stránky a programy, pro které dosud nebylo vytvořeno přihlášení

V kontextové nabídce jsou zobrazeny následující možnosti:

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

## Webové stránky a programy, pro které již bylo vytvořeno přihlášení

V kontextové nabídce jsou zobrazeny následující možnosti:

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

**POZNÁMKA:** Je možné, že správce tohoto počítače nastavil aplikaci HP Client Security tak, aby při ověřování identity vyžadoval více pověření.

## Přidání přihlášení

Přihlášení k webu nebo programu lze snadno přidat zadáním přihlašovacích informací. Od tohoto okamžiku již bude nástroj Password Manager zadávat tyto informace za vás. Tato přihlášení můžete využít při otevření webové stránky nebo programu.

Chcete-li přidat přihlášení, postupujte takto:

1. Otevřete přihlašovací obrazovku pro požadovaný web nebo program.
2. Klikněte nebo klepněte na ikonu **Password Manager** a pak v závislosti na tom, zda se jedná o přihlášení k webu nebo programu, klikněte nebo klepněte na jednu z následujících položek:
   - V případě webu klikněte nebo klepněte na položku **Přidat [název domény] do nástroje Password Manager**.
   - V případě programu klikněte nebo klepněte na položku **Přidat tuto přihlašovací obrazovku do nástroje Password Manager**.
3. Zadejte přihlašovací údaje. Přihlašovací pole na obrazovce a odpovídající pole v dialogovém okně jsou označena výrazným oranžovým okrajem.
   a. Chcete-li přihlašovací pole vyplnit pomocí některé z předem nastavených možností, klikněte nebo klepněte na šipku vpravo od pole.
   b. Chcete-li zobrazit heslo pro toto přihlášení, klikněte nebo klepněte na položku **Zobrazit heslo**.
   c. Chcete-li, aby přihlašovací pole byla vyplněna, ale nikoli odeslána, zrušte zaškrtnutí políčka **Automaticky odeslat přihlašovací údaje**.
   d. Kliknutím nebo klepnutím na tlačítko **OK** vyberte požadovanou metodu ověření (otisky prstů, čipová karta, karta s detekcí přiblížení, bezkontaktní karta, telefon s rozhraním Bluetooth, kód PIN nebo heslo) a poté se přihlaste pomocí vybrané metody ověřování.

      Z ikony **Password Manager** je odebrán symbol plus, což znamená, že přihlášení bylo vytvořeno.
   e. Pokud nástroj Password Manager nezjistí pole pro přihlášení, klikněte na možnost **Další pole**.
      - Zaškrtněte pole pro každé pole, které je požadováno pro přihlášení nebo zrušte zaškrtnutí pole pro jakákoliv pole, která nejsou požadována.
      - Klikněte nebo klepněte na možnost **Zavřít**.

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

## Úprava přihlášení

Chcete-li upravit přihlášení, postupujte takto:

1. Otevřete přihlašovací obrazovku pro požadovaný web nebo program.
2. Chcete-li zobrazit dialogové okno umožňující upravit přihlašovací informace, klikněte nebo klepněte na ikonu **Password Manager** a poté na položku **Upravit přihlášení**.

   Přihlašovací pole na obrazovce a odpovídající pole v dialogovém okně jsou označena výrazným oranžovým okrajem.

   Informace účtu můžete upravovat také ze stránky Password Manager tak, že kliknete nebo klepnete na přihlášení a zobrazíte možnosti úprav a následně vyberete možnost **Upravit**.
3. Upravte přihlašovací informace.
   - Chcete-li upravit údaj **Název účtu**, zadejte do pole nový název.
   - Chcete-li přidat nebo upravit název **Kategorie**, změňte název v poli **Kategorie**.

- Chcete-li vyplnit přihlašovací pole **Uživatelské jméno** pomocí některé z předem nastavených možností, klikněte nebo klepněte na šipku dolů vpravo od pole.

  Předem nastavené možnosti jsou k dispozici pouze při provádění úprav přihlášení pomocí příkazu Upravit v kontextové nabídce ikony nástroje Password Manager.

- Chcete-li vyplnit přihlašovací pole **Heslo** pomocí některé z předem nastavených možností, klikněte nebo klepněte na šipku dolů vpravo od pole.

  Předem nastavené možnosti jsou k dispozici pouze při provádění úprav přihlášení pomocí příkazu Upravit v kontextové nabídce ikony nástroje Password Manager.

- Chcete-li k přihlášení přidat další pole z obrazovky, klikněte nebo klepněte na položku **Další pole**.
- Chcete-li zobrazit heslo pro toto přihlášení, klikněte nebo klepněte na ikonu **Zobrazit heslo**.
- Chcete-li, aby přihlašovací pole byla vyplněna, ale nikoli odeslána, zrušte zaškrtnutí políčka **Automaticky odeslat přihlašovací údaje**.
- Chcete-li toto přihlášení označit příkazem kompromitovaného hesla, zaškrtněte políčko **Toto heslo je kompromitováno**.

  Po uložení změn budou všechna další přihlášení využívající stejné heslo také označena jako kompromitovaná. Poté můžete navštívit každý z postižených účtů a změnit jejich hesla.

4. Klikněte nebo klepněte na tlačítko **OK**.

## Použití nabídky rychlých odkazů v nástroji Password Manager

Nástroj Password Manager nabízí rychlý a snadný způsob spouštění webů a programů, pro něž jste vytvořili přihlášení. Dvakrát klikněte nebo dvakrát klepněte na přihlášení k webu nebo programu v nabídce **Rychlé odkazy nástroje Password Manager** nebo na stránce Password Manager aplikace HP Client Security. Otevře se přihlašovací obrazovka a budou vyplněny přihlašovací údaje.

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

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

▲ Stiskněte klávesovou zkratku pro nástroj **Password Manager**. (Výchozí nastavení z výroby je Ctrl+klávesa Windows+h). Chcete-li změnit klávesovou zkratku, na domovské stránce aplikace HP Client Security klikněte na možnost **Password Manager** a poté klikněte nebo klepněte na možnost **Nastavení**.

## Uspořádání přihlášení do kategorií

Chcete-li uspořádat přihlašovací údaje, vytvořte pro ně jednu nebo více kategorií.

Chcete-li přiřadit přihlášení do kategorie, postupujte takto:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na možnost **Password Manager**.
2. Klikněte nebo klepněte na položku účtu a poté klikněte nebo klepněte na možnost **Upravit**.
3. V poli **Kategorie** zadejte název kategorie.
4. Klikněte nebo klepněte na tlačítko **Uložit**.

Chcete-li odebrat účet z kategorie, postupujte takto:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na možnost **Password Manager**.
2. Klikněte nebo klepněte na položku účtu a poté klikněte nebo klepněte na možnost **Upravit**.
3. V poli **Kategorie** smažte název kategorie.
4. Klikněte nebo klepněte na tlačítko **Uložit**.

Chcete-li přejmenovat kategorii, postupujte takto:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na možnost **Password Manager**.
2. Klikněte nebo klepněte na položku účtu a poté klikněte nebo klepněte na možnost **Upravit**.
3. V poli **Kategorie** změňte název kategorie.
4. Klikněte nebo klepněte na tlačítko **Uložit**.

## Správa přihlášení

Nástroj Password Manager usnadňuje správu přihlašovacích údajů pro uživatelská jména, hesla a účty pro vícenásobné přihlášení z jednoho centrálního místa.

Vaše přihlášení jsou uvedena na stránce Password Manager.

Chcete-li provádět správu přihlášení, postupujte takto:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na možnost **Password Manager**.
2. Klikněte nebo klepněte na existující přihlašovací údaje, vyberte jednu z následujících možností a poté postupujte dle pokynů na obrazovce:
   - **Upravit** – úprava přihlášení. Další informace naleznete v části Úprava přihlášení na stránce 20.
   - **Přihlásit** – Přihlášení k vybranému účtu.
   - **Odstranit** – Odstranění přihlášení pro vybraný účet.

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

1. Otevřete přihlašovací obrazovku pro požadovaný web nebo program.
2. Kliknutím nebo klepnutím na ikonu **Password Manager** zobrazte kontextovou nabídku.
3. Klikněte nebo klepněte na položku **Přidat přihlášení** a poté postupujte podle pokynů na obrazovce.

## Vyhodnocení síly hesla

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

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

Při zadávání hesla během vytvoření přihlášení pro účet v nástroji Password Manager se pod heslem zobrazuje barevný pruh, který indikuje sílu hesla. Barvy mají následující význam:

- **Červená** – Slabá
- **Žlutá** – Přijatelná
- **Zelená** – Silná

## Nastavení ikony Password Manager

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

1. Chcete-li určit, jak má nástroj Password Manager pracovat s webovými stránkami obsahujícími přihlášení, klikněte nebo klepněte na ikonu a poté klikněte nebo klepněte na možnost **Nastavení ikony**.
   - **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky** – Klikněte nebo klepněte na tuto možnost, chcete-li, aby nástroj Password Manager zobrazoval výzvu k přidání přihlášení vždy, když se zobrazí přihlašovací obrazovka, pro niž dosud nebylo vytvořeno přihlášení.
   - **Nezahrnovat tuto obrazovku** – toto políčko zaškrtněte, chcete-li, aby nástroj Password Manager již nezobrazoval výzvu k přidání přihlášení pro tuto přihlašovací obrazovku.
   - **Nezobrazovat výzvu k přidání přihlašovacích údajů pro přihlašovací obrazovky** – vyberte přepínač.
2. Postup přidání přihlašovacích údajů pro obrazovku, která byla dříve vyloučena:
   a. Přihlaste se k dříve vyloučené webové stránce.
   b. Chcete-li, aby si nástroj Password Manager pamatoval heslo pro tuto stránku, klikněte nebo klepněte na možnost **Pamatovat** v rozevíracím okně. Heslo bude uloženo a bude vytvořeno přihlášení pro tuto obrazovku.
3. Chcete-li otevřít další nastavení nástroje Password Manager, klikněte nebo klepněte na ikonu nástroje Password Manager, klikněte nebo klepněte na možnost **Spustit nástroj Password Manager** a poté klikněte nebo klepněte na možnost **Nastavení** na stránce Password Manager.

## Import a export přihlášení

Na stránce Import a export nástroje Password Manager můžete importovat přihlášení uložená webovými prohlížeči ve vašem počítači. Můžete také importovat údaje ze záložního souboru aplikace HP Client Security a exportovat údaje do záložního souboru aplikace HP Client Security.

▲ Chcete-li otevřít stránku Import a export, klikněte nebo klepněte na možnost **Import a export** na stránce Password Manager.

Postup při importování hesel z prohlížeče:

1. Klikněte nebo klepněte na prohlížeč, ze kterého chcete importovat hesla (zobrazí se pouze nainstalované prohlížeče).
2. Zrušte zaškrtnutí u účtů, pro které nechcete importovat hesla.
3. Klikněte nebo klepněte na tlačítko **Importovat**.

Importování dat z nebo exportování dat do záložního souboru aplikace HP Client Security lze provést pomocí přiřazených odkazů (v části **Další možnosti)** na stránce Import a export.

**POZNÁMKA:** Tato funkce importuje a exportuje pouze údaje nástroje Password Manager. Informace o zálohování a obnovení dalších údajů aplikace HP Client Security, viz Zálohování a obnova dat na stránce 27.

Chcete-li importovat data ze záložního souboru HP Client Security, postupujte takto:

1. Na stránce Import a export nástroje HP Password Manager klikněte nebo klepněte na možnost **Importovat data ze záložního souboru HP Client Security**.
2. Ověřte svoji identitu.
3. Vyberte dříve vytvořený záložní soubor nebo zadejte cestu k souboru do zadaného pole a klikněte nebo klepněte na tlačítko **Procházet**.
4. Zadejte heslo použité na ochranu souboru a klikněte nebo klepněte na tlačítko **Další**.
5. Klikněte nebo klepněte na možnost **Obnovit**.

Chcete-li exportovat data do záložního souboru HP Client Security, postupujte takto:

1. Na stránce Import a export nástroje HP Password Manager klikněte nebo klepněte na možnost **Exportovat data do záložního souboru HP Client Security**.
2. Ověřte svoji identitu a poté klikněte nebo klepněte na tlačítko **Další**.
3. Zadejte název záložního souboru. Ve výchozím nastavení bude tento soubor uložen do složky Dokumenty. Chcete-li určit jiné umístění, klikněte nebo klepněte na tlačítko **Procházet**.
4. Zadejte a potvrďte heslo na ochranu souboru a klikněte nebo klepněte na tlačítko **Uložit**.

## Nastavení

Podle potřeby můžete přizpůsobit nastavení nástroje Password Manager:

- **Zobrazit výzvu k přidání přihlášení pro přihlašovací obrazovky** – ikona nástroje **Password Manager** se symbolem plus se zobrazí vždy, když je detekována přihlašovací obrazovka webové stránky nebo programu, a indikuje, že je možné do trezoru hesel přidat přihlášení k této obrazovce do nabídky **Přihlašovací údaje**.

  Chcete-li tuto funkci zakázat, zrušte zaškrtnutí pole u možnosti **Zobrazit výzvu k přidání přihlašovacích údajů pro přihlašovací obrazovky**.

- **Spustit Password Manager pomocí Ctrl+Win+h** – výchozí klávesová zkratka, která otevře nabídku **Rychlé odkazy nástroje Password Manager** je Ctrl+klávesa Windows+h.

  Chcete-li tuto kombinaci kláves změnit, klikněte nebo 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.

  Nelze použít kombinace vyhrazené pro systém Windows nebo aplikace systému Windows.

- Chcete-li nastavení vrátit na výchozí nastavení výrobce, klikněte nebo klepněte na možnost **Obnovit výchozí nastavení**.

# Rozšířená nastavení

Správci mohou otevřít následující nastavení výběrem ikony ozubeného kola **(Nastavení)** na domovské stránce aplikace HP Client Security.

- **Zásady pro správce** – Umožňuje konfigurovat zásady přihlášení a relace pro správce.
- **Zásady pro standardní uživatele** – Umožňuje konfigurovat zásady přihlášení a relace pro standardní uživatele.
- **Bezpečnostní funkce** – Umožňuje zvýšit zabezpečení počítače nastavením ochrany systému Windows pomocí silného ověřování a/nebo povolením ověřování před spuštěním systému Windows.
- **Uživatelé** – Umožňuje spravovat uživatele a jejich pověření.
- **Moje zásady** – Umožňuje zobrazit vaše zásady ověřování a stav registrací.
- **Zálohování a obnova** – Umožňuje zálohovat nebo obnovit data aplikace HP Client Security.
- **O aplikaci HP Client Security** – Zobrazí informace o verzi nástroje HP Client Security.

## Zásady pro správce

Můžete konfigurovat zásady přihlašování a relace pro správce tohoto počítače. Zde nastavené zásady přihlašování řídí vyžadovaná oprávnění pro přihlášení místního správce k systému Windows. Zde nastavené zásady relace řídí vyžadovaná oprávnění pro ověření identity místního správce v rámci relace systému Windows.

Ve výchozím nastavení jsou všechny nové nebo změněné zásady vynucovány okamžitě po kliknutí nebo klepnutí na tlačítko **Použít**.

Postup při přidání nové zásady:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na ikonu **Ozubeného kola**.
2. Na stránce Rozšířená nastavení klikněte nebo klepněte na možnost **Zásady pro správce**.
3. Klikněte nebo klepněte na možnost **Přidat novou zásadu**.
4. Kliknutím na šipku dolů vyberte primární a (volitelně) sekundární pověření pro novou zásadu a klikněte nebo klepněte na tlačítko **Přidat**.
5. Klikněte na tlačítko **Použít**.

Chcete-li opozdit účinnost nové nebo změněné zásady:

1. Klikněte nebo klepněte na možnost **Tuto zásadu vynutit okamžitě**.
2. Vyberte možnost **Tuto zásadu vynutit v určené datum**.
3. Zadejte datum nebo pomocí vyskakovacího kalendáře vyberte datum, kdy má být zásada začít být vynucována.
4. V případě potřeby určete, kdy mají být uživatelé informování o nové zásadě.
5. Klikněte na tlačítko **Použít**.

## Zásady pro standardní uživatele

Můžete konfigurovat zásady přihlašování a relace pro standardní uživatele tohoto počítače. Zde nastavené zásady přihlašování řídí vyžadovaná oprávnění pro přihlášení standardního uživatele k

systému Windows. Zde nastavené zásady relace řídí vyžadovaná oprávnění pro ověření identity standardního uživatele v rámci relace systému Windows.

Ve výchozím nastavení jsou všechny nové nebo změněné zásady vynucovány okamžitě po kliknutí nebo klepnutí na tlačítko **Použít**.

Postup při přidání nové zásady:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na ikonu **Ozubeného kola**.
2. Na stránce Rozšířená nastavení klikněte nebo klepněte na možnost **Zásady pro standardní uživatele**.
3. Klikněte nebo klepněte na možnost **Přidat novou zásadu**.
4. Kliknutím na šipku dolů vyberte primární a (volitelně) sekundární pověření pro novou zásadu a klikněte nebo klepněte na tlačítko **Přidat**.
5. Klikněte na tlačítko **Použít**.

Chcete-li opozdit účinnost nové nebo změněné zásady:

1. Klikněte nebo klepněte na možnost **Tuto zásadu vynutit okamžitě**.
2. Vyberte možnost **Tuto zásadu vynutit v určené datum**.
3. Zadejte datum nebo pomocí vyskakovacího kalendáře vyberte datum, kdy má být zásada začít být vynucována.
4. V případě potřeby určete, kdy mají být uživatelé informování o nové zásadě.
5. Klikněte na tlačítko **Použít**.

# Bezpečnostní funkce

Můžete povolit bezpečnostní funkce produktu HP Client Security, které poskytují ochranu proti neautorizovanému přístupu k počítači.

Nastavení bezpečnostních funkcí:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na ikonu **Ozubeného kola**.
2. Na stránce Rozšířená nastavení klikněte nebo klepněte na možnost **Bezpečnostní funkce**.
3. Povolte funkce zabezpečení zaškrtnutím odpovídajících políček a poté klikněte nebo klepněte na tlačítko **Použít**. Čím více funkcí zvolíte, tím lépe bude počítač zabezpečen.

   Tato nastavení platí pro všechny uživatele.

   - **Zabezpečení přihlášení do systému Windows** – Chrání účty systému Windows, neboť pro přístup požaduje použití přihlašovacích údajů aplikace HP Client Security.
   - **Zabezpečení před spuštěním (Ověřování po zapnutí)** – Chrání počítač před spuštěním systému Windows. Tento výběr není k dispozici, pokud jej systém BIOS nepodporuje.
   - **Povolit funkci One Step Logon** – Toto nastavení umožňuje uživateli počítače přeskočit přihlášení do systému Windows, pokud bylo předtím provedeno ověření po zapnutí nebo na úrovni funkce Drive Encryption.
4. Klikněte nebo klepněte na možnost **Uživatelé** a pak klikněte nebo klepněte na panel uživatelů.

# Uživatelé

Můžete monitorovat a spravovat uživatele aplikace HP Client Security v tomto počítači.

Chcete-li přidat dalšího uživatele systému Windows do aplikace HP Client Security, postupujte takto:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na ikonu **Ozubeného kola**.
2. Na stránce Rozšířená nastavení klikněte nebo klepněte na možnost **Uživatelé**.
3. Klikněte nebo klepněte na možnost **Přidat dalšího uživatele systému Windows do aplikace HP Client Security**.
4. Zadejte jméno uživatele, kterého chcete přidat, a pak klikněte nebo klepněte na tlačítko **OK**.
5. Zadejte heslo uživatele pro systém Windows.

   Na stránce Uživatelé se zobrazí panel pro přidaného uživatele.

Chcete-li odstranit uživatele systému Windows z aplikace HP Client Security, postupujte takto:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na ikonu **Ozubeného kola**.
2. Na stránce Rozšířená nastavení klikněte nebo klepněte na možnost **Uživatelé**.
3. Klikněte nebo klepněte na jméno uživatele, kterého chcete odstranit
4. Klikněte nebo klepněte na možnost **Odstranit uživatele** a na potvrzení klikněte nebo klepněte na možnost **Ano**.

Chcete-li zobrazit souhrn zásad přihlášení a relace platné pro uživatele, postupujte takto:

▲ Klikněte nebo klepněte na možnost **Uživatelé** a pak klikněte nebo klepněte na panel uživatelů.

# Moje zásady

Můžete zobrazit své zásady ověřování a stav registrace. Stránka Moje zásady také obsahuje odkazy na stránky Zásady pro správce a Zásady pro standardní uživatele.

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na ikonu **Ozubeného kola**.
2. Na stránce Rozšířená nastavení klikněte nebo klepněte na možnost **Moje zásady**.

   Zobrazí se zásady přihlašování a relace vynucované pro aktuálně přihlášeného uživatele.

Stránka Moje zásady obsahuje také odkazy na stránky Zásady pro správce na stránce 25 a Zásady pro standardní uživatele na stránce 25.

# Zálohování a obnova dat

Doporučuje se pravidelně zálohovat data aplikace HP Client Security. Četnost zálohování závisí na tom, jak často se tato data mění. Pokud například denně přidáváte nová přihlášení, měli byste 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 nástroje Password Manager. Nástroje Drive Encryption má nezávislou metodu zálohování. Nástroj Device Access Manager a informace o ověřování otiskem prstu zálohování neumožňují.

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

Chcete-li zálohovat data, postupujte takto:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na ikonu **Ozubeného kola**.
2. Na stránce Rozšířená nastavení klikněte nebo klepněte na možnost **Zásady pro správce**.
3. Klikněte nebo klepněte na možnost **Zálohování a obnovení**.
4. Klikněte nebo klepněte na příkaz **Zálohovat** a ověřte svoji identitu.
5. Vyberte modul, který chcete zahrnout do zálohy, a pak klikněte nebo klepněte na tlačítko **Další**.
6. Zadejte název souboru se zálohou. Ve výchozím nastavení bude tento soubor uložen do složky Dokumenty. Chcete-li určit jiné umístění, klikněte nebo klepněte na tlačítko **Procházet**.
7. Zadejte a potvrďte heslo na ochranu souboru.
8. Klikněte nebo klepněte na tlačítko **Uložit**.

Chcete-li obnovit data, postupujte takto:

1. Na domovské stránce aplikace HP Client Security klikněte nebo klepněte na ikonu **Ozubeného kola**.
2. Na stránce Rozšířená nastavení klikněte nebo klepněte na možnost **Zásady pro správce**.
3. Klikněte nebo klepněte na možnost **Zálohování a obnovení**.
4. Vyberte možnost **Obnovit** ověřte svoji identitu.
5. Vyberte dříve vytvořený soubor se zálohou. Zadejte cestu do příslušného pole. Chcete-li určit jiné umístění, klikněte nebo klepněte na tlačítko **Procházet**.
6. Zadejte heslo použité na ochranu souboru a klikněte nebo klepněte na tlačítko **Další**.
7. Vyberte moduly, pro které chcete obnovit data.
8. Klikněte nebo klepněte na možnost **Obnovit**.

# 5 HP Drive Encryption (pouze vybrané modely)

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

Výchozí obrazovka aplikace HP Client Security umožňuje správcům systému Windows aktivovat nástroj Drive Encryption, zálohovat šifrovací klíč a přidat či odebrat jednotky nebo oddíly určené k šifrování. Další informace naleznete v nápovědě softwaru HP Client Security.

Aplikace Drive Encryption umožňuje provádět následující úlohy:

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

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

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

## Spuštění aplikace Drive Encryption

Správci mohou k nástroji aplikaci Drive Encryption přistupovat spuštěním aplikace HP Client Security.

1. Na úvodní obrazovce Start klikněte nebo ťukněte na aplikaci **HP Client Security** (Windows 8).

   – nebo –

   Na ploše systému Windows dvakrát klikněte nebo dvakrát klepněte na ikonu **HP Client Security** v oznamovací oblasti umístěné na pravé straně hlavního panelu

2. Klikněte nebo klepněte na ikonu **Drive Encryption**.

# Obecné úlohy

## Aktivace aplikace Drive Encryption pro standardní pevné disky

Standardní pevné disky jsou šifrovány prostřednictvím softwarového šifrování. Chcete-li zašifrovat jednotku nebo oddíl disku, postupujte dle následujících kroků:

1. Spusťte nástroj **Drive Encryption**. Další informace naleznete v části Spuštění aplikace Drive Encryption na stránce 29.
2. Zaškrtněte políčko u pevného disku nebo oddílu, který chcete šifrovat, a klikněte nebo klepněte na položku **Záložní klíč**.

**POZNÁMKA:** Chcete-li zajistit vyšší zabezpečení, zaškrtněte políčko **Vyšší zabezpečení pomocí zakázání režimu spánku**. Když zakážete režim spánku, neexistuje absolutně žádné riziko, že se přihlašovací údaje použité k odblokování jednotky uloží do paměti.

3. Vyberte jednu nebo více možností zálohování a klikněte nebo klepněte na možnost **Zálohovat**. Další informace naleznete v části Zálohování šifrovacích klíčů na stránce 33.
4. V průběhu zálohování šifrovacího klíče můžete pokračovat ve své práci. Nerestartujte počítač.

**POZNÁMKA:** Budete vyzváni k restartu počítače. Po restartu se před spuštěním systému Windows zobrazí obrazovka před spuštěním šifrování jednotky vyžadující přihlášení.

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

Další informace naleznete v nápovědě softwaru HP Client Security.

## Aktivace aplikace Drive Encryption pro samošifrující jednotky

Jednotky s automatickým šifrováním splňující normy OPAL organizace Trusted Computing Group pro správu jednotek s automatickým šifrováním je možné šifrovat softwarově nebo hardwarově. Hardwarové šifrování je daleko rychlejší než softwarové šifrování. Nemůžete si ale vybrat, které oddíly disku zašifrovat. Zašifrován je celý disk včetně všech oddílů disku.

Chcete-li zašifrovat určité oddíly, pak musíte použít softwarové šifrování. Ujistěte se, že není zaškrtnuto políčko **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Povolit pouze hardwarové šifrování pro jednotky s automatickým šifrováním).

Pomocí následujících kroků můžete aktivovat nástroj Drive Encryption u jednotek s automatickým šifrováním:

1. Spusťte nástroj **Drive Encryption**. Další informace naleznete v části Spuštění aplikace Drive Encryption na stránce 29.
2. Zaškrtněte políčko u jednotky, kterou chcete šifrovat, a klikněte nebo klepněte na položku **Záložní klíč**.

**POZNÁMKA:** Chcete-li zajistit vyšší zabezpečení, zaškrtněte políčko **Vyšší zabezpečení pomocí zakázání režimu spánku**. Když zakážete režim spánku, neexistuje absolutně žádné riziko, že se přihlašovací údaje použité k odblokování jednotky uloží do paměti.

3. Vyberte jednu nebo více možností zálohování a klikněte nebo klepněte na možnost **Zálohovat**. Další informace naleznete v části Zálohování šifrovacích klíčů na stránce 33.
4. V průběhu zálohování šifrovacího klíče můžete pokračovat ve své práci. Nerestartujte počítač.

**POZNÁMKA:** Pro jednotky s automatickým šifrováním se zobrazí výzva k vypnutí počítače.

Další informace naleznete v nápovědě softwaru HP Client Security.

## Deaktivace aplikace Drive Encryption

1. Spusťte nástroj **Drive Encryption**. Další informace naleznete v části Spuštění aplikace Drive Encryption na stránce 29.
2. Zaškrtněte nebo zrušte zaškrtnutí políček pro všechny šifrované jednotky a klikněte nebo klepněte na tlačítko **Použít**.

   Bude zahájena deaktivace aplikace Drive Encryption.

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

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

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

## Přihlášení po aktivaci aplikace Drive Encryption

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

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

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

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

### Přihlášení jednoho uživatele:

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

### Přihlášení více uživatelů:

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

**POZNÁMKA:** Podporovány jsou následující čipové karty:

### Podporované čipové karty

- Gemalto Cyberflex Access 64k V2c

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

## Šifrování dalších pevných disků

Důrazně doporučujeme k ochraně dat pomocí šifrování pevného disku používat nástroj HP Drive Encryption. Po aktivaci můžete následujícím postupem šifrovat všechny přidané pevné disky nebo vytvořené oddíly:

1. Spusťte nástroj **Drive Encryption**. Další informace naleznete v části Spuštění aplikace Drive Encryption na stránce 29.
2. U softwarově šifrovaných jednotek vyberte oddíly, které chcete zašifrovat.

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

– nebo –

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

# Pokročilé úlohy

## Správa Drive Encryption (Šifrování jednotek) (úloha správce)

Správci mohou pomocí nástroje Drive Encryption prohlížet stav šifrování (Šifrováno nebo Nešifrováno) všech pevných disků v počítači.

- Je-li nastaven stav Povoleno, aplikace Drive Encryption byla aktivována a nakonfigurována. Jednotka je v některém z následujících stavů:

### Softwarové šifrování

- Nešifrováno
- Šifrováno
- Šifrování
- Dešifrování

### Hardwarové šifrování

- Šifrováno
- Nešifrováno (další jednotky)

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

Správci mohou pomocí funkce Drive Encryption zašifrovat jeden nebo více jednotek pevných disků v počítači nebo dešifrovat libovolné oddíly jednotky, které již byly zašifrovány.

1. Spusťte nástroj **Drive Encryption**. Další informace naleznete v části Spuštění aplikace Drive Encryption na stránce 29.
2. V části **Stav jednotky** zaškrtněte nebo zrušte zaškrtnutí políček u oddílů pevných disků, které chcete zašifrovat nebo dešifrovat, a poté klikněte nebo klepněte na tlačítko **Použít**.

**POZNÁMKA:** Je-li oddíl šifrován nebo dešifrován, indikátor průběhu zobrazuje procento zašifrování oddílu.

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

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

## Správa disku

- **Přezdívka** – Jednotkám a oddílům můžete přidělit přezdívky pro snazší identifikaci.
- **Odpojené jednotky** – Nástroj Drive Encryption může sledovat disky, které jsou odebrány z počítače. Disk, který je odebrán z počítače, je automaticky přesunut do seznamu Odpojeno. Pokud bude disk vrácen do systému, znovu se objeví v seznamu Připojeno.
- Pokud již nepotřebujete sledovat nebo spravovat odpojenou jednotku, můžete ji odebrat ze seznamu Odpojeno.
- Nástroj Drive Encryption zůstává aktivován, dokud není zrušeno zaškrtnutí políčka u všech připojených jednotek a seznam Odpojeno není prázdný.

## Zálohování a obnova (úloha správce)

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

### Zálohování šifrovacích klíčů

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

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

1. Spusťte nástroj **Drive Encryption**. Další informace naleznete v části Spuštění aplikace Drive Encryption na stránce 29.
2. Zaškrtněte políčko u požadované jednotky a klikněte nebo klepněte na možnost **Záložní klíč**.

3. V části **Vytvořit klíč obnovy nástroje HP Drive Encryption** vyberte jednu či více z následujících možností:

   - **Vyměnitelné úložiště** – Zaškrtněte toto políčko a vyberte úložné zařízení, kde bude uložen šifrovací klíč.
   - **SkyDrive** – Zaškrtněte políčko. Musíte být připojeni k internetu. Přihlaste se ke službě Microsoft SkyDrive a klikněte nebo klepněte na možnost **Ano**.

   **POZNÁMKA:** Chcete-li použít záložní klíč nástroje HP Drive Encryption, který je uložený pomocí služby SkyDrive, musíte jej stáhnout ze služby SkyDrive na vyměnitelné úložné zařízení a poté toto zařízení vložit do počítače.

   - **TPM** (pouze u vybraných modelů) – Umožňuje obnovení dat pomocí hesla TPM.

   **UPOZORNĚNÍ:** Pokud jsou údaje TPM vymazány nebo dojde k poškození počítače, ztratíte přístup k záloze. V případě výběru této metody byste měli použít ještě nějakou další metodu zálohování.

4. Klikněte nebo klepněte na tlačítko **Zálohovat**.

   Šifrovací klíč bude uložen do vybraného paměťového zařízení.

### Obnovení přístupu k aktivovanému počítači pomocí záložních klíčů

Správci mohou provést obnovení pomocí klíče nástroje Drive Encryption zálohovaného na vyjímatelné paměťové zařízení při aktivaci nebo výběrem možnosti **Záložní klíč** v nástroji Drive Encryption.

1. Vložte vyjímatelné paměťové zařízení obsahující záložní klíč.
2. Zapněte počítač.
3. Po zobrazení dialogového okna pro přihlášení je službě HP Drive Encryption klikněte nebo klepněte na možnost **Obnovit**.
4. Zadejte umístění nebo název souboru obsahujícího záložní klíč a klikněte nebo klepněte na tlačítko **Obnovit**.
5. Jakmile se zobrazí dialogové okno s potvrzením, klikněte nebo klepněte na tlačítko **OK**.

   Zobrazí se přihlašovací obrazovka systému Windows.

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

## Provedení obnovení HP SpareKey

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

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

1. Zapněte počítač.
2. Jakmile se zobrazí stránka nástroje HP Drive Encryption, přejděte na stránku pro přihlášení uživatelů.

3. Klikněte na možnost **SpareKey**.

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

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

   Zobrazí se přihlašovací obrazovka systému Windows.

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

# 6 HP File Sanitizer (pouze u vybraných modelů)

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

Aplikaci HP File Sanitizer nelze použít k odstraňování a čištění obsahu následujících typů jednotek:

- jednotky SSD, včetně svazků pole RAID v zařízení SSD,
- externí jednotky připojené pomocí rozhraní USB, Firewire nebo eSATA.

Pokud se pokusíte provést odstraňování nebo čištění souborů v jednotce SSD, zobrazí se výstraha a operace nebude provedena.

## Bezpečné odstranění

Skartace se liší od standardní akce odstraňování v systému Windows®. Při skartaci dat pomocí aplikace File Sanitizer dojde k přepsání souborů nesmyslnými daty, čímž se prakticky znemožní získání původních informací. Jednoduché odstranění systémem Windows může soubor (položku) ponechat nepoškozený na pevném disku nebo ve stavu, kdy lze data vyšetřovacími metodami obnovit.

Můžete naplánovat požadovanou dobu ničení, nebo můžete ničení aktivovat ručně výběrem ikony **File Sanitizer** na výchozí obrazovce nástroje HP Client Security nebo pomocí ikony **File Sanitizer** na pracovní ploše systému Windows. Další informace naleznete v části Nastavení plánu ničení na stránce 38, Zničení pomocí kliknutí pravým tlačítkem myši na stránce 40 nebo Ruční spuštění operace ničení na stránce 40.

**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 na pevném disku pouze odstraní odkaz na data nebo jejich umístění. Obsah položky na pevném disku nadále zůstává, dokud není jeho umístění na pevném disku přepsáno 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 neposkytuje žádné další zabezpečení zničených položek.

Můžete naplánovat požadovanou dobu čištění volného prostoru, nebo můžete čištění volného prostoru aktivovat ručně výběrem ikony **File Sanitizer** na výchozí obrazovce nástroje HP Client Security nebo pomocí ikony **File Sanitizer** na pracovní ploše systému Windows. Další informace naleznete v části Nastavení plánu čištění volného prostoru na stránce 39, Ruční spuštění čištění volného prostoru na stránce 41 nebo Použití ikony File Sanitizer na stránce 40.

# Spouštění File Sanitizer

1. Na úvodní obrazovce Start klikněte nebo ťukněte na aplikaci **HP Client Security** (Windows 8).

   – nebo –

   Na ploše systému Windows dvakrát klikněte nebo dvakrát klepněte na ikonu **HP Client Security** v oznamovací oblasti umístěné na pravé straně hlavního panelu

2. V části **Data** klikněte nebo klepněte na možnost **File Sanitizer**.

nebo

▲ Dvakrát klikněte nebo dvakrát klepněte na ikonu **File Sanitizer** na pracovní ploše systému Windows.

– nebo –

▲ Klikněte pravým tlačítkem myši nebo klepněte a podržte ikonu **File Sanitizer** na pracovní ploše systému Windows a vyberte možnost **Spustit aplikaci File Sanitizer**.

# Postupy nastavení

**Ničení** – Nástroj File Sanitizer bezpečně odstraní nebo zničí vybrané kategorie položek.

1. V části **Ničení** zaškrtněte políčko pro každý typ souboru, který chcete zničit, nebo zrušte zaškrtnutí políček u typů souborů, které nechcete zničit.

   - **Koš** – Zničí všechny položky v koši.
   - **Dočasné soubory systému** – Zničí všechny soubory nalezené v dočasné složce systému. Jsou vyhledávány následující proměnné prostředí v uvedeném pořadí, přičemž první nalezená cesta je považována za systémovou složku:
     - TMP
     - TEMP
   - **Dočasné soubory Internetu** – Zničí kopie webových stránek, obrázků a médií uložené webovými prohlížeči z důvodu jejich rychlejšího zobrazování.
   - **Soubory cookie** – Zničí všechny soubory uložené v počítači webovými stránkami, které uchovávají předvolby, jako jsou přihlašovací údaje.

2. Ničení zahájíte kliknutím nebo klepnutím na příkaz **Ničení**.

**Čištění** – Zapisuje náhodně vygenerovaná data do volného prostoru a zabraňuje tak obnovení odstraněných položek.

▲ Čištění zahájíte kliknutím nebo klepnutím na příkaz **Čištění**.

**Možnosti aplikace File Sanitizer** – Zaškrtnutím políček můžete vybrat následující možnosti. Zrušením jejich zaškrtnutí můžete dané možnosti zakázat:

- **Povolit ikonu na ploše** – Zobrazí ikonu File Sanitizer na ploše systému Windows.
- **Povolit kliknutí pravým tlačítkem** – Umožní kliknout pravým tlačítkem nebo klepnout a držet položku a následně vybrat příkaz **HP File Sanitizer – Ničení**.

- **Před ručním ničením vyžadovat heslo systému Windows** – Před ručním zničením položky vyžaduje ověření pomocí hesla systému Windows.
- **Zničit soubory cookie a dočasné internetové soubory při ukončení prohlížeče** – Při zavření webového prohlížeče zničí všechny vybrané webové položky, jako například historii adres URL webového prohlížeče.

## Nastavení plánu ničení

Můžete naplánovat dobu, kdy má být automaticky provedeno zničení, nebo můžete položky kdykoli zničit ručně. Další informace naleznete v části Postupy nastavení na stránce 37;

1. Spusťte aplikaci File Sanitizer a poté klikněte nebo klepněte na tlačítko **Nastavení**.
2. Chcete-li naplánovat ničení vybraných položek v budoucnosti, v části **Plán ničení** vyberte možnost **Nikdy**, **Jednou**, **Denně**, **Týdně** nebo **Měsíčně** a vyberte den a čas:
   a. Klikněte nebo klepněte na pole pro hodinu, minutu a AM/PM (dopoledne/odpoledne).
   b. Posunujte se, dokud se nezobrazí požadovaná hodnota na stejné úrovni s ostatními poli.
   c. Klikněte nebo klepněte na prázdné místo kolem polí pro nastavení času.
   d. Opakujte tyto kroky pro všechna pole až do úplného výběru požadovaného nastavení.
3. Jsou vypsány následující čtyři typy položek:
   - **Koš** – Zničí všechny položky v koši.
   - **Dočasné soubory systému** – Zničí všechny soubory nalezené v dočasné složce systému. Jsou vyhledávány následující proměnné prostředí v uvedeném pořadí, přičemž první nalezená cesta je považována za systémovou složku:
     - TMP
     - TEMP
   - **Dočasné soubory Internetu** – Zničí kopie webových stránek, obrázků a médií uložené webovými prohlížeči z důvodu jejich rychlejšího zobrazování.
   - **Soubory cookie** – Zničí všechny soubory uložené v počítači webovými stránkami, které uchovávají předvolby, jako jsou přihlašovací údaje.

   Jsou-li zaškrtnuty, budou tyto položky v naplánovanou dobu zničeny.
4. Výběr dalších vlastních položek ke zničení:
   a. V části **Scheduled Shred List** (Seznam naplánovaného zničení) klikněte nebo klepněte na možnost **Přidat složku** a navigujte k požadovanému souboru či složce.
   b. Klikněte nebo klepněte na možnost **Otevřít** a pak klikněte nebo klepněte na tlačítko **OK**.

   Chcete-li odebrat položku ze seznamu naplánovaného zničení, zrušte zaškrtnutí políčka u dané položky.

## Nastavení plánu čištění volného prostoru

Čištění volného prostoru neposkytuje žádné další zabezpečení zničených položek.

1. Spusťte aplikaci File Sanitizer a poté klikněte nebo klepněte na tlačítko **Nastavení**.
2. Chcete-li naplánovat čištění volného prostoru vybraných položek v budoucnosti, v části **Plán čištění** vyberte možnost **Nikdy**, **Jednou**, **Denně**, **Týdně** nebo **Měsíčně** a vyberte den a čas:
   a. Klikněte nebo klepněte na pole pro hodinu, minutu a AM/PM (dopoledne/odpoledne).
   b. Posunujte se, dokud se nezobrazí požadovaný čas na stejné úrovni s ostatními poli.
   c. Klikněte nebo klepněte na prázdné místo kolem polí pro nastavení času.
   d. Opakujte tyto kroky až do úplného výběru požadovaného nastavení.

**POZNÁMKA:** Operace čištění volného prostoru může být časově náročná. Ověřte, zda je počítač připojen k napájení. Ačkoli je čištění prováděno na pozadí, počítač může fungovat pomaleji z důvodu zvýšeného využití procesoru. Čištění volného prostoru lze provést mimo pracovní dobu nebo ve chvíli, kdy není počítač používán.

## Ochrana souborů před zničením

Ochrana složek nebo souborů před ničením:

1. Spusťte aplikaci File Sanitizer a poté klikněte nebo klepněte na tlačítko **Nastavení**.
2. V části **Never Shred List** (Seznam výjimek ze zničení) klikněte nebo klepněte na možnost **Přidat složku** a navigujte k požadovanému souboru či složce.
3. Klikněte nebo klepněte na možnost **Otevřít** a pak klikněte nebo klepněte na tlačítko **OK**.

**POZNÁMKA:** Soubory uvedené v tomto seznamu jsou chráněny.

Chcete-li odebrat položku ze seznamu výjimek zničení, zrušte zaškrtnutí políčka u dané položky.

# Obecné úlohy

File Sanitizer můžete použít k provedení následujících úkolů:

- **Použití ikony File Sanitizer pro spuštění bezpečného odstranění** – Přetáhněte soubory na ikonu **File Sanitizer** na ploše Windows. Podrobnosti naleznete v části Použití ikony File Sanitizer na stránce 40.
- **Ruční skartace konkrétních položek nebo všech vybraných položek** – Skartujte položky kdykoli, bez nutnosti čekání na naplánovaný čas skartace. Podrobnosti naleznete v částech Zničení pomocí kliknutí pravým tlačítkem myši na stránce 40 nebo Ruční spuštění operace ničení na stránce 40.
- **Ruční aktivace čištění volného místa** – Čištění volného místa můžete aktivovat kdykoli. Podrobnosti naleznete v části Ruční spuštění čištění volného prostoru na stránce 41.
- **Zobrazit soubory protokolů** – Slouží k zobrazení souborů protokolů skartace a čištění volného místa, které obsahují jakékoli chyby při poslední operaci skartace nebo čištění volného místa. Podrobnosti naleznete v části Zobrazování protokolů na stránce 41.

**POZNÁMKA:** Operace skartace nebo čištění volného prostoru může trvat značně dlouhou dobu. Přestože bezpečné odstraňování a čištění volného prostoru probíhá na pozadí, počítač může fungovat pomaleji kvůli zvýšeným nárokům na procesor.

## Použití ikony File Sanitizer

⚠ **UPOZORNĚNÍ:** Skartované položky nelze znovu obnovit. Pečlivě zvažte, které položky chcete vybrat pro ruční ničení.

Když ručně spustíte operaci ničení, je zničen standardní seznam ničených položek v okně File Sanitizer (viz Postupy nastavení na stránce 37).

Operaci ničení můžete ručně spustit jedním z následujících způsobů:

1. Spusťte aplikaci File Sanitizer (viz Spouštění File Sanitizer na stránce 37) a poté klikněte nebo klepněte na příkaz **Ničení**.
2. Po zobrazení dialogového okna s žádostí o potvrzení se ujistěte, že jsou zaškrtnuty položky, které chcete zničit, a poté klikněte nebo klepněte na tlačítko **OK**.

– nebo –

1. Klikněte pravým tlačítkem myši nebo klepněte a podržte ikonu **File Sanitizer** na pracovní ploše systému Windows a klikněte nebo klepněte na příkaz **Zničit nyní**.
2. Po zobrazení dialogového okna s žádostí o potvrzení se ujistěte, že jsou zaškrtnuty položky, které chcete zničit, a poté klikněte nebo klepněte na tlačítko **Ničení**.

## Zničení pomocí kliknutí pravým tlačítkem myši

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

Pokud je v okně File Sanitizer vybrána možnost **Povolit zničení kliknutím pravým tlačítkem**, můžete zničit položky následujícím způsobem:

1. Přejděte do umístění dokumentu nebo složky, kterou chcete zničit.
2. Klikněte pravým tlačítkem myši nebo klepněte a podržte soubor nebo složku a vyberte možnost **HP File Sanitizer – Ničení**.

## Ruční spuštění operace ničení

⚠ **UPOZORNĚNÍ:** Skartované položky nelze znovu obnovit. Pečlivě zvažte, které položky chcete vybrat pro ruční ničení.

Když ručně spustíte operaci ničení, je zničen standardní seznam ničených položek v okně File Sanitizer (viz Postupy nastavení na stránce 37).

Operaci ničení můžete ručně spustit jedním z následujících způsobů:

1. Spusťte aplikaci File Sanitizer (viz Spouštění File Sanitizer na stránce 37) a poté klikněte nebo klepněte na příkaz **Ničení**.
2. Po zobrazení dialogového okna s žádostí o potvrzení se ujistěte, že jsou zaškrtnuty položky, které chcete zničit, a poté klikněte nebo klepněte na tlačítko **OK**.

– nebo –

1. Klikněte pravým tlačítkem myši nebo klepněte a podržte ikonu **File Sanitizer** na pracovní ploše systému Windows a klikněte nebo klepněte na příkaz **Zničit nyní**.
2. Po zobrazení dialogového okna s žádostí o potvrzení se ujistěte, že jsou zaškrtnuty položky, které chcete zničit, a poté klikněte nebo klepněte na tlačítko **Ničení**.

## Ruční spuštění čištění volného prostoru

Když ručně spustíte operaci čištění, je čištěn standardní seznam ničených položek v okně File Sanitizer (viz Postupy nastavení na stránce 37).

Operaci čištění můžete ručně spustit jedním z následujících způsobů:

1. Spusťte aplikaci File Sanitizer (viz Spouštění File Sanitizer na stránce 37) a poté klikněte nebo klepněte na příkaz **Čištění**.
2. Jakmile se zobrazí dialogové okno s potvrzením, klikněte nebo klepněte na tlačítko **OK**.

– nebo –

1. Klikněte pravým tlačítkem myši nebo klepněte a podržte ikonu **File Sanitizer** na pracovní ploše systému Windows a klikněte nebo klepněte na příkaz **Vyčistit nyní**.
2. Jakmile se zobrazí dialogové okno s potvrzením, klikněte nebo klepněte na tlačítko **Čištění**.

## Zobrazování protokolů

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

**POZNÁMKA:** Úspěšně zničené nebo vyčištěné soubory se v souborech protokolu 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 následujících složkách:

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

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

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

# 7 HP Device Access Manager (pouze vybrané modely)

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

**POZNÁMKA:** Některá člověkem ovládaná nebo vstupní zařízení, jako je myš, klávesnice, zařízení TouchPad a čtečka otisků prstů, nejsou aplikací Device Access Manager řízena. Další informace naleznete v části Třídy nespravovaných zařízení na stránce 45.

Správci operačního systému Windows® používají aplikaci HP Device Access Manager 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.
- Ověřování Just In Time Authentication (JITA) umožňuje přihlášení předdefinovaných uživatelů za účelem přístupu k zařízením, která jsou jinak zakázána.
- Správci a důvěryhodní uživatelé mohou být ze zákazu uplatněného aplikací Device Access Manager vyloučeni pomocí jejich přidání do skupiny správců zařízení. Členství v této skupině je spravováno pomocí rozšířených nastavení.
- Přístup k zařízením je možno udělovat nebo odepírat na základě členství ve skupinách nebo pro jednotlivé uživatele.
- U zařízení typů jednotky CD-ROM nebo DVD mohou být práva čtení a zápisu udělena nebo odepřena odděleně.

Aplikace HP Device Access Manager je během dokončení nastavení pomocí průvodce nastavením HP Client Security automaticky konfigurována s následujícími funkcemi:

- Pro skupiny Uživatelé a Správci je povoleno ověřování Just In Time Authentication (JITA) pro vyměnitelná média.
- Zásady pro zařízení umožňují plný přístup k ostatním zařízením.

## Spuštění aplikace Device Access Manager

1. Na úvodní obrazovce Start klikněte nebo ťukněte na aplikaci **HP Client Security** (Windows 8).

   – nebo –

   Na ploše systému Windows dvakrát klikněte nebo dvakrát klepněte na ikonu **HP Client Security** v oznamovací oblasti umístěné na pravé straně hlavního panelu

2. V části **Zařízení** klikněte nebo klepněte na možnost **Oprávnění pro zařízení**.

   - Standardní uživatelé mohou zobrazit svá aktuální přístupová oprávnění k zařízením (viz Uživatelské zobrazení na stránce 43).
   - Správci mohou zobrazit a provádět změny přístupu k zařízením, který je aktuálně konfigurován pro počítač, kliknutím nebo klepnutím na příkaz **Změnit** a zadáním hesla správce (viz Systémové zobrazení na stránce 43).

## Uživatelské zobrazení

Pokud je vybrána možnost **Device Permission** (Oprávnění pro zařízení), bude k dispozici uživatelské zobrazení. V závislosti na nastavených zásadách mohou standardní uživatelé správci zobrazit svá vlastní přístupová oprávnění ke třídám zařízení nebo jednotlivým zařízením v tomto počítači.

- **Aktuální uživatel** – Zobrazí se jméno uživatele, který je právě přihlášen.
- **Třída zařízení** – Zobrazí se typy zařízení.
- **Přístup** – Zobrazí se váš aktuálně konfigurovaný přístup k jednotlivým typům zařízení nebo konkrétním zařízením.
- **Délka** – Zobrazí se časový limit vašeho přístupu k jednotkám CD/DVD-ROM a vyměnitelným diskům.
- **Nastavení** – Správci mohou změnit, které jednotky mají přístup řízený pomocí nástroje Device Access Manager.

## Systémové zobrazení

V systémovém zobrazení mohou správci povolit nebo zakázat přístup k zařízením v tomto počítači pro skupiny uživatelé nebo Správci.

▲ Správci mohou otevřít systémové zobrazení kliknutím nebo klepnutím na tlačítko **Změnit**, zadáním hesla správce a výběrem jedné z následujících možností:

- **Device Access Manager** – Chcete-li zapnout nebo vypnout nástroj HP Device Access Manager s ověřováním Just In Time, klikněte nebo klepněte na možnosti **Zapnout** nebo **Vypnout**.
- **Uživatelé a skupiny v tomto počítači** – Zobrazuje skupiny Uživatelé a Správci, které mají povolen nebo zakázán přístup k vybraným třídám zařízení.
- **Třída zařízení** – Zobrazuje všechny zařízení a třídy zařízení, která jsou v systému nainstalována nebo která byla v systému nainstalována dříve. Chcete-li seznam rozbalit, klikněte na ikonu **+**. Budou zobrazena všechna zařízení připojená k počítači a skupiny Uživatelé a Správci budou rozbaleny a bude zobrazeno jejich členství. Chcete-li aktualizovat zobrazení, klikněte na ikonu zahnuté šipky (Obnovit).
  - Ochrana je zpravidla použita pro třídu zařízení. Pokud je přístup nastaven na možnost **Povolit**, vybraný uživatel nebo skupina bude mít přístup k libovolnému zařízení v rámci třídy zařízení.
  - Ochrana může být rovněž použita pro konkrétní zařízení.
  - Konfigurace ověřování v reálném čase JITA (Just In Time Authentication) umožňuje vybraným uživatelům přístup k jednotkám DVD/CD-ROM a vyměnitelným médiím prostřednictvím vlastního ověření. Další informace naleznete v části Konfigurace JITA na stránce 44.
  - Je možné povolit nebo zakázat přístup k dalším třídám zařízení, například k vyměnitelným médiím (například jednotky USB flash), sériovým a paralelním portům, zařízením Bluetooth®, modemům, kartám PCMCIA/ExpressCard, zařízením 1394, čtečkám otisků prstů a čtečkám čipových karet. Pokud je odepřen přístup k čtečkám otisků prstů či čipových karet, je možné tato zařízení použít k ověření, avšak nebude možné je použít na úrovni zásad relace.

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

- Když vyberete nastavení na úrovni Skupina nebo Třída zařízení, budete dotázáni, zda chcete nastavení uplatnit i pro podřízené objekty:

  **Ano** – Nastavení bude použito i v nižších úrovních.

  **Ne** – Nastavení nebude použito v nižších úrovních.

- Některé třídy zařízení, jako jsou například jednotky CD-ROM a DVD, mohou být dále řízeny povolením nebo odmítnutím přístupu pro operace čtení a pro operace zápisu.

**POZNÁMKA:** Skupinu správci nelze přidat do seznamu uživatelů.

- **Přístup** – Klikněte nebo klepněte na šipku dolů a vyberte jeden z následujících požadovaných typů přístupu:
  - **Povolit – Plný přístup**
  - **Povolit – Jen pro čtení**
  - **Povolit – Vyžadováno JITA** – Další informace viz Konfigurace JITA na stránce 44.

    Pokud je vybrán tento typ přístup, v části **Délka** kliknutím nebo klepnutím na šipku dolů vyberte časový limit.
  - **Odmítnout**
- **Délka** – Kliknutím nebo klepnutím na šipku dolů vyberte časový limit pro přístup k jednotkám DVD/CD-ROM nebo vyměnitelným diskům (viz Konfigurace JITA na stránce 44).

## Konfigurace JITA

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

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

Dobu použití funkce JITA lze povolit na stanovený počet minut nebo na neomezenou dobu. Uživatelé bez omezení budou mít přístup k zařízení od chvíle ověření až do odhlášení ze systému.

Pokud je uživateli přiděleno omezené období ověřování JITA, jednu minutu před vypršením platnosti ověřování JITA se uživateli zobrazí dotaz, zda si přeje přístup prodloužit. Období JITA končí odhlášením uživatele od systému nebo přihlášením jiného uživatele. Při příštím přihlášení uživatele a pokusu o přístup k zařízení, pro něž je povolena funkce JITA, se zobrazí výzva k zadání přihlašovacích údajů.

Funkce JITA je dostupná pro následující třídy za řízení:

- Jednotky DVD/CD-ROM
- Vyjímatelné diskové jednotky

### Vytvoření zásady JITA pro uživatele nebo skupinu

Správci mohou uživatelům nebo skupinám povolit přístup k zařízením prostřednictvím ověřování v reálném čase JITA (Just In Time Authentication).

1. Spusťte nástroj **Device Access Manager** a poté klikněte nebo klepněte na položku **Změnit**.
2. Vyberte uživatele nebo skupinu a v části **Přístup** pro **Vyjímatelné diskové jednotky** nebo **Jednotky DVD/CD-ROM** klikněte nebo klepněte na šipku dolů a vyberte možnost **Povolit – Vyžadováno JITA**.
3. V části **Délka** klikněte nebo klepněte na šipku dolů a vyberte trvání přístupu JITA.

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

### Zakázání zásady JITA pro uživatele nebo skupinu

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

1. Spusťte nástroj **Device Access Manager** a poté klikněte nebo klepněte na položku **Změnit**.
2. Vyberte uživatele nebo skupinu a v části **Přístup** pro **Vyjímatelné diskové jednotky** nebo **Jednotky DVD/CD-ROM** klikněte nebo klepněte na šipku dolů a vyberte možnost **Zakázat – Vyžadováno JITA**.

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

# Nastavení

Okno **Nastavení** umožňuje správcům zobrazit a změnit jednotky, ke kterým je řízen přístup pomocí nástroje Device Access Manager.

**POZNÁMKA:** Při konfiguraci písmen jednotek musí být spuštěna aplikace Device Access Manager (viz Systémové zobrazení na stránce 43).

## Třídy nespravovaných zařízení

Aplikace HP Device Access Manager nespravuje tyto třídy zařízení:

- Vstupně-výstupní zařízení
  - CD-ROM
  - Disková jednotka
  - Řadič disketové jednotky (FDC)
  - Řadič pevného disku (HDC)
  - Třída zařízení lidského rozhraní (HID)
  - Zařízení infračerveného lidského rozhraní
  - Myš
  - Víceportové sériově připojené zařízení
  - Klávesnice
  - Tiskárny podporující technologii Plug and play (PnP)

- Tiskárna
- Upgrade tiskárny

- Napájení
  - Podpora pokročilé správy napájení (APM)
  - Baterie
- Různé
  - Počítač
  - Dekodér
  - Displej
  - Jednotný ovladač zobrazení Intel®
  - Karta s právními informacemi
  - Ovladač médií
  - Měnič médií
  - Technologie paměti
  - Monitor
  - Multifunkční
  - Síťový klient
  - Síťová služba
  - Síťový přenos
  - Procesor
  - Adaptér SCSI
  - Bezpečnostní urychlovač
  - Bezpečnostní zařízení
  - Systém
  - Neznámé
  - Svazek
  - Snímek objemu

# 8 HP Trust Circles

HP Trust Circles je bezpečnostní aplikace pro zabezpečení souborů a dokumentů, která kombinuje šifrování složek a souborů s příhodnou funkcí sdílení dokumentů v důvěryhodných skupinách. Tato aplikace šifruje soubory umístěné ve složkách určených uživatelem a chrání je v rámci skupiny Trust Circle. Jakmile jsou soubory jednou chráněny, mohou je používat a sdílet pouze členové skupiny Trust Circle. Pokud se chráněný soubor dostane k uživateli, který není členem skupiny, zůstane soubor zašifrovaný a tento uživatel nebude mít přístup k jeho obsahu.

## Otevření aplikace Trust Circles

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

   – nebo –

   na ploše systému Windows dvakrát klikněte na ikonu **HP Client Security** v oznamovací oblasti umístěné na pravé straně hlavního panelu

2. V části **Data** klikněte nebo klepněte na možnost **Trust Circles**.

## Začínáme

Existují dva způsoby, jak odeslat e-mailová pozvání a jak na ně odpovědět:

- **Použití aplikace Microsoft® Outlook** – Použití služby Trust Circles s produktem Microsoft Outlook automatizuje zpracování všech pozvání aplikace Trust Circle a odpovědí od jiných uživatelů aplikace Trust Circle.
- **Použití Gmail, Yahoo, Outlook.com nebo jiných e-mailových služeb (SMTP)** – Když zadáte své jméno, e-mailovou adresu a heslo, aplikace Trust Circles použije vaše e-mailové služby k odeslání e-mailových pozvání členům vybraným pro zapojení do vaší skupiny Trust Circle.

Nastavení vašeho základního profilu:

1. Zadejte své jméno a e-mailovou adresu a klikněte nebo klepněte na tlačítko **Další**.

   Jméno se bude zobrazovat všem členům, kteří jsou pozváni k účasti ve vaší skupině Trust Circle. E-mailová adresa slouží k odesílání, příjmu či odpovídání na pozvání.

2. Zadejte heslo ke svému e-mailovému účtu a klikněte nebo klepněte na tlačítko **Další**.

   Bude odeslána zkušební e-mailová zpráva na ověření správnosti nastavení e-mailu.

   **POZNÁMKA:** Počítač musí být připojen k síti.

3. V poli **Trust Circle Name** (Název skupiny Trust Circle) zadejte název skupiny Trust Circle a klikněte nebo klepněte na tlačítko **Další**.

4. Přidejte členy a složky a poté klikněte nebo klepněte na tlačítko **Další**. Bude vytvořena skupina Trust Circle obsahující vybrané složky a budou odeslána e-mailová pozvání členům, které jste vybrali. Pokud z jakýchkoli důvodů nelze odeslat pozvání, zobrazí se oznámení. Členy lze kdykoli pozvat znovu z okna Trust Circle klepnutím na možnost **Your Trust Circles** (Vaše skupiny Trust Circle) a dvojím kliknutím či dvojím klepnutím na skupinu Trust Circle. Další informace naleznete v části Trust Circles na stránce 48.

# Trust Circles

Skupinu Trust Circle můžete vytvořit během úvodního nastavení po zadání své e-mailové adresy nebo v zobrazení Trust Circle:

▲ V zobrazení Trust Circle klikněte nebo klepněte na příkaz **Create Trust Circle** (Vytvořit skupinu Trust Circle) a zadejte název skupiny Trust Circle.

- Chcete-li přidat členy do skupiny Trust Circle, klikněte nebo klepněte na ikonu **M+** vedle panelu **Členové** a poté postupujte podle pokynů na obrazovce.
- Chcete-li přidat složky do skupiny Trust Circle, klikněte nebo klepněte na ikonu **+** vedle panelu **Složky** a poté postupujte podle pokynů na obrazovce.

## Přidání složek do skupiny Trust Circle

### Přidání složek do nové skupiny Trust Circle:

- Během vytváření skupiny Trust Circle můžete přidat složky kliknutím nebo klepnutím na ikonu **+** vedle panelu **Složky**. Dále postupujte podle pokynů na obrazovce.

  – nebo –

- V aplikaci Průzkumník Windows klikněte pravým tlačítkem myši nebo klepněte a podržte složku, která aktuálně není součástí skupiny Trust Circle, vyberte možnost **Trust Circle** poté vyberte možnost **Create Trust Circle from Folder** (Vytvořit skupinu Trust Circle ze složky).

**TIP:** Můžete vybrat jednu nebo více složek.

### Přidání složek do již existující skupiny Trust Circle:

- V zobrazení Trust Circle klikněte na položku **Your Trust Circles** (Vaše skupiny Trust Circle), dvakrát klikněte nebo dvakrát klepněte na existující skupinu Trust Circle, čímž zobrazíte aktuální složky, klikněte nebo klepněte na ikonu **+** vedle panelu **Složky** a poté postupujte podle pokynů na obrazovce.

  – nebo –

- V aplikaci Průzkumník Windows klikněte pravým tlačítkem myši nebo klepněte a podržte složku, která aktuálně není součástí skupiny Trust Circle, vyberte možnost **Trust Circle** poté vyberte možnost **Add to existing Trust Circle from Folder** (Přidat do existující skupiny Trust Circle ze složky).

**TIP:** Můžete vybrat jednu nebo více složek.

Po přidání složky do skupiny Trust Circle aplikace Trust Circles automaticky zašifruje složku i její obsah. Po zašifrování všech souborů se zobrazí oznámení. Kromě toho se u všech ikon zašifrovaných složek a souborů v těchto složkách zobrazí zelený symbol zámku, který indikuje, že jsou tyto složky a soubory plně chráněny.

## Přidání členů do skupiny Trust Circle

K přidání členů do skupiny Trust Circle je třeba provést tři kroky:

1. **Pozvání** – Vlastník skupiny Trust Circle nejprve pozve členy. E-mailová zpráva s pozváním může být zaslána většímu počtu uživatelů nebo distribučním seznamům/skupinám.
2. **Přijetí** – Pozvaní uživatelé dostanou pozvání a rozhodnou se, zda jej přijmou nebo odmítnou. Pokud pozvaný uživatel přijme pozvání, bude odesílateli pozvání odeslána e-mailová odpověď. Pokud bylo pozvání odesláno skupině, každý člen obdrží pozvání a rozhodne se, zda jej přijme, nebo odmítne.
3. **Zaregistrování** – Odesílatel pozvání má finální příležitost rozhodnout, zda přidá člena do skupiny Trust Circle. Pokud se odesílatel pozvání rozhodne zaregistrovat člena, bude zvanému uživateli odesláno příslušné oznámení. Odesílatel pozvání a zvaný uživatel mohou volitelně ověřit zabezpečení procesu pozvání. Zvanému uživateli se zobrazí ověřovací kód, který musí po telefonu přečíst odesílateli pozvání. Po ověření kódů může odesílatel pozvání zaslat finální registrační e-mail.

**Přidání členů do nové skupiny Trust Circle:**

▲ Během vytváření skupiny Trust Circle můžete přidat členy kliknutím nebo klepnutím na ikonu **M+** vedle panelu **Členové**. Dále postupujte podle pokynů na obrazovce.

- Pokud používáte aplikaci Outlook, vyberte kontakty v adresáři aplikace Outlook a klikněte na tlačítko **OK**.
- Pokud používáte jinou e-mailovou službu, buď zadejte nové e-mailové adresy ručně do skupiny Trust Circle, nebo si je můžete nechat načíst z e-mailové adresy registrované v aplikaci Trust Circle.

**Přidání členů do již existující skupiny Trust Circle:**

▲ V zobrazení Trust Circle klikněte na položku **Your Trust Circles** (Vaše skupiny Trust Circle), dvakrát klikněte nebo dvakrát klepněte na existující skupinu Trust Circle, čímž zobrazíte aktuální členy, klikněte nebo klepněte na ikonu **M+** vedle panelu **Členové** a poté postupujte podle pokynů na obrazovce.

- Pokud používáte aplikaci Outlook, vyberte kontakty v adresáři aplikace Outlook a klikněte na tlačítko **OK**.
- Pokud používáte jinou e-mailovou službu, buď zadejte nové e-mailové adresy ručně do skupiny Trust Circle, nebo si je můžete nechat načíst z e-mailové adresy registrované v aplikaci Trust Circle.

## Přidání souborů do skupiny Trust Circle

Můžete přidat soubory do skupiny Trust Circle jedním z následujících způsobů:

- Zkopírujte nebo přesuňte soubor do existující složky ve skupině Trust Circle.

  – nebo –

- V aplikaci Průzkumník Windows klikněte pravým tlačítkem nebo klepněte a podržte soubor, který aktuálně není zašifrován, vyberte možnost **Trust Circle** a poté **Encrypt** (Šifrovat). Zobrazí se výzva k výběru skupiny Trust Circle, do které má být soubor přidán.

**TIP:** Můžete vybrat jeden nebo více souborů.

## Zašifrované složky

Každý člen skupiny Trust Circle může zobrazit a upravovat soubory patřící do této skupiny Trust Circle.

**POZNÁMKA:** Nástroj Trust Circle Manager/Reader nezajišťuje synchronizaci souborů mezi členy.

Soubory musí být sdíleny pomocí stávajících dostupných prostředků, například pomocí e-mailů, ftp nebo poskytovatelů cloudových úložišť. Soubory zkopírované, přesunuté nebo vytvořené ve složce ve skupině Trust Circle jsou okamžitě chráněny.

## Odebrání složek ze skupiny Trust Circle

Odebrání složky ze skupiny Trust Circle dešifruje složku a veškerý její obsah a odebere její ochranu

- V zobrazení Trust Circle klikněte na položku **Your Trust Circles** (Vaše skupiny Trust Circle), dvakrát klikněte nebo dvakrát klepněte na existující skupinu Trust Circle, čímž zobrazíte aktuální složky, a poté klikněte nebo klepněte na ikonu **koše** vedle dané složky.

  – nebo –

- V aplikaci Průzkumník Windows klikněte pravým tlačítkem nebo klepněte a podržte složku, která je součástí skupiny Trust Circle, vyberte možnost **Trust Circle** a poté **Remove from trust circle** (Odebrat ze skupiny Trust Circle).

**TIP:** Můžete vybrat jednu nebo více složek.

## Odebrání souboru ze skupiny Trust Circle

Chcete-li odebrat soubor ze skupiny Trust Circle, v aplikaci Průzkumník Windows klikněte pravým tlačítkem nebo klepněte a podržte soubor, který je aktuálně zašifrován, vyberte možnost **Trust Circle** a poté **Decrypt File** (Dešifrovat soubor).

## Odebrání členů ze skupiny Trust Circle

Ze skupiny Trust Circle není možné odebrat člena, který byl plně zaregistrován. Alternativou je vytvořit novou skupinu Trust Circle se všemi ostatními členy a přesunout všechny soubory a složky do nové skupiny Trust Circle a poté odstranit původní skupinu Trust Circle. To zajistí, že všechny nové soubory, které daný člen obdrží, pro něj nebudou přístupné, avšak vše, co jste s ním předtím sdíleli, bude pro člena staré skupiny Trust Circle nadále přístupné.

Pokud člen není kompletně zaregistrován, (člen byl zatím pouze pozván k připojení do skupiny Trust Circle nebo nepřijal pozvání do skupiny Trust Circle), můžete jej odebrat ze skupiny Trust Circle jedním z následujících způsobů:

- V zobrazení Trust Circle klikněte nebo klepněte na položku **Your Trust Circles** (Vaše skupiny Trust Circle) a pak dvakrát klikněte nebo dvakrát klepněte na skupinu Trust Circle, čímž zobrazíte aktuální seznam jejích členů. Klikněte nebo klepněte na ikonu **Koše** vedle jména člena, kterého chcete odebrat.
- V zobrazení Trust Circle klikněte nebo klepněte na položku **Členové** a poté dvakrát klikněte nebo dvakrát klepněte na člena, čímž zobrazíte skupiny Trust Circle, v nichž je členem. Klikněte nebo klepněte na ikonu **Koše** vedle skupiny Trust Circle, čímž odeberete člena z této skupiny.

## Odstranění skupiny Trust Circle

Chcete-li odstranit skupinu Trust Circle, ne podmínkou členství v této skupině.

▲ V zobrazení Trust Circle klikněte nebo klepněte na položku **Your Trust Circles** (Vaše skupiny Trust Circle) a klikněte nebo klepněte na ikonu **Koš** vedle skupiny Trust Circle, která má být odstraněna.

To odebere danou skupinu Trust Circle z této stránky a všem členům této skupiny Trust Circle odešle e-mailové zprávy s informací o odstranění skupiny. Všechny soubory a složky, které byly zahrnuty v dané skupině Trust Circle, budou dešifrovány.

# Nastavení předvoleb

V zobrazení Trust Circle klikněte nebo klepněte na položku **Preferences** (Předvolby). Zobrazí se tři karty

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

| Option (Možnost) | Popis |
|---|---|
| **Username** (Uživatelské jméno) | Zobrazuje právě používané uživatelské jméno. Chcete-li jej změnit, zadejte do textového pole nové uživatelské jméno. Změny budou automaticky uloženy. |
| **Email Address** (E-mailová adresa) | Zobrazuje právě používanou e-mailovou dresu. Chcete-li ji změnit, klikněte nebo klepněte na možnost **Change Email Settings** (Změnit nastavení e-mailu) a postupujte podle pokynů na obrazovce. |
| **New Member Confirmation** (Potvrzení nového člena) | Můžete si vybrat z následujících možností:<br>◦ **Confirm Automatically** (Potvrdit automaticky) – Po přijetí souhlasu od zvaného uživatele bude zvaný uživatel potvrzen jako člen skupiny Trust Circle bez nutnosti ručního zásahu a bude mu zaslán potvrzovací e-mail.<br>◦ **Confirm Manually** (Potvrdit ručně) – Po přijetí souhlasu od zvaného uživatele je vyžadováno ruční potvrzení zaregistrování zvaného uživatele jako člena skupiny Trust Circle. Uživateli poté bude zaslán potvrzovací e-mail.<br>◦ **Require Verification** (Požadovat ověření) – Po přijetí souhlasu od zvaného uživatele je k plnému zaregistrování zvaného uživatele vyžadován ověřovací kód. Vlastník skupiny Trust Circle musí kontaktovat pozvaného uživatele a vyžádat si od něj ověřovací kód. Po zadání správného kódu jsou odeslány potvrzovací e-maily. |
| **Periodic Authentication** (Periodické ověřování) | Periodické ověřování po uživateli vyžaduje zadání hesla systému Windows po uplynutí určité časové prodlevy (počítána v minutách) a dále při provádění citlivých operací. Toto nastavení umožňuje vypnout či zapnout ověřování uživatelů. |
| **Authentication Timeout** (Prodleva ověřování) | Určete požadovanou dobu (v minutách), po které bude vyžadováno ověření. |
| **Don't show confirmation message** (Nezobrazovat zprávu s potvrzením) | Výběrem tohoto políčka zakážete zobrazování zpráv s potvrzením, zrušením zaškrtnutí políčka zobrazíte zprávy s potvrzením. |
| **I'd like to help improve the HP Trust Circle through anonymous usage tracking** (Rád bych pomohl vylepšit aplikaci HP Trust Circle pomocí anonymního sledování použití) | Zaškrtněte toto políčko, pokud se chcete zúčastnit tohoto programu, zrušením zaškrtnutí políčka účast zrušíte. |

- **Backup/Restore** (Záloha/obnovení)

| Option (Možnost) | Popis |
|---|---|
| **Zálohování** | Zkopíruje vaše údaje aplikace Trust Circle Manager/Reader (nastavení a skupiny Trust Circle) do záložního souboru. V případě havárie nebo selhání systému můžete tento soubor použít k obnovení nové instalace aplikace Trust Circles do stavu v okamžiku uložení tohoto souboru.<br><br>**POZNÁMKA:** Jsou uložena pouze data vaší aplikace Trust Circle (skupiny Trust Circle, nastavení a členové). Vlastní soubory uložené v rámci skupin Trust Circle nejsou zálohovány. Tyto soubory musí být zálohovány samostatně.<br><br>Postup při zálohování uživatelských dat a nastavení aplikace Trust Circle:<br><br>**1.** Klikněte nebo klepněte na tlačítko **Zálohovat**.<br><br>**2.** Určete název souboru a adresář pro záložní soubor a klikněte nebo klepněte na příkaz **Uložit**.<br><br>**3.** Zadejte heslo, potvrďte jej a klikněte nebo klepněte na tlačítko **OK**. Toto heslo bude vyžadováno k obnovení souboru. |
| **Obnovení** | Obnoví nastavení a skupiny Trust Circles ze záložního souboru, obvykle po havárii systému nebo migraci na jiný počítač.<br><br>Postup při obnovení uživatelských dat a nastavení aplikace Trust Circle Manager:<br><br>**1.** Klikněte nebo klepněte na možnost **Obnovit**.<br><br>**2.** Přejděte k adresáři a názvu záložního soubor a klikněte nebo klepněte na příkaz **Otevřít**.<br><br>**3.** Zadejte heslo, které bylo vytvořeno při vytvoření zálohy. |

- **About** (O aplikaci) – Informace o verzi aplikace Trust Circle Manager/Reader. Jsou zobrazeny odkazy umožňující provedení upgradu aplikace Trust Circle Manager na verzi Pro nebo zobrazení prohlášení o ochraně soukromí společnosti HP.

# 9 Obnova po krádeži (pouze u vybraných modelů)

Nástroj Computrace (nutno zakoupit zvlášť) umožňuje na dálku monitorovat, spravovat a sledovat počítač.

Po aktivaci se služba Computrace z konfiguruje ze střediska Absolute Software Customer Center. Z tohoto střediska Customer Center může správce konfigurovat službu Computrace tak, aby monitorovala či spravovala počítač. Pokud je systém odcizen či přemístěn, středisko Customer Center může pomoci místním oprávněným složkám jej nalézt a znovu získat. Po konfiguraci může služba Computrace pokračovat ve funkci i po vymazání či výměně pevného disku.

Postup při aktivaci služby Computrace:

1. Připojte se k Internetu.
2. Spusťte nástroj HP Client Security. Další informace naleznete v části Spuštění aplikace HP Client Security na stránce 9.
3. Klikněte na možnost **Obnova po krádeži**.
4. Chcete-li spustit Průvodce aktivací služby Computrace, klikněte na tlačítko **Začněte**.
5. Zadejte kontaktní údaje spolu s údaji pro platbu platební kartou, nebo vložte předem zakoupený klíč produktu.

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

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

Přihlášení k zákaznickému centru:

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

Pomocí účtu v zákaznickém centru můžete následující:

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

▲ Klikněte na položku **Learn More** (Zjistit více) a zobrazte další informace o službě Computrace.

# 10 Výjimky při lokalizaci hesel

Na úrovni funkce ověřování po zapnutí a úrovni aplikace HP Drive Encryption je podpora lokalizace hesel omezená. Další informace naleznete v části Na úrovni funkce ověřování po zapnutí a úrovni aplikace Drive Encryption nejsou podporovány editory IME systému Windows na stránce 54.

## Jak postupovat, pokud bylo heslo odmítnuto

Heslo může být odmítnuto z následujících důvodů:

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

  1. Pomocí nástroje **Ovládací panely** přidejte podporované rozvržení klávesnice (v části Čínština přidejte americké rozvržení klávesnice).
  2. Podporovanou klávesnici nastavte na výchozí zadávání.
  3. Spusťte aplikaci HP Client Security a pak zadejte heslo systému Windows.

- Uživatel používá znak, který není podporován. Řešení:

  1. Změňte heslo systému Windows tak, aby obsahovalo jen podporované znaky. Další informace o nepodporovaných znacích najdete v části Práce se speciálními klávesami na stránce 55.
  2. Spusťte aplikaci HP Client Security a pak zadejte heslo systému Windows.

## Na úrovni funkce ověřování po zapnutí a úrovni aplikace Drive Encryption nejsou podporovány editory IME systému Windows

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

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

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

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

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

# Změna hesla pomocí rozvržení klávesnice, které je rovněž podporováno

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

**POZNÁMKA:** Tento problém mohou správci vyřešit pomocí stránky Uživatelé aplikace HP Client Security (dostupné prostřednictvím ikony **Ozubeného kola** na domovské stránce) Pomocí této možnosti je třeba uživatele z aplikace HP Client Security odstranit, poté je třeba v operačním systému vybrat požadované rozvržení klávesnice a nakonec znovu pro stejného uživatele spustit průvodce nastavením aplikace HP Client Security. V systému BIOS dojde k uložení požadovaného rozvržení klávesnice a hesla zadaná pomocí tohoto rozvržení budou v systému BIOS nastavena správně.

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

# Práce se speciálními klávesami

- Čínština, slovenština, kanadská francouzština a čeština

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

- Korejština

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

- V následující tabulce jsou uvedeny nepodporované znaky:

| Language (Jazyk) | Windows | BIOS | Drive Encryption |
|---|---|---|---|
| Arabština | Stisknutím klávesy ٰ, ً nebo ٌ dojde k vytvoření dvou znaků. | Stisknutím klávesy ٰ, ً nebo ٌ dojde k vytvoření jednoho znaku. | Stisknutím klávesy ٰ, ً nebo ٌ dojde k vytvoření jednoho znaku. |
| Kanadská francouzština | Stisknutím klávesy ç, è, à nebo é spolu s klávesou caps lock dojde v systému Windows k vytvoření znaku Ç, È, À, resp. É. | Stisknutím klávesy ç, è, à nebo é spolu s klávesou caps lock dojde v rámci Ověřování po zapnutí k vytvoření znaku ç, è, à, resp. é. | Stisknutím klávesy ç, è, à nebo é spolu s klávesou caps lock dojde v rámci aplikace HP Drive Encryption k vytvoření znaku ç, è, à, resp. é. |

| Language (Jazyk) | Windows | BIOS | Drive Encryption |
|---|---|---|---|
| Španělština | Rozvržení klávesnice 40a není podporováno. I přesto toto rozvržení funguje, protože je softwarem převedeno na rozvržení c0a. Avšak z důvodu velkých rozdílů mezi těmito rozvrženími klávesnice je španělsky mluvícím uživatelům doporučeno změnit rozvržení klávesnice systému Windows na 1040a (Španělské - variace) nebo 080a (Latinskoamerické). | Není k dispozici | Není k dispozici |
| Mezinárodní (Spojené státy) | ◦ Nelze použít klávesy ¡, ¤, ‘, ’, ¥ a × v horní řadě.<br>◦ Nelze použít klávesy å, ® a Þ v druhé řadě.<br>◦ Nelze použít klávesy á, ð a ø ve třetí řadě.<br>◦ Nelze použít klávesu æ v dolní řadě. | Není k dispozici | Není k dispozici |
| Čeština | ◦ Nelze použít klávesu ğ.<br>◦ Nelze použít klávesu į.<br>◦ Nelze použít klávesu ų.<br>◦ Nelze použít klávesy ė, ı a ż.<br>◦ Nelze použít klávesy ģ, ķ, ļ, ņ a ŗ. | Není k dispozici | Není k dispozici |
| Slovenština | Nelze použít klávesu ż. | ◦ Klávesy š, ś a ş lze použít pouze na softwarové klávesnici.<br>◦ Stisknutím znaménkové klávesy ţ dojde k vytvoření dvou znaků. | Není k dispozici |
| Maďarština | Nelze použít klávesu ż. | Stisknutím klávesy ţ dojde k vytvoření dvou znaků. | Není k dispozici |
| Slovinština | Klávesu žŽ nelze použít v systému Windows a klávesa alt v systému BIOS představuje znaménkovou klávesu. | V systému BIOS nelze použít klávesy ú, Ú, ů, Ů, ş, Ş, ś, Ś, š a Š. | Není k dispozici |
| Japanese (Japonština) | Pokud je to možné, je lépe používat editor IME Microsoft Office 2007. Navzdory názvu se v tomto případě vlastně jedná o podporované rozvržení klávesnice 411. | Není k dispozici | Není k dispozici |

# Slovníček

**aktivace**
úkol, který je nutné dokončit, aby bylo možné získat přístup k funkcím aplikace Drive Encryption. Správci mohou aplikaci Drive Encryption aktivovat pomocí Průvodce nastavením aplikace HP Client Security nebo pomocí aplikace HP Client Security. Proces aktivace se skládá z aktivace softwaru, zašifrování jednotky a vytvoření počátečního záložního šifrovacího klíče ve vyjímatelném paměťovém zařízení.

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

**automatické bezpečné odstranění**
Ničení, které uživatel naplánuje v aplikaci File Sanitizer.

**bezkontaktní karta**
Plastová karta obsahující elektronický čip, kterou je možné použít pro ověření totožnosti.

**Bluetooth**
Technologie využívající rádiové přenosy, aby počítače, tiskárny, myši, mobilní telefony a ostatní zařízení mohla bezdrátově komunikovat na kratší vzdálenost.

**čipová karta**
Hardwarové zařízení, které je možné spolu s kódem PIN použít pro ověření totožnosti.

**čištění volného prostoru**
Zapisování nahodilých dat přes odstraněné položky a nepoužitý prostor. Tento proces potlačí existenci odstraněných položek tak, že je obnovení původní položky náročnější.

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

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

**Domovská stránka**
Centrální místo, v němž lze přistupovat k funkcím a nastavením aplikace HP Client Security.

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

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

**hardwarové šifrování**
Použití samošifrujících jednotek splňujících specifikace OPAL organizace Trusted Computing Group pro správu samošifrujících disků k provedení okamžitého zašifrování. Hardwarové šifrování je okamžité a trvá pouze pár minut. Softwarové šifrování naopak může trvat několik hodin.

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

**identita**

Skupina pověření a nastavení v aplikaci HP Client Security, se kterou se zachází stejně jako s účtem nebo profilem určitého uživatele.

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

**karta s detekcí přiblížení**
plastová karta obsahující počítačový čip, kterou lze použít k ověření společně s jinými přihlašovacími údaji a získat tak zvýšenou úroveň zabezpečení.

**Kód PIN**
Osobní identifikační číslo zaregistrovaného uživatele, které slouží k ověřování.

**manuální skartace**
Okamžité bezpečné odstranění položky nebo vybraných položek, prováděné mimo naplánovanou dobu skartace.

**metoda zabezpečeného přihlašování**
Způsob použitý pro přihlášení se k počítači.

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

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

**otisk prstu**
Digitální sejmutí obrazu otisku prstu. Skutečný otisk prstu není v aplikaci HP Client Security nikdy uložen.

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

**ověřování**
proces ověření, že jste osoba, za kterou se vydáváte, a to prostřednictvím přihlašovacích údajů, jako jsou heslo systému Windows, otisk prstu, čipová karta, bezkontaktní karta nebo karta s detekcí přiblížení.

**Ověřování Just In Time Authentication.**
Viz nápověda softwaru HP Device Access Manager.

**Ověřování před spuštěním aplikace Drive Encryption.**
Přihlašovací obrazovka, která se zobrazí před spuštěním systému Windows. Uživatel musí zadat své uživatelské jméno a heslo systému Windows či kód PIN čipové karty nebo přiložit zaregistrovaný prst. Při použití přihlášení One-Step Logon umožní zadání správných informací na přihlašovací obrazovce aplikace Drive Encryption ve většině případů přímý přístup do systému Windows, aniž by bylo nutné se znovu přihlašovat na přihlašovací obrazovce systému Windows.

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

**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 aplikaci HP Client Security, jež se skládá z uživatelského jména a hesla (a případně další zvolené informace) a který lze použít pro přihlášení k webovým stránkám nebo k jiným programům.

**Přihlašovací obrazovka Drive Encryption (Šifrování jednotky)**

Viz ověřování před spuštěním aplikace Drive Encryption.

**Přihlašovací údaj**
Specifická informace nebo hardwarové zařízení používané k ověření totožnosti jednotlivého uživatele.

**připojené zařízení**
Hardwarové zařízení, které je zapojené do portu v počítači.

**restart**
Proces restartování počítače.

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

**skartace**
Provedení algoritmu přepisujícího data obsažená v položce nesmyslnými daty.

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

**Skupina Trust Circle**
Skupiny zajišťující ochranu dat svázáním dat s definovanou skupinou důvěryhodných uživatelů. To zabraňuje, aby se data záměrně či náhodně dostala do nesprávných rukou. Data jsou kryptograficky vázána na skupinu Trust Circle pomocí technologie Zero Overhead Key Management společnosti CryptoMill. To zabraňuje dešifrování dokumentů či jiných citlivých informací mimo skupinu Trust Circle.

**Složka Trust Circle**
Jakákoli složka, která je chráněna v rámci skupiny Trust Circle.

**softwarové šifrování**
Použití softwaru k zašifrování jednotlivých sektorů pevného disku. Tento proces je pomalejší než hardwarové šifrování

**správce**
Viz *Správce systému Windows*.

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

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

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

**Trust Circle Manager/Reader**
Aplikace Trust Circle Reader může pouze přijímat pozvání zasílaná uživateli aplikace Trust Circle Manager. Aplikace Trust Circle Manager umožňuje vytváření skupin Trust Circle. Zahrnuje také funkce pro pozvání dalších uživatelů pomocí e-mailu do skupiny Trust Circle a přijímání pozvánek do skupin Trust Circle od ostatních. Jakmile je mezi členy vytvořena skupina Trust Circle, je možné bezpečně sdílet soubory chráněné v rámci této skupiny Trust Circle.

**třída zařízení**
Všechna zařízení určitého typu, např. jednotky.

**Účet uživatele systému Windows**
uživatel, který je oprávněn přihlásit se do sítě či do konkrétního počítače.

**uživatel**

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

**Vestavěný bezpečnostní čip TPM (Trusted Platform Module)**
Funkce TPM ověřuje počítač namísto uživatele pomocí uložení informací specifických pro hostitelský systém, jako jsou šifrovací klíče, digitální certifikáty a hesla. Funkce TPM minimalizuje riziko kompromitování informací v počítači při krádeži počítače či útoku externího hackera.

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

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

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

# Rejstřík