HP ProtectTools

Úvodní informace

První vydání: Leden 2007

Číslo dokumentu: 419699-221

Obsah

1 Úvod

Software HP ProtectTools Security Manager poskytuje funkce zabezpečení, které chrání před neoprávněným přístupem k počítačům, sítím a důležitým datům. Funkce pokročilého zabezpečení jsou k dispozici prostřednictvím následujících softwarových modulů:

- Smart Card Security pro HP ProtectTools,
- Java Card Security pro HP ProtectTools,
- Embedded Security pro HP ProtectTools,
- BIOS Configuration pro HP ProtectTools,
- Credential Manager pro HP ProtectTools,
- Device Access Manager pro HP ProtectTools.

Obsah nabídky dostupných softwarových modulů je závislý na modelu počítače. Nástroj Embedded Security pro HP ProtectTools například vyžaduje, aby byl v počítači nainstalován integrovaný bezpečnostní čip Trusted Platform Module (TPM; jen na některých modelech) a nástroj Smart Card Security pro HP ProtectTools vyžaduje doplňkovou čipovou kartu a čtečku.

Softwarové moduly HP ProtectTools lze předem nainstalovat, zavést, případně je můžete stáhnout ze stránek společnosti HP. Další informace získáte na stránkách http://www.hp.com.

Poznámka Pokyny v této příručce přepokládají, že jsou již nainstalovány odpovídající moduly softwaru HP ProtectTools.

Spuštění nástroje HP ProtectTools Security Manager

Spuštění nástroje HP ProtectTools Security Manager z ovládacího panelu systému Windows®:

▲ Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.

Poznámka Po dokončení konfigurace modulu Credential Manager můžete nástroj HP ProtectTools spustit také pomocí přihlášení do modulu Credential Manager na obrazovce pro přihlášení do systému Windows. Další informace naleznete v části „Přihlášení do systému Windows pomocí nástroje Credential Manager“ v kapitole 6 „Credential Manager pro HP ProtectTools“.

Představení bezpečnostních rolí

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

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

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

- Security officer (Správce zabezpečení) — Určuje úroveň zabezpečení společnosti nebo sítě a určuje, jaké funkce zabezpečení se mají požít, například čipové karty, čtečky otisků prstů nebo klíče USB.

Poznámka Množství funkcí nástroje HP ProtectTools lze upravit správcem zabezpečení v součinnosti se společností HP. Další informace získáte na stránkách http://www.hp.com.

- IT administrator (Správce IT) — Aplikuje a spravuje funkce zabezpečení určené správcem zabezpečení. Může současně aktivovat a deaktivovat některé funkce. Pokud se správce zabezpečení například rozhodne použít čipové karty, může správce IT aktivovat režim zabezpečení čipových karet systému BIOS.
- User (Uživatel) — Používá funkce zabezpečení. Pokud například správce zabezpečení a správce IT aktivovali v systému použití čipových karet, může uživatel nastavit kód PIN čipové karty a používat ji pro ověřování.

Správa hesel nástroje HP ProtectTools

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

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

Heslo nástroje HP ProtectTools	Nastavuje se v tomto modulu nástroje HP ProtectTools.	Funkce
Heslo pro správce nástroje Computer Setup **Poznámka** Označuje se také jako heslo správce systému BIOS, heslo nástroje Setup po stisknutí klávesy f10, bezpečnostní heslo nástroje Setup.	Modul BIOS Configuration, správce IT	Omezuje přístup k nástroji Computer Setup.
Heslo vyžadované po zapnutí	BIOS Configuration	Omezuje přístup k obsahu počítače, když se počítač zapíná, restartuje nebo obnovuje z režimu spánku.
Heslo správce čipové karty **Poznámka** Označuje se také jako heslo karty správce systému BIOS	Modul Smart Card Security, správce IT	Používá se k ověření při spuštění pomocí čipové karty (v rámci systému BIOS). Umožňuje přístup k nástroji Computer Setup a obsahu počítače ve chvíli, kdy se počítač zapíná, restartuje nebo obnovuje z režimu spánku. Současně umožňuje vytvoření souborů pro obnovu pro účely obnovení karet uživatelů nebo správců.
Heslo uživatele čipové karty **Poznámka** Označuje se také jako heslo karty uživatele systému BIOS	Zabezpečení pomocí čipových karet	Používá se k ověření při spuštění pomocí čipové karty (v rámci systému BIOS). Umožňuje přístup k obsahu počítače při jeho zapnutí, restartování a přechodu z režimu spánku.
Kód PIN čipové karty	Zabezpečení pomocí čipových karet	Chrání přístup k obsahu čipové karty a ověřuje uživatele čipové karty. Při použití pro ověřování při spuštění omezuje kód PIN čipové karty současně přístup k nástroji Computer Setup a k obsahu počítače.
Heslo k souboru pro obnovu čipové karty	Zabezpečení pomocí čipových karet	Brání v přístupu k souboru pro obnovu, který obsahuje hesla systému BIOS.
Kód PIN karty Java™ Card	Zabezpečení karty Java Card	Chrání přístup k obsahu karty Java Card a ověřuje uživatele karty Java Card. Při použití pro ověřování při spuštění omezuje kód PIN karty Java Card současně přístup k nástroji Computer Setup a k obsahu počítače.
Heslo základního uživatelského klíče	Modul Embedded Security (Integrované zabezpečení)	Používá se k přístupu k funkcím integrovaného zabezpečení, jako je zabezpečené šifrování elektronické pošty, souborů a složek. Pokud se používá pro ověření při spuštění, současně omezuje

Heslo nástroje HP ProtectTools	Nastavuje se v tomto modulu nástroje HP ProtectTools.	Funkce
Poznámka Současně se označuje jako: heslo integrovaného zabezpečení		přístup k obsahu počítače – při jeho zapnutí, restartování a přechodu z režimu spánku.
Heslo známky nouzové obnovy **Poznámka** Současně se označuje jako: Heslo klíče známky nouzové obnovy	Modul Embedded Security, správce IT	Chrání přístup ke známce nouzové obnovy, což je soubor zálohy integrovaného bezpečnostního čipu.
Heslo vlastníka	Modul Embedded Security, správce IT	Chrání systém a čip TPM před neoprávněným přístupem k funkcím integrovaného zabezpečení.
Heslo pro přihlášení do nástroje Credential Manager	Credential Manager	Heslo nabízí 2 možnosti použití: • Lze je použít k samostatnému přihlášení k nástroji Credential Manager po přihlášení k systému Windows. • Lze je použít namísto přihlášení k systému Windows, kdy umožní přístup k systému Windows i k nástroji Credential Manager současně.
Heslo souboru obnovení nástroje Credential Manager	Modul Credential Manager, správce IT	Omezuje přístup k souboru pro obnovu nástroje Credential Manager.
Heslo pro přihlášení do systému Windows	Ovládací panel systému Windows	Lze jej použít k ručnímu přihlášení nebo jej lze uložit na čipovou kartu.

Vytvoření bezpečného hesla

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

- Používejte hesla s alespoň 7 znaky a pokud možno s více než 8 znaky.
- V hesle používejte zároveň znaky s velkým i malým písmenem.
- Pokud je to možné, používejte zároveň písmena i čísla a speciální znaky a znaménka interpunkce.
- V klíčovém slově nahraďte písmena čísly nebo speciálními znaky. Například můžete číslem 1 nahradit písmena I nebo L.
- Kombinujte slova ze 2 a více jazyků.
- Rozdělujte slova nebo fráze uprostřed pomocí čísel nebo speciálních znaků, například „Mary2-2Cat45”.
- Nepoužívejte jako heslo slovo, které lze najít ve slovníku.
- Nepoužívejte jako heslo svoje jméno nebo jakékoliv jiné osobní údaje jako datum narození, jména domácích mazlíčků nebo jméno matky za svobodna, i přesto, že byste je napsali pozpátku.
- Hesla pravidelně měňte. Stačí vždy změnit pouze několik znaků.
- Pokud si zapíšete heslo, neskladujte jej na běžně přístupném místě v blízkosti počítače.
- Neukládejte heslo do souboru na počítači, například do zprávy elektronické pošty.
- Nesdílejte s nikým uživatelské účty ani nikomu neprozrazujte hesla.

2 Smart Card Security pro HP ProtectTools

Modul Smart Card Security pro HP ProtectTools řídí nastavení a konfiguraci čipových karet u počítačů vybavených doplňkovou čtečkou čipových karet.

S modulem Smart Card Security můžete:

- Přistupovat k funkcím zabezpečení čipové karty.
- Inicializovat čipovou kartu, aby ji bylo možno s dalšími moduly HP ProtectTools, například Credential Manager pro HP ProtectTools.
- Zapnout ověření pomocí čipových karet po zapnutí počítače v nástroji Computer Setup a konfigurovat jednotlivé čipové karty pro uživatele a správce Tato funkce vyžaduje, aby uživatel vložil čipovou kartu do čtečky a zadal volitelný kód PIN. Teprve poté je povoleno zavedení operačního systému.
- Nastavit a změnit heslo pro ověření uživatelů čipové karty.
- Zálohovat a obnovit hesla systému BIOS uložená na čipové kartě.

Inicializace čipové karty

Před použitím čipové karty je třeba ji inicializovat.

Postup při inicializaci čipové karty:

1. Vložte čipovou kartu do čtečky.
2. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
3. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **Smart Card**.
4. V pravém podokně klepněte na tlačítko **Initialize** (Inicializovat).
5. Do prvního políčka v dialogovém okně **Initialize the smart card** (Inicializace čipové karty) zadejte své jméno.
6. Do příslušných políček zadejte a potvrďte kód PIN čipové karty. Kód PIN musí mít 4 až 8 číselných znaků.

   UPOZORNĚNÍ Abyste zabránili ztrátě přístupu k počítači, nezapomeňte kód PIN čipové karty. Pokud jej zapomenete, práce s počítačem může být znemožněna. Nebude-li kód PIN zadán správně nejpozději pátým pokusem, bude čipová karta zamčena a stane se nepoužitelnou. Počitadlo neúspěšných pokusů se po zadání správného kódu PIN vynuluje.

7. Inicializaci dokončete klepnutím na tlačítko **OK**.

Režim zabezpečení systému BIOS čipovou kartou

Pokud je zapnut režim ochrany systému BIOS čipovou kartou, je ke spuštění počítače třeba použít čipovou kartu.

Aktivace režimu zabezpečení systému BIOS čipovou kartou sestává z následujících kroků:

1. V konfiguraci systému BIOS zapněte podporu pro ověřování čipovými kartami při spuštění. Viz část „Aktivace a deaktivace podpory ověřování při spouštění pomocí čipových karet Smart Card nebo karet Java Card“ v Kapitole 5, „BIOS Configuration pro HP ProtectTools“.

   Poznámka Aktivace tohoto nastavení vám umožní používat čipovou kartu pro ověřování při spuštění. Dokud nezapnete podporu pro ověřování čipovými kartami při spuštění, nebudou funkce režimu zabezpečení systému BIOS čipovou kartou dostupné.

2. V části Smart Card Security (Zabezpečení čipovou kartou) povolte zabezpečení systému BIOS čipovou kartou. Viz část „Zapnutí režimu zabezpečení systému BIOS čipovou kartou a nastavení hesla správce čipových karet“ dále v této kapitole.

3. Nastavte heslo správce čipových karet.

   Poznámka Nastavení hesla správce čipových karet je součástí aktivace režimu zabezpečení systému BIOS čipovou kartou.

Heslo správce čipových karet není stejné jako heslo k nástroji Computer Setup. Heslo správce čipových karet propojuje čipovou kartu s počítačem pro účely identifikace a umožňuje také následující:

- přístup k nástroji Computer Setup a obsahu počítače, když je počítač zapnutý,
- vytvořit nové čipové karty pro správce a uživatele,
- vytvořit soubor pro obnovu, pomocí kterého lze obnovit čipovou kartu uživatele i správce.

Zapnutí režimu zabezpečení systému BIOS čipovou kartou a nastavení hesla správce čipových karet

Postup zapnutí režimu zabezpečení systému BIOS čipovou kartou a nastavení hesla správce čipových karet:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **BIOS**.
3. V pravém podokně u položky BIOS Security Mode (Režim zabezpečení systému BIOS) klepněte na tlačítko **Enable** (Povolit).
4. Klepněte na tlačítko **Další**.
5. Na výzvu zadejte heslo k nástroji Computer Setup a klepněte na tlačítko **Next** (Další).
6. Vložte novou čipovou kartu správce a postupujte podle pokynů na obrazovce. Tyto pokyny se různí a mohou zahrnovat následující úlohy:
   - Inicializace čipové karty. Podrobné pokyny viz „Inicializace čipové karty“.
   - Nastavení hesla správce čipových karet. Podrobné pokyny viz „Uložení hesla karty správce nebo uživatele“.
   - Vytvoření souboru pro obnovu. Podrobné pokyny viz „Vytvoření souboru pro obnovu.“.

Vypnutí režimu zabezpečení systému BIOS čipovou kartou

Po vypnutí režimu ochrany systému BIOS čipovou kartou budou hesla správců a uživatelů čipových karet deaktivována a pro přístup k počítači již nebude čipová karta potřebná.

Poznámka Pokud byl předtím režim zabezpečení systému BIOS čipovou kartou zapnutý, tlačítko na stránce „Smart Card Security BIOS“ se změní na Disable (Zakázat).

Postup vypnutí zabezpečení čipovou kartou:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **BIOS**.
3. V pravém podokně u položky BIOS Security Mode (Režim zabezpečení systému BIOS) klepněte na možnost **Disable** (Zakázat).
4. Vložte kartu s aktuálním heslem správce čipových karet a klepněte na tlačítko **Další**
5. Na výzvu zadejte kód PIN této karty a klepněte na tlačítko **Finish** (Dokončit).

Změna hesla správce čipových karet

Nastavení hesla správce čipových karet je součástí aktivace režimu zabezpečení systému BIOS čipovou kartou. Poté, co bylo nastaveno, můžete toto heslo změnit. Další informace o hesle správce čipových karet naleznete v předchozí části „Režim zabezpečení systému BIOS čipovou kartou“ v této kapitole.

Poznámka Následující postup slouží k aktualizaci hesla správce čipových karet uloženého na kartě a v nástroji Computer Setup.

Postup při změně hesla správce čipových karet:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **BIOS**.
3. V pravém podokně u položky **BIOS Security Mode** (Režim zabezpečení systému BIOS) vedle položky **BIOS administrator card** (BIOS karta správce) klepněte na možnost **Change** (Změnit).
4. Zadejte kód PIN čipové karty a klepněte na tlačítko **Next** (Další).
5. Vložte novou kartu správce a klepněte na tlačítko **Next** (Další).
6. Zadejte kód PIN této karty a klepněte na tlačítko **Finish** (Dokončit).

Nastavení a změna hesla uživatele čipové karty

Postup nastavení nebo změny hesla uživatele čipové karty:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **BIOS**.
3. V pravém podokně u položky **BIOS Security Mode** (Režim zabezpečení systému BIOS) vedle položky **BIOS administrator card** (BIOS karta uživatele) klepněte na tlačítko **Set** (Nastavit).

   Poznámka Pokud již v nástroji Computer Setup existuje heslo uživatele, klepněte na tlačítko **Change** (Změnit).

4. Zadejte kód PIN čipové karty a klepněte na tlačítko **Next** (Další).
5. Vložte novou kartu uživatele a klepněte na tlačítko **Next** (Další).
   - Pokud se již na kartě nachází heslo uživatele, zobrazí se dialogové okno **Finish** (Dokončit). Vynechejte kroky 6 až 8 a pokračujte krokem 9.
   - Pokud se na kartě nenachází žádné heslo uživatele, spustí se BIOS Password Wizard (Průvodce heslem systému BIOS).
6. V průvodci heslem systému BIOS máte dvě možnosti:
   - Zadat heslo ručně.
   - Vygenerovat náhodné heslo o délce 32 byte

   Poznámka Použití známého hesla umožňuje vytvářet duplikáty karet bez použití souboru pro obnovu. Vygenerování náhodného hesla poskytuje vyšší úroveň zabezpečení, avšak pro vytvoření záložních karet je třeba mít soubor pro obnovu.

7. V části **Boot Requirements** (Požadavky při spouštění) zaškrtněte políčko, pokud požadujete zadání kódu PIN čipové karty při spouštění.

   Poznámka Pokud zadání kódu PIN čipové karty při spouštění nepožadujete, ponechte toto políčko prázdné.

8. Zadejte kód PIN čipové karty a klepněte na tlačítko **OK**. Systém vás vyzve k vytvoření souboru pro obnovu.

   Poznámka Vytvoření souboru pro obnovu důrazně doporučujeme. Další informace naleznete v části „Vytvoření souboru pro obnovu.“ dále v této kapitole.

9. V dialogovém okně **Finish** (Dokončení) zadejte kód PIN čipové karty a klepněte na tlačítko **Finish** (Dokončit).

Uložení hesla karty správce nebo uživatele

Pokud chcete vytvořit záložní kartu a nastavili jste již heslo správce, můžete je uložit na novou kartu.

UPOZORNĚNÍ Tímto postupem aktualizujete pouze heslo uložené na kartě, ne však heslo v nástroji Computer Setup. S novou kartou nebudete mít přístup k počítači.

Postup uložení hesla správce nebo uživatele karty:

1. Vložte čipovou kartu do čtečky.
2. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
3. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **BIOS**.
4. V pravém podokně v části **BIOS Password on Smart Card** (Heslo systému BIOS na čipové kartě) klepněte na tlačítko **Store** (Uložit).
5. V průvodci heslem systému BIOS máte dvě možnosti:
   - Zadat heslo ručně
   - Vygenerovat náhodné heslo o délce 32 byte

   Poznámka Použití známého hesla umožňuje vytvářet duplikáty karet bez použití souboru pro obnovu. Vygenerování náhodného hesla poskytuje vyšší úroveň zabezpečení, avšak pro vytvoření záložních karet je třeba mít soubor pro obnovu.
6. V části **Access Privilege** (Oprávnění přístupu) vyberte typ karty **Administrator** (Správce) nebo **User** (Uživatel).
7. V části **Boot Requirements** (Požadavky při spouštění) zaškrtněte políčko, pokud požadujete zadání kódu PIN čipové karty při spouštění.

   Poznámka Pokud zadání kódu PIN čipové karty při spouštění nepožadujete, ponechte toto políčko prázdné.
8. Zadejte kód PIN čipové karty a klepněte na tlačítko **OK**.
9. V dialogovém okně **Finish** (Dokončení) znovu zadejte kód PIN čipové karty a klepněte na tlačítko **Finish** (Dokončit).

   Systém vás vyzve k vytvoření souboru pro obnovu.

   Poznámka Vytvoření souboru pro obnovu čipové karty důrazně doporučujeme. Další informace naleznete v části „Vytvoření souboru pro obnovu.“ dále v této kapitole.

Obecné úlohy

Aktualizace nastavení systému BIOS pro čipové karty

Má-li se při restartu počítače požadovat kód PIN čipové karty:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **BIOS**.
3. V pravém podokně v části **BIOS Password on Smart Card** (Heslo systému BIOS na čipové kartě) klepněte na tlačítko **Store** (Uložit).
4. Zaškrtněte políčko, pokud se má při restartu požadovat kód PIN.

   Poznámka Chcete-li tento požadavek odstranit, zrušte zaškrtnutí tohoto políčka.

5. Zadejte kód PIN čipové karty a klepněte na tlačítko **OK**.

Výběr čtečky čipových karet

Před použitím čipové karty ověřte, zda je v nástroji Smart Card Security vybrána správná čtečka čipových karet. Není-li v nástroji Smart Card Security vybrána správná čtečka, některé z jeho funkcí mohou být nedostupné nebo nesprávně zobrazené.

Postup výběru čtečky čipových karet:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **General** (Obecné).
3. V pravém podokně v části **Smart Card Reader** (Čtečka čipových karet) klepněte na správnou čtečku.
4. Vložte čipovou kartu do čtečky. Informace ze čtečky se automaticky obnoví.

Změna kódu PIN čipové karty

Postup při změně kódu PIN čipové karty:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **Smart Card**.
3. V pravém podokně v části **Change PIN** (Změnit kód PIN) klepněte na tlačítko **Change PIN**.
4. Zadejte současný kód PIN čipové karty.
5. Nastavte a potvrďte nový kód PIN.
6. V dialogovém okně s informacemi klepněte na tlačítko **OK**.

Zálohování a obnova čipových karet

Poté, co jste inicializovali čipovou kartu a karta je připravena k použití, důrazně doporučujeme vytvořit soubor pro obnovu čipové karty. Soubor pro obnovu slouží k přenesení dat z jedné čipové karty na jinou kartu. Také jej lze použít pro zálohu původní čipové karty nebo k obnovení dat při ztrátě či krádeži karty.

UPOZORNĚNÍ Aby nenastalo, že soubor pro obnovu nebude odpovídat aktualizovaným informacím na čipové kartě, ihned vytvořte nový soubor pro obnovu a uložte jej na bezpečném místě. Máte-li k čipové kartě záložní kartu, musíte také aktualizovat informace na této kartě použitím nového souboru pro obnovu na tuto záložní kartu.

Vytvoření souboru pro obnovu.

Postup při vytvoření souboru pro obnovu:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **Smart Card**.
3. V pravém podokně v části **Recovery** (Obnova) klepněte na tlačítko **Create** (Vytvořit).
4. Zadejte kód PIN čipové karty a klepněte na tlačítko **OK**.
5. Do pole **Filename** (Název souboru) zadejte jméno a cestu k souboru.

   UPOZORNĚNÍ Abyste předešli ztrátě přístupu k počítači, neukládejte soubor pro obnovu na pevný disk počítače, neboť bez čipové karty k němu nebudete mít přístup. Soubor obnovy uložený na pevném disku může být přístupný dalším osobám, což představuje určité bezpečnostní riziko.

6. Zadejte a potvrďte heslo k souboru pro obnovu a klepněte na tlačítko **OK**.

UPOZORNĚNÍ Abyste předešli ztrátě dat v souboru pro obnovu čipové karty, nesmíte zapomenout heslo k tomuto souboru. Není možné znovu vytvořit kartu ze souboru obnovy, pokud zapomenete heslo.

Obnova dat na čipové kartě

Data na čipové kartě je možno obnovit ze souboru pro obnovu. To je užitečné zejména v případě ztráty nebo krádeže karty, případně pokud chcete vytvořit záložní čipovou kartu. Při použití karty, na níž jsou uložena předchozí data, budou tato data přepsána.

Před zahájením akce potřebujete následující:

- přístup k počítači s nainstalovaným softwarem Smart Card Security,
- soubor pro obnovu čipové karty,
- heslo k souboru pro obnovu čipové karty,
- čipovou kartu.

Postup při obnovení čipové karty:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Smart Card Security** (Zabezpečení čipovou kartou) a poté klepněte na položku **Smart Card**.
3. Vložte disketu nebo jiné médium obsahující soubor pro obnovu čipové karty.
4. Vložte čipovou kartu do čtečky. Pokud čipová karta není inicializovaná, budete k její inicializaci vyzváni. Podrobné pokyny k inicializaci čipové karty naleznete v části „Inicializace čipové karty“ dříve v této kapitole.
5. V pravém podokně v části **Recovery** (Obnova) klepněte na tlačítko **Restore** (Obnovit).
6. Ověřte, že je vybráno správné jméno souboru pro obnovu, a zadejte heslo k tomuto souboru.
7. Zadejte kód PIN čipové karty.
8. Klepněte na tlačítko **OK**. Obsah původní čipové karty se nahraje do nové karty.

Vytvoření záložní čipové karty

Důrazně doporučujeme, abyste si vytvořili duplikáty čipových karet pro účely zálohování. K vytvoření záložní karty lze použít dva postupy v závislosti na tom, zda bylo heslo na čipové kartě zadáno ručně nebo vygenerováno náhodně.

Vytvoření náhradní čipové karty s náhodně vygenerovaným heslem:

- Vložte čipovou kartu do čtečky a načtěte na ni příslušný soubor pro obnovu. Další informace naleznete v části „Obnova dat na čipové kartě“ dříve v této kapitole.

Vytvoření náhradní čipové karty s ručně zadaným heslem:

1. Novou čipovou kartu inicializujte. Pokyny naleznete v části „Inicializace čipové karty“ dříve v této kapitole.
2. Na novou čipovou kartu uložte heslo správce nebo uživatele karty. Pokyny naleznete v části „Uložení hesla karty správce nebo uživatele“ dříve v této kapitole.

3 Java Card Security pro HP ProtectTools

Modul Java Card Security pro HP ProtectTools spravuje instalaci a konfiguraci karet Java Card u počítačů s doplňkovou čtečkou čipových karet.

Modul Java Card Security nabízí tyto funkce:

- Přístup k bezpečnostním funkcím karty Java Card.
- Aktivace funkce ověření v prostředí před zavedením systému pomocí karet Java Card v nastavení systému pomocí nástroje Computer Setup a konfigurace jednotlivých karet Java Card pro uživatele a správce. Tato funkce vyžaduje, aby před spuštěním operačního systému uživatel vložil kartu Java Card a zadal kód PIN.
- Nastavení a změna kódu PIN pro ověření uživatelů při použití karty Java Card.
- Záloha a obnovení ověřování karet Java Card po zapnutí.

Obecné úlohy

Stránka „General“ („Obecné“) umožňuje provádění následujících operací:

- Změna kódu PIN karty Java Card
- Výběr čtečky karet Smart Card

Poznámka Čtečku čipových karet mohou využívat karty Java Card i čipové karty. Tato funkce je dostupná, pouze pokud je k počítači připojeno více čteček čipových karet.

Změna kódu PIN karty Java Card

Změna kódu PIN karty Java Card

Poznámka Kód PIN karty Java Card musí obsahovat 4 - 8 číselných znaků.

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karty Java Card) a poté klepněte na položku **General** (Obecné).
3. Vložte kartu Java Card (s existujícím PIN kódem) do čtečky čipových karet.
4. V pravém podokně klepněte na položku **Change** (Změnit).
5. V dialogovém okně **Change PIN** (Změnit PIN) zadejte aktuální kód PIN do pole **Current PIN** (Aktuální PIN).
6. Do pole **New PIN** (Nový PIN) zadejte nový kód PIN, a pak ho zadejte ještě jednou do pole **Confirm New PIN** (Potvrdit nový PIN).
7. Klepněte na tlačítko **OK**.

Výběr čtečky čipových karet

Před použitím karty Java Card zkontrolujte, zda je vybrána správná čtečka čipových karet v modulu Java Card Security. Pokud není v modulu Java Card Security vybrána správná čtečka, některé z funkcí mohou být nedostupné nebo se nemusí zobrazovat správně.

Postup při výběru čtečky čipových karet:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karty Java Card) a poté klepněte na položku **General** (Obecné).
3. Vložte kartu Java Card do čtečky čipových karet.
4. V pravém podokně v části **Smart Card Reader** (Čtečka čipových karet) klepněte na správnou čtečku.

Pokročilé operace (určeno pouze pro správce)

Stránka „Advanced“ („Pokročilé“) umožňuje provádění následujících operací:

- Přiřazení kódu PIN pro kartu Java Card
- Přiřazení názvu kartě Java Card
- Nastavení ověřování po zapnutí
- Záloha a obnovení karet Java Card

Poznámka Pro přístup ke stránce „Advanced“ („Pokročilé“) musíte mít heslo k nástroji Computer Setup.

Přiřazení kódu PIN kartě Java Card

Kartě Java Card musíte přiřadit kód PIN dříve, než je použita pro ověření po zapnutí.

Přiřazení kódu PIN kartě Java Card:

Poznámka Kód PIN karty Java Card musí obsahovat 4 - 8 číselných znaků.

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karty Java Card) a poté klepněte na položku **General** (Obecné).
3. Vložte novou kartu Java Card do čtečky čipových karet.
4. Po otevření dialogového okna **Change PIN** (Změnit PIN) zadejte nový kód PIN do polí **New PIN** (Nový PIN) a **Confirm New PIN** (Potvrdit nový PIN).
5. Klepněte na tlačítko **OK**.

Přiřazení názvu kartě Java Card

Kartě Java Card musíte přiřadit název dříve, než je použita pro ověření po zapnutí.

Přiřazení názvu kartě Java Card:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karet Java Card) a poté klepněte na položku **Advanced** (Pokročilé).
3. Po zobrazení dialogového okna **Setup Password** zadejte své heslo pro nástroj Computer Setup a klepněte na tlačítko **OK**.
4. Vložte kartu Java Card do čtečky čipových karet.

   Poznámka Pokud jste dosud nepřiřadili této kartě kód PIN, otevře se dialogové okno Change PIN (Změna kódu PIN) umožňující zadání nového kódu PIN.

5. V pravém podokně v nabídce **Java Card** klepněte na položku **Change** (Změnit).
6. Zadejte nový název karty Java Card do pole **Name** (Název).
7. Zadejte aktuální PIN kód karty Java Card do pole **PIN**.
8. Klepněte na tlačítko **OK**.

Nastavení ověřování po zapnutí

Pokud je aktivována možnost ověřování po zapnutí, je vyžadováno použití karty Java Card pro spuštění počítače.

Proces aktivace ověřování karet Java Card po zapnutí v sobě zahrnuje následující kroky:

1. Aktivace podpory ověřování karet Java Card po zapnutí v nastavení systému BIOS nebo pomocí nástroje Computer Setup Viz část „Aktivace a deaktivace podpory ověřování při spouštění pomocí čipových karet Smart Card nebo karet Java Card“ v Kapitole 5, „BIOS Configuration pro HP ProtectTools“.
2. Povolení ověřování po zapnutí kartou Java Card v modulu Java Card Security. Viz část „Aktivace ověřování karet Java Card po zapnutí a vytvoření karty Java Card pro správce.“ dále v této kapitole.
3. Vytvoření a aktivace karty Java Card pro správce.

Aktivace ověřování karet Java Card po zapnutí a vytvoření karty Java Card pro správce.

Aktivace ověřování karet Java Card po zapnutí:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karet Java Card) a poté klepněte na položku **Advanced** (Pokročilé).
3. Po zobrazení dialogového okna **Computer Setup Password** zadejte své heslo pro nástroj Computer Setup a klepněte na tlačítko **OK**.
4. Vložte kartu Java Card do čtečky čipových karet.

   Poznámka Pokud jste dosud nepřiřadili této kartě kód PIN, otevře se dialogové okno **Change PIN** (Změnit PIN) umožňující zadání nového kódu PIN.

5. V pravém podokně v nabídce **Power-on authentication** (Ověřování po zapnutí) zaškrtněte políčko **Enable** (Povolit).
6. Pokud nemáte aktivovánu funkci DriveLock, zadejte PIN kód karty Java Card a klepněte na tlačítko **OK**.

   – nebo –

   Pokud máte aktivovánu funkci DriveLock:

   a. klepněte na položku **Make Java card identity unique** (Vytvořit identitu karty Java Card jako jedinečnou),

      – nebo –

      klepněte na položku **Make the Java card identity the same as the DriveLock password** (Vytvořit identitu karty Java Card totožnou s heslem Drivelock).

      Poznámka Pokud je aktivována na počítači funkce DriveLock, je možné nastavit identitu karty Java Card totožnou s uživatelským heslem Drivelock, což umožňuje ověření totožnosti pro DriveLock i kartu Java Card pouze pomocí karty Java Card při spuštění počítače.

   b. Je-li třeba, zadejte uživatelské heslo do polí **DriveLock password** (Heslo DriveLock) a **Confirm password** (Potvrdit heslo).

   c. Zadejte kód PIN karty Java Card.

   d. Klepněte na tlačítko **OK**.

7. Pokud jste vyzváni k vytvoření souboru obnovy, hledejte podrobnosti na „Vytvoření souboru pro obnovu“ nebo klepněte na tlačítko **Cancel** (Storno) a vytvořte soubor obnovy později.

Vytvoření uživatelské karty Java Card

Poznámka Pro vytvoření uživatelské karty Java Card musí být aktivováno ověřování po zapnutí a nastavena karta správce.

Vytvoření uživatelské karty Java Card

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karet Java Card) a poté klepněte na položku **Advanced** (Pokročilé).
3. Po zobrazení dialogového okna **Setup Password** zadejte své heslo pro nástroj Computer Setup a klepněte na tlačítko **OK**.
4. Vložte kartu Java Card, která bude používána jako uživatelská karta.
5. V pravém podokně v nabídce **Power-on authentication** (Ověřování po zapnutí) klepněte na položku **Create** (Vytvořit) vedle **User card identity** (Identita uživatelské karty).
6. Zadejte PIN kód pro uživatelskou kartu Java Card a klepněte na tlačítko OK.

Deaktivace ověřování karet Java Card po zapnutí

Pokud deaktivujete možnost ověřování karet Java Card po zapnutí, nebude již potřeba pro přístup k počítači používat kartu Java Card.

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karet Java Card) a poté klepněte na položku **Advanced** (Pokročilé).
3. Po zobrazení dialogového okna **Setup Password** zadejte své heslo pro nástroj Computer Setup a klepněte na tlačítko **OK**.
4. Vložte kartu Java Card, zadejte kód PIN a klepněte na tlačítko **OK**.
5. V pravém podokně v nabídce **Power-on authentication** (Ověřování po zapnutí) zrušte zaškrtnutí políčka **Enable** (Povolit).

Záloha a obnovení karet Java Card

Po přiřazení identity ověřování po zapnutí kartě Java Card doporučujeme vytvořit soubor obnovy karty Java Card. Soubor obnovy lze použít pro přenos dat identity pro ověřování po zapnutí z jedné karty Java Card na druhou. Tento soubor může být také použit pro vytvoření zálohy původní karty Java Card nebo k obnově dat v případě ztráty nebo krádeže karty Java Card.

UPOZORNĚNÍ Abychom se vyhnuli situacím, kdy se soubor obnovy neshoduje s aktualizovanými informacemi, jež obsahuje karta Java Card, je nutné okamžitě vytvořit nový soubor obnovy na výměnném médiu a uložit jej na bezpečné místo. Pokud vlastníte záložní kartu Java Card, je nutné aktualizovat rovněž informace uložené na záložní kartě Java Card opětovným přenesením nového souboru obnovy na záložní kartu Java Card.

Vytvoření souboru pro obnovu

Postup vytvoření souboru pro obnovu:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karet Java Card) a poté klepněte na položku **Advanced** (Pokročilé).
3. Po zobrazení dialogového okna **Setup Password** zadejte své heslo pro nástroj Computer Setup a klepněte na tlačítko **OK**.
4. V pravém podokně v části **Recovery** (Obnova) klepněte na tlačítko **Create** (Vytvořit).
5. Do pole **Filename** (Název souboru) zadejte jméno a cestu k souboru.

   UPOZORNĚNÍ Abyste se vyhnuli ztrátě přístupu k počítači, neukládejte soubor obnovy na pevný disk počítače; bez karty Java Card nebudete schopni získat k tomuto souboru přístup. Soubor obnovy uložený na pevném disku může být přístupný dalším osobám, což představuje určité bezpečnostní riziko.

6. Zadejte heslo souboru obnovy do pole **Recovery file password** (Heslo souboru obnovy) a poté ještě jednou do pole **Confirm password** (Potvrdit heslo).
7. Zadejte kód PIN karty Java Card a klepněte na tlačítko **OK**.

UPOZORNĚNÍ Chcete-li předejít ztrátě dat v souboru obnovy karty Java Card, zapamatujte si heslo souboru obnovy. Není možné znovu vytvořit kartu ze souboru obnovy, pokud zapomenete heslo.

Obnovení dat karty Java Card

Data karty Java Card můžete obnovit ze souboru obnovy. Tato možnost je zvláště užitečná, pokud byla karta ztracena nebo ukradena, nebo také pro vytvoření záložní karty Java Card. Při použití karty, na níž jsou uložena předchozí data, budou tato data přepsána.

Před zahájením akce potřebujete následující:

- Přístup k počítači, na němž je nainstalován software Java Card Security
- Soubor obnovy karty Java Card
- Heslo souboru obnovy karty Java Card
- Java Card

Obnovení karty Java Card:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Java Card Security** (Zabezpečení karet Java Card) a poté klepněte na položku **Advanced** (Pokročilé).
3. Po zobrazení dialogového okna **Setup Password** zadejte své heslo pro nástroj Computer Setup a klepněte na tlačítko **OK**.
4. Vložte disketu nebo jiné médium obsahující soubor obnovy karty Java Card.
5. Vložte kartu Java Card do čtečky. Pokud dosud nebyl kartě přiřazen kód PIN, budete vyzváni k jeho vytvoření. Podrobné informace o přiřazení kódu PIN kartě Java Card naleznete v části „Přiřazení kódu PIN kartě Java Card“ dříve v této kapitole.
6. V pravém podokně v nabídce Recovery (Obnovení) klepněte na položku **Restore** (Obnovit).
7. Ověřte, že je vybráno správné jméno souboru pro obnovu, a zadejte heslo k tomuto souboru.
8. Zadejte kód PIN karty Java Card.
9. Klepněte na tlačítko **OK**.

   Obsah původní karty Java Card je přenesen na novou kartu Java Card.

Vytvoření záložní karty Java Card

Důrazně doporučujeme vytvářet záložní kopie karet Java Card.

Vytvoření náhradní karty Java Card:

- ▲ Vložte kartu Java Card do čtečky a nahrajte na ni příslušný soubor obnovy. Další informace naleznete v části „Obnovení dat karty Java Card“ dříve v této kapitole.

4 Embedded Security pro HP ProtectTools

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

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

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

Integrovaný bezpečnostní čip TPM rozšiřuje a aktivuje ostatní funkce zabezpečení nástroje HP ProtectTools Security Manager. Například modul Credential Manager pro HP ProtectTools může využívat integrovaný čip k ověřování uživatelů při přihlášení do systému Windows. U vybraných modelů čip integrovaného zabezpečení TPM navíc aktivuje funkce rozšířeného zabezpečení systému BIOS, které se nastavují prostřednictvím modulu BIOS Configuration pro HP ProtectTools.

Nastavení

UPOZORNĚNÍ Aby se snížilo bezpečnostního riziko, doporučuje se, aby správce IT okamžitě inicializoval integrovaný bezpečnostní čip Pokud nebude inicializován integrovaný bezpečnostní čip, může dojít k tomu, že k počítači získá přístup neoprávněný uživatel nebo počítačový virus, který ovládne procesy vlastníka, mezi nimi například správu archívu pro nouzovou obnovu, nebo bude provádět změny přístupových práv uživatelů

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

Aktivace integrovaného bezpečnostního čipu

Integrovaný bezpečnostní čip musí být aktivován v nástroji Computer Setup. Tento postup nelze provést v modulu BIOS Configuration pro HP ProtectTools.

Aktivace integrovaného bezpečnostního čipu:

1. Spusťte nástroj Computer Setup zapnutím nebo restartováním počítače a následným stisknutím klávesy f10 v okamžiku, kdy je v dolním levém rohu obrazovky zobrazena zpráva „f10 = ROM Based Setup“ (f10 = konfigurační nástroj v paměti ROM).
2. Pokud nebylo nastaveno heslo správce, pomocí kláves se šipkami vyberte položky **Security** (Zabezpečení) **> Setup password** (Heslo správce) a stiskněte klávesu Enter.
3. Zadejte heslo do polí **New password** (Nové heslo) a **Verify new password** (Potvrdit nové heslo) a stiskněte klávesu F10.
4. V nabídce **Security** (Zabezpečení) pomocí kláves se šipkami vyberte položku **TPM Embedded Security** (Integrované zabezpečení TPM) a stiskněte klávesu Enter.
5. U položky **Embedded Security** (Integrované zabezpečení) v případě, že je zařízení skryté vyberte volbu **Available** (Dostupné).
6. Vyberte položku **Embedded security device state** (Stav integrovaného bezpečnostního zařízení) a změňte její hodnotu na **Enable** (Aktivní).
7. Stisknutím klávesy F10 přijmete změny v konfiguraci integrovaného zabezpečení.
8. Jestliže chcete uložit nastavení a ukončit nástroj Computer Setup, pomocí kláves se šipkami vyberte položku **File > Save Changes and Exit** (Soubor > Uložit změny a Konec).

Inicializace integrovaného bezpečnostního čipu

Během inicializace integrovaného zabezpečení je třeba:

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

Inicializace integrovaného bezpečnostního čipu:

1. Klepněte pravým tlačítkem na ikonu nástroje HP ProtectTools Security Manager v oznamovací oblasti v pravé části hlavního panelu a potom klepněte na položku **Embedded Security Initialization** (Inicializace integrovaného zabezpečení).

   Spustí se průvodce HP ProtectTools Embedded Security Initialization Wizard.

2. Klepněte na tlačítko **Další**.
3. Nastavte a potvrďte heslo vlastníka a klepněte na tlačítko **Next** (Další).

   Otevře se dialogové okno Setup Emergency Recovery (Nastavení nouzové obnovy).

4. Klepnutím na tlačítko **Next** (Další) potvrďte výchozí umístění archívu pro obnovu nebo klepněte na tlačítko **Browse** (Procházet), vyberte jiné umístění a potom klepněte na tlačítko **Next** (Další).
5. Nastavte a potvrďte heslo známky nouzové obnovy a klepněte na tlačítko **Next** (Další).
6. Klepněte na tlačítko **Browse** (Procházet), vyberte umístění archívu pro nouzovou obnovu a poté klepněte na tlačítko **Next** (Další).
7. Klepněte na tlačítko **Next** (Další) na obrazovce „Summary” (Přehled).

   - Pokud nechcete v tuto chvíli vytvořit základní uživatelský účet, zrušte označení zaškrtávacího políčka **Start the Embedded Security User Initialization Wizard** (Spustit průvodce inicializací uživatele integrovaného zabezpečení) a klepněte na tlačítko **Finish** (Dokončit). Průvodce můžete kdykoli spustit ručně a vytvořit základní uživatelský účet podle pokynů v následující části.
   - Pokud chcete vytvořit základní uživatelský účet, označte zaškrtávací políčko **Start the Embedded Security User Initialization Wizard** (Spustit průvodce inicializací uživatele integrovaného zabezpečení) a klepněte na tlačítko **Finish** (Dokončit). Spustí se průvodce Embedded Security User Initialization Wizard. Další informace naleznete v pokynech v následující části.

Vytvoření základního uživatelského účtu

Vytvoření základního uživatelského účtu v modulu integrovaného zabezpečení

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

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

Vytvoření základního uživatelského účtu a aktivace uživatelských bezpečnostních funkcí:

1. Pokud není spuštěn průvodce Embedded Security User Initialization Wizard vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager** (Správce zabezpečení HP ProtectTools).
2. V levém podokně klepněte na možnost **Embedded Security** (Integrované zabezpečení) a potom vyberte položku **User Settings** (Uživatelská nastavení).
3. V pravém podokně u položky **Embedded Security Features** (Funkce integrovaného zabezpečení) klepněte na volbu **Configure** (Konfigurovat).

   Spustí se průvodce Embedded Security User Initialization Wizard.
4. Klepněte na tlačítko **Další**.
5. Nastavte a potvrďte heslo základního uživatelského klíče a klepněte na tlačítko **Next** (Další).
6. Klepnutím na tlačítko **Next** (Další) potvrdíte nastavení.
7. Vyberte požadované funkce zabezpečení a klepněte na tlačítko **Next** (Další).
8. Klepněte znovu na tlačítko **Next** (Další).

Poznámka Chcete-li používat zabezpečenou elektronickou poštu, musíte nejprve nakonfigurovat klienta elektronické pošty, aby používal digitální certifikát vytvořený pomocí modulu Embedded Security. Pokud není digitální certifikát k dispozici, musíte jej získat od certifikační autority. Pokyny týkající se konfigurace elektronické pošty a získání digitálního certifikátu naleznete v elektronické nápovědě klienta elektronické pošty.

9. Pokud existuje více než jeden šifrovací certifikát, vyberte vyhovující certifikát a klepněte na tlačítko **Next** (Další).
10. Vyberte písmeno jednotky a popisku disku PSD a klepněte na tlačítko **Next** (Další).
11. Vyberte velikost a umístění disku PSD a klepněte na tlačítko **Next** (Další).
12. Klepněte na tlačítko **Next** (Další) na obrazovce „Summary” (Přehled).
13. Klepněte na tlačítko **Finish** (Dokončit).

Obecné úlohy

Jakmile vytvoříte základní uživatelský účet, můžete provádět následující operace:

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

Používání osobního zabezpečeného disku

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

Šifrování souborů a složek

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

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

Šifrování souborů a složek:

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

Odesílání a přijímání šifrované elektronické pošty

Integrované zabezpečení umožňuje odesílat a přijímat šifrovanou elektronickou poštu, postupy se však liší v závislosti na programu, který používáte pro přístup k elektronické poště. Další informace naleznete v elektronické nápovědě modulu Embedded Security a elektronické nápovědě klienta elektronické pošty.

Změna hesla základního uživatelského klíče

Změna hesla základního uživatelského klíče:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Embedded Security** (Integrované zabezpečení) a potom klepněte na položku **User Settings** (Uživatelská nastavení).
3. V pravém panelu u položky **Basic User Key password** (Heslo základního uživatelského klíče) klepněte na volbu **Change** (Změnit).
4. Zadejte staré heslo a potom nastavte a potvrďte nové heslo.
5. Klepněte na tlačítko **OK**.

Pokročilé operace

Zálohování a obnova

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

Vytvoření souboru zálohy

Vytvoření souboru zálohy:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Embedded Security** (Integrované zabezpečení) a poté klepněte na položku **Backup** (Zálohování).
3. V pravém podokně klepněte na tlačítko **Backup** (Zálohování).
4. Klepněte na tlačítko **Browse** (Procházet) a vyberte umístění, kde bude uložen soubor zálohy.
5. Určete, zda se k zálohovaným informacím má připojit archív pro nouzovou obnovu.
6. Klepněte na tlačítko **Další**.
7. Klepněte na tlačítko **Finish** (Dokončit).

Obnovení certifikačních údajů ze souboru zálohy

Obnovení dat se souboru zálohy:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Embedded Security** (Integrované zabezpečení) a potom klepněte na položku **Backup** (Zálohování).
3. V pravém podokně klepněte na tlačítko **Restore** (Obnovit).
4. Klepněte na tlačítko **Browse** (Procházet) a vyberte soubor zálohy v uloženém umístění.
5. Klepněte na tlačítko **Next** (Další).
6. Určete, zda se má spustit průvodce Embedded Security User Initialization Wizard.
   - Pokud se rozhodnete spustit průvodce inicializací, klepněte na tlačítko Finish (Dokončit) a podle pokynů na obrazovce dokončete inicializaci. Další informace naleznete v části „Vytvoření základního uživatelského účtu“ dříve v této kapitole.
   - Pokud se rozhodnete průvodce inicializací nespouštět, klepněte na tlačítko **Finish** (Dokončit).

Změna hesla vlastníka

Změna hesla vlastníka:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Embedded Security** (Integrované zabezpečení) a potom klepněte na položku **Advanced** (Pokročilé).
3. V pravém podokně klepněte u možnosti **Owner Password** (Heslo vlastníka) na položku **Change** (Změnit).
4. Zadejte staré heslo vlastníka a potom nastavte a potvrďte nové heslo vlastníka.
5. Klepněte na tlačítko **OK**.

Resetování hesla uživatele

Správce může pomoci uživateli resetováním zapomenutého hesla. Další informace naleznete v elektronické nápovědě.

Aktivace a deaktivace integrovaného zabezpečení

V případě, že nechcete používat bezpečnostní funkce je možné deaktivovat funkce integrovaného zabezpečení.

Funkce integrovaného zabezpečení lze aktivovat a deaktivovat na 2 různých úrovních:

- Temporary disabling (Dočasná deaktivace) — Při použití této volby se integrované zabezpečení automaticky znovu aktivuje při restartu systému Windows. Tato volba je standardně dostupná všem uživatelům.
- Permanent disabling (Trvalá deaktivace) — Při použití této volby je při opětovné aktivaci integrovaného zabezpečení vyžadováno heslo vlastníka. Tato volba je dostupná pouze správcům.

Trvalá deaktivace integrovaného zabezpečení

Trvalá deaktivace integrovaného zabezpečení:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Embedded Security** (Integrované zabezpečení) a potom klepněte na položku **Advanced** (Pokročilé).
3. V pravém podokně u položky **Embedded Security** (Integrované zabezpečení) klepněte na volbu **Disable** (Deaktivovat).
4. Zadejte heslo vlastníka do dialogu pro zadání hesla a klepněte na tlačítko **OK**.

Aktivace integrovaného zabezpečení po trvalé deaktivaci

Aktivace integrovaného zabezpečení po trvalé deaktivaci:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Embedded Security** (Integrované zabezpečení) a potom klepněte na položku **Advanced** (Pokročilé).

3. V pravém podokně u položky **Embedded Security** (Integrované zabezpečení) klepněte na volbu **Enable** (Aktivovat).

4. Zadejte heslo vlastníka do dialogu pro zadání hesla a klepněte na tlačítko **OK**.

Migrace klíčů pomocí průvodce Migration Wizard

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

Další informace naleznete v elektronické nápovědě modulu Embedded Security.

5 BIOS Configuration pro HP ProtectTools

Modul BIOS Configuration pro HP ProtectTools umožňuje přístup k bezpečnostním a konfiguračním nastavením systému BIOS (Computer Setup). Uživatelům systému Windows tak umožňuje přístup k funkcím zabezpečení sytému, které jsou spravovány modulem Computer Setup.

Modul BIOS Configuration nabízí tyto funkce:

- správa hesla při spuštění a hesla správce,
- konfigurace ostatních funkcí ověření po zapnutí, například aktivace hesel u karet Smart Card a integrované ověření,
- aktivace a deaktivace funkcí hardwaru, například zavádění z jednotky CD-ROM nebo různé porty hardwaru,
- konfigurace možností zavádění, včetně aktivace funkce MultiBoot a změny pořadí zavádění.

Poznámka Řada funkcí modulu BIOS Configuration pro HP ProtectTools je dostupná také v modulu Computer Setup.

Obecné úlohy

Modul BIOS Configuration umožňuje spravovat různá nastavení počítače, která by jinak byla přístupná pouze po stisknutí klávesy f10 při spuštění počítače a následném spuštění nástroje Computer Setup.

Správa možností zavádění

Pomocí modulu BIOS Configuration můžete spravovat různá nastavení úloh, které se spouštějí po spuštění nebo restartování počítače.

Správa možností zavádění:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS).
3. V dialogu systému pro zadání hesla správce systému BIOS zadejte heslo správce nástroje Computer Setup a klepněte na tlačítko **OK**.

   Poznámka Dialog pro zadání hesla správce systému BIOS se zobrazí pouze, pokud již bylo nastaveno heslo správce nástroje Computer Setup. Další informace o nastavení hesla správce nástroje Computer Setup naleznete dále v této kapitole v části „Nastavení hesla správce“.
4. V levém panelu klepněte na možnost **System Configuration** (Konfigurace systému).
5. V pravém panelu vyberte prodlevu (v sekundách) pro klávesy f9, f10 a f12 a pro **Express Boot Popup Delay (Sec)** (Délka zobrazení nabídky zavádění programu Express /sek./).
6. Aktivujte nebo deaktivujte nástroj **MultiBoot**.
7. Pokud jste aktivovali nástroj MultiBoot, vyberte pořadí zavádění tak, že zvolíte zařízení pro zavádění a následně upravíte jeho pořadí v seznamu pomocí kláves šipka nahoru a šipka dolů.
8. Klepnutím na tlačítko **Apply** (Použít) a potom na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Aktivace a deaktivace možností konfigurace systému

Poznámka Některé z níže uvedených položek nemusí váš počítač podporovat.

Aktivace nebo deaktivace zařízení nebo možností zabezpečení:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS).
3. V dialogu systému pro zadání hesla správce systému BIOS zadejte heslo správce nástroje Computer Setup a klepněte na tlačítko **OK**.
4. V levém panelu klepněte na možnost **System Configuration** (Konfigurace systému) a potom aktivujte nebo deaktivujte volbu konfigurace systému nebo nakonfigurujte volbu konfigurace systému v pravém panelu:
   - Port Options (Možnosti portů)
     - Serial Port (sériový port)
     - Infrared Port (infračervený port)
     - Parallel Port (paralelní port)
     - SD Slot (slot SD)
     - USB Port (port USB)
     - 1394 Port (port 1394)
     - Cardbus Slot (slot Cardbus)
     - ExpressCard slot (Zásuvka pro karty ExpressCard)
   - Boot options (Možnosti zavádění)
     - f9, f10, and f12 Delay (Sec) (Prodleva pro klávesy f9, f10 a f12 /v sekundách/)
     - MultiBoot
     - Express Boot Popup Delay (Sec) (Délka zobrazení nabídky zavádění programu Express /v sekundách/).
     - CD-ROM Boot (Zavedení z jednotky CD-ROM)
     - Floppy Boot (Zavedení z disketové jednotky)
     - Internal Network Adapter Boot (Zavedení z interního síťového adaptéru)
     - Internal Network Adapter Boot Mode (PXE or RPL) (Nastavení režimu zavádění ze síťového adaptéru /PXE nebo RPL/)
     - Boot Order (Pořadí zavádění)
   - Device Configuration (Konfigurace zařízení)
     - NumLock at Boot (Aktivace funkce NumLock při zavádění)
     - Swapping fn/Ctrl Keys (Prohození kláves fn a Ctrl)

- Multiple Pointing Devices (Více polohovacích zařízení)
- USB Legacy Support (podpora starších verzí rozhraní USB)
- Parallel port mode (standard, bidirectional, EPP, or ECP) (Režim paralelního portu / standardní, obousměrný, EPP nebo ECP/)
- Data Execution Prevention (Ochrana proti spuštění dat)
- SATA Native Mode (Nativní režim rozhraní SATA)
- Dual Core CPU (procesor se dvěma jádry)
- Automatic Intel® SpeedStep Functionality Support (Automatická podpora funkce Intel® SpeedStep)
- Fan Always on While on AC Power (Ventilátor je při napájení ze sítě vždy v provozu)
- BIOS DMA Data Transfers (Převody dat BIOS DMA)
- Intel or AMD PSAE Execution Disable (Deaktivace zákazu vykonávání kódu Intel nebo AMD PSAE)

- Built-In Device Options (Možnosti vestavěného zařízení)
  - Embedded WLAN Device Radio (Vestavěné rádiové zařízení WLAN)
  - Embedded WWAN Device Radio (Vestavěné rádiové zařízení WWAN)
  - Embedded Bluetooth® Device Radio (Vestavěné rádiové zařízení Bluetooth®)
  - LAN/WLAN Switching (přepínání mezi sítí LAN a WAN)
  - Wake on LAN from Off (Aktivace ze sítě LAN při vypnutí)

5. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje ProtectTools uložíte provedené změny a opustíte nabídku nástroje.

Pokročilé operace

Správa nastavení nástroje HP ProtectTools

Některé z funkcí nástroje HP ProtectTools Security Manager lze spravovat v modulu BIOS Configuration.

Aktivace a deaktivace podpory ověřování při spouštění pomocí čipových karet Smart Card nebo karet Java Card

Zapnutí této volby umožňuje používat karty smart card nebo Java Card k ověření uživatele při spuštění počítače.

Poznámka Chcete-li plně aktivovat funkci ověřování při spouštění, musíte zároveň provést konfiguraci nastavení čipových karet nebo karet Java Card pomocí modulu Smart Card Security pro HP ProtectTools nebo Java Card Security pro HP ProtectTools.

Povolení podpory ověřování při spuštění pomocí čipových karet:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS).
3. V dialogu systému pro zadání hesla správce systému BIOS zadejte heslo správce nástroje Computer Setup a klepněte na tlačítko **OK**.
4. V levém panelu klepněte na položku **Security** (Zabezpečení).
5. U volby **Smart Card Security** (Zabezpečení pomocí čipové karty) klepněte na možnost **Enable** (Aktivovat).

   Poznámka Chcete-li deaktivovat ověřování při spouštění pomocí čipových karet, klepněte na možnost **Disable** (Deaktivovat).

6. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Aktivace a deaktivace podpory ověřování při spuštění pomocí integrovaného zabezpečení

Zapnutí této volby umožňuje používat integrovaný bezpečnostní čip TPM (pokud je k dispozici) k ověření uživatele při spuštění počítače.

Poznámka Chcete-li plně aktivovat funkci ověřování při spouštění, musíte zároveň provést konfiguraci nastavení integrovaného bezpečnostního čipu TPM pomocí modulu Embedded Security pro HP ProtectTools.

Aktivace podpory ověřování při spuštění pomocí integrovaného zabezpečení:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS).
3. V dialogu systému pro zadání hesla správce systému BIOS zadejte heslo správce nástroje Computer Setup a klepněte na tlačítko **OK**.
4. V levém panelu klepněte na položku **Security** (Zabezpečení).
5. U volby **Embedded Security** (Integrované zabezpečení) klepněte na možnost **Enable Power-on Authentication Support** (Aktivovat podporu ověření při spouštění).

   

   Poznámka Chcete-li deaktivovat podporu ověřování při spouštění pomocí integrovaného zabezpečení, klepněte na možnost **Disable** (Deaktivovat).

6. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Aktivace a deaktivace automatické ochrany pevného disku DriveLock

Pokud bude tato volba aktivní, budou hesla zámku jednotek DriveLock automaticky generována a nastavena v jednotce pevného disku a budou chráněna integrovaným bezpečnostním čipem TPM.

Poznámka Automaticky generované hesla se nenastaví v jednotce pevného disku dokud se počítač nerestartuje a uživatel úspěšně nezadá heslo integrovaného zabezpečení TPM v dialogu pro zadání hesla.

Volba aktivace automatické aktivace zámku jednotek DriveLock je k dispozici pouze pokud:

- V počítači je nainstalovaný a inicializovaný bezpečnostní čip TPM. Pokyny týkající se aktivace a inicializace bezpečnostního čipu TPM naleznete v části „Aktivace integrovaného bezpečnostního čipu“ a „Inicializace integrovaného bezpečnostního čipu“ v Kapitole 4, „Embedded Security pro HP ProtectTools“.
- nebyla zatím aktivována žádná hesla zámku jednotek DriveLock.

Poznámka Pokud byly na počítači již ručně nastavena hesla zámku jednotek DriveLock, je třeba je nejprve deaktivovat a teprve potom, je možné aktivovat automatickou ochranu zámkem jednotek DriveLock.

Aktivace a deaktivace automatické ochrany zámkem jednotek DriveLock:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS).
3. V dialogu systému pro zadání hesla správce systému BIOS zadejte heslo správce nástroje Computer Setup a klepněte na tlačítko **OK**.
4. V levém panelu klepněte na položku **Security** (Zabezpečení).
5. U volby **Embedded Security** (Integrované zabezpečení) vyberte možnost **Enable** (Aktivovat) u položky **Automatic DriveLock Support** (Automatická podpora zámku jednotek DriveLock).

   Poznámka Chcete-li vypnout automatickou ochranu zámkem jednotek DriveLock, klepněte na možnost **Disable** (Deaktivovat).

6. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Správa hesel nástroje Computer Setup

Pomocí modulu BIOS Configuration můžete nastavovat a měnit hesla při spuštění a hesla správce nástroje Computer Setup a zároveň spravovat různá nastavení hesel.

UPOZORNĚNÍ Hesla, která nastavíte na obrazovce „Passwords” (Hesla) v modulu BIOS Configuration, se uloží okamžitě po klepnutí na tlačítko **Apply** (Použít) nebo na tlačítko **OK** v okně HP ProtectTools. Nastavené heslo si zapamatujte, protože změnu nastavení hesla nelze provést bez zadání předcházejícího hesla.

Heslo vyžadované při spuštění může chránit váš přenosný počítač před neoprávněným použitím.

Poznámka Poté, co nastavíte heslo vyžadované při spuštění, bude tlačítko Set (Nastavit) na obrazovce „Passwords” (Hesla) nahrazeno tlačítkem Change (Změnit).

Heslo pro nastavení nástroje Computer Setup omezuje přístup k nastavením a identifikačním informacím systému v nástroji Computer Setup. Po uložení bude heslo vyžadováno při přístupu k nástroji Computer Setup a při provádění změn pomocí nástroje Computer Setup. Pokud nastavíte heslo správce, budete požádáni o zadání tohoto hesla při přístupu na obrazovku BIOS Configuration nástroje HP ProtectTools.

Poznámka Poté, co nastavíte heslo správce, bude tlačítko Set (Nastavit) na obrazovce „Passwords” (Hesla) nahrazeno tlačítkem Change (Změnit).

Nastavení hesla vyžadovaného při spuštění

Nastavení hesla vyžadovaného při spuštění:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS) a potom klepněte na položku **Security** (Zabezpečení).
3. V pravém panelu u položky **Power-On Password** (Heslo při spuštění) klepněte na volbu **Set** (Nastavit).
4. Zadejte a potvrďte heslo v polích **Enter Password** (Zadání hesla) a **Verify Password** (Potvrzení hesla).
5. Klepněte na tlačítko **OK** v dialogovém okně Passwords (Hesla).
6. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Změna hesla vyžadovaného při spuštění

Změna hesla vyžadovaného při spuštění:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS) a potom klepněte na položku **Security** (Zabezpečení).
3. V pravém panelu u položky **Power-On Password** (Heslo při spuštění) klepněte na volbu **Change** (Změnit).
4. Do textového pole **Old password** (Staré heslo) zadejte aktuální heslo.
5. Zadejte a potvrďte nové heslo do pole **Enter New Password** (Zadejte nové heslo).
6. Klepněte na tlačítko **OK** v dialogovém okně **Passwords** (Hesla).
7. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Nastavení hesla správce

Nastavení hesla správce nástroje Computer Setup:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS) a potom klepněte na položku **Security** (Zabezpečení).
3. V pravém panelu u položky **Setup Password** (Heslo správce) klepněte na volbu **Set** (Nastavit).
4. Zadejte a potvrďte heslo v polích **Enter Password** (Zadání hesla) a **Confirm Password** (Potvrzení hesla).
5. Klepněte na tlačítko **OK** v dialogovém okně **Passwords** (Hesla).
6. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Změna hesla správce

Změna hesla správce nástroje Computer Setup:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS) a potom klepněte na položku **Security** (Zabezpečení).
3. V pravém panelu u položky **Setup Password** (Heslo správce) klepněte na volbu **Change** (Změnit).
4. Do textového pole **Old password** (Staré heslo) zadejte aktuální heslo.
5. Zadejte a potvrďte nové heslo v polích **Enter New Password** (Zadání nového hesla) a **Verify New Password** (Potvrzení nového hesla).
6. Klepněte na tlačítko **OK** v dialogovém okně **Passwords** (Hesla).
7. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Nastavení možností hesel

Pomocí modulu BIOS Configuration pro HP ProtectTools můžete nastavit možnosti hesel a zvýšit bezpečnost vašeho systému.

Aktivace a deaktivace silného zabezpečení

UPOZORNĚNÍ Aby nedošlo k tomu, že počítač bude trvale nepoužitelný, uložte heslo správce, heslo při spuštění nebo kód PIN čipové karty na bezpečném místě mimo počítač. Bez těchto hesel nebo kódu PIN nebude možné počítač používat.

Aktivace silného zabezpečení poskytuje rozšířenou ochranu hesel při spuštění a hesel správce a dalších způsobů ověření při spuštění.

Aktivace nebo deaktivace silného zabezpečení:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS) a potom klepněte na položku **Security** (Zabezpečení).
3. V pravém panelu u položky **Password Options** (Možnosti hesel) aktivujte nebo deaktivujte volbu **Stringent Security** (Silné zabezpečení).

Poznámka Chcete-li deaktivovat silné zabezpečení, zrušte zaškrtnutí u pole **Enable Stringent Security** (Aktivovat silné zabezpečení).

4. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

Aktivace a deaktivace ověřování při spuštění při restartování systému Windows

Tato volba umožňuje zvýšit bezpečnost tím, že bude po uživateli vyžadováno zadání hesla po zapnutí, hesla TPM nebo hesla karty Smart card po restartování systému Windows.

Aktivace nebo deaktivace ověřování při spuštění při restartování systému Windows:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **BIOS Configuration** (Konfigurace systému BIOS) a potom klepněte na položku **Security** (Zabezpečení).
3. V pravém panelu u položky **Password Options** (Možnosti hesel) aktivujte nebo deaktivujte volbu **Require password on restart** (Vyžadovat heslo po restartování).
4. Klepnutím na tlačítko **Apply** (Použít) a poté na **OK** v okně nástroje HP ProtectTools uložíte provedené změny.

6 Credential Manager pro HP ProtectTools

Modul Credential Manager pro HP ProtectTools poskytuje funkce zabezpečení, které chrání před neoprávněným přístupem k počítači. Mezi tyto funkce patří:

- alternativní možnosti k zadávání hesla při přihlašování k operačnímu systému Windows, například použití čtečky čipových karet nebo biometrické čtečky otisků prstů; další informace naleznete v části „Registrace přihlašovacích údajů“ dále v této kapitole,
- funkce jednotného přihlášení, která automaticky uchovává informace o přihlašovacích údajích pro webové stránky, aplikace a zabezpečené síťové zdroje,
- podpora volitelných bezpečnostních zařízení, například karet Smart Card nebo biometrických čteček otisků prstů.
- podpora dalších bezpečnostních nastavení, jako je vyžadování ověření za pomoci volitelného zabezpečovacího zařízení k odemknutí počítače.

Nastavení

Přihlášení k modulu Credential Manger

V závislosti na konfiguraci se můžete přihlásit k modulu Credential Manager pomocí kteréhokoli z následujících způsobů:

- pomocí nástroje Credential Manager Logon Wizard (doporučeno),
- pomocí ikony nástroje HP ProtectTools Security Manager v oznamovací oblasti,
- pomocí nástroje HP ProtectTools Security Manager.

Poznámka Pokud pro přihlášení k modulu Credential Manager použijete přihlašovací okno modulu Credential Manager na přihlašovací obrazovce systému Windows, přihlásíte se současně i do systému Windows.

Při prvním spuštění modulu Credential Manager se přihlaste pomocí svého obvyklého přihlašovacího hesla pro systém Windows. Následně se automaticky vytvoří účet modulu Credential Manager, který bude obsahovat přihlašovací údaje pro přihlášení do systému Windows.

Po přihlášení k modulu Credential Manager můžete zaregistrovat další přihlašovací údaje, jako je například otisk prstu nebo čipová karta Smart card. Další informace naleznete v části „Registrace přihlašovacích údajů“ dále v této kapitole.

Při dalším přihlášení můžete nastavit zásady přihlašování a použít jakoukoliv kombinaci zaregistrovaných přihlašovacích údajů.

Používání nástroje Credential Manager Logon Wizard

Chcete-li se k modulu Credential Manger přihlásit pomocí nástroje Credential Manager Logon Wizard, postupujte následujícím způsobem:

1. Spusťte nástroj Credential Manager Logon Wizard jedním z následujících způsobů:
   - z přihlašovací obrazovky systému Windows,
   - poklepáním na ikonu nástroje **HP ProtectTools Security Manager** v oznamovací oblasti.
   - ze stránky „Credential Manager” nástroje Protect Tools Security Manager klepnutím na odkaz **Log On** (Přihlášení) v pravé horní části okna.
2. Klepněte na tlačítko **Další**.
3. Do textového pole **User Name** (Uživatelské jméno) zadejte uživatelské jméno.
4. Do textového pole **Password** (Heslo) zadejte heslo a klepněte na tlačítko **Next** (Další).
5. Klepněte na tlačítko **Finish** (Dokončit).

První přihlášení

Před jeho vytvořením musíte být přihlášeni do systému Windows pomocí účtu správce, ale nesmíte být zároveň přihlášeni k modulu Credential Manager.

1. Otevřete nástroj HP ProtectTools Security Manager poklepáním na ikonu HP ProtectTools Security Manager v oznamovací oblasti. Otevře se okno nástroje HP ProtectTools Security Manager.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Log On** (Přihlásit) v pravém horním rohu pravého podokna. Spustí se nástroj Credential Manager Logon Wizard.
3. Do textového pole **Password** (Heslo) zadejte své heslo pro přístup k systému Windows a klepněte na tlačítko **Next** (Další).

Registrace přihlašovacích údajů

Pomocí stránky „My Identity“ (Identita) můžete zaregistrovat různé způsoby ověření nebo přihlašovací údaje. Poté, co budou zaregistrovány, je lze použít pro přihlášení k nástroji Credential Manager.

Registrace otisků prstů

Čtečka otisků prstů umožňuje přihlášení do systému Windows prostřednictvím otisku prstu namísto použití hesla systému Windows.

Nastavení čtečky otisků prstů

1. Po přihlášení k nástroji Credential Manager přejeďte prstem přes čidlo čtečky otisku prstů. Otevře se okno nástroje Credential Manager Registration Wizard.
2. Klepněte na tlačítko **Další**.

   Poznámka Standardně modul Credential Manager vyžaduje registraci *alespoň* 2 různých prstů.

   Výchozím prstem je pravý ukazovák (jeho otisk by měl být sejmut jako první). Výchozí prst můžete změnit klepnutím na prst, který chcete zaregistrovat jako první, buď na levé, nebo na pravé ruce. Jakmile klepnete na prst, bude jeho výběr zvýrazněn obrysem.

3. Pomalu přejeďte prstem shora dolů přes čidlo čtečky. Postupujte podle pokynů v průvodci a opakovaně přejíždějte stejným prstem přes snímač, dokud prst na obrazovce nezezelená.

   Poznámka K registraci otisku je nutné přejet přes čidlo vícekrát.

   Pokud budete potřebovat přerušit snímání a začít znovu, klepněte pravým tlačítkem myši na zvýrazněný prst na obrazovce a poté klepněte na položku **Clear** (Vymazat) nebo **Clear All** (Vymazat vše).

4. Postupujte podle pokynů v průvodci a zaregistrujte podle nich druhý prst.

   Poznámka Pokud klepnete na položku **Finish** (Dokončit) dříve, než zaregistrujete alespoň dva prsty, zobrazí se chybové hlášení. Pokračujte klepnutím na tlačítko **OK**.

5. Jestliže jste úspěšně zaregistrovali alespoň dva prsty, klepněte na tlačítko **Next** (Další).
6. Chcete-li se přihlásit k systému Windows sejmutím otisku prstu, ujistěte se, že je vybráno zaškrtávací políčko **Yes, I want to use Credential Manager to logon to Windows** (Ano, chci použít nástroj Credential Manager pro přihlášení k systému Windows). Klepněte na tlačítko **Finish** (Dokončit).
7. Pokud chcete zaregistrovat otisky prstů jiného uživatele systému Windows, přihlaste se do systému Windows prostřednictvím účtu daného uživatele a zopakujte kroky 1 až 6.

Přihlášení k systému Windows pomocí zaregistrovaného otisku prstu

1. Ihned po zaregistrování otisků prstů restartujte systém Windows.
2. Při zobrazení úvodní obrazovky systému Windows sejměte otisk kteréhokoli ze svých zaregistrovaných prstů k přihlášení k systému Windows.

Registrace karty Java Card, čipové karty, známky nebo virtuální známky.

Poznámka Pro tento postup musíte mít nainstalovánu čtečku čipových karet. Nemáte-li čtečku nainstalovánu, můžete zaregistrovat virtuální známku podle pokynů v části „Vytvoření virtuální známky“.

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.

3. V pravém panelu klepněte na možnost **Register Smart Card or Token** (Registrovat čipovou kartu nebo známku). Otevře se okno nástroje Credential Manager Registration Wizard.
4. Klepněte na tlačítko **Další**.
5. Vyberte způsob ověření, který chcete zaregistrovat, a klepněte na tlačítko **Next** (Další).
6. Postupujte podle pokynů na obrazovce a dokončete registraci.

Registrace známky USB eToken

1. Ujistěte se, že jsou nainstalovány ovladače USB eToken.

   

   Poznámka Více informací naleznete v uživatelské příručce USB eToken.

2. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
3. V levém podokně klepněte na možnost **Credential Manager**.
4. V pravém panelu klepněte na možnost **Register Smart Card or Token** (Registrovat čipovou kartu nebo známku). Otevře se okno nástroje Credential Manager Registration Wizard.
5. Klepněte na tlačítko **Další**.
6. U volby **Device Type** (Typ zařízení) klepněte na položku **USB eToken** a poté klepněte na tlačítko **Next** (Další).
7. Postupujte podle pokynů na obrazovce a dokončete registraci.

Registrace dalších přihlašovacích údajů

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.
3. V pravém panelu klepněte na možnost **Register Credentials** (Registrovat přihlašovací údaje). Otevře se okno nástroje Credential Manager Registration Wizard.
4. Klepněte na tlačítko **Další**.
5. Vyberte způsob ověření, který chcete zaregistrovat, a klepněte na tlačítko **Next** (Další).
6. Postupujte podle pokynů na obrazovce a dokončete registraci.

Obecné úlohy

Všichni uživatelé mají přístup ke stránce „My Identity“ (Identita) nástroje Credential Manager. Prostřednictvím stránky „My Identity“ (Identita) můžete provádět následující úlohy:

- Vytvoření virtuální známky
- Změna hesla pro přihlášení do systému Windows
- Správa kódu PIN známky
- Správa identity
- Uzamčení počítače

Poznámka Tato možnost je dostupná pouze tehdy, je-li aktivováno klasické přihlašovací okno nástroje Credential Manager. Viz „Příklad 1 — Použití stránky „Advanced Settings” (Pokročilá nastavení) k umožnění přihlášení k systému Windows z nástroje Credential Manager“.

Vytvoření virtuální známky

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

Vytvoření nové virtuální známky:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.
3. V pravém panelu klepněte na možnost **Virtual Token** (Virtuální známka). Otevře se okno nástroje Credential Manager Registration Wizard.

   Poznámka Není-li možnost Virtual Token (Virtuální známka) k dispozici, použijte postup pro „Registrace dalších přihlašovacích údajů“.

4. Klepněte na tlačítko **Další**.
5. Klepněte na položku **Virtual Token** (Virtuální token) a potom na tlačítko **Next** (Další).
6. Zadejte název a umístění souboru virtuálního tokenu (nebo klepněte na tlačítko **Browse** (Procházet) a vyhledejte umístění souboru) a potom klepněte na tlačítko **Next** (Další).
7. Zadejte a potvrďte hlavní kód PIN a uživatelský kód PIN.
8. Klepněte na tlačítko **Finish** (Dokončit).

Změna hesla pro přihlášení do systému Windows

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.

3. V pravém panelu klepněte na položku **Change Windows Password** (Změnit heslo pro přihlášení k systému Windows).
4. Do textového pole **Old Password** (Staré heslo) zadejte staré heslo.
5. Zadejte nové heslo v polích **New Password** (Nové heslo) a **Confirm Password** (Potvrzení hesla).
6. Klepněte na tlačítko **Finish** (Dokončit).

Změna kódu PIN tokenu

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.
3. V pravém podokně klepněte na položku **Change Token PIN** (Změnit PIN známky).
4. Vyberte známku, u které chcete změnit kód PIN, a klepněte na tlačítko **Next** (Další).
5. Postupujte podle pokynů na obrazovce a dokončete změnu kódu PIN.

Správa identity

Zálohování identity

Doporučuje se zálohovat identitu v nástroji Credential Manager pro případ, že by došlo ke ztrátě dat nebo k jejich neúmyslnému odstranění.

Zálohování identity:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.
3. V pravém podokně klepněte na tlačítko **Backup Identity** (Zálohovat identitu).
4. Vyberte prvky, které chcete zálohovat, a klepněte na tlačítko **Next** (Další).
5. Na stránce „Device Type“ (Typ zařízení) vyberte typ zařízení, které chcete použít k vytvoření zálohy, a klepněte na tlačítko **Next** (Další).

Poznámka Musíte znát heslo nebo kód PIN zařízení, které jste vybrali pro vytvoření souboru zálohy.

6. Postupujte podle pokynů na obrazovce a poté klepněte na tlačítko **Finish** (Dokončit).

Obnovení identity

Obnovení identity:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.
3. V pravém podokně klepněte na tlačítko **Restore Identity** (Obnovit identitu).
4. Na stránce „Device Type“ (Typ zařízení) vyberte typ zařízení, na kterém je uložena záloha, a poté klepněte na tlačítko **Next** (Další).

   

   Poznámka Musíte znát heslo nebo kód PIN zařízení, které jste vybrali pro vytvoření souboru zálohy.

5. Postupujte podle pokynů na obrazovce a poté klepněte na tlačítko **Finish** (Dokončit).
6. Klepněte na tlačítko **Yes** (Ano) v dialogovém okně pro potvrzení.

Vymazání identity ze systému

Poznámka Tato skutečnost neovlivní účet uživatele systému Windows.

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.
3. V pravém podokně klepněte na možnost **Clear Identity for this Account** (Vymazat identitu pro tento účet).
4. Klepněte na tlačítko **Yes** (Ano) v dialogovém okně pro potvrzení. Vaše identita bude odhlášena a odstraněna ze systému.

Uzamčení počítače

Tato funkce je dostupná, jestliže se přihlašujete k systému Windows pomocí nástroje Credential Manager. K uzamčení počítače ve chvíli, kdy jej nepoužíváte, můžete použít funkci Lock Workstation. Tím zabráníte přístupu neoprávněných osob k počítači. Pouze vy a členové skupiny správců mohou počítač odemknout.

Poznámka Tato možnost je dostupná pouze tehdy, je-li aktivováno klasické přihlašovací okno nástroje Credential Manager. Viz „Příklad 1 — Použití stránky „Advanced Settings" (Pokročilá nastavení) k umožnění přihlášení k systému Windows z nástroje Credential Manager".

Pro zvýšení bezpečnosti lze nakonfigurovat funkci Lock Workstation, aby k odemčení počítače vyžadovala použití čipové karty, čtečky otisků prstů nebo známky. Další informace naleznete v části „Konfigurace nastavení nástroje Credential Manager" dále v této kapitole.

Uzamčení počítače:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager**.
3. V pravém podokně klepněte na možnost **Lock Workstation** (Uzamknout pracovní stanici). Zobrazí se přihlašovací obrazovka systému Windows. K odemčení počítače musíte použít heslo systému Windows nebo nástroje Credential Manager Logon Wizard.

Použití přihlášení k systému Windows

K přihlášení do systému Windows můžete použít nástroj Credential Manager na místním počítači nebo v rámci síťové domény. Při prvním přihlášení do nástroje Credential Manager systém automaticky přidá místní uživatelský účet systému Windows mezi síťové účty určené pro použití se službou Network Logon (Přihlášení k síti).

Přihlášení do systému Windows pomocí nástroje Credential Manager

Nástroj Credential Manager lze použít pro přihlášení k síti systému Windows nebo k místnímu účtu.

1. Pokud jste zaregistrovali svůj otisk prstu pro přihlašování k systému Windows, sejměte jej, abyste se mohli přihlásit.
2. Pokud jste nezaregistrovali svůj otisk prstu pro přihlašování k systému Windows, klepněte na ikonu klávesnice v levém horním rohu obrazovky vedle ikony otisku prstu. Spustí se nástroj Credential Manager Logon Wizard.
3. Klepněte na šipku vedle pole **User name** (Uživatelské jméno) a zadejte své jméno.
4. Do textového pole **Password** (Heslo) zadejte heslo a klepněte na tlačítko **Next** (Další).

5. Vyberte položku **More > Wizard Options** (Více > Možnosti průvodce).

   a. Chcete-li, aby bylo toto uživatelské jméno výchozí při vašem příštím přihlášení k počítači, vyberte zaškrtávací políčko **Use last user name on next logon** (Použít poslední uživatelské jméno při příštím přihlášení).

   b. Chcete-li tyto zásady přihlašování nastavit jako výchozí způsob, vyberte zaškrtávací políčko **Use last policy on next logon** (Použít poslední zásady při příštím přihlášení).

6. Postupujte podle pokynů na obrazovce. Pokud ověření proběhne úspěšně, dojde k přihlášení k účtu systému Windows a k nástroji Credential Manager.

Přidání účtu

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepněte na možnost **Windows Logon** (Přihlášení k systému Windows) a poté klepněte na položku **Add a Network Account** (Přidat nový síťový účet). Spustí se nástroj Add Network Account Wizard.
4. Zapište uživatelské jméno do pole **User name** (Uživatelské jméno) nebo vyhledejte uživatelské jméno klepnutím na tlačítko **Browse** (Prohledat).
5. Vyberte doménu ze seznamu dostupných domén.
6. Zadejte a potvrďte heslo.

Poznámka Chcete-li, aby nástroj Credential Manager tento účet ověřoval, ujistěte se, že je vybráno zaškrtávací políčko **Validate network account when Next or Finish button clicked** (Ověřovat síťový účet při stisknutí tlačítka Další nebo Dokončit).

7. Klepněte na tlačítko **Finish** (Dokončit).

Odstranění účtu

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepněte na možnost **Windows Logon** (Přihlášení k systému Windows) a poté klepněte na položku **Manage Network Accounts** (Správa síťových účtů). Otevře se dialogové okno **Manage Network Accounts** (Správa síťových účtů).
4. Klepněte na účet, který chcete odstranit a poté klepněte na tlačítko **Remove** (Odstranit).
5. V dialogovém okně pro potvrzení klepněte na tlačítko **Yes** (Ano).
6. Klepněte na tlačítko **OK**.

Používání jednotného přihlášení

Nástroj Credential Manager obsahuje funkci Single Sign On (Jednotné přihlášení), která uchovává jména uživatelů a hesla pro různé aplikace sítě Internet i systému Windows a automaticky zadává přihlašovací údaje při přístupu k registrovanému programu.

Poznámka Zabezpečení a ochrana soukromí jsou klíčovými faktory použití funkce jednotného přihlášení. Všechny přihlašovací údaje jsou šifrovány a jsou dostupné pouze po úspěšném přihlášení k nástroji Credential Manager.

Poznámka Současně můžete funkci Single Sign On nakonfigurovat, aby před přihlášením k zabezpečeným stránkám nebo programu prováděla ověřování přihlašovacích údajů pomocí čipové karty, čtečky otisků prstů nebo známky. Tato funkce je zvláště užitečná ve chvíli, kdy se přihlašujete k programu nebo k webovým stránkám, které obsahují osobní informace, jako jsou čísla bankovních účtů. Další informace naleznete v části „Konfigurace nastavení nástroje Credential Manager“ dále v této kapitole.

Registrace nové aplikace

Nástroj Credential Manager zobrazí výzvu pro registraci aplikace při spuštění aplikace ve chvíli, kdy jste přihlášeni k nástroji Credential Manager. Aplikaci lze zaregistrovat také ručně.

Používání automatické registrace

1. Spusťte aplikaci, která vyžaduje přihlášení.
2. Klepněte na ikonu Credential Manager SSO v dialogovém okně s heslem pro otevření programu nebo webových stránek.
3. Zadejte své heslo pro přístup k programu nebo webovým stránkám a klepněte na tlačítko **OK**. Zobrazí se dialogové okno Credential Manager Single Sign On (Jednotné přihlášení nástroje Credential Manager).
4. Klepněte na tlačítko **More** (Více) a vyberte některou z následujících možností:
   - Do not use SSO for this site or application. (Nepoužívat SSO pro tuto stránku nebo aplikaci.)
   - Prompt to select account for this application. (Zobrazovat výzvu k vybrání účtu pro tuto aplikaci.)
   - Fill in credentials but do not submit. (Vyplnit přihlašovací údaje, ale neodesílat.)
   - Authenticate user before submitting credentials. (Ověřovat uživatele před odesláním přihlašovacích údajů.)
   - Show SSO shortcut for this application. (Zobrazit zástupce SSO pro tuto aplikaci.)
5. Klepnutím na tlačítko **Yes** (Ano) potvrďte registraci.

Používání ruční registrace (pomocí přetažení)

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepněte na možnost **Single Sign On** (Jednotné přihlášení) a poté klepněte na položku **Register New Application** (Zaregistrovat novou aplikaci). Spustí se nástroj SSO Application Wizard.
4. Spusťte aplikaci, kterou chcete zaregistrovat, a počkejte, dokud se neobjeví obrazovka pro zadání hesla.

5. Na obrazovce „Drag and Drop Registration” (Registrace pomocí přetažení) průvodce SSO Registration Wizard vyberte druh činnosti, kterou chcete zautomatizovat.

Poznámka Ve většině případů budete chtít zautomatizovat **Logon simple dialog** (Jednoduchý přihlašovací dialog).

6. Přetáhněte ikonu ze stránky průvodce do místa v aplikaci, kde se nachází pole pro zadání hesla. Jakmile se oblast označí, uvolněte tlačítko ukazovacího zařízení.
7. Na stránce „Application Information” (Informace o aplikaci) průvodce SSO Registration Wizard zadejte název a popis aplikace.
8. Klepněte na tlačítko **Finish** (Dokončit).
9. Zadejte údaje pro přihlášení, například uživatelské jméno a heslo, do pole pro zadání přihlašovacích údajů aplikace.
10. V dialogovém okně Credential Manager Single Sign On (Jednotné přihlášení nástroje Credential Manager) buď potvrďte název pověření, nebo na něj klepněte pravým tlačítkem a upravte jej. Klepněte na tlačítko **Yes** (Ano).
11. Klepněte na tlačítko **More** (Více) a vyberte některou z následujících možností:
    - Do not use SSO for this site or application. (Nepoužívat SSO pro tuto stránku nebo aplikaci.)
    - Prompt to select account for this application. (Zobrazovat výzvu k vybrání účtu pro tuto aplikaci.)
    - Fill in credentials but do not submit. (Vyplnit přihlašovací údaje, ale neodesílat.)
    - Authenticate user before submitting credentials. (Ověřovat uživatele před odesláním přihlašovacích údajů.)
    - Show SSO shortcut for this application. (Zobrazit zástupce SSO pro tuto aplikaci.)
12. Klepnutím na tlačítko **Yes** (Ano) potvrďte registraci.

Správa aplikací a přihlašovacích údajů

Úprava vlastností aplikace

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně u položky **Single Sign On** (Jednotné přihlášení) klepněte na volbu **Manage Applications and Credentials** (Správa aplikací a přihlašovacích údajů).
4. Vyberte aplikaci, kterou chcete upravit, a klepněte na tlačítko **Properties** (Vlastnosti).
5. Chcete-li změnit název a popis aplikace, klepněte na kartu **General** (Obecné). Nastavení změníte zaškrtnutím nebo zrušením zaškrtnutí políček u souvisejících nastavení.
6. Chcete-li zobrazit a upravit skript jednotného přihlášení aplikace, klepněte na kartu **Script** (Skript).
7. Klepnutím na tlačítko **OK** uložíte provedené změny.

Odstranění aplikací z jednotného přihlášení

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně u položky **Single Sign On** (Jednotné přihlášení) klepněte na volbu **Manage Applications and Credentials** (Správa aplikací a přihlašovacích údajů).
4. Vyberte aplikaci, kterou chcete odstranit, a klepněte na tlačítko **Remove** (Odstranit).
5. Klepněte na tlačítko **Yes** (Ano) v dialogovém okně pro potvrzení.
6. Klepněte na tlačítko **OK**.

Exportování aplikace

Aplikace je možné exportovat za účelem vytvoření záložní kopie skriptu jednotného přihlášení aplikace. Tento soubor lze použít pro obnovení dat jednotného přihlášení. Jedná se o doplňkovou aktivitu k zálohování souboru identity, který obsahuje pouze informace o přihlašovacích údajích.

Exportování aplikace:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně u položky **Single Sign On** (Jednotné přihlášení) klepněte na volbu **Manage Applications and Credentials** (Správa aplikací a přihlašovacích údajů).
4. Klepněte na aplikaci, kterou chcete exportovat. Poté klepněte na položky **More > Applications > Export Script** (Více – Aplikace – Skript exportu).
5. Postupujte podle pokynů na obrazovce a dokončete export.
6. Klepněte na tlačítko **OK**.

Importování aplikace

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně u položky **Single Sign On** (Jednotné přihlášení) klepněte na volbu **Manage Applications and Credentials** (Správa aplikací a přihlašovacích údajů).
4. Klepněte na aplikaci, kterou chcete importovat. Poté vyberte položky **More > Applications > Import Script** (Více – Aplikace – Skript importu).
5. Postupujte podle pokynů na obrazovce a dokončete import.
6. Klepněte na tlačítko **OK**.

Úprava přihlašovacích údajů

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně u položky **Single Sign On** (Jednotné přihlášení) klepněte na volbu **Manage Applications and Credentials** (Správa aplikací a přihlašovacích údajů).
4. Vyberte aplikaci, kterou chcete upravit, a klepněte na tlačítko **More** (Více).
5. Vyberte některou z následujících možností:
   - Aplikace
     - Přidat novou
     - Odebrat
     - Vlastnosti
     - Skript importu
     - Skript exportu
   - Pověření
     - Vytvořit nové
   - Zobrazit heslo

     Poznámka Před zobrazením hesla musíte provést ověření své identity.
6. Postupujte podle pokynů na obrazovce.
7. Klepnutím na tlačítko **OK** uložíte změny.

Použití ochrany aplikací

Tato funkce umožňuje provádět konfiguraci přístupu k aplikacím. Přístup můžete omezit na základě následujících kritérií:

- Kategorie uživatele
- Doba používání
- Nečinnost uživatele

Omezení přístupu k aplikaci

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepněte v části **Application Protection** (Ochrana aplikace) na položku **Manage Protected Applications** (Správa chráněných aplikací). Zobrazí se dialogové okno Application Protection Service (Služba ochrany aplikací).

4. Vyberte kategorii uživatelů, jejichž přístup chcete spravovat.

Poznámka Nejedná-li se o kategorii Everyone (Všichni), může být nutné vybrat možnost **Override default settings** (Potlačit výchozí nastavení) k potlačení nastavení pro kategorii Everyone.

5. Klepněte na tlačítko **Add** (Přidat). Spustí se nástroj Add a Program Wizard.
6. Klepněte na aplikaci, kterou chcete chránit, a poté klepněte na tlačítko **OK**. Zobrazí se dialogové okno Properties (Vlastnosti) pro vybranou aplikaci.
7. Klepněte na kartu **General** (Obecné). Vyberte jedno z následujících nastavení:
   - Zakázáno (Nelze použít)
   - Povoleno (Lze použít bez omezení)
   - Omezeno (Použití závisí na nastavení)
8. Vyberete-li omezené použití, budou k dispozici následující nastavení:
   a. Chcete-li použití omezit na základě času, dne nebo data, klepněte na kartu **Schedule** (Časový plán) a proveďte konfiguraci nastavení.
   b. Chcete-li použití omezit na základě nečinnosti, klepněte na kartu **Advanced** (Rozšířená nastavení) a vyberte dobu nečinnosti.
9. Klepnutím na tlačítko **OK** zavřete dialogové okno pro úpravu vlastností aplikace.
10. Klepněte na tlačítko **OK**.

Odstranění ochrany aplikace

Odstranění omezení nastavených pro aplikaci:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepněte v části **Application Protection** (Ochrana aplikace) na položku **Manage Protected Applications** (Správa chráněných aplikací). Zobrazí se dialogové okno Application Protection Service (Služba ochrany aplikací).
4. Vyberte kategorii uživatelů, jejichž přístup chcete spravovat.

Poznámka Nejedná-li se o kategorii Everyone (Všichni), může být nutné vybrat možnost **Override default settings** (Potlačit výchozí nastavení) k potlačení nastavení pro kategorii Everyone.

5. Vyberte aplikaci, kterou chcete odstranit, a klepněte na tlačítko **Remove** (Odstranit).
6. Klepněte na tlačítko **OK**.

Změna nastavení omezení pro chráněnou aplikaci

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepněte v části **Application Protection** (Ochrana aplikace) na položku **Manage Protected Applications** (Správa chráněných aplikací). Zobrazí se dialogové okno Application Protection Service (Služba ochrany aplikací).
4. Vyberte kategorii uživatelů, jejichž přístup chcete spravovat.

   

   Poznámka Nejedná-li se o kategorii Everyone (Všichni), může být nutné vybrat možnost **Override default settings** (Potlačit výchozí nastavení) k potlačení nastavení pro kategorii Everyone.

5. Klepněte na aplikaci, kterou chcete změnit, a poté klepněte na tlačítko **Properties** (Vlastnosti). Zobrazí se dialogové okno Properties (Vlastnosti) pro vybranou aplikaci.
6. Klepněte na kartu **General** (Obecné). Vyberte jedno z následujících nastavení:
   - Zakázáno (Nelze použít)
   - Povoleno (Lze použít bez omezení)
   - Omezeno (Použití závisí na nastavení)
7. Vyberete-li omezené použití, budou k dispozici následující nastavení:
   a. Chcete-li použití omezit na základě času, dne nebo data, klepněte na kartu **Schedule** (Časový plán) a proveďte konfiguraci nastavení.
   b. Chcete-li použití omezit na základě nečinnosti, klepněte na kartu **Advanced** (Rozšířená nastavení) a vyberte dobu nečinnosti.
8. Klepnutím na tlačítko **OK** zavřete dialogové okno pro úpravu vlastností aplikace.
9. Klepněte na tlačítko **OK**.

Pokročilé operace (určeno pouze pro správce)

Stránka „Authentication and Credentials” (Ověřování a přihlašovací údaje) a stránka „Advanced Settings” (Pokročilá nastavení) nástroje Credential Manager jsou dostupné pouze pro uživatele s oprávněním správce. Prostřednictvím těchto stránek můžete provádět následující úlohy:

- Určení způsobu přihlašování uživatelů a správců
- Konfigurace vlastních požadavků na ověřování
- Konfigurace vlastností pověření
- Konfigurace nastavení nástroje Credential Manager

Určení způsobu přihlašování uživatelů a správců

Na stránce „Authentication and Credentials” (Ověřování a přihlašovací údaje) můžete určit, který druh nebo kombinace přihlašovacích údajů budou vyžadovány při přihlašování uživatelů nebo správců.

Určení způsobu přihlašování uživatelů a správců:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepnìte na kartu **Authentication** (Ověřování).
4. Vyberte kategorii - **Users** (Uživatelé) nebo **Administrators** (Správci) - ze seznamu kategorií.
5. Vyberte způsob nebo kombinaci způsobů ověření ze seznamu.
6. Klepnutím na tlačítko **Apply** (Použít) a potom na **OK** uložíte provedené změny.

Konfigurace vlastních požadavků na ověřování

Pokud skupina ověřovacích přihlašovacích údajů, které vyžadujete, není uvedena na kartě Authentication (Ověřování) stránky „Authentication and Credentials“ (Ověřování a přihlašovací údaje), můžete vytvořit vlastní požadavky.

Konfigurace vlastních požadavků:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepněte na kartu **Authentication** (Ověřování).
4. Vyberte kategorii - **Users** (Uživatelé) nebo **Administrators** (Správci) - ze seznamu kategorií.
5. Vyberte položku **Custom** (Vlastní) v seznamu způsobů ověření.
6. Klepněte na tlačítko **Configure** (Konfigurovat).
7. Vyberte způsoby ověření, které chcete používat.
8. Vyberte kombinaci způsobů ověření označením jedné z následujících voleb:
   - Use logický součin ke kombinování způsobů ověřování

     (Uživatelé se budou muset prokázat pomocí všech způsobů ověření při každém přihlášení.)
   - Použijte logický součet k vytvoření požadavku na jeden ze dvou nebo několika způsobů ověřování.

     (Uživatelé si budou moci zvolit jakýkoliv z vybraných způsobů ověření při každém přihlášení.)
9. Klepněte na tlačítko **OK**.
10. Klepnutím na tlačítko **Apply** (Použít) a potom na **OK** uložíte provedené změny.

Konfigurace vlastností přihlašovacích údajů

Na kartě Credentials (Přihlašovací údaje) stránky „Authentication and Credentials” (Ověřování a přihlašovací údaje) můžete zobrazit seznam dostupných způsobů ověřování a upravovat jejich nastavení.

Konfigurace přihlašovacích údajů:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Authentication and Credentials** (Ověřování a přihlašovací údaje).
3. V pravém podokně klepněte na kartu **Credentials** (Přihlašovací údaje).

4. Klepněte na přihlašovací údaje, které chcete upravit:

   - Chcete-li přihlašovací údaje zaregistrovat, klepněte na volbu **Register** (Zaregistrovat)a potom postupujte podle pokynů na obrazovce.
   - Chcete-li odstranit přihlašovací údaje, klepněte na volbu **Clear** (Odstranit) a potom klepněte na tlačítko **Yes** (Ano) v dialogovém okně pro potvrzení.
   - Chcete-li upravit vlastnosti přihlašovacích údajů, klepněte na volbu **Properties** (Vlastnosti)a potom postupujte podle pokynů na obrazovce.

5. Klepněte na tlačítko **Apply** (Použít) a potom na tlačítko **OK**.

Konfigurace nastavení nástroje Credential Manager

Na stránce „Settings” (Nastavení) můžete prohlížet a upravovat různá nastavení pomocí následujících karet:

- General (Obecné) — Umožňuje upravovat nastavení základní konfigurace.
- Single Sign On (Jednotné přihlášení) — Umožňuje upravovat nastavení určující chování funkce Single Sign On u aktuálního uživatele, jako jsou například způsob provedení detekce přihlašovacích obrazovek, automatické přihlášení k registrovaným přihlašovacím dialogům a zobrazování hesla.
- Services and Applications (Služby a aplikace) — Umožňuje zobrazovat dostupné služby a modifikovat jejich nastavení.
- Security (Zabezpečení) — Umožňuje vybrat software čtečky otisků prstů a nastavit úroveň zabezpečení čtečky.
- Smart Cards and Tokens (Čipové karty a známky) — Umožňuje zobrazovat a upravovat vlastnosti všech dostupných čipových karet a známek.

Úprava nastavení nástroje Credential Manager:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Advanced Settings** (Pokročilá nastavení).
3. V pravém podokně označte odpovídající kartu pro nastavení, která chcete upravit.
4. Postupujte podle pokynů na obrazovce a dokončete úpravu nastavení.
5. Klepnutím na tlačítko **Apply** (Použít) a potom na **OK** uložíte provedené změny.

Příklad 1 — Použití stránky „Advanced Settings” (Pokročilá nastavení) k umožnění přihlášení k systému Windows z nástroje Credential Manager

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Advanced Settings** (Pokročilá nastavení).
3. V pravém podokně klepněte na kartu **General** (Obecné).
4. U možnosti **Select the way users log on to Windows (requires restart)** (Vybrat způsob, jakým se uživatelé přihlašují k systému Windows - vyžaduje restartování) vyberte zaškrtávací políčko

Use Credential Manager with classic logon prompt (Použít nástroj Credential Manager s klasickým přihlašovacím oknem).

5. Klepnutím na tlačítko **Apply** (Použít) a potom na **OK** uložíte provedené změny.
6. Restartujte počítač.

Poznámka Vybrání zaškrtávacího políčka **Use Credential Manager with classic logon prompt** (Použít nástroj Credential Manager s klasickým přihlašovacím oknem) vám umožní uzamknout počítač. Viz „Uzamčení počítače“.

Příklad 2 — Použití stránky „Advanced Settings” (Pokročilá nastavení) k nastavení vyžadujícímu ověření uživatele před použitím jednotného přihlášení

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Credential Manager** a poté klepněte na položku **Advanced Settings** (Pokročilá nastavení).
3. V pravém podokně klepněte na kartu **Single Sign On** (Jednotné přihlášení).
4. U položky **When registered logon dialog or Web page is visited** (Při spuštění přihlašovacího dialogu registrované aplikace nebo návštěvě registrované stránky) označte zaškrtávací políčko **Validate user before submitting credentials** (Ověřit uživatele před odesláním přihlašovacích údajů).
5. Klepnutím na tlačítko **Apply** (Použít) a potom na **OK** uložíte provedené změny.
6. Restartujte počítač.

7 Device Access Manager pro HP ProtectTools

Tento nástroj zabezpečení je dostupný pouze pro správce. Nástroj Device Access Manager pro HP ProtectTools obsahuje funkce zabezpečení, které poskytují ochranu před neoprávněným přístupem k zařízením připojeným k počítačovému systému. Mezi tyto funkce patří:

- Pro každého uživatele se vytvářejí profily zařízení, které definují přístup k zařízením.
- Přístup k zařízením je možno udělovat nebo odepírat na základě členství ve skupinách.

Spouštění služeb na pozadí

Pro profily zařízení, které mají být použity, musí být spuštěna služba na pozadí HP ProtectTools Device Locking/Auditing. Pokusíte-li se použít profily zařízení poprvé, otevře nástroj HP ProtectTools Security Manager dialogové okno s dotazem, zda chcete spustit službu na pozadí. Klepnutím na tlačítko **Yes** (Ano) spusťte službu na pozadí a nastavte ji tak, aby se spouštěla při každém zavádění systému.

Jednoduchá konfigurace

Funkce umožňuje odepírat přístup u následujících tříd zařízení:

- zařízení USB pro všechny uživatele, kteří nejsou správci,
- všechna výměnná média (diskety, zásuvné paměťové jednotky atd.) pro všechny uživatele, kteří nejsou správci,
- všechny jednotky DVD/CD-ROM pro všechny uživatele, kteří nejsou správci,
- všechny sériové a paralelní porty pro všechny uživatele, kteří nejsou správci.

Odepření přístupu ke třídě zařízení všem uživatelům, kteří nejsou správci:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **Device Access Manager** a poté klepněte na položku **Simple Configuration** (Jednoduchá konfigurace).
3. V pravém panelu označte zaškrtávací políčko u zařízení, ke kterému chcete odepřít přístup.
4. Klepněte na tlačítko **Použít**.

Poznámka Není-li spuštěna služba na pozadí, dojde nyní k pokusu o její spuštění. Povolte ji klepnutím na tlačítko **Yes** (Ano).

5. Klepněte na tlačítko **OK**.

Konfigurace třídy zařízení (pokročilá)

K dispozici je několik možností výběru, které umožňují udělování nebo odepírání přístupu konkrétních uživatelů nebo skupin uživatelů k různým typům zařízení.

Přidání uživatele nebo skupiny

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **Device Access Manager** a poté klepněte na položku **Device Class Configuration** (Konfigurace třídy zařízení).
3. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat.
4. Klepněte na tlačítko **Add** (Přidat). Otevře se dialogové okno Select Users or Groups (Vyberte uživatele nebo skupiny).
5. Vybráním položky **Advanced > Find Now** (Pokročilé – Spustit hledání) vyhledejte uživatele nebo skupiny, které chcete přidat.
6. Klepněte na uživatele, kterému chcete odepřít přístup, a poté klepněte na tlačítko **OK**.
7. Klepněte na tlačítko **OK**.

Odstranění uživatele nebo skupiny

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **Device Access Manager** a poté klepněte na položku **Device Class Configuration** (Konfigurace třídy zařízení).
3. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat.
4. Klepněte na uživatele nebo skupinu, které chcete odstranit, a klepněte na tlačítko **Remove** (Odstranit).
5. Klepněte na tlačítko **Apply** (Použít) a poté na tlačítko **OK**.

Odepření přístupu uživateli nebo skupině

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **Device Access Manager** a poté klepněte na položku **Device Class Configuration** (Konfigurace třídy zařízení).
3. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat.
4. V seznamu **User/Groups** (Uživatel/Skupiny) přidejte uživatele nebo skupinu, kterým chcete odepřít přístup.
5. Klepněte na tlačítko **Deny** (Odepřít) vedle uživatele nebo skupiny, kterým chcete odepřít přístup.
6. Klepněte na tlačítko **Apply** (Použít) a poté na tlačítko **OK**.

Povolení přístupu ke třídě zařízení jednomu uživateli ze skupiny

Přístup ke třídě zařízení můžete povolit jednomu uživateli ze skupiny, zatímco všem ostatním uživatelům z této skupiny bude přístup odepřen.

Povolení přístupu jednomu uživateli, nikoli však skupině:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém panelu klepněte na možnost **Device Access Manager** a poté klepněte na položku **Device Class Configuration** (Konfigurace třídy zařízení).
3. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat.
4. V seznamu **User/Groups** (Uživatel/Skupiny) přidejte skupinu, které chcete odepřít přístup.
5. Klepněte na tlačítko **Deny** (Odepřít) vedle skupiny, které chcete odepřít přístup.
6. Přejděte do složky pod složkou požadované třídy a přidejte konkrétního uživatele. Klepnutím na tlačítko **Allow** (Povolit) udělte tomuto uživateli přístup.
7. Klepněte na tlačítko **Apply** (Použít) a poté na tlačítko **OK**.

Povolení přístupu ke konkrétnímu zařízení jednomu uživateli ze skupiny

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

Umožnění přístupu ke konkrétnímu zařízení jednomu uživateli, nikoli však skupině:

1. Vyberte položku **Start > Všechny programy > HP ProtectTools Security Manager**.
2. V levém podokně klepněte na možnost **Device Access Manager** a poté klepněte na položku **Device Class Configuration** (Konfigurace třídy zařízení).
3. V seznamu zařízení klepněte na třídu zařízení, kterou chcete konfigurovat, a poté přejděte do složky pod touto třídou.
4. V seznamu **User/Groups** (Uživatel/Skupiny) přidejte skupinu, které chcete odepřít přístup.
5. Klepněte na tlačítko **Deny** (Odepřít) vedle skupiny, které chcete odepřít přístup.
6. V seznamu zařízení přejděte ke konkrétnímu zařízení, k němuž chcete povolit přístup konkrétnímu uživateli.
7. Klepněte na tlačítko **Add** (Přidat). Otevře se dialogové okno Select Users or Groups (Vyberte uživatele nebo skupiny).
8. Vybráním položek **Advanced > Find Now** (Pokročilé – Spustit hledání) vyhledejte uživatele nebo skupiny, které chcete přidat.
9. Klepněte na uživatele, kterému chcete povolit přístup, a poté klepněte na tlačítko **OK**.
10. Klepnutím na tlačítko **Allow** (Povolit) udělíte tomuto uživateli přístup.
11. Klepněte na tlačítko **Apply** (Použít) a poté na tlačítko **OK**.

Slovníček

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

Automatická aktivace zámku jednotek Drivelock (Automatic DriveLock) Funkce zabezpečení, která zajišťuje generování hesel pro zámek jednotek DriveLock a jejich ochranu prostřednictvím integrovaného bezpečnostního čipu TPM. Je-li uživatel během spouštění systému ověřen integrovaným bezpečnostním čipem TPM na základě zadání správného hesla základního uživatelského klíče TPM, odemkne systém BIOS jednotku pevného disku, ke které tak uživatel získá přístup.

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

Certifikační autorita Služba, která vydává certifikáty vyžadované pro funkci infrastruktury používající veřejné klíče.

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

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

Digitální certifikát Elektronické pověření, které ověřuje identitu osoby nebo společnosti tím, že přiřazuje identitu vlastníka digitálního certifikátu k páru elektronických klíčů, které se používají k podepisování digitálních informací.

Digitální podpis Data odeslaná se souborem, která ověřují totožnost odesílatele. Současně se ověřuje, zda nebyl soubor po podpisu upraven.

Doména Skupina počítačů, které jsou součástí jedné sítě a které sdílejí společnou adresářovou databázi. Domény jsou jednoznačně pojmenovány a každá obsahuje sadu společných pravidel a procedur.

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

Heslo správce čipové karty Heslo, které přiřazuje čipovou kartu správce počítači v nástroji Computer Setup pro účely identifikace při spuštění nebo restartování. Toto heslo může ručně nastavit správce nebo je lze náhodně vygenerovat.

Heslo uživatele čipové karty Heslo, které přiřazuje čipovou kartu uživatele počítači v nástroji Computer Setup pro účely identifikace při spuštění nebo restartování. Toto heslo může ručně nastavit správce nebo je lze náhodně vygenerovat.

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

Infrastruktura veřejného klíče (Public Key Infrastructure - PKI) Standard, který definuje rozhraní pro vytváření, používání a spravování certifikátů a šifrovacích klíčů.

Integrovaný bezpečnostní čip Trusted Platform Module (TPM) (pouze u vybraných modelů) Integrovaný bezpečnostní čip, který chrání vysoce citlivá uživatelská data před útočníky. Jedná se o důvěryhodnou autoritu na dané platformě. Čip TPM poskytuje šifrovací algoritmy a operace, které splňují specifikace skupiny pro důvěryhodné použití výpočetní techniky Trusted Computing Group (TCG).

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

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

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

Osobní zabezpečený disk (Personal secure drive -PSD) Poskytuje chráněné úložiště pro citlivé informace.

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

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

Poskytovatel služeb šifrování (Cryptographic service provider - CSP) Poskytovatel nebo knihovna šifrovacích algoritmů, které lze použít v řádně definovaném rozhraní, aby prováděli určité funkce šifrování.

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

Profil systému BIOS Skupina nastavení systému BIOS, která lze uložit a použít u jiného účtu.

Přenesení Procedura, která umožňuje správu, obnovu a převod klíčů a certifikátů.

Restartování Proces vypnutí a zapnutí počítače.

Režim zabezpečení systému BIOS Nastavení v nabídce zabezpečení čipovou kartu, které ve chvíli, kdy je zapnuto, vyžaduje k ověření uživatele použití čipové karty a zadání platného osobního identifikačního čísla (PIN).

Silné zabezpečení Funkce silného zabezpečení v konfiguraci systému BIOS poskytuje rozšířenou ochranu hesel při spuštění a hesel správce a dalších způsobů ověření při spuštění.

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

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

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

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

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

Virtuální token Bezpečnostní funkce, která funguje podobným způsobem jako čipová karta se čtečkou. Token se ukládá buď na pevný disk počítače, nebo do registru systému Windows. Při přihlášení pomocí virtuálního tokenu je uživatel v rámci dokončení procesu ověření vyzván k zadání osobního identifikačního čísla (PIN).

Rejstřík