Příručka správy stolního počítače
Kancelářské počítače

Jediné záruky na produkty a služby společnosti HP jsou výslovně uvedeny v přesně vymezených prohlášeních týkajících se záruk na tyto produkty nebo služby. Ze žádných zde uvedených informací nelze vyvozovat existenci dalších záruk. Společnost HP neodpovídá za technické nebo redakční chyby ani za opomenutí vyskytující se v tomto dokumentu.

Příručka správy stolního počítače

Kancelářské počítače

Třetí vydání (červenec 2008)

Číslo dokumentu: 451272-223

O této příručce

Tato příručka obsahuje definice a pokyny k použití funkcí zabezpečení a správy, které jsou u některých modelů předem nainstalovány.

⚠ **VAROVÁNÍ!** Text označený tímto způsobem znamená, že nerespektování uvedených pokynů může ve svých důsledcích vést ke zranění nebo k ohrožení života.

△ **UPOZORNĚNÍ:** Text označený tímto symbolem informuje, že nerespektování uvedených pokynů může vést k poškození zařízení nebo ke ztrátě dat.

POZNÁMKA: Text označený tímto způsobem představuje důležité doplňující informace.

Obsah

1 Přehled správy stolního počítače

Nástroj HP Client Management Solutions nabízí standardní řešení pro správu a řízení stolních počítačů, pracovních stanic a notebooků v síťovém prostředí. Společnost HP se stala průkopníkem v oblasti správy stolních počítačů v roce 1995, kdy představila první stolní počítače umožňující úplnou správu. Společnost HP je držitelem patentu na tuto technologii. Od té doby stojí společnost HP v čele skupiny sestávající z dalších společností působících v této průmyslové oblasti, jež vyvíjejí standardy a infrastrukturu vyžadovanou pro efektivní nasazení, konfiguraci a správu stolních počítačů, pracovních stanic a notebooků. Společnost HP vyvíjí vlastní software pro správu a úzce spolupracuje s předními poskytovateli softwarových řešení, aby byla zajištěna kompatibilita mezi nástrojem HP Client Management Solutions a těmito produkty. Nástroj HP Client Management Solutions je důležitou součástí naší snahy poskytovat komplexní řešení, která pomáhají snižovat náklady na vlastnictví a údržbu osobních počítačů po celou dobu jejich životnosti.

Klíčové funkce a vlastnosti správy stolních počítačů:

- počáteční konfigurace a nasazení,
- vzdálená instalace systému,
- aktualizace a správa softwaru,
- aktualizace paměti ROM,
- konfigurace hardwarových doplňků,
- evidence majetku a zabezpečení,
- zobrazení informací o selhání systému a jeho obnovení.

POZNÁMKA: Podpora konkrétních funkcí popsaných v této příručce se může lišit v závislosti na modelu nebo verzi softwaru.

2 Úvodní konfigurace a nasazení

Počítač je dodán s předinstalovanou bitovou kopií systémového softwaru. Po krátkém procesu „rozbalení“ softwaru je počítač připraven k použití.

Je možné, že budete chtít předinstalovanou bitovou kopii softwaru nahradit vlastní sadou systémového softwaru s aplikacemi. Existuje několik metod nasazení vlastní bitové kopie softwaru. Jedná se o následující metody:

- Instalace dalších softwarových aplikací po rozbalení předinstalované bitové kopie softwaru.
- Použití nástrojů pro zavedení softwaru, jako například HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (založený na technologii Radia) nebo Altiris Deployment Solution pro nahrazení předinstalovaného softwaru vlastní bitovou kopií softwaru.
- Klonování disku pro zkopírování obsahu jednoho pevného disku na jiný.

Nejvhodnější metoda nasazení závisí na prostředí, v němž jsou informační technologie využívány, a procesech.

Systém HP Backup and Recovery, nástroj ROM-based setup a hardware ACPI poskytují dodatečnou pomoc při obnově systémového softwaru, správě konfigurace, řešení potíží a správě napájení.

POZNÁMKA: Informace o vytváření sady disků obnovy viz část HP Backup and Recovery Manager na stránce 11.

Nástroj HP Agent

Správce používaný oběma verzemi softwaru HP Client Automation (Standard i Enterprise) je v počítači předem zaveden. Po instalaci umožňuje komunikaci s konzolou pro správu HP.

Instalace nástroje HP Agent:

1. Klepněte na tlačítko **Start**.
2. Klepněte na položku **Všechny programy**.
3. Klepněte na položku **HP Manageability**.
4. Klepněte na položku **Radia Management Agent Readme**.
5. Přečtěte si pokyny v souboru Readme a v souladu s těmito pokyny nainstalujte nástroj HP Agent.

Nástroj HP Software Agent je klíčovou komponentou infrastruktury, která slouží k aktivaci všech řešení softwaru HP Client Automation. Chcete-li získat informace o dalších komponentách infrastruktury nezbytných pro implementaci řešení HP configuration management, navštivte webové stránky http://h20229.www2.hp.com/solutions/ascm/index.html.

Nástroj Altiris Deployment Solution Agent

Tento program je v počítači předem zaveden. Po instalaci umožňuje komunikaci s konzolou Deployment Solution správce.

Instalace nástroje Altiris Deployment Solution Agent:

1. Klepněte na tlačítko **Spustit**.
2. Klepněte na položku **Všechny programy**.
3. V systému Windows Vista klepněte na **Install Altiris DAgent** (Instalovat nástroj Altiris DAgent). V systému Windows XP klepněte na **Install Altiris AClient** (Instalovat nástroj Altiris AClient).
4. Při instalaci a nastavení klienta aplikace společnosti Altiris postupujte podle pokynů na obrazovce.

Tento nástroj je klíčovou komponentou infrastruktury a slouží k aktivaci řešení Altiris Deployment Solution, které je součástí nástroje Altiris Client Management Suite. Chcete-li získat informace o dalších komponentách infrastruktury nezbytných pro implementaci nástroje Altiris Client Management Suite, navštivte webové stránky http://www.hp.com/go/easydeploy.

3 Vzdálená instalace systému

Vzdálená instalace systému umožňuje spuštění a nastavení systému pomocí systémových a konfiguračních informací uložených na síťovém serveru inicializací prostředí Preboot Execution Environment (PXE). Funkce vzdálené instalace systému se obvykle používá jako nástroj pro instalaci a konfiguraci systému a lze ji použít k následujícím úkolům:

- formátování pevného disku,
- nasazení softwaru v jednom nebo více nových počítačích,
- vzdálená aktualizace systému BIOS v přepisovatelné paměti ROM (vzdálená aktualizace paměti ROM na stránce 15),
- konfigurace nastavení systému BIOS.

Chcete-li spustit nástroj Remote System Installation (Vzdálená instalace systému), stiskněte poté, co se v pravém dolním rohu obrazovky s logem společnosti HP zobrazí zpráva **F12 = Network Service Boot** (F12 = Zavedení systému pomocí síťové služby), klávesu F12. Dále postupujte podle pokynů na obrazovce. Výchozí pořadí spouštění je nastaveno v konfiguraci systému BIOS, kterou lze změnit tak, aby spouštění vždy probíhalo v prostředí PXE.

4 Aktualizace a správa softwaru

Společnost HP dodává několik nástrojů pro správu a aktualizaci softwaru ve stolních počítačích, pracovních stanicích a noteboocích:

- nástroj HP Client Management Interface,
- nástroj HP SoftPaq Download Manager,
- nástroj HP System Software Manager,
- nástroj HP ProtectTools Security Manager,
- verze Starter, Standard a Enterprise softwaru HP Client Automation,
- software HP Client Manager od společnosti Symantec,
- nástroj Altiris Client Management Suite,
- nástroj HP Client Catalog pro produkty Microsoft System Center & SMS,
- nástroj HP Backup and Recovery Manager,
- osobní počítače Intel vPro s technologií Active Management Technology,
- nástroj Verdiem Surveyor,
- nástroj HP Proactive Change Notification,
- služba HP Subscriber's Choice.

Nástroj HP Client Management Interface

Bez ohledu na to, jaké nástroje pro správu systému používá vaše oddělení ID, správa softwaru a hardwaru je z hlediska nákladů a pružnosti firmy velmi důležitá. Správce IT může k aplikaci HP Client Management Interface přistupovat psaním jednoduchých skriptů, které je možné integrovat k řešení pro správu dle výběru.

Rozhraní HP Client Management Interface (HP CMI) umožňuje hladkou integraci nových kancelářských počítačů HP do spravovaného prostředí IT. Rozhraní HP CMI představuje rozhraní, které zjednodušuje integraci kancelářských počítačů HP s oblíbenými nástroji pro průmyslovou systémovou správu (včetně nástrojů Microsoft Systems Management Server, IBM Tivoli Software a HP Operations) a aplikacemi pro správu vyvinutými pro vnitropodnikové použití. Při použití rozhraní HP CMI mohou nástroje pro systémovou správu a aplikace vyžádat podrobný výpis inventáře, získat informace o stavu a spravovat nastavení systému BIOS prostřednictvím komunikace přímo s klientským počítačem, což snižuje nutnost použití spojovacího softwaru, aby se docílilo integrace.

Nástroj HP Client Management Interface je v souladu se standardy MS WMI (Microsoft Windows Management Interface), WBEM (Web-Based Enterprise Management), SMBIOS (System Management BIOS) a ACPI (Advanced Configuration and Power Interface). Nástroj HP CMI představuje základní technologii využívanou nástrojem HP Client Management Solutions. S nástrojem HP CMI společnosti HP je volba způsobu spravování klientských počítačů HP na vás.

Nástroj HP Client Management Interface ve spojení se softwarem pro správu systému umožňuje provádět následující činnosti:

- Odesílání žádostí o podrobné informace týkající se inventáře klientů – získání podrobných informací o procesorech, pevných discích, paměti, systémech BIOS, ovladačích, včetně informací o čidlech (například informace o rychlosti ventilátoru, napětí a teplotě).
- Příjem informací o stavu počítačů – můžete nastavit odesílání široké škály upozornění na stav hardwaru klientů (například překročení teploty, zastavení ventilátoru a změny konfigurace hardwaru) do konzoly pro správu systému, aplikace nebo na místní klientský počítač. Upozornění jsou odesílána v reálném čase, a to v reakci na události spojené s hardwarem.
- Správa nastavení systému BIOS – můžete používat funkce F10, včetně vzdáleného nastavování a změny hesel systému BIOS a nastavování pořadí spouštění počítačů pomocí konzoly pro vzdálenou správu, která je nainstalovaná na jednom nebo všech klientských systémech, aniž by u jednotlivých počítačů byla nutná fyzická přítomnost.

Další informace o aplikaci HP Client Management Interface najdete na webové stránce http://www.hp.com/go/hpcmi/.

Nástroj HP SoftPaq Download Manager

Software HP SoftPaq Download Manager představuje volně přístupné a snadno použitelné rozhraní pro vyhledávání a stahování softwarových aktualizací pro klientské počítače HP. Po upřesnění typu modelu, operačního systému a jazyka můžete rychle vyhledat, třídit a vybírat potřebné softwarové balíčky. Software HP SoftPaq Download Manager si můžete stáhnout na adrese http://www.hp.com/go/sdm.

Nástroj HP System Software Manager

HP System Software Manager (SSM) je bezplatný nástroj, který automatizuje vzdálené nasazení ovladačů zařízení a aktualizací systému BIOS pro podnikové počítače HP připojené do sítě. Po spuštění nástroj bezobslužně (bez zásahu uživatele) určí revizní úrovně ovladačů a systému BIOS nainstalovaných v každém síťovém klientském počítači a porovná tyto údaje se systémovým softwarem SoftPaqs, který byl testován a uložen v centrálním úložišti souborů. Nástroj SSM potom automaticky aktualizuje veškerý systémový software počítačů v síti s nižší úrovní revize na poslední úrovně dostupné v úložišti. Nástroj SSM umožňuje distribuci aktualizací SoftPaq pouze do správných modelů klientských systémů, proto jej mohou správci s důvěrou a účinně používat k aktualizování systémového softwaru.

Nástroj System Software Manager lze integrovat s nástroji pro podnikovou distribuci softwaru, jako např. Client Automation solutions, HP Client Manager od společnosti Symantec a Microsoft Systems Management Server (SMS). Pomocí nástroje System Software Manager můžete distribuovat aktualizace vytvořené zákazníky nebo jinými společnostmi, které byly zabaleny do formátu tohoto nástroje.

Nástroj SSM lze bezplatně stáhnout z webu http://www.hp.com/go/ssm.

POZNÁMKA: Nástroj SSM aktuálně nepodporuje vzdálenou paměť ROM v systémech s povoleným nástrojem Windows Vista BitLocker, které používají měření TPM k ochraně klíčů BitLocker, protože přepsání systému BIOS by zrušilo platnost důvěryhodného certifikátu vytvořeného nástrojem BitLocker pro danou platformu. Aby bylo možné přepsat systém BIOS, vypněte nástroj BitLocker prostřednictvím možnosti Zásady skupiny.

Je možné povolit podporu nástroje BitLocker bez měření TPM systému BIOS, čímž předejdete zrušení platnosti klíčů nástroje BitLocker. Společnost HP doporučuje úschovu bezpečné zálohy přihlašovacích údajů nástroje BitLocker pro případ nouzové obnovy.

Nástroj HP ProtectTools Security Manager

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:

- Credential Manager for HP ProtectTools,
- Embedded Security for HP ProtectTools,
- Java Card Security for HP ProtectTools,
- BIOS Configuration for HP ProtectTools,
- Drive Encryption for HP ProtectTools,
- Device Access Manager for HP ProtectTools,
- nástroj File Sanitizer pro software HP ProtectTools,
- nástroj Privacy Manager pro software HP ProtectTools.

Obsah nabídky dostupných softwarových modulů je závislý na modelu počítače. Nástroj Embedded Security for HP ProtectTools je například k dispozici pouze pro počítače s nainstalovaným integrovaným bezpečnostním čipem Trusted Platform Module (TPM).

Moduly softwaru HP ProtectTools lze předem nainstalovat, zavést, případně je můžete stáhnout z webu HP. Pro vybrané počítače HP Compaq je software HP ProtectTools dostupný jako volitelný produkt. Další informace získáte na stránkách http://www.hp.com/products/security.

Verze Starter a Standard softwaru HP Client Automation

Software HP Client Automation je řešení pro správu hardwaru a softwaru v systémech Windows Vista, Windows XP a prostředí tenkého klienta HP. Snadno se používá a zavádí a současně představuje silný základ pro splnění budoucích požadavků. Je nabízen ve dvou edicích:

- Verze Starter je bezplatná aplikace pro správu stolních počítačů, přenosných počítačů a pracovních stanic HP. Poskytuje podrobné informace o hardwaru a softwaru, vzdálené ovládání, sledování výstrah HP, aktualizace systému BIOS a ovladačů HP, integraci s nástroji HP Protect Tools a doplňkovou podporu technologie Intel AMT. Verze Starter také podporuje zavádění a správu tenkých klientů HP.
- Placená verze Standard zahrnuje veškeré funkce verze Starter. Navíc umožňuje zavedení a přenesení systému Windows, správu oprav, distribuci softwaru a měření využití softwaru.

Verze Starter a Standard aplikace HP Client Automation poskytují možnost přechodu na verzi Enterprise (založena na technologii Radia) pro automatizovanou správu velkých neustále se měnících prostředí IT.

Více informací o řešeních HP Client Automation najdete na webu http://www.hp.com/go/client.

HP Client Automation verze Enterprise

Verze Enterprise softwaru HP Client Automation je řešení založené na zásadách, které umožňuje správcům získávat informace o používaném softwaru, zavádět, opravovat a průběžně spravovat software a obsah na různých klientských platformách. Verze Enterprise softwaru HP Client Automation umožňuje správcům IT provádět následující činnosti:

- Automatizace procesu správy po celý životní cyklus, a to od zjišťování, zavádění a průběžné správy po přenášení a vyřazování.
- Automatické zavádění a průběžná správa veškerého softwaru (operační systémy, aplikace, opravy, nastavení a obsah).
- Správa softwaru prakticky na libovolném zařízení, včetně stolních a přenosných počítačů a pracovních stanic, a to v různorodých a samostatných infrastrukturách.
- Správa softwaru ve většině operačních systémů.

Průběžná správa konfigurací vede k výraznému snížení nákladů IT, urychluje uvádění produktů (softwaru a obsahu) na trh a zvyšuje produktivitu a spokojenost uživatelů.

Více informací o řešeních HP Client Automation najdete na webu http://www.hp.com/go/client.

software HP Client Manager od společnosti Symantec

Software HP Client Manager od společnosti Symantec vyvinutý spolu s aplikací Altiris je volně dostupný pro všechny podporované kancelářské počítače HP, přenosné počítače a pracovní stanice. Nástroj SSM integrovaný v softwaru HP Client Manager umožňuje centrální evidenci, monitorování a správu hardwarových prvků klientských systémů HP.

Software HP Client Manager lze použít k následujícím činnostem:

- získání cenných informací o hardwaru (o nastavení procesoru, paměti, grafiky a zabezpečení),
- sledování stavu systému a řešení problémů ještě před jejich vznikem,
- automatické stahování a instalace ovladačů a aktualizací systému BIOS, aniž by u každého počítače byla nutná fyzická přítomnost,
- vzdálená konfigurace nastavení systému BIOS a zabezpečení,
- automatizace procesů za účelem rychlého řešení potíží s hardwarem,

dokonalá integrace s nástroji HP Instant Support, což zkracuje dobu nutnou pro řešení potíží,

- diagnostika – vzdálené spouštění a zobrazování zpráv na stolních počítačích, noteboocích a pracovních stanicích HP,
- kontrola stavu systému – zjišťování známých problémů s hardwarem klientských systémů HP,
- Active Chat – připojení k technické podpoře HP za účelem řešení problémů,
- databáze HP Knowledgebase – přístup k odborným informacím,
- automatizované stahování a doručování balíčků SoftPaq pro rychlé odstraňování problémů s hardwarem,
- rozpoznání, inventarizace a inicializace systémů pomocí integrovaného bezpečnostního čipu HP ProtectTools,
- možnost zobrazení upozornění na stav přímo na klientském systému,
- získávání základních inventárních informací pro jiné klienty než HP,
- instalace a nastavení bezpečnostního čipu TPM,
- centrální plán záloh a obnovování klientů,
- přidaná podpora pro správu Intel AMT.

Více informací o nástroji HP Client Manager od společnosti Symantec najdete na webové adrese http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Sada nástrojů Altiris Client Management Suite představuje snadno použitelné řešení pro úplné řízení životního cyklu stolních počítačů, notebooků a pracovních stanic. Sada nástrojů Altiris Client Manager Suite úrovně 1 obsahuje následující produkty společnosti Altiris:

- Inventory Solution,
- Deployment Solution,
- Software Delivery Solution,
- Patch Management Solution,
- Application Metering Solution,
- Application Management Solution,
- Carbon Copy Solution.

Více informací o softwaru Altiris Client Management Suite najdete na webové adrese http://www.altiris.com/Products/ClientManagementSuite.aspx.

nástroj HP Client Catalog pro produkty Microsoft System Center & SMS

Nástroj HP Client Catalog umožňuje správcům IT použít produkty od společnosti Microsoft pro automatizované nasazení softwarových aktualizací HP (Softpaqs) do kancelářských počítačů HP. Soubor katalogu obsahuje podrobné informace o platformách kancelářských počítačů HP, přenosných počítačů a pracovních stanic. Ve spojení s funkcemi uživatelského inventáře a aktualizace obsaženými v produktech Microsoft jej lze využít k automatizovanému aktualizování ovladačů pro klientské počítače HP.

Nástroj HP Client Catalog podporuje následující produkty Microsoft:

- System Center Configuration Manager 2007,
- System Center Essentials 2007,
- Systems Management Server (SMS) 2003 R2.

Více informací o nástroji HP Client Catalog for SMS najdete na webové adrese http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

HP Backup and Recovery Manager

Nástroj HP Backup and Recovery Manager je snadno použitelná a všestranná aplikace, která umožňuje zálohovat a obnovit primární pevný disk počítače. Aplikace pracuje v prostředí systému Windows a vytváří zálohy systému, všech aplikací a datových souborů. Vytváření záloh lze naplánovat tak, aby probíhalo automaticky v určitých intervalech, nebo je lze vytvářet ručně. Důležité soubory lze archivovat odděleně od pravidelných záloh.

Nástroj HP Backup and Recovery Manager je předinstalován na disku C: a vytvoří oddíl pro obnovu pevného disku.

Body obnovení a zálohy souborů lze kopírovat na disky CD či DVD, všechny zálohy pak lze kopírovat na síťové či sekundární pevné disky.

Společnost HP důrazně doporučuje vytvořit sadu disků obnovy ještě předtím, než začnete počítač používat, a naplánovat pravidelné automatické vytváření bodů obnovy.

Postup při vytvoření sady disků obnovy:

1. Klepnutím na položku **Start** > **HP Backup and Recovery** > **HP Backup and Recovery Manager** spusťte nástroj Backup and Recovery Wizard (Průvodce zálohováním a obnovou). Klepněte na tlačítko **Next** (Další).
2. Vyberte položku **Create a set of recovery discs (Recommended)** (Vytvořit sadu disků obnovy – doporučeno) a poté klepněte na tlačítko **Next** (Další).
3. Postupujte podle pokynů průvodce.

Další informace o používání nástroje HP Backup and Recovery Manager naleznete v *Uživatelské příručce nástroje HP Backup and Recovery Manager* po vybrání položek **Start** > **HP Backup and Recovery** > **HP Backup and Recovery Manager Manual** (Příručka nástroje HP Backup and Recovery Manager).

POZNÁMKA: Sadu disků obnovy můžete objednat prostřednictvím střediska podpory společnosti HP. Přejděte na následující web, vyberte oblast a klepněte na položku **Technical support after you buy** (Technická podpora zakoupených produktů) v části **Call HP** (Volat společnost HP). Zde naleznete telefonní číslo na středisko podpory ve své oblasti.

http://welcome.hp.com/country/us/en/wwcontact_us.html

technologie správy

Modely jsou dodávány se standardní technologií nebo technologií vPro. Obě umožňují snadnější vyhledání, opravu a zabezpečení síťové výpočetní techniky. Obě technologie rovněž umožňují spravovat počítač bez ohledu na to, zda je systém zapnut, vypnut nebo nereaguje.

Funkce technologie správy zahrnují:

- zjišťování informací o inventáři hardwaru,
- generování upozornění,
- zapínání, vypínání a restartování zařízení,
- vzdálená diagnostika a opravy,
  - funkce Serial-over-LAN (umožňuje ovládání osobních počítačů během jejich zavádění),
  - funkce IDE-Redirect (umožňuje spouštění systému ze vzdálené spustitelné jednotky, disku nebo pomocí bitového obrazu ISO),
- hardwarové odpojení a obnova (omezení nebo přerušení přístupu do počítačové sítě při zjištění virové hrozby).

POZNÁMKA: Základní informace o technologii Intel vPro najdete na webové stránce http://www.intel.com/vpro.

Informace o technologii Intel vPro specifické pro produkty HP najdete v technické dokumentaci na webové stránce http://www.hp.com/support. Vyberte možnost United States (English) a poté možnost **See support and troubleshooting information** (Informace o řešení problémů a podpoře), zadejte číslo modelu počítače a stiskněte klávesu Enter. V kategorii **Resources** (Prostředky) klepněte na možnost **Manuals (guides, supplements, addendums, etc)** (Příručky /průvodci, dodatky atd./). V části **Quick jump to manuals by category** (Odkazy na příručky podle kategorie) klepněte na možnost **White papers** (Technická dokumentace).

Mezi dostupné technologie správy patří:

- AMT (obsahuje nástroj DASH 1.0),
- ASF.

Technologie ASF a AMT nelze konfigurovat současně, jsou však obě podporovány.

Konfigurace systémů Intel vPro pro použití technologie AMT nebo ASF:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Microsoft Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat**.
2. Před tím, než se spustí operační systém, stiskněte kombinaci kláves Ctrl+P.

   POZNÁMKA: Pokud kombinaci kláves Ctrl+P nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí kláves Ctrl+P.

Tato klávesová zkratka aktivuje nástroj Intel Management Engine BIOS Execution (MEBx). Tento nástroj umožňuje uživatelům nastavovat různé aspekty technologie pro správu. Některé z možností konfigurace jsou uvedeny níže:

- Main Menu (Hlavní nabídka)
  - Intel ® ME Configuration (Konfigurace Intel ® ME),
  - Intel ® AMT Configuration (Konfigurace Intel ® AMT),
  - Change Intel ® ME Password (Změna hesla Intel ® ME),
  - Ukončit.
- Intel ® ME Configuration (Konfigurace platformy Intel ® ME)
  - Intel ® ME State Control (enable/disable) (Ovládání stavu Intel ® ME (povolit/zakázat)),
  - Intel ® ME State Control (enable/disable) (Místní aktualizace firmaru Intel ® ME (povolit/zakázat)),
  - Intel ® ME Features Control (Ovládání funkcí Intel ® ME),
  - Intel ® ME Power Control (Ovládání napájení Intel ® ME).
- Intel ® AMT Configuration (Konfigurace Intel ® AMT)
  - Host Name (Hostitelský název),
  - TCP/IP,
  - Provision Model (Enterprise, SMB),
  - Setup and Configuration (Instalace a konfigurace),
  - Un-Provision,
  - SOL/IDE-R (enable/disable) (SOL/IDE-R (povolit/zakázat)),
  - Password Policy (Směrnice týkající se hesla),
  - Secure Firmware Update (enable/disable) (enable/disable) (Bezpečná aktualizace firmwaru (povolit/zakázat)),
  - Set PRTC (Nastavení PRTC),
  - Idle Timeout (Časový limit nečinnosti).
- Change Intel ® ME Password (Změna hesla Intel ® ME) (Společnost HP doporučuje změnit toto heslo. Výchozím heslem je **admin**.)

Aby bylo možné provádět vzdálenou správu systémů AMT, správce musí používat vzdálenou konzolu podporující systémy AMT. Konzoly pro správu podniků jsou k dispozici u dodavatelů, jako například HP, Altiris a Microsoft SMS. V režimu SMB poskytuje klient rozhraní webového prohlížeče. Chcete-li k této funkci získat přístup, otevřete prohlížeč z libovolného systému v síti a zadejte `http://název_hostitele:16992`, kde `název_hostitele` je název přiřazený systému. Místo názvu hostitele lze také použít adresu IP.

Verdiem Surveyor

Software Verdiem Surveyor slouží ke správě výdajů za energii spotřebované počítačem. Software Surveyor provádí měření a podává zprávy o tom, kolik energie každý počítač spotřebuje. Také ovládá nastavení napájení počítače, což umožňuje správcům v sítích snadno použít strategie pro úsporu energie. Ze stránky podpory společnosti HP lze stáhnout balíček Softpaq obsahující nástroj Surveyor a poté ho lze nainstalovat na podporované modely stolních počítačů. Licence nástroje Surveyor pro správu počítačů lze zakoupit prostřednictvím zástupce společnosti HP.

HP Proactive Change Notification

Program Proactive Change Notification používá web Subscriber's Choice a umožňuje aktivní a automatické provádění následujících úloh:

- odesílání e-mailů PCN (Proactive Change Notification), které upozorňují na změny hardwaru a softwaru u většiny běžně dostupných počítačů a serverů, a to až 60 dní předem;
- odesílání e-mailů obsahujících informační bulletiny, rady a poznámky pro zákazníky, bulletiny týkající se zabezpečení a upozornění na ovladače pro většinu běžně dostupných počítačů a serverů.

Můžete vytvořit vlastní profil a zajistit tak, že budete dostávat pouze informace vztahující se ke specifickému prostředí informačních technologií. Chcete-li zjistit další informace o programu Proactive Change Notification nebo si vytvořit vlastní profil, navštivte webovou stránku http://h30046.www3.hp.com/subhub.php.

Služba Subscriber’s Choice

Subscriber’s Choice je klientská služba společnosti HP.

Na základě vašeho profilu vám společnost HP bude dodávat přizpůsobené tipy k produktům, články o funkcích produktů nebo upozornění na ovladače a možnosti podpory.

Funkce upozornění na ovladače a možnosti podpory (Driver and Support Alerts/Notifications) služby Subscriber’s Choice odesílá e-maily s oznámením, že informace, k jejichž odběru jste se přihlásili ve svém profilu, jsou k dispozici. Chcete-li zjistit další informace o službě Subscriber’s Choice a vytvořit si vlastní profil, navštivte webovou stránku http://h30046.www3.hp.com/subhub.php.

Nepoužívaná řešení

Dodávka dvou softwarových balíčků Altiris Local Recovery a Dantz Retrospect pro kancelářské stolní počítače, notebooky a pracovní stanice společnosti HP byla ukončena. Všechny nové kancelářské stolní počítače, notebooky a pracovní stanice uvedené na trh v roce 2006 budou dodávány s nástrojem HP Backup and Recovery Manager.

5 aktualizace paměti ROM

Systém BIOS počítače je uložen v programovatelné paměti ROM typu flash (jen ke čtení). Vytvoříte-li pomocí nástroje Computer Setup (F10) heslo pro nastavení, můžete paměť ROM chránit před nechtěnou aktualizací nebo neúmyslným přepsáním. To je důležité k zajištění provozní integrity počítače. Budete-li chtít aktualizovat systém BIOS, můžete si nejnovější bitové obrazy systému BIOS stáhnout z webových stránek společnosti HP http://www.hp.com/support/files, kde najdete informace o podpoře a ovladače.

△ **UPOZORNĚNÍ:** Chcete-li zajistit maximální ochranu paměti ROM, vytvořte heslo pro nastavení. Toto heslo brání neoprávněným upgradům paměti ROM. Nástroj System Software Manager umožňuje správci systému nastavit heslo pro nastavení u několika počítačů současně. Další informace najdete na webové adrese http://www.hp.com/go/ssm.

vzdálená aktualizace paměti ROM

Vzdálená aktualizace paměti ROM umožňuje správci systému bezpečně aktualizovat systém BIOS ve vzdálených počítačích HP přímo z centrální konzoly pro správu sítě. Provedení tohoto úkolu vzdáleně ve více počítačích zajistí jednotné nasazení a lepší kontrolu nad bitovými kopiemi systému BIOS v počítačích HP v síti. Zlepší se také produktivita a sníží celkové náklady na vlastnictví.

POZNÁMKA: Nástroj SSM aktuálně nepodporuje vzdálenou paměť ROM v systémech s povoleným nástrojem Windows Vista BitLocker, které používají měření TPM k ochraně klíčů BitLocker, protože přepsání systému BIOS by zrušilo platnost důvěryhodného certifikátu vytvořeného nástrojem BitLocker pro danou platformu. Aby bylo možné přepsat systém BIOS, vypněte nástroj BitLocker prostřednictvím možnosti Zásady skupiny.

Chcete-li využít vzdálenou aktualizaci paměti ROM, musí být počítač zapnut standardně nebo pomocí funkce Remote Wakeup (Vzdálené spuštění).

Další informace o vzdálené aktualizaci paměti ROM naleznete v části věnované nástroji HP Client Manager Software nebo System Software Manager na webových stránkách http://www.hp.com/go/ssm/.

Nástroj HPQFlash

Nástroj HPQFlash slouží k místní aktualizaci nebo obnově systému BIOS jednotlivých osobních počítačů z operačního systému Windows.

Chcete-li o nástroji HPQFlash získat více informací, navštivte webovou stránku http://www.hp.com/support/files a po zobrazení výzvy zadejte číslo modelu počítače.

6 Boot Block Emergency Recovery Mode (režim nouzové obnovy zaváděcího bloku)

Funkce Boot Block Emergency Recovery Mode (Režim nouzové obnovy zaváděcího bloku) umožňuje obnovu systému v případě selhání aktualizace paměti ROM. Pokud například dojde během aktualizace systému BIOS k výpadku proudu, aktualizace paměti ROM se nedokončí. Systém BIOS nebude kvůli této události funkční. Zaváděcí blok je část paměti ROM chráněná před přepsáním, která při každém zapnutí počítače kontroluje neporušenost bitového obrazu systému BIOS.

- Pokud je bitový obraz systému BIOS platný, systém se spustí běžným způsobem.
- Pokud je bitový obraz systému BIOS neplatný, systém BIOS zaváděcího bloku pro bezpečné zavedení umožňuje najít na vyměnitelných médiích soubory bitového obrazu systému BIOS. Pokud je nalezen požadovaný bitový obraz systému BIOS, bude automaticky použit k aktualizaci obsahu paměti ROM.

Pokud je zjištěn neplatný bitový obraz systému BIOS, indikátor napájení systému 8krát zabliká červeně (v jednosekundových intervalech). Současně zazní z reproduktoru 8 pípnutí. Pokud není poškozena část paměti ROM obsahující bitový obraz paměti ROM pro obrazový výstup, zobrazí se zpráva **Boot Block Emergency Recovery Mode** (Režim nouzové obnovy zaváděcího bloku).

Systém, který se přepne do režimu obnovení Boot Block Emergency Recovery Mode (Režim nouzové obnovy zaváděcího bloku), obnovíte podle následujících pokynů:

1. Vypněte napájení.
2. Vložte disk CD nebo zařízení USB typu flash obsahující v kořenovém adresáři požadovaný soubor bitového obrazu systému BIOS.

   POZNÁMKA: Média musejí být naformátována pomocí systému souborů FAT12, FAT16 nebo FAT32.

3. Zapněte počítač.

   Pokud nebyl nalezen žádný vhodný bitový obraz systému BIOS, budete vyzváni k vložení média obsahujícího požadovaný soubor.

   Pokud se paměť ROM úspěšně přeprogramuje, systém se automaticky vypne.
4. Vyjměte vyměnitelné médium, které bylo použito pro upgrade systému BIOS.
5. Počítač znovu spusťte.

POZNÁMKA: Nástroj BitLocker zabraňuje systému Windows Vista ve spouštění, pokud je v optické jednotce disk CD obsahující bitový obraz systému BIOS. Pokud povolíte nástroj BitLocker, před spuštěním systému Windows Vista nejprve tento disk CD vyjměte.

7 Replikace nastavení:

Následující postupy umožňují správci snadno kopírovat konfiguraci nastavení mezi počítači stejného modelu. Lze tak rychleji a konzistentněji nakonfigurovat více počítačů.

POZNÁMKA: Oba postupy vyžadují disketu nebo podporované zařízení USB flash.

Kopírování do jednoho počítače

UPOZORNĚNÍ: Konfigurace nastavení závisí na modelu. Pokud se provedení zdrojového a cílového počítače liší, může dojít k poškození systému souborů. Například nekopírujte konfiguraci nastavení z počítače dc7xxx do počítače dx7xxx.

1. Vyberte konfiguraci nastavení, kterou chcete kopírovat. Vypněte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Vypnout**.
2. Jestliže používáte zařízení USB typu flash, vložte je nyní do počítače.
3. Zapněte počítač.
4. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

   POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.
5. Jestliže používáte disketu, vložte ji nyní do jednotky.
6. Zvolte možnosti **File** (Soubor) > **Replicated Setup** (Replikované nastavení) > **Save to Removable Media** (Uložit na vyměnitelné médium). Podle pokynů na obrazovce vytvořte konfigurační disketu nebo médium USB typu flash.
7. Vypněte počítač, který chcete konfigurovat, a vložte do jednotky konfigurační disketu nebo médium USB typu flash.
8. Zapněte konfigurovaný počítač.
9. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.
10. Klepněte na položky **File** (Soubor) > **Replicated Setup** (Replikované nastavení) > **Restore from Removable Media** (Obnovit z vyměnitelného média) a postupujte podle pokynů na obrazovce.
11. Po dokončení konfigurace restartujte počítač.

Kopírování do více počítačů

△ **UPOZORNĚNÍ:** Konfigurace nastavení závisí na modelu. Pokud se provedení zdrojového a cílového počítače liší, může dojít k poškození systému souborů. Například nekopírujte konfiguraci nastavení z počítače dc7xxx do počítače dx7xxx.

U této metody trvá trochu déle příprava konfiguračního média (disketa nebo USB typu flash), ale kopírování konfigurace do cílových počítačů je značně rychlejší.

POZNÁMKA: K tomuto postupu je nutné spustitelné médium. Jestliže nemáte k dispozici systém Windows XP, ve kterém byste vytvořili spustitelnou disketu, použijte metodu kopírování do jednoho počítače (viz část Kopírování do jednoho počítače na stránce 18).

1. Vytvořte spustitelné médium (disketa nebo USB typu flash). Naleznete na stránce Podporovaná zařízení USB flash na stránce 20 nebo Nepodporovaná zařízení USB flash na stránce 21.

   △ **UPOZORNĚNÍ:** Ne všechny počítače lze spouštět z média USB typu flash. Pokud je ve výchozím pořadí spouštění v nástroji Computer Setup (F10) uvedeno zařízení USB před pevným diskem, je možné počítač spouštět z média USB typu flash. Jinak je nutné použít spustitelnou disketu.

2. Vyberte konfiguraci nastavení, kterou chcete kopírovat. Vypněte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Vypnout**.

3. Jestliže používáte zařízení USB typu flash, vložte je nyní do počítače.

4. Zapněte počítač.

5. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

   POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.

6. Jestliže používáte disketu, vložte ji nyní do jednotky.

7. Zvolte možnosti **File** (Soubor) > **Replicated Setup** (Replikované nastavení) > **Save to Removable Media** (Uložit na vyměnitelné médium). Podle pokynů na obrazovce vytvořte konfigurační disketu nebo médium USB typu flash.

8. Stáhněte nástroj systému BIOS pro replikaci nastavení (repset.exe) a zkopírujte jej na konfigurační disketu nebo médium USB typu flash. Tento nástroj získáte zadáním adresy http://welcome.hp.com/country/us/en/support.html a následným zadáním modelu počítače.

9. Na konfigurační disketě nebo médiu USB typu flash vytvořte soubor autoexec.bat s následujícím příkazem:

   ```
   repset.exe
   ```

10. Vypněte konfigurovaný počítač. Vložte do něj konfigurační disketu nebo médium USB typu flash a zapněte jej. Konfigurační nástroj bude automaticky spuštěn.

11. Po dokončení konfigurace restartujte počítač.

Vytváření spustitelného zařízení:

Podporovaná zařízení USB flash

Podporovaná zařízení obsahují předem nainstalovanou bitovou kopii, která zjednodušuje proces jejich změny na spustitelné zařízení. Veškerá zařízení USB typu flash od společnosti HP a Compaq obsahují předem nainstalovaný bitový obraz. Pokud používané zařízení USB typu flash tuto bitovou kopii neobsahuje, použijte postup dále v této kapitole (viz část Nepodporovaná zařízení USB flash na stránce 21).

K vytvoření spustitelného média USB typu flash potřebujete:

- podporované zařízení USB typu flash,
- spustitelnou disketu pro systém DOS s programy FDISK a SYS (Pokud program SYS není k dispozici, lze použít program FORMAT, ale všechny existující soubory v zařízení USB typu flash budou ztraceny.),
- počítač, který lze spouštět z média USB typu flash.

△ **UPOZORNĚNÍ:** Některé starší počítače nelze spouštět z média USB typu flash. Pokud je ve výchozím pořadí spouštění v nástroji Computer Setup (F10) uvedeno zařízení USB před pevným diskem, je možné počítač spouštět z média USB typu flash. Jinak je nutné použít spustitelnou disketu.

1. Vypněte počítač.
2. Vložte zařízení USB typu flash do jednoho z portů USB na počítači a odeberte všechna ostatní zařízení USB pro ukládání dat kromě disketových jednotek USB.
3. Vložte spustitelnou disketu DOS s programy FDISK.COM a SYS.COM nebo FORMAT.COM do disketové jednotky a zapněte počítač, aby zavedl systém z této diskety.
4. Spusťte program FDISK z umístění **A:** zadáním `FDISK` v příkazovém řádku a stisknutím klávesy Enter. Zobrazí-li se výzva, klepnutím na tlačítko **Yes** (Ano) (**Y**) povolíte podporu velkých disků.
5. Zadáním možnosti Choice [`5`] (Výběr) zobrazte jednotky v systému. Zařízení USB typu flash bude ta jednotka, jejíž velikost se blíží velikosti jedné z uvedených jednotek. Obvykle půjde o poslední jednotku v seznamu. Poznamenejte si písmeno jednotky.

   Jednotka zařízení USB typu flash: _____

   △ **UPOZORNĚNÍ:** Pokud jednotka neodpovídá zařízení USB typu flash, nepokračujte. Může dojít ke ztrátě dat. Zkontrolujte všechny porty USB, zda neobsahují paměťová zařízení. Pokud ano, odeberte je, restartujte počítač a pokračujte krokem 4. Pokud ne, systém nepodporuje zařízení USB typu flash nebo je toto zařízení vadné. NEPOKOUŠEJTE SE dále převádět zařízení USB typu flash na spustitelné médium.
6. Ukončete nástroj FDISK stisknutím klávesy Esc. Znovu se zobrazí příkazový řádek **A:**.
7. Jestliže spustitelná disketa systému DOS obsahuje program SYS.COM, přejděte ke kroku 8, jinak ke kroku 9.
8. Na příkazovém řádku **A:** zadejte příkaz `SYS x:`, kde x zastupuje písmeno jednotky, které jste si poznamenali výše.

   △ **UPOZORNĚNÍ:** Ověřte si, zda jste písmeno jednotky zařízení USB typu flash zadali správně.

Po přenosu systémových souborů se program SYS vrátí na příkazový řádek **A:**. Přejděte ke kroku 13.

9. Zkopírujte všechny soubory, které chcete zachovat, ze zařízení USB typu flash do dočasného adresáře na jiné jednotce (například na vnitřní pevný disk systému).

10. Na příkazovém řádku **A:** zadejte příkaz `FORMAT /S X:`, kde `X` představuje písmeno jednotky, které jste si poznamenali výše.

△ **UPOZORNĚNÍ:** Ověřte si, zda jste písmeno jednotky zařízení USB typu flash zadali správně.

Příkaz FORMAT zobrazí jednu nebo více zpráv a v každém případě si vyžádá váš souhlas. Stiskněte vždy klávesu `Y`. Příkaz FORMAT zformátuje zařízení USB flash, přidá systémové soubory a zeptá se, jaké označení chcete svazku přidělit.

11. Stisknutím klávesy Enter nezadáte žádný popisek. Pokud popisek požadujete, zadejte jej.

12. Zkopírujte všechny soubory, které jste uložili v kroku 9, zpět na zařízení USB.

13. Vyjměte disketu a restartujte počítač. Počítač zavede systém ze zařízení USB jako z jednotky C.

POZNÁMKA: Výchozí pořadí spouštění se liší v každém počítači a lze je změnit v nástroji Computer Setup (F10).

Pokud jste použili systém DOS v systému Windows 9x, může se nakrátko zobrazit logo systému Windows. Jestliže tuto obrazovku nechcete zobrazovat, přidejte do kořenového adresáře zařízení USB typu flash soubor LOGO.SYS s nulovou délkou.

Přejděte zpět k části Kopírování do více počítačů na stránce 19.

Nepodporovaná zařízení USB flash

K vytvoření spustitelného média USB typu flash potřebujete:

- zařízení USB typu flash,
- spustitelnou disketu pro systém DOS s programy FDISK a SYS (Pokud program SYS není k dispozici, lze použít program FORMAT, ale všechny existující soubory v zařízení USB typu flash budou ztraceny.),
- počítač, který lze spouštět z média USB typu flash.

△ **UPOZORNĚNÍ:** Některé starší počítače nelze spouštět z média USB typu flash. Pokud je ve výchozím pořadí spouštění v nástroji Computer Setup (F10) uvedeno zařízení USB před pevným diskem, je možné počítač spouštět z média USB typu flash. Jinak je nutné použít spustitelnou disketu.

1. Pokud se v systému nacházejí karty PCI s připojenými jednotkami SCSI, ATA RAID nebo SATA, vypněte počítač a odpojte napájecí kabel.

△ **UPOZORNĚNÍ:** Napájecí kabel je NUTNÉ odpojit.

2. Otevřete počítač a vyjměte karty PCI.

3. Vložte zařízení USB typu flash do jednoho z portů USB na počítači a odeberte všechna ostatní zařízení USB pro ukládání dat kromě disketových jednotek USB. Zavřete kryt počítače.

4. Připojte k počítači napájecí kabel a zapněte počítač.

5. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

   POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.

6. Přejděte na možnost **Advanced** (Upřesnit) > **PCI Devices** (Zařízení PCI) a zakažte řadiče disků PATA i SATA. Při zakazování řadiče disků SATA si poznamenejte hodnotu IRQ, které je řadič přiřazen. Tuto hodnotu bude třeba později znovu přiřadit. Ukončete nástroj s potvrzením změn.

   Hodnota IRQ řadiče disků SATA: _____

7. Vložte spustitelnou disketu DOS s programy FDISK.COM a SYS.COM nebo FORMAT.COM do disketové jednotky a zapněte počítač, aby zavedl systém z této diskety.

8. Spusťte program FDISK a odstraňte existující oddíly v zařízení USB typu flash. Vytvořte nový oddíl a označte jej jako aktivní. Stisknutím klávesy Esc ukončete program FDISK.

9. Pokud se systém po ukončení programu FDISK automaticky nerestartuje, stiskněte klávesy Ctrl + Alt + Del a restartujte systém z diskety DOS.

10. Na příkazovém řádku **A:** zadejte příkaz `>FORMAT C: /S` a stiskněte klávesu Enter. Program FORMAT zformátuje zařízení USB typu flash, přidá systémové soubory a zeptá se na popisek svazku (Volume Label).

11. Stisknutím klávesy Enter nezadáte žádný popisek. Pokud popisek požadujete, zadejte jej.

12. Vypněte počítač a odpojte napájecí kabel. Otevřete počítač a nainstalujte znovu odebrané karty PCI. Zavřete kryt počítače.

13. Připojte k počítači napájecí kabel, vyjměte disketu a zapněte počítač.

14. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

15. Klepněte na položky **Advanced** (Upřesnit) > **PCI Devices** (Zařízení PCI) a znovu povolte řadiče disků PATA a SATA, které jste zakázali v kroku 6. U řadiče disků SATA nastavte původní hodnotu IRQ.

16. Uložte změny a ukončete program. Počítač zavede systém ze zařízení USB jako z jednotky C.

   POZNÁMKA: Výchozí pořadí spouštění se liší v každém počítači a lze je změnit v nástroji Computer Setup (F10). Více informací o použití nástroje Computer Setup naleznete v *Příručce k nástroji Computer Setup (F10)*.

   Pokud jste použili systém DOS v systému Windows 9x, může se nakrátko zobrazit logo systému Windows. Jestliže tuto obrazovku nechcete zobrazovat, přidejte do kořenového adresáře zařízení USB typu flash soubor LOGO.SYS s nulovou délkou.

Přejděte zpět k části Kopírování do více počítačů na stránce 19.

8 Tlačítko režimů napájení

Pokud je povoleno rozhraní ACPI (Advanced Configuration and Power Interface), může vypínač napájení počítač zapnout, vypnout nebo převést do pohotovostního režimu. Funkce úsporného režimu počítač nevypne zcela, přepne jej však do režimu nízké spotřeby. To umožňuje rychlé vypnutí počítače bez nutnosti zavřít aplikace a také rychlé obnovení původního provozního stavu bez ztráty dat.

Chcete-li změnit konfiguraci tlačítka napájení, proveďte následující kroky:

1. Klepněte levým tlačítkem myši na tlačítko **Start** a potom vyberte možnosti **Ovládací panely** > **Možnosti napájení**.
2. V okně **Možnosti napájení – vlastnosti** klepněte na kartu **Upřesnit**.
3. Ve skupinovém rámečku **Tlačítka napájení** vyberte možnost **Přepnout do úsporného režimu**.

Po konfiguraci vypínače napájení na funkci úsporného režimu převedete systém stisknutím vypínače do režimu nízké spotřeby energie (úsporného režimu). Dalším rychlým stisknutím vypínače uvedete systém do plného provozního stavu. Chcete-li systém zcela vypnout, stiskněte vypínač a podržte jej po dobu čtyř sekund.

△ **UPOZORNĚNÍ:** Nepoužívejte vypínač k vypnutí počítače s výjimkou případu, že systém nereaguje. Vypnutí počítače bez interakce s operačním systémem může způsobit poškození nebo ztrátu dat na pevném disku.

9 Podpora na stránkách společnosti HP

Technici společnosti HP pečlivě testují a ladí software společnosti HP i software jiných výrobců a vyvíjejí podpůrný software pro konkrétní operační systémy, aby zajistili nejvyšší úroveň výkonu, kompatibility a spolehlivosti počítačů HP.

Při přechodu na nový nebo vylepšený operační systém je velmi důležité nasazení podpůrného softwaru určeného pro příslušný operační systém. Jestliže plánujete používání verze systému Microsoft Windows, která se liší od verze dodávané s počítačem, je nutné nainstalovat odpovídající nástroje a ovladače zařízení, aby byla zajištěna podpora a správné fungování všech funkcí.

Společnost HP zjednodušila umísťování, přístup, hodnocení a instalaci nejnovějších verzí podpůrného softwaru. Tento software lze stáhnout z webové adresy http://www.hp.com/support.

Na tomto webu jsou k dispozici nejnovější ovladače zařízení, nástroje a bitové kopie přepisovatelné paměti ROM potřebné ke spuštění nejnovějšího operačního systému Microsoft Windows v počítači HP.

10 Průmyslové standardy

Produkty pro správu společnosti HP lze integrovat s dalšími aplikacemi pro správu systému a jsou založeny na následujících standardech:

- WBEM (Web-Based Enterprise Management),
- rozhraní WMI (Windows Management Interface),
- technologie Wake on LAN,
- rozhraní ACPI,
- SMBIOS,
- podpora prostředí PXE (Pre-boot Execution).

11 Evidence inventárních čísel a zabezpečení

Funkce evidence inventárních čísel (sledování majetku) obsažené v počítači poskytují důležité údaje o evidenci inventárních čísel, které lze spravovat pomocí produktů HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager a dalších aplikací pro správu systému. Dokonalá automatická integrace funkcí evidence inventárních čísel a těchto produktů umožňuje zvolit nástroj pro správu, který nejlépe odpovídá danému prostředí, a maximálně zhodnotit investice do stávajících nástrojů.

Společnost HP také nabízí několik produktů pro řízení přístupu k cenným součástem a informacím. Nástroj HP Embedded Security for ProtectTools zabraňuje neoprávněnému přístupu k datům, kontroluje integritu systému a ověřuje uživatele, kteří chtějí získat přístup do systému. (Další informace najdete v příručce *HP ProtectTools Security Manager Guide* (Příručka správce zabezpečení HP ProtectTools) na adrese http://www.hp.com/products/security.) Funkce zabezpečení, například HP Embedded Security for ProtectTools, senzor počítačového rámu a zámek počítačového rámu, které jsou dostupné u některých modelů, pomáhají zabránit neoprávněnému přístupu k vnitřním součástem počítače. Zákazem paralelních nebo sériových portů či portů USB nebo zákazem možnosti spuštění z vyměnitelných médií můžete chránit cenná data. Upozornění na změnu paměti (Memory Change) a upozornění senzoru počítačového rámu (Smart Cover Sensor) mohou být automaticky směrována aplikacím pro správu systému, a tím aktivně upozorňovat na manipulaci s vnitřními součástmi počítače.

POZNÁMKA: Nástroj HP Embedded Security for ProtectTools, senzor počítačového rámu (Smart Cover Sensor) a zámek počítačového rámu (Smart Cover Lock) jsou k dispozici u některých systémů jako volitelné doplňky.

Nastavení zabezpečení v počítačích HP provádějte pomocí následujících nástrojů:

- Místně pomocí nástroje Computer Setup. Další informace a pokyny týkající se použití nástroje Computer Setup naleznete v *Příručce k nástroji Computer Setup (F10)* dodané s počítačem. Některé počítače jsou vybaveny nástrojem HP BIOS Configuration for ProtectTools, což je komponenta ProtectTools založená na systému Windows, která umožňuje správcům konfigurovat nastavení zabezpečení systému BIOS v rámci spuštěného operačního systému.
- Vzdáleně, pomocí nástrojů HP Client Manager od společnosti Symantec, HP Client Automation nebo System Software Manager. Tento software umožňuje spolehlivé a jednotné nasazení a řízení nastavení zabezpečení.

Následující tabulka a části obsahují informace týkající se místní správy funkcí zabezpečení počítače pomocí nástroje Computer Setup (F10).

Tabulka 11-1 Přehled funkcí zabezpečení

Možnost	Popis
Heslo pro nastavení	Umožňuje nastavit a povolit heslo pro nastavení (pro správce).

Tabulka 11-1 Přehled funkcí zabezpečení (pokračování)

	POZNÁMKA: Pokud je nastaveno heslo pro nastavení, je vyžadováno při změnách možností nástroje Computer Setup, obsahu paměti ROM a některých nastavení prostředků Plug and Play systému Windows.
Heslo pro spuštění	Umožňuje nastavit a povolit heslo pro spuštění. Po vypnutí a zapnutí systému se zobrazí výzva k zadání hesla pro spuštění. Pokud uživatele zadá nesprávné heslo, systém se nespustí. **POZNÁMKA:** Toto heslo se neobjevuje po softwarovém restartu, provedeném například pomocí klávesové zkratky Ctrl + Alt + Delete nebo po výběru možnosti **Restart** (Restartovat) v systému Windows, není-li to v části **Password Options** (Možnosti hesla) nastaveno jinak (viz níže).
Možnosti hesla (Tato položka se zobrazí pouze v případě, že je nastaveno heslo pro spuštění nebo heslo pro nastavení.)	Umožňuje provádět následující akce: • Zamknout prostředky starších verzí (pouze je-li zadáno heslo pro nastavení). • Povolit nebo zakázat režim síťového serveru (pouze je-li zadáno heslo pro spuštění)., • Určete, zda bude při restartování (Ctrl+Alt+Delete) požadováno heslo (zobrazí se, jen pokud je nastaveno heslo pro spuštění). • Enable/Disable Setup Browse Mode (Povolit/zakázat procházení nastavení) (zobrazí se, jen pokud je nastaveno heslo pro nastavení) (bez zadání hesla pro nastavení umožňuje prohlížení, ne však změnu, možností nastavení F10). • Enable/disable Stringent Password (Povolit/zakázat heslo Stringent)(objeví se, pokud jste nastavili heslo pro spouštění). Je-li toto heslo povoleno, bude použito pro obejití můstku hesla a zakázání hesla pro spouštění. Více informací naleznete v dokumentu *Příručka správy stolního počítače*.
Smart Cover (Zámek Smart Cover) (některé modely)	Umožňuje provádět následující akce: • zamknout nebo odemknout zámek počítačového rámu, • nastavit senzor počítačového rámu na možnost Disable (Zakázat)/Notify User (Upozornit uživatele)/Setup Password (Heslo pro nastavení). **POZNÁMKA:** Pokud je vybrána možnost *Notify User* (Upozornit uživatele) a senzor rozpozná, že byl sejmut kryt, bude uživatel na tuto skutečnost upozorněn. Jestliže je vybrána možnost *Setup Password* (Heslo pro nastavení) a senzor rozpozná, že byl sejmut kryt, bude při spuštění počítače požadováno zadání hesla pro nastavení. Tato funkce je podporována pouze u některých modelů.
Zabezpečení zařízení	Umožňuje nastavení možnosti Device Available (Zařízení dostupné)/Device Hidden (Zařízení skryto) pro: • sériové porty, • paralelní port, • zadní porty USB, • čelní porty USB, • interní porty USB, • zvuk systému, • síťové řadiče (u některých modelů), • starší typy disketových jednotek, • zařízení Embedded Security (u některých modelů). • SATA0, • SATA1 (některé modely),

Tabulka 11-1 Přehled funkcí zabezpečení (pokračování)

	• SATA2 (některé modely), • SATA3 (některé modely), • eSATA (některé modely).
Zavedení systému pomocí síťové služby	Povoluje nebo zakazuje možnost zavést do počítače operační systém nainstalovaný na síťovém serveru. (Tato funkce je k dispozici pouze u modelů se síťovou kartou, která musí být umístěna na sběrnici PCI nebo integrována na systémové desce.)
ID systému	Umožňuje nastavit tyto možnosti: • 18bajtové inventární číslo majetku (Asset Tag) přidělené počítači ve společnosti. • Označení vlastnictví (80 bytový identifikátor zobrazený během testu POST). • Sériové číslo rámu nebo číslo UUID (Universal Unique Identifier). Číslo UUID lze aktualizovat pouze v případě, že aktuální sériové číslo rámu je neplatné. (Tato identifikační čísla jsou obvykle nastavena výrobcem a slouží k jednoznačné identifikaci systému.) • Jazyk klávesnice (například angličtina nebo němčina) pro zadání ID systému.
Zabezpečovací funkce DriveLock	Umožňuje nastavit či změnit hlavní nebo uživatelské heslo vyžadované při přístupu k pevným diskům. Pokud je tato funkce aktivována, bude uživatel během testu POST vyzván k zadaní jednoho z hesel funkce DriveLock. V případě, že nebude ani jedno heslo zadáno správně, nebude možné získat přístup k pevnému disku a to až do okamžiku, než bude při následném spuštění po vypnutí zadáno správné heslo. **POZNÁMKA:** Tato volba se zobrazí pouze v případě, že je k systému připojena alespoň jedna jednotka podporující funkci DriveLock.
System Security (Zabezpečení systému) (některé modely: tyto možnosti jsou závislé na hardwaru)	Data Execution Prevention (Omezení spuštění dat)(některé modely) (povolit/zakázat) – zabraňuje narušení zabezpečení operačního systému. Virtualization Technology (Virtualizační technologie) (některé modely) (povolit/zakázat) – řídí virtualizační funkce procesoru. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače. Virtualization Technology Directed I/O (Virtualizační technologie pro řízený vstup a výstup) (některé modely) (povolit/zakázat) – řídí funkce čipové sady pro přemapování DMA při virtualizaci. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače. Trusted Execution Technology (Technologie důvěryhodného spouštění) (některé modely) (povolit/zakázat) – řídí funkce procesoru a čipové sady potřebné pro podporu virtuálního zařízení. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače. Chcete-li tuto funkci aktivovat, je nutné povolit následující funkce: • Embedded Security Device Support (Podpora integrovaného bezpečnostního zařízení), • Virtualization Technology (Virtualizační technologie), • Virtualization Technology Directed I/O (Virtualizační technologie pro řízený vstup a výstup). Embedded Security Device Support (Podpora integrovaného bezpečnostního zařízení) (některé modely) (povolit/zakázat) – umožňuje aktivaci a deaktivaci integrovaného bezpečnostního zařízení. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače.

Tabulka 11-1 Přehled funkcí zabezpečení (pokračování)

	POZNÁMKA: Aby bylo možné nastavit integrované bezpečnostní zařízení, je nutné nastavit heslo nástroje Setup. • Reset to Factory Settings (Obnovit nastavení výrobce) (některé modely) (neresetovat/resetovat) – obnovením nastavení výrobce smažete všechny bezpečnostní klíče. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače. **UPOZORNĚNÍ:** Integrované bezpečnostní zařízení je důležitou komponentou mnoha bezpečnostních schémat. Smazáním bezpečnostních klíčů zabráníte přístupu k datům chráněným integrovaným bezpečnostním zařízením. Zvolíte-li obnovení nastavení výrobce, může dojít ke značné ztrátě dat. • Power-on authentication support (Podpora ověřování při zapnutí) (některé modely) (povolit/zakázat) – řídí schéma ověření hesla po zapnutí, které používá integrované bezpečnostní zařízení. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače. • Reset authentication credentials (Resetovat přihlašovací údaje pro ověření) (některé modely) (neresetovat/resetovat) – vybráním této možnosti deaktivujete podporu ověřování po zapnutí a odstraníte ověřovací informace z integrovaného bezpečnostního zařízení. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače. OS management of Embedded Security Device (Řízení integrovaného bezpečnostního zařízení operačním systémem) (některé modely) (povolit/zakázat) – tato volba umožňuje uživateli omezit kontrolu operačního systému nad integrovaným bezpečnostním zařízením. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače. Tato volba umožňuje uživateli omezit kontrolu operačního systému nad integrovaným bezpečnostním zařízením. • Reset of Embedded Security Device through OS (Reset integrovaného bezpečnostního zařízení prostřednictvím operačního systému) (některé modely) (povolit/zakázat) – tato volba umožňuje uživateli omezit schopnost operačního systému požadovat obnovení nastavení výrobce na integrovaném bezpečnostním zařízení. Změna nastavení vyžaduje vypnutí a opětovné zapnutí počítače. **POZNÁMKA:** Aby bylo možné povolit tuto možnost, je třeba nastavit heslo nástroje Setup. Smart Card BIOS Password Support (Podpora karet Smart Card místo hesla systému BIOS) (některé modely) (povolit/zakázat) – umožňuje uživateli povolit nebo zakázat použití karty Smart Card místo hesla nástroje Setup a hesla pro spuštění. Aby se tato volba projevila, vyžaduje nastavení dodatečnou inicializaci v nástroji ProtectTools. PAVP (některé modely) (zakázáno/min/max) – PAVP slouží pro povolení technologie Protected Audio Video Path v chipsetu. Tato akce umožňuje zobrazení obsahu s vysokým rozlišením, jehož přehrávání by za normálních okolností bylo zakázáno. Hodnota Max přidělí funkci PAVP 96 megabajtů systémové paměti.
Setup Security Level (Úroveň zabezpečení nastavení)	Umožňuje nastavit pro koncové uživatele omezený přístup k některým možnostem nastavení, aniž by bylo nutno znát heslo pro nastavení. Tato funkce umožňuje správcům chránit systém před změnami důležitých možností nastavení a současně povolit uživatelům zobrazení systémových nastavení a umožnit konfiguraci možností, které nejsou pro funkčnost systému zásadní. Správce určuje oprávnění přístupu k jednotlivým možnostem nastavení pomocí nabídky Setup Security Level (Úroveň zabezpečení nastavení). Standardně je ke všem možnostem nastavení přiřazeno heslo pro nastavení. To znamená, že chce-li uživatel kteroukoli z těchto možností změnit, musí během testu POST zadat požadované heslo pro nastavení. Správce může pro jednotlivé možnosti vybrat nastavení None (Žádné). To znamená, že uživatel může změnit vybrané možnosti, pokud bylo nastavení otevřeno pomocí neplatných hesel. Možnost None (Žádné) bude nahrazena možností Power-On Password (Heslo pro spuštění), pokud je heslo pro spuštění povoleno. **POZNÁMKA:** Pokud chcete uživateli povolit přístup k nastavení bez znalosti hesla pro nastavení, je nutno pod položkou Setup Browse Mode (Režim procházení nastavení) vybrat možnost Enable (Povolit).

Zabezpečení pomocí hesla

Heslo pro spuštění zabraňuje neoprávněnému použití počítače tím, že při každém spuštění nebo restartování počítače vyžaduje zadání hesla pro přístup k aplikacím či datům. Heslo pro nastavení zabraňuje neoprávněnému přístupu k nástroji Computer Setup. Lze jej také použít jako nadřazené heslo namísto hesla pro spuštění. To znamená, že pokud po výzvě k zadání hesla pro spuštění zadáte heslo pro nastavení, budete moci počítač používat.

Je možné vytvořit heslo pro nastavení platné pro celou síť, které správci systému umožní přihlášení ke všem počítačům v síti a jejich správu bez toho, aby znal nastavené heslo pro spuštění.

Vytvoření hesla pro přihlášení pomocí nástroje Computer Setup

Pokud je systém vybaven zařízením integrovaného zabezpečení (Embedded Security), další informace najdete v *Příručce k nástroji HP ProtectTools Security Manager* na webové stránce http://www.hp.com. Vytvoření hesla pro nastavení pomocí nástroje Computer Setup zabrání změně konfigurace počítače (použití nástroje Computer Setup – F10), dokud nebude zadáno heslo.

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat**.
2. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

POZNÁMKA: Pokud klávesu F10 nestisknete v pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.

3. Vyberte možnost **Security** (Zabezpečení) a poté příkaz **Setup Password** (Heslo pro nastavení) a postupujte podle pokynů na obrazovce.
4. Před ukončením práce zvolte možnosti **File** (Soubor) > **Save Changes and Exit** (Uložit změny a ukončit program).

Vytvoření hesla pro spuštění pomocí nástroje Computer Setup

Vytvoření hesla pro spuštění pomocí nástroje Computer Setup zabraňuje použití počítače po jeho spuštění, pokud není zadáno heslo. Pokud je heslo pro spuštění nastaveno, zobrazí se v nabídce nástroje Computer Setup **Security** (Zabezpečení) položka **Password Options** (Možnosti nastavení hesla). Jednou z těchto možností je **Password Prompt on Warm Boot** (Požadovat heslo při restartování). Jestliže je možnost **Password Prompt on Warm Boot** (Požadovat heslo při restartování) povolena, je nutno heslo zadat při každém restartování počítače.

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat**.
2. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.

3. Vyberte možnost **Security** (Zabezpečení) a poté možnost **Power-On Password** (Heslo pro spuštění) a postupujte podle pokynů na obrazovce.

4. Před ukončením práce zvolte možnosti **File** (Soubor) > **Save Changes and Exit** (Uložit změny a ukončit program).

Zadání hesla při spuštění

Při zadávání hesla pro spuštění postupujte podle následujících pokynů:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat počítač**.

2. Jakmile se na obrazovce objeví ikona klíče, zadejte aktuální heslo a stiskněte klávesu Enter.

POZNÁMKA: Pište opatrně. Z bezpečnostních důvodů se psaná písmena nezobrazují na obrazovce.

Jestliže heslo nezadáte správně, zobrazí se ikona zlomeného klíče. Zadejte heslo znovu. Po třech neúspěšných pokusech musíte počítač vypnout, znovu ho zapnout a teprve potom můžete pokračovat.

Zadání hesla pro nastavení

Pokud je systém vybaven zařízením integrovaného zabezpečení (Embedded Security), další informace najdete v *Příručce k nástroji HP ProtectTools Security Manager* na webové stránce http://www.hp.com.

Pokud bylo v počítači vytvořeno heslo pro nastavení, budete vyzváni k jeho zadání při každém spuštění nástroje Computer Setup.

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat**.

2. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.

3. Jakmile se na obrazovce objeví ikona klíče, zadejte heslo pro nastavení a stiskněte klávesu Enter.

POZNÁMKA: Pište opatrně. Z bezpečnostních důvodů se psaná písmena nezobrazují na obrazovce.

Jestliže heslo nezadáte správně, zobrazí se ikona zlomeného klíče. Zadejte heslo znovu. Po třech neúspěšných pokusech musíte počítač vypnout, znovu ho zapnout a teprve potom můžete pokračovat.

Změna hesla pro spuštění nebo hesla pro nastavení

Pokud je systém vybaven zařízením integrovaného zabezpečení (Embedded Security), další informace najdete v *Příručce k nástroji HP ProtectTools Security Manager* na webové stránce http://www.hp.com.

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat počítač**.
2. Chcete-li změnit heslo pro spuštění, přejděte ke kroku 3.

   Chcete-li změnit heslo pro nastavení, vstupte do nástroje Computer Setup stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

   POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.
3. Jakmile se zobrazí ikona klíče, zadejte aktuální heslo, lomítko (/) nebo alternativní oddělovací znak, nové heslo, další lomítko (/) nebo alternativní oddělovací znak a opět nové heslo: `aktuální heslo/nové heslo/nové heslo`

   POZNÁMKA: Pište opatrně. Z bezpečnostních důvodů se psaná písmena nezobrazují na obrazovce.
4. Stiskněte klávesu Enter.

Nové heslo vejde v platnost po novém zapnutí počítače.

POZNÁMKA: Informace o alternativních oddělovacích znacích naleznete v části Národní oddělovací znaky klávesnice na stránce 33. Heslo pro spuštění a heslo pro nastavení lze změnit také pomocí příkazů nabídky Security (Zabezpečení) nástroje Computer Setup.

Odstranění hesla pro spuštění nebo hesla pro nastavení

Pokud je systém vybaven zařízením integrovaného zabezpečení (Embedded Security), další informace najdete v *Příručce k nástroji HP ProtectTools Security Manager* na webové stránce http://www.hp.com.

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat počítač**.
2. Chcete-li odstranit heslo pro spuštění, přejděte ke kroku 3.

   Chcete-li heslo pro nastavení smazat, vstupte do nástroje Computer Setup stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

   POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.
3. Po zobrazení ikony klíče zadejte aktuální heslo a lomítko (/) nebo alternativní oddělovací znak: `aktuální heslo/`
4. Stiskněte klávesu Enter.

POZNÁMKA: Informace o alternativních oddělovacích znacích naleznete v části Národní oddělovací znaky klávesnice na stránce 33. Heslo pro spuštění a heslo pro nastavení lze změnit také pomocí příkazů nabídky Security (Zabezpečení) nástroje Computer Setup.

Národní oddělovací znaky klávesnice

Každá klávesnice je vytvořena tak, aby splňovala specifické požadavky dané země. Syntax a klávesy používané ke změně nebo odstranění hesla závisí na klávesnici dodávané s počítačem.

Národní oddělovací znaky klávesnice					
/	arabská	-	řecká	/	ruská
=	belgická	.	hebrejská	-	slovenská
-	BHČCSS*	-	maďarská	-	španělská
/	brazilská	-	italská	/	švédská / finská
/	čínská	/	japonská	-	švýcarská
-	česká	/	korejská	/	čínská (Tchaj-wan)
-	dánská	-	Latinská Amerika	/	thajská
!	francouzská	-	norská	.	turecká
é	francouzská (Kanada)	-	polská	/	anglická (USA)
-	německá	-	portugalská		

* Bosna a Hercegovina, Černá Hora, Chorvatsko, Slovinsko a Srbsko

Vymazání hesel

Pokud zapomenete heslo, nebudete mít přístup k počítači. Pokyny k vymazání hesel naleznete v příručce *Poradce při potížích*.

Pokud je systém vybaven zařízením integrovaného zabezpečení (Embedded Security), další informace najdete v *Příručce k nástroji HP ProtectTools Security Manager* na webové stránce http://www.hp.com.

DriveLock

Funkce DriveLock představuje standardní zabezpečení před neoprávněným přístupem k datům na pevných discích ATA. Funkce DriveLock byla implementována jako rozšíření nástroje Computer Setup. Je k dispozici, jen pokud jsou zjištěny pevné disky podporující příkazy zabezpečení rozhraní ATA. Funkce DriveLock je určena pro zákazníky společnosti HP, pro něž je zabezpečení dat prvořadou záležitostí. Pro takové zákazníky je cena pevného disku a ztráta na něm uložených dat bezvýznamnou ve srovnání se škodami, které mohou vzniknout v důsledku neoprávněného přístupu k datům. V zájmu zachování požadované úrovně zabezpečení a současně praktické potřeby zjistit zapomenuté heslo využívá tato implementace funkce DriveLock schéma zabezpečení se dvěma hesly. Jedno heslo nastavuje a používá správce systému. Druhé heslo obvykle nastavuje a používá koncový uživatel. Pokud byla zapomenuta obě hesla, neexistuje žádná možnost, jak jednotku odemknout. Proto je nejvhodnější používat funkci DriveLock v případě, že data pevného disku jsou replikována v podnikovém informačním systému nebo jsou pravidelně zálohována. Dojde-li ke ztrátě obou hesel funkce DriveLock, pevný disk nelze používat. Pro uživatele, kteří neodpovídají výše uvedenému profilu, může tato

skutečnost představovat nepřijatelné riziko. Pro uživatele, kteří klientskému profilu vyhovují, může být toto riziko únosné v závislosti na povaze dat, která jsou na pevném disku uložena.

Použití zámku DriveLock

Pokud systém zjistí přítomnost jednoho či více pevných disků podporujících příkazy zabezpečení rozhraní ATA, v programu Computer Setup v nabídce Security (Zabezpečení) se zobrazí možnost DriveLock. Uživateli jsou k dispozici možnosti pro nastavení hlavního hesla nebo povolení funkce DriveLock. K povolení funkce DriveLock je nezbytné zadat uživatelské heslo. Počáteční konfiguraci funkce DriveLock provádí obvykle správce systému. Z tohoto důvodu musí být nejdříve nastaveno hlavní heslo. Společnost HP doporučuje správcům systému, aby hlavní heslo nastavili bez ohledu na to, zda mají v úmyslu funkci DriveLock povolit či zakázat. Tím bude správci umožněna úprava nastavení funkce DriveLock v případě, že jednotka bude někdy uzamknuta. Po nastavení hlavního hesla může správce systému funkci DriveLock povolit nebo zakázat.

V případě uzamčené jednotky pevného disku bude test POST k odemknutí zařízení vyžadovat heslo. Pokud se nastavené heslo pro spuštění shoduje s uživatelským heslem zařízení, uživatel nebude testem POST vyzván k jeho opětovnému zadání. V opačném případě se zobrazí výzva k zadání hesla funkce DriveLock. Po spuštění lze použít hlavní nebo uživatelské heslo. Při restartování zadejte totéž heslo, které bylo použito k odemknutí jednotky během předchozího spuštění. Uživatelé mají dva pokusy k zadání správného hesla. Nebude-li při spouštění ani jeden z pokusů úspěšný, test POST bude pokračovat, avšak jednotka zůstane nepřístupná. Nebude-li při restartování systému Windows ani jeden z pokusů úspěšný, test POST bude ukončen a uživatel bude vyzván k vypnutí a zapnutí systému.

Aplikace DriveLock

Funkce zabezpečení DriveLock je nejvhodnější pro podnikové prostředí. Správce systému zde odpovídá za konfiguraci pevného disku, což mimo jiné zahrnuje i nastavení hlavního hesla a dočasného uživatelského hesla funkce DriveLock. V případě, že uživatel heslo zapomene nebo zařízení převezme jiný zaměstnanec, může být hlavní heslo vždy využito k novému nastavení uživatelského hesla a obnovení přístupu k jednotce pevného disku.

Společnost HP doporučuje správcům systému, kteří se rozhodnou funkci DriveLock povolit, aby rovněž vytvořili podnikové zásady pro nastavení a údržbu hlavních hesel. Tím by se mělo zabránit situaci, kdy zaměstnanec úmyslně či neúmyslně nastaví obě hesla funkce DriveLock a poté podnik opustí. V takovém případě by se stal pevný disk nepoužitelným a bylo by nutné jej vyměnit. Podobně by se mohlo stát, že by vinou nenastavení hlavního hesla byl správcům systému odepřen přístup k jednotce pevného disku. Nemohli by pak provádět běžná zjišťování neoprávněného softwaru, používat jiné funkce řízení inventárních čísel ani poskytovat podporu.

Společnost HP nedoporučuje použití funkce DriveLock u uživatelů s méně přísnými požadavky na zabezpečení. Do této kategorie spadá osobní používání nebo takové využití, které běžně nevyžaduje správu citlivých dat na pevných discích. U takových uživatelů riziko možné ztráty pevného disku vinou zapomenutí obou hesel značně převyšuje hodnotu dat, k jejichž ochraně byla funkce DriveLock vytvořena. Přístup k nástroji Computer Setup a funkci DriveLock může být omezen prostřednictvím hesla pro nastavení. Pokud správce určí heslo pro nastavení a neposkytne je koncovým uživatelům, nebudou moci funkci DriveLock aktivovat.

senzor počítačového rámu

Senzor počítačového rámu dostupný u některých modelů je kombinací hardwarové a softwarové technologie, která vás upozorní, když byl odstraněn kryt počítače nebo boční panel. Zabezpečení je trojí úrovně a je popsáno v následující tabulce.

Tabulka 11-2 Senzor počítačového rámu – úrovně ochrany

Úroveň	Nastavení	Popis
Úroveň 0	Zakázáno	Senzor počítačového rámu je vypnutý (výchozí nastavení).
Úroveň 1	Upozornění uživatele	Po restartování počítače se na obrazovce zobrazí zpráva oznamující odejmutí krytu nebo bočního panelu počítače.
Úroveň 2	Heslo pro nastavení	Po restartování počítače se na obrazovce zobrazí zpráva oznamující odejmutí krytu nebo bočního panelu počítače. Pokud chcete pokračovat, musíte zadat heslo pro nastavení.

POZNÁMKA: Toto nastavení lze změnit pomocí nástroje Computer Setup. Další informace o nástroji Computer Setup naleznete v *Příručce k nástroji Computer Setup (F10)*.

Nastavení úrovně ochrany senzorem počítačového rámu

Chcete-li nastavit úroveň ochrany pomocí senzoru počítačového rámu, proveďte následující kroky:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat**.
2. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

   POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.
3. Zvolte možnosti **Security** (Zabezpečení) > **Smart Cover** (Zámek počítačového rámu) > **Cover Removal Sensor** (Senzor počítačového rámu) a vyberte požadovanou úroveň zabezpečení.
4. Před ukončením práce zvolte možnosti **File** (Soubor) > **Save Changes and Exit** (Uložit změny a ukončit program).

zámek Smart Cover Lock

Zámek počítačového rámu je ovládán prostřednictvím softwaru a jsou jím vybaveny některé počítače společnosti HP. Tento zámek zabraňuje neoprávněnému přístupu k vnitřním součástem počítače. Počítače se dodávají se zámkem Smart Cover Lock v odemknuté pozici.

△ **UPOZORNĚNÍ:** Chcete-li zajistit maximální zabezpečení zámku krytu, vytvořte heslo pro nastavení. Heslo pro nastavení předchází neoprávněnému přístupu do nástroje Computer Setup.

POZNÁMKA: Zámek počítačového rámu je volitelná funkce, která je k dispozici u některých modelů.

Uzamknutí zámku počítačového rámu

Chcete-li zámek počítačového rámu aktivovat a uzamknout, proveďte následující kroky:

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat**.
2. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

   POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.
3. Zvolte možnosti **Security** (Zabezpečení) > **Smart Cover** > **Cover Lock** (Zámek počítačového rámu) > **Lock** (Zamknout).
4. Před ukončením práce zvolte možnosti **File** (Soubor) > **Save Changes and Exit** (Uložit změny a ukončit program).

Odemknutí zámku počítačového rámu

1. Zapněte nebo restartujte počítač. Pokud pracujete v systému Windows, zvolte možnost **Start** > **Vypnout** > **Restartovat**.
2. Do nástroje Computer Setup vstoupíte stisknutím klávesy F10 po zapnutí počítače, před tím, než se spustí operační systém. V případě potřeby můžete stisknutím klávesy Enter přeskočit úvodní obrazovku.

   POZNÁMKA: Pokud klávesu F10 nestisknete v tu pravou dobu, bude možné získat k nástroji přístup až po opětovném restartování počítače a stisknutí klávesy F10.
3. Zvolte možnosti **Security** (Zabezpečení) > **Smart Cover** > **Cover Lock** (Zámek počítačového rámu) > **Unlock** (Odemknout).
4. Před ukončením práce zvolte možnosti **File** (Soubor) > **Save Changes and Exit** (Uložit změny a ukončit program).

Použití klíče Smart Cover FailSafe Key

Je-li zámek Smart Cover Lock zapnutý a nemůžete zadat heslo, které by jej deaktivovalo, budete k otevření krytu počítače potřebovat bezpečnostní klíč Smart Cover. Tento klíč je nutné použít, nastane-li některá z následujících situací:

- výpadek napájení,
- selhání při spuštění počítače,
- selhání některé součásti počítače (například procesoru nebo zdroje),
- zapomenutí hesla.

△ **UPOZORNĚNÍ:** Klíč Smart Cover FailSafe Key je specializovaným nástrojem poskytovaným společností HP. Buďte připraveni, objednejte si tento klíč u autorizovaného prodejce nebo poskytovatele služeb dříve, než jej budete potřebovat.

Bezpečnostní klíč můžete získat některým z následujících způsobů:

- Obraťte se na autorizovaného prodejce nebo poskytovatele služeb společnosti HP.
- Zavolejte na příslušné telefonní číslo uvedené v záruční smlouvě.

Další informace o použití bezpečnostního klíče Smart Cover naleznete v *Referenční příručce hardwaru*.

Úprava pro lankový zámek

Zadní panel počítače (některé modely) je přizpůsoben pro použití lankového zámku, který umožňuje fyzické zajištění počítače na pracovním místě.

Obrázky s pokyny naleznete v *Referenční příručce hardwaru*.

Technologie identifikace pomocí otisku prstu

Technologie identifikace pomocí otisku prstů společnosti HP odstraňuje nutnost zadávání hesel, čímž zlepšuje zabezpečení sítě, zjednodušuje proces přihlášení a omezuje náklady spojené se správou podnikových sítí. Tato cenově dostupná technologie již není určena pouze pro supermoderní vysoce zabezpečené organizace.

POZNÁMKA: Podpora technologie identifikace pomocí otisku prstu se u různých modelů počítačů liší.

Upozornění na chyby a obnova

Funkce zobrazení informací o selhání systému a jeho obnovení spojuje novátorské technologie hardwaru a softwaru s cílem zabránit ztrátě důležitých dat a minimalizovat prostoje.

Jestliže je počítač připojen k síti spravované pomocí nástroje HP Client Manager, odešle počítač informace o chybě do aplikace pro správu sítě. Pomocí softwaru HP Client Manager lze vzdáleně naplánovat automatické spuštění diagnostických činností ve všech spravovaných počítačích a vytvořit souhrnnou zprávu o chybových testech.

Drive Protection System (systém pro ochranu jednotky)

Nástroj DPS (Drive Protection System) je diagnostický nástroj, který je součástí pevných disků nainstalovaných v některých modelech počítačů HP. Systém DPS je navržen tak, aby usnadňoval diagnostiku problémů, které by mohly vést k výměně pevného disku, na kterou se nevztahuje záruka.

Během výroby počítačů HP jsou všechny nainstalované pevné disky otestovány nástrojem DPS a získané klíčové informace jsou trvale zapsány na pevný disk. Výsledky testů jsou na pevný disk zapsány při každém spuštění systému DPS. Poskytovatel služeb může tyto informace použít ke zjištění okolností, za kterých bylo nutné spustit systém DPS. Pokyny k použití nástroje DPS najdete v příručce *Poradce při potížích*.

Napájecí zdroj s ochranou proti přepětí

Integrovaný napájecí zdroj s ochranou proti přepětí poskytuje vyšší spolehlivost při zasažení počítače nepředvídatelným přepětím v napájecí síti. Tento napájecí zdroj vydrží přepětí až 2 000 V, aniž by došlo k prostojům či ztrátě dat.

Tepelné čidlo

Tepelné čidlo je kombinací hardwarové a softwarové technologie, která slouží k monitorování vnitřní teploty počítače. Tato funkce zobrazí zprávu s upozorněním, pokud budou překročeny normálních teplotní hodnoty, a umožní tak včasnou reakci, která může předejít poškození vnitřních součástí počítače nebo ztrátě dat.

△ **UPOZORNĚNÍ:** Při vysokých teplotách může dojít k poškození systému nebo ztrátě dat.

Rejstřík