Ръководство за управление на настолни компютри

Бизнес компютри на HP

Ръководство за управление на настолни компютри

Бизнес компютри на HP

Четвърто издание (септември 2009 г.)

Номенклатурен номер на документа: 581009-261

Информация за настоящото издание

Настоящото ръководство съдържа дефиниции и инструкции за експлоатацията на функциите за сигурност и управление, които са предварително инсталирани на някои модели.

⚠ **ПРЕДУПРЕЖДЕНИЕ!** Обозначеният по този начин текст показва, че неизпълняването на инструкциите може да причини наранявания или смърт.

△ **ВНИМАНИЕ:** Обозначеният по този начин текст показва, че неизпълняването на инструкциите може да причини повреда на оборудването или загуба на информация.

ЗАБЕЛЕЖКА: Обозначеният по този начин текст предоставя важна допълнителна информация.

Съдържание

1 Общ преглед на управлението на настолни компютри

HP Client Management Solutions (Решенията на HP за управление на клиентски компютри) предоставя стандартизирани решения за управление и контрол на настолни компютри, работни станции и преносими компютри в мрежова среда. HP станаха пионери в сферата на управлението на настолни компютри през 1995 година с представянето на първите изцяло управляеми настолни персонални компютри. HP притежава патент за технологията на управление. Оттогава насам HP полага усилия в целия отрасъл за разработването на стандартите и инфраструктурата, необходими за ефективното внедряване, конфигуриране и управление на настолни компютри, работни станции и преносими компютри. HP разработва свой софтуер за управление и работи в тясно сътрудничество с водещите доставчици на софтуерни решения в отрасъла, за да осигури съвместимост между HP Client Management Solutions и техните изделия. HP Client Management Solutions представляват важен момент от нашия общ ангажимент да ви доставяме решения, които помагат за снижаване на общите разходи за притежаване и поддръжка на компютрите през целия им жизнен цикъл.

Основните възможности и функции за управление на настолния компютър са следните:

- Първоначално конфигуриране и инсталиране
- Дистанционно инсталиране на системи
- Актуализация и управление на софтуера
- Флашване на ROM
- Конфигурация на хардуерните опции
- Проследяване на имущество и сигурност
- Уведомяване при грешки и възстановяване

ЗАБЕЛЕЖКА: Поддържането на специфични функции, описани в това ръководство, може да се различава според модела или версията на софтуера.

2 Първоначално конфигуриране и инсталиране

Компютърът се доставя с предварително инсталирано копие на системния софтуер. След бързо „разопаковане” на софтуера компютърът е готов за използване.

Може да предпочетете да замените предварително инсталирания софтуер със системен или приложен софтуер, отговарящ на вашите предпочитания. Има няколко метода за инсталиране на персонализиран пакет от софтуер. Те включват:

- Инсталиране на допълнителни софтуерни приложения след декомпресиране на предварително инсталирания софтуер.
- Ползване на софтуерни средства за внедряване като HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (по технология Radia) за замяна на предварително инсталирания софтуер с персонализиран образ на софтуера.
- Използване на процедура за дисково клониране, за да се копира съдържанието от един твърд диск на друг.

Кой ще е най-добрият метод за инсталиране зависи от съответните информационни технологии и процеси във вашата компания.

ROM-базираното инсталиране и хардуерът ACPI предоставят допълнителна помощ при възстановяването на системния софтуер, управлението на конфигурацията, отстраняването на неизправности и контрола на електрозахранването.

HP Client Automation Agent

Агентът за управление, който се ползва от HP Client Automation Standard Edition и Enterprise Edition, е предварително зареден в компютъра. Когато е инсталиран, той дава възможност за комуникация с конзолата за управление на HP.

За да инсталирате HP Client Automation Agent:

1. Натиснете върху **Старт**.
2. Натиснете върху **Всички програми**.
3. Натиснете върху **HP Manageability** (Управляемост от HP).
4. Щракнете върху **HP Management Agent Readme** според желания от вас език.
5. Прегледайте и следвайте указанията във файла Readme, за да инсталирате HP Client Automation Agent.

HP Client Automation Agent е важен инфраструктурен компонент за включването на всички решения на HP Client Automation. За да научите за другите инфраструктурни компоненти, необходими за реализирането на решенията за управление на конфигурацията на HP, посетете http://h20229.www2.hp.com/solutions/ascm/index.html.

HP Client Manager

HP Client Manager (HPCM) е безплатно решение, разработено от Symantec, за всички поддържани бизнес компютри на HP, настолни и преносими, работни станции и компютри HP Blade. HPCM интегрира специфични за HP инструменти, като System Software Manager, HP Instant Support Professional Edition и HP Client Management Interface, с цел осъществяване на централизиран модел за управление, проследяване и контрол на целия поддържан от HP хардуер.

HP Client Manager 7.0 представя нова портална страница за интегрирано обслужване, където администраторът може да извършва следните управленски дейности:

- Inventory (Инвентар)
- Alerts (Известия)
- BIOS Management (Управление на BIOS)
- Driver Updates (Актуализиране на драйвери)
- Стартиране на HP Instant Support Health Scan and Diagnostics
- Извършване на задания за вградена защита
- Преглед на общото състояние на HP Health Alert Trend за последните 3-6 месеца
- Преглед на общата съвместимост на поддържаните компютри с HP Instant Support Health Scan and Diagnostics.
- Преглед на Summary of HP Computers – структура на поддържаните настолни и преносими компютри, работни станции и компютри HP Blade
- Преглед на известията: Asset (актив), Treshold (праг), Hardware Health (Състояние на хардуера)
- Reports (Отчети)
- Административни задачи за актуализиране на специфични инструменти на HP

Можете да изтеглите HPCM от http://www.symantec.com/business/theme.jsp, като щракнете върху **HP Client Manager** в **Strategic Partner Products**. От страницата за изтегляне можете да получите и постоянен безплатен лиценз.

Видеофайлове с указания за извършване на различни задачи с HPCM се публикуват и на адрес http://www.symantec.com/connect. Потърсете **HP Client Manager 7.0**, за да прегледате видеофайловете с последователни указания за различни задачи в HCPM.

3 Дистанционно инсталиране на системи

Дистанционното инсталиране на системи ви позволява да инсталирате системата с помощта на информацията за софтуера и конфигурацията, разположена на мрежов сървър, чрез стартиране на Preboot Execution Environment (PXE). Функцията „Дистанционно инсталиране на системи“ обикновено служи като инструмент за инсталиране и конфигуриране на системата и може да се използва за следните задачи:

- Форматиране на твърд диск
- Инсталиране на копие от софтуерната конфигурация на един или повече нови компютри
- Дистанционно актуализиране на системния BIOS във флаш ROM паметта (Дистанционна промяна на ROM паметта на страница 14)

ЗАБЕЛЕЖКА: Има инструменти за презапис на системния BIOS направо от операционната система Microsoft Windows.

- Конфигуриране на системните BIOS настройки

За да стартирате Remote System Installation (Дистанционно инсталиране на системи), натиснете F12, когато в долния десен ъгъл на екрана с емблемата на HP се появи съобщението **F12 = Network Service Boot** (F12 = Стартиране от мрежа), когато компютърът зарежда. Следвайте инструкциите на екрана, за да продължите. Редът на стартиране по подразбиране е настройка в BIOS, която може да се промени така, че компютърът винаги да опитва PXE стартиране.

4 Актуализация и управление на софтуер

HP предоставя няколко инструмента за управление и актуализация на софтуера на настолните и преносимите компютри и работните станции:

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, Standard Edition и Enterprise Edition
- HP Client Manager от Symantec
- Altiris Client Management Premium Suite
- HP Client Catalog за Microsoft System Center и продуктите за SMS
- Компютри с марка Intel vPro с Active Management Technology (Технология за активно управление)
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

Независимо от това какви инструменти за системно управление ползва вашият компютърен отдел, управлението и на хардуерните, и на софтуерните активи е важно за снижаване на разходите за компютърна техника и развиване на ефективна дейност. Компютърният администратор може да влезе в интерфейса на HP Client Management, като напише прости скриптове и ги интегрира в избраното решение за управление.

С помощта на HP Client Management Interface (HP CMI) новите компютри от бизнес клас на HP се интегрират безпроблемно във вашата управлявана компютърна среда. HP CMI осигурява интерфейс, който улеснява интегрирането на компютрите от бизнес клас на HP с популярните в отрасъла инструменти за системно управление (включително Microsoft Systems Management Server, IBM Tivoli Software и HP Operations) и разработени за собствени нужди приложения за управление. С помощта на HP CMI инструментите и приложенията за системно управление могат да поискат подробна инвентаризация на клиентите, да получат информация за здравословното

състояние и да управляват настройките на системния BIOS, като общуват направо с клиентския компютър и намаляват нуждата от софтуерен агент или съединител, за да постигнат интеграцията.

HP Client Management Interface е изградено на отраслови стандарти, включващи Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) и Advanced Configuration and Power Interface (ACPI). HP CMI е базова технология, която се ползва в HP Client Management Solutions. С HP CMI HP ви осигурява гъвкавост при избора как да се управляват клиентските компютри на HP.

HP Client Management Interface, ползван заедно със софтуера за системно управление, може да:

- Заяви подробна инвентаризация на клиента — да снеме изчерпателна информация за процесорите, твърдите дискове, паметта, BIOS, драйверите, включително информация от датчиците (напр. скорост на вентилатора, напрежение и температура).
- Получи информация за здравословното състояние — да се абонира за широк набор сигнали за хардуера на клиента (прегряване, блокирал вентилатор, промени в хардуерната конфигурация), които да бъдат изпращани до конзолата за системно управление, до някое приложение или до локалния клиентски компютър. Сигналите се изпращат в реално време, когато се предизвикат от хардуерни събития.
- Управлява системните BIOS настройки — да извършва F10 функции, включително задаване и промяна на BIOS паролите и реда на първоначално зареждане на устройствата дистанционно от конзолата за управление на сървъра за всяка от клиентските системи, без да има нужда да се посещава всяка машина.

За повече информация по интерфейса на HP Client Management посетете http://www.hp.com/go/hpcmi/.

HP SoftPaq Download Manager

HP SoftPaq Download Manager е безплатен и лесен за ползване интерфейс за намиране и изтегляне на актуализации за софтуера за клиентски компютри на HP във вашата среда. Като посочите моделите, операционната система и езика, можете лесно да намерите необходимите актуализации. За да изтеглите HP SoftPaq Download Manager, посетете http://www.hp.com/go/sdm.

HP System Software Manager

HP System Software Manager (SSM) е безплатна помощна програма, която автоматизира дистанционното инсталиране на драйверите и осъвременяването на BIOS на вашите свързани в мрежа бизнес компютри от HP. Когато SSM се стартира, тя автоматично (без участието на потребителя) определя актуалността на драйверите и BIOS-а, инсталирани на всяка от клиентските компютърни системи в мрежата, и сравнява този списък със списъка на системните SoftPaqs, изпитани и запазени на централния файлов архив. След това, при установено различие, SSM автоматично обновява системния софтуер с най-новите версии, запазени във файловия архив. Тъй като единствената функция на SSM е да позволява на обновените SoftPaq да достигнат до съответните клиентски компютърни системи, администраторите могат уверено и ефективно да използват SSM, за да подсигуряват навременното обновяване на системния софтуер.

System Software Manager се интегрира с такива инструменти за разпространение на софтуер в организации като решенията HP Client Automation, HP Client Manager от Symantec и Microsoft Systems Management Server (SMS). Използвайки SSM, вие можете да разпространявате

файлове, специално създадени за обновяване на системите, които са запазени във формата на SSM.

Можете да изтеглите SSM безплатно, като посетите http://www.hp.com/go/ssm.

ЗАБЕЛЕЖКА: Засега SSM не поддържа дистанционен презапис на ROM в системи с Windows с включена система за шифроване на устройства BitLocker, ползващи TPM мерки за защита на BitLocker ключовете, тъй като презаписването на BIOS би направило невалиден надеждния подпис, създаден от BitLocker за платформата. За да презапишете системния BIOS, изключете BitLocker от груповите правила.

Можете да включите поддръжката за BitLocker без TPM измервания от BIOS, за да избегнете анулиране на ключовете за BitLocker. HP ви препоръчва да пазите на сигурно място резервно копие от идентификационните данни за BitLocker в случай на аварии при възстановяване.

HP ProtectTools Security Manager

Защитният софтуер HP ProtectTools предоставя защитни функции в помощ срещу неоторизиран достъп до компютъра, мрежите и критично важни данни. Допълнителна защитна функционалност, достъпна от HP ProtectTools Security Manager, се предоставя от следните софтуерни модули:

HP ProtectTools Security Manager е основната конзола за достъп до всички останали модули.

- Credential Manager за HP ProtectTools
- Drive Encryption за HP ProtectTools
- Privacy Manager за HP ProtectTools
- File Sanitizer за HP ProtectTools
- Java Card Security за HP ProtectTools
- Embedded Security за HP ProtectTools
- Device Access Manager за HP ProtectTools
- LoJack Pro за HP ProtectTools

HP ProtectTools може да се ползва в две предоставени версии: HP ProtectTools Security Manager (потребителска версия) и HP ProtectTools Administrative Console (администраторска версия). Както администраторската, така и потребителската версия са достъпни от менюто **Старт** > **Всички програми**.

Софтуерните модули, налични за вашия компютър, може да се различават в зависимост от вашия модел. Embedded Security за HP ProtectTools например е наличен само за компютри с инсталиран чип за защита Trusted Platform Module (TPM).

Модулите на HP ProtectTools могат да бъдат предварително инсталирани, предварително заредени или достъпни за изтегляне от уебсайта на HP. За отделни настолни компютри HP Pro HP ProtectTools се предлага допълнително след закупуване. Посетете http://www.hp.com/products/security за повече информация.

HP Client Automation Starter Edition и Standard Edition

HP Client Automation е решение за управление на хардуер и софтуер за средите Windows Vista, Windows XP и HP Thin Client, което се ползва лесно и внедрява бързо, като същевременно осигурява стабилна база за бъдещи потребности. То се предлага в две издания:

- Starter Edition е безплатен продукт за управление на настолни компютри, преносими компютри и работни станции на HP, който осигурява инвентаризация на хардуера и софтуера, дистанционно управление, следене на сигналите на HP, актуализации на HP BIOS и драйвери, интеграция с HP Protect Tools и поддържане на добавки за Intel AMT. Starter Edition поддържа също така внедряване и управление на HP Thin Clients.
- Standard Edition се закупува допълнително и включва всички функции на Starter Edition, като добавя внедряване и миграция на Windows, възможности за управление на корекциите, разпространение на софтуер и измерване ползването на софтуера.

HP Client Automation Starter Edition и Standard Edition осигуряват път за мигриране до HP Client Automation Enterprise Edition (по технология Radia) за автоматизирано управление на големи, хетерогенни и постоянно променящи се компютърни среди.

За повече информация за решенията на HP Client Automation посетете http://www.hp.com/go/client.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition е базирано на правилници решение, което позволява на администраторите да инвентаризират, внедряват, инсталират корекции и непрекъснато да управляват софтуера и съдържанието в хетерогенни клиентски платформи. С HP Client Automation Enterprise Edition компютърният специалист може:

- да автоматизира целия процес на управление на жизнения цикъл от откриването, внедряването и текущото управление до миграцията и бракуването
- автоматично да внедрява и непрекъснато да управлява цялата съвкупност от софтуер (операционни системи, приложения, корекции, настройки и съдържание) до желаното състояние
- да управлява софтуера на практически всяко едно устройство, включително настолни компютри, работни станции и преносими компютри в хетерогенна или самостоятелна инфраструктура
- да управлява софтуера на повечето операционни системи

С непрекъснатото управление на конфигурацията клиентите на HP съобщават за значителни икономии на компютърни разходи, намалено време за излизане на пазара за софтуер и съдържание и увеличена производителност и удовлетворение на потребителя.

За повече информация за решенията на HP Client Automation посетете http://www.hp.com/go/client.

HP Client Manager от Symantec

HP Client Manager от Symantec, разработен съвместно с Altiris, се предлага безплатно на всички произведени от HP бизнес компютри, настолни и преносими, и работни станции. SSM е вграден

в HP Client Manager и позволява централно проследяване, наблюдение и управление на хардуерните аспекти на клиентските системи на HP.

Използвайте HP Client Manager от Symantec да:

- Получите ценна хардуерна информация, като информация за настройките на процесора, паметта, видеокартата или защитата на компютъра
- Наблюдавате състоянието на системата и да разрешавате проблемите, дори преди да се появят
- Автоматично изтегля и инсталира драйвери и актуализации за BIOS, без да се посещава всеки компютър
- Конфигурирате BIOS и настройките на защитата дистанционно
- Автоматизирате процесите, за да разрешавате по-бързо хардуерните проблеми

Тясната интеграция с инструментите HP Instant Support намалява времето, необходимо за отстраняване на хардуерни проблеми.

- Диагностика — дистанционно стартиране и преглед на справки за настолни модели, преносими модели и работни станции на HP
- Сканиране на системното здраве — проверка за известни проблеми с хардуера във вашата инсталирана база на клиентски системи на HP
- Активен чат — свързвате се с поддръжката за клиенти на HP, за да решавате проблеми
- База знания на HP — връзка към експертна информация
- Автоматична процедура за събиране и доставка на SoftPaq за бързо разрешаване на хардуерни проблеми
- Разпознаване, инвентаризирани и инициализиране на системи с вграден чип за защита HP ProtectTools
- Опция сигналите за здравето на системата да се появяват локално на клиентската система
- Съобщаване на основна инвентарна информация за клиенти, които не са HP
- Инсталиране и конфигуриране на защитния чип TPM
- Централно насрочване на резервно копиране и възстановяване за клиенти
- Добавяне на поддръжка за управление на Intel AMT

За повече информация по HP Client Manager от Symantec посетете http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite е лесно за ползване решение за пълния жизнен цикъл на управлението на софтуера на настолни и преносими компютри и работни станции. Client Management Suite включва следните продукти на Altiris:

- Inventory Solution (решение за инвентаризация)
- Deployment Solution (решение за внедряване)

- Software Delivery Solution (решение за доставка на софтуер)
- Patch Management Solution (решение за управление на поправките)
- Application Metering Solution (решение за измерване на производителността на софтуера)
- Application Management Solution (решение за управление на приложенията)
- Решение Carbon Copy

За повече информация по Altiris Client Management Suite посетете http://www.symantec.com/business/client-management-suite.

HP Client Catalog за Microsoft System Center и продуктите за SMS

HP Client Catalog позволява на компютърните специалисти, използващи продукти на Microsoft, да автоматизират внедряването на актуализации за софтуер на HP (Softpaqs) в бизнес компютри на HP. Каталожният файл съдържа подробна информация за платформата на HP бизнес настолни компютри, преносими компютри и работни станции. Той може да се ползва заедно с потребителските функции за инвентаризация и актуализация на продуктите на Microsoft, за да осигури автоматизирани актуализации на драйверите и корекции на управляваните клиентски компютри на HP.

Продуктите на Microsoft, поддържани от HP Client Catalog, включват:

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

За повече информация по HP Client Catalog за SMS посетете http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

Технология за дистанционно управление

Моделите включват или технология vPro, или стандартна технология. И двете позволяват по-добро откриване, лекуване и защита на мрежовите компютърни активи. И двете технологии позволяват компютрите да бъдат управлявани, когато системата е включена, изключена или при блокирала операционна система.

Трите форми за дистанционно управляване за настолни бизнес компютри са Alert Standard Format (ASF), Intel Active Management Technology (AMT) и Desktop and mobile Architecture for Systems Hardware (DASH).

Функциите на технологията за дистанционно управление включват:

- Откриване на мрежи
- Информация за хардуерния инвентар
- Наблюдение на състоянието на платформите
- Управление на захранването — включване и изключване, цикли на включване и изключване

- Дистанционна диагностика и ремонт
  - Пренасочване на текстовата конзола – позволява контролиране на конзолата на отдалечения компютър по време на зареждането му.
  - Пренасочване на носители – позволява зареждане на системата от отдалечено стартово устройство. Двата варианта за това са IDE-Redirect (IDE-R) (Пренасочване на IDE) при платформи AMT и USB Media Redirection (Пренасочване на USB носител).
- Хардуерно изолиране и възстановяване — ограничаване или спиране на достъпа до мрежата при засичане на дейност, подобна на вирус
- Проследяване и проверка на събитията в платформата
- Интегриран портал за управление на уеб сървър за отдалечен достъп и конфигуриране.
- Технологиите за дистанционно управление са интегрирани с партньорските конзоли за управление на HP.

ЗАБЕЛЕЖКА: Не всички функции по-горе са налице за всички платформи.

Конфигуриране на Management Engine (Машина за управление) на Intel

ЗАБЕЛЕЖКА: За общо запознаване с технологията Intel vPro посетете http://www.intel.com/vpro.

За информация по технологията Intel vPro, която е специфична за HP, вижте техническите описания на адрес http://www.hp.com/support. Изберете вашата държава и език, изберете **See support and troubleshooting information** (Вижте информация за поддръжка и отстраняване на неизправности), въведете номера на модела и натиснете Enter. В категорията **Resources** (Ресурси) щракнете върху **Manuals (guides, supplements, addendums, etc.)** (Наръчници (ръководства, притурки, приложения и т.н.)). В **Quick jump to manuals by category** (Бърз преход към наръчници по категория) щракнете върху **White papers** (Технически документи).

Наличните технологии на управление включват:

- AMT (включва DASH 1.0)
- ASF
- DASH 1.1 (с ползване на Broadcom NIC)

ASF и AMT не могат да се конфигурират по едно и също време, но и двете се поддържат.

За да конфигурирате системи Intel vPro за AMT или ASF:

1. Включете или рестартирайте компютъра. Ако сте в Microsoft Windows, щракнете върху **Старт** > **Изключване** > **Рестартиране**.
2. Веднага след включването на компютъра натиснете активния клавиш Ctrl+P, преди компютърът да зареди операционната система.

   ЗАБЕЛЕЖКА: Ако не успеете да натиснете клавиша Ctrl+P в подходящия момент, за да влезете в помощната програма, ще трябва да рестартирате компютъра, след което пак да натиснете клавиша Ctrl+P, преди компютърът да зареди операционната система, за да влезете в помощната програма.

Този активен клавиш стартира помощната програма за настройка Intel Management Engine BIOS Execution (MEBx). Тази помощна програма позволява на потребителя да конфигурира различни страни от технологията за управление. Някои от опциите за конфигурация са дадени по-долу:

- Главно меню
  - Intel ® ME Configuration (Конфигурация на Intel ® ME)
  - Intel ® AMT Configuration (Конфигурация на Intel ® AMT)
  - Change Intel ® ME Password (Промяна на паролата на Intel ® ME)
  - Exit (Изход)
- Intel ® ME Platform Configuration (Конфигурация на платформа Intel ® ME)
  - Intel ® ME State Control (Контрол на състоянието на Intel ® ME) (разреши/забрани)
  - Intel ® ME Firmware Local Update (Локално актуализиране на Intel ® ME фърмуер) (разреши/забрани)
  - Intel ® ME Features Control (Контрол на функциите на Intel ® ME)
  - Intel ® ME Power Control (Контрол на захранването на Intel ® ME)
- Intel ® AMT Configuration (Конфигурация на Intel ® AMT)
  - Host Name (Име на хост)
  - TCP/IP
  - Provision Model (Модел на обслужване) (Enterprise, SMB)
  - Setup and Configuration (Настройка и конфигурация)
  - Un-Provision (Прекратяване на обслужването)
  - SOL/IDE-R (разреши/забрани)
  - Password Policy (Правила за паролите)
  - Secure Firmware Update (Защитена актуализация на фърмуер) (разреши/забрани)
  - Set PRTC (Задаване на PRTC)
  - Idle Timeout (Срок на бездействие)
- Change Intel ® ME Password (Промяна на паролата на Intel ® ME) (HP силно препоръчва тази парола да се смени. Стандартната парола е **admin**.)

За да могат да се управляват дистанционно AMT системи, администраторът трябва да ползва дистанционна конзола, която поддържа AMT. Конзоли за фирмено управление се предлагат от доставчици като HP, Altiris и Microsoft SMS. В режим SMB клиентът осигурява интерфейс на уеб браузър. За да ползвате тази функция, отворете браузър от всяка друга система в мрежата и въведете `http://host_name:16992` където `host_name` е мрежовото име, дадено на системата. Друг вариант е да се ползва IP адресът вместо мрежовото име.

За да конфигурирате системи с NIC с функции за Broadcom DASH

Проверете актуалната документация на сайта http://www.hp.com в **Поддръжка и отстраняване на неизправности**, посочете своя модел, изберете **Manuals** (Наръчници) и **White papers** (Технически документи) за DASH или Broadcom NIC.

Verdiem Surveyor

Verdiem Surveyor е софтуерно решение в помощ на управлението на енергийните разходи на компютрите. Surveyor измерва и докладва енергийния разход на всеки компютър. То осигурява още контрол над настройките на захранването на компютъра, като позволява на администраторите с лекота да прилагат стратегии за пестене на енергия в мрежите си. Можете да свалите HP SoftPaq, съдържащ агента Surveyor, и да го инсталирате на поддържаните комерсиално модели настолни компютри. Лицензи за Surveyor за управление на компютри можете да закупите от своя представител на HP.

HP Proactive Change Notification

Програмата Proactive Change Notification (Проактивно уведомяване при промени) използва уебсайта „Subscriber's Choice” (избор на абоната), за да прави автоматично следните неща:

- Изпращане (до 60 дни предварително) на електронни съобщения от Proactive Change Notification (PCN), уведомяващи за промени в хардуера и софтуера на повечето компютри и сървъри, предназначени за търговски цели.
- Да изпраща електронни съобщения с бюлетини за клиенти, за защитата, бележки и уведомявания за драйвери за повечето търговски компютри и сървъри.

Вие създавате ваш собствен профил, за да сте сигурни, че само вие получавате информацията за определена ИТ среда. За да научите повече за програмата за проактивно уведомяване при промени и да си създадете профил по избор, посетете http://h30046.www3.hp.com/subhub.php

изборът на абоната

изборът на абоната (Subscriber’ s Choice) е услуга за потребителите на HP.

На базата на вашия профил, HP ще ви предоставя персонализирани съвети за продукти, актуални статии и/или уведомявания/предупреждения за поддръжка и драйвери.

Услугата Subscriber’s Choice Driver and Support Alerts/Notifications (Уведомления/предупреждения относно поддръжката и драйвери от сайта Subscriber’s Choice) ще изпраща имейл съобщения, чрез които ще ви уведомява, че информацията, за която сте се абонирали в профила си, е налична за преглед и изтегляне. За да научите повече за Subscriber’s Choice (Избора на абоната) и да създадете профил по избор, посетете http://h30046.www3.hp.com/subhub.php.

Остарели решения

Двата софтуерни пакета Altiris Local Recovery и Dantz Retrospect вече няма да се доставят с бизнес моделите на HP за настолни и преносими компютри и работни станции.

5 промяна на ROM паметта

BIOS на компютъра се съхранява в програмируем флаш ROM (памет само за четене). Можете да защитите ROM от неволно актуализиране или презапис, като създадете парола за настройки в помощната програма Computer Setup (Настройка на компютъра) (F10). Това е важно за осигуряване на оперативната цялост на компютъра. Ако е необходимо да актуализирате BIOS, можете да свалите актуални образи на BIOS от страницата за драйвери и поддръжка на HP: http://www.hp.com/support/files.

△ **ВНИМАНИЕ:** За максимална защита на ROM се погрижете да зададете парола за настройки. Паролата за настройки предотвратява неоторизирано актуализиране на BIOS. System Software Manager позволява системният администратор да зададе парола за настройки на един или няколко компютъра едновременно. За повече информация посетете http://www.hp.com/go/ssm.

Дистанционна промяна на ROM паметта

Дистанционната промяна на ROM паметта позволява на системните администратори спокойно да актуализират BIOS на отдалечени компютри на HP направо от централизирана конзола за управление на мрежата. Когато системните администратори могат да извършват тази дейност дистанционно върху много компютри, това осигурява съгласувано внедряване и по-голям контрол върху образите на BIOS на компютрите HP в мрежата. Това също увеличава продуктивността и намалява разходите.

ЗАБЕЛЕЖКА: Засега SSM не поддържа дистанционен презапис на ROM в системи с Windows с включена система за шифроване на устройства BitLocker, ползващи TPM мерки за защита на BitLocker ключовете, тъй като презаписването на BIOS би направило невалиден надеждния подпис, създаден от BitLocker за платформата. За да презапишете системния BIOS, изключете BitLocker от груповите правила.

Компютърът трябва да е включен от бутона за захранване или чрез Remote Wakeup (Дистанционно включване), за да се използва Remote ROM Flash (Дистанционна промяна на ROM паметта).

За повече информация за дистанционния презапис на ROM вижте HP Client Manager Software или System Software Manager на адрес http://www.hp.com/go/ssm/.

HPQFlash

Помощната програма HPQFlash се използва за актуализиране и възстановяване на системната BIOS памет на отделни компютри посредством операционната система Windows.

За повече информация за HPQFlash посетете http://www.hp.com/support/files и при поискване въведете номера на модела на компютъра.

6 Режим на аварийно възстановяване на блока за първоначално зареждане

Режимът за аварийно възстановяване на блока за първоначално зареждане позволява възстановяване на системата при малко вероятния случай на неуспешна промяна на ROM паметта. Например, ако спре захранването при актуализация на BIOS, промяната на ROM паметта няма да бъде пълна. Това ще направи системната BIOS неизползваема. Блокът за първоначално зареждане е защитена от промяна част от ROM паметта, която съдържа програма, проверяваща дали BIOS образът е валиден, когато системата бъде включена.

- Ако образът на системната BIOS е валиден, системата стартира нормално.
- Ако системният образ на BIOS не е валиден, безопасна Boot Block BIOS осигурява достатъчно функции, за да се търсят файлове с образи на BIOS по преносими носители. Ако бъде намерен подходящ образ на BIOS, той автоматично се записва в ROM паметта.

Когато бъде засечен невалиден образ на системната BIOS, индикаторът за захранване на системата ще мига червено 8 пъти, веднъж на всяка секунда. Едновременно с това високоговорителят ще издаде 8 звукови сигнала. Ако частта от системната ROM памет, съдържаща ROM паметта за видеоразширението не е повредена, на екрана ще се покаже **Boot Block Emergency Recovery Mode** (Авариен режим за възстановяване на блока за първоначално зареждане).

За да възстановите системата, след като тя влезе в авариен режим за възстановяване на блока за първоначално зареждане, изпълнете следните стъпки:

1. Изключете захранването.
2. Поставете компактдиск или USB флаш устройство, което съдържа желания файл с образ на BIOS в главната си директория.

   ЗАБЕЛЕЖКА: Носителят трябва да бъде форматиран с файлове система FAT12, FAT16 или FAT32.

3. Включете компютъра.

   Ако не бъде намерен подходящ образ на BIOS, ще получите указание да поставите носител, съдържащ файл с образ на BIOS.

   Ако системата успешно препрограмира ROM паметта, тя автоматично ще се изключи.

4. Извадете използвания носител за актуализация на BIOS.
5. Включете захранването, за да рестартирате компютъра.

ЗАБЕЛЕЖКА: Защитеното стартиране не позволява Windows Vista да се зареди, когато компактдиск, съдържащ файла с образ на BIOS, се намира в оптичното устройство. Ако защитеното стартиране е включено, извадете този компактдиск, преди да се опитате да заредите Windows Vista.

7 Копиране на настройките

Следните процедури дават на администраторите възможност лесно да копират настройките от една конфигурация на друга при едни и същи модели. Така конфигурацията на много компютри е по-постоянна и по-бърза.

ЗАБЕЛЕЖКА: И двете процедури изискват флопидисково устройство или поддържано USB флаш устройство.

ЗАБЕЛЕЖКА: System Software Manager (SSM) може да се ползва за дублиране на информацията за настройката на компютъра направо от операционната система Windows. За повече информация вижте ръководството за потребителя на SSM на адрес http://www.hp.com/go/ssm.

Копиране на един компютър

ВНИМАНИЕ: Всяка конфигурация на настройките е специфична за модела. Файловата система може да се повреди, ако компютрите не са един и същ модел. Например не копирайте настройките от компютър dc7xxx на dx7xxx.

1. Изберете конфигурация за копиране. Изключете компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Изключване**.
2. Ако използвате USB устройство с флаш памет, поставете го сега.
3. Включете компютъра.
4. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

   ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.
5. Ако използвате дискета, поставете я.
6. Щракнете върху **Файл** > **Replicated Setup** (Копирани настройки) > **Save to Removable Media** (Запис върху сменяем носител). Следвайте инструкциите на екрана, за да създадете дискетата или USB флаш устройството с конфигурацията.
7. Изключете компютъра, който конфигурирате, и поставете дискетата или USB флаш устройството с конфигурацията.
8. Включете компютъра, който ще конфигурирате.

9. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

10. Щракнете върху **Файл** > **Replicated Setup** (Копирани настройки) > **Restore from Removable Media** (Възстановяване от сменяем носител) и следвайте указанията на екрана.

11. Рестартирайте компютъра, когато конфигурацията завърши.

Копиране на много компютри

△ **ВНИМАНИЕ:** Всяка конфигурация на настройките е специфична за модела. Файловата система може да се повреди, ако компютрите не са един и същ модел. Например не копирайте настройките на конфигурацията от компютър dc7xxx на компютър dx7xxx.

Този метод отнема повече време за подготовка на дискетата или USB флаш устройството с конфигурацията, но копирането на останалите компютри е значително по-бързо.

ЗАБЕЛЕЖКА: За тази процедура е нужна стартираща дискета или създаването на стартиращо USB флаш устройство. Ако нямате Windows XP, за да създадете стартираща дискета, използвайте метода за копиране на един компютър (вж. Копиране на един компютър на страница 17).

1. Създайте стартираща дискета или USB флаш устройство. Вж. Поддържано USB флаш устройство на страница 19 или Неподдържано USB флаш устройство на страница 20.

   △ **ВНИМАНИЕ:** Не всички компютри могат да стартират от USB флаш устройство. Ако редът на стартиране в Computer Setup показва USB устройство като възможност, компютърът може да стартира от USB флаш устройство. В противен случай трябва да се използва стартираща дискета.

2. Изберете конфигурация за копиране. Изключете компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Изключване**.

3. Ако използвате USB устройство с флаш памет, поставете го сега.

4. Включете компютъра.

5. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

   ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

6. Ако използвате дискета, поставете я.

7. Щракнете върху **Файл** > **Replicated Setup** (Копирани настройки) > **Save to Removable Media** (Запис върху сменяем носител). Следвайте инструкциите на екрана, за да създадете дискетата или USB флаш устройството с конфигурацията.

8. Изтеглете BIOS програмата за копиране на настройките (repset.exe) и я копирайте на дискетата или USB флаш устройството с конфигурацията. За да получите тази помощна програма, отидете на http://welcome.hp.com/country/us/en/support.html и въведете номера на модела на компютъра.

9. Върху дискетата или USB флаш устройството създайте файл autoexec.bat със следната команда:

   ```
   repset.exe
   ```

10. Изключете компютъра, който ще конфигурирате. Поставете дискетата или USB флаш устройството и включете компютъра. Програмата за конфигуриране ще стартира автоматично.

11. Рестартирайте компютъра, когато конфигурацията завърши.

Създаване на стартиращо устройство

Поддържано USB флаш устройство

Поддържаните устройства имат предварително инсталиран образ, за да се опрости процесът на превръщането им в стартиращи. Всички устройства HP или Compaq, както и повечето от другите USB флаш устройства, имат такъв предварително инсталиран образ. Ако използваното USB флаш устройство няма такъв образ, ползвайте процедурата, описана по-долу в този раздел (вж. Неподдържано USB флаш устройство на страница 20).

За да създадете стартиращо USB флаш устройство, трябва да имате:

- устройство, което поддържа USB флаш медия.
- стартираща под DOS дискета, на която са записани програмите FDISK и SYS (Ако нямате SYS, можете да използвате FORMAT, но файловете, които са записани на USB флаш устройството, ще бъдат изгубени.)
- компютър, който може да стартира от USB флаш устройство

△ **ВНИМАНИЕ:** Възможно е някои по-стари модели компютри да не могат да стартират от USB флаш устройство. Ако редът на стартиране в Computer Setup показва USB устройство като възможност, компютърът може да стартира от USB флаш устройство. В противен случай трябва да се използва стартираща дискета.

1. Изключете компютъра.

2. Включете USB флаш устройството в един от USB портовете на компютъра и изключете всички останали USB устройства за съхранение без USB флопидисковите.

3. Поставете стартираща дискета с DOS с програмите FDISK.COM и SYS.COM или FORMAT.COM и включете компютъра, за да стартира от DOS дискетата.

4. Стартирайте FDISK от показалеца **A:**, като наберете `FDISK` и натиснете Enter. Ако се появи съобщение, натиснете **Yes** (Да) (**Y**), за да разрешите поддръжка на големи дискове.

5. Въведете избор [`5`], за да се покажат устройствата в системата. USB флаш устройството, ще бъде устройството, чийто размер донякъде съответства на едно от показаните устройства. Това обикновено е последното устройство от списъка. Отбележете буквата на устройството.

   USB флаш устройство: _____

△ **ВНИМАНИЕ:** Ако показаният диск не съответства на USB флаш устройство, не продължавайте. Може да се изтрият данни. Проверете всички останали USB портове за допълнителни устройства за съхранение. Ако има такива, изключете ги, рестартирайте компютъра и продължете към стъпка 4. Ако няма такива, системата не поддържа USB флаш устройство или то е повредено. НЕ правете USB флаш устройството стартиращо.

6. Излезте от FDISK, като натиснете клавиш Esc, за да се върнете към показалеца **A:**.
7. Ако на стартиращата дискета има SYS.COM, преминете към стъпка 8. В противен случай преминете към стъпка 9.
8. На показалеца **A:** въведете `SYS x:`, където x е отбелязаната по-горе буква на устройството.

△ **ВНИМАНИЕ:** Уверете се, че сте въвели правилната буква за USB флаш устройството.

След като бъдат прехвърлени системните файлове, SYS ще се върне към показалеца **A:**. Преминете към стъпка 13.

9. Копирайте файловете от USB флаш устройството, които искате да запазите, във временна директория на друго устройство (например на твърдия диск на системата).
10. На показалеца **A:** въведете `FORMAT /S X:`, където `X` е отбелязаната по-горе буква на устройството.

△ **ВНИМАНИЕ:** Уверете се, че сте въвели правилната буква за USB флаш устройството.

FORMAT ще покаже едно или няколко съобщения, които ви питат дали искате да продължите. Всеки път въвеждайте `Y`. FORMAT ще форматира USB флаш устройството, ще добави системни файлове и ще попита за етикет на диска.

11. Натиснете клавиша Enter, ако не искате етикет, или въведете такъв.
12. Копирайте записаните файлове от стъпка 9 обратно в USB флаш устройството.
13. Извадете дискетата и рестартирайте компютъра. Компютърът ще се рестартира с USB флаш устройството, което ще е с буквата C.

ЗАБЕЛЕЖКА: Редът на стартиране е различен при различните компютри и може да се промени в помощната програма Computer Setup (F10) (Настройка на компютъра).

Ако сте използвали DOS версия от Windows 9x, може да се появи екран с емблемата на Windows. Ако не искате този екран, добавете файл с нулев размер LOGO.SYS в главната директория на USB флаш устройството.

Върнете се на Копиране на много компютри на страница 18.

Неподдържано USB флаш устройство

За да създадете стартиращо USB флаш устройство, трябва да имате:

- устройство, което поддържа USB флаш медия
- стартираща под DOS дискета, на която са записани програмите FDISK и SYS (Ако нямате SYS, можете да използвате FORMAT, но файловете, които са записани на USB флаш устройството ще бъдат изгубени.)
- компютър, който може да стартира от USB флаш устройство

△ **ВНИМАНИЕ:** Възможно е някои по-стари модели компютри да не могат да стартират от USB флаш устройство. Ако редът на стартиране в Computer Setup показва USB устройство като възможност, компютърът може да стартира от USB флаш устройство. В противен случай трябва да се използва стартираща дискета.

1. Ако в системата има PCI карти, към които са включени SCSI, ATA RAID или SATA устройства, изключете компютъра и извадете кабела от контакта.

   △ **ВНИМАНИЕ:** Кабелът за захранване ТРЯБВА да е изключен.

2. Отворете компютъра и извадете PCI платките.
3. Включете USB флаш устройството в един от USB портовете на компютъра и изключете всички останали USB устройства за съхранение без USB флопидисковите. Затворете капака на компютъра.
4. Включете кабела и компютъра.
5. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

   ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

6. Отидете на **Advanced** (Разширени) > **PCI Devices** (PCI устройства), за да забраните PATA и SATA контролерите. При забраняване на SATA контролера отбележете IRQ, което се задава на контролера. По-късно отново ще трябва да зададете IRQ. Излезте от програмата, като потвърдите промените.

   SATA IRQ: _____

7. Поставете стартираща дискета с DOS с програмите FDISK.COM и/или SYS.COM или FORMAT.COM и включете компютъра, за да стартира от дискетата.
8. Изпълнете FDISK и изтрийте съществуващите дялове на USB флаш устройството. Създайте нов дял и го маркирайте като активен. Излезте от FDISK, като натиснете клавиша Esc.
9. Ако системата не стартира автоматично при изход от FDISK, натиснете клавиша Ctrl+Alt+Del за рестартиране от дискетата с DOS.
10. На показалеца **A:** въведете `FORMAT C: /S` и натиснете Enter. Format ще форматира USB флаш устройството, ще добави системни файлове и ще попита за етикет на диска.
11. Натиснете клавиша Enter, ако не искате етикет, или въведете такъв.
12. Изключете компютъра и извадете щепсела от контакта. Отворете компютъра и отново инсталирайте PCI платките, които преди това сте извадили. Затворете капака на компютъра.
13. Включете кабела за захранване на компютъра, извадете дискетата и включете компютъра.
14. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

15. Отидете на **Advanced** (Разширени) > **PCI Devices** (PCI устройства) и отново разрешете PATA и SATA контролерите, които забранихте в стъпка 6. Задайте първоначалното IRQ на SATA контролера.

16. Запишете промените и излезте. Компютърът ще се рестартира с USB флаш устройството, което ще е с буквата C.

ЗАБЕЛЕЖКА: Последователността на зареждане по подразбиране е различна за различните компютри и може да се променя от помощната програма Computer Setup (Настройка на компютъра) (F10). За инструкции вижте *Помощна програма Computer Setup (Настройка на компютъра) (F10)*

Ако сте използвали DOS версия от Windows 9x, може да се появи екран с емблемата на Windows. Ако не искате този екран, добавете файл с нулев размер LOGO.SYS в главната директория на USB флаш устройството.

Върнете се на Копиране на много компютри на страница 18.

8 Двупозиционен бутон за захранване

Ако Advanced Configuration and Power Interface (Интерфейс за разширена конфигурация и електроенергия) е разрешен, бутонът за захранване може да функционира като бутон за вкл./изкл. или като бутон за режим на готовност. Функцията за готовност не изключва изцяло захранването, а поставя компютъра в режим с ниско енергопотребление. Това ви позволява бързо да изключвате компютъра, без да затваряте приложенията, и после бързо да се върнете към тях, без да губите никакви данни.

За да промените конфигурацията на бутона за захранване, изпълнете следните стъпки:

1. Щракнете с левия клавиш върху бутона **Старт**, изберете **Контролен панел** > **Power Options** (Опции на захранването).
2. В **Power Options Properties** (Свойства на опциите на захранването), изберете раздела **Advanced** (Разширени).
3. В раздела **Power Button** (Бутон на захранването) изберете **Stand by** (Готовност).

След като конфигурирате бутона за захранване да работи като бутон за състояние на готовност, натиснете го, за да може компютърът да превключи на този режим. Натиснете бутона отново за бързо превключване в нормален режим. За да изключите изцяло захранването от компютъра, натиснете и задръжте бутона за четири секунди.

△ **ВНИМАНИЕ:** Не използвайте бутона за захранване за изключване на системата, освен ако тя е блокирала; изключването без помощта на операционната система може да повреди или изтрие данни от твърдия диск.

9 Поддръжка през уебсайта на HP

Инженерите на HP полагат усилия за тестването и отстраняването на неизправности в разработения от HP, както и от други доставчици, софтуер. Те разработват специфичен софтуер за поддръжка на операционни системи, за да гарантират производителността, съвместимостта и надеждността за всички компютри на HP.

Когато преминавате на нова или актуализирана операционна система, важно е да се използва съответният софтуер за поддръжка на тази операционна система. Ако възнамерявате да работите с версия на Microsoft Windows, която е различна от включената към компютъра, трябва да инсталирате съответните драйвери и помощни програми, за да сте сигурни, че всички функции се поддържат и работят правилно.

HP облекчи задачата за намиране, достъп, оценяване и инсталиране на последните актуализации на софтуера за поддръжка. Можете да изтеглите софтуера от http://www.hp.com/support.

Уебсайтът съдържа последните драйвери, помощни програми и ROM копия, които са необходими, за да работи последната операционна система Microsoft Windows на компютър на HP.

10 Отраслови стандарти

Решенията за управление на HP се интегрират с други приложения за системно управление и се базират на отраслови стандарти като:

- Web-базирано корпоративно управление (WBEM)
- Интерфейс за управление на Windows (WMI)
- Технология „Wake on LAN”
- ACPI
- SMBIOS
- Поддръжка на изпълнение преди стартиране (Pre-boot Execution)

11 Проследяване на активи и защита

Вградените в компютъра функции за проследяване на активи предоставят ключови данни за активите, които могат да се управляват с помощта на софтуера HP Systems Insight Manager, HP Client Manager, решението HP Configuration Management, HP Client Configuration Manager или други подобни приложения за системно управление. Безпроблемното автоматично интегриране между тези функции за проследяване на активи и продуктите ви позволяват да изберете инструмента за управление, който е най-подходящ за съответната среда и съответно да се възползвате от направените инвестиции в наличния инструментариум.

HP предлага също така някои решения за контролиране на достъпа до ценни компоненти и информация. HP Embedded Security for ProtectTools, ако е инсталиран, предотвратява неоторизиран достъп до данни, проверява целостността на системата и удостоверява външни потребители, които се опитват да получат достъп до системата. (За повече информация вижте *Ръководството за HP ProtectTools Security Manager* на http://www.hp.com/products/security.) Функциите за защита, каквито са HP Embedded Security for ProtectTools, интелигентният датчик и интелигентната ключалка на капака, с които са снабдени някои модели, помагат за предотвратяването на неоторизиран достъп до вътрешните компоненти на персоналния компютър. Като забраните паралелните, серийните или USB портове или възможността за стартиране от сменям носител, можете да защитите ценни активи на данни. Уведомяванията за смяна на памет или от интелигентния датчик на капака може автоматично да се препращат към приложения за системно управление за проактивно уведомяване при достъп до вътрешните компоненти на компютъра.

ЗАБЕЛЕЖКА: HP Embedded Security за ProtectTools, интелигентният датчик и интелигентната ключалка на капака се предлагат като допълнения за някои системи.

Използвайте следните помощни програми, за да управлявате настройките за защита на компютъра на HP:

- Локално, с помощната програма за настройка на компютъра. Вижте *Ръководството за помощната програма Computer Setup (Настройка на компютъра) (F10)*, включено в компютъра, за допълнителна информация за компютъра и указания за ползването й.
- Дистанционно с HP Client Manager от Symantec, HP Client Automation или System Software Manager. Този софтуер позволява сигурно и последователно внедряване и контрол на настройките за защита.

Следната таблица и раздели се отнасят до функциите за управление на защитата локално на компютъра чрез програмите в Computer Setup (Настройка на компютъра).

Таблица 11-1 Преглед на функциите за защита

Опция	Описание
Setup Password (Парола за настройки)	Позволява ви да въведете и активирате парола за настройки (администратора).

Таблица 11-1 Преглед на функциите за защита (продължение)

	ЗАБЕЛЕЖКА: Ако е зададена парола за настройки, тя ще се изисква при промяна на опции в Computer Setup, изтриване на ROM паметта и при промяна на някои опции тип Plug & Play в Windows.
Power-On Password (Парола при включване на захранването)	Позволява ви да въведете и активирате парола при включване на захранването. След задействането на електрическия цикъл се появява подкана да въведете паролата за включване. Ако не бъде въведена правилната парола, компютърът няма да зареди операционната система. **ЗАБЕЛЕЖКА:** Тази парола не се появява при "топло" рестартиране, като например с клавишите Ctrl+Alt+Delete или **Restart (Рестартиране) от средата на Windows**, стига да не е разрешена от **Password Options** (Опции за парола) (вижте по-долу).
Password Options (Опции за парола) (Този избор ще се появява само ако е зададена парола при включване или за настройка).	Позволява: • Заключване на стари модели периферия (все едно е зададена парола) • Разрешаване/забраняване на режим на мрежов сървър (все едно е зададена парола при включване) • Указване дали се изисква парола при "топло" рестартиране (Ctrl+Alt+Delete) (появява се, ако е зададена парола при включване). • Enable/Disable Setup Browse Mode (Разрешаване/забраняване на Режим на настройка на преглед) (появява се, ако е зададена парола) (позволява да се разглеждат, а не да се променят, опциите на F10 Setup, без да се въвежда парола за настройките) • Enable/disable Stringent Password (Разрешаване/забраняване на строгата парола) (показва се, ако е зададена парола при включване), която, когато е разрешена, пренебрегва настройката на мостчето за парола на платката за забрана на паролата при включване Вижте *Ръководството за управление на настолни компютри* за повече информация.
Smart Cover (Интелигентен капак) (на някои модели)	Позволява да: • Отключвате/заключвате интелигентния капак • Настроите сензора за интелигентния капак на Disable (Забранен)/Notify User (Уведомяване на потребителя)/Setup Password (Парола при настройки). **ЗАБЕЛЕЖКА:** *Notify User* (Уведомяване на потребителя) уведомява потребителя, че сензорът е засякъл отваряне на капака. *Setup Password* (Парола за настройка)изисква въвеждането на парола при стартирането на компютъра, ако сензорът засече отваряне на капака. Тази функция се поддържа само при някои модели.
Device Security (Защита на устройствата)	Позволява ви да зададете опцията Device Available/Device Hidden (Механизмът е наличен/скрит) за: • Серийни портове • Паралелен порт • Rear USB ports (Задните USB портове) • Предни USB портове • Internal USB ports (Вътрешните USB портове) • Системен звук • Мрежови контролери (при някои модели) • Стар модел дискети

Таблица 11-1 Преглед на функциите за защита (продължение)

	• Механизъм за вградена защита (при някои модели) • SATA0 • SATA1 (при някои модели) • SATA2 (при някои модели) • SATA3 (при някои модели) • eSATA (при някои модели)
LoJack for HP ProtectTools	Позволява да контролирате, управлявате и проследявате компютъра дистанционно. След първоначално активиране LoJack Pro for HP ProtectTools се конфигурира от Absolute Software Customer Center. От Customer Center администраторът може да конфигурира LoJack for HP ProtectTools за контрол и управление на компютъра. Ако системата е поставена на неправилно място или откраднатa, Customer Center може да помогне на местните власти за откриването и връщането на компютъра. Ако е конфигуриран, LoJack Pro може да продължи да работи дори когато твърдият диск е изтрит или сменен.
Network Service Boot (Стартиране от мрежа)	Разрешава/забранява възможността на компютъра да стартира от операционна система, инсталирана на мрежов сървър. (Тази функция е налична само при моделите с мрежови платки; мрежовата платка трябва да е или PCI платка за разширение, или да е вградена в дънната платка.)
System IDs (Системни идентификатори)	Позволяват ви да зададете: • Asset Tag (18-байтов идентификатор) – идентификационен номер, даден на този компютър от фирмата. • Етикет за собственост (80-байтов идентификатор), който се показва при POST. • Серийния номер на шасито или универсалния уникален идентификатор (UUID). UUID може да се промени само ако серийният номер на шасито е невалиден. (Тези идентификатори обикновено се задават фабрично и се използват за идентифицирането на всяка една система.) • Клавиатурната настройка за езика (напр. английски или немски) за записа на системния идентификатор.
DriveLock защита	Позволява ви да въведете или промените главна или потребителска парола за твърди дискове. Когато тази функция е разрешена, по време на POST се появява съобщение за въвеждане на една от потребителските пароли. Ако нито една от тях не се въведе правилно, твърдият диск няма да може да се използва, докато не се въведе правилната парола при следващи "студени рестартирания" на компютъра. **ЗАБЕЛЕЖКА:** Тази възможност за избор ще се появи само когато в системата е инсталирано поне едно дисково устройство, което поддържа функцията DriveLock.
Setup Security Level (Настройка на ниво на защита)	Осигурява начин да се разреши на крайните потребители ограничен достъп за промяна на конкретни опции за настройка, без да е необходимо да знаят паролата за настройки. Тази функция предоставя на администратора по-голяма гъвкавост за защита при извършването на промени на основни опции за настройка, но също така да разрешава на потребителя да разглежда системните настройки и конфигурира второстепенните опции. Администраторът указва правата на достъп до индивидуални опции за настройка за всеки конкретен случай посредством Setup Security Level (Настройка на ниво на защита). По подразбиране всички опции за настройка са с парола (Setup Password), за което потребителят трябва да въведе правилна парола по време на POST, за да може да промени опциите. Администраторът може да зададе на отделни елементи стойност None (Няма) и така потребителят може да извършва промени на тези опции, дори когато влезе в менюто с настройките с невалидна парола. Ако е разрешена Power-On Password (Парола при включване на захранването), тогава стойността None (Няма) се заменя от тази парола.

Таблица 11-1 Преглед на функциите за защита (продължение)

	ЗАБЕЛЕЖКА: Setup Browse Mode (Режим на настройка на преглед) трябва да е в положение Enable (Разрешаване), за да може потребителят да влезе в Setup, без да знае паролата за достъп.
System Security (Защита на системата) (при някои модели тези опции зависят от хардуера)	Data Execution Prevention (Предотвратяване на изпълнение на данни) (наличен при някои модели) (разреши/забрани) – помага за предотвратяване на пробиви в защитата на операционната система. Virtualization Technology (Технология за виртуализация) (при някои модели) (разреши/забрани) – управлява функциите за виртуализация на процесора. Промяната на тази настройка изисква изключване и повторно включване на компютъра. Virtualization Technology Directed I/O (Технология за виртуализация насочен вход/изход) (при някои модели) (разреши/забрани) – управлява функциите за виртуализация при пренасочването на DMA на чипсета. Промяната на тази настройка изисква изключване и повторно включване на компютъра. Trusted Execution Technology (Технология за надеждно изпълнение) (при някои модели) (разреши/забрани) – управлява съответните функции на процесора и чипсета, необходими за поддръжка на виртуално устройство. Промяната на тази настройка изисква изключване и повторно включване на компютъра. За да разрешите тази функция, трябва да разрешите следните функции: • Поддръжка на механизъм за вградена защита • Технология на виртуализация • Технология на виртуализация насочен вход/изход Embedded Security Device Support (Поддръжка на механизъм за вградена защита) (при някои модели) (разреши/забрани) – разрешава включването и изключването на механизма за вградена защита. Промяната на тази настройка изисква изключване и повторно включване на компютъра. **ЗАБЕЛЕЖКА:** За да конфигурирате механизма за вградена защита, трябва да въведете парола за настройка. • Reset to Factory Settings (Възстановяване на фабричните настройки) (при някои модели) (Не възстановявай/Възстанови) – възстановяването на фабричните настройки ще изтрие всички ключове за защита. Промяната на тази настройка изисква изключване и повторно включване на компютъра. **ВНИМАНИЕ:** Механизмът за вградена защита е критичен компонент на много защитни схеми. Изтриването на ключовете за защита ще предотврати достъпа до данните, защитени от механизма за вградена защита. Изборът на връщане към фабричните настройки може да доведе до значителна загуба на данни. • Reset authentication credentials (Нулиране на идентификационните данни за удостоверяване) (при някои модели) (Не нулирай/нулирай) – избирането на нулиране забранява поддръжката на удостоверяване при включване и изчиства информацията за удостоверяване от механизма за вградена защита. Промяната на тази настройка изисква изключване и повторно включване на компютъра. OS management of Embedded Security Device (Управление от ОС на механизма за вградена защита) (при някои модели) (разреши/забрани) – тази опция позволява на потребителя да ограничи контрола на операционната система върху механизма за вградена защита. Промяната на тази настройка изисква изключване и повторно включване на компютъра. Тази опция позволява на потребителя да ограничи контрола на ОС върху механизма за вградена защита. • Reset of Embedded Security Device through OS (Нулиране на механизма за вградена защита от ОС) (при някои модели) (разреши/забрани) – тази опция позволява на потребителя да ограничи способността на операционната система да заяви връщане към фабричните настройки на механизма за вградена защита. Промяната на тази настройка изисква изключване и повторно включване на компютъра.

Таблица 11-1 Преглед на функциите за защита (продължение)

	ЗАБЕЛЕЖКА: За да разрешите тази опция, трябва да бъде въведена парола за настройка.
	PAVP (при някои модели) (забранено/мин./макс.) – PAVP включва Protected Audio Video Path (Път към защитено аудио и видео) в чипсета. Това може да разреши гледането на защитено съдържание с висока разделителна способност, което иначе ще бъде забранено за възпроизвеждане. Избирането на Max (Макс.) ще задели 96 мегабайта системна памет специално за PAVP.

Защита с парола

Паролата за стартиране предотвратява неоторизираната употреба на компютъра, като въвеждането ѝ се изисква при включване или рестартиране за достъп до приложения или данни. Паролата за настройки предотвратява неоторизирания достъп до Computer Setup (Настройка на компютъра) и може да се използва за нулиране на паролата за включване. Тоест, когато трябва да въведете паролата за включване, въвеждането на паролата за настройки вместо нея също ще позволи достъп до компютъра.

Може да се зададе парола за настройки за цялата мрежа, за да може системният администратор да се регистрира във всички системи на мрежата с цел поддръжка, без да е нужно да знае паролата за включване на компютъра, дори ако такава е била зададена.

ЗАБЕЛЕЖКА: System Software Manager (SSM) може да се ползва за създаване и управление на пароли на BIOS направо от операционната система Windows. За повече информация вижте ръководството за потребителя на SSM на адрес http://www.hp.com/go/ssm.

ЗАБЕЛЕЖКА: HP Client Management Interface (HP CMI) осигурява достъп до управлението на настройките на BIOS, включително и до паролите, направо от операционната система Windows. За повече информация вижте HP Client Management Interface Technical Whitepaper на адрес http://www.hp.com/go/hpcmi.

Задаване на парола за настройки с Computer Setup (Настройка на компютъра)

Ако системата е оборудвана с механизъм за вградена защита, вижте *HP ProtectTools Security Manager Guide* на адрес http://www.hp.com. Поставянето на парола за настройки в Computer Setup (Настройка на компютъра) предотвратява преконфигурирането на компютъра от помощната програма до въвеждане на паролата.

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Рестартиране**.
2. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

   ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.
3. Изберете **Security** (Защита) и след това **Setup Password** (Парола за настройки) и следвайте инструкциите на екрана.
4. Преди да излезете, щракнете върху **Файл** > **Запис на настройките и изход**.

Задаване на парола за включване с помощта на Computer Setup (Настройка на компютъра)

Задаването на парола за включване чрез Computer Setup (Настройка на компютъра) предотвратява достъпа до компютъра при включването му, освен ако не се въведе паролата. Когато има зададена парола за включване, в Computer Setup (Настройка на компютъра) има **Password Options** (Опции за парола) под менюто **Security** (Защита). Опциите за паролата включват **Password Prompt on Warm Boot** (Искане на парола при топло рестартиране). Когато **Password Prompt on Warm Boot** (Искане на парола при топло рестартиране) е разрешено, паролата трябва да бъде въвеждана при всяко рестартиране на компютъра.

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Рестартиране**.
2. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

3. Изберете **Security** (Защита) и след това **Power-On Password** (Парола при включване) и следвайте инструкциите на екрана.
4. Преди да излезете, щракнете върху **Файл** > **Запис на настройките и изход**.

Въвеждане на парола за включване

За да въведете парола за включване, изпълнете следните стъпки:

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Restart the Computer** (Рестартирайте компютъра).
2. Когато на монитора се появи иконата с ключ, въведете текущата парола и натиснете клавиша Enter.

ЗАБЕЛЕЖКА: Въвеждайте внимателно; знаците не се появяват на екрана от съображения за сигурност.

Ако въведете неправилна парола, се показва счупен ключ. Опитайте отново. След три неуспешни опита трябва да изключите компютъра и пак да го включите, за да продължите.

Въвеждане на парола за настройки

Ако системата е оборудвана с механизъм за вградена защита, вижте *HP ProtectTools Security Manager Guide* на адрес http://www.hp.com.

Ако на компютъра има зададена парола за настройки, ще се появи съобщение за въвеждането ѝ при всеки опит за влизане в Computer Setup (Настройка на компютъра).

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Рестартиране**.

2. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

3. Когато на монитора се появи иконата с ключ, въведете паролата за настройки и натиснете клавиша Enter.

ЗАБЕЛЕЖКА: Въвеждайте внимателно; знаците, които въвеждате, не се появяват на екрана от съображения за сигурност.

Ако въведете неправилна парола, се показва счупен ключ. Опитайте отново. След три неуспешни опита трябва да изключите компютъра и пак да го включите, за да продължите.

Смяна на паролата за настройки или включване

Ако системата е оборудвана с механизъм за вградена защита, вижте *HP ProtectTools Security Manager Guide* на адрес http://www.hp.com.

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Restart the Computer** (Рестартирайте компютъра).

2. За да смените паролата при включване, минете на стъпка 3.

   За да промените паролата за настройки, щом включите компютъра и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

3. Когато се появи иконата с ключ, въведете текущата парола, наклонена черта (/) или друг разделителен знак, новата парола, друга наклонена черта (/) или друг разделителен знак, а след това новата парола отново, както е показано: `текуща парола/нова парола/нова парола`

ЗАБЕЛЕЖКА: Въвеждайте внимателно; знаците не се появяват на екрана от съображения за сигурност.

4. Натиснете клавиша Enter.

Новата парола ще е валидна при следващото включване на компютъра.

ЗАБЕЛЕЖКА: Вижте Национални разделители от клавиатурата на страница 33 за информация за другите разделителни знаци. Паролата за включване и тази за настройки също могат да се сменят с помощта на опциите за защита в Computer Setup (Настройка на компютъра).

Изтриване на паролата за настройки или включване

Ако системата е оборудвана с механизъм за вградена защита, вижте *HP ProtectTools Security Manager Guide* на адрес http://www.hp.com.

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Restart the Computer** (Рестартирайте компютъра).
2. За да изтриете паролата при включване, минете на стъпка 3.

   За да изтриете паролата за настройки, щом включите компютъра и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

3. Когато се появи иконата с ключ, въведете текущата парола и след нея наклонена черта (/) или подобен разделител, както е показано: `текуща парола/`
4. Натиснете клавиша Enter.

ЗАБЕЛЕЖКА: Вижте Национални разделители от клавиатурата на страница 33 за информация за другите разделителни знаци. Паролата за включване и тази за настройки също могат да се сменят с помощта на опциите за защита в Computer Setup (Настройка на компютъра).

Национални разделители от клавиатурата

Всяка клавиатура е проектирана така, че да отговаря на специфични за съответната страна изисквания. Синтаксисът и клавишите, които използвате, за да смените или изтривате паролата, зависят от клавиатурата, която е била доставена с компютъра.

Национални разделители от клавиатурата

/	Арабски	-	Гръцки	/	Руски
=	Белгийски	.	Иврит	-	Словашки
-	БХХЧСС*	-	Унгарски	-	Испански
/	Бразилски	-	Италиански	/	Шведски/Финландски
/	Китайски	/	Японски	-	Швейцарски
-	Чешки	/	Корейски	/	Тайвански
-	Датски	-	Латиноамерикански	/	Тайландски
!	Френски	-	Норвежки	.	Турски
й	Канадски френски	-	Полски	/	Американски английски
-	Немски	-	Португалски		

* За Босна и Херцеговина, Хърватия, Черна гора, Сърбия и Словения

Изчистване на пароли

Ако забравите паролата, нямате достъп до компютъра. Указания за изчистването на пароли ще намерите в *Troubleshooting Guide (Ръководство за отстраняване на неизправности)*.

Ако системата е оборудвана с механизъм за вградена защита, вижте *HP ProtectTools Security Manager Guide* на адрес http://www.hp.com.

DriveLock (Заключване на устройства)

DriveLock (Заключване на устройства) е стандартна за отрасъла функция за защита, която предотвратява неоторизирания достъп до данните в ATA твърди дискове. DriveLock (Заключване на устройства) функционира като допълнение към Computer Setup (Настройка на компютъра). Тя е на разположение само когато бъдат разпознати твърди дискове, които поддържат набора команди за ATA защита. DriveLock (Заключване на устройства) е предназначена за клиенти на HP, за които защитата на данните е от изключително значение. За такива клиенти цената на твърдия диск и загубата на данните върху него са несъразмерни с последствията, до които може да се стигне при неоторизиран достъп до тези данни. За да се балансира това ниво на защита с практическата нужда от възможност за възстановяване на забравена парола, схемата на HP DriveLock използва защита с две пароли. Едната парола е предназначена да се задава и използва от системен администратор, а другата обикновено се задава и ползва от крайния потребител. Няма „задна вратичка”, която може да се използва за отключването на диск, ако и двете пароли се загубят. Затова функцията DriveLock (Заключване на устройства) се използва най-безопасно, когато данните на твърдия диск се копират на корпоративна информационна система или редовно се архивират. В случай че и двете пароли за DriveLock бъдат загубени, твърдият диск е практически неизползваем. За потребители, които не влизат в описания по-горе профил, това може да е недопустим риск. За потребители, които влизат в описания по-горе профил на клиенти, това може да е нормален риск, като се имат предвид съхранените на твърдия диск данни.

Използване на DriveLock (Заключване на устройства)

Когато един или повече твърди дискове, които поддържат набора от команди за ATA защита, бъдат разпознати, опцията DriveLock се появява под менюто Security (Защита) в Computer Setup (Настройка на компютъра). Потребителите имат възможност да зададат главната парола или да разрешат DriveLock. За да се разреши DriveLock, трябва да се въведе потребителска парола. Тъй като първоначалната конфигурация на DriveLock (Заключване на устройства) обикновено се изпълнява от системен администратор, най-напред трябва да се зададе главна парола. HP препоръчва на системните администратори да задават главна парола, независимо дали възнамеряват да разрешат или забранят DriveLock (Заключване на устройства). Така системните администратори ще могат да променят настройките на DriveLock (Заключване на устройства), ако в бъдеще устройството се заключи. След като се зададе главната парола, системният администратор може да разреши или забрани DriveLock (Заключване на устройства).

Ако има заключен твърд диск, при POST ще се изисква парола за отключването му. Ако е зададена парола за включване и тя съвпада с тази на устройството, при POST няма да се изисква повторно въвеждане на паролата. В противен случай ще се появи съобщение за въвеждане на парола за DriveLock (Заключване на устройства). При студено рестартиране могат да се използват или главната, или потребителската парола. При топло рестартиране трябва да се въведе същата парола, която е била ползвана за отключване на устройството преди предшестващия студен рестарт. Потребителите разполагат с две възможности да въведат правилната парола. При студено рестартиране, ако никой от двата опита не бъде успешен, POST ще продължи, но устройството ще остане недостъпно. При топло рестартиране или рестартиране

от Windows, ако нито един от опитите не успее, POST ще блокира и потребителят ще получи инструкция да изключи захранването и да го включи отново.

Приложения на DriveLock (Заключване на устройства)

Най-практично е да се ползва функцията за защита DriveLock във фирмена среда. Системният администратор ще носи отговорност за конфигурирането на твърдия диск, което ще включва, освен другото, задаването на главната парола за DriveLock и временна потребителска парола. В случай на забравена парола или ако оборудването се предаде за използване от друг служител, винаги може да се използва главната парола за нулирането на потребителската и да се възстанови достъпът до твърдия диск.

HP препоръчва на корпоративните системни администратори, които решат да разрешат функцията DriveLock (Заключване на устройства), да създадат също така и корпоративен правилник за задаване и поддръжка на главни пароли. Това е добре да се прави с цел да се предотвратят ситуации, при които служител умишлено или неумишлено зададе и двете пароли на DriveLock, преди да напусне фирмата. При такива случаи твърдите дискове са неизползваеми и трябва да се сменят. Също така, ако не зададат главна парола, системните администратори може да попаднат в ситуация, в която нямат достъп до твърдия диск и не могат да изпълнят рутинни проверки за неоторизиран софтуер, други функции за контрол на активите и поддръжка.

За потребители с по-малки изисквания за защита HP не препоръчва разрешаването на функцията DriveLock (Заключване на устройства). Потребителите в тази категория са самостоятелни потребители или такива, които по принцип не пазят важни данни на твърдия си диск. За тези потребители потенциалната загуба на твърд диск вследствие на загуба и на двете пароли е много по-голяма от стойността на данните, които функцията DriveLock (Заключване на устройства) е проектирана да пази. Достъпът до Computer Setup (Настройка на компютъра) и функцията DriveLock (Заключване на устройства) може да се ограничи чрез паролата за настройки. Когато зададат парола за настройки и не я казват на крайните потребители, системните администратори могат да ограничат разрешаването на функцията DriveLock (Заключване на устройства) от страна на крайните потребители.

Интелигентен датчик на капака

Датчикът за сваляне на капака, с който са снабдени някои модели, е съчетание от хардуерна и софтуерна технология, която може да ви предупреждава, когато капакът или страничният панел на компютъра са били сваляни. Съществуват три нива на защита, както е описано в следващата таблица.

Таблица 11-2 Нива на защитата на интелигентния датчик на капака

Ниво	Настройка	Описание
Ниво 0	Забранен	Интелигентният датчик на капака е забранен (по подразбиране).
Ниво 1	Уведомяване на потребителя	При рестартиране на компютъра на екрана се появява съобщение за това, че е бил отварян капакът или страничният панел на компютъра.
Ниво 2	Setup Password (Парола за настройки)	При рестартиране на компютъра на екрана се появява съобщение за това, че е бил отварян капакът или страничният панел на компютъра. Трябва да въведете паролата за настройки, за да продължите.

ЗАБЕЛЕЖКА: Тези настройки могат да се променят с помощта на Computer Setup (Настройка на компютъра). За повече информация за Computer Setup (Настройка на компютъра) вижте *Ръководството на помощната програма Computer Setup (Настройка на компютъра) (F10)*.

Настройка на нивото на защита на интелигентния датчик на капака

За да настроите нивото на защита на интелигентния датчик на капака, изпълнете следните стъпки:

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Рестартиране**.
2. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

   ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

3. Изберете **Security** (Защита) > **Smart Cover** (Интелигентен капак) > **Cover Removal Sensor** (Датчик за сваляне на капака) и изберете желаното ниво на защита.
4. Преди да излезете, щракнете върху **Файл** > **Запис на настройките и изход**.

Интелигентна ключалка на капака

Интелигентната ключалка на капака е ключалка за капак, която се управлява от софтуер и е налична при определени компютри на HP. Тази ключалка предотвратява неоторизиран достъп до вътрешните компоненти. Компютърът се доставя с незаключена интелигентна ключалка на капака.

△ **ВНИМАНИЕ:** За максимална защита с ключалката на капака задайте парола за настройки. Паролата за настройки предотвратява неоторизирания достъп до Computer Setup (Настройка на компютъра).

ЗАБЕЛЕЖКА: Интелигентната ключалка на капака се предлага допълнително за някои системи.

Заключване на интелигентната ключалка на капака

За да активирате и заключите интелигентната ключалка, изпълнете следните стъпки:

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Рестартиране**.
2. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

   ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

3. Изберете **Security** (Защита) > **Smart Cover** (Интелигентен капак) > **Cover Lock** (Ключалка на капака) > **Lock option** (Заключване).
4. Преди да излезете, щракнете върху **Файл** > **Запис на настройките и изход**.

Отключване на ключалката на капака

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Старт** > **Изключване** > **Рестартиране**.
2. За да стигнете до настройките на компютъра, щом го включите и преди да зареди операционната система, натиснете F10. Натиснете Enter, за да прескочите заглавния екран, ако е нужно.

   ЗАБЕЛЕЖКА: Ако не натиснете клавиша F10 в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете клавиша F10, преди компютърът да зареди операционната система, за да влезете в помощната програма.

3. Изберете **Security** (Защита) > **Smart Cover** (Интелигентен капак) > **Cover Lock** (Заключване на капака) > **Unlock** (Отключване).
4. Преди да излезете, щракнете върху **Файл** > **Запис на настройките и изход**.

Използване на ключа FailSafe на капака

Ако активирате ключалката на капака и не можете да въведете паролата, за да я деактивирате, ще ви трябва ключ FailSafe за капака, за да го отворите. Този ключ ще ви трябва в следните случаи:

- Прекъсване на електрозахранването
- Неуспешно начално стартиране
- Повреда на компютърен компонент (напр. процесор или захранване)
- Забравена парола

ВНИМАНИЕ: Ключът FailSafe на интелигентния капак е специализиран инструмент, който се предлага от HP. Подгответе се - поръчайте този ключ, преди да ви потрябва при оторизиран риселър или доставчик на услуги.

За да получите ключа FailSafe, направете едно от следните неща:

- Обърнете се към оторизиран риселър или сервиз на HP.
- Обадете се на съответния телефонен номер от гаранцията.

За повече информация относно ползването на ключа FailSafe на интелигентния капак вижте *Hardware Reference Guide (Ръководство за справки по хардуера)*.

Наличие на кабелна ключалка

На задния панел на компютъра (при някои модели) се намира кабелна ключалка, чрез която компютърът може физически да се прикрепи към работно място.

За илюстрирани указания вижте *Hardware Reference Guide (Ръководство за справки относно хардуера)*.

Технология за идентифициране по отпечатъци на пръсти

Елиминирайки нуждата от въвеждането на потребителски пароли, технологията за идентифициране по отпечатъци на пръсти на HP увеличава мрежовата сигурност, опростява процеса на регистриране и намалява разходите за управление на корпоративните мрежи. Технологията е ценово достъпна и вече не е предназначена само за високотехнологични организации с високи изисквания към защитата.

ЗАБЕЛЕЖКА: Поддръжката на технологията за идентифициране по отпечатъци на пръсти е различна в зависимост от модела.

Уведомяване при грешки и възстановяване

Функциите за уведомяване при грешки и възстановяване комбинират нови хардуерни и софтуерни технологии, за да предотвратят загубата на данни от критично значение и да намалят непланирания престой на системите.

Ако компютърът е свързан към мрежа, която се управлява от HP Client Manager, той изпраща съобщение за грешка на приложението за управление на мрежата. С HP Client Manager Software можете също така дистанционно да планирате автоматичното изпълнение на диагностика на всички управляеми компютри и да генерирате обобщен отчет за неуспешните тестове.

Система за защита на устройства

Системата за защита на устройства (DPS) е инструмент за диагностика, вграден в твърди дискове, инсталирани в определени компютри на HP. DPS е проектирана да бъде в помощ при диагностиката на проблемите, които могат да доведат до замяна на твърдите дискове.

При сглобяването на компютрите на HP всеки твърд диск се тества с DPS, като на диска се оставя постоянен запис на важна информация. При всяко изпълнение на DPS системата резултатите от теста се записват на твърдия диск. Тази информация може да се използва от сервиза при диагностиката на проблеми, които са довели до изпълнението на софтуера DPS. Указания за ползването на DPS ще намерите в *Troubleshooting Guide (Ръководство за отстраняване на неизправности)*.

Устойчив на токови удари захранващ блок

Вграденият захранващ блок, устойчив на токови удари, осигурява по-голяма надеждност при евентуални токови удари. Това захранване може да издържи на токов удар до 2000 волта, без да се наруши работата на системата или да се загубят данни.

Датчик за температура

Датчикът за температура е хардуерна и софтуерна функция, която следи вътрешната температура на компютъра. Тази функция показва предупредително съобщение при нарушение на нормалния диапазон, което ви дава време да вземете мерки, преди вътрешните компоненти да се повредят или да се загубят данни.

△ **ВНИМАНИЕ:** Високата температура може да доведе до повреда на системата или загуба на данни.

Азбучен указател

P

S

U

V