Посібник з керування настільними системами

Бізнес-ПК HP

Посібник з керування настільними системами

Бізнес-ПК HP

Четверте видання (вересень 2009 р.)

Код документа: 581009-BD1

Про цей документ

У цьому посібнику ви знайдете визначення та вказівки з використання функцій безпеки та керування, попередньо встановлених на деяких моделях.

⚠ **УВАГА!** Таке позначення тексту вказує, що недотримання цих вказівок може призвести до травм чи смерті.

△ **ПОПЕРЕДЖЕННЯ.** Таке позначення тексту вказує, що недотримання цих вказівок може призвести до пошкодження обладнання чи втрати даних.

ПРИМІТКА. Таке позначення тексту вказує на важливу додаткову інформацію.

Зміст

1 Огляд керування настільними системами

2 Початкова конфігурація та розгортання

HP Client Automation Agent 2
HP Client Manager 3

3 Дистанційне встановлення системи

4 Оновлення і керування програмним забезпеченням

HP Client Management Interface 5
Диспетчер HP SoftPaq Download Manager 6
HP System Software Manager 6
HP ProtectTools Security Manager 7
HP Client Automation Starter Edition і Standard Edition 8
Client Automation Starter Edition, Standard Edition та Enterprise Edition 8
HP Client Manager from Symantec 9
Altiris Client Management Suite 10
HP Client Catalog for Microsoft System Center & SMS Products 10
Remote Management Technology (Технологія віддаленого керування) 10
Налаштування Intel Management Engine 11
Verdiem Surveyor 13
HP Proactive Change Notification 13
Subscriber's Choice 13
Рішення, що тепер не надаються 13

5 Флеш-ПЗП

Remote ROM Flash 14
HPQFlash 14

6 Режим Boot Block Emergency Recovery

7 Тиражування параметрів

Копіювання на окремий комп'ютер 16

Копіювання на кілька комп'ютерів 17
Створення завантажувального пристрою 18
Підтримуваний носій даних USB-флеш 18
Непідтримуваний носій даних USB-флеш 19

8 Кнопка живлення з двома положеннями

9 Підтримка через веб-сайт HP

10 Галузеві стандарти

11 Відстеження ресурсів і безпека

Використання пароля 28
Встановлення пароля налаштування з використанням утиліти Computer Setup 29
Встановлення пароля вмикання з використанням утиліти Computer Setup 29
Введення пароля увімкнення живлення 30
Введення пароля налаштування 30
Зміна пароля вмикання або пароля налаштування 31
Видалення пароля вмикання або пароля налаштування 31
Розділові знаки на різних клавіатурних розкладках 32
Скидання паролів 32
DriveLock 32
Використання DriveLock 33
Прикладні програми DriveLock 33
Датчик переміщення кришки 35
Налаштування рівня захисту функції Smart Cover Sensor 35
Smart Cover Lock 35
Блокування у Smart Cover Lock 36
Розблокування у Smart Cover Lock 36
Використання Smart Cover FailSafe Key 36
Cable Lock Provision 37
Технологія ідентифікації за відбитками пальців 37
Повідомлення про неполадки і відновлення 37
Система захисту дисків 37
Захищене від стрибків напруги джерело живлення 37
Термодатчик 38

Покажчик 39

1 Огляд керування настільними системами

Рішення компанії HP з клієнтського керування є стандартними рішеннями для контролю і керування настільними системами, робочими станціями і портативними ПК у мережевому середовищі. Компанія HP першою запропонувала програму керування настільними системами з випуском перших у галузі повністю керованих настільних персональних комп'ютерів у 1995 році. Компанія HP є володарем патенту на технологію керування. Відтоді вона очолила галузеву ініціативу з розробки інфраструктури і стандартів, необхідних для ефективного розгортання, конфігурації і керування настільним системами, робочими станціями і портативними ПК. Наразі компанія займається розробкою власного ПЗ з керування і тісно співпрацює з провідними постачальниками програмних рішень для забезпечення сумісності між рішеннями з клієнтського керування і цими продуктами. Рішення компанії HP з клієнтського керування є важливим елементом нашої політики з надання рішень, що допомагають у зниженні загальної вартості володіння і обслуговування ПК протягом всього їхнього життєвого циклу.

Основні характеристики і функції керування настільними системами:

- Початкові конфігурація і розгортання
- Дистанційне встановлення системи
- Оновлення і керування програмним забезпеченням
- Флеш-ПЗП
- Налаштування параметра “Обладнання”
- Відстеження ресурсів і безпека
- Повідомлення про неполадки і відновлення

ПРИМІТКА. Підтримка спеціальних функцій, описана в даному посібнику, може змінюватися залежно від моделі або версії програмного забезпечення.

2 Початкова конфігурація та розгортання

Комп'ютер постачається з попередньо встановленим образом системного програмного забезпечення. Після завершення короткого процеса “розпаковування” програмного забезпечення комп'ютер готовий до роботи.

Ви можете замінити попередньо встановлений образ програмного забезпечення на індивідуальний набір системного і прикладного програмного забезпечення. Існує декілька методів розгортання індивідуального образу програмного забезпечення, а саме:

- Встановлення додаткових програм після розгортання попередньо встановленого образу програмного забезпечення.
- За допомогою засобів розгортання програмного забезпечення, таких як HP Client Automation Standard Edition або HP Client Automation Enterprise Edition (на основі технології Radia), можна замінити попередньо встановлене програмне забезпечення на персоналізований образ.
- Використання процесу “клонування” дисків для копіювання вмісту одного жорсткого диска на інший.

Оптимальний метод розгортання залежить від вашого інформаційного середовища і процесів.

ROM-based setup (Налаштування за допомогою ПЗП) і ACPI hardware (Обладнання ACPI) надають подальшу допомогу з відновлення системного програмного забезпечення, керування конфігурацією та усунення несправностей, а також керування живленням.

HP Client Automation Agent

Цей агент керування, що використовується у версіях HP Client Automation Standard Edition і Enterprise Edition, попередньо встановлений на комп’ютері. Після встановлення ця програма дозволяє з’єднання з консоллю керування HP.

Щоб установити HP Client Automation Agent:

1. Натисніть **Пуск**.
2. Виберіть **Усі програми**.
3. Натисніть **Керування компонентами HP**.
4. Клацніть **HP Management Agent Readme**, що відповідає бажаній для вас мові.
5. Перегляньте й виконайте інструкції, що містяться у файлі Readme, щоб установити HP Client Automation Agent.

Агент HP Client Automation Agent є ключовим інфраструктурним компонентом, який дозволяє працювати з усіма вирішеннями HP Client Automation. Детальніше дізнатися про інші інфраструктурні компоненти, необхідні для реалізації рішень із керування конфігурацією HP, можна на сайті http://h20229.www2.hp.com/solutions/ascm/index.html.

HP Client Manager

Утиліта HP Client Manager (HPCM) — це безкоштовне вирішення, розроблене компанією Symantec, для всіх підтримуваних моделей бізнес-ПК, ноутбуків, робочих станцій і Blade-ПК HP. HPCM поєднує власні інструменти HP, такі як System Software Manager, HP Instant Support Professional Edition і HP Client Management Interface, формуючи централізовану модель для керування, відстеження та моніторингу всього підтримуваного обладнання HP.

HP Client Manager 7.0 містить новітню сторінку порталу (Portal Page), яка слугує єдиним центром для виконання адміністратором таких завдань із керування:

- Інвентаризація
- Попередження
- Керування BIOS
- Оновлення драйверів
- Виконання служби HP Instant Support Health Scan and Diagnostics
- Виконання завдань щодо вбудованої безпеки
- Перегляд загального тренду попереджень про стан системи HP за останні 3-6 місяців
- Перегляд загальної сумісності підтримуваних комп'ютерів зі службою HP Instant Support Health Scan and Diagnostics
- Перегляд підсумків щодо комп'ютерів HP – зведення за різноманітними підтримуваними настільними ПК, ноутбуками, робочими станціями та Blade-ПК HP
- Перегляд попереджень: Asset (Актив), Threshold (Поріг), Hardware Health (Стан обладнання)
- Звіти
- Адміністративні завдання для оновлення власних інструментів HP

HPCM можна завантажити за адресою http://www.symantec.com/business/theme.jsp, клацнувши **HP Client Manager** у розділі **Strategic Partner Products**. Безкоштовну постійну ліцензію можна також отримати на сторінці завантаження.

Відеопосібники з HPCM також опубліковано на веб-сайті http://www.symantec.com/connect. Виконайте пошук за ключовими словами **HP Client Manager 7.0**, щоб переглянути покрокові відеопосібники з виконання різноманітних завдань в HPCM.

3 Дистанційне встановлення системи

Функція дистанційного встановлення системи дозволяє встановлювати й запускати систему за допомогою програмного забезпечення і даних про конфігурацію, що зберігаються на мережевому сервері, шляхом ініціалізації середовища Preboot Execution Environment (PXE). Функція дистанційного встановлення системи здебільшого слугує як інструмент встановлення і конфігурації системи, але також може використовуватись для таких задач:

- Форматування жорсткого диску
- Розгортання образу програмного забезпечення на один або декілька нових ПК
- Дистанційне оновлення системи BIOS у флеш-ПЗП (Remote ROM Flash на сторінці 14)

ПРИМІТКА. Існують засоби для перепрограмування системної BIOS з операційної системи Microsoft Windows.

- Налаштування параметрів системи BIOS

Для запуску функції дистанційного встановлення системи натисніть F12, коли під час завантаження комп'ютера з'явиться повідомлення **F12 = Network Service Boot** (Завантаження через мережу) у нижньому лівому куті екрану з логотипом HP. Дотримуйтесь вказівок на екрані для продовження процесу. Порядок завантаження за замовчуванням – це один з параметрів конфігурації BIOS, який можна змінити для постійної спроби звертання до завантаження з PXE.

4 Оновлення і керування програмним забезпеченням

HP надає декілька інструментів для керування та оновлення програмного забезпечення настільних систем, робочих станцій та ноутбуків:

- HP Client Management Interface
- Диспетчер HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter Edition, Standard Edition та Enterprise Edition
- HP Client Manager
- Комплект рішень Altiris Client Management Suite
- HP Client Catalog for Microsoft System Center & SMS Products
- ПК марки Intel vPro з технологією Active Management Technology
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

Незалежно від того, які інструменти керування системою використовуються у вашому відділі IT, керування програмними і апаратними засобами є важливим чинником для зниження витрат на сектор IT і підтримання життєдіяльності вашого бізнесу. IT-адміністратор може отримати доступ до інтерфейсу HP Client Management Interface, написавши прості сценарії та інтегрувавши їх у вибране рішення керування.

Завдяки інтерфейсу HP CMI (HP Client Management Interface) нові комп'ютери для бізнес-класу від HP легко інтегруються у кероване інформаційне середовище. HP CMI забезпечує інтерфейс, що спрощує інтеграцію ПК бізнес-класу від HP з популярними засобами керування системою (такими як, наприклад, Microsoft Systems Management Server, IBM Tivoli Software і HP OpenView Operations) і власними розробками компаній. За допомогою інтерфейсу HP CMI засоби і програми керування системою можуть отримувати детальні клієнтські дані й інформацію про стан системи, а також керувати системними параметрами BIOS шляхом безпосереднього обміну даними з

клієнтським комп’ютером, зменшуючи потребу у спеціальному агенті або програмному забезпеченні для досягнення належного рівня інтеграції.

Інтерфейс HP Client Management Interface заснований на галузевих стандартах, серед яких Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) і Advanced Configuration і Power Interface (ACPI). HP CMI – це основна технологія, що використовується у рішеннях HP Client Management Solutions. Завдяки HP CMI компанія HP забезпечує гнучкість у виборі способу керування клієнтськими комп'ютерами HP.

Використовуючи інтерфейс HP Client Management Interface у сполученні зі спеціальними програмами керування системою, можна:

- Отримувати детальні дані – охоплювати всебічну інформацію про процесори, жорсткі диски, пам'ять, BIOS і драйвери, зокрема показники сенсорів (такі як швидкість обертання вентиляторів, напруга і температура).
- Отримувати інформацію про стан системи – реєструватися для отримання широкого діапазону клієнтських повідомлень про стан апаратного забезпечення (таких як перегрівання, зупинення вентилятора і зміна конфігурації обладнання) на консоль керування системою, програму або локальний клієнтський комп'ютер. Повідомлення надсилаються у реальному часі в процесі виникнення ситуацій, пов'язаних з апаратним забезпеченням.
- Керувати системними параметрами BIOS – виконувати функції F10, такі як дистанційне установлення і змінювання паролів BIOS та порядку завантаження пристроїв з консолі керування системою або з будь-якої з ваших клієнтських систем, навіть не підходячи до кожної окремої машини.

Детальнішу інформацію щодо інтерфейсу HP Client Manager Interface див. у розділі http://www.hp.com/go/hpcmi/.

Диспетчер HP SoftPaq Download Manager

HP SoftPaq Download Manager — безкоштовний і зручний інтерфейс для визначення та завантаження оновлень програмного забезпечення на комп’ютери-клієнти HP у вашому середовищі. Вказавши моделі, операційну систему та мову, ви зможете швидко визначити, відсортувати та обрати необхідне програмне забезпечення Softpaq. Щоб завантажити інтерфейс HP SoftPaq Download Manager, відвідайте веб-сторінку http://www.hp.com/go/sdm.

HP System Software Manager

HP System Software Manager (SSM) – це безкоштовна утиліта для автоматизації дистанційного розгортання драйверів пристроїв та оновлень BIOS на мережних бізнес-ПК HP. Після запуску SSM без участі користувача визначає версії драйверів та BIOS, встановлених на кожній мережній клієнтській системі, і порівнює ці дані з перевіреним системним програмним забезпеченням SoftPaqs, яке зберігається на центральному файловому сервері. SSM автоматично оновлює знайдені застарілі версії системного програмного забезпечення на мережних ПК останніми версіями, доступними на файловому сервері. Оскільки SSM дозволяє лише поширення оновлень SoftPaq на відповідні моделі клієнтських систем, адміністратори можуть бути впевненні в ефективності використання SSM для оновлень системного програмного забезпечення.

System Software Manager інтегрується з корпоративними інструментами поширення ПЗ, такими як HP Client Automation solutions, HP Client Manager from Symantec і Microsoft Systems Management Server (SMS). За допомогою SSM можна поширювати оновлення, створені замовником, або оновлення від сторонніх виробників, попередньо перетворивши їх у формат SSM.

SSM можна безкоштовно завантажити з веб-сторінки http://www.hp.com/go/ssm.

ПРИМІТКА. SSM наразі не підтримує віддалене перепрограмування ROM на системах з увімкнутою технологією Windows BitLocker Drive Encryption, де використовуються вимірювання TPM для захисту ключів BitLocker, оскільки перепрограмування BIOS зробило б недійсною довірену сигнатуру, створену технологією BitLocker для платформи. Щоб перепрограмувати системну BIOS, вимкніть технологію BitLocker за допомогою засобу Group Policy (Групова політика).

Можна увімкнути підтримку BitLocker без схем безпеки TPM для BIOS, щоб клавіші BitLocker не стали недійсними. Компанія HP рекомендує створити резервну копію облікових даних BitLocker у випадку аварійного відновлення.

HP ProtectTools Security Manager

Захисне програмне забезпечення HP ProtectTools містить функції безпеки, які допомагають у захисті від неавторизованого доступу до комп'ютера, мереж і критичних даних. Удосконалені функції безпеки надаються нижченаведеними програмними модулями й доступні через програму HP ProtectTools Security Manager:

HP ProtectTools Security Manager — це єдина консоль, через яку можна отримати доступ до всіх інших модулів.

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Credential Manager for ProtectTools
- HP ProtectTools Security Manager
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro for HP ProtectTools

Пакет HP ProtectTools містить дві версії, якими можна скористатися: HP ProtectTools Security Manager і HP ProtectTools Administrative Console. Як адміністраторська, так і користувацька версії доступні в меню **Пуск** > **Усі програми**.

Не всі програмні модулі можна використовувати з кожною моделлю комп'ютера. Наприклад, модуль Embedded Security for HP ProtectTools можна використовувати тільки на комп'ютерах, на яких встановлена мікросхема Trusted Platform Module (TPM).

Модулі програмного забезпечення ProtectTools можуть бути встановлені чи завантажені попередньо або доступні для завантаження на веб-сайті HP. Для вибраних настільних систем HP Pro програмне забезпечення HP ProtectTools доступне як післяпродажна опція. За додатковою інформацією звертайтеся на веб-сайт http://www.hp.com/products/security.

HP Client Automation Starter Edition і Standard Edition

HP Client Automation є рішенням апаратного та програмного забезпечення для Windows Vista, Windows XP та середовищ HP Thin Client, простим у використанні та швидким у розгортанні, яке забезпечує основу для майбутніх вимог. Воно пропонується у двох виданнях:

- Версія Starter Edition є безкоштовним продуктом для управління настільними системами, портативними ПК і робочими станціями HP, який включає апаратне та програмне забезпечення, пульт дистанційного керування, контроль попереджень HP, оновлення параметру HP BIOS і драйверів, інтеграцію з інструментами HP Protect Tools і підтримку додаткових програм для технології Intel AMT. Версія Starter Edition також підтримує розгортання та управління клієнтами HP Thin Clients.
- Версія Standard Edition, доступна для придбання, включає всі функціональні характеристики версії Starter Edition, а також розгортання та міграцію Windows, керування пакетами виправлень, поширення програмного забезпечення та облік його використання.

З версій HP Client Automation Starter Edition і Standard Edition можна перейти на версію HP Client Automation Enterprise Edition (на основі технології Radia) для автоматичного управління масштабними та гетерогенними IT-середовищами, які постійно змінюються.

Детальнішу інформацію щодо рішення HP Client Automation solutions див. на веб-сторінці http://www.hp.com/go/client.

Client Automation Starter Edition, Standard Edition та Enterprise Edition

Версія HP Client Automation Enterprise Edition є рішенням, яке базується на політиці та дозволяє адміністраторам каталогізувати, розгортати, виправляти й постійно керувати програмним забезпеченням і вмістом у межах гетерогенних клієнтських платформ. Версія HP Client Automation Enterprise Edition дозволяє спеціалісту з інформаційних технологій:

- Автоматизувати весь процес керування життєвим циклом, починаючи від знаходження, розгортання і керування поточними ресурсами до переносу і списання.
- Автоматично розгортати і постійно керувати усім комплектом програмного забезпечення (операційні системи, програми, виправлення, параметри і вміст) для досягнення потрібного стану.
- Керувати програмним забезпеченням майже на усіх пристроях, включаючи настільні і переносні комп’ютери і робочі станції в гетерогенній або ізольованій інфраструктурі.
- Керувати програмним забезпеченням в більшості операційних систем.

Програма дозволяє постійно керувати конфігурацією, завдяки цьому клієнти HP повідомляють про значне зменшення витрат у сфері IT, прискорення часу виведення на ринок нового програмного забезпечення і вмісту, а також збільшення продуктивності роботи і задоволення користувачів.

Детальнішу інформацію щодо рішення HP Client Automation solutions див. на веб-сторінці http://www.hp.com/go/client.

HP Client Manager from Symantec

Утиліта HP Client Manager from Symantec, розроблена Altiris, безкоштовна для всіх моделей бізнес-ПК, ноутбуків та робочих станцій HP. SSM інтегрується в HP Client Manager і забезпечує централізоване відстеження, моніторинг та керування апаратними ресурсами клієнтських комп'ютерів HP.

Використовуйте HP Client Manager from Symantec для:

- отримання корисної інформації, такої як тип процесора, пам'ять, графічний адаптер та параметри безпеки
- моніторингу стану системи для виправлення несправностей до їх виникнення
- автоматичного отримання і встановлення драйверів і оновлених версій BIOS, не підходячи до кожного ПК
- дистанційного налаштування параметрів BIOS та безпеки
- автоматизації процесів швидкого вирішення апаратних проблем

Тісна інтеграція з інструментами HP Instant Support дозволяє зменшити час на усунення несправностей з обладнанням.

- Діагностика – дистанційний запуск і перегляд звітів на настільних, портативних системах і робочих станціях від HP
- Перевірка стану системи – перевірка наявності відомих проблем з обладнанням у базі встановлених систем від HP
- Система активного спілкування (чат) – під'єднайтеся до служби підтримки клієнтів HP для усунення несправностей
- База знань HP – доступ до експертної інформації
- Автоматизований процес збору і доставки SoftPaq для швидкого усунення проблем з обладнанням
- Ідентифікація, інвентаризація та ініціалізація систем зі вбудованою мікросхемою безпеки HP ProtectTools
- Параметри відображення повідомлень про стан локально на клієнтській системі
- Звітування основної інвентаризаційної інформації для клієнтів від інших виробників
- Установка і налаштування мікросхеми безпеки TPM
- Централізовано сплануйте резервне копіювання і відновлення клієнта
- Додаткова підтримка для керування Intel AMT

Детальнішу інформацію щодо HP Client Manager from Symantec див. у розділі http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite — це просте у використанні вирішення для керування повним життєвим циклом програмного забезпечення настільних ПК, ноутбуків і робочих станцій. Client Management Suite містить такі продукти Altiris:

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

Детальнішу інформацію щодо Altiris Client Management Suite див. у розділі http://www.symantec.com/business/client-management-suite.

HP Client Catalog for Microsoft System Center & SMS Products

HP Client Catalog дозволяє спеціалістам у сфері IT-технологій за допомогою продуктів Microsoft автоматизувати розгортання оновлень програмного забезпечення HP (Softpaqs) на бізнес-ПК HP. Файл каталогу містить детальну інформацію щодо платформи на настільних системах, ноутбуках і робочих станціях бізнес-класу виробництва HP. Його можна використовувати у сполученні зі спеціальними обліковими записами та функціями оновлення продуктів Microsoft для забезпечення автоматизованого оновлення драйверів і пакетів на керованих клієнтських комп'ютерах HP.

Продукти Microsoft, які підтримуються утилітою HP Client Catalog, включають:

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

Детальнішу інформацію щодо HP Client Catalog для SMS див. у розділі http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

Remote Management Technology (Технологія віддаленого керування)

Моделі оснащено технологією vPro чи стандартною. Обидві дозволяють покращити знаходження, відновлення і захист комп'ютерного обладнання в мережі. Завдяки обом технологіям персональними комп'ютерами можна керувати навіть тоді, коли система перебуває у вимкненому стані або у стані збою.

На бізнес-ПК доступні три форми віддаленого керування: Alert Standard Format (ASF), Intel Active Management Technology (AMT) та Desktop and mobile Architecture for Systems Hardware (DASH).

Технологія віддаленого керування має такі можливості:

- Виявлення мережних комп'ютерів і пристроїв
- Інформація про парк обладнання
- Моніторинг стану платформи
- Керування енергоспоживанням – вмикання/вимикання/скидання живлення
- Дистанційна діагностика і ремонт
  - Переспрямування текстової консолі — робить можливим консольне керування віддаленим ПК на етапі його завантаження
  - Переспрямування носіїв — робить можливим завантаження системи з віддаленого завантажуваного привода, диска або ISO-образу (два режими цієї функції — IDE-Redirect (IDE-R) на платформах AMT та USB Media Redirection)
- Апаратна ізоляція і відновлення – обмеження або перекриття доступу ПК до мережі при виявленні підозрілої активності
- Відстеження й аудит подій платформи
- Інтегрований портал керування веб-сервером для віддаленого доступу та налаштування
- Технології віддаленого керування інтегровано з партнерами консолі керування HP

ПРИМІТКА. Усі вищенаведені функції доступні не на всіх платформах.

Налаштування Intel Management Engine

ПРИМІТКА. Огляд технології Intel vPro можна знайти на сайті http://www.intel.com/vpro.

Інформацію щодо технології Intel vPro, пов'язану з використанням обладнання HP, дивіться у технічних описах на сайті http://www.hp.com/support. Виберіть країну та мову, виберіть пункт **See support and troubleshooting information** (Переглянути інформацію про підтримку і усунення проблем), введіть номер моделі комп'ютера і натисніть клавішу Enter. У категорії **Resources** (Ресурси) виберіть **Manuals (guides, supplements, addendums, etc)** (Посібники, довідники, додатки тощо). У категорії **Quick jump to manuals by category** (Швидкий перехід до посібників за категорією) виберіть **White papers** (Технічні описи).

Доступні технології керування такі:

- AMT (включає DASH 1.0)
- ASF
- DASH 1.1 (з використанням Broadcom NIC)

Технології ASF і AMT не можна конфігурувати одночасно, але вони обидві підтримуються.

Щоб налаштувати систему Intel vPro для роботи з технологією AMT або ASF:

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Microsoft Windows, виберіть **Пуск** > **Завершення роботи** > **Перезавантаження**.
2. Щойно комп'ютер увімкнеться, натисніть гарячу клавішу Ctrl+P, поки комп'ютер не завантажив операційну систему.

ПРИМІТКА. Якщо ви не натиснете клавішу Ctrl+P вчасно, слід перезавантажити комп'ютер і знову натиснути Ctrl+P, поки комп'ютер не завантажив операційну систему.

За допомогою цієї гарячої клавіші відкривається вікно конфігурації Intel Management Engine BIOS Execution (MEBx). Ця програма дозволяє користувачу налаштовувати різні параметри технології керування. Деякі параметри конфігурації наведено нижче:

- Головне меню
  - Конфігурація Intel ® ME
  - Конфігурація Intel ® AMT
  - Змінити пароль Intel ® ME
  - Exit (Вихід)
- Конфігурація платформи Intel ® ME
  - Intel ® ME State Control (Контроль стану платформи ME) (вмикання/вимикання)
  - Intel ® ME Firmware Local Update (Локальне оновлення мікропрограми ME) (вмикання/вимикання)
  - Intel ® ME Features Control (Керування функціями ME)
  - Intel ® ME Power Control (Керування живленням ME)
- Конфігурація Intel ® AMT
  - Host Name (Ім'я головного комп'ютера)
  - TCP/IP
  - Provision Model (Модель автоконфігурації) (корпорація, малий бізнес)
  - Встановлення і конфігурація
  - Un-Provision (Скидання автоконфігурації)
  - SOL/IDE-R (вмикання/вимикання)
  - Політика паролів
  - Secure Firmware Update (Оновлення вбудованого ПЗ із безпеки) (вмикання/вимикання)
  - Встановити PRTC
  - Інтервал очікування
- Зміна пароля Intel ® ME (HP наполегливо рекомендує змінити цей пароль. Пароль за замовчуванням — **admin**.)

Для віддаленого керування системами AMT адміністратор повинен використовувати віддалену консоль, що підтримує AMT. Корпоративні консолі керування доступні від таких постачальників як HP, Altiris і Microsoft SMS. У режимі SMB (малий і середній бізнес) клієнтом надається веб-інтерфейс. Для доступу до цієї функції відкрийте браузер з будь-якої іншої системи в мережі і введіть `http://host_name:16992`, де `host_name` – це ім'я, назначене цій системі. Ви також можете скористатися IP-адресою замість імені сервера.

Для налаштування систем із NIC-платою Broadcom із підтримкою DASH:

Перевірте останню документацію на веб-сайті http://www.hp.com у розділі **Support & Troubleshooting** (Підтримка й усунення неполадок), відтак виберіть конкретну модуль, виберіть пункт **Manuals** (Посібники), а потім **White papers** (Технічні описи) щодо DASH або NIC-плати Broadcom.

Verdiem Surveyor

Verdiem Surveyor – це програмне рішення, що допомагає керувати витратами енергії ПК. Surveyor вимірює, яку кількість енергії споживає кожний комп'ютер і звітує про це. Програма також керує настройками енергоживлення ПК і дає змогу адміністраторам легко реалізовувати стратегії зберігання енергії у мережах. Комплект програм HP SoftPaq, що включає агент Surveyor, можна завантажити на веб-сторінці підтримки HP і встановити на моделях настільних систем для бізнесу, що підтримують використання таких програм. Ліцензії Surveyor для керування ПК можна придбати у представництвах компанії HP.

HP Proactive Change Notification

Програма повідомлення про зміни Proactive Change Notification використовує веб-сайт Subscriber's Choice для виконання таких профілактичних і автоматизованих дій:

- Відсилання поштових повідомлень PCN (Proactive Change Notification) на вашу адресу, де міститиметься опис змін у апаратному і програмному забезпеченні, які мають відбутися у більшості комерційних ПК і серверів, максимум за 60 днів до події
- Відсилання електронних повідомлень з інформаційними бюлетенями, рекомендаціями і коментарями для клієнтів, а також з бюлетенями безпеки і сповіщеннями про вихід нових драйверів для більшості комерційних комп'ютерів та серверів

Ви створюєте власний профіль, щоб гарантовано отримувати лише ту інформацію, що стосується певного IT-середовища. Детальніше дізнатися про програму Proactive Change Notification і те, як створювати власний профіль, можна на веб-сайті http://h30046.www3.hp.com/subhub.php

Subscriber's Choice

Subscriber's Choice – це клієнтська послуга компанії HP.

На основі вашого профілю компанія HP надаватиме вам персоналізовані поради щодо використання продуктів, надсилатиме тематичні статті і/або сповіщення про нові драйвери і можливості підтримки.

Функція сповіщення про нові драйвери і можливості підтримки Subscriber's Choice забезпечує надсилання електронних повідомлень про те, що інформація, яку ви замовили на свій профіль, доступна для перегляду і отримання. Детальніше дізнатися про службу Subscriber's Choice і те, як створювати власний профіль, можна на сайті http://h30046.www3.hp.com/subhub.php

Рішення, що тепер не надаються

Два програмні пакети, Altiris Local Recovery та Dantz Retrospect, більше не постачатимуться з бізнес-ПК, ноутбуками та робочими станціями HP.

5 Флеш-ПЗП

BIOS комп’ютера зберігається у флеш-ПЗП (постійному запам’ятовувальному пристрої) з можливістю програмування. Установивши пароль налаштування за допомогою утиліти Computer Setup (F10), можна захистити ПЗП від випадкового оновлення або перезаписування. Це важливо для забезпечення операційної цілісності комп’ютера. У разі потреби в оновленні BIOS можна завантажити останні образи BIOS зі сторінки драйверів і підтримки HP, http://www.hp.com/support/files.

△ **ПОПЕРЕДЖЕННЯ.** Для максимального захисту ПЗП не забудьте встановити пароль налаштування. Пароль налаштування запобігає неавторизованому оновленню ПЗП. Програма System Software Manager дозволяє системному адміністратору встановити пароль налаштування одночасно на один або кілька ПК. За додатковою інформацією звертайтеся на веб-сайт http://www.hp.com/go/ssm.

Remote ROM Flash

Remote ROM Flash дозволяє системному адміністратору безпечно оновлювати BIOS на віддалених комп'ютерах HP безпосередньо з централізованої консолі керування. Можливість виконувати це завдання дистанційно на кількох комп'ютерах веде до узгодженого розгортання і зростання контролю образів BIOS на мережевих ПК HP. Це також забезпечує більшу продуктивність і нижчу вартість володіння.

ПРИМІТКА. SSM наразі не підтримує віддалене перепрограмування ROM на системах з увімкнутою технологією Windows BitLocker Drive Encryption, де використовуються вимірювання TPM для захисту ключів BitLocker, оскільки перепрограмування BIOS зробило б недійсною довірену сигнатуру, створену технологією BitLocker для платформи. Щоб перепрограмувати системну BIOS, вимкніть технологію BitLocker за допомогою засобу Group Policy (Групова політика).

Для використання можливостей програми Remote ROM Flash необхідно ввімкнути живлення комп'ютера або увімкнути його за допомогою програми Remote Wakeup.

Для отримання додаткової інформації про віддалене перепрограмування ПЗП (Remote ROM Flash) див. HP Client Manager або System Software Manager на веб-сайті http://www.hp.com/go/ssm/.

HPQFlash

Утиліта HPQFlash використовується для локального оновлення чи відновлення системного BIOS в операційній системі Windows на індивідуальних ПК.

Для отримання додаткової інформації про HPQFlash відвідайте веб-сайт http://www.hp.com/support/files і введіть номер моделі комп’ютера у відповідь на запит.

6 Режим Boot Block Emergency Recovery

Режим аварійного відновлення завантажувального блоку Boot Block Emergency Recovery дозволяє виконувати відновлення системи навіть у разі збою флеш-ПЗП. Наприклад, якщо підчас оновлення BIOS стався збій живлення, флеш-ПЗП буде неповним і BIOS не буде працювати. Завантажувальний блок (Boot Block) – це флеш-захищений розділ ПЗП, що містить код для перевірки правильності системного флеш-ПЗП при ввімкненні системи.

- Якщо системний BIOS правильний, система розпочне роботу в нормальному режимі.
- Якщо образ системного BIOS неправильний, надійний Boot Block BIOS надасть додаткову підтримку для пошуку знімного носія для файлів образу BIOS. Якщо знайдено дійсний файл образу BIOS, його автоматично буде записано до ПЗП.

Якщо знайдено неправильний образ BIOS, індикатор живлення системи блимне червоним 8 разів, щосекунди. Водночас пролунає 8 сигналів. Якщо фрагмент системного ПЗП, що містить образ параметрів графічної підсистеми ПЗП, не пошкоджено, на екрані відобразиться **Boot Block Emergency Recovery Mode**.

Після входу в режим Boot Block Emergency Recovery виконайте наступні кроки для відновлення системи:

1. Вимкніть живлення.
2. Вставте компакт-диск чи носій даних USB-флеш, що містять потрібний файл образу BIOS у кореневому каталозі.

   ПРИМІТКА. Носій має бути відформатовано з використанням файлової системи FAT12, FAT16 чи FAT32.

3. Увімкніть комп'ютер.

   Якщо відповідний образ BIOS не знайдено, система попросить вставити носій, що містить файл образу BIOS.

   Якщо перепрограмування ПЗП виконано, система автоматично вимкнеться.

4. Витягніть знімні носії, використовувані для оновлення BIOS.
5. Увімкніть комп'ютер і перезапустіть.

ПРИМІТКА. BitLocker запобігає завантаженню Windows Vista, якщо компакт-диск, що містить образ BIOS є оптичним приводом. Якщо BitLocker активовано, видаліть цей компакт-диск перед спробою завантажити Windows Vista.

7 Тиражування параметрів

Наведені процедури дають адміністраторові можливість легко копіювати одну конфігурацію налаштування на інші комп'ютери тієї ж моделі. Це забезпечує більш швидке й узгоджене налаштування кількох комп'ютерів.

ПРИМІТКА. Для обох процедур необхідний дисковод або носій даних USB-флеш.

ПРИМІТКА. Програму System Software Manager (SSM) можна використовувати для відтворення інформації про налаштування ПК з операційної системи Windows. Для отримання додаткової інформації див. Посібник користувача SSM на веб-сайті http://www.hp.com/go/ssm.

Копіювання на окремий комп'ютер

△ **ПОПЕРЕДЖЕННЯ.** Конфігурація параметрів залежить від конкретної моделі. Різниця у моделях вихідного комп'ютера та комп'ютера призначення може призвести до пошкодження файлової системи. Наприклад, не копіюйте конфігурацію налаштування з моделі ПК dc7xxx на модель ПК dx7xxx.

1. Виберіть конфігурацію параметрів, яку Ви хочете скопіювати. Вимкніть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Завершення роботи**.
2. Якщо ви використовуєте носій даних USB-флеш, підключіть його до комп'ютера.
3. Увімкніть комп'ютер.
4. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп’ютер і знову натиснути F10, поки комп’ютер не завантажив операційну систему.
5. Якщо ви використовуєте дискету, зараз вставте її у дисковод.
6. Виберіть **File** (Файл) > **Replicated Setup** (Тиражування параметрів) > **Save to Removable Media** (Зберегти на змінний носій). Виконайте вказівки на екрані, щоб створити дискету конфігурації або носій даних USB-флеш.
7. Вимкніть комп'ютер, який потрібно налаштувати, і вставте дискету конфігурації або носій даних USB-флеш.
8. Увімкніть комп'ютер, який потрібно налаштувати.
9. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

10. Виберіть **File** (Файл) > **Replicated Setup** (Тиражування параметрів) > **Restore from Removable Media** (Відновити зі змінного носія).

11. Після завершення конфігурації перезапустіть комп'ютер.

Копіювання на кілька комп'ютерів

△ **ПОПЕРЕДЖЕННЯ.** Конфігурація параметрів залежить від конкретної моделі. Різниця у моделях вихідного комп'ютера та комп'ютера призначення може призвести до пошкодження файлової системи. Наприклад, не копіюйте конфігурацію налаштування з моделі ПК dc7xxx на модель ПК dx7xxx.

За цим методом підготовка дискети або носія даних USB-флеш забере трохи більше часу, проте копіювання даних конфігурації на комп'ютери призначення значно прискориться.

ПРИМІТКА. Для цієї процедури або для створення завантажувального носія даних USB-флеш необхідна завантажувальна дискета. Якщо система Windows XP недоступна для створення завантажувальної дискети, використовуйте метод копіювання на один комп'ютер (див. Копіювання на окремий комп'ютер на сторінці 16).

1. Створення завантажувальних дискети або носія даних USB-флеш. Див. розділ Підтримуваний носій даних USB-флеш на сторінці 18 або Непідтримуваний носій даних USB-флеш на сторінці 19.

   △ **ПОПЕРЕДЖЕННЯ.** Не всі комп'ютери можна завантажити з носіїв даних USB-флеш. Якщо за порядком завантаження за замовчуванням в утиліті Computer Setup (F10) USB-пристрій вказано перед жорстким диском, комп'ютер може завантажуватися з носія даних USB-флеш. В іншому разі необхідно використовувати дискету.

2. Виберіть конфігурацію параметрів, яку Ви хочете копіювати. Вимкніть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Завершення роботи**.

3. Якщо ви використовуєте носій даних USB-флеш, підключіть його до комп'ютера.

4. Увімкніть комп'ютер.

5. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп’ютер і знову натиснути F10, поки комп’ютер не завантажив операційну систему.

6. Якщо ви використовуєте дискету, зараз вставте її у дисковод.

7. Виберіть **File** (Файл) > **Replicated Setup** (Тиражування параметрів) > **Save to Removable Media** (Зберегти на змінний носій). Виконайте вказівки на екрані, щоб створити дискету конфігурації або носій даних USB-флеш.

8. Завантажте утиліту BIOS для тиражування параметрів (repset.exe) і копіюйте її на дискету або носій даних USB-флеш. Цю утиліту можна отримати на веб-сайті http://welcome.hp.com/country/us/en/support.html. Для цього треба вказати номер моделі комп’ютера.

9. На дискеті конфігурації або носії даних USB-флеш створіть файл autoexec.bat з такою командою:

   ```
   repset.exe
   ```

10. Вимкніть комп'ютер, який потрібно налаштувати. Вставте дискету конфігурації або носій даних USB-флеш і ввімкніть комп'ютер. Конфігураційну утиліту буде запущено автоматично.

11. Після завершення конфігурації перезапустіть комп'ютер.

Створення завантажувального пристрою

Підтримуваний носій даних USB-флеш

Підтримувані пристрої містять попередньо встановлений образ для спрощеного перетворення їх на завантажувальні. Усі носії даних USB-флеш виробництва HP чи Compaq та більшість інших таких пристроїв містять згаданий попередньо встановлений образ. Якщо використовуваний носій даних USB-флеш не містить цей образ, ви можете скористатися процедурою пізніше у цьому розділі (див. розділ Непідтримуваний носій даних USB-флеш на сторінці 19).

Для створення завантажувального носія даних USB-флеш необхідно мати:

- носій даних USB-флеш, що підтримується
- завантажувальну дискету DOS, яка містить програми FDISK і SYS (Якщо програма SYS недоступна, можна використати програму FORMAT, проте в такому разі буде втрачено усі файли на носії даних USB-флеш.)
- ПК, який можна завантажити з носія даних USB-флеш

△ **ПОПЕРЕДЖЕННЯ.** Деякі старі ПК не можна завантажити з носія даних USB-флеш. Якщо за порядком завантаження за замовчуванням в утиліті Computer Setup (F10) USB-пристрій вказано перед жорстким диском, комп'ютер може завантажуватися з носія даних USB-флеш. В іншому разі необхідно використовувати дискету.

1. Вимкніть комп'ютер.

2. Вставте носій даних USB-флеш в один із портів USB комп'ютера і видаліть усі змінні носії USB, окрім USB-приводів для зчитування гнучких дисків.

3. Вставте завантажувальну дискету з DOS, що містить FDISK.COM і SYS.COM або FORMAT.COM, у дисковод і увімкніть комп'ютер, щоб завантажитися з дискети з DOS.

4. Запустіть програму FDISK з рядка **A:**, набравши `FDISK` і натиснувши Enter. На вимогу клацніть **Так** (**Y**), щоб увімкнути підтримку великих дисків.

5. Введіть свій вибір [`5`] для відображення накопичувачів у системі. Носій даних USB-флеш відповідатиме за розміром одному із дисків у списку. Він завжди буде останнім за порядком. Запишіть літеру цього диска.

   Диск носія даних USB-флеш: _____

   △ **ПОПЕРЕДЖЕННЯ.** Якщо літера диска не відповідає пристрою USB-флеш, ви не можете продовжувати виконання процедури. Можлива втрата даних. Перевірте усі USB-порти на наявність додаткових носіїв даних. Якщо такі пристрої є, витягніть їх, перезавантажте комп'ютер і продовжуйте з кроку 4. Якщо таких пристроїв немає, то система не підтримує носій даних USB-флеш або носій даних USB-флеш пошкоджено. НЕ продовжуйте спроби створення завантажувального носія даних USB-флеш.

6. Вийдіть з програми FDISK, натиснувши клавішу Esc, щоб повернутися до рядка **A:**.

7. Якщо ваша завантажувальна дискета з DOS містить програму SYS.COM, перейдіть до кроку 8. В іншому разі перейдіть до кроку 9.

8. У рядку **A:** введіть `SYS x:`, де x – літера диска, яку ви записали раніше.

△ **ПОПЕРЕДЖЕННЯ.** Перевірте, чи ви правильно ввели літеру диска для носія даних USB-флеш.

Після перенесення системних файлів програма SYS знову відобразить рядок **A:**. Перейдіть до кроку 13.

9. Скопіюйте усі файли, які ви хочете перенести з носія даних USB, у тимчасовий каталог на іншому диску (наприклад, на внутрішньому системному жорсткому диску).

10. У рядку **A:** введіть `FORMAT /S X:`, де `X` – літера диска, яку ви записали раніше.

△ **ПОПЕРЕДЖЕННЯ.** Перевірте, чи ви правильно ввели літеру диска для носія даних USB-флеш.

FORMAT відобразить одне або декілька попереджень і запит на продовження виконання операції. Щоразу вводьте `Y`. FORMAT відформатує носій даних USB-флеш, додасть системні файли і попросить ввести мітку тому.

11. Натисніть Enter або введіть мітку за бажанням.

12. Скопіюйте файли, збережені на кроці 9, на носій даних USB-флеш.

13. Витягніть дискету і перезавантажте комп'ютер. Комп'ютер завантажиться з носія даних USB-флеш, як з диска C.

ПРИМІТКА. Порядок завантаження за замовчуванням залежить від конкретного комп'ютера і може бути змінений в утиліті Computer Setup (F10).

Якщо ви скористалися версією для DOS у Windows 9x, то, можливо, на декілька секунд побачите екран з логотипом Windows. Щоб цей екран не з'являвся, додайте порожній файл з назвою LOGO.SYS у кореневий каталог носія даних USB-флеш.

Поверніться до розділу Копіювання на кілька комп'ютерів на сторінці 17.

Непідтримуваний носій даних USB-флеш

Для створення завантажувального носія даних USB-флеш необхідно мати:

- носій даних USB-флеш
- завантажувальну дискету DOS, яка містить програми FDISK і SYS (Якщо програма SYS недоступна, можна використати програму FORMAT, проте в такому разі буде втрачено усі файли на носії даних USB-флеш.)
- ПК, який можна завантажити з носія даних USB-флеш

△ **ПОПЕРЕДЖЕННЯ.** Деякі старі ПК не можна завантажити з носія даних USB-флеш. Якщо за порядком завантаження за замовчуванням в утиліті Computer Setup (F10) USB-пристрій вказано перед жорстким диском, комп'ютер може завантажуватися з носія даних USB-флеш. В іншому разі необхідно використовувати дискету.

1. Якщо в системі є PCI-плати з підключеними дисками SCSI, ATA RAID або SATA, вимкніть комп'ютер і відключіть шнур живлення.

   △ **ПОПЕРЕДЖЕННЯ.** Шнур живлення ОБОВ'ЯЗКОВО потрібно вимкнути.

2. Відкрийте корпус комп'ютера і витягніть PCI-плати.
3. Вставте носій даних USB-флеш у один з портів USB комп'ютера і видаліть усі змінні носії USB окрім USB-приводів для зчитування гнучких дисків. Закрийте корпус комп'ютера.
4. Під'єднайте шнур живлення й увімкніть комп'ютер.
5. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп’ютер і знову натиснути F10, поки комп’ютер не завантажив операційну систему.

6. Перейдіть до розділу **Advanced** (Додатково) > **PCI Devices** (Пристрої PCI), щоб вимкнути обидва контролери PATA і SATA. При вимиканні контролера SATA запишіть IRQ, якому призначено даний контролер. Пізніше може знадобитися перепризначити IRQ. Вийдіть із налаштування, потім слід підтвердити зміни.

   SATA IRQ: _____

7. Вставте завантажувальну дискету з DOS, що містить FDISK.COM і SYS.COM або FORMAT.COM, у дисковод і увімкніть комп'ютер, щоб завантажитися з дискети з DOS.
8. Запустіть програму FDISK і видаліть усі розділи на носії даних USB-флеш. Створіть новий розділ і позначте його як активний. Вийдіть з програми FDISK, натиснувши клавішу Esc.
9. Якщо система автоматично не перезавантажиться після виходу з програми FDISK, натисніть Ctrl+Alt+Del для перезавантаження з дискети DOS.
10. У рядку **A:** введіть `FORMAT C: /S` і натисніть Enter. Буде відформатовано носій даних USB-флеш, додано системні файли, а також з'явиться запит на мітку тому.
11. Натисніть Enter або введіть мітку за бажанням.
12. Вимкніть комп'ютер і витягніть шнур живлення. Відкрийте корпус комп'ютера і встановіть PCI-плати, які ви попередньо витягнули. Закрийте корпус комп'ютера.
13. Під'єднайте шнур живлення, витягніть дискету й увімкніть комп'ютер.
14. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.
15. Перейдіть до розділу **Advanced** (Додатково) > **PCI Devices** (Пристрої PCI) і знову ввімкніть контролери PATA і SATA, які Ви вимкнули під час виконання кроку 6. Назначте контролеру SATA його початковий IRQ.
16. Збережіть зміни і вийдіть. Комп'ютер завантажиться з носія даних USB-флеш, як з диска C.

ПРИМІТКА. Порядок завантаження за промовчанням різниться залежно від комп’ютера, і його можна змінити в утиліті Computer Setup (F10). Див. документ *Утиліта Computer Setup (F10)* для отримання інструкцій.

Якщо ви скористалися версією для DOS у Windows 9x, ви, можливо, на декілька секунд побачите екран з логотипом Windows. Щоб цей екран не з'являвся, додайте порожній файл з назвою LOGO.SYS у кореневий каталог носія даних USB-флеш.

Поверніться до розділу Копіювання на кілька комп'ютерів на сторінці 17.

8 Кнопка живлення з двома положеннями

Якщо увімкнуто функцію Advanced Configuration і Power Interface (ACPI), кнопка живлення може функціонувати як кнопка вмикання/вимикання, а також як кнопка переходу в режим очікування. В режимі очікування живлення комп'ютера не вимикається повністю, однак комп'ютер перебуває у стані низького енергоспоживання. Це дозволить вам швидко вимикати комп'ютер без закриття програм і повертатися до того самого стану роботи без будь-якої втрати даних.

Щоб змінити конфігурацію кнопки живлення, виконайте таку процедуру:

1. Клацніть лівою кнопкою миші на кнопці **Пуск** і виберіть **Панель керування** > **Електроживлення**.
2. У властивостях **Електроживлення** виберіть вкладку **Додатково**.
3. У розділі **Кнопка живлення** виберіть **Перехід до режиму очікування**.

Після налаштування кнопки очікування для функціонування як кнопка переходу в режим очікування натисніть кнопку живлення для переходу системи в режим низького енергоспоживання (очікування). Натисніть кнопку ще раз для швидкого повернення системи в режим повного енергоспоживання. Для повного вимкнення системи натисніть і утримуйте кнопку живлення протягом чотирьох секунд.

△ **ПОПЕРЕДЖЕННЯ.** Не використовуйте кнопку живлення для вимикання комп'ютера, якщо система не відповідає; вимикання живлення без участі операційної системи може призвести до пошкодження жорсткого диска або втрати даних.

9 Підтримка через веб-сайт HP

Інженери компанії HP ретельно тестують і вдосконалюють програмне забезпечення виробництва HP та інших компаній, а також розробляють спеціальне програмне забезпечення, призначене для конкретних операційних систем, щоб забезпечити високу продуктивність, сумісність і надійність для комп'ютерів HP.

При переході на нову або оновлену операційну систему важливо забезпечити роботу програмного забезпечення підтримки, розробленого для цієї ОС. Якщо ви плануєте користуватися іншою версією Microsoft Windows, ніж та, що встановлена на вашому комп'ютері, вам необхідно буде встановити відповідні драйвери пристроїв і утиліти, щоб забезпечити підтримку і належну роботу всіх можливостей системи.

Компанія HP зробила завдання пошуку, отримання, оцінки та встановлення останнього програмного забезпечення для підтримки простішим. Програмне забезпечення можна завантажити з веб-сайту http://www.hp.com/support.

Цей веб-сайт містить свіжі драйвери пристроїв, утиліти і образи ПЗП, необхідні для запуску останньої версії операційної системи Microsoft Windows на вашому комп'ютері HP.

10 Галузеві стандарти

Рішення компанії HP для керування інтегруються з іншими програмами для керування системами і створені на основі галузевих стандартів, наприклад:

- Протокол WBEM (Web-Based Enterprise Management) для керування підприємством на основі веб-технологій
- Інструментарій WMI (Windows Management Interface) для керування ОС Windows
- Технологія “Wake on LAN”
- ACPI
- SMBIOS
- Підтримка функції PXE (Pre-boot Execution)

11 Відстеження ресурсів і безпека

Функції відстеження ресурсів, вбудовані в комп’ютер, надають дані відстеження, що можуть керуватися за допомогою програмних рішень HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager, а також інших програм для керування системою. Органічна автоматична інтеграція між функціями відстеження ресурсів і цими продуктами дає змогу вам вибирати інструмент керування, найбільш придатний для вашого середовища, а також керувати капіталовкладеннями у наявні інструменти.

HP також пропонує декілька рішень для контролю доступу до цінних компонентів та даних. Якщо встановлено програму HP Embedded Security for ProtectTools, ви можете блокувати несанкціонований доступ до даних, перевіряти цілісність системи і виконувати автентифікацію інших користувачів, що прагнуть отримати доступ до системи. (Щоб отримати детальнішу інформацію, див. *Посібник до HP ProtectTools Security Manager* на веб-сайті http://www.hp.com/products/security.) Функції безпеки, такі як HP Embedded Security for ProtectTools, Smart Cover Sensor і Smart Cover Lock, доступні для деяких моделей, допомагають запобігти несанкціонованому доступу до внутрішніх компонентів ПК. Вимикаючи паралельні, послідовні або USB-порти, або вимикаючи можливість завантаження зі змінного носія, можна захистити цінні ресурси. Попередження про зміну пам’яті (Memory Change) і відкриття корпусу (Smart Cover Sensor) можна автоматично перенаправляти до програм керування системою, забезпечуючи проактивні сповіщення про втручання у внутрішні компоненти комп’ютера.

ПРИМІТКА. Функції HP Embedded Security for ProtectTools, Smart Cover Sensor і Smart Cover Lock доступні як додаткові варіанти постачання тільки для деяких систем.

Для керування параметрами безпеки на комп'ютері HP використовуйте такі утиліти:

- Локально, за допомогою утиліт Computer Setup. Див. *Посібник з використання утиліти Computer Setup (F10)*, наданий разом із комп’ютером, для отримання додаткових відомостей та інструкцій щодо використання утиліт Computer Setup.
- Дистанційно, з використанням HP Client Manager from Symantec, HP Client Automation або System Software Manager. Це програмне забезпечення дає змогу організовувати безпечне й узгоджене розгортання і контролювати параметри безпеки.

Наступні таблиця і розділи стосуються функцій керування безпекою, що використовуються на комп'ютері локально за допомогою утиліт Computer Setup (F10).

Таблиця 11-1 Огляд функцій безпеки

Параметр	Опис
Setup Password (Пароль налаштування)	Дозволяє встановити та увімкнути пароль налаштування (пароль адміністратора). **ПРИМІТКА.** Якщо встановлено пароль налаштування, необхідно змінити параметри Computer Setup, флеш-ПЗП і внести зміни в деякі параметри “plug and play” у Windows.

Таблиця 11-1 Огляд функцій безпеки (продовження)

Power-On Password (Пароль завантаження)	Дозволяє встановити й задіяти пароль вмикання. Запит пароля завантаження буде здійснено після кожного циклу завантаження. Якщо користувач не введе правильний пароль завантаження, пристрій не завантажиться. **ПРИМІТКА.** Цей пароль не з'являтиметься після "теплого старту", як, наприклад, при натисканні Ctrl+Alt+Delete або при виборі **Restart from Windows** (Перезавантаження системи у Windows), доки цей параметр не буде включений у нижчезазначеному розділі **Password Options** (Параметри пароля).
Password Options (Параметри пароля) (Цей варіант вибору з'являється, тільки якщо встановлено пароль вмикання або налаштування.)	Дозволяє: • Заблокувати застарілі пристрої (з'являється, якщо встановлено пароль налаштування) • Вмикати/вимикати режим мережевого сервера (з'являється, якщо встановлено пароль вмикання) • Визначає, чи потрібне введення паролю після "теплого старту" (Ctrl+Alt+Delete) (з'являється, якщо встановлено пароль вмикання) • Вмикати/вимикати режим перегляду параметрів (з'являється, якщо встановлено пароль налаштування) (дозволяє переглядати, але не змінювати, параметри F10 Setup Options без введення паролю налаштування) • Вмикати/вимикати обов'язковий пароль (з'являється, якщо встановлено пароль вмикання), який, за умови активації, пропускає встановлену перемичку паролю та вимикає пароль вмикання. Див. *Посібник з керування настільними системами* для отримання додаткової інформації.
Smart Cover (Кришка корпусу) (для деяких моделей)	Дозволяє: • Блокувати/розблоковувати функцію Cover Lock. • Налаштовувати функцію Cover Removal Sensor: Disable/Notify User/Setup Password (Вимкнути/Повідомити користувача/Встановити пароль). **ПРИМІТКА.** *Notify User* (Повідомити користувача) попереджає користувача, якщо сенсор виявив переміщення кришки корпуса. *Setup Password* (Пароль налаштування) вимагає введення пароля для завантаження комп'ютера, якщо сенсор виявив переміщення кришки корпуса. Ця функція підтримується лише у деяких моделях.
Device Security (Безпека пристроїв)	Дозволяє налаштовувати відображення/приховування таких пристроїв: • Serial ports (Послідовні порти) • Parallel port (Паралельний порт) • Задні порти USB • Front USB ports (Передні порти USB) • Внутрішні порти USB • System audio (Аудіосистема) • Network controllers (Мережеві контролери) (деякі моделі) • Застаріла дискета: • Embedded security device (Вбудований пристрій безпеки) (деякі моделі) • SATA0 • SATA1 (деякі моделі)

Таблиця 11-1 Огляд функцій безпеки (продовження)

	• SATA2 (деякі моделі) • SATA3 (деякі моделі) • eSATA (деякі моделі)
LoJack for HP ProtectTools	Дозволяє віддалено здійснювати моніторинг комп'ютера, керувати ним і відстежувати його. Після активації програма LoJack Pro for HP ProtectTools налаштовується з центру підтримки клієнтів Absolute Software. У центрі підтримки клієнтів адміністратор може налаштувати LoJack for HP ProtectTools на моніторинг комп'ютера або керування ним. У разі зміни розташування або викрадення системи центр підтримки клієнтів може допомогти місцевим уповноваженим органам відшукати та повернути комп'ютер на місце. Після налаштування програма LoJack Pro продовжуватиме функціонувати навіть у разі стирання або заміни жорсткого диска.
Network Service Boot (Завантаження через мережу)	Дозволяє вмикати/вимикати можливість комп'ютера завантажувати операційну систему, встановлену на мережевому сервері. (Функція доступна тільки для моделей з NIC; мережевий адаптер має бути або платою для шини PCI, або вбудований на материнській платі.)
System IDs (Системні ідентифікатори)	Дозволяють налаштовувати: • Код ресурсу (18-байтовий ідентифікатор) чи ідентифікаційний номер властивості, призначеного компанією цьому комп'ютеру. • Код власника (80-байтовий ідентифікатор), що відображається під час перевірки POST. • Серійний номер корпуса або номер універсального унікального ідентифікатора (Universal Unique Identifier – UUID). UUID може бути оновлено, тільки якщо поточний серійний номер корпуса неправильний. (Ці номери ідентифікаторів стандартно встановлюються під час виробництва і використовуються для ідентифікації системи.) • Параметри розкладки клавіатури (наприклад, англійська або німецька) для введення системного ідентифікатора.
DriveLock Security (Функція безпеки DriveLock)	Дозволяє призначити або змінити пароль адміністратора або користувача для жорстких дисків. Якщо функцію увімкнуто, то впродовж самотестування при увімкненні живлення користувачеві потрібно буде вводити один з паролів DriveLock. Якщо паролі введено неправильно, жорсткий диск буде недоступним до введення правильного пароля під час наступного "холодного старту". **ПРИМІТКА.** Цей варіант з'явиться, тільки якщо до системи підключено як мінімум один диск з підтримкою функції DriveLock.
Setup Security Level (Рівень безпеки Setup)	Надає користувачам обмежений доступ до меню налаштувань з можливістю зміни деяких параметрів, без запиту пароля налаштування. Ця функція дозволяє адміністратору заборонити зміни важливих параметрів без позбавлення користувача можливості перегляду системної конфігурації і зміни другорядних параметрів. Адміністратор визначає права доступу до кожного окремого значення системних параметрів через меню Setup Security Level. За замовчуванням усім параметрам призначається пароль налаштування, а це означає, що користувачу треба буде ввести правильний пароль під час процедури POST для зміни будь-якого з параметрів. Адміністратор може вимкнути паролі для деяких пунктів, дозволивши користувачу змінювати вказані параметри, якщо для доступу до конфігурації було введено неправильний пароль. Функція None (Немає) замінюється функцією Power-On Password (Пароль вмикання), якщо її увімкнено. **ПРИМІТКА.** Режим перегляду параметрів Setup має бути увімкнено, щоб користувач міг входити в меню Setup без введення пароля налаштування.
System Security (Безпека системи) (для деяких моделей ці параметри залежать від обладнання)	Data Execution Prevention (Заборона виконання даних) (деякі моделі) (enable/disable) (увімкнути/вимкнути) запобігає виникненню порушень у захисті операційної системи. Virtualization Technology (Технологія віртуалізації) (enable/disable) (увімкнути/вимкнути) контролює функції віртуалізації процесора. Для зміни цього параметра необхідно увімкнути і вимкнути комп'ютер.

Таблиця 11-1 Огляд функцій безпеки (продовження)

	Virtualization Technology Directed I/O (Спрямований ввід/вивід технології віртуалізації) (деякі моделі) (enable/disable) (увімкнути/вимкнути) контролює функції віртуалізації перерозподілу даних DMA мікросхеми. Для зміни цього параметра необхідно увімкнути і вимкнути комп'ютер. Trusted Execution Technology (Надійна технологія виконання) (деякі моделі) (enable/disable) (увімкнути/вимкнути) контролює базові функції процесора та мікросхем, необхідні для підтримки віртуального пристрою. Для зміни цього параметра необхідно увімкнути і вимкнути комп'ютер. Щоб увімкнути цю функцію, необхідно увімкнути такі функції: • Підтримка вбудованого пристрою безпеки • Технологія віртуалізації • Технологія віртуалізації Intel - напрямлене введення і виведення Embedded Security Device Support (Підтримка вбудованого пристрою безпеки) (деякі моделі) (enable/disable) (увімкнути/вимкнути) дає дозвіл на вмикання та вимикання вбудованого пристрою безпеки. Для зміни цього параметра необхідно увімкнути і вимкнути комп'ютер. **ПРИМІТКА.** Щоб налаштувати вбудований пристрій безпеки, необхідно задати пароль налаштування. • Reset to Factory Settings (Відновити заводські параметри) (деякі моделі) (Do not reset/ Reset) (Не відновлювати/Відновити) – відновлення заводських параметрів призведе до видалення всіх ключів безпеки. Для зміни цього параметра необхідно увімкнути і вимкнути комп'ютер. **ПОПЕРЕДЖЕННЯ.** Вбудований пристрій безпеки – один з найважливіших компонентів багатьох схем безпеки. У разі стирання ключів безпеки доступ до даних, захищених вбудованим пристроєм безпеки, буде неможливим. Вибір параметра "Reset to Factory Settings" (Скинути параметри до заводських значень) може призвести до втрати значного обсягу даних. • Reset authentication credentials (Скинути дані про успішну перевірку справжності) (деякі моделі) (Do not reset/Reset) (Не скидати/Скинути) – скидання вимикає підтримку перевірки справжності при завантаженні та стирає інформацію автентифікації вбудованого пристрою безпеки. Для зміни цього параметра необхідно увімкнути і вимкнути комп'ютер OS management of Embedded Security Device (Керування вбудованим пристроєм безпеки з операційної системи) (деякі моделі) (enable/disable) (увімкнути/вимкнути) дозволяє користувачу обмежувати контроль операційної системи над вбудованим пристроєм безпеки. Для зміни цього параметра необхідно увімкнути і вимкнути комп'ютер. Вмикання цього параметра дозволяє користувачеві обмежувати керування вбудованим пристроєм безпеки через ОС. • Reset of Embedded Security Device through OS (Скидати параметри вбудованого пристрою безпеки через операційну систему) (деякі моделі) (enable/disable) (увімкнути/вимкнути) дозволяє користувачу обмежувати можливість операційної системи робити запит на відновлення заводських параметрів вбудованого пристрою безпеки. Для зміни цього параметра необхідно увімкнути і вимкнути комп'ютер. **ПРИМІТКА.** Щоб увімкнути цей параметр, необхідно вказати пароль налашту-вання. PAVP (деякі моделі) (вимкнути/мін./макс.) - PAVP вмикає Protected Audio Video Path (Захищений аудіо/відеотракт) у мікросхемі. Це дасть можливість перегляду захищеного вмісту високої чіткості зображення, який за інших умов може бути захищений від відтворення. При виборі параметру Max (Максимальний) 96 Мб системної пам'яті буде призначено PAVP.

Використання пароля

Використання пароля вмикання запобігає несанкціонованому використанню комп'ютера. Необхідно вводити пароль для доступу до програм або даних щоразу при вмиканні або перезапуску комп'ютера. Пароль налаштування запобігає несанкціонованому доступу до

утиліти Computer Setup і може також використовуватися як заміна пароля вмикання. Тобто коли видається запит на введення пароля вмикання, замість нього для отримання доступу до комп'ютера можна ввести пароль налаштування.

Глобальний мережевий пароль налаштування встановлюється для того, щоб дозволити системному адміністратору входити в мережеві системи для проведення обслуговування, не знаючи пароля вмикання, навіть якщо такий пароль встановлено.

ПРИМІТКА. Програму System Software Manager (SSM) можна використовувати для створення паролів BIOS і керування ними з операційної системи Windows. Для отримання додаткової інформації див. Посібник користувача SSM на веб-сайті http://www.hp.com/go/ssm.

ПРИМІТКА. HP Client Management Interface (HP CMI) надає доступ до керування параметрами BIOS, зокрема до паролів BIOS, з операційної системи Windows. Для отримання додаткових відомостей див. HP Client Management Interface Technical Whitepaper (Технічний опис HP Client Management Interface) за адресою http://www.hp.com/go/hpcmi.

Встановлення пароля налаштування з використанням утиліти Computer Setup

Якщо систему обладнано вбудованим пристроєм безпеки, див. *Посібник до HP ProtectTools Security Manager* за адресою http://www.hp.com. Установивши пароль налаштування за допомогою утиліти Computer Setup, можна запобігти переналаштуванню комп'ютера (використанню утиліти Computer Setup (F10)), доки не буде введено пароль.

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Перезавантаження**.
2. Щойно комп'ютер увімкнеться, натисніть клавішу F10, поки комп'ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп'ютер і знову натиснути F10, поки комп'ютер не завантажив операційну систему.
3. Виберіть **Security** (Безпека), потім виберіть **Setup Password** (Пароль налаштування) і дотримуйтесь вказівок на екрані.
4. Перед тим як вийти, натисніть **File** (Файл) > **Save Changes and Exit** (Зберегти зміни і вийти).

Встановлення пароля вмикання з використанням утиліти Computer Setup

Встановлений за допомогою утиліти Computer Setup пароль вмикання запобігає доступу до комп'ютера при вмиканні живлення до того моменту, поки не буде введено пароль. Коли встановлено пароль вмикання, програма Computer Setup відображує пункт **Password Options** (Параметри пароля) в меню **Security** (Безпека). Серед параметрів пароля є параметр **Password**

Prompt on Warm Boot (Запит пароля при “теплому старті”). Коли увімкнено **Password Prompt on Warm Boot**, пароль необхідно вводити кожного разу при завантаженні комп'ютера.

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Перезавантаження**.
2. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп’ютер і знову натиснути F10, поки комп’ютер не завантажив операційну систему.

3. Виберіть **Security** (Безпека), потім **Power-On Password** (Пароль вмикання) і дотримуйтесь вказівок на екрані.
4. Перед тим як вийти, натисніть **File** (Файл) > **Save Changes and Exit** (Зберегти зміни і вийти).

Введення пароля увімкнення живлення

Щоб ввести пароль вмикання, виконайте таку процедуру:

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Restart the Computer** (Перезапустіть комп’ютер).
2. Коли на дисплеї з'явиться піктограма ключа, введіть поточний пароль, потім натисніть Enter.

ПРИМІТКА. Вводьте пароль уважно; з міркувань безпеки введені вами літери не відображаються на екрані.

Якщо пароль введено неправильно, з'явиться піктограма зламаного ключа. Спробуйте ще раз. Після трьох невдалих спроб необхідно вимкнути комп'ютер, а потім увімкнути його ще раз, щоб продовжити.

Введення пароля налаштування

Якщо систему обладнано вбудованим пристроєм безпеки, див. *Посібник до HP ProtectTools Security Manager* за адресою http://www.hp.com.

Якщо на комп'ютері встановлено пароль налаштування, його потрібно буде вводити кожного разу при запуску Computer Setup.

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Перезавантаження**.
2. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп’ютер і знову натиснути F10, поки комп’ютер не завантажив операційну систему.

3. Коли на дисплеї з'явиться піктограма ключа, введіть пароль налаштування, потім натисніть Enter.

ПРИМІТКА. Вводьте пароль уважно; з міркувань безпеки введені вами літери не відображаються на екрані.

Якщо пароль введено неправильно, з'явиться піктограма зламаного ключа. Спробуйте ще раз. Після трьох невдалих спроб необхідно вимкнути комп'ютер, а потім увімкнути його ще раз, щоб продовжити.

Зміна пароля вмикання або пароля налаштування

Якщо систему обладнано вбудованим пристроєм безпеки, див. *Посібник до HP ProtectTools Security Manager* за адресою http://www.hp.com.

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Restart the Computer** (Перезапустіть комп'ютер).
2. Для зміни пароля вмикання живлення перейдіть до кроку 3.

   Щоб змінити пароль налаштування, щойно комп'ютер увімкнеться, натисніть клавішу F10, поки комп'ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп'ютер і знову натиснути F10, поки комп'ютер не завантажив операційну систему.
3. Коли з'явиться піктограма ключа, введіть поточний пароль, косу риску (/) або інший розділовий знак, новий пароль, ще одну риску (/) або інший розділовий знак і, нарешті, новий пароль, як показано: `поточний пароль/новий пароль/новий пароль`

   ПРИМІТКА. Вводьте пароль уважно; з міркувань безпеки введені вами літери не відображаються на екрані.
4. Натисніть Enter.

Новий пароль набере сили при наступному вмиканні комп'ютера.

ПРИМІТКА. Див. розділ Розділові знаки на різних клавіатурних розкладках на сторінці 32 для отримання інформації про альтернативні розділові знаки. Пароль вмикання і пароль налаштування можна змінити також за допомогою пункту Security options (Параметри безпеки) в утиліті Computer Setup.

Видалення пароля вмикання або пароля налаштування

Якщо систему обладнано вбудованим пристроєм безпеки, див. *Посібник до HP ProtectTools Security Manager* за адресою http://www.hp.com.

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Restart the Computer** (Перезапустіть комп'ютер).
2. Для видалення пароля вмикання живлення перейдіть до кроку 3.

   Щоб видалити пароль налаштування, щойно комп'ютер увімкнеться, натисніть клавішу F10, поки комп'ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп'ютер і знову натиснути F10, поки комп'ютер не завантажив операційну систему.
3. Коли з'явиться основна піктограма, введіть поточний пароль і косу риску (/) або альтернативний розділовий символ, як показано: `поточний пароль/`
4. Натисніть Enter.

ПРИМІТКА. Див. розділ Розділові знаки на різних клавіатурних розкладках на сторінці 32 для отримання інформації про альтернативні розділові знаки. Пароль вмикання і пароль налаштування можна змінити також за допомогою пункту Security options (Параметри безпеки) в утиліті Computer Setup.

Розділові знаки на різних клавіатурних розкладках

Клавіатури створюються у відповідності до локальних вимог. Синтаксис і клавіші, що ви їх використовуєте для зміни або видалення пароля, залежать від типу клавіатури, що постачалася з вашим комп'ютером.

Розділові знаки на різних клавіатурних розкладках

/	Арабська	-	Грецька	/	Російська
=	Бельгійська	.	Іврит	-	Словацька
-	БГХЧСС*	-	Угорська	-	Іспанська
/	Бразильська	-	Італійська	/	Шведська/фінська
/	Китайська	/	Японська	-	Швейцарська
-	Чеська	/	Корейська	/	Тайванська
-	Датська	-	Латиноамериканська	/	Тайська
!	Французька	-	Норвезька	.	Турецька
й	Канадська французька	-	Польська	/	Американська англійська
-	Німецька	-	Португальська		

* Боснія-Герцеговина, Хорватія, Чорногорія, Сербія і Словенія

Скидання паролів

Якщо Ви забули пароль, ви не зможете отримати доступ до комп'ютера. Див. *Інструкції з усунення несправностей* для отримання інструкцій з видаленні паролів.

Якщо систему обладнано вбудованим пристроєм безпеки, див. *Посібник до HP ProtectTools Security Manager* за адресою http://www.hp.com.

DriveLock

DriveLock є стандартною функцією безпеки, що допомагає запобігти несанкціонованому доступу до даних на жорсткому диску ATA. DriveLock реалізовано як розширення утиліти Computer Setup. Ця функція доступна тільки за наявності жорстких дисків, що підтримують набір команд ATA Security. DriveLock призначено для клієнтів HP, для яких головною є безпека даних. Для таких клієнтів вартість жорсткого диска і втрата даних, що на ньому зберігаються, є несуттєвими порівняно зі збитками, спричиненими несанкціонованим доступом до вмісту таких даних. Для урівноваження зазначеного рівня безпеки і практичної необхідності у розв'язанні проблеми забутого пароля функція DriveLock від HP використовує двопарольну схему безпеки. Один пароль призначено для встановлення і використання системним адміністратором, тоді як інший зазвичай встановлюється і використовується кінцевим користувачем. У даній схемі відсутній “чорний вхід”, що може бути використаний для розблокування диску, якщо обидва паролі втрачено. Таким чином, використання DriveLock є найбільш безпечним, коли дані, що містяться на жорсткому

диску, дублюються в корпоративній системі даних або регулярно створюються їх резервні копії. Якщо обидва паролі DriveLock втрачено, жорсткий диск відображається як невикористовуваний. Для користувачів, які не відповідають попередньо визначеному профілю клієнта, подібний варіант подій може бути неприйнятним ризиком. Для користувачів, які відповідають профілю клієнта, це може бути прийнятним ризиком відповідно до характеру даних, що зберігаються на жорсткому диску.

Використання DriveLock

Коли буде знайдено один або кілька жорстких дисків, що підтримують набір команд безпеки ATA, в меню “Безпека” утиліти Computer Setup з'явиться параметр DriveLock. Користувачеві надаються параметри налаштування пароля адміністратора або вмикання функції DriveLock. Щоб увімкнути DriveLock, необхідно надати пароль користувача. Оскільки початкове налаштування DriveLock зазвичай виконується системним адміністратором, спершу необхідно встановити пароль адміністратора. Компанія HP рекомендує системним адміністраторам встановити головний пароль незалежно від того, чи вони хочуть задіяти функцію DriveLock, чи вимкнути її. Це надасть адміністраторам можливість змінити параметри DriveLock, якщо диск буде заблоковано. Якщо пароль адміністратора призначено, системні адміністратори можуть увімкнути функцію DriveLock або не вмикати її.

Якщо у системі є заблокований жорсткий диск, під час самотестування при ввімкненні живлення потрібно буде ввести пароль для розблокування пристрою. Якщо встановлено пароль ввімкнення живлення, і він відповідає паролю користувача пристрою, то під час самотестування при ввімкненні живлення не потрібно буде вводити пароль повторно. В іншому випадку користувач повинен ввести пароль DriveLock. При “холодному старті” можна використовувати головний або користувацький пароль. При “теплому старті” слід вводити той самий пароль, що використовувався для розблокування жорсткого диска під час “холодного старту”, що передував розблокуванню. Для введення правильного пароля надається дві спроби. При “холодному старті” якщо жодна зі спроб не виявилася вдалою, процедура POST триватиме далі, але жорсткий диск залишатиметься недоступним. При “теплому старті” або перезапуску з Windows якщо жодна зі спроб не виявилася вдалою, процедура POST зупиниться, і користувачу буде запропоновано вимкнути комп'ютер і знову ввімкнути його.

Прикладні програми DriveLock

Найкращою областю практичного застосування функції DriveLock є корпоративне середовище. Системний адміністратор несе відповідальність за конфігурування жорсткого диску, що, окрім усього іншого, включає встановлення головного пароля DriveLock і тимчасового пароля користувача. Якщо користувач забуде свій пароль або обладнання буде передано іншому співробітникові, завжди можна скористатися паролем адміністратора для скидання пароля користувача і поновлення доступу до жорсткого диска.

Компанія HP рекомендує корпоративним системним адміністраторам, що обирають вмикання функції DriveLock, також встановлювати корпоративну політику налаштування і підтримки паролів адміністратора. Це необхідно для попередження ситуацій ненавмисного або навмисного призначення користувачем обох паролів DriveLock перед звільненням з компанії. У такому випадку жорсткий диск буде відображатися як непридатний до використання і потребуватиме заміни. Так само, не призначивши пароль адміністратора, системні адміністратори можуть виявити, що жорсткий диск блоковано і неможливо виконувати щоденні перевірки на наявність неавторизованого програмного забезпечення, інші функції контролю ресурсів, а також реалізувати підтримку діяльності системи.

Користувачам з менш суворими вимогами до безпеки компанія HP не рекомендує вмикати функцію DriveLock. До такої категорії входять персональні користувачі або користувачі, які не мають вразливих даних на своїх жорстких дисках. Для них потенційна втрата жорсткого диска,

спричинена втратою обох паролів, є набагато шкідливішою, ніж втрата тих даних, які мають бути захищені функцією DriveLock. Доступ до утиліт Computer Setup і DriveLock може бути обмежено паролем налаштування. Вказуючи пароль налаштування і не надаючи його кінцевим користувачам, системні адміністратори можуть запобігати вмиканню функції DriveLock користувачами.

Датчик переміщення кришки

Датчик переміщення кришки, встановлений в деяких моделях, є комбінацією апаратних і програмних засобів, що можуть сповіщати вас про зняття кришки або бічної панелі комп'ютера. Існує три рівні захисту, як показано у наведеній нижче таблиці.

Таблиця 11-2 Рівні захисту датчика переміщення кришки

Рівень	Значення параметра	Опис
Рівень 0	Disabled (Вимкнено)	Функцію Smart Cover Sensor вимкнено (за замовчуванням).
Рівень 1	Notify User (Повідомляти користувача)	При перезавантаженні комп'ютера на екрані з'являється повідомлення про те, що кришку корпусу або передню панель комп'ютера було знято.
Рівень 2	Setup Password (Пароль налаштування)	При перезавантаженні комп'ютера на екрані з'являється повідомлення про те, що кришку корпусу або передню панель комп'ютера було знято. Для продовження необхідно ввести пароль налаштування.

ПРИМІТКА. Ці параметри можна змінити за допомогою утиліти Computer Setup. Див. *Computer Setup (F10) Utility Guide (Посібник з використання утиліти Computer Setup (F10)* для отримання додаткової інформації про використання програми Computer Setup.

Налаштування рівня захисту функції Smart Cover Sensor

Щоб встановити рівень захисту датчика переміщення кришки, виконайте таку процедуру:

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Перезавантаження**.
2. Щойно комп'ютер увімкнеться, натисніть клавішу F10, поки комп'ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп'ютер і знову натиснути F10, поки комп'ютер не завантажив операційну систему.

3. Виберіть **Security** (Безпека) > **Smart Cover** (Кришка корпусу) > **Cover Removal Sensor** (Датчик переміщення кришки) і потрібний рівень захисту.
4. Перед тим як вийти, натисніть **File** (Файл) > **Save Changes and Exit** (Зберегти зміни і вийти).

Smart Cover Lock

Функція Smart Cover Lock, встановлена на деяких комп'ютерах, – це програмно керване блокування кришки корпусу. Це блокування запобігає несанкціонованому доступу до внутрішніх компонентів. Комп'ютер постачається з функцією SmartCover Lock, встановленою в режим "не заблоковано".

△ **ПОПЕРЕДЖЕННЯ.** Для максимальної безпеки блокування кришки корпусу важливо встановити пароль налаштування. Пароль налаштування дозволяє запобігти несанкціонованому доступу до утиліти Computer Setup.

ПРИМІТКА. Функція Smart Cover Lock постачається додатково із деякими системами.

Блокування у Smart Cover Lock

Щоб увімкнути й заблокувати замок Smart Cover Lock, виконайте таку процедуру:

1. Увімкніть або перезапустіть комп'ютер. Якщо Ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Перезавантаження**.
2. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп’ютер і знову натиснути F10, поки комп’ютер не завантажив операційну систему.

3. Виберіть **Security** (Безпека) > **Smart Cover** (Кришка корпусу) > **Cover Lock** (Замок кришки) > **Lock** (Блокувати).
4. Перед тим як вийти, натисніть **File** (Файл) > **Save Changes and Exit** (Зберегти зміни і вийти).

Розблокування у Smart Cover Lock

1. Увімкніть або перезапустіть комп'ютер. Якщо ви працюєте у Windows, виберіть **Пуск** > **Завершення роботи** > **Перезавантаження**.
2. Щойно комп’ютер увімкнеться, натисніть клавішу F10, поки комп’ютер не завантажив операційну систему, щоб увійти до утиліти Computer Setup. Натисніть клавішу Enter, щоб пропустити заставку, якщо це необхідно.

   ПРИМІТКА. Якщо ви не натиснете клавішу F10 вчасно, слід перезавантажити комп’ютер і знову натиснути F10, поки комп’ютер не завантажив операційну систему.

3. Виберіть **Security** (Безпека) > **Smart Cover** (Кришка корпусу) > **Cover Lock** (Замок кришки) > **Unlock** (Розблокувати).
4. Перед тим як вийти, натисніть **File** (Файл) > **Save Changes and Exit** (Зберегти зміни і вийти).

Використання Smart Cover FailSafe Key

Якщо ви увімкнули функцію Smart Cover Lock і не можете ввести пароль для розблокування, то для відкривання корпусу комп'ютера необхідно скористатися Smart Cover FailSafe Key. Цією функцією треба скористатися за таких обставин:

- Порушення живлення
- Неполадка запуску
- Збій компонента ПК (наприклад, процесора або блоку живлення)
- Забуто пароль

△ **ПОПЕРЕДЖЕННЯ.** Функція Smart Cover FailSafe Key – це спеціалізований інструмент, що постачається компанією HP. Підготуйтеся; замовте його до того, як він вам знадобиться, в авторизованого посередника чи постачальника послуг.

Щоб отримати FailSafe Key, зробіть наступне:

- Зверніться до авторизованого представника HP або постачальника Інтернет-послуг.
- Зателефонуйте за номером, зазначеним у гарантійному талоні.

Для отримання докладнішої інформації щодо використання Smart Cover FailSafe Key див. *Довідковий посібник з апаратного забезпечення*.

Cable Lock Provision

На задній панелі комп'ютера (для деяких моделей) розташований фіксатор кабелю, що дозволяє фізично закріпити комп'ютер в робочій області.

Інструкції з ілюстраціями див. у *Довідковому посібнику з апаратного забезпечення*.

Технологія ідентифікації за відбитками пальців

Щоб уникнути необхідності введення паролів, користувач може скористатися перевагами технології HP ідентифікації за відбитками пальців – зростання мережевої безпеки, спрощення процедури входу і зменшення витрат, пов'язаних з керуванням корпоративними мережами. Завдяки помірній ціні це рішення призначається не лише високотехнологічним організаціям з високим рівнем безпеки.

ПРИМІТКА. Підтримка технології ідентифікації за відбитками пальців залежить від моделі.

Повідомлення про неполадки і відновлення

Функції повідомлення про неполадки і відновлення складаються з сучасних апаратних і програмних засобів, що дозволяють запобігати втраті важливих даних і мінімізувати незапланований простій обладнання.

Якщо комп'ютер підключено до мережі, яка управляється диспетчером HP Client Manager, то комп'ютер надсилатиме повідомлення про неполадку програмі управління мережею. За допомогою програми HP Client Manager також можна дистанційно планувати діагностику для її автоматичного запуску на усіх керованих ПК і створювати звіти про непройдені тести.

Система захисту дисків

Програма самоперевірки системи Drive Protection System (DPS) – це інструмент діагностики, вбудований у жорсткі диски певних моделей комп'ютерів HP. Система DPS допомагає виявляти проблеми, які можуть призвести до пошкодження дисків, що не покриваються гарантією.

При виробництві комп'ютерів HP кожен жорсткий диск, що встановлюється в систему, перевіряється за допомогою DPS, та на нього записується вся важлива інформація. При кожному запуску DPS результати перевірки записуються на жорсткий диск. Постачальник послуг може скористатись цією інформацією, щоб встановити умови, за яких вам довелось запускати програму DPS. Див. *Інструкції з усунення несправностей*, щоб дізнатися про використання програми DPS.

Захищене від стрибків напруги джерело живлення

Вбудоване захищене від стрибків напруги джерело живлення підвищує надійність системи, коли вона вражається непередбаченим стрибком напруги. Цей блок живлення номінально здатен витримувати стрибки напруги до 2000 вольт без вимушеного простою системи або втрати даних.

Термодатчик

Термодатчик – це апаратна і програмна функція, що відстежує внутрішню температуру комп'ютера. Ця функція відображає попередження при перевищенні допустимого діапазону температур, що дозволяє завчасно вжити необхідних заходів ще до того, як буде вражено внутрішні компоненти або втрачено дані.

△ **ПОПЕРЕДЖЕННЯ.** Висока температура навколишнього середовища може призвести до пошкодження системи чи втрати даних.

Покажчик

Б

безпека
- DriveLock 32
- ProtectTools Security Manager 7
- Smart Cover Lock 35
- Датчик переміщення кришки 35
- параметри 25
- пароль 28
- технологія ідентифікації за відбитками пальців 37
- фіксатор кабелю 37
- функцій, таблиця 25

блокування Smart Cover Lock 36

В

введення
- пароль вмикання 30
- пароль налаштування 30

Веб-сайти
- Altiris Client Management Suite 10
- Служба підтримки HP 11
- HP Client Automation Agent 3
- HP Client Automation Center 8
- HP Client Catalog for SMS 10
- HP Client Management Interface 6
- HP Client Manager 3
- HP Client Manager from Symantec 9
- HPQFlash 14
- HP System Software Manager 7
- Proactive Change Notification 13
- Remote ROM Flash 14
- Subscriber's Choice 13
- Завантаження BIOS 14
- Завантаження System Software Manager 6
- Завантаження програмного забезпечення та драйверів 17
- підтримка програмного забезпечення 23
- технологія Intel vPro 11
- Фіксатори для бізнес-комп'ютерів HP 7
- Флеш-ПЗП 14

видалення пароля 31

відновлення, програми з 2

відстеження ресурсів 25

внутрішня температура комп'ютера 38

Г

галузеві стандарти 24

Д

Датчик переміщення кришки
- встановлення 35
- рівні захисту 35

джерело живлення, захищене від стрибків напруги 37

диск, захист 37

дистанційне встановлення 4

Дистанційне встановлення системи 4

діагностичний засіб для жорстких дисків 37

доступ до комп'ютера, контроль 25

Ж

жорсткі диски, діагностичний засіб для 37

З

завантажувальний пристрій
- носій даних USB-флеш 18
- створення 18

замовлення FailSafe Key 36

замок кришки 35

засоби розгортання, програмне забезпечення 2

захист жорсткого диску 37

зміна операційної системи, підтримка 23

зміна пароля 31

зміни, повідомлення про 13

І

Інтернет-адреси. *Див.* Веб-сайти

К

клавіатурні розкладки й розділові знаки 32

клонування, програми і засоби 2

кнопка живлення, налаштування 22

кнопка живлення з двома положеннями 22

контроль з доступом до комп'ютера 25

конфігурація налаштування, тиражування 16

Н

налаштування
- копіювання на кілька комп'ютерів 17
- копіювання на окремий комп'ютер 16

налаштування кнопки живлення 22

носій даних USB-флеш, завантажувальний 18, 19

О

образ з попередньо встановленим ПЗ 2
операційні системи, підтримка для зміни 23

П

пароль
  безпека 28
  видалення 31
  вмикання живлення 29, 30
  зміна 31
  налаштування 29, 30
  скидання 32
пароль вмикання
  введення 30
  видалення 31
  встановлення 29
  зміна 31
пароль налаштування
  введення 30
  видалення 31
  встановлення 29
  зміна 31
повідомлення про зміни 13
Повідомлення про неполадки і відновлення 37
початкова конфігурація 2
програмне забезпечення
  Altiris Client Management Suite 10
  HP Client Automation Starter Edition, Standard Edition та Enterprise Edition 8
  HP Client Catalog for Microsoft System Center & SMS Products 10
  HP Client Management Interface 5
  HP Client Manager from Symantec 9
  HP ProtectTools Security Manager 7
  HP System Software Manager 6
  Proactive Change Notification (PCN) 13
  Remote Management Technology (Технологія віддаленого керування) 10
  Verdiem Surveyor 13
  відновлення 2
  відстеження ресурсів 25
  Дистанційне встановлення системи 4
  засоби оновлення і керування 5
  інтеграція 2
  розгортання 2
  Система захисту дисків 37

Р

режим Boot Block Emergency Recovery 15
рішення, що тепер не надаються 13
розблокування Smart Cover Lock 36
розділові знаки, таблиця 32
розкладки й розділові знаки 32

С

скидання паролів 32
стрибки напруги, захист від 37

Т

температура комп'ютера, внутрішня 38
термодатчик 38
технологія ідентифікації за відбитками пальців 37

У

установка
  початкова 2

Ф

Флеш-ПЗП 14

A

Altiris
  Client Management Suite 10

B

BIOS
  HPQFlash 14
  Remote ROM Flash 14
  режим Boot Block Emergency Recovery 15
Boot Block Emergency Recovery, режим 15

C

cable lock provision 37
Client Automation Starter Edition, Standard Edition та Enterprise Edition 8
Client Management Interface 5
Client Manager from Symantec 9

D

DriveLock 32

E

Emergency Recovery, Boot Block 15

F

FailSafe Key, замовлення 36

H

HP
  Client Automation Starter Edition, Standard Edition та Enterprise Edition 8
  Client Catalog for Microsoft System Center & SMS Products 10
  Client Management Interface 5
  Client Manager from Symantec 9
  ProtectTools Security Manager 7
  System Software Manager 6
HP Client Manager 3
HPQFlash 14

P

Preboot Execution Environment (PXE) 4
Proactive Change Notification (PCN) 13
ProtectTools Security Manager 7
PXE (Preboot Execution Environment) 4

R
Remote Management Technology
(Технологія віддаленого
керування) 10
Remote ROM Flash 14

S
Smart Cover FailSafe Key,
замовлення 36
Smart Cover Lock
FailSafe Key 36
блокування 36
розблокування 36
Subscriber's Choice 13
System Software Manager 6

V
Verdiem Surveyor 13