Podręcznik zarządzania komputerami typu desktop

Komputery Business PC

Podręcznik zarządzania komputerami typu desktop

Komputery Business PC

Wydanie trzecie (lipiec 2008)

Numer katalogowy dokumentu: 451272-243

Informacje o podręczniku

Niniejszy przewodnik zawiera definicje i instrukcje dotyczące korzystania z funkcji zabezpieczeń i zarządzania preinstalowanych w niektórych modelach.

⚠ **OSTRZEŻENIE!** Tak oznaczane są zalecenia, których nieprzestrzeganie może doprowadzić do obrażeń ciała lub śmierci.

△ **OSTROŻNIE:** Tak oznaczane są zalecenia, których nieprzestrzeganie może doprowadzić do uszkodzenia sprzętu lub utraty danych.

UWAGA: Tak oznaczane są ważne informacje uzupełniające.

Spis treści

1 Przegląd zarządzania komputerami typu desktop

2 Konfiguracja wstępna i rozmieszczenie

HP Software Agent 3
Altiris Deployment Solution Agent 3

3 Zdalne instalowanie systemu

4 Aktualizowanie oprogramowania i zarządzanie nim

Interfejs HP Client Management Interface 5
HP SoftPaq Download Manager 6
Oprogramowanie HP System Software Manager 7
Oprogramowanie HP ProtectTools Security Manager 7
HP Client Automation Starter i Standard Edition 8
HP Client Automation Enterprise Edition 8
HP Client Manager from Symantec 10
Altiris Client Management Suite 11
HP Client Catalog for Microsoft System Center & SMS Products 11
Program HP Backup & Recovery Manager 12
Technika zarządzania 13
Verdiem Surveyor 15
HP Proactive Change Notification 15
Subscriber's Choice 15
Wycofane rozwiązania 15

5 Pamięć ROM typu flash

Zdalne programowanie pamięci ROM 16
HPQFlash 16

6 Tryb awaryjny odzyskiwania bloku rozruchowego

7 Powielanie konfiguracji

Kopiowanie na jeden komputer 18

Kopiowanie na wiele komputerów 19
Tworzenie urządzenia rozruchowego 20
Obsługiwane urządzenia USB typu flash 20
Nieobsługiwane urządzenia USB typu flash 22

8 Dwufunkcyjny przycisk zasilania

9 Witryna wsparcia firmy HP

10 Standardy przemysłowe

11 Śledzenie zasobów i funkcje zabezpieczeń
Zabezpieczanie hasłem 31
Ustawianie hasła konfiguracyjnego za pomocą programu Computer Setup 31
Ustawianie hasła uruchomieniowego za pomocą programu Computer Setup 31
Wprowadzanie hasła uruchomieniowego 32
Wprowadzanie hasła konfiguracyjnego 32
Zmiana hasła uruchomieniowego lub konfiguracyjnego 33
Usuwanie hasła uruchomieniowego lub konfiguracyjnego 34
Separatory dla różnych układów klawiatury 34
Czyszczenie haseł 35
Blokada DriveLock 35
Korzystanie z zabezpieczenia DriveLock 35
Zastosowania zabezpieczenia DriveLock 36
Czujnik Smart Cover Sensor 37
Ustawianie poziomów zabezpieczeń czujnika Smart Cover Sensor 37
Blokada Smart Cover Lock 37
Włączanie blokady Smart Cover Lock 38
Wyłączanie blokady Smart Cover Lock 38
Korzystanie z klucza Smart Cover FailSafe Key 38
Zabezpieczająca blokada kablowa 39
Identyfikacja na podstawie analizy linii papilarnych 39
Powiadamianie o usterkach i ich usuwanie 39
System ochrony dysków 39
Zasilacz z zabezpieczeniem antyprzepięciowym 40
Czujnik termiczny 40

Indeks 41

1 Przegląd zarządzania komputerami typu desktop

System HP Client Management Solutions zawiera oparte na standardach rozwiązania służące do sterowania i sprawowania nadzoru nad komputerami typu desktop, stacjami roboczymi i komputerami przenośnymi w środowisku sieciowym. W 1995 roku firma HP jako pierwsza w branży wprowadziła na rynek rodzinę komputerów osobistych typu desktop z zaimplementowaną funkcją zdalnego zarządzania. Firma HP jest posiadaczem patentu na technologię zarządzania. Od tego czasu prowadzone były na szeroką skalę prace mające na celu rozwój standardów i infrastruktury, pozwalające na efektywne rozmieszczanie i konfigurowanie komputerów stacjonarnych, przenośnych i stacji roboczych oraz zarządzanie nimi. Opracowywano własne oprogramowanie zarządzające oraz podjęto ścisłą współpracę z głównymi producentami oprogramowania tego typu, co umożliwiło zachowanie zgodności między dostarczanymi przez nich programami a systemem HP Client Management Solutions. System ten jest istotnym elementem prowadzonych działań, których celem jest opracowanie rozwiązań wspomagających obniżanie całkowitych kosztów posiadania i utrzymania komputerów PC podczas całego cyklu ich życia.

Najważniejsze funkcje i możliwości zarządzania komputerami typu desktop to:

- Początkowa konfiguracja i rozmieszczanie
- Zdalne instalowanie systemu
- Aktualizowanie programów i zarządzanie nimi
- Pamięć ROM typu flash
- Konfiguracja opcji sprzętu
- Śledzenie i funkcje zabezpieczeń zasobów
- Powiadamianie o usterkach i ich usuwanie

UWAGA: Obsługa poszczególnych funkcji opisanych w tym podręczniku może się różnić w zależności od modelu lub wersji oprogramowania.

2 Konfiguracja wstępna i rozmieszczenie

Komputer został dostarczony wraz z preinstalowanym obrazem oprogramowania systemowego. Dzięki temu po szybkim „rozpakowaniu” oprogramowania komputer jest gotowy do pracy.

Użytkownik może zastąpić preinstalowany obraz oprogramowania dowolnym systemem operacyjnym i aplikacjami dostosowanymi do własnych potrzeb. Istnieje kilka metod rozmieszczania takiego oprogramowania. Zostały one wymienione poniżej:

- Zainstalowanie dodatkowych aplikacji po rozpakowaniu preinstalowanego obrazu oprogramowania.
- Wykorzystanie narzędzi do rozmieszczania oprogramowania, takich jak programy: HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (z zastosowaniem technologii Radia) lub Altiris Deployment Solution, do zastąpienia preinstalowanego oprogramowania obrazem oprogramowania dostosowanym do potrzeb.
- Skopiowanie zawartości jednego dysku twardego na inny (w ramach procesu klonowania danych).

Najlepsza metoda rozmieszczania zależy od charakteru środowiska informatycznego oraz realizowanych w nim procesów.

System HP Backup and Recovery, program konfiguracyjny w pamięci ROM oraz sprzęt ACPI zapewnia wsparcie przy odzyskiwaniu oprogramowania systemowego, zarządzaniu konfiguracją i rozwiązywaniu związanych z tym problemów oraz zarządzaniu energią.

UWAGA: Informacje na temat tworzenia zestawu dysków do odzyskiwania można znaleźć w rozdziale Program HP Backup & Recovery Manager na stronie 12.

HP Software Agent

Agent zarządzania wykorzystywany w programach HP Client Automation Standard Edition i Enterprise Edition jest wstępnie załadowany do komputera. Po zainstalowaniu umożliwia komunikację z konsolą zarządzającą firmy HP.

Aby zainstalować program HP Software Agent:

1. Kliknij przycisk **Start**.
2. Kliknij polecenie **Wszystkie programy**.
3. Kliknij polecenie **HP Manageability**.
4. Kliknij polecenie **Radia Management Agent Readme**.
5. Aby zainstalować program HP Software Agent, należy zapoznać się z instrukcjami zawartymi w pliku Readme i wykonać je.

Program HP Software Agent jest podstawowym składnikiem infrastruktury służącym do włączenia wszystkich rozwiązań HP Client Automation. Informacje o innych elementach infrastruktury, niezbędnych do implementacji rozwiązań zarządzania konfiguracją firmy HP, można znaleźć w witrynie http://h20229.www2.hp.com/solutions/ascm/index.html.

Altiris Deployment Solution Agent

Ten program jest wstępnie załadowany na komputerze. Po zainstalowaniu umożliwia komunikację z konsolą Deployment Solution administratora.

Aby zainstalować program Altiris Deployment Solution Agent:

1. Kliknij przycisk **Start**.
2. Kliknij polecenie **Wszystkie programy**.
3. W systemie Windows Vista kliknij opcję **Install Altiris DAgent** (Zainstaluj program Altiris DAgent). W systemie Windows XP kliknij opcję **Install Altiris AClient** (Zainstaluj program Altiris AClient).
4. Wykonaj instrukcje wyświetlane na ekranie, aby zainstalować i skonfigurować klienta Altiris.

Ten agent jest kluczowym elementem infrastruktury umożliwiającym wykorzystanie oprogramowania Altiris Deployment Solution, będącego częścią pakietu Altiris Management Suite. Informacje o innych elementach infrastruktury, niezbędnych do implementacji oprogramowania Altiris Client Management Suite, można znaleźć w witrynie http://www.hp.com/go/easydeploy.

3 Zdalne instalowanie systemu

Zdalna instalacja systemu pozwala uruchomić i skonfigurować system, korzystając z oprogramowania i informacji o konfiguracji, znajdujących się na serwerze sieciowym, poprzez inicjację środowiska PXE (Preboot Execution Environment). Funkcja zdalnej instalacji systemu jest zazwyczaj stosowana jako narzędzie do instalacji i konfiguracji systemu i można ją wykorzystywać do następujących zadań:

- Formatowanie dysku twardego.
- Rozmieszczanie obrazu oprogramowania na jednym lub kilku nowych komputerach.
- Zdalne aktualizowanie systemu BIOS w pamięci ROM typu flash (Zdalne programowanie pamięci ROM na stronie 16).
- Konfigurowanie ustawień systemu BIOS.

Aby rozpocząć proces zdalnego instalowania systemu, należy nacisnąć klawisz F12, gdy komunikat **F12 = Network Service Boot** pojawi się w prawym dolnym narożniku ekranu powitalnego z logo firmy HP podczas uruchamiania komputera. Następnie należy postępować zgodnie z wyświetlanymi instrukcjami, kontynuując proces. Domyślna kolejność rozruchu jest ustawieniem konfiguracyjnym systemu BIOS, które można zmienić na opcję podejmowania każdorazowo próby uruchomienia środowiska PXE.

4 Aktualizowanie oprogramowania i zarządzanie nim

Firma HP oferuje kilka narzędzi służących do zarządzania oprogramowaniem zainstalowanym na komputerach typu desktop, stacjach roboczych i komputerach przenośnych oraz aktualizowania go:

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, Standard i Enterprise Edition
- HP Client Manager from Symantec
- Altiris Client Management Suite
- HP Client Catalog for Microsoft System Center & SMS Products
- HP Backup and Recovery Manager
- komputery PC typu Intel vPro z techniką Active Management Technology
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

Interfejs HP Client Management Interface

Bez względu na narzędzia do zarządzania systemem stosowane przez dział IT, zarządzanie zarówno zasobami sprzętowymi, jak i programowymi jest istotnym czynnikiem utrzymującym niskie koszty technologii informatycznych i podnoszącym sprawność przedsiębiorstwa. Administrator IT może uzyskać dostęp do interfejsu HP Client Management Interface, pisząc proste skrypty i dostosowując je do wybranych rozwiązań zarządzania.

Dzięki interfejsowi HP Client Management (HP CMI) nowe komputery HP Business można łatwo zintegrować z zarządzanym środowiskiem infrastruktury informatycznej. Interfejs HP CMI upraszcza integrację komputerów HP Business z wykorzystaniem popularnych narzędzi zarządzania systemami przemysłowymi (w tym oprogramowania Microsoft Systems Management Server, oprogramowania IBM Tivoli i HP Operations) oraz samodzielnie opracowanych aplikacji zarządzających. Korzystając z interfejsu HP CMI, narzędzia i aplikacje do zarządzania mogą przeprowadzać szczegółową

inwentaryzację komputera klienta, otrzymywać informacje o stanie sprawności i zarządzać ustawieniami systemu BIOS, komunikując się bezpośrednio z komputerem klienta, co redukuje potrzebę korzystania z oprogramowania agenta lub konektora w celu osiągnięcia integracji.

Interfejs HP Client Management Interface jest oparty na takich standardach przemysłowych jak: Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) i Advanced Configuration and Power Interface (ACPI). Interfejs HP CMI jest podstawową techniką stosowaną w rozwiązaniach HP Client Management Solutions. Interfejs HP CMI oferuje elastyczność wyboru metody zarządzania komputerami klienckimi firmy HP.

Interfejs HP Client Management Interface w połączeniu z oprogramowaniem do zarządzania systemem umożliwia:

- Wysyłanie żądań podania szczegółowej inwentaryzacji stacji klienta i pobieranie szczegółowych informacji o procesorach, dyskach twardych, pamięci, ustawieniach systemu BIOS, sterownikach, a także informacji z czujników (jak prędkość wentylatora, napięcie i temperatura).
- Odbiór informacji o kondycji sprzętu – szeroki zakres alarmów o stanie sprzętu (jak przegrzanie, awaria wentylatora czy zmiany konfiguracji) może być wysyłany do konsoli zarządzającej systemu, aplikacji lub do komputera lokalnego. Alerty są wysyłane w czasie rzeczywistym, po ich wywołaniu przez zdarzenia systemowe.
- Zarządzanie ustawieniami systemu BIOS – realizacja funkcji klawisza F10, łącznie ze zdalnym ustawianiem i zmianą haseł systemu BIOS oraz zmianą kolejności urządzeń startowych z konsoli zarządzającej systemu na dowolnym lub na wszystkich komputerach klienckich bez potrzeby bezpośredniego dostępu do każdej z maszyn.

Więcej informacji o interfejsie HP Client Management Interface można znaleźć na stronie http://www.hp.com/go/hpcmi/.

HP SoftPaq Download Manager

Program HP SoftPaq Download Manager to darmowy, łatwy w użyciu interfejs służący do wyszukiwania i pobierania aktualizacji oprogramowania do posiadanych modeli komputerów klienckich HP. Określając modele, system operacyjny i język, można szybko odnaleźć, uporządkować i wybrać potrzebne pakiety Softpaq. Aby pobrać program HP SoftPaq Download Manager, należy odwiedzić witrynę http://www.hp.com/go/sdm.

Oprogramowanie HP System Software Manager

Oprogramowanie HP System Software Manager (SSM) jest bezpłatnym programem narzędziowym do zdalnego rozmieszczania sterowników sprzętu i aktualizacji systemu BIOS na komputerach HP Business PC w sieci. Oprogramowanie SSM, działając dyskretnie (bez interakcji ze strony użytkownika), określa poziomy wersji sterowników i systemu BIOS zainstalowanych w każdym sieciowym systemie klienckim i porównuje te informacje z plikami SoftPaq oprogramowania systemowego, które zostały przetestowane i są przechowywane w centralnym magazynie plików. Następnie program ten aktualizuje wszelkie oprogramowanie systemowe o niższych wersjach na sieciowych komputerach PC do nowszych wersji dostępnych w magazynie plików. Ponieważ program SSM umożliwia dystrybucję aktualizacji SoftPaq tylko na właściwe modele systemów klienckich, administratorzy mogą za jego pomocą utrzymywać aktualność oprogramowania systemowego w sposób pewny i efektywny.

Oprogramowanie System Software Manager integruje się z narzędziami dystrybucji oprogramowania klasy korporacyjnej, takimi jak rozwiązania HP Client Automation, HP Client Manager from Symantec i Microsoft Systems Management Server (SMS). Za pomocą oprogramowania SSM można rozprowadzać aktualizacje tworzone przez klientów i aktualizacje innych firm, które zostały spakowane w formacie SSM.

Oprogramowanie SSM można pobrać bezpłatnie ze strony http://www.hp.com/go/ssm.

UWAGA: Obecnie oprogramowanie SSM nie obsługuje zdalnie pamięci ROM typu flash w systemach z włączonym programem Windows Vista BitLocker i korzystających ze środków TPM do ochrony kluczy BitLocker, ponieważ zapisanie systemu BIOS może unieważnić zaufany podpis utworzony przez program BitLocker dla danej platformy. Należy wyłączyć program BitLocker za pośrednictwem zasad grupy, aby zapisać system BIOS w pamięci typu flash.

Można włączyć obsługę programu BitLocker bez użycia środków TPM systemu BIOS, aby uniknąć unieważnienia kluczy BitLocker. Firma HP zaleca zachowanie bezpiecznej kopii zapasowej poświadczeń BitLocker umożliwiającej ich odzyskanie w przypadku awarii.

Oprogramowanie HP ProtectTools Security Manager

Oprogramowanie HP ProtectTools Security Manager zapewnia funkcje zabezpieczeń pomagające chronić komputer, sieci i najważniejsze dane przez nieautoryzowanym dostępem. Rozszerzone funkcje zabezpieczeń są dostępne w następujących modułach oprogramowania:

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Device Access Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Privacy Manager for HP ProtectTools

Moduły oprogramowania dostępne dla danego komputera mogą się różnić w zależności od modelu. Na przykład moduł Embedded Security for HP ProtectTools jest dostępny tylko w komputerach

z zainstalowanym wbudowanym układem elektronicznym zabezpieczeń TPM (Trusted Platform Module).

Moduły oprogramowania HP ProtectTools mogą być preinstalowane, wstępnie załadowane lub dostępne do pobrania w witrynie firmy HP w sieci Web. Dla wybranych komputerów biurkowych HP Compaq oprogramowanie HP ProtectTools jest dostępne jako opcja porynkowa. Więcej informacji można znaleźć na stronie http://www.hp.com/products/security.

HP Client Automation Starter i Standard Edition

Program HP Client Automation jest sprzętowym i programowym rozwiązaniem do zarządzania w systemach Windows Vista, Windows XP i środowiskach HP Thin Client, zapewniającym łatwe i szybkie wdrażanie oraz solidne podstawy dla przyszłych zastosowań. Jest oferowany w dwóch wersjach:

- Bezpłatna wersja Starter Edition służy do zarządzania komputerami biurkowymi, komputerami notebook i stacjami roboczymi HP, umożliwia inwentaryzację sprzętu i oprogramowania, zdalne sterowanie, monitorowanie za pomocą alertów HP, aktualizacje systemu BIOS i sterowników HP, integracje z oprogramowaniem HP Protect Tools i dodatkową obsługę technologii Intel AMT. Wersja Starter Edition wspiera także rozmieszczanie i zarządzanie środowiskiem HP Thin Client.
- Wersja Standard Edition (dostępna w sprzedaży) zawiera wszystkie funkcje wersji Starter Edition, a ponadto wdrażanie i migrację systemu Windows, możliwość zarządzania poprawkami oprogramowania, dystrybucję oprogramowania i pomiar korzystania z oprogramowania.

Programy HP Client Automation Starter i Standard Edition umożliwiają migrację do programu HP Client Automation Enterprise Edition (opartego na technologii Radia) służącego do automatycznego zarządzania dużymi, heterogenicznymi i nieustannie zmieniającymi się środowiskami informatycznymi.

Więcej informacji o rozwiązaniach HP Client Automation można znaleźć na stronie http://www.hp.com/go/client.

HP Client Automation Enterprise Edition

Oprogramowanie HP Client Automation Enterprise Edition jest rozwiązaniem opartym na zasadach, za pomocą którego administratorzy mogą inwentaryzować, wdrażać, instalować poprawki i zarządzać w sposób ciągły oprogramowaniem i zawartością na heterogenicznych platformach klienckich. Oprogramowanie HP Client Automation Enterprise Edition umożliwia informatykom wykonywanie następujących zadań:

- Automatyczna procedura zarządzania pełnym cyklem eksploatacji od eksploracji, wdrażania i bieżącego zarządzania do migracji i zakończenia użytkowania.
- Automatyczne wdrażanie i nieprzerwane zarządzanie całym pakietem oprogramowania (systemami operacyjnymi, aplikacjami, poprawkami, ustawieniami i zawartością) zapewniające pożądany stan.
- Zarządzanie oprogramowaniem na niemal dowolnym urządzeniu, w tym komputerach biurkowych, stacjach roboczych i komputerach przenośnych w heterogonicznej lub autonomicznej infrastrukturze.
- Zarządzanie oprogramowaniem w większości systemów operacyjnych.

Dzięki ciągłemu zarządzaniu konfiguracją klienci firmy HP obserwują znaczne oszczędności kosztów IT, przyspieszony czas wprowadzenia na rynek dla oprogramowania i zawartości.

Więcej informacji o rozwiązaniach HP Client Automation można znaleźć na stronie http://www.hp.com/go/client.

HP Client Manager from Symantec

Oprogramowanie HP Client Manager from Symantec, opracowane przy współpracy firmy Altiris, jest dostępne bezpłatnie dla wszystkich modeli komputerów biurkowych HP Business, komputerów notebook i stacji roboczych. Oprogramowanie SSM jest zintegrowane z programem HP Client Manager i umożliwia centralne śledzenie, monitorowanie i zarządzanie aspektami sprzętowymi systemów klienckich HP.

Oprogramowanie HP Client Manager from Symantec służy do realizacji następujących zadań:

- Uzyskiwanie cennych informacji dotyczących sprzętu, takiego jak procesor, pamięć, karta wideo, i ustawienia zabezpieczeń.
- Monitorowanie kondycji systemu w celu rozwiązywania problemów jeszcze przed ich wystąpieniem.
- Automatyczne pobieranie i instalowanie aktualizacji sterowników i systemu BIOS bez potrzeby fizycznego dostępu do każdego komputera.
- Zdalne konfigurowanie systemu BIOS i ustawień zabezpieczeń.
- Automatyzowanie procesów w celu szybkiego rozwiązywania problemów związanych ze sprzętem.

Ścisła integracja z narzędziami HP Instant Support skraca czas rozwiązywania problemów ze sprzętem.

- Diagnostyka – zdalne uruchamianie i przeglądanie na komputerze HP typu desktop, przenośnym lub na stacji roboczej.
- Sprawdzanie kondycji systemu – kontrola, czy na zainstalowanych systemach klienckich firmy HP nie występują typowe problemy ze sprzętem.
- Aktywna rozmowa – połączenie online z obsługą klienta firmy HP w celu rozwiązania problemów.
- Baza wiedzy firmy HP – łącze do informacji eksperckiej.
- Proces automatycznego kompletowania i dostarczenia pakietów SoftPaq, w celu szybkiego rozwiązania problemów ze sprzętem.
- Identyfikacja, inwentaryzacja i inicjacja systemów z wbudowanym mikroukładem zabezpieczeń HP ProtectTools Embedded Security.
- Opcja wyświetlania alarmów o kondycji sprzętu lokalnie na komputerze klienckim.
- Raportowanie podstawowych informacji inwentaryzacyjnych dla komputerów innych firm.
- Instalowanie i konfigurowanie mikroukładu zabezpieczeń TPM.
- Centralnie planowanie tworzenia kopii zapasowych i odzyskiwania.
- Dodatkowa obsługa zarządzania technologią Intel AMT.

Więcej informacji o oprogramowaniu HP Client Manager from Symantec można znaleźć na stronie http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Oprogramowanie Altiris Client Management Suite jest łatwym w użyciu rozwiązaniem zarządzania pełnym cyklem życia oprogramowania komputerów typu desktop, komputerów przenośnych i stacji roboczych. Oprogramowanie Client Management Suite Level 1 zawiera następujące produkty firmy Altiris:

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

Więcej informacji o oprogramowaniu Alitris Client Management Suite można znaleźć na stronie http://www.altiris.com/Products/ClientManagementSuite.aspx.

HP Client Catalog for Microsoft System Center & SMS Products

Oprogramowanie HP Client Catalog umożliwia zawodowym informatykom, wykorzystującym produkty firmy Microsoft, automatyzację rozmieszczania aktualizacji oprogramowania HP (Softpaq) na komputerach HP Business. Plik katalogu zawiera szczegółowe informacje o platformie sprzętowej, złożonych z komputerów biurkowych HP Business, komputerów notebook i stacji roboczych. Może być używany łącznie z niestandardową aplikacją inwentaryzacyjną oraz funkcjonalnością aktualizacji produktów firmy Microsoft do zapewnienia automatycznej aktualizacji sterowników i poprawek na zarządzanych komputerach klienckich HP.

Do produktów Microsoft obsługiwanych przez oprogramowanie HP Client Catalog należą:

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

Więcej informacji o oprogramowaniu HP Client Catalog for SMS można znaleźć na stronie http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

Program HP Backup & Recovery Manager

HP Backup and Recovery Manager to łatwa w użyciu, uniwersalna aplikacja, która umożliwia tworzenie kopii zapasowych podstawowego dysku twardego komputera i jego odzyskiwanie. Aplikacja działa w systemie Windows i służy do tworzenia kopii zapasowych systemu Windows, wszystkich aplikacji i wszystkich plików danych. Wykonywanie kopii zapasowych można zaplanować, aby były one tworzone automatycznie w określonych interwałach, lub można wykonywać je ręcznie. Ważne pliki można archiwizować osobno, oprócz zwykłych kopii zapasowych.

Program Backup and Recovery Manager jest preinstalowany na dysku C: i tworzy partycję przywracania.

Punkty przywracania i kopie zapasowe plików można kopiować na dyski CD lub DVD, a wszystkie kopie zapasowe można kopiować do sieci lub na pomocnicze dyski twarde.

Firma HP zdecydowanie zaleca utworzenie zestawu dysków do przywracania zaraz po rozpoczęciu korzystania z komputera oraz zaplanowanie regularnego tworzenia punktów przywracania.

Aby utworzyć zestaw dysków do przywracania:

1. Kliknij kolejno przycisk **Start** > polecenie **HP Backup and Recovery** > polecenie **HP Backup and Recovery Manager**, aby otworzyć kreatora Backup and Recovery Wizard, a następnie kliknij przycisk **Next** (Dalej).
2. Wybierz opcję **Tworzenie dysków do odzyskiwania (zalecane)** i kliknij przycisk **Next** (Dalej).
3. Postępuj zgodnie z instrukcjami kreatora.

Aby uzyskać więcej informacji na temat narzędzia HP Backup and Recovery Manager, należy zapoznać się z podręcznikiem *HP Backup and Recovery Manager User Guide* (Podręcznik użytkownika programu HP Backup and Recovery), wybierając kolejno **Start** > **HP Backup and Recovery** > **HP Backup and Recovery Manager Manual**.

UWAGA: Zestaw dysków do odzyskiwania można zamówić przez telefon w centrum pomocy technicznej firmy HP. Przejdź do następującej witryny sieci Web, wybierz kraj/region i kliknij łącze **Technical support after you buy** (Pomoc techniczna po zakupie) w obszarze **Call HP** (Skontaktuj się z firmą HP), aby uzyskać lokalny numer telefonu centrum pomocy technicznej.

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

Technika zarządzania

W modelach zastosowano technologię vPro lub technologię standardową. Obydwie umożliwiają rozpoznawanie, diagnozowanie i ochronę komputerowych zasobów sieciowych. Obydwie technologie umożliwiają zarządzanie komputerami PC niezależnie od tego, czy są one włączone, wyłączone lub ich system operacyjny jest zawieszony.

Funkcjonalność techniki zarządzania obejmuje:

- Informacja inwentaryzacyjna sprzętu
- Alarmowanie
- Zarządzanie energią – włączanie/wyłączanie zasilania, zasilanie cykliczne
- Zdalna diagnostyka i naprawa
    - Serial-over-LAN – umożliwia sterowanie zdalnym komputerem z konsoli w trakcie rozruchu
    - IDE-Redirect – umożliwia uruchamianie systemu ze zdalnego napędu startowego, dysku lub obrazu ISO
- Sprzętowa izolacja i odzyskiwanie – ograniczenie lub odcięcie dostępu komputera do sieci, jeśli wykryto podejrzaną aktywność, która może być spowodowana wirusem

UWAGA: Przegląd techniki Intel vPro można znaleźć w witrynie http://www.intel.com/vpro.

Informacje o technice Intel vPro specyficzne dla produktów firmy HP można znaleźć w dokumentacji zamieszczonej w witrynie http://www.hp.com/support. Wybierz swój kraj i język, kliknij link **Wsparcie i pomoc techniczna**, wprowadź numer modelu komputera i naciśnij klawisz Enter. Dalsze strony są zazwyczaj dostępne jedynie w języku angielskim. W kategorii **Resources** (Zasoby) kliknij pozycję **Manuals (guides, supplements, addendums, etc)** (Instrukcje, podręczniki itp.). W polu **Quick jump to manuals by category** (Szybki wybór podręcznika wg kategorii) kliknij pozycję **White papers** (Dokumentacja).

Do dostępnych technik zarządzania należą:

- AMT (obejmuje DASH 1.0)
- ASF

Techniki ASF i AMT nie mogą być skonfigurowane jednocześnie, lecz obie są obsługiwane.

Aby skonfigurować system Intel dla techniki AMT lub ASF:

1. Włącz lub uruchom ponownie komputer. W systemie Microsoft Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie**.
2. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij skrót klawiaturowy Ctrl+P.

UWAGA: Jeśli klawisze Ctrl+P nie zostaną naciśnięte w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawiszy Ctrl+P przed uruchomieniem systemu operacyjnego.

Ten skrót klawiaturowy uruchamia narzędzie konfiguracyjne Intel Management Engine BIOS Execution (MEBx). Narzędzie to umożliwia użytkownikowi konfigurowanie różnych aspektów techniki zarządzania. Niektóre z opcji konfiguracyjnych wymieniono poniżej:

- Main Menu (Menu główne)
  - Intel ® ME Configuration (Konfiguracja Intel ® ME)
  - Intel ® AMT Configuration (Konfiguracja Intel ® AMT)
  - Change Intel ® ME Password (Zmień hasło Intel ® ME)
  - Exit (Wyjście)
- Intel ® ME Platform Configuration (Konfiguracja platformy Intel ® ME)
  - Intel ® ME State Control (enable/disable) (Sterowanie stanem Intel ® ME [włącz/wyłącz])
  - Intel ® ME Firmware Local Update (enable/disable) (Lokalna aktualizacja oprogramowania układowego Intel ® ME [włącz/wyłącz])
  - Intel ® ME Features Control (Sterowanie funkcjami Intel ® ME)
  - Intel ® ME Power Control (Sterowanie zasilaniem Intel ® ME)
- Intel ® AMT Configuration (Konfiguracja Intel ® AMT)
  - Host Name (Nazwa hosta)
  - TCP/IP
  - Provision Model (Enterprise, SMB) (Model prowizjoningu)
  - Setup and Configuration (Instalacja i konfiguracja)
  - Un-Provision (Deprowizjoning)
  - SOL/IDE-R (enable/disable) (włącz/wyłącz)
  - Password Policy (Zasady haseł)
  - Secure Firmware Update (enable/disable) (Bezpieczna aktualizacja oprogramowania układowego [włącz/wyłącz])
  - Set PRTC (Ustaw PRTC)
  - Idle Timeout (Limit czasu bezczynności)
- Change Intel ® ME Password (Zmień hasło Intel ® ME) (Firma HP zdecydowanie zaleca zmianę tego hasła. Domyślne hasło to **admin**.)

Aby zarządzać zdalnie systemami AMT, administrator musi korzystać ze zdalnej konsoli obsługującej technikę AMT. Konsole do zarządzania przedsiębiorstwem są dostępne u takich dostawców jak: HP, Altiris i Microsoft SMS. W trybie SMB jako interfejs służy przeglądarka sieci Web na stacji klienta. Aby uzyskać dostęp do tej funkcji, należy uruchomić przeglądarkę na innym komputerze w sieci i wprowadzić adres `http://nazwa_hosta:16992`, gdzie `nazwa_hosta` oznacza nazwę przypisaną do danego komputera. Zamiast nazwy hosta można też podać adres IP.

Verdiem Surveyor

Oprogramowanie Verdiem Surveyor jest rozwiązaniem pomagającym w zarządzaniu kosztami zasilania komputera. Program Surveyor mierzy i raportuje wielkość zużycia energii dla każdego komputera. Ponadto zapewnia kontrolę nad ustawieniami zasilania komputerów, umożliwiając administratorom łatwe wdrażanie strategii oszczędzania energii we wszystkich zarządzanych przez nich sieciach. Oprogramowanie HP SoftPaq zawierające agenta Surveyor można pobrać z witryny pomocy technicznej firmy HP i zainstalować na obsługiwanych modelach komputerów biurkowych. Licencje oprogramowania Surveyor na zarządzanie komputerami można zakupić za pośrednictwem przedstawiciela firmy HP.

HP Proactive Change Notification

Program Proactive Change Notification używa witryny sieci Web Subscriber's Choice w celu proaktywnego i automatycznego wykonywania następujących zadań:

- Wysyłanie pocztą e-mail proaktywnych powiadomień o zmianach (Proactive Change Notification – PCN), które nawet z 60-dniowym wyprzedzeniem informują o zmianach w sprzęcie i oprogramowaniu dla większości komercyjnych komputerów i serwerów.
- Wysyłanie wiadomości e-mail zawierających biuletyny, porady dla klientów, ważne informacje, biuletyny dotyczące zabezpieczeń oraz alerty sterowników dla większości komercyjnych komputerów i serwerów.

Użytkownik tworzy własny profil w celu zapewnienia sobie otrzymywania tylko informacji związanych z określonym środowiskiem informatycznym. Aby uzyskać więcej informacji o programie Proactive Change Notification i utworzyć profil niestandardowy, należy odwiedzić stronę http://h30046.www3.hp.com/subhub.php.

Subscriber’s Choice

Subscriber’s Choice to usługa kliencka firmy HP.

W oparciu o profil użytkownika firma HP dostarcza mu spersonalizowane porady dotyczące produktów, polecane artykuły i/lub alerty/powiadomienia dotyczące sterowników i wsparcia technicznego.

Funkcja alertów/powiadomień dotyczących sterowników i wsparcia usługi Subscriber’s Choice dostarcza wiadomości e-mail z powiadomieniem, że informacje subskrybowane w profilu są dostępne do przejrzenia i pobrania. Aby uzyskać więcej informacji o rozwiązaniu Subscriber’s Choice i utworzyć profil niestandardowy, należy odwiedzić stronę http://h30046.www3.hp.com/subhub.php.

Wycofane rozwiązania

Dwa pakiety oprogramowania, Altiris Local Recovery i Dantz Retrospect, nie są już dostarczane z komputerami HP Business Desktop, komputerami przenośnymi ani ze stacjami roboczymi. Nowe komputery HP Business Desktop, komputery przenośnie i stacje robocze, począwszy od roku 2006, są dostarczane z programem HP Backup and Recovery Manager.

5 Pamięć ROM typu flash

System BIOS komputera jest przechowywany w programowalnej pamięci ROM (read only memory) typu flash. W celu zabezpieczenia jej przed nieumyślnym zaktualizowaniem lub zastąpieniem można ustawić hasło konfiguracyjne w programie Computer Setup (F10). Zapewni to operacyjną integralność komputera. Jeżeli zajdzie potrzeba uaktualnienia systemu BIOS, można pobrać najnowsze obrazy BIOS ze strony sterowników i wsparcia technicznego HP (http://www.hp.com/support/files).

△ **OSTROŻNIE:** Aby zapewnić maksymalną ochronę pamięci ROM, trzeba pamiętać o ustawieniu hasła konfiguracyjnego. Hasło konfiguracyjne zapobiega nieautoryzowanym uaktualnieniom pamięci ROM. Za pomocą programu System Software Manager administrator systemu może jednocześnie ustawić takie hasło na jednym lub kilku komputerach pracujących w sieci. Więcej informacji można znaleźć na stronie http://www.hp.com/go/ssm.

Zdalne programowanie pamięci ROM

Funkcja zdalnego zarządzania pamięcią ROM typu flash umożliwia administratorowi systemu zdalne uaktualnianie systemu BIOS komputerów HP pracujących w sieci z jednej centralnej konsoli administracyjnej. Dzięki niej wprowadzane zmiany są identyczne na wszystkich komputerach, a administrator ma większą kontrolę nad procesem uaktualniania obrazów BIOS na sieciowych komputerach firmy HP. W rezultacie poprawia się wydajność pracy oraz obniżają się ogólne koszty związane z eksploatacją sieci w przedsiębiorstwie.

UWAGA: Obecnie oprogramowanie SSM nie obsługuje zdalnie pamięci ROM typu flash w systemach z włączonym programem Windows Vista BitLocker i korzystających ze środków TPM do ochrony kluczy BitLocker, ponieważ zapisanie systemu BIOS może unieważnić zaufany podpis utworzony przez program BitLocker dla danej platformy. Należy wyłączyć program BitLocker za pośrednictwem zasad grupy, aby zapisać system BIOS w pamięci typu flash.

Aby możliwe było skorzystanie z funkcji zdalnego zarządzania pamięcią ROM typu flash, komputer musi zostać włączony ręcznie lub zdalnie za pomocą funkcji zdalnego przywracania ze stanu wstrzymania (Remote Wakeup).

Więcej informacji o zdalnym zarządzaniu pamięcią ROM typu flash można znaleźć w części poświęconej programowi HP Client Manager Software lub System Software Manager w witrynie http://www.hp.com/go/ssm/.

HPQFlash

Program narzędziowy HPQFlash służy do lokalnego aktualizowania lub przywracania systemu BIOS na pojedynczych komputerach z poziomu systemu operacyjnego Windows.

Aby uzyskać więcej informacji o narzędziu HPQFlash, należy odwiedzić stronę http://www.hp.com/support/files i po wyświetleniu monitu wprowadzić numer modelu komputera.

6 Tryb awaryjny odzyskiwania bloku rozruchowego

Tryb awaryjny odzyskiwania bloku rozruchowego umożliwia odzyskanie systemu w mało prawdopodobnym przypadku nieudanej aktualizacji pamięci ROM typu flash. Na przykład, jeśli podczas uaktualniania systemu BIOS wystąpi awaria zasilania, proces aktualizacji pamięci ROM może zostać niedokończony. W wyniku tego system BIOS może stać się bezużyteczny. Blok rozruchowy stanowi część pamięci ROM, jest jednak zabezpieczony przed aktualizacją. Zawiera on kod, który sprawdza poprawność obrazu systemu BIOS po włączeniu zasilania systemu.

- Jeżeli sprawdzenie poprawności przebiegnie pomyślnie, system zostanie uruchomiony w zwykły sposób.
- Jeśli system BIOS jest niepoprawny, system BIOS w bezpiecznym bloku rozruchowym umożliwi przeszukanie nośników wymiennych pod kątem plików obrazów systemu BIOS. Po odnalezieniu właściwego pliku obrazu systemu BIOS zostanie on automatycznie wczytany do pamięci ROM.

Po wykryciu nieprawidłowego obrazu systemu BIOS dioda zasilania zamiga na czerwono 8 razy w jednosekundowych odstępach. Jednocześnie głośnik wyemituje 8 sygnałów dźwiękowych. Jeśli część systemowej pamięci ROM zawierająca obraz opcjonalnej pamięci ROM wideo nie jest uszkodzona, na ekranie zostanie wyświetlony komunikat **Boot Block Emergency Recovery Mode**.

Aby odzyskać system po uruchomieniu go w trybie awaryjnego odzyskiwania bloku rozruchowego:

1. Wyłącz zasilanie.
2. Włóż dysk CD lub urządzenie USB typu flash zawierające żądany plik obrazu systemu BIOS w katalogu głównym.

   UWAGA: Nośnik musi być sformatowany przy użyciu systemu plików FAT12, FAT16 lub FAT32.

3. Włącz komputer.

   Jeśli nie zostanie odnaleziony obraz systemu BIOS, zostanie wyświetlony monit o włożenie nośnika zawierającego plik obrazu systemu BIOS.

   Jeśli system pomyślnie przeprogramuje pamięć ROM, nastąpi automatyczne wyłączenie zasilania systemu.

4. Wyjmij nośnik wymienny użyty do uaktualnienia systemu BIOS.
5. Włącz zasilanie, aby uruchomić ponownie komputer.

UWAGA: Program BitLocker zapobiega uruchomieniu systemu Windows Vista, jeśli dysk CD zawierający plik obrazu systemu BIOS znajduje się w napędzie optycznym. Jeśli program BitLocker jest włączony, przed próbą uruchomienia systemu Windows Vista należy usunąć dysk CD.

7 Powielanie konfiguracji

Używając poniższych procedur, administrator może w prosty sposób kopiować ustawienia konfiguracyjne z jednego komputera na inne (ten sam model). Umożliwia to zachowanie zgodności danych konfiguracyjnych na wielu komputerach.

UWAGA: Obydwie procedury wymagają napędu dyskietek lub napędu USB flash obsługiwanego typu.

Kopiowanie na jeden komputer

OSTROŻNIE: Ustawienia konfiguracyjne są specyficzne dla modelu komputera. Jeśli modele komputera źródłowego i docelowego są różne, może dojść do uszkodzenia systemu plików. Przykładowo: nie należy kopiować ustawień konfiguracyjnych z komputera dc7xxx na komputer dx7xxx.

1. Wybierz ustawienia konfiguracyjne do skopiowania. Wyłącz komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Zamknij system**.
2. Jeżeli używane jest urządzenie USB typu flash, podłącz je teraz.
3. Włącz komputer.
4. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

   UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.
5. Jeżeli używana jest dyskietka, włóż ją teraz.
6. Kliknij kolejno **File** (Plik) > **Replicated Setup** (Zreplikowane ustawienia) > **Save to Removable Media** (Zapisz na nośniku wymiennym). Postępuj zgodnie z instrukcjami pojawiającymi się na ekranie, aby zapisać ustawienia konfiguracyjne na dyskietce lub w urządzeniu USB typu flash.
7. Wyłącz komputer, który ma zostać skonfigurowany, a następnie włóż dyskietkę konfiguracyjną do napędu lub podłącz urządzenie USB typu flash.
8. Włącz komputer.
9. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

10. Kliknij kolejno **File** (Plik) > **Replicated Setup** (Zreplikowane ustawienia) > **Restore from Removable Media** (Przywróć z nośnika wymiennego), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

11. Po ukończeniu konfiguracji uruchom ponownie komputer.

Kopiowanie na wiele komputerów

△ **OSTROŻNIE:** Ustawienia konfiguracyjne są specyficzne dla modelu komputera. Jeśli modele komputera źródłowego i docelowego są różne, może dojść do uszkodzenia systemu plików. Przykładowo: nie należy kopiować ustawień konfiguracyjnych z komputera dc7xxx na komputer dx7xxx.

Wprawdzie przygotowanie dyskietki konfiguracyjnej lub urządzenia USB typu flash przy użyciu tej metody trwa nieznacznie dłużej, dane są kopiowane na komputery docelowe znacznie szybciej.

UWAGA: Do wykonania tej procedury lub utworzenia rozruchowego urządzenia USB typu flash wymagana jest dyskietka rozruchowa. Jeśli nie jest dostępny komputer z systemem umożliwiającym utworzenie dyskietki rozruchowej (Windows XP), należy skorzystać z metody kopiowania na jeden komputer (zobacz część Kopiowanie na jeden komputer na stronie 18).

1. Utwórz dyskietkę rozruchową lub rozruchowe urządzenie USB typu flash. Informacje można znaleźć w rozdziale Obsługiwane urządzenia USB typu flash na stronie 20 lub Nieobsługiwane urządzenia USB typu flash na stronie 22.

   △ **OSTROŻNIE:** Nie wszystkie komputery można uruchomić za pomocą urządzenia USB typu flash. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności rozruchu urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

2. Wybierz ustawienia konfiguracyjne do skopiowania. Wyłącz komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Zamknij system**.

3. Jeżeli używane jest urządzenie USB typu flash, podłącz je teraz.

4. Włącz komputer.

5. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

   UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.

6. Jeżeli używana jest dyskietka, włóż ją teraz.

7. Kliknij kolejno **File** (Plik) > **Replicated Setup** (Zreplikowane ustawienia) > **Save to Removable Media** (Zapisz na nośniku wymiennym). Postępuj zgodnie z instrukcjami pojawiającymi się na ekranie, aby zapisać ustawienia konfiguracyjne na dyskietce lub w urządzeniu USB typu flash.

8. Pobierz program narzędziowy BIOS służący do replikowania ustawień konfiguracyjnych (repset.exe) i skopiuj go na dyskietkę konfiguracyjną lub konfiguracyjne urządzenie USB typu flash. Aby pobrać ten program, wejdź na stronę http://welcome.hp.com/country/us/en/support.html i wprowadź numer modelu komputera.

9. Na dyskietce konfiguracyjnej lub w konfiguracyjnym urządzeniu USB typu flash utwórz plik autoexec.bat zawierający następujące polecenie:

repset.exe.

10. Wyłącz komputer, który ma zostać skonfigurowany. Włóż dyskietkę konfiguracyjną lub konfiguracyjne urządzenie USB typu flash, a następnie włącz komputer. Program konfiguracyjny zostanie uruchomiony automatycznie.

11. Po ukończeniu konfiguracji uruchom ponownie komputer.

Tworzenie urządzenia rozruchowego

Obsługiwane urządzenia USB typu flash

Obsługiwane urządzenia są wyposażone w preinstalowany obraz, co upraszcza proces przekształcania ich w urządzenia rozruchowe. W obraz taki są wyposażone wszystkie urządzenia USB typu flash firmy HP lub Compaq i większość urządzeń tego typu innych firm. Jeśli używane urządzenie USB typu flash nie jest wyposażone w taki obraz, należy użyć procedury opisanej dalej w tej części (zobacz Nieobsługiwane urządzenia USB typu flash na stronie 22).

Do utworzenia rozruchowego urządzenia USB typu flash wymagane są następujące elementy:

- Obsługiwane urządzenie USB typu flash.
- Rozruchowa dyskietka DOS zawierająca programy FDISK i SYS. (Jeśli program SYS jest niedostępny, można użyć programu FORMAT, lecz spowoduje to utratę wszystkich plików zapisanych już w urządzeniu USB typu flash).
- Komputer PC, którego rozruch można przeprowadzić z urządzenia USB typu flash.

△ **OSTROŻNIE:** W przypadku niektórych starszych komputerów PC rozruch z urządzenia USB typu flash może być niemożliwy. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności rozruchu urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

1. Wyłącz komputer.

2. Podłącz urządzenie USB typu flash do jednego z portów USB komputera i odłącz wszystkie inne urządzenia pamięci masowej USB (oprócz napędów dyskietek USB).

3. Włóż do napędu dyskietkę rozruchową DOS z programem FDISK.COM oraz programem SYS.COM lub FORMAT.COM. Następnie włącz komputer, aby uruchomić go z dyskietki DOS.

4. Uruchom program FDISK z wiersza poleceń **A:**, wpisując polecenie `FDISK` i naciskając klawisz Enter. Jeżeli pojawi się monit, wybierz **Tak** (**T**), aby włączyć obsługę dużych dysków.

5. Wprowadź numer [5], aby wyświetlić listę napędów w systemie. Urządzenie USB typu flash można zidentyfikować po rozmiarze dysku. Odpowiada mu napęd, którego rozmiar jest najbardziej zbliżony – zazwyczaj ostatni napęd z listy. Zanotuj literę napędu.

   Napęd urządzenia USB typu flash: _____

△ **OSTROŻNIE:** Jeśli ten napęd nie odpowiada urządzeniu USB typu flash, nie należy kontynuować procedury. Może to spowodować utratę danych. Należy sprawdzić wszystkie porty USB pod kątem innych urządzeń pamięci masowej. W przypadku ich znalezienia należy odłączyć te urządzenia, a następnie uruchomić ponownie komputer i kontynuować procedurę od punktu 4. Jeśli takie urządzenia nie zostaną znalezione, może to oznaczać, że system nie obsługuje urządzeń USB typu flash lub podłączone urządzenie USB typu flash jest uszkodzone. NIE należy kontynuować procedury przekształcania urządzenia USB typu flash w urządzenie rozruchowe.

6. Wyjdź z programu FDISK, naciskając klawisz Esc w celu powrotu do wiersza **A:**.
7. Jeśli dyskietka rozruchowa DOS zawiera program SYS.COM, przejdź do punktu 8. W przeciwnym razie przejdź do punktu 9.
8. W wierszu **A:** wprowadź polecenie `SYS x:` gdzie x oznacza zanotowaną wcześniej literę napędu.

△ **OSTROŻNIE:** Należy pamiętać o wprowadzeniu poprawnej litery napędu dla urządzenia USB typu flash.

Po przetransferowaniu plików systemowych program SYS powróci do wiersza **A:**. Przejdź do punktu 13.

9. Wybierz pliki, które chcesz zachować, i skopiuj je z urządzenia USB typu flash do katalogu tymczasowego na innym dysku (np. wewnętrznym dysku twardym systemu).
10. W wierszu **A:** wprowadź polecenie `FORMAT /S X:`, gdzie `X` oznacza zanotowaną wcześniej literę napędu.

△ **OSTROŻNIE:** Należy pamiętać o wprowadzeniu poprawnej litery napędu dla urządzenia USB typu flash.

Polecenie FORMAT powoduje wyświetlenie co najmniej jednego komunikatu, za każdym razem wyświetlając pytanie, czy chcesz kontynuować. Za każdym razem wprowadzaj `T`. Polecenie FORMAT wykona formatowanie urządzenia USB typu flash, doda pliki systemowe i wyświetli pytanie o nazwę woluminu.

11. Wprowadź etykietę (jeśli jest potrzebna) lub naciśnij klawisz Enter, aby ją pominąć.
12. Skopiuj wszystkie pliki zapisane w punkcie 9 na urządzenie USB typu flash.
13. Wyjmij dyskietkę i uruchom ponownie komputer. Komputer zostanie uruchomiony z urządzeniem USB typu flash jako dyskiem C.

UWAGA: Na każdym komputerze może być określona inna domyślna kolejność rozruchu urządzeń – do jej zmiany służy program narzędziowy Computer Setup (F10).

W wersji DOS dla środowiska Windows 9x może się chwilowo pojawić ekran z logo systemu Windows. Jeśli ten ekran nie ma być wyświetlany, w katalogu głównym urządzenia USB typu flash należy dodać plik o rozmiarze zerowym i nazwie LOGO.SYS.

Powrót do Kopiowanie na wiele komputerów na stronie 19.

Nieobsługiwane urządzenia USB typu flash

Do utworzenia rozruchowego urządzenia USB typu flash wymagane są następujące elementy:

- Urządzenie USB typu flash.
- Rozruchowa dyskietka DOS zawierająca programy FDISK i SYS. (Jeśli program SYS jest niedostępny, można użyć programu FORMAT, lecz spowoduje to utratę wszystkich plików zapisanych już w urządzeniu USB typu flash).
- Komputer PC, którego rozruch można przeprowadzić z urządzenia USB typu flash.

△ **OSTROŻNIE:** W przypadku niektórych starszych komputerów PC rozruch z urządzenia USB typu flash może być niemożliwy. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności rozruchu urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

1. Jeśli w systemie znajdują się karty PCI z dołączonymi napędami SCSI, ATA RAID lub SATA, wyłącz komputer i odłącz kabel zasilający.

   △ **OSTROŻNIE:** Kabel zasilający MUSI zostać odłączony.

2. Zdejmij obudowę komputera i wyjmij karty PCI.
3. Podłącz urządzenie USB typu flash do jednego z portów USB komputera i odłącz wszystkie inne urządzenia pamięci masowej USB (oprócz napędów dyskietek USB). Zamknij obudowę komputera.
4. Podłącz kabel zasilający i włącz komputer.
5. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

   UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.

6. Wybierz kolejno **Advanced** (Zaawansowane) > **PCI Devices** (Urządzenia PCI), aby wyłączyć kontrolery PATA i SATA. Wyłączając kontroler SATA, należy zanotować przerwanie IRQ, do którego jest on przypisany. Informacja ta będzie potrzebna do ponownego przypisania przerwania IRQ. Zamknij program konfiguracyjny i potwierdź zmiany.

   Przerwanie IRQ SATA: _____

7. Włóż do napędu dyskietkę rozruchową DOS z programem FDISK.COM oraz programem SYS.COM lub FORMAT.COM. Następnie włącz komputer, aby uruchomić go z dyskietki DOS.
8. Uruchom program FDISK i usuń wszystkie istniejące partycje urządzenia USB typu flash. Utwórz nową partycję i oznacz ją jako aktywną. Zamknij program FDISK, naciskając klawisz Esc.
9. Jeśli po zamknięciu programu FDISK system nie zostanie automatycznie ponownie uruchomiony, naciśnij kombinację klawiszy Ctrl+Alt+Del, aby ponownie uruchomić system z dyskietki DOS.
10. W wierszu **A:** wprowadź polecenie `FORMAT C: /S`, a następnie naciśnij klawisz Enter. Spowoduje to sformatowanie urządzenia USB typu flash i dodanie plików systemowych. Zostanie również wyświetlone zapytanie o etykietę woluminu.

11. Wprowadź etykietę (jeśli jest potrzebna) lub naciśnij klawisz Enter, aby ją pominąć.

12. Wyłącz komputer i odłącz kabel zasilający. Otwórz obudowę komputera i ponownie zainstaluj wszystkie wyjęte wcześniej karty PCI. Zamknij obudowę komputera.

13. Podłącz kabel zasilający, wyjmij z napędu dyskietkę, a następnie włącz komputer.

14. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

15. Wybierz kolejno **Advanced** (Zaawansowane) > **PCI devices** (Urządzenia PCI) i ponownie włącz kontrolery PATA i SATA, które zostały wyłączone w punkcie 6. Przypisz kontroler SATA do jego pierwotnego przerwania IRQ.

16. Zapisz zmiany i zakończ pracę programu. Komputer zostanie uruchomiony z urządzeniem USB typu flash jako dyskiem C.

UWAGA: Domyślna kolejność rozruchu jest różna w zależności od komputera; można ją zmienić w programie narzędziowym Computer Setup (F10). Aby uzyskać instrukcje, zapoznaj się z *Program Computer Setup (F10)*.

W wersji DOS dla środowiska Windows 9x może się chwilowo pojawić ekran z logo systemu Windows. Jeśli ten ekran nie ma być wyświetlany, w katalogu głównym urządzenia USB typu flash należy dodać plik o rozmiarze zerowym i nazwie LOGO.SYS.

Powrót do Kopiowanie na wiele komputerów na stronie 19.

8 Dwufunkcyjny przycisk zasilania

Jeżeli aktywny jest interfejs zaawansowanego zarządzania konfiguracją i zasilaniem (ACPI), przycisk zasilania komputera może działać jako włącznik/wyłącznik zasilania lub jako przycisk wstrzymania. Działanie funkcji wstrzymania polega na tym, że komputer nie jest zupełnie wyłączany, ale wprowadzany w stan niskiego poboru energii. Pozwala to na szybkie zmniejszenie zużycia energii (przejście do trybu oszczędzania energii) bez konieczności zamykania programów, a także szybki powrót do tego samego stanu bez ryzyka utraty danych.

Aby zmienić sposób działania przycisku zasilania, wykonaj następujące czynności:

1. Kliknij przycisk **Start**, a następnie wybierz kolejno **Panel sterowania** > **Opcje zasilania**.
2. W oknie **Właściwości: Opcje zasilania** wybierz kartę **Zaawansowane**.
3. W sekcji **Przycisk zasilania** wybierz opcję **Stan wstrzymania**.

Po skonfigurowaniu przycisku zasilania jako przycisku wstrzymania jego naciśnięcie spowoduje przejście systemu w stan niskiego poboru energii (stan wstrzymania). Ponowne jego naciśnięcie spowoduje szybkie uaktywnienie systemu i przejście komputera do trybu pełnego zasilania. Aby całkowicie wyłączyć komputer, należy nacisnąć przycisk zasilania i przytrzymać go w tej pozycji przez kilka sekund.

△ **OSTROŻNIE:** Przycisku zasilania należy używać do wyłączania komputera tylko w przypadku braku odpowiedzi systemu. Wyłączanie zasilania bez interakcji ze strony systemu operacyjnego może doprowadzić do uszkodzenia lub utraty danych zgromadzonych na dysku twardym.

9 Witryna wsparcia firmy HP

Personel techniczny firmy HP na bieżąco testuje i usuwa błędy w programach własnych oraz dostarczanych przez innych producentów, jak również prowadzi prace nad oprogramowaniem wspomagającym, przeznaczonym dla różnych systemów operacyjnych. Zapewnia to wydajność, zgodność i niezawodność komputerów firmy HP.

Wskazane jest, aby podczas zmiany lub uaktualniania systemów operacyjnych zaimplementować zaprojektowane dla nich oprogramowanie wspomagające. Jeśli planowane jest korzystanie z wersji systemu Microsoft Windows innej niż zainstalowana fabrycznie, należy zainstalować odpowiednie sterowniki urządzeń oraz programy narzędziowe (dzięki temu wszystkie dostępne funkcje będą realizowane poprawnie).

Dzięki staraniom firmy HP procesy odnajdywania, uzyskiwania dostępu, uaktualniania i instalowania najnowszego oprogramowania wspomagającego są bardzo proste. Programy można pobierać z witryny http://www.hp.com/support.

W witrynie tej dostępne są najnowsze wersje sterowników urządzeń, programy narzędziowe oraz możliwe do aktualizowania obrazy pamięci ROM, niezbędne do pracy najnowszej wersji systemu Windows na komputerach firmy HP.

10 Standardy przemysłowe

Opracowane przez firmę HP rozwiązania do zarządzania integrują się z innymi aplikacjami do zarządzania systemem i są oparte na standardach przemysłowych, takich jak:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Technologia Wake on LAN
- ACPI
- SMBIOS
- Środowisko Pre-boot Execution (PXE)

11 Śledzenie zasobów i funkcje zabezpieczeń

Komputery firmy HP są wyposażone w funkcje śledzenia zasobów. Zgromadzone dane dotyczące stanu kluczowych zasobów mogą być przetwarzane za pomocą oprogramowania HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager lub innych aplikacji do zarządzania systemem. Ze względu na całkowitą i automatyczną integrację funkcji śledzenia zasobów ze wspomnianymi programami użytkownik może wybrać narzędzie do zarządzania najlepiej odpowiadające jego środowisku pracy oraz podnoszące efektywność już używanego oprogramowania narzędziowego.

Firma HP oferuje również kilka rozwiązań służących do kontroli dostępu do cennych podzespołów i informacji. Oprogramowanie HP Embedded Security for ProtectTools (po zainstalowaniu) zapobiega nieautoryzowanemu dostępowi do danych, a także sprawdza integralność systemu i uwierzytelnia innych użytkowników próbujących uzyskać dostęp do systemu. (Więcej informacji można znaleźć w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie http://www.hp.com/products/security). Dostępne w niektórych modelach funkcje zabezpieczeń, takie jak HP Embedded Security for ProtectTools, blokada Smart Cover Lock i czujnik Smart Cover Sensor zapobiegają nieautoryzowanemu dostępowi do wewnętrznych podzespołów komputera. Z kolei wyłączając porty szeregowe, równoległe lub USB albo wyłączając możliwość rozruchu systemu z nośników wymiennych, można chronić cenne dane. Alerty dotyczące zmiany rozmiaru pamięci oraz otwarcia obudowy mogą być automatycznie przesyłane do aplikacji zarządzania systemem, przez co będą pełniły funkcję proaktywnego powiadamiania o ingerencji w wewnętrzne elementy komputera.

UWAGA: HP Embedded Security for ProtectTools, czujnik Smart Cover Sensor i blokada Smart Cover Lock są dostępne jako opcje w niektórych systemach.

Ustawienia zabezpieczeń komputerów firmy HP mogą być zarządzane na dwa sposoby:

- Lokalnie, za pomocą oprogramowania narzędziowego Computer Setup. Dodatkowe informacje i instrukcje dotyczące korzystania z narzędzi programu Computer Setup można znaleźć w *Podręczniku do programu Computer Setup (F10)* dołączonym do komputera. Niektóre komputery są wyposażone w program HP BIOS Configuration for ProtectTools, który jest aplikacją systemu Windows – składnikiem narzędzi ProtectTools umożliwiającym administratorowi konfigurowanie ustawień zabezpieczeń systemu BIOS przy uruchomionym systemie operacyjnym.
- Zdalnie, za pomocą programów HP Client Manager from Symantec, HP Client Automation lub System Software Manager umożliwiających bezpieczne rozmieszczanie i kontrolowanie jednolitych ustawień zabezpieczeń.

Poniższa tabela oraz dalsze części dotyczą lokalnego zarządzania funkcjami zabezpieczeń komputera za pomocą oprogramowania narzędziowego Computer Setup (F10).

Tabela 11-1 Przegląd funkcji zabezpieczeń

Opcja	Opis
Setup Password (Hasło konfiguracyjne)	Umożliwia ustawianie i włączanie hasła konfiguracyjnego (administratora). **UWAGA:** Jeżeli ustawione zostanie hasło konfiguracyjne, wymagane jest jego wprowadzanie przy próbie: zmiany opcji programu Computer Setup, programowania pamięci ROM i zmiany niektórych ustawień plug and play w systemie Windows.
Power-On Password (Hasło uruchomieniowe)	Umożliwia ustawianie i włączanie hasła uruchomieniowego. Monit o podanie hasła uruchomieniowego pojawia się po wyłączeniu i włączeniu zasilania. Jeśli użytkownik nie wprowadzi poprawnego hasła uruchomieniowego, to maszyna nie zostanie uruchomiona. **UWAGA:** Hasło nie jest wyświetlane w przypadku miękkiego restartu, na przykład po naciśnięciu klawiszy Ctrl + Alt + Delete lub wybraniu opcji **Uruchom ponownie** w systemie Windows, chyba że takie zachowanie zostanie włączone w sekcji **Password Options** (Opcje haseł) (patrz poniżej).
Password Options (Opcje haseł) (To ustawienie jest wyświetlane tylko w przypadku, gdy ustawione jest hasło uruchomieniowe lub hasło konfiguracyjne).	Umożliwia: • Blokowanie starszych zasobów (ustawienie dostępne po ustawieniu hasła konfiguracyjnego). • Włączanie/wyłączanie trybu serwera sieciowego (ustawienie dostępne po ustawieniu hasła uruchomieniowego). • Określanie, czy hasło jest wymagane w przypadku ponownego uruchamiania bez wyłączania zasilania (Ctrl+Alt+Delete) (ustawienie dostępne po ustawieniu hasła uruchomieniowego). • Włącza/wyłącza tryb przeglądania konfiguracji (ustawienie dostępne po ustawieniu hasła uruchomieniowego) (umożliwia przeglądanie ustawień opcji programu F10 Setup bez podawania hasła uruchomieniowego, bez możliwości wprowadzania zmian). • Enable/disable Stringent Password (Włącz/wyłącz konieczność hasła) (pojawia się, gdy jest ustawione hasło przy uruchamianiu); włączenie tej opcji powoduje obejście zworki hasła na płycie głównej, co uniemożliwia wyłączenie za jej pomocą hasła przy uruchamianiu. Aby uzyskać więcej informacji, zapoznaj się z *Podręcznikiem zarządzania komputerami typu desktop*.
Smart Cover (niektóre modele)	Umożliwia: • Włączanie/wyłączanie blokady Cover Lock. • Ustawianie czujnika zdjęcia obudowy na Disable (Wyłączony), Notify User (Powiadamianie użytkownika) lub Setup Password (Hasło konfiguracyjne). **UWAGA:** Funkcja **Notify User** służy do powiadamiania użytkownika o tym, że obudowa została zdjęta. Jeśli zostanie wybrana funkcja **Setup Password**, to aby można było uruchomić komputer ze zdjętą obudową, wymagane jest wprowadzenie hasła konfiguracyjnego. Funkcja ta jest obsługiwana jedynie w niektórych modelach.
Device Security (Ochrona urządzeń)	Umożliwia włączanie/wyłączanie ukrywania wybranych urządzeń: • Porty szeregowe • Port równoległy • Tylne porty USB • Przednie porty USB • Wewnętrzne porty USB • System audio • Kontrolery sieciowe (niektóre modele)

Tabela 11-1 Przegląd funkcji zabezpieczeń (ciąg dalszy)

	• Legacy diskette (Zwykła dyskietka) • Wbudowane urządzenie zabezpieczające (niektóre modele) • SATA0 • SATA1 (niektóre modele) • SATA2 (niektóre modele) • SATA3 (niektóre modele) • eSATA (niektóre modele)
Network Service Boot (Uruchamianie z sieci)	Włącza/wyłącza możliwość uruchomiania komputera z systemu operacyjnego zainstalowanego na serwerze sieciowym. (Funkcja ta jest dostępna tylko w modelach wyposażonych w kartę interfejsu sieciowego (NIC). Kontroler sieciowy musi być kartą rozszerzenia PCI lub zintegrowany z płytą główną.)
System IDs (Identyfikatory systemowe)	Umożliwia ustawianie następujących opcji: • Etykieta zasobu (18-bajtowy identyfikator), numer identyfikacyjny środka trwałego przydzielony komputerowi przez firmę. • Etykieta właściciela (80-bajtowy identyfikator) wyświetlana podczas autotestu POST. • Numeru seryjnego podstawy montażowej lub uniwersalnego unikatowego identyfikatora (UUID). Identyfikator UUID można aktualizować tylko, jeśli bieżący numer seryjny podstawy montażowej jest błędny. (Zazwyczaj numery te są ustawiane fabrycznie i służą za unikatowe identyfikatory systemu). • Układu klawiatury (np. angielska lub niemiecka) do wprowadzania systemowych danych identyfikacyjnych.
DriveLock Security (Blokada DriveLock)	Umożliwia przydzielanie i modyfikowanie hasła głównego lub hasła użytkownika dla dysków twardych. Włączenie tej funkcji spowoduje, że podczas autotestu POST użytkownik będzie proszony o podanie jednego z haseł DriveLock. Jeśli żadne z nich nie zostanie pomyślnie wprowadzone, dysk twardy chroniony hasłem będzie niedostępny do momentu wprowadzenia poprawnego hasła podczas kolejnego uruchomienia komputera. **UWAGA:** Opcja ta jest wyświetlana tylko w przypadku, gdy w systemie został zainstalowany co najmniej jeden napęd obsługujący blokadę DriveLock.
System Security (Zabezpieczenie systemu) — niektóre modele: te opcje są niezależne od sprzętu	Data Execution Prevention (some models) (enable/disable) (Tryb Data Execution Prevention, niektóre modele, włączenie/wyłączenie) – pomaga w zapobieganiu naruszaniu zabezpieczeń systemu operacyjnego. Virtualization Technology (some models) (enable/disable) (Technika wirtualizacji, niektóre modele, włączenie/wyłączenie) – steruje funkcjami wirtualizacji procesora. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. Virtualization Technology Directed I/O (some models) (enable/disable) (Kierowane urządzenia we/wy techniki wirtualizacji, niektóre modele, włączenie/wyłączenie) – steruje funkcjami ponownego mapowania DMA wirtualizacji w układzie chipset. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. Trusted Execution Technology (some models) (enable/disable) (Technika zaufanego wykonywania, tylko niektóre modele, włączanie/wyłączanie) – steruje podległymi funkcjami procesora i układu chipset, wymaganymi do obsługi urządzenia wirtualnego. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. Aby włączyć tę funkcję, należy włączyć następujące funkcje: • obsługa wbudowanego urządzenia zabezpieczającego, • technika wirtualizacji, • kierowane urządzenia we/wy techniki wirtualizacji.

Tabela 11-1 Przegląd funkcji zabezpieczeń (ciąg dalszy)

	Embedded Security Device Support (some models) (enable/disable) (Obsługa wbudowanego urządzenia zabezpieczającego, niektóre modele, włączanie/wyłączanie) – umożliwia uaktywnienie lub dezaktywację wbudowanego urządzenia zabezpieczającego. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. **UWAGA:** Aby skonfigurować wbudowane urządzenie zabezpieczające, należy ustawić hasło konfiguracyjne. • Reset to Factory Settings (some models) (Do not reset/Reset) (Resetowanie do ustawień fabrycznych, niektóre modele, nie resetuj/resetuj) – przywrócenie domyślnych ustawień fabrycznych spowoduje usunięcie wszystkich kluczy bezpieczeństwa. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. **OSTROŻNIE:** Wbudowane urządzenie zabezpieczające jest krytycznym składnikiem wielu schematów zabezpieczeń. Usunięcie kluczy bezpieczeństwa uniemożliwi dostęp do danych chronionych za pomocą wbudowanego urządzenia zabezpieczającego. Wybranie opcji resetowania do ustawień fabrycznych może spowodować utratę wielu danych. • Power-on authentication support (some models) (enable/disable) (Obsługa uwierzytelniania przy uruchamianiu, niektóre modele, włączenie/wyłączenie) – steruje schematem uwierzytelniania za pomocą hasła podczas uruchamiania, wykorzystującym wbudowane urządzenie zabezpieczające. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. • Reset authentication credentials (some models) (Do not reset/Reset) (Resetowanie poświadczeń uwierzytelniania, niektóre modele, brak resetowania/resetowanie) – wybranie opcji resetowania wyłącza obsługę uwierzytelniania przy uruchamianiu i usuwa informacje dotyczące uwierzytelniania z wbudowanego urządzenia zabezpieczającego. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. OS management of Embedded Security Device (some models) (enable/disable) (Zarządzanie wbudowanym urządzeniem zabezpieczającym w systemie operacyjnym, niektóre modele, włączenie/wyłączenie) – ta opcja umożliwia użytkownikowi ograniczenie sterowania wbudowanym urządzeniem zabezpieczającym w systemie operacyjnym. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. Opcja umożliwia ograniczenie możliwości sterowania tym urządzeniem za pomocą systemu operacyjnego. • Reset of Embedded Security Device through OS (some models) (enable/disable) (Resetowanie wbudowanego urządzenia zabezpieczającego w systemie operacyjnym, niektóre modele, włączenie/wyłączenie) – opcja umożliwia użytkownikowi ograniczenie możliwości żądania w systemie operacyjnym przywrócenia ustawień fabrycznych wbudowanego urządzenia zabezpieczającego. Zmiana tego ustawienia wymaga wyłączenia komputera, a następnie włączenia go ponownie. **UWAGA:** Włączenie tej opcji wymaga ustawionego hasła konfiguracyjnego. Smart Card BIOS Password Support (some models) (enable/disable) (Obsługa hasła systemu BIOS karty inteligentnej, niektóre modele, włączenie/wyłączenie) – umożliwia użytkownikowi włączanie/wyłączanie używania karty inteligentnej zamiast hasła uruchomieniowego i konfiguracyjnego. Ustawienie to wymaga dodatkowej inicjalizacji w programie ProtectTools, aby opcja została wprowadzona. PAVP (Some models) (disabled/min/max)(niektóre modele) (wyłączenie/min/maks) – opcja PAVP umożliwia włączenie zabezpieczonej ścieżki audio-wideo (Protected Audio Video Path) w układzie chipset. Może to umożliwić oglądanie niektórych zabezpieczonych zawartości o wysokiej rozdzielczości, której odtwarzanie byłoby w przeciwnym przypadku zabronione. Wybranie ustawienia Max powoduje przypisanie 96 MB pamięci systemowej do wyłącznej dyspozycji opcji PAVP.
Setup Security Level (Poziom zabezpieczeń programu Setup)	Daje możliwość zezwalania użytkownikom końcowym na ograniczony dostęp do określonych opcji programu konfiguracyjnego i możliwość ich zmiany bez znajomości hasła konfiguracyjnego. Ta funkcja umożliwia administratorowi elastyczność przy ochronie istotnych opcji konfiguracyjnych przed zmianami, jednocześnie umożliwiając użytkownikowi przeglądanie ustawień systemu i konfigurowanie mniej ważnych opcji. Administrator określa prawa dostępu do poszczególnych opcji konfiguracyjnych kolejno, korzystając z menu opcji Setup Security Level. Do wszystkich opcji

Tabela 11-1 Przegląd funkcji zabezpieczeń (ciąg dalszy)

	konfiguracyjnych jest domyślnie przypisane hasło konfiguracyjne, co oznacza, że użytkownik musi podać poprawne hasło konfiguracyjne podczas testu POST, aby móc zmienić dowolną z opcji. Administrator może zmienić ustawienia poszczególnych elementów na None (brak), co oznacza, że użytkownik może zmienić tę opcję, podając niewłaściwe hasło. Ustawienie None (brak) jest zamieniane na ustawienie Power-On Password, jeśli hasło uruchomieniowe jest włączone. **UWAGA:** Aby użytkownik miał dostęp do programu konfiguracyjnego bez znajomości hasła konfiguracyjnego, opcja Setup Browse Mode (Tryb przeglądania konfiguracji) musi być włączona.

Zabezpieczanie hasłem

Hasło uruchomieniowe zapobiega nieautoryzowanemu dostępowi do komputera. Jego podanie jest wymagane przy każdorazowym włączaniu lub ponownym uruchamianiu komputera. Hasło konfiguracyjne zapobiega nieautoryzowanemu dostępowi do programu Computer Setup. Można go również używać jako hasła uruchomieniowego. Oznacza to, że podanie hasła konfiguracyjnego zamiast uruchomieniowego umożliwi uzyskanie dostępu do zasobów komputera.

Administrator systemu może dysponować własnym, sieciowym hasłem konfiguracyjnym. Dzięki niemu ma on dostęp do wszystkich komputerów oraz możliwość sprawowania kontroli nad działaniem całego systemu, nawet jeżeli stanowiska są chronione za pomocą haseł uruchomieniowych.

Ustawianie hasła konfiguracyjnego za pomocą programu Computer Setup

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie http://www.hp.com. Ustawienie hasła konfiguracyjnego za pomocą programu Computer Setup zapobiega przypadkowym i nieautoryzowanym zmianom konfiguracji komputera, gdyż dostęp do programu Computer Setup (F10) będzie możliwy wyłącznie po podaniu tego hasła.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie**.
2. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

   UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.
3. Wybierz menu **Security** (Zabezpieczenia), wybierz opcję **Setup Password** (Hasło konfiguracyjne), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjęciem z programu kliknij kolejno **File** (Plik) > **Save Changes and Exit** (Zapisz zmiany i zakończ).

Ustawianie hasła uruchomieniowego za pomocą programu Computer Setup

Po ustawieniu hasła uruchomieniowego za pomocą programu Computer Setup dostęp do danych komputera jest możliwy dopiero po podaniu poprawnego hasła. Ustawienie tego hasła spowoduje również wyświetlenie w menu **Security** (Zabezpieczenia) programu Computer Setup pozycji **Password Options** (Opcje hasła). Do opcji hasła należy **Password Prompt on Warm Boot** (Wymaganie hasła przy ponownym uruchamianiu). Jeżeli włączona zostanie opcja wymagania hasła przy ponownym

uruchamianiu **Password Prompt on Warm Boot**, wprowadzanie hasła będzie konieczne również przy każdym ponownym uruchomieniu komputera.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie**.
2. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.

3. Wybierz menu **Security** (Zabezpieczenia), wybierz opcję **Power On Password** (Hasło uruchomieniowe), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjęciem z programu kliknij kolejno **File** (Plik) > **Save Changes and Exit** (Zapisz zmiany i zakończ).

Wprowadzanie hasła uruchomieniowego

Aby wprowadzić hasło uruchomieniowe, wykonaj następujące czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie komputer**.
2. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie naciśnij klawisz Enter.

UWAGA: Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

Jeżeli zostanie podane nieprawidłowe hasło, na ekranie pojawi się ikona przedstawiająca przełamany klucz. Należy spróbować ponownie wpisać poprawne hasło. Po trzech nieudanych próbach wprowadzenia hasła komputer należy wyłączyć, a następnie włączyć i ponownie wprowadzić hasło.

Wprowadzanie hasła konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie http://www.hp.com.

Jeżeli ustawiono hasło konfiguracyjne komputera, jego podanie będzie wymagane przy każdej próbie uruchomienia programu Computer Setup.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie**.
2. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.

3. Po pojawieniu się ikony klucza wpisz hasło konfiguracyjne, a następnie naciśnij klawisz Enter.

UWAGA: Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

Jeżeli zostanie podane nieprawidłowe hasło, na ekranie pojawi się ikona przedstawiająca przełamany klucz. Należy spróbować ponownie wpisać poprawne hasło. Po trzech nieudanych próbach wprowadzenia hasła komputer należy wyłączyć, a następnie włączyć i ponownie wprowadzić hasło.

Zmiana hasła uruchomieniowego lub konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie http://www.hp.com.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie komputer**.
2. Aby zmienić hasło uruchomieniowe, przejdź do punktu 3.

   Aby zmienić hasło programu Setup, zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

   UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.
3. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie dwa razy nowe hasło, rozdzielając je znakiem ukośnika (/) lub innym separatorem, zgodnie ze wzorem: `bieżące hasło/nowe hasło/nowe hasło`

   UWAGA: Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.
4. Naciśnij klawisz Enter.

Nowe hasło zacznie obowiązywać po następnym włączeniu komputera.

UWAGA: Informacje na temat innych separatorów można znaleźć w części Separatory dla różnych układów klawiatury na stronie 34. Hasła uruchomieniowe i konfiguracyjne można również zmieniać przy użyciu opcji menu Security (Zabezpieczenia) w programie Computer Setup.

Usuwanie hasła uruchomieniowego lub konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie http://www.hp.com.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie komputer**.
2. Aby usunąć hasło uruchomieniowe, przejdź do punktu 3.

   Aby usunąć hasło programu Setup, zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.

3. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie znak ukośnika (/) lub inny separator, zgodnie ze wzorem: `bieżące hasło/`
4. Naciśnij klawisz Enter.

UWAGA: Informacje na temat innych separatorów można znaleźć w części Separatory dla różnych układów klawiatury na stronie 34. Hasła uruchomieniowe i konfiguracyjne można również zmieniać przy użyciu opcji menu Security (Zabezpieczenia) w programie Computer Setup.

Separatory dla różnych układów klawiatury

Konstrukcja każdej klawiatury uwzględnia wymagania specyficzne dla danego języka. z tego względu separatory oraz klawisze używane podczas zmiany lub usuwania hasła zależą od typu klawiatury dołączonej do komputera.

Separatory dla różnych układów klawiatury

/	arabska	-	grecka	/	rosyjska
=	belgijska	.	hebrajska	-	słowacka
-	BHCCSS*	-	węgierska	-	hiszpańska
/	brazylijska	-	włoska	/	szwedzka/fińska
/	chińska	/	japońska	-	szwajcarska
-	czeska	/	koreańska	/	tajwańska
-	duńska	-	południowoamery-kańska	/	tajska
!	francuska	-	norweska	.	turecka
é	francuska (Kanada)	-	polska	/	angielska (USA)
-	niemiecka	-	portugalska		

* dla Bośni i Hercegowiny, Chorwacji, Czarnogóry, Serbii i Słowenii

Czyszczenie haseł

Utrata hasła uniemożliwia dostęp do komputera. W *Podręczniku rozwiązywania problemów* można znaleźć instrukcje dotyczące czyszczenia haseł.

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie http://www.hp.com.

Blokada DriveLock

DriveLock to będąca standardem przemysłowym funkcja zabezpieczeń, która zapobiega nieautoryzowanemu dostępowi do danych przechowywanych na dyskach twardych ATA. Funkcja ta jest zaimplementowana jako rozszerzenie programu Computer Setup. Jest ona dostępna tylko po wykryciu w systemie dysków twardych obsługujących zestaw poleceń ATA Security. Funkcja DriveLock została opracowana z myślą o klientach firmy HP, dla których bezpieczeństwo danych jest sprawą priorytetową. Chodzi o klientów, dla których całkowity koszt dysku twardego i danych na nim przechowywanych (w przypadku ich utraty) jest nieporównywalnie mniejszy od strat, jakie może spowodować dostęp do tych danych przez osoby niepowołane. W celu uzyskania kompromisu między wymaganym poziomem zabezpieczeń i koniecznością dostępu do danych w przypadku utraty hasła implementacja funkcji DriveLock wykorzystuje schemat zabezpieczeń oparty na dwóch hasłach. Pierwsze z nich jest ustawiane i stosowane przez administratora systemu, drugie natomiast – przez użytkownika końcowego. Jeżeli oba hasła zostaną utracone, dostęp do dysku zostanie całkowicie zablokowany. Dlatego też w celu zwiększenia bezpieczeństwa związanego ze stosowaniem funkcji DriveLock zalecane jest replikowanie lub tworzenie kopii zapasowych danych przechowywanych na dysku w wewnętrznym systemie informacyjnym przedsiębiorstwa. W przypadku utraty obu haseł używanie zabezpieczonego dysku jest niemożliwe. W praktyce oznacza to utratę całego dysku wraz z zawartymi na nim danymi, co może być problemem dla wielu użytkowników. Jednak dla wspomnianych na początku tej części użytkowników (tzn. ceniących sobie bezpieczeństwo danych) ryzyko utraty dysku i danych bez możliwości ich odczytania przez osoby nieupoważnione jest do przyjęcia.

Korzystanie z zabezpieczenia DriveLock

Jeśli wykryto, że co najmniej jeden z dysków twardych obsługuje zestaw poleceń ATA Security, to w menu Security programu Computer Setup pojawia się opcja DriveLock. W tym menu możliwe jest ustawienie hasła głównego lub włączenie funkcji DriveLock. Jeżeli blokada DriveLock ma zostać włączona, należy podać hasło użytkownika. Ponieważ funkcja ta jest zwykle najpierw konfigurowana przez administratora systemu, jako pierwsze musi zostać ustawione hasło główne. Ustawienie tego hasła jest zalecane, jeżeli planowane jest włączenie funkcji DriveLock, jak również jeżeli funkcja ta nie ma być używana. Umożliwi to administratorowi zmianę ustawień tej opcji w przypadku zablokowania dysku w przyszłości. Po ustawieniu hasła administrator systemu może włączyć funkcję DriveLock lub pozostawić ją wyłączoną.

Jeżeli w systemie zostanie wykryty zablokowany dysk twardy, podczas autotestu POST konieczne będzie podanie odpowiedniego hasła. Jeżeli ustawione jest hasło uruchomieniowe i jest ono takie samo jak hasło użytkownika urządzenia, podczas autotestu POST nie pojawi się prośba o wprowadzenie hasła. W przeciwnym wypadku użytkownik otrzyma monit o podanie hasła funkcji DriveLock. Podczas uruchamiania komputera można podać hasło główne lub hasło użytkownika. Podczas ponownego uruchamiania należy podać to samo hasło, które zostało użyte do odblokowania napędu przy pierwotnym uruchomieniu. Użytkownik może podjąć dwie próby wprowadzenia poprawnego hasła. Jeżeli odpowiednie hasło nie zostanie wprowadzone podczas uruchamiania komputera, to system zostanie uruchomiony, ale zablokowany dysk będzie niedostępny. Jeśli przy ponownym uruchamianiu

lub restarcie z systemu Windows żadna z prób nie powiedzie się, to autotest POST zostanie wstrzymany, a użytkownik zostanie poinformowany o konieczności wyłączenia i włączenia zasilania.

Zastosowania zabezpieczenia DriveLock

Najbardziej praktycznym zastosowaniem funkcji zabezpieczeń DriveLock jest korzystanie z niej w środowisku korporacyjnym. Administrator systemu jest odpowiedzialny za skonfigurowanie dysku twardego, co jest między innymi związane z ustawieniem hasła głównego funkcji DriveLock i tymczasowego hasła użytkownika. W przypadku utraty hasła użytkownika lub przekazania komputera innemu pracownikowi zmiana hasła użytkownika i uzyskanie ponownego dostępu do dysku są możliwe za pomocą hasła głównego.

Firma HP zaleca, aby administratorzy systemu w przedsiębiorstwach, w których stosowana jest funkcja DriveLock, ustanowili ogólne zasady dotyczące ustawiania i obsługi haseł głównych. Jeżeli zasady te nie zostaną ustanowione, może wystąpić sytuacja, w której oba hasła funkcji zostaną ustawione (celowo bądź przez przypadek) przez pracownika na krótko przed zakończeniem jego zatrudnienia (np. Z powodu zwolnienia lub przejścia na emeryturę). Po odejściu pracownika zablokowany przez niego dysk nie będzie mógł być używany i konieczna będzie jego wymiana. Podobnie jeżeli administrator nie ustawi hasła głównego, może nie być możliwe przeprowadzenie sprawdzenia zainstalowanego oprogramowania oraz obsługa innych funkcji kontroli dostępu.

Włączanie funkcji DriveLock nie jest zalecane w przypadku użytkowników, których wymagania dotyczące bezpieczeństwa danych nie są tak wysokie. Kategoria ta obejmuje użytkowników indywidualnych oraz użytkowników, którzy nie przechowują zwykle na swoich dyskach poufnych danych. Dla tych użytkowników ostateczne zablokowanie dysku spowodowane utratą obu haseł funkcji DriveLock jest znacznie bardziej kosztowne niż ewentualne ujawnienie zapisanych na nim danych. Dostęp do opcji DriveLock (i programu Computer Setup) może zostać ograniczony przy użyciu hasła konfiguracyjnego. Dzięki ustawieniu tego hasła administrator systemu może uniemożliwić użytkownikom samodzielne włączanie blokady DriveLock.

Czujnik Smart Cover Sensor

Czujnik zdjęcia pokrywy, dostępny w niektórych modelach, jest kombinacją techniki sprzętowej i programowej, która może powiadamiać o usunięcie pokrywy lub panelu bocznego komputera. Istnieją trzy poziomy zabezpieczeń, jak to opisano w poniższej tabeli.

Tabela 11-2 Poziomy zabezpieczeń czujnika Smart Cover Sensor

Poziom	Ustawienie	Opis
Poziom 0	Disabled (Wyłączone)	Czujnik Smart Cover Sensor jest wyłączony (ustawienie domyślne)
Poziom 1	Notify User (Powiadamianie użytkownika)	Po ponownym uruchomieniu komputera na ekranie pojawi się komunikat informujący o zdjęciu obudowy lub panelu bocznego komputera.
Poziom 2	Setup Password (Hasło konfiguracyjne)	Po ponownym uruchomieniu komputera na ekranie pojawi się komunikat informujący o zdjęciu obudowy lub panelu bocznego komputera. Aby kontynuować, należy wprowadzić hasło konfiguracyjne.

UWAGA: Ustawienia te można zmieniać w programie Computer Setup. Aby uzyskać więcej informacji dotyczących programu Computer Setup, zobacz *Podręcznik do programu Computer Setup (F10)*.

Ustawianie poziomów zabezpieczeń czujnika Smart Cover Sensor

Aby ustawić poziom zabezpieczeń czujnika Smart Cover Sensor, wykonaj poniższe czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie**.
2. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

   UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.
3. Wybierz kolejno **Security** (Zabezpieczenia) > **Smart Cover** (Obudowa inteligentna) > **Cover Removal Sensor** (Czujnik zdjęcia obudowy), a następnie wybierz żądany poziom zabezpieczeń.
4. Przed wyjęciem z programu kliknij kolejno **File** (Plik) > **Save Changes and Exit** (Zapisz zmiany i zakończ).

Blokada Smart Cover Lock

Smart Cover Lock jest sterowaną programowo blokadą obudowy komputera dostępną w niektórych komputerach firmy HP. Blokada zapobiega nieautoryzowanemu dostępowi do wewnętrznych elementów komputera. Komputer jest dostarczany z wyłączoną blokadą SmartCover Lock.

△ **OSTROŻNIE:** Aby zapewnić maksymalną ochronę blokadą pokrywy, trzeba pamiętać o ustawieniu hasła konfiguracyjnego. Hasło konfiguracyjne zabezpiecza przed nieuprawnionym dostępem do programu Computer Setup.

UWAGA: Blokada Smart Cover Lock jest dostępna jako opcja w niektórych systemach.

Włączanie blokady Smart Cover Lock

Aby włączyć blokadę Smart Cover Lock, wykonaj poniższe czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie**.
2. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

   UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.
3. Wybierz kolejno **Security** (Zabezpieczenia) > **Smart Cover** (Obudowa inteligentna) > **Cover Lock** (Blokada obudowy) > **Lock** (Zablokuj).
4. Przed wyjęciem z programu kliknij kolejno **File** (Plik) > **Save Changes and Exit** (Zapisz zmiany i zakończ).

Wyłączanie blokady Smart Cover Lock

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie**.
2. Zaraz po włączeniu komputera, przed uruchomieniem systemu operacyjnego, naciśnij klawisz F10, aby uruchomić program Computer Setup. W razie potrzeby możesz nacisnąć klawisz Enter, aby pominąć ekran tytułowy.

   UWAGA: Jeśli klawisz F10 nie zostanie naciśnięty w odpowiednim czasie, to dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera i ponownym naciśnięciu klawisza F10 przed uruchomieniem systemu operacyjnego.
3. Wybierz kolejno **Security** (Zabezpieczenia) > **Smart Cover** (Obudowa inteligentna) > **Cover Lock** (Blokada Obudowy) > **Unlock** (Odblokuj).
4. Przed wyjęciem z programu kliknij kolejno **File** (Plik) > **Save Changes and Exit** (Zapisz zmiany i zakończ).

Korzystanie z klucza Smart Cover FailSafe Key

Jeżeli włączona jest blokada Smart Cover Lock i z różnych powodów nie można wprowadzić wyłączającego ją hasła konfiguracyjnego, obudowę komputera można otworzyć za pomocą klucza Smart Cover FailSafe Key. Sytuacje, w których niezbędne jest użycie klucza, to:

- Brak zasilania
- Błąd podczas uruchamiania komputera
- Wadliwe elementy komputera (np. wadliwy procesor lub zasilacz)
- Utrata hasła.

△ **OSTROŻNIE:** Klucz Smart Cover FailSafe Key jest specjalizowanym narzędziem, dostępnym w firmie HP. Bądź przygotowany – zamów ten klucz u autoryzowanego sprzedawcy lub usługodawcy, zanim będzie potrzebny.

Aby nabyć klucz FailSafe Key, należy:

- Skontaktować się z autoryzowanym sprzedawcą lub serwisantem produktów firmy HP.
- Zadzwonić pod odpowiedni numer wskazany w gwarancji.

Aby uzyskać więcej informacji o korzystaniu z oprogramowania Smart Cover FailSafe Key, zobacz *Instrukcję obsługi sprzętu*.

Zabezpieczająca blokada kablowa

Panel tylny komputera (niektóre modele) umożliwia podłączenie blokady kablowej, która służy do fizycznego zabezpieczenia sprzętu.

Ilustrowane instrukcje zawiera *Instrukcja obsługi sprzętu*.

Identyfikacja na podstawie analizy linii papilarnych

Dzięki wprowadzeniu opracowanej przez firmę HP technologii identyfikacji użytkownika na podstawie analizy linii papilarnych przestaje być konieczne wprowadzanie haseł, a tym samym podnosi się poziom bezpieczeństwa w sieci, uproszczeniu ulega proces logowania, a także obniżają się koszty związane z zarządzaniem siecią komputerową przedsiębiorstwa. Rozwiązanie to stało się dostępne po atrakcyjnej cenie dla wielu przedsiębiorstw, nie tylko tych wysoko zaawansowanych technologicznie i korzystających z rozbudowanych systemów zabezpieczeń.

UWAGA: W zależności od modelu technologia ta jest wykorzystywana w różny sposób.

Powiadamianie o usterkach i ich usuwanie

Funkcja powiadamiania o usterkach i ich usuwania łączy w sobie zalety nowoczesnej technologii sprzętowej i programowej, dzięki czemu znacznie maleje ryzyko utraty istotnych danych oraz wystąpienia nieplanowanych przestojów w pracy.

Jeśli komputer jest podłączony do sieci pracującej pod kontrolą programu HP Client Manager, powiadomienie o usterce jest przesyłane do tej aplikacji. Za pomocą programu HP Client Manager Software można też zdalnie planować automatyczne uruchamianie diagnostyki na wszystkich zarządzanych komputerach i tworzyć raporty podsumowujące dotyczące testów, które zakończyły się niepowodzeniem.

System ochrony dysków

System ochrony dysków Drive Protection System (DPS) jest narzędziem diagnostycznym, zintegrowanym z dyskami twardymi instalowanymi w niektórych komputerach HP. System ten ułatwia diagnozowanie problemów, w wyniku których mogłaby zaistnieć potrzeba nieobjętej gwarancją wymiany dysku twardego.

Podczas montażu komputerów firmy HP każdy instalowany w nich dysk twardy jest testowany przy użyciu programu DPS, a kluczowe informacje są na nim zapisywane na stałe. Każdorazowe uruchomienie programu DPS powoduje zapisanie wygenerowanych przez niego wyników na dysku twardym. Informacje te mogą pomóc serwisantowi w zdiagnozowaniu warunków, które spowodowały uruchomienie oprogramowania DPS. W *Podręczniku rozwiązywania problemów* można znaleźć informacje dotyczące używania systemu DPS.

Zasilacz z zabezpieczeniem antyprzepięciowym

Zintegrowany zasilacz z zabezpieczeniem antyprzepięciowym zapewnia większą niezawodność pracy komputera w przypadku wystąpienia gwałtownych zmian napięcia w sieci. Bez ryzyka utraty danych i przestojów systemu wytrzymuje on skoki napięcia do 2 000 V.

Czujnik termiczny

Czujnik termiczny jest rozwiązaniem sprzętowo-programowym, śledzącym temperaturę wewnątrz komputera. Umożliwia to wyświetlenie komunikatu ostrzegawczego po przekroczeniu normalnego zakresu, co daje czas na wykonanie odpowiednich czynności, zanim elementy wewnętrzne ulegną uszkodzeniu lub dane zostaną utracone.

△ **OSTROŻNIE:** Wysoka temperatura może spowodować uszkodzenie systemu lub utratę danych.

Indeks

A

adresy internetowe. *Patrz* witryny internetowe
Altiris
  AClient 3
  Client Management Suite 11
  Deployment Solution Agent 3

B

Backup and Recovery Manager 12
BIOS
  HPQFlash 16
  tryb awaryjny odzyskiwania bloku rozruchowego 17
  zdalne programowanie pamięci ROM 16
blokada DriveLock 35
blokada obudowy 37
blokada Smart Cover Lock
  klucz FailSafe 38
  włączanie 38
  wyłączanie 38

C

Client Management Interface, interfejs 5
Client Manager from Symantec 10
czujnik Smart Cover Sensor
  poziomy ochrony 37
  ustawianie 37
czujnik termiczny 40

D

dostęp do komputera, kontrola 27
dwufunkcyjny przycisk zasilania 24
dysk, ochrona 39
dyski twarde, narzędzie diagnostyczne 39

F

firmy HP
  Backup and Recovery Manager 12
  Client Automation Starter, Standard i Enterprise Edition 8
  Client Catalog for Microsoft System Center & SMS Products 11
  Client Management Interface, interfejs 5
  Client Manager from Symantec 10
  ProtectTools Security Manager 7
  System Software Manager 7

H

hasło
  czyszczenie 35
  konfigurowanie 31, 32
  uruchomieniowe 31, 32
  usuwanie 34
  zabezpieczenia 31
  zmiana 33
hasło konfiguracyjne
  ustawianie 31
  usuwanie 34
  wprowadzanie 32
  zmiana 33
hasło uruchomieniowe
  ustawianie 31
  usuwanie 34
  wprowadzanie 32
  zmiana 33
HPQFlash 16

I

identyfikacja na podstawie analizy linii papilarnych 39

K

kabel zabezpieczający z blokadą 39
klucz FailSafe, zamawianie 38
klucz Smart Cover FailSafe Key, zamawianie 38
konfiguracja
  wstępna 2
konfiguracja instalacji, powielanie 18
konfiguracja przycisku zasilania 24
konfiguracja wstępna 2
konfigurowanie
  kopiowanie na jeden komputer 18
  kopiowanie na wiele komputerów 19
konfigurowanie przycisku zasilania 24
kontrola dostępu do komputera 27

N

narzędzia do klonowania, oprogramowanie 2
narzędzia do rozmieszczania, oprogramowanie 2
narzędzie diagnostyczne dla dysków twardych 39

O

obraz preinstalowanego oprogramowania 2
ochrona dysku twardego 39
odzyskiwanie, oprogramowanie 2

oprogramowanie
Altiris AClient 3
Altiris Client Management Suite 11
Altiris Deployment Solution Agent 3
HP Client Automation Starter, Standard i Enterprise Edition 8
HP Client Catalog for Microsoft System Center & SMS Products 11
HP Client Management Interface, interfejs 5
HP Client Manager from Symantec 10
HP ProtectTools Security Manager, oprogramowanie 7
HP System Software Manager 7
integracja 2
narzędzia do aktualizacji i zarządzania 5
odzyskiwanie 2
Proactive Change Notification (PCN) 15
program HP Backup & Recovery Manager 12
rozmieszczanie 2
system ochrony dysków 39
śledzenie zasobów 27
Technika zarządzania 13
Verdiem Surveyor 15
zdalne instalowanie systemu 4

P
powiadamianie o usterkach i ich usuwanie 39
powiadamianie o zmianach 15
Proactive Change Notification (PCN) 15
programowanie pamięci ROM typu flash 16
ProtectTools Security Manager 7
PXE (Preboot Execution Environment) 4

S
separatory, różne układy klawiatury 34
separatory, tabela 34
separatory dla różnych układów klawiatury 34
standardy przemysłowe 26
Subscriber's Choice 15
System Software Manager 7
systemy operacyjne, wsparcie zmiany 25

Ś
śledzenie zasobów 27
środowisko Preboot Execution Environment (PXE) 4

T
Technika zarządzania 13
temperatura, wnętrze komputera 40
tryb awaryjny odzyskiwania, blok rozruchowy 17
tryb awaryjny odzyskiwania bloku rozruchowego 17
tryb odzyskiwania, awaria bloku rozruchowego 17

U
urządzenie rozruchowe
tworzenie 20
urządzenie USB typu flash 20
urządzenie USB typu flash, rozruchowe 20, 22
usuwanie haseł 35
usuwanie hasła 34

V
Verdiem Surveyor 15

W
wewnętrzna temperatura komputera 40
witryny internetowe
Altiris Client Management Suite 11
BIOS, pobieranie oprogramowania 16
HP Client Automation Center 8, 9
HP Client Catalog for Microsoft SMS 11
HP Client Management Interface 6
HP Client Management Solutions 3
HP Client Manager from Symantec 10
HPQFlash 16
HP Softpaq Download Manager 6
HP System Software Manager 7
Intel vPro, technika 13
oprogramowanie 25
pamięć ROM typu flash 16
pobieranie sterowników i oprogramowania 19
Proactive Change Notification 15
Subscriber’s Choice 15
wsparcie firmy HP 12, 13
zabezpieczenia komputera HP Business 8
Zarządzanie konfiguracją 3
zdalne programowanie pamięci ROM 16
włączanie blokady Smart Cover Lock 38
wprowadzanie
hasło konfiguracyjne 32
hasło uruchomieniowe 32
wycofane rozwiązania 15
wyłączanie blokady Smart Cover Lock 38

Z
zabezpieczenia
blokada DriveLock 35
blokada kablowa 39
blokada Smart Cover Lock 37
czujnik Smart Cover Sensor 37
funkcje, tabela 28
hasło 31
identyfikacja na podstawie analizy linii papilarnych 39
ProtectTools Security Manager 7
ustawienia 27

zamawianie klucza FailSafe 38
zasilacz, z zabezpieczeniem antyprzepięciowym 40
zasilacz z zabezpieczeniem antyprzepięciowym 40
zdalne instalowanie systemu 4
zdalne konfigurowanie 4
zdalne programowanie pamięci ROM 16
zgłaszanie zmian 15
zmiana hasła 33
zmiana systemów operacyjnych, wsparcie 25