



i n v e n t

# **Podręcznik zarządzania komputerami typu desktop**

Komputery Business Desktop

Numer katalogowy dokumentu: 361202-241

**Maj 2004**

W tym podręczniku zawarte są definicje i instrukcje dotyczące korzystania z funkcji zabezpieczeń oraz systemu inteligentnego zarządzania Intelligent Manageability, które są zainstalowane fabrycznie na wybranych modelach komputerów.

© Copyright 2004 Hewlett-Packard Development Company, L.P.  
Informacje zawarte w niniejszym dokumencie mogą zostać zmienione  
bez uprzedzenia.

Microsoft oraz Windows są znakami towarowymi firmy Microsoft Corporation  
w USA i w innych krajach.

Warunki gwarancji na produkty i usługi firmy HP są ujęte w odpowiednich  
informacjach o gwarancji towarzyszących tym produktom i usługom. Żadne  
z podanych tu informacji nie powinny być uznawane za jakiegokolwiek gwarancje  
dodatkowe. Firma HP nie ponosi odpowiedzialności za błędy techniczne lub  
wydawnicze, jakie mogą wystąpić w tekście.

Niniejszy dokument zawiera prawnie zastrzeżone informacje, które są  
chronione prawami autorskimi. Żadna część tego dokumentu nie może być  
kopiowana, reprodukowana ani tłumaczona na inny język bez uprzedniej  
pisemnej zgody firmy Hewlett-Packard.



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

---



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

---

## **Podręcznik zarządzania komputerami typu desktop**

Komputery Business Desktop

Wydanie pierwsze — Maj 2004

Numer katalogowy dokumentu: 361202-241

---

# Spis treści

## Podręcznik zarządzania komputerami typu desktop

Początkowa konfiguracja i rozmieszczanie . . . . .	2
Zdalne instalowanie systemu . . . . .	3
Aktualizowanie oprogramowania i zarządzanie nim . . . . .	4
HP Client Manager Software . . . . .	4
Altiris Client Management Solutions . . . . .	5
System Software Manager . . . . .	6
Proactive Change Notification . . . . .	7
Subscriber's Choice . . . . .	7
Pamięć ROM typu flash . . . . .	8
Zdalne zarządzanie pamięcią ROM typu flash . . . . .	8
HPQFlash . . . . .	9
Bezpieczny blok uruchamiania pamięci ROM . . . . .	9
Replikowanie ustawień konfiguracyjnych . . . . .	12
Dwufunkcyjny przycisk zasilania . . . . .	23
Witryna sieci Web . . . . .	24
Współpraca z innymi producentami . . . . .	24
Śledzenie zasobów i funkcje zabezpieczeń . . . . .	25
Zabezpieczanie hasłem . . . . .	30
Ustawianie hasła konfiguracyjnego za pomocą programu Computer Setup . . . . .	31
Ustawianie hasła uruchomieniowego za pomocą programu Computer Setup . . . . .	32
Funkcja DriveLock . . . . .	37
Czujnik Smart Cover Sensor . . . . .	39
Blokada Smart Cover Lock . . . . .	41
Zabezpieczenie głównego rekordu rozruchowego . . . . .	44
Czynności wykonywane przed partycjonowaniem lub formatowaniem bieżącego dysku rozruchowego . . . . .	46
Zabezpieczająca blokada kablowa . . . . .	47
Identyfikacja na podstawie analizy linii papilarnych . . . . .	47

Powiadamianie o usterkach i ich usuwanie . . . . .	48
System ochrony dysków . . . . .	48
Zasilacz z zabezpieczeniem antyprzepięciowym . . . . .	49
Czujnik termiczny . . . . .	49

## **Indeks**

---

# Podręcznik zarządzania komputerami typu desktop

System HP Intelligent Manageability obejmuje standardowe rozwiązania służące do sterowania i sprawowania nadzoru nad komputerami stacjonarnymi, przenośnymi i stacjami roboczymi 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 — zakrojone na szeroką skalę — prace mające na celu rozwój standardów i infrastruktury, pozwalających na efektywne rozmieszczanie i konfigurowanie komputerów stacjonarnych, przenośnych i stacji roboczych oraz zarządzanie nimi. W związku z tym podjęto ścisłą współpracę z wiodącymi producentami oprogramowania, co umożliwiło zachowanie zgodności między dostarczonymi przez nich programami a systemem Intelligent Manageability. System ten jest istotnym elementem prowadzonych działań, których celem jest opracowanie rozwiązań wspomagających decyzje klientów podczas czterech faz cyklu życia komputerów typu desktop — planowania, rozmieszczania, zarządzania i unowocześniania.

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
- Śledzenie i funkcje zabezpieczeń zasobów
- Powiadamianie o usterkach i ich usuwanie



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

---

## Początkowa konfiguracja i rozmieszczanie

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.
- Zastąpienie preinstalowanego oprogramowania dostosowanym obrazem oprogramowania za pomocą narzędzi rozmieszczania (np. Altiris Deployment Solution™).
- 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. Informacje pomocne w wyborze tej metody można uzyskać w części dotyczącej rozmieszczania komputera, dostępnej w witrynie sieci Web poświęconej zalecanym rozwiązaniom i oferowanym usługom (<http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html>).

Informacje o odzyskiwaniu oprogramowania systemowego, zarządzaniu konfiguracją i energią oraz rozwiązywaniu problemów można znaleźć na dysku CD *Restore Plus!*, a także w dokumentacji dotyczącej programu Computer Setup i sprzętu obsługującego funkcję ACPI.

## Zdalne instalowanie systemu

Funkcja zdalnego instalowania systemu umożliwia uruchomienie i skonfigurowanie systemu operacyjnego za pomocą oprogramowania i informacji konfiguracyjnych znajdujących się na serwerze sieciowym, poprzez inicjację środowiska Preboot Execution Environment (PXE). Funkcja zdalnego instalowania systemu służy zazwyczaj do instalowania i konfigurowania systemu operacyjnego, lecz może również zostać użyta do przeprowadzenia następujących zadań:

- formatowanie dysku twardego,
- rozmieszczanie obrazu oprogramowania na jednym lub kilku nowych komputerach,
- zdalne aktualizowanie systemu BIOS w pamięci ROM typu flash („Zdalne zarządzanie pamięcią ROM typu flash” na stronie 8),
- konfigurowanie ustawień systemu BIOS.

Aby rozpocząć proces zdalnego instalowania systemu, należy nacisnąć klawisz **F12** (po pojawieniu się — w prawym dolnym rogu ekranu z logo firmy HP — komunikatu „F12 = Network Service Boot”), a następnie postępować zgodnie z wyświetlanymi instrukcjami. Domyślna kolejność uruchamiania jest ustawieniem konfiguracyjnym systemu BIOS, które można zmienić na opcję podejmowania każdorazowo próby uruchomienia środowiska PXE.

Firmy HP oraz Altiris wspólnie opracowały narzędzia pozwalające na łatwiejsze i szybsze przeprowadzanie rozmieszczania komputerów oraz zarządzanie nimi w ramach przedsiębiorstwa. Dzięki znacznemu obniżeniu całkowitych kosztów związanych z wdrożeniem systemu informatycznego, komputery klienckie firmy HP stanowią najodpowiedniejsze — pod kątem zarządzania — rozwiązanie dla przedsiębiorstwa.

## Aktualizowanie oprogramowania i zarządzanie nim

Firma HP oferuje kilka narzędzi służących do zarządzania oprogramowaniem zainstalowanym na komputerach typu desktop i stacjach roboczych oraz aktualizowania go — HP Client Manager Software, Altiris Client Management Solutions, System Software Manager, Proactive Change Notification oraz Subscriber's Choice.

### HP Client Manager Software

Narzędzie HP Client Manager Software (HP CMS) pomaga klientom firmy HP w zarządzaniu stroną sprzętową komputerów klienckich za pomocą następujących funkcji:

- Szczegółowe widoki spisu sprzętu dla celów zarządzania zasobami.
- Monitorowanie stanu komputera i diagnostyka.
- Proaktywne powiadomienia o zmianach w środowisku sprzętowym.
- Dostępne poprzez sieć Web raporty o szczegółach krytycznych dla działalności, takich jak komputery z ostrzeżeniami termicznymi, alerty pamięci i wiele innych.
- Zdalne aktualizowanie oprogramowania systemowego, np. sterowników sprzętowych i pamięci ROM BIOS.
- Zdalna zmiana kolejności uruchamiania.

Więcej informacji o oprogramowaniu HP Client Manager można znaleźć na stronie:

[http://h18000.www1.hp.com/im/client\\_mgr.html](http://h18000.www1.hp.com/im/client_mgr.html).



## Altiris Client Management Solutions

Firmy HP oraz Altiris wspólnie opracowały kompleksowe, ściśle zintegrowane rozwiązania do zarządzania systemami, które pozwalają obniżyć koszty posiadania klienckich komputerów firmy HP. Oprogramowanie HP Client Manager Software jest podstawą dodatkowych rozwiązań Altiris Client Management Solutions, które dotyczą następujących dziedzin:

- Zarządzanie spisem i zasobami
  - ❑ Zgodność licencji na oprogramowanie
  - ❑ Śledzenie komputera i generowanie raportów
  - ❑ Śledzenie kontraktów leasingowych i środków trwałych
- Rozmieszczanie i migracja
  - ❑ Migracja systemu Windows XP Professional lub Home Edition
  - ❑ Rozmieszczanie systemu
  - ❑ Migracje osobowości
- Punkt pomocy i rozwiązywanie problemów
  - ❑ Zarządzanie kuponami punktu pomocy
  - ❑ Zdalne usuwanie problemów
  - ❑ Zdalne rozwiązywanie problemów
  - ❑ Odzyskiwanie komputerów klienckich po awarii
- Zarządzanie oprogramowaniem i operacjami
  - ❑ Bieżące zarządzanie komputerami typu desktop
  - ❑ Rozmieszczanie oprogramowania systemowego firmy HP
  - ❑ Samonaprawianie aplikacji

Więcej informacji oraz szczegóły dotyczące pobierania w pełni funkcjonalnej 30-dniowej wersji ewaluacyjnej rozwiązań firmy Altiris można znaleźć na stronie

<http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

W przypadku wybranych modeli komputerów stacjonarnych i przenośnych w skład fabrycznie załadowanego obrazu wchodzi agent zarządzania Altiris. Agent ten umożliwia komunikację z oprogramowaniem Altiris Development Solution, za pomocą którego można wykonać nowe rozmieszczanie sprzętu lub migrację osobowości do nowego systemu operacyjnego przy użyciu łatwych w obsłudze kreatorów. Rozwiązania Altiris stanowią wygodne narzędzie dystrybucji oprogramowania. Używane w połączeniu z oprogramowaniem System Software Manager lub HP Client Manager Software, umożliwiają też administratorom aktualizowanie oprogramowania ROM BIOS oraz sterowników urządzeń z poziomu centralnej konsoli.

Więcej informacji można znaleźć na stronie  
<http://h18000.www1.hp.com/im/index.html>.

## **System Software Manager**

Program narzędziowy System Software Manager (SSM) służy do równoczesnego aktualizowania oprogramowania systemowego zainstalowanego w różnych systemach. Po jego uruchomieniu na komputerze klienckim wykrywane są wersje sprzętu i oprogramowania, a następnie wybrane programy są aktualizowane plikami pochodzącymi z repozytorium centralnego, zwanego także magazynem plików. Wersje sterowników obsługiwane przez oprogramowanie SSM są oznaczone specjalną ikoną w witrynie pobierania sterowników oraz na dysku CD Support Software. Aby pobrać oprogramowanie SSM i uzyskać więcej informacji na jego temat, należy odwiedzić stronę:  
<http://www.hp.com/go/ssm>.

## 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 z nawet 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 swój 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?jumpid=go/pcn>.

## 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 zasubskrybowane w profilu są dostępne do przejrzania 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>.

## Pamięć ROM typu flash

Komputer jest standardowo wyposażony w programowalną pamięć 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 pamięci ROM, można:

- zamówić u przedstawiciela firmy HP dyskietkę zawierającą uaktualniony pakiet ROMPaq,
- pobrać najnowszą wersję plików ROMPaq ze strony sterowników i wsparcia technicznego HP (<http://www.hp.com/support/files>).



**PRZESTROGA:** 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 zarządzanie pamięcią ROM typu flash

Funkcja zdalnego zarządzania pamięcią ROM typu flash umożliwia administratorowi systemu zdalne uaktualnianie pamięci ROM 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 zawartości pamięci ROM na sieciowych komputerach firmy HP. W rezultacie ulega poprawie wydajność pracy oraz obniżają się ogólne koszty związane z eksploatacją sieci w przedsiębiorstwie.



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 na stronie <http://h18000.www1.hp.com/im/prodinfo.html>.

## HPQFlash

Program narzędziowy HPQFlash służy do lokalnego aktualizowania lub przywracania systemowej pamięci ROM na pojedynczych komputerach poprzez system operacyjny Windows.

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

## Bezpieczny blok uruchamiania pamięci ROM

Bezpieczny blok uruchamiania pamięci ROM (FailSafe Boot Block ROM) umożliwia odzyskiwanie zasobów systemowych w przypadku nieudanej aktualizacji pamięci ROM typu flash (np. w razie awarii zasilania podczas aktualizacji tej pamięci). Blok ten stanowi część pamięci ROM, jest jednak zabezpieczony przed aktualizacją. Jego zadaniem jest sprawdzanie poprawności zawartości pamięci ROM typu flash po włączeniu zasilania systemu.

- Jeżeli sprawdzenie poprawności przebiegnie pomyślnie, system zostanie uruchomiony w zwykły sposób.
- Jeżeli w systemowej pamięci ROM zostaną wykryte błędy, bezpieczny blok uruchamiania umożliwi uruchomienie systemu z dyskietki ROMPaq, która przeprogramuje uszkodzoną pamięć.



Niektóre modele komputerów obsługują odzyskiwanie z dysku CD ROMPaq. Obrazy ISO ROMPaq są dołączone do wybranych modeli w możliwych do pobrania plikach ROM softpaqs.

Jeżeli blok uruchamiania wykryje nieprawidłową systemową pamięć ROM, dioda zasilania zamiga osiem razy (kolor czerwony) w odstępach jednosekundowych, po czym nastąpi 2-sekundowa pauza. Odtworzonych też zostanie 8 sygnałów dźwiękowych. Na ekranie zostanie wyświetlony komunikat o pracy w trybie odzyskiwania bloku uruchamiania (niektóre modele).

Aby odzyskać system po uruchomieniu go w trybie odzyskiwania bloku uruchamiania:

1. Jeżeli w napędzie dyskietek znajduje się dyskietka lub w napędzie CD znajduje się dysk CD, wyjmij dyskietkę lub dysk CD, a następnie wyłącz zasilanie.
2. Włóż dyskietkę ROMPaq do napędu dyskietek lub (w przypadku niektórych modeli) dysk CD ROMPaq do napędu CD.
3. Włącz komputer.

Jeżeli dyskietka ROMPaq lub dysk CD ROMPaq nie zostaną znalezione, pojawi się monit o włożenie odpowiedniego nośnika do napędu i ponowne uruchomienie komputera.

Jeżeli ustawiono hasło konfiguracyjne, włączy się wskaźnik Caps Lock na klawiaturze i pojawi się monit o wprowadzenie hasła.

4. Wprowadź hasło konfiguracyjne.

Włączenie się wszystkich trzech diod klawiatury po uruchomieniu systemu z dyskietki oznacza, że pamięć ROM została pomyślnie przeprogramowana. Gdy proces dobiegnie końca, zostanie również wyemitowana seria sygnałów dźwiękowych o coraz wyższej częstotliwości.

5. Wyjmij dyskietkę lub dysk CD i wyłącz zasilanie.
6. Włącz zasilanie, aby uruchomić ponownie komputer.

Poniższa tabela zawiera wykaz kombinacji wskaźników klawiatury używanych przez blok uruchamiania pamięci ROM (gdy do komputera jest podłączona klawiatura PS/2), jak również znaczenie i stan związany z każdą kombinacją.

## Kombinacje wskaźników klawiatury używane przez blok uruchamiania pamięci ROM

Tryb bezpiecznego bloku uruchamiania	Kolor diody na klawiaturze	Stan diody na klawiaturze	Stan/Komunikat
Num Lock	Zielona	Włączona	Brak dyskietki ROMPaq lub dysku CD ROMPaq, dyskietka lub dysk jest uszkodzony bądź napęd nie jest gotowy.
Caps Lock	Zielona	Włączona	Wprowadź hasło.
Num, Caps, Scroll Lock	Zielona	Migają pojedynczo w następującej kolejności: Num, Caps, Scroll Lock	Klawiatura jest zablokowana w trybie sieciowym.
Num, Caps, Scroll Lock	Zielona	Włączona	Blok uruchamiania pamięci ROM typu flash — operacja zakończona pomyślnie. Wyłącz zasilanie, a następnie uruchom komputer ponownie.



Wskaźniki diagnostyczne nie migają w przypadku klawiatury podłączonej przez złącze USB.

## Replikowanie ustawień konfiguracyjnych

Przy użyciu 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.



W przypadku obu procedur wymagany jest napęd dyskietek lub obsługiwane urządzenie USB typu flash, np. HP Drive Key.

---

## Kopiowanie na jeden komputer



**PRZESTROGA:** 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 dc7100 typu ultra-slim desktop do komputera dx6100 typu slim tower.

---

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 naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.
- 



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

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 dyskiecie 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 naciśnij i przytrzymaj klawisz **F10**, aż otworzy się 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



**PRZESTROGA:** 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 dc7100 typu ultra-slim desktop do komputera dx6100 typu slim tower.

---

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

---



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 12).

---

1. Utwórz dyskietkę rozruchową lub rozruchowe urządzenie USB typu flash. Zobacz część „Obsługiwane urządzenie USB typu flash” na stronie 16 lub „Nieobsługiwane urządzenie USB typu flash” na stronie 20.



**PRZESTROGA:** Nie wszystkie komputery można uruchomić za pomocą urządzenia USB typu flash. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności uruchamiania 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 naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

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/support/files> 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 urządzenie USB typu flash

Obsługiwane urządzenia, takie jak HP Drive Key lub DiskOnKey, są wyposażone w preinstalowany obraz, co upraszcza proces przekształcania ich w urządzenia rozruchowe. Jeśli używane urządzenie USB typu flash nie jest wyposażone w taki obraz, należy użyć procedury opisanej dalej w tej części (zobacz „Nieobsługiwane urządzenie USB typu flash” na stronie 20).



---

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

---

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

- Jeden z następujących komputerów:
  - ❑ HP Compaq Business Desktop, seria dc7100
  - ❑ HP Compaq Business Desktop, seria dx6100
  - ❑ HP Compaq Business Desktop, seria d530 — typu ultra-slim desktop, small form factor lub convertible minitower
  - ❑ Compaq Evo D510 typu ultra-slim desktop
  - ❑ Compaq Evo D510 typu convertible minitower/small form factor

W zależności od indywidualnych ustawień systemu BIOS, przyszłe komputery będą mogły obsługiwać również uruchamianie za pomocą urządzenia USB typu flash.



---

**PRZESTROGA:** Jeśli używany jest komputer inny niż wyżej wymienione, należy upewnić się, czy urządzenie USB jest wymienione przed dyskiem twardym na liście kolejności uruchamiania w programie Computer Setup (F10).

---

- Jeden z następujących modułów pamięci:
  - HP Drive Key 16 MB
  - HP Drive Key 32 MB
  - DiskOnKey 32 MB
  - HP Drive Key 64 MB
  - DiskOnKey 64 MB
  - HP Drive Key 128 MB
  - DiskOnKey 128 MB
  - HP Drive Key 256 MB
  - DiskOnKey 256 MB
- Dyskietka rozruchowa DOS z programami 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.
  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 A:\, wpisując **FDISK** i naciskając klawisz Enter. Po wyświetleniu monitu kliknij przycisk **Yes (Y)**, aby włączyć obsługę napędów o dużej pojemności.
  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: \_\_\_\_\_



**PRZESTROGA:** 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.
- 



**PRZESTROGA:** 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.
- 



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

---

Polecenie FORMAT spowoduje wyświetlenie jednego lub większej liczby ostrzeżeń i za każdym razem pojawi się pytanie, czy proces ma być kontynuowany. W odpowiedzi należy każdorazowo wpisać literę **Y**. Polecenie FORMAT spowoduje 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 pomiąć.
12. Skopiuj wszystkie pliki zapisane w punkcie 9 na urządzenie USB typu flash.
13. Wyjmij dyskiętkę i uruchom ponownie komputer. Komputer zostanie uruchomiony z urządzeniem USB typu flash jako dyskiem C.



Na każdym komputerze może być określona inna domyślna kolejność uruchamiania urządzeń — do jej zmiany służy program narzędziowy Computer Setup (F10).

W wersji DOS dla środowiska Windows 9x może się chwilowo pojawić ekran z logo 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 13.

## Nieobsługiwane urządzenie USB typu flash

---



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

---

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

- Jeden z następujących komputerów:
  - ❑ HP Compaq Business Desktop, seria dc7100
  - ❑ HP Compaq Business Desktop, seria dx6100
  - ❑ HP Compaq Business Desktop, seria d530 — typu ultra-slim desktop, small form factor lub convertible minitower
  - ❑ Compaq Evo D510 typu ultra-slim desktop
  - ❑ Compaq Evo D510 typu convertible minitower/small form factor

W zależności od indywidualnych ustawień systemu BIOS, przyszłe komputery będą mogły obsługiwać również uruchamianie za pomocą urządzenia USB typu flash.

---



**PRZESTROGA:** Jeśli używany jest komputer inny niż wyżej wymienione, należy upewnić się, czy urządzenie USB jest wymienione przed dyskiem twardym na liście kolejności uruchamiania w programie Computer Setup (F10).

---

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



**PRZESTROGA:** Kabel zasilający MUSI zostać odłączony.

---



2. Zdejmij pokrywę 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 pokrywę komputera.
4. Podłącz kabel zasilający i włącz komputer.
5. Zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

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 później potrzebna do ponownego przypisania przerwania IRQ. Zamknij program konfiguracyjny i potwierdź zmiany.

Przerwanie IRQ SATA: \_\_\_\_\_

7. Włóż do napędu dyskietskę 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 pokrywę komputera i ponownie zainstaluj wszystkie wyjęte wcześniej karty PCI. Zamknij pokrywę komputera.
13. Podłącz kabel zasilający, wyjmij z napędu dyskietkę, a następnie włącz komputer.
14. Zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, aż otworzy się 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.



---

Na każdym komputerze może być określona inna domyślna kolejność uruchamiania urządzeń — do jej zmiany służy program narzędziowy Computer Setup (F10). Więcej informacji na ten temat można znaleźć w *Podręczniku do programu Computer Setup* na dysku CD *Documentation*.

W wersji DOS dla środowiska Windows 9x może się chwilowo pojawić ekran z logo 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 13.

## Dwufunkcyjny przycisk zasilania

Jeżeli aktywny jest interfejs zaawansowanego zarządzania konfiguracją i energią (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 (przejsie 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 natomiast 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.



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

---

## Witryna sieci Web

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. Oprogramowanie można pobrać ze 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.

## Współpraca z innymi producentami

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)

## 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 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. Wbudowany mikroukład zabezpieczeń ProtectTools Embedded Security (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 *Getting Started, HP ProtectTools Embedded Security Manager* na dysku CD *Documentation*). Dostępne w wybranych modelach funkcje zabezpieczeń, takie jak ProtectTools, blokada Smart Cover Lock i czujnik Smart Cover Sensor, zapobiegają nieautoryzowanemu dostępowi do wewnętrznych podzespołów komputera. Z kolei wyłączając porty szeregowo, równoległe lub USB albo wyłączając możliwość uruchamiania systemu z nośników wymiennych, można chronić cenne dane. Alerty dotyczące zmiany rozmiaru pamięci oraz otwarcia pokrywy mogą być automatycznie przesyłane do aplikacji zarządzania systemem, przez co będą pełniły funkcję proaktywnego powiadamiania o ingerencji w wewnętrzne elementy komputera.



Pakiet 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 programu Computer Setup można znaleźć w *Podręczniku do programu Computer Setup (F10)* na dysku CD *Documentation*.
- Zdalnie, za pomocą programu HP Client Manager Software lub System Software Manager, umożliwiającego bezpieczne rozmieszczanie i kontrolowanie jednolitych ustawień zabezpieczeń z poziomu prostego narzędzia wiersza polecenia.

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

---



## Przegląd funkcji zabezpieczeń

---

Opcja	Opis
Setup Password (Hasło konfiguracyjne)	<p>Umożliwia ustawianie i włączanie hasła konfiguracyjnego (administratora).</p> <p> Jeżeli ustawione zostanie hasło konfiguracyjne, jego wprowadzanie jest wymagane przy próbie: zmiany opcji programu Computer Setup, uaktualnienia pamięci ROM typu flash i zmiany określonych ustawień plug and play w systemie Windows.</p> <p>Więcej informacji znajduje się w <i>Podręczniku rozwiązywania problemów</i> na dysku CD <i>Documentation</i>.</p>
Power-On Password (Hasło uruchomieniowe)	<p>Umożliwia ustawianie i włączanie hasła uruchomieniowego.</p> <p>Więcej informacji znajduje się w <i>Podręczniku rozwiązywania problemów</i> na dysku CD <i>Documentation</i>.</p>
Password Options (Opcje hasła) (Opcja ta zostanie wyświetlona tylko pod warunkiem, że ustawiono hasło uruchomieniowe).	<p>Umożliwia określenie, czy przy ponownym uruchomieniu komputera za pomocą kombinacji klawiszy <b>CTRL+ALT+DEL</b> wymagane jest podanie hasła.</p> <p>Więcej informacji znajduje się w <i>Podręczniku zarządzania komputerami typu desktop</i> na dysku CD <i>Documentation</i>.</p>
Pre-Boot Authorization (Autoryzacja przed rozruchem)	<p>Umożliwia włączanie/wyłączanie karty inteligentnej, która może być używana w zastępstwie hasła uruchomieniowego.</p>
	<p>Więcej informacji o programie Computer Setup można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Documentation</i>.</p> <p>Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.</p>



---

## Przegląd funkcji zabezpieczeń (ciąg dalszy)

Opcja	Opis
Smart Cover (Pokrywa inteligentna)	<p>Funkcja ta umożliwia:</p> <ul style="list-style-type: none"> <li>• Włączanie/wyłączanie blokady Smart Cover Lock.</li> <li>• Włączanie/wyłączanie czujnika Cover Removal Sensor.</li> </ul> <p> Funkcja <i>Notify User</i> służy do powiadamiania użytkownika o tym, że pokrywa została zdjęta. Aby można było uruchomić komputer ze zdjętą pokrywą, wymagane jest wprowadzenie <i>hasła konfiguracyjnego</i>.</p> <p>Funkcja ta jest obsługiwana jedynie w niektórych modelach. Więcej informacji znajduje się w <i>Podręczniku zarządzania komputerami typu desktop</i> na dysku CD <i>Documentation</i>.</p>
Embedded Security (Wbudowany mikroukład zabezpieczeń)	<p>Funkcja ta umożliwia:</p> <ul style="list-style-type: none"> <li>• Włączanie/wyłączanie urządzenia obsługującego wbudowany mikroukład zabezpieczeń.</li> <li>• Przywracanie fabrycznych ustawień urządzenia.</li> </ul> <p>Funkcja ta jest obsługiwana jedynie w niektórych modelach. Więcej informacji można znaleźć w <i>Podręczniku wbudowanego mikroukładu zabezpieczeń HP ProtectTools</i> na dysku CD <i>Documentation</i>.</p>
Device Security (Zabezpieczenia urządzeń)	<p>Włącza/wyłącza porty szeregowy, port równoległy, przednie porty USB, dźwięk systemowy, kontrolery sieci (wybrane modele), urządzenia MultiBay (wybrane modele) oraz kontrolery SCSI (wybrane modele).</p>
Network Service Boot (Uruchamianie z sieci)	<p>Włącza/wyłącza możliwość uruchamiania 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 zainstalowany w magistrali PCI lub bezpośrednio na płycie głównej.</p>
	<p>Więcej informacji o programie Computer Setup można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Documentation</i>.</p> <p>Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.</p>

## Przegląd funkcji zabezpieczeń (ciąg dalszy)

---

Opcja	Opis
System IDs (Identyfikatory systemowe)	<p>Umożliwia ustawianie:</p> <ul style="list-style-type: none"><li>Etykiety zasobu (identyfikator składający się z 18 znaków) i etykiety właściciela (identyfikator składający się z 80 znaków i wyświetlany podczas autotestu POST).</li></ul> <p>Więcej informacji znajduje się w <i>Podręczniku zarządzania komputerami typu desktop</i> na dysku CD <i>Documentation</i>.</p> <ul style="list-style-type: none"><li>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).</li></ul> <p>Układu klawiatury (np. angielska lub niemiecka) do wprowadzania systemowych danych identyfikacyjnych.</p>
DriveLock	<p>Umożliwia przydzielenie bądź zmodyfikowanie hasła głównego lub hasła użytkownika dysków twardych MultiBay (funkcja nieobsługiwana w przypadku dysków twardych SCSI). Włączenie tej funkcji spowoduje, że podczas autotestu POST konieczne będzie wprowadzenie jednego z haseł blokady DriveLock. Jeśli żadne z nich nie zostanie pomyślnie wprowadzone, dysk twardy chroniony hasłem będzie niedostępny do momentu wprowadzenia poprawnego hasła podczas kolejnego uruchomienia komputera.</p> <p> Opcja ta jest wyświetlana tylko w przypadku, gdy co najmniej dysk MultiBay w systemie obsługuje funkcję DriveLock.</p> <p>Więcej informacji znajduje się w <i>Podręczniku zarządzania komputerami typu desktop</i> na dysku CD <i>Documentation</i>.</p>
	<p>Więcej informacji o programie Computer Setup można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Documentation</i>.</p> <p>Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.</p>



---



---

**Przegląd funkcji zabezpieczeń (ciąg dalszy)**



---

<b>Opcja</b>	<b>Opis</b>
Master Boot Record Security (Zabezpieczenie głównego rekordu rozruchowego)	<p>Umożliwia włączanie/wyłączanie zabezpieczenia głównego rekordu rozruchowego (MBR).</p> <p>Włączenie tej funkcji blokuje zapisywanie zmian w głównym rekordzie rozruchowym na bieżącym dysku rozruchowym. Przy każdym włączaniu lub ponownym uruchamianiu komputera główny rekord rozruchowy dysku rozruchowego jest porównywany z poprzednio zapisanym głównym rekordem rozruchowym. Jeśli zostaną wykryte zmiany, użytkownik będzie miał do wyboru trzy opcje: zapisanie rekordu MBR na bieżącym dysku rozruchowym, odtworzenie uprzednio zapisanych ustawień rekordu MBR lub wyłączenie funkcji zabezpieczenia rekordu MBR. Do wykonania każdej z tych czynności niezbędne jest wprowadzenie hasła konfiguracyjnego (jeżeli zostało ustawione).</p> <p> Przed partycjonowaniem lub formatowaniem bieżącego dysku rozruchowego należy wyłączyć funkcję zabezpieczenia rekordu MBR. Rekord MBR może być aktualizowany przez niektóre narzędzia modyfikacji dysków (np. FDISK lub FORMAT).</p> <p>Jeżeli funkcja zabezpieczenia MBR została włączona, a dostęp do dysku jest obsługiwany przez system BIOS, zapisywanie zmian do rekordu MBR nie jest możliwe, a w narzędziach modyfikacji dysków wyświetlane są komunikaty o błędach.</p> <p>Jeżeli funkcja zabezpieczenia MBR została włączona, a dostęp do dysku jest obsługiwany przez system operacyjny, wszelkie zmiany w rekordzie MBR zostaną wykryte przez system BIOS podczas kolejnego uruchomienia systemu. Wtedy wyświetlone zostanie ostrzeżenie.</p>
	<p>Więcej informacji o programie Computer Setup można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Documentation</i>.</p> <p>Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.</p>


---

## Przegląd funkcji zabezpieczeń (ciąg dalszy)


---

Opcja	Opis
Save Master Boot Record (Zapisz główny rekord rozruchowy)	Zapisuje kopię zapasową głównego rekordu rozruchowego (MBR) bieżącego dysku rozruchowego. Opcja ta jest wyświetlana tylko przy włączonej funkcji zabezpieczenia MBR.
Restore Master Boot Record (Przywróć główny rekord rozruchowy)	Przywraca główny rekord rozruchowy (MBR) z kopii zapasowej na bieżący dysk rozruchowy.  Opcja ta jest wyświetlana tylko wtedy, gdy: <ul style="list-style-type: none"><li>włączono zabezpieczenie MBR,</li><li>zapisano kopię zapasową rekordu MBR,</li><li>bieżący dysk rozruchowy jest tym, na podstawie którego utworzono kopię zapasową rekordu MBR.</li></ul>

---

 **PRZESTROGA:** Przywrócenie uprzednio zapisanego głównego rekordu rozruchowego (MBR) po jego zmodyfikowaniu przez narzędzie dyskowe lub system operacyjny może uniemożliwić dostęp do danych. Przywracanie uprzednio zapisanego głównego rekordu rozruchowego powinno być przeprowadzane tylko w przypadku jego uszkodzenia lub zainfekowania przez wirusa.

---

 Więcej informacji o programie Computer Setup można znaleźć w *Podręczniku do programu Computer Setup (F10)* na dysku CD *Documentation*.

Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.

---

## 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 hasłem konfiguracyjnym obowiązującym w całej sieci. 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 wbudowanego mikroukładu zabezpieczeń HP ProtectTools* na dysku CD *Documentation*. 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 hasła.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie**.
2. Zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

3. Wybierz menu **Security (Zabezpieczenia)**, wybierz opcję **Setup Password (Hasło konfiguracyjne)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjściem 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, 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 naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

3. Wybierz menu **Security (Zabezpieczenia)**, wybierz opcję **Power-On Password (Hasło uruchomieniowe)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjściem 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**.



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 wbudowanego mikroukładu zabezpieczeń HP ProtectTools* na dysku CD *Documentation*.

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 naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.
- 



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

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



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 wbudowanego mikroukładu zabezpieczeń HP ProtectTools* na dysku CD *Documentation*.

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 konfiguracyjne, zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

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**



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.



Informacje na temat innych separatorów można znaleźć w części „Separatory dla różnych układów klawiatury” na stronie 36. 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 wbudowanego mikroukładu zabezpieczeń HP ProtectTools* na dysku CD *Documentation*.

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 konfiguracyjne, zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



---

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

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**.



---

Informacje na temat innych separatorów można znaleźć w części „[Separatory dla różnych układów klawiatury](#)”. 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

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

\* dotyczy Bośni-Hercegowiny, Chorwacji, Słowenii i Jugosławii

## Czyszczenie haseł

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

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku wbudowanego mikroukładu zabezpieczeń HP ProtectTools* na dysku CD *Documentation*.



## Funkcja DriveLock

DriveLock to będąca standardem przemysłowym funkcja zabezpieczeń, która zapobiega nieautoryzowanemu dostępowi do danych przechowywanych na dyskach twardech MultiBay. Funkcja ta jest zaimplementowana jako rozszerzenie programu Computer Setup. Jest ona dostępna tylko po wykryciu w systemie dysku twardego z obsługą funkcji DriveLock.

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 nieporównanie 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 użytkowników wspomnianych na początku tej części (tzn. ceniących sobie bezpieczeństwo danych) ryzyko utraty dysku i danych bez możliwości ich odczytania przez osoby nieupoważnione jest do przyjęcia.

## Korzystanie z funkcji DriveLock

Opcja DriveLock jest dostępna w menu Security (Zabezpieczenia) programu Computer Setup. W tym menu możliwe jest ustawienie hasła głównego lub włączenie funkcji DriveLock. Jeżeli funkcja DriveLock ma zostać włączona, należy podać hasło użytkownika. Ponieważ funkcja ta jest zwykle najpierw skonfigurowana 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 twardej, 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 monit o wprowadzenie hasła. W przeciwnym wypadku użytkownik otrzyma monit o podanie hasła funkcji DriveLock. Można wprowadzić również hasło główne. Użytkownik może podjąć dwie próby wprowadzenia poprawnego hasła. Jeżeli odpowiednie hasło nie zostanie wprowadzone, autotest POST będzie kontynuowany, ale zablokowany dysk będzie niedostępny.

## Zastosowania funkcji DriveLock

Najbardziej praktycznym zastosowaniem funkcji zabezpieczeń DriveLock jest korzystanie z niej w środowisku korporacyjnym, w którym administrator systemu udostępnia użytkownikom niektórych komputerów dyski twarde MultiBay. Administrator systemu jest odpowiedzialny za skonfigurowanie dysku twardego MultiBay, co jest między innymi związane z ustawieniem hasła głównego funkcji DriveLock. 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.

Zalecane jest, 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. Przez określenie hasła konfiguracyjnego i zablokowanie dostępu do niego przez użytkowników końcowych, administratorzy systemów mogą ograniczyć użytkownikom możliwość włączania funkcji DriveLock.


## **Czujnik Smart Cover Sensor**

Cover Removal Sensor to dostępna w wybranych modelach komputera funkcja będąca połączeniem technologii sprzętowych i programowych, która może wysyłać alerty informujące o zdjęciu pokrywy lub panelu dostępu komputera. Czujnik ten oferuje trzy poziomy zabezpieczeń, opisane w poniższej tabeli.

## Poziomy zabezpieczeń czujnika Smart Cover Sensor

---

Poziom	Ustawienie	Opis
Poziom 0	Disabled (Wyłączony)	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 pokrywy lub panelu bocznego komputera.
Poziom 2	Setup Password (Hasło konfiguracyjne)	Po ponownym uruchomieniu komputera na ekranie pojawi się komunikat informujący o zdjęciu pokrywy lub panelu bocznego komputera. Aby kontynuować, należy wprowadzić hasło konfiguracyjne.

 Ustawienia te można zmieniać w programie Computer Setup. Więcej informacji o programie Computer Setup można znaleźć w *Podręczniku do programu Computer Setup (F10)* na dysku CD *Documentation*.

---

## 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 naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

3. Wybierz kolejno **Security (Zabezpieczenia) > Smart Cover (Pokrywa inteligentna) > Cover Removal Sensor (Czujnik zdjęcia pokrywy)**, a następnie wybierz żądany poziom zabezpieczeń.
4. Przed wyjściem 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 pokrywy komputera dostępną w wybranych komputerach firmy HP. Blokada zapobiega nieautoryzowanemu dostępowi do wewnętrznych elementów komputera. Komputer jest dostarczany z wyłączoną blokadą SmartCover Lock.



**PRZESTROGA:** Aby zabezpieczyć ustawienia blokady SmartCover Lock, należy pamiętać o ustawieniu hasła konfiguracyjnego. Hasło to zapobiega nieautoryzowanemu dostępowi do programu Computer Setup.



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 naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

3. Wybierz kolejno **Security (Zabezpieczenia) > Smart Cover (Pokrywa inteligentna) > Cover Lock (Blokada pokrywy) > Lock (Zablokuj)**.
4. Przed wyjściem 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 naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

3. Wybierz kolejno **Security (Zabezpieczenia) > Smart Cover (Pokrywa inteligentna) > Cover Lock (Blokada pokrywy) > Unlock (Odblokuj)**.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

## Używanie klucza Smart Cover FailSafe Key

Jeżeli włączona jest blokada Smart Cover Lock i z różnych powodów nie można wprowadzić wyłączającego ją hasła konfiguracyjnego, pokrywę 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.



**PRZESTROGA:** Klucz Smart Cover FailSafe Key jest specjalistycznym narzędziem dostępnym w firmie HP. Ze względu na duże prawdopodobieństwo wystąpienia wymienionych wyżej sytuacji, klucz taki najlepiej zamówić odpowiednio wcześniej u autoryzowanego sprzedawcy lub serwisanta.

---

Aby nabyć klucz FailSafe Key, należy:

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

Więcej informacji dotyczących korzystania z klucza Smart Cover FailSafe Key można znaleźć w *Instrukcji obsługi sprzętu* na dysku CD *Documentation*.

## Zabezpieczenie głównego rekordu rozruchowego

Główny rekord rozruchowy (Master Boot Record, MBR) zawiera informacje wymagane do pomyślnego uruchomienia systemu z dysku i uzyskania dostępu do danych przechowywanych na tym dysku. Funkcja zabezpieczenia głównego rekordu rozruchowego wykrywa i raportuje wprowadzone przypadkowo lub złośliwie zmiany tego rekordu (np. spowodowane działaniem wirusów lub niewłaściwym wykorzystaniem narzędziowych programów dyskowych). Możliwe jest również odtworzenie tej wersji rekordu, przy której nastąpiło ostatnie poprawne uruchomienie systemu.

Aby włączyć zabezpieczenie głównego rekordu rozruchowego, wykonaj następujące czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie**.
2. Zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

3. Wybierz kolejno **Security (Zabezpieczenia) > Master Boot Record Security (Zabezpieczenie głównego rekordu rozruchowego) > Enabled (Włączone)**.
4. Wybierz kolejno **Security (Zabezpieczenia) > Save Master Boot Record (Zapisz główny rekord rozruchowy)**.
5. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

Po włączeniu zabezpieczenia głównego rekordu rozruchowego system BIOS uniemożliwia wprowadzenie zmian w tym rekordzie na bieżącym dysku rozruchowym w trybie MS-DOS lub w trybie awaryjnym systemu Windows.





Większość systemów operacyjnych umożliwia dostęp do głównego rekordu rozruchowego na bieżącym dysku rozruchowym. W przypadku korzystania z jednego z takich systemów BIOS nie jest w stanie przeciwdziałać wprowadzaniu zmian w tym rekordzie.

---

Przy każdym włączaniu lub ponownym uruchamianiu komputera główny rekord rozruchowy dysku rozruchowego jest porównywany z poprzednio zapisanymi ustawieniami MBR. Jeżeli wykryte zostaną zmiany, a poprzednio zapisany główny rekord rozruchowy należał do bieżącego dysku rozruchowego, wyświetlany jest następujący komunikat:

1999—Master Boot Record has changed.

Press any key to enter Setup to configure MBR Security.

Po uruchomieniu programu Computer Setup należy:

- zapisać główny rekord rozruchowy bieżącego dysku rozruchowego,
- odtworzyć zapisany poprzednio główny rekord rozruchowy LUB
- wyłączyć zabezpieczenie rekordu MBR.

Do wykonania tych czynności niezbędne jest wprowadzenie hasła konfiguracyjnego (jeżeli zostało ono ustawione).

Jeżeli wykryte zostaną zmiany, a poprzednio zapisany główny rekord rozruchowy **nie** należał do bieżącego dysku rozruchowego, wyświetlany jest następujący komunikat:

2000—Master Boot Record Hard Drive has changed.

Press any key to enter Setup to configure MBR Security.

Po uruchomieniu programu Computer Setup należy:

- zapisać główny rekord rozruchowy bieżącego dysku rozruchowego LUB
- wyłączyć zabezpieczenie rekordu MBR.

Do wykonania tych czynności niezbędne jest wprowadzenie hasła konfiguracyjnego (jeżeli zostało ono ustawione).

Jeżeli poprzednio zapisany główny rekord rozruchowy został uszkodzony (choć zdarza się to bardzo rzadko), wyświetlany jest następujący komunikat:

1998—Master Boot Record has been lost.

Press any key to enter Setup to configure MBR Security.

Po uruchomieniu programu Computer Setup należy:

- zapisać główny rekord rozruchowy bieżącego dysku rozruchowego LUB
- wyłączyć zabezpieczenie rekordu MBR.

Do wykonania tych czynności niezbędne jest wprowadzenie hasła konfiguracyjnego (jeżeli zostało ono ustawione).

## **Czynności wykonywane przed partycjonowaniem lub formatowaniem bieżącego dysku rozruchowego**

Przed partycjonowaniem lub formatowaniem bieżącego dysku rozruchowego należy wyłączyć funkcję zabezpieczenia rekordu MBR. Główny rekord rozruchowy może być aktualizowany przez niektóre dyskowe programy narzędziowe (np. FDISK lub FORMAT). Jeżeli zabezpieczenie rekordu MBR pozostanie włączone, podczas partycjonowania lub formatowania dysku mogą pojawić się komunikaty o błędach wykrytych przez wymienione programy narzędziowe, a po ponownym uruchomieniu komputera może także zostać wyświetlone ostrzeżenie związane z zabezpieczeniem. Aby wyłączyć zabezpieczenie głównego rekordu rozruchowego, wykonaj następujące czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie**.
2. Zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, aż otworzy się program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu i przytrzymaniu klawisza **F10**.

Jeżeli używana jest klawiatura PS/2, może się pojawić komunikat o błędzie klawiatury — należy go zignorować.

---

3. Wybierz kolejno **Security (Zabezpieczenia) > Master Boot Record Security (Zabezpieczenie głównego rekordu rozruchowego) > Disabled (Wyłączone)**.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

## Zabezpieczająca blokada kablowa

Z tyłu komputera znajduje się gniazdo blokady kablowej, umożliwiające przymocowanie komputera do nieruchomego obiektu przy stanowisku pracy.

Szczegółowe instrukcje (wraz z rysunkami) można znaleźć w *Instrukcji obsługi sprzętu* na dysku CD *Documentation*.

## 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.

---



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

---

Więcej informacji można znaleźć na stronie:

<http://h18004.www1.hp.com/products/security/>.

## 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 obniża ryzyko utraty istotnych danych oraz wystąpienia nieplanowanych przestołów 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 wybranych typach komputerów osobistych 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. Informacje dotyczące używania systemu DPS znajdują się w *Podręczniku rozwiązywania problemów* na dysku CD *Documentation*.

## 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 2000 V.

## Czujnik termiczny

Czujnik termiczny, łącząc w sobie funkcje programowe i sprzętowe, jest urządzeniem rejestrującym temperaturę wewnątrz komputera. W momencie przekroczenia dopuszczalnej temperatury wyświetlany jest odpowiedni komunikat. Dzięki odpowiednio wczesnemu ostrzeżeniu użytkownik może podjąć odpowiednie kroki, które zapobiegą uszkodzeniu komputera i utracie danych.

## A

adresy internetowe, zobacz  
    witryny sieci Web  
adresy URL (witryny sieci Web), zobacz  
    witryny sieci Web  
Altiris 5

## B

bezpieczny blok uruchamiania  
    pamięci ROM 10  
blokada Smart Cover Lock, włączanie 42

## C

Computer Setup 12  
cover lock, smart 41  
czujnik termiczny 49

## D

DiskOnKey  
    *zobacz też* HP Drive Key  
    rozruchowe 16 — 22  
dostęp do komputera, kontrolowanie 25  
dostosowywanie oprogramowania 2  
Drivelock 37 — 39  
dwufunkcyjny przycisk zasilania 23  
dysk rozruchowy, ważne informacje 46  
dysk, klonowanie 2  
dysk, ochrona 48  
dyski twarde, narzędzie diagnostyczne 48

## F

FailSafe Key  
    przestrogi 43  
    zamawianie 43  
formatowanie dysku, ważne informacje 46

## H

hasło 36  
    konfiguracyjne 31, 33  
    uruchomieniowe 32  
    usuwanie 35  
    zabezpieczenie 30  
    zmiana 34  
hasło konfiguracyjne  
    ustawianie 31  
    usuwanie 35  
    wprowadzanie 33  
    zmiana 34  
hasło uruchomieniowe  
    usuwanie 35  
    wprowadzanie 32  
    zmiana 34  
HP Client Manager 4  
HP Drive Key  
    *zobacz też* DiskOnKey  
    rozruchowe 16 — 22

## I

identyfikacja na podstawie analizy linii  
    papilarnych 47

## K

klucz Smart Cover FailSafe Key,  
    zamawianie 43  
konfiguracja  
    replikowanie 12  
konfigurowanie  
    początkowe 2  
konfigurowanie przycisku zasilania 23  
kontrolowanie dostępu do komputera 25

## **N**

narzędzia klonowania, oprogramowanie 2  
 narzędzia rozmieszczania,  
     oprogramowanie 2  
 narzędzie diagnostyczne dla dysków  
     twardych 48  
 nieprawidłowa systemowa pamięć ROM 9

## **O**

ochrona dysku twardego 48  
 odzyskiwanie systemu 9  
 odzyskiwanie, oprogramowanie 2  
 oprogramowanie 25  
     aktualizowanie na wielu komputerach 6  
     bezpieczny blok uruchamiania pamięci  
         ROM 10  
     Computer Setup 12  
     Drive Protection System 48  
     integracja 2  
     odzyskiwanie 2  
     powiadamianie o usterkach i ich  
         usuwanie 48  
     System Software Manager 6  
     zabezpieczenie głównego rekordu  
         rozruchowego 44 — 46  
     zdalne instalowanie systemu 3  
     zdalne zarządzanie pamięcią ROM  
         typu flash 8

## **P**

pamięć ROM  
     nieprawidłowa 9  
     wskaźniki klawiatury, tabela 11  
 partycjonowanie dysku, ważne  
     informacje 46  
 PCN (Proactive Change Notification) 7  
 początkowa konfiguracja 2  
 powiadamianie o usterkach 48

powiadomienia o zmianach 7  
 powiadomienie o zmianie 7  
 Preboot Execution Environment (PXE) 3  
 preinstalowany obraz oprogramowania 2  
 Proactive Change Notification (PCN) 7  
 przestrogi  
     FailSafe Key 43  
     zabezpieczanie pamięci ROM 8  
     zabezpieczenie blokady Smart  
         Cover Lock 41  
 przycisk zasilania  
     dwufunkcyjny 23  
     konfigurowanie 23  
 PXE (Preboot Execution Environment) 3

## **R**

ROM  
     Zdalne zarządzanie pamięcią typu flash 8  
 ROM, uaktualnianie 8

## **S**

separatory klawiatury, narodowe 36  
 separatory różnych klawiatur 36  
 separatory, tabela 36  
 Smart Cover Lock 41 — 43  
     wyłączanie 42  
 Smart Cover Sensor 39  
     poziomy zabezpieczeń 40  
     ustawianie 41  
 SSM (System Software Manager) 6  
 System Software Manager (SSM) 6  
 system, odzyskiwanie 9  
 systemy operacyjne, ważne informacje 24

## **Ś**

śledzenie zasobów 25

## **T**

temperatura wewnętrzna komputera 49

**U**

- uaktualnianie pamięci ROM 8
- urządzenie rozruchowe
  - DiskOnKey 16 — 22
  - HP Drive Key 16 — 22
  - tworzenie 16 — 22
  - urządzenie USB typu flash 16 — 22
- urządzenie USB typu flash,
  - rozruchowe 16 — 22
- usuwanie 36
- usuwanie haseł 36
- usuwanie hasła 35

**W**

- wewnętrzna temperatura komputera 49
- witryny sieci Web
  - Altiris 5, 6
  - HP Client Manager 4
  - HPQFlash 9
- identyfikacja na podstawie analizy linii papilarnych 47
- obsługa oprogramowania 24
- pamięć ROM typu flash 8
- pliki ROMPaq 8
- Proactive Change Notification 7
- replikowanie ustawień
  - konfiguracyjnych 15, 16
- rozmieszczanie komputera 2
- Subscriber's Choice 7
- System Software Manager (SSM) 6
- zdalne zarządzanie pamięcią ROM typu flash 8
- włączanie blokady Smart Cover Lock 42
- wprowadzanie
  - hasło konfiguracyjne 33
  - hasło uruchomieniowe 32

- wskaźniki klawiatury, pamięć ROM,
  - tabela 11
- wyłączanie blokady Smart Cover Lock 42

**Z**

- zabezpieczająca blokada kablowa 47
- zabezpieczanie Multibay 37 — 39
- zabezpieczanie pamięci ROM, przestroga 8
- zabezpieczenia
  - DriveLock 37 — 39
  - funkcje, tabela 26
  - główny rekord rozruchowy 44 — 46
  - MultiBay 37 — 39
  - Smart Cover Lock 41 — 43
  - Smart Cover Sensor 39
  - ustawienia, konfigurowanie 25
- zabezpieczenie
  - hasłem 30
- zabezpieczenie antyprzebieciowe,
  - zasilacz 49
- zabezpieczenie blokady Smart Cover Lock,
  - przestroga 41
- zabezpieczenie głównego rekordu rozruchowego 44 — 46
- zamawianie klucza FailSafe Key 43
- zasilacz, z zabezpieczeniem antyprzebieciowym 49
- zdalna instalacja 3
- zdalne instalowanie systemu, dostęp 3
- zdalne zarządzanie pamięcią ROM typu flash 8
- zmiana hasła 34
- zmiana systemów operacyjnych, ważne informacje 24