

Ghid de gestionare a computerului

PC-uri comerciale

© Copyright 2008 Hewlett-Packard
Development Company, L.P. Informațiile
conținute în acest document pot fi modificate
fără înștiințare prealabilă.

Microsoft, Windows și Windows Vista sunt fie
mărci comerciale, fie mărci comerciale
înregistrate ale Microsoft Corporation în
Statele Unite și/sau în alte țări.

Intel și vPro sunt mărci comerciale ale Intel
Corporation din S.U.A. și din alte țări.

Singurele garanții pentru produsele și
serviciile HP sunt cele stabilite expres prin
certIFICATELE DE GARANȚIE care însoțesc aceste
produse și servicii. Nimic din acest document
nu trebuie interpretat ca o garanție
suplimentară. HP nu este răspunzător pentru
nici o eroare sau omisiune tehnică sau
editorială din acest document.

Acest document conține informații patentate
care sunt protejate prin drepturile de autor.
Nici o parte din acest document nu se poate
fotocopia, reproduce sau traduce în altă
limbă fără obținerea în prealabil a acordului
scris al Hewlett-Packard Company.

Ghid de gestionare a computerului

PC-uri comerciale

Ediția a treia (iulie 2008)

Cod document: 451272-273

Despre acest manual

Acest ghid furnizează definiții și instrucțiuni pentru utilizarea caracteristicilor de securitate și de gestionare care sunt instalate în prealabil pe unele modele.

- △ **AVERTISMENT!** Textul evidențiat în această manieră indică faptul că nerespectarea instrucțiunilor poate avea ca rezultat rănirea fizică sau pierderea vieții.
- △ **ATENȚIE:** Textul evidențiat în această manieră indică faptul că nerespectarea instrucțiunilor poate avea ca rezultat deteriorarea echipamentului sau pierderea de informații.
- 📝 **NOTĂ:** Textul evidențiat în această manieră furnizează informații suplimentare importante.

Cuprins

1 Prezentare generală a modurilor de gestionare a computerului

2 Configurația inițială și desfășurarea

HP Software Agent (Agent software HP)	3
Agentul soluției de desfășurare Altiris	3

3 Remote System Installation (Instalarea de la distanță a sistemului)

4 Actualizarea și gestionarea software-ului

HP Client Management Interface	5
HP SoftPaq Download Manager	6
HP System Software Manager	7
HP ProtectTools Security Manager	7
HP Client Automation, edițiile Starter și Standard	8
HP Client Automation, ediția Enterprise	8
HP Client Manager from Symantec	9
Altiris Client Management Suite	10
HP Client Catalog pentru produse Microsoft System Center & SMS	10
HP Backup and Recovery Manager	11
Tehnologia de gestionare	12
Verdiem Surveyor	14
HP Proactive Change Notification	14
Subscriber's Choice (Opțiunea abonatului)	14
Soluții retrase	14

5 Actualizare ROM

Actualizarea de la distanță a memoriei ROM	15
HPQFlash	15

6 Boot Block Emergency Recovery Mode (Mod de recuperare de urgență a blocului de încărcare)

7 Multiplicarea instalării

Copierea pe un singur computer	18
--------------------------------------	----

Copierea pe mai multe computere	19
Crearea unui dispozitiv de încărcare	20
Dispozitive de memorie flash USB acceptate	20
Dispozitive de memorie flash USB neacceptate	21

8 Buton de alimentare cu două stări

9 Asistență la site-ul Web HP

10 Standarde în domeniu

11 Urmărirea și securitatea activelor

Securitate prin parole	30
Stabilirea unei parole de setare prin intermediul utilitarului Computer Setup	30
Stabilirea unei parole de pornire prin utilitarul Computer Setup	30
Introducerea unei parole de pornire	31
Introducerea unei parole de setare	31
Modificarea unei parole de pornire sau de setare	32
Ștergerea unei parole de pornire sau de setare	32
Caractere de delimitare pentru tastaturile naționale	33
Ștergerea parolelor	33
DriveLock (Blocare unitate)	33
Utilizarea DriveLock	34
Aplicații DriveLock	34
Smart Cover Sensor (Senzor capac inteligent)	35
Setarea nivelului de protecție pentru Smart Cover Sensor (Senzor capac inteligent)	35
Smart Cover Lock (Zăvor capac inteligent)	35
Blocarea dispozitivului Smart Cover Lock (Zăvor capac inteligent)	36
Deblocarea dispozitivului Smart Cover Lock (Zăvor capac inteligent)	36
Utilizarea cheii Smart Cover FailSafe	36
Disponibilitate pentru dispozitiv de blocare cu cablu	37
Tehnologie de identificare a amprentelor	37
Notificarea și remedierea defectelor	37
Drive Protection System (Sistem de protecție a unităților)	37
Sursa de alimentare cu toleranță la supratensiune	38
Senzor termic	38


Index	39
--------------------	-----------

1 Prezentare generală a modurilor de gestionare a computerului

HP Client Management Solutions (Soluții HP de gestionare a sistemelor client) furnizează soluții bazate pe standarde pentru gestionarea și controlul computerelor de birou, stațiilor de lucru și PC-urilor portabile într-un mediu de rețea. HP a introdus în 1995 caracteristica de gestionare a computerelor de birou, odată cu realizarea primelor computere personale de birou cu gestionare completă. HP este un deținător de patent pentru tehnologia de gestionare. De atunci, HP a condus o importantă inițiativă în întreaga industrie pentru a dezvolta standardele și infrastructura necesare pentru a desfășura, a configura și a gestiona computere de birou, stații de lucru și PC-uri portabile. HP își dezvoltă propriul software de gestionare și colaborează îndeaproape cu cei mai importanți furnizori în domeniu de soluții software de gestionare, pentru a asigura compatibilitatea dintre soluțiile HP de gestionare a sistemelor client și produsele acestora. Soluțiile HP de gestionare a sistemelor client reprezintă un aspect important al preocupărilor noastre extinse de a vă furniza soluții care să vă ajute să reduceți costul total de proprietate și costurile de întreținere ale PC-urilor, pe întreaga lor durată de viață.

Posibilitățile și caracteristicile esențiale ale gestionării computerelor de birou sunt:

- Configurația inițială și desfășurarea
- Remote System Installation (Instalarea de la distanță a sistemului)
- Actualizarea și gestionarea software-ului
- Actualizarea memoriei ROM
- Configurarea opțiunilor pentru hardware
- Urmărirea și securitatea activelor
- Notificarea și remedierea defectelor

 **NOTĂ:** Suportul tehnic pentru anumite caracteristici descrise în acest ghid poate să difere în funcție de model sau de versiunea de software.

2 Configurația inițială și desfășurarea

Computerul este livrat cu o imagine a software-ului de sistem instalată în prealabil. După un proces scurt de „despachetare” a software-ului, computerul este gata de utilizare.

Dacă preferați, imaginea software instalată în prealabil poate să fie înlocuită cu un set particularizat de software de sistem și de aplicații. Există câteva metode pentru desfășurarea unei imagini software particularizate. Acestea includ:

- Instalarea de aplicații software suplimentare după despachetarea imaginii software instalate în prealabil.
- Utilizarea instrumentelor de desfășurare a software-ului, precum HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (bazat pe tehnologia Radia) sau Altiris Deployment Solution, pentru a înlocui software-ul preinstalat cu o imagine software particularizată.
- Utilizarea unui proces de clonare a discului pentru a copia conținutul unei unități de disc pe alta.

Cea mai bună metodă de desfășurare depinde de mediul și procesele IT de care dispuneți.

Sistemul HP Backup and Recovery, ROM-Based Setup și hardware-ul ACPI oferă asistență suplimentară privind recuperarea software-ului de sistem, gestionarea și depanarea configurației și gestionarea energiei.

 **NOTĂ:** Consultați [HP Backup and Recovery Manager, la pagina 11](#) pentru informații despre crearea unui set de discuri de recuperare.

HP Software Agent (Agent software HP)

Pe computer este încărcat în prealabil agentul de gestionare utilizat de ambele ediții ale HP Client Automation, Standard și Enterprise. Când este instalat, el activează comunicarea cu consola de gestionare HP.

Pentru a instala HP Software Agent (Agent software HP):

1. Faceți clic pe **Start**.
2. Faceți clic pe **Toate programele**.
3. Faceți clic pe **HP Manageability** (Maniabilitate HP).
4. Faceți clic pe **Radia Management Agent Readme** (Fișier Readme pentru agentul de gestionare Radia).
5. Citiți și urmați instrucțiunile cuprinse în fișierul Readme pentru a instala HP Software Agent (Agent software HP).

Agentul HP Software este o componentă esențială de infrastructură pentru activarea tuturor soluțiilor HP Client Automation. Pentru a afla mai multe despre alte componente de infrastructură necesare pentru implementarea soluțiilor HP de gestionare a configurației, vizitați <http://h20229.www2.hp.com/solutions/ascm/index.html>.

Agentul soluției de desfășurare Altiris

Acest program este încărcat în prealabil pe computer. Când este instalat, el activează comunicarea cu consola administratorului soluției de desfășurare.

Pentru a instala agentul soluției de desfășurare Altiris:

1. Faceți clic pe **Start**.
2. Faceți clic pe **Toate programele**.
3. Pentru Windows Vista, faceți clic pe **Install Altiris DAgent** (Instalare Altiris DAgent). Pentru Windows XP, faceți clic pe **Install Altiris AClient** (Instalare Altiris AClient).
4. Pentru a instala și a configura clientul Altiris, urmați instrucțiunile de pe ecran.

Acest agent este o componentă esențială de infrastructură pentru a activa Altiris Deployment Solution, care este o componentă din Altiris Client Management Suite. Pentru a afla mai multe despre alte componente de infrastructură necesare pentru implementarea Altiris Client Management Suite, vizitați <http://www.hp.com/go/easydeploy>.

3 Remote System Installation (Instalarea de la distanță a sistemului)

Remote System Installation vă permite să porniți și să configurați sistemul utilizând software-ul și informațiile de configurare situate pe un server din rețea prin inițierea Preboot Execution Environment (PXE). Caracteristica Remote System Installation se utilizează de obicei ca instrument de instalare și configurare a sistemului și se poate utiliza pentru următoarele activități:

- Formatarea unei unități de disc
- Desfășurarea unei imagini software pe unul sau mai multe PC-uri noi
- Actualizarea de la distanță a componentei BIOS a sistemului din memoria flash ROM ([Actualizarea de la distanță a memoriei ROM, la pagina 15](#))
- Configurarea setărilor componentei BIOS a sistemului

Pentru a iniția Remote System Installation (Instalarea de la distanță a sistemului), apăsați **F12** când apare mesajul **F12 = Network Service Boot** (Încărcare sistem prin servicii de rețea) în colțul din dreapta jos al ecranului cu sigla HP, în timpul încărcării sistemului în computer. Urmați instrucțiunile de pe ecran pentru a continua procesul. Ordinea implicită de încărcare a sistemului este o setare a configurației BIOS care se poate modifica pentru a încerca întotdeauna să încarce mediul PXE.

4 Actualizarea și gestionarea software-ului

HP furnizează câteva instrumente pentru gestionarea și actualizarea software-ului de pe computere de birou, stații de lucru și computere portabile:

- HP Client Management Interface (Interfață de gestionare client HP)
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation, edițiile Starter, Standard și Enterprise
- HP Client Manager from Symantec
- Altiris Client Management Suite (Suită de gestionare a clientului Altiris)
- HP Client Catalog pentru produse Microsoft System Center & SMS
- HP Backup and Recovery Manager
- PC-uri marcate Intel vPro cu tehnologie de gestionare activă
- Verdiem Surveyor (Supraveghetor Verdiem)
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

Indiferent de instrumentele de gestionare a sistemelor pe care le utilizează departamentul dvs. IT, gestionarea activelor hardware și software este importantă pentru a menține costurile IT scăzute și performanțele ridicate ale activității. Administratorul IT poate să acceseze interfața pentru gestionarea sistemelor client prin scrierea unor scripturi simple și integrarea acelor scripturi în soluția de gestionare aleasă.

Cu HP Client Management Interface (HP CMI), noile computere HP pentru afaceri se integrează nemijlocit în mediul IT gestionat. HP CMI oferă o interfață care simplifică integrarea computerelor HP pentru afaceri cu instrumente populare de gestionare a sistemelor industriale (inclusiv Microsoft Systems Management Server, IBM Tivoli Software și HP Operations) și aplicații de gestionare particularizate dezvoltate local. Utilizând HP CMI, instrumentele și aplicațiile de gestionare a sistemelor pot să necesite un inventar amănunțit al clientului, să primească informații despre starea de sănătate

și să gestioneze setările de sistem BIOS prin comunicarea directă cu computerul client, reducând necesitatea pentru software-ul agent sau conector pentru a obține integrarea.

HP CMI se bazează pe standarde în domeniu care includ MS WMI (Microsoft Windows Management Interface – Interfață de gestionare Microsoft Windows), WBEM (Web-Based Enterprise Management – Management de întreprindere bazat pe Web), SMBIOS (System Management BIOS – BIOS cu gestionare a sistemului) și ACPI (Advanced Configuration and Power Interface – Interfață complexă pentru configurare și alimentare). HP CMI este o tehnologie de bază utilizată în soluțiile HP de gestionare a sistemelor client. Prin HP CMI, HP vă oferă flexibilitate în alegerea modului în care gestionați computerele client HP.

HP CMI, utilizată împreună cu un software de gestionare a sistemului, are următoarele posibilități:

- Solicită informații amănunțite despre inventarul sistemelor client – Obțineți informații detaliate despre procesoare, unități de disc, memorie, BIOS, drivere, inclusiv informații despre senzori (viteza ventilatorului, tensiunea și temperatura).
- Primește informații despre starea de sănătate – Vă abonați la o gamă largă de avertizări referitoare la hardware-ul sistemelor client (precum depășirea temperaturii, blocarea ventilatorului sau modificarea configurației hardware), care pot fi trimise către consola de gestionare a sistemului, către o aplicație sau către un computer client local. Avertizările se trimit în timp real, atunci când sunt declanșate de evenimentele hardware.
- Gestionează setările BIOS ale sistemelor – Efectuați de la distanță funcții F10, inclusiv setarea și schimbarea parolelor de BIOS sau a ordinii de încărcare a computerului, de la consola de gestionare a sistemului, la unul sau la toate sistemele client, fără să fie necesar să vizitați fiecare aparat.

Pentru informații suplimentare despre HP CMI, vizitați <http://www.hp.com/go/hpcmi/>.

HP SoftPaq Download Manager


HP SoftPaq Download Manager este o interfață gratuită, ușor de utilizat, pentru localizarea și descărcarea actualizărilor de software ale clientului HP pentru modelele PC din mediul dvs. Specificându-vă modelele, sistemul de operare și limba, aveți posibilitatea să localizați, să sortați și să selectați pachetele de software necesare. Pentru a descărca HP SoftPaq Download Manager, vizitați <http://www.hp.com/go/sdm>.

HP System Software Manager

HP System Software Manager (SSM) este un utilitar gratuit care automatizează desfășurarea la distanță a driverelor de dispozitive și a actualizărilor de BIOS pentru PC-urile comerciale legate în rețea. Când SSM se execută, determină (fără intervenția utilizatorului) nivelurile de revizuire ale driverelor și ale BIOS-ului instalate pe fiecare sistem client din rețea și compară acest inventar cu pachetele SoftPaq de software de sistem care au fost testate și stocate într-un depozit central de fișiere. SSM actualizează apoi automat toate revizuirile mai vechi ale software-ului de sistem de pe PC-urile din rețea la cele mai recente niveluri disponibile în depozitul de fișiere. Deoarece SSM permite distribuirea de actualizări de pachete SoftPaq numai către modelele corecte de sisteme client, administratorii pot să utilizeze cu încredere și eficiență SSM pentru a menține software-ul de sistem actualizat.

System Software Manager se integrează cu instrumentele de distribuire a software-ului la nivel de întreprindere precum soluțiile HP Client Automation, HP Client Manager from Symantec și Microsoft Systems Management Server (SMS). Utilizând SSM, aveți posibilitatea să distribuiți actualizări create de client sau de alți furnizori, care au fost împachetate în format SSM.

SSM se poate descărca gratuit, vizitând <http://www.hp.com/go/ssm>.

 **NOTĂ:** SSM nu acceptă în prezent actualizarea ROM de la distanță pe sistemele la care este activat Windows Vista BitLocker și care utilizează măsurători TPM pentru a proteja cheile BitLocker, deoarece prin actualizarea BIOS-ului s-ar invalida semnătura de încredere pe care a creat-o BitLocker pentru platformă. Dezactivați BitLocker prin politica de grup pentru a actualiza BIOS-ul sistemului.

Puteți să activați suportul BitLocker fără măsurători TPM ale BIOS-ului pentru a evita invalidarea cheilor BitLocker. HP recomandă să păstrați o copie sigură a elementelor de acreditare BitLocker pentru situații în care este necesară o recuperare urgentă.

HP ProtectTools Security Manager

Software-ul HP ProtectTools Security Manager (Manager de securitate HP ProtectTools) furnizează caracteristici de securitate care vă ajută să vă protejați împotriva accesului neautorizat la computer, la rețele și la datele critice. Funcționalitatea de securitate îmbunătățită este furnizată de următoarele module software:

- Credential Manager for HP ProtectTools (Manager acreditări pentru HP ProtectTools)
- Embedded Security for HP ProtectTools (Securitate încorporată pentru HP ProtectTools)
- Java Card Security for HP ProtectTools (Securitate card Java pentru HP ProtectTools)
- BIOS Configuration for HP ProtectTools (Configurație BIOS pentru HP ProtectTools)
- Drive Encryption for HP ProtectTools (Criptare unități pentru HP ProtectTools)
- Device Access Manager for HP ProtectTools (Manager de acces la dispozitiv pentru HP ProtectTools)
- HP ProtectTools Security Manager
- Privacy Manager for HP ProtectTools

Modulele software disponibile pentru computerul dvs. pot fi diferite, în funcție de model. De exemplu, Embedded Security for HP ProtectTools (Securitate încorporată pentru HP ProtectTools) este disponibil numai pentru computere pe care este instalat cipul de securitate încorporat TPM (Trusted Platform Module).

Modulele software HP ProtectTools pot fi preinstalate, încărcate în prealabil sau disponibile pentru descărcare de pe site-ul Web HP. Pentru anumite computere de birou HP Compaq, HP ProtectTools este disponibil ca opțiune achiziționată ulterior cumpărării. Pentru informații suplimentare, vizitați <http://www.hp.com/products/security>.

HP Client Automation, edițiile Starter și Standard

HP Client Automation este o soluție de gestionare a hardware-ului și software-ului pentru medii Windows Vista, Windows XP și HP Thin Client, este simplu de utilizat și rapid de desfășurat și asigură o bază puternică pentru cerințele viitoare. Este oferită în două ediții:

- Ediția Starter este un produs gratuit pentru gestionarea computerelor de birou, portabile și stațiilor de lucru HP, asigurând inventarul de hardware și software, comanda de la distanță, monitorizarea alertelor HP, actualizări pentru BIOS și pentru drivere HP, integrarea cu HP Protect Tools și suport suplimentar pentru Intel AMT. De asemenea, ediția Starter acceptă desfășurarea și gestionarea sistemelor HP Thin Client.
- Ediția Standard, disponibilă pentru cumpărare, include întreaga funcționalitate asigurată de ediția Starter și are în plus: desfășurare și migrare pentru sisteme Windows, posibilități de gestionare a corecțiilor, distribuție de software și măsurare a utilizării software-ului.

HP Client Automation prin edițiile Starter și Standard oferă o cale de migrare la ediția Enterprise a HP Client Automation (bazată pe tehnologia Radia) pentru gestionarea automatizată a mediilor IT mari, eterogene și în continuă schimbare.

Pentru informații suplimentare despre soluțiile HP Client Automation, vizitați <http://www.hp.com/go/client>.

HP Client Automation, ediția Enterprise

HP Client Automation, ediția Enterprise, este o soluție bazată pe politică, ce permite administratorilor să inventarieze, să desfășoare, să aplice corecții și să gestioneze în mod continuu software și conținut pe platforme client eterogene. Cu HP Client Automation ediția Enterprise, specialistul IT poate:

- Să automatizeze procesul de gestionare pe întregul ciclu de viață, începând de la descoperire, desfășurare și gestionare continuă până la migrare și scoatere din funcțiune
- Să desfășoare automat și să gestioneze continuu un întreg pachet de software (sisteme de operare, aplicații, corecții, setări și conținut) pentru a obține starea dorită
- Să gestioneze software realmente pe orice dispozitiv, inclusiv computere de birou și portabile și stații de lucru, într-o infrastructură eterogenă sau de sine stătătoare
- Să gestioneze software pe majoritatea sistemelor de operare

Având la dispoziție un sistem de gestiune continuă a configurației, clienții HP raportează economii importante ale costurilor IT, un timp accelerat de plasare pe piață a software-ului și conținutului, o mai mare productivitate și o satisfacție crescută a utilizatorilor.

Pentru informații suplimentare despre soluțiile HP Client Automation, vizitați <http://www.hp.com/go/client>.

HP Client Manager from Symantec

HP Client Manager from Symantec, dezvoltat cu Altiris, este disponibil gratuit pentru toate modelele HP de calculatoare de birou, calculatoare portabile și stații de lucru acceptate. SSM are integrare în HP Client Manager și permite urmărirea, monitorizarea și gestionarea la nivel central a aspectelor hardware ale sistemelor client HP.

Utilizați HP Client Manager from Symantec pentru:

- Obținerea de informații valoroase despre hardware, precum CPU, memorie, video și setări de securitate
- Monitorizarea stării de sănătate a sistemului pentru a rezolva problemele înainte să apară
- Obținerea și instalarea automată a actualizărilor de drivere și BIOS, fără vizitarea fiecărui PC
- Configurarea de la distanță a setărilor BIOS și de securitate
- Automatizarea proceselor pentru rezolvarea mai rapidă a problemelor hardware

Integrarea strânsă cu instrumentele HP Instant Support reduce timpul de depanare hardware.

- Diagnosticarea – executați de la distanță și vizualizați rapoarte despre modelele HP de calculatoare de birou, portabile sau stații de lucru
- Scanarea stării de sănătate a sistemului – căutați probleme hardware cunoscute în baza instalată de sisteme client HP
- Chat activ – vă conectați la asistența pentru clienți HP pentru a rezolva problemele
- Baza de cunoștințe HP – legătură către informații oferite de experți
- Proces automat de colectare și livrare de pachete SoftPaq, pentru o rezolvare rapidă a problemelor hardware
- Identificarea, inventarierea și inițializarea sistemelor cu ajutorul cipului de securitate încorporat HP ProtectTools
- Posibilitatea de a afișa local, pe sistemul client, avertizări despre starea de sănătate
- Raportarea informațiilor de inventariere de bază pentru sistemele client non-HP
- Instalarea și configurarea cipului de securitate TPM
- Programarea centralizată a copierii de rezervă și recuperării aplicațiilor client
- Suport suplimentar pentru gestionare Intel AMT

Pentru informații suplimentare despre HP Client Manager from Symantec, vizitați <http://www.hp.com/go/clientmanager>.

Altiris Client Management Suite

Altiris Client Management Suite (Suită de gestionare a clientului Altiris) este o soluție simplu de utilizat pentru gestionarea pe întregul ciclu de viață a software-ului pentru computere de birou, computere portabile și stații de lucru. Client Management Suite Level 1 (Suită de gestionare a clientului, nivel 1) include următoarele produse Altiris:

- Inventory Solution (Soluție de inventar)
- Deployment Solution (Soluție de desfășurare)
- Software Delivery Solution (Soluție de livrare software)
- Patch Management Solution (Soluție de gestionare a corecțiilor)
- Application Metering Solution (Soluție de măsurare a aplicațiilor)
- Application Management Solution (Soluție de gestionare a aplicațiilor)
- Carbon Copy Solution (Soluție copiere indigo)

Pentru informații suplimentare despre Altiris Client Management Suite, vizitați <http://www.altiris.com/Products/ClientManagementSuite.aspx>.

HP Client Catalog pentru produse Microsoft System Center & SMS

HP Client Catalog permite specialiștilor IT care utilizează produse Microsoft să automatizeze desfășurarea actualizărilor software de la HP (SoftPak) pe PC-uri de birou HP. Fișierul catalog conține informații detaliate despre platformă privind computerele de birou și mobile, precum și pentru stațiile de lucru HP. Se poate utiliza împreună cu caracteristicile particularizate pentru inventar și caracteristici de actualizare ale produselor Microsoft pentru a oferi actualizări automatizate la drivere și corecții pentru computerele client HP gestionate.

Produsele Microsoft acceptate de HP Client Catalog includ:

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

Pentru informații suplimentare despre HP Client Catalog for SMS, vizitați <http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html>.

HP Backup and Recovery Manager

HP Backup and Recovery Manager este o aplicație multilaterală, ușor de utilizat, care vă permite să efectuați copierea de rezervă și recuperarea conținutului unității de disc principale a PC-ului. Aplicația lucrează în sistemul de operare Windows pentru a crea copii de rezervă ale sistemului Windows, ale tuturor aplicațiilor și fișierelor de date. Copiile de rezervă pot fi programate să se realizeze automat la intervale de timp bine stabilite sau pot fi inițiate manual. Fișierele importante pot fi arhivate separat de copiile de rezervă obișnuite.

HP Backup and Recovery Manager este preinstalat pe unitatea C: și creează o partiție de recuperare.


Copiile de rezervă ale punctelor de recuperare și ale fișierelor se pot face pe discul CD sau DVD, în timp ce toate copiile de rezervă pot fi realizate în rețea sau pe unitățile de disc secundare.

HP vă recomandă în mod special să creați imediat un set de discuri de recuperare, înainte să utilizați computerul și să programați cu regularitate copii de rezervă realizate automat prin puncte de recuperare.

Pentru a crea setul de discuri de recuperare:

1. Faceți clic pe **Start > HP Backup and Recovery > HP Backup and Recovery Manager**, pentru a deschide expertul pentru copiere de rezervă și recuperare, apoi faceți clic pe **Next** (Următorul).
2. Selectați **Create a set of recovery discs (Recommended)** (Creare set de discuri de recuperare – Recomandat) și faceți clic pe **Next** (Următorul).
3. Urmați instrucțiunile din expert.

Pentru informații suplimentare despre utilizarea aplicației HP Backup and Recovery Manager, consultați *Ghidul utilizatorului aplicației HP Backup and Recovery Manager* selectând **Start > HP Backup and Recovery > Manual HP Backup and Recovery Manager**.

 **NOTĂ:** Puteți să comandați un set de discuri de recuperare de la HP apelând la centrul de asistență HP. Accesați următorul site Web, selectați țara/regiunea dvs. și faceți clic pe legătura **Technical support after you buy** (Asistență tehnică după cumpărare) de sub antetul **Call HP** (Apelare HP) pentru a obține numărul de telefon al centrului de asistență pentru țara/regiunea dvs.


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

Tehnologia de gestionare

Modelele includ tehnologie vPro sau tehnologie standard. Ambele permit o mai bună identificare, remediere și protecție a activelor de calcul legate la rețea. Ambele tehnologii permit gestionarea PC-urilor chiar dacă sistemul este pornit, oprit sau dacă sistemul de operare este blocat.

Caracteristicile tehnologiei de gestionare includ:

- Informații despre inventarul hardware
- Avertizare
- Gestionarea alimentării – pornire, oprire, alimentare ciclică
- Diagnosticare și reparare de la distanță
 - Serial-over-LAN (Serial prin rețeaua LAN) – permite controlul de la consolă al PC-urilor de la distanță în timpul fazei de încărcare
 - IDE-Redirect (Redirecționare IDE) – permite încărcarea sistemului de la distanță, de pe o unitate, un disc sau dintr-o imagine ISO
- Izolarea și recuperarea pe baza hardware-ului – limitează sau întrerupe accesul la rețeaua de PC-uri, dacă se detectează o activitate asemănătoare cu a unui virus

 **NOTĂ:** Pentru o prezentare generală a tehnologiei Intel vPro, vizitați <http://www.intel.com/vpro>.

Pentru informații specifice HP despre tehnologia Intel vPro, consultați cărțile albe de la adresa <http://www.hp.com/support>. Selectați țara/regiunea și limba, selectați **See support and troubleshooting information** (Vizualizare informații despre asistență și depanare), introduceți numărul de model al computerului și apăsați **Enter**. În categoria **Resources** (Resurse), faceți clic pe **Manuals (guides, supplements, addendums, etc.)** (Manuale, ghiduri, suplimente, anexe etc.). Sub **Quick jump to manuals by category** (Salt rapid la manuale după categorie), faceți clic pe **White papers** (Cărți albe).


Tehnologiile de gestionare disponibile includ:

- AMT (include DASH 1.0)
- ASF

Este posibil ca ASF și AMT să nu fie configurate simultan, dar ambele sunt acceptate.

Pentru a configura sistemele Intel vPro pentru AMT sau ASF:

1. Porniți sau reporniți computerul. Dacă sunteți în Microsoft Windows, faceți clic pe **Start > Închidere > Repornire**.
2. Imediat după pornirea computerului, apăsați combinația de taste **Ctrl+P**, atunci când indicatorul luminos al monitorului se aprinde verde, înaintea încărcării de către computer a sistemului de operare.

 **NOTĂ:** Dacă nu ați apăsat **Ctrl+P** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **Ctrl+P** pentru a accesa utilitarul.

Cu această combinație de taste se intră în utilitarul de configurare Intel Management Engine BIOS Execution (MEBx). Acest utilitar îi permite utilizatorului să configureze diferite aspecte ale tehnologiei de gestionare. Unele dintre opțiunile de configurare sunt listate mai jos:

- Main Menu (Meniu principal)
 - Intel® ME Configuration (Configurație Intel® ME)
 - Intel® AMT Configuration (Configurație Intel® AMT)
 - Change Intel® ME Password (Schimbare parolă Intel® ME)
 - Exit (Ieșire)
- Intel® Platform Configuration (Configurație platformă Intel®)
 - Intel® ME State Control (Control stare Intel® ME) (activare/dezactivare).
 - Intel® ME Firmware Local Update (Actualizare firmware Intel® ME) (activare/dezactivare)
 - Intel® ME Features Control (Control caracteristici Intel® ME)
 - Intel® ME Power Control (Control energie Intel® ME)
- Intel® AMT Configuration (Configurație Intel® AMT)
 - Host Name (Nume gazdă)
 - TCP/IP
 - Provision Model (Model identificare) (Enterprise, SMB)
 - Setup and Configuration (Instalare și configurare)
 - Un-Provision (Ștergere date identificare)
 - SOL/IDE-R (activare/dezactivare)
 - Password Policy (Politică parole)
 - Secure Firmware Update (Actualizare securizată firmware) (activare/dezactivare)
 - Set PRTC (Setare PRTC)
 - Idle Timeout (Expirare inactivitate)
- Change Intel® ME Password (Schimbare parolă Intel® ME - HP recomandă cu insistență ca această parolă să fie schimbată. Parola implicită este **admin**.)

Pentru a gestiona de la distanță sistemele AMT, administratorul trebuie să utilizeze o consolă la distanță care acceptă AMT. Consolele de gestionare la nivel de întreprindere sunt disponibile de la furnizori precum HP, Altiris și Microsoft SMS. În mod SMB, clientul furnizează o interfață de browser Web. Pentru a accesa această caracteristică, deschideți un browser din orice alt sistem din rețea și introduceți `http://nume_gazdă:16992`, unde `nume_gazdă` este numele asociat sistemului. Ca variantă, în locul numelui de gazdă se poate utiliza adresa IP.

Verdiem Surveyor

Verdiem Surveyor (Supraveghetor Verdiem) este o soluție software care ajută la gestionarea costurilor pentru energia consumată de PC-uri. Supraveghetorul măsoară și raportează câtă energie consumă fiecare PC. De asemenea, asigură controlul asupra setărilor de gestionare a energiei PC-urilor, permițând administratorilor să implementeze simplu strategii de economisire a energiei în rețelele lor. Un modul HP SoftPaq care conține agentul Surveyor poate fi descărcat de pe site-ul de asistență HP și instalat pe modelele de computere de birou comerciale acceptate. Licențele Surveyor pentru gestionarea PC-urilor pot fi achiziționate prin reprezentantul HP local.

HP Proactive Change Notification

Programul de notificare în timp real a modificărilor (PCN) utilizează site-ul Web Subscriber's Choice (Opțiunea abonatului) pentru a realiza în timp real și în mod automat:

- Trimiterea către dvs. a mesajelor de e-mail Proactive Change Notification (PCN) care vă informează despre modificările hardware și software din majoritatea computerelor și serverelor comerciale, cu până la 60 de zile înainte de efectuarea acestor modificări
- Trimiterea către dvs. a mesajelor de e-mail tip Customer Bulletin (Buletin pentru clienți), Customer Advisory (Recomandare pentru clienți), Customer Note (Notă pentru clienți), Security Bulletin (Buletin de securitate) și alerte cu privire la drivere, pentru majoritatea computerelor și serverelor comerciale

Pentru a avea siguranța că numai dvs. primiți informațiile legate de un anumit mediu IT, creați propriul profil. Pentru a afla mai multe despre programul Proactive Change Notification (Notificare în timp real a modificărilor) și despre crearea unui profil particularizat, vizitați <http://h30046.www3.hp.com/subhub.php>

Subscriber's Choice (Opțiunea abonatului)

Subscriber's Choice este un serviciu HP bazat pe clienți.

Pe baza profilului dumneavoastră, HP vă trimite sfaturi personalizate cu privire la produse, vă prezintă articole și/sau alerte/notificări cu privire la drivere și la asistență.

Alertele/notificările despre drivere și asistență de la Subscriber's Choice (Opțiunea abonatului) constau în mesaje de e-mail prin care sunteți înștiințat că informațiile pentru care v-ați abonat în profilul dvs. sunt disponibile pentru a fi examinate și preluate. Pentru a afla mai multe despre Subscriber's Choice (Opțiunea abonatului) și despre crearea unui profil particularizat, vizitați <http://h30046.www3.hp.com/subhub.php>.

Soluții retrase

Două pachete de software, Altiris Local Recovery și Dantz Retrospect, nu vor mai fi livrate pe computere de birou, computere portabile sau stații de lucru profesionale HP. Începând cu noile computere de birou, portabile și stații de lucru profesionale lansate în 2006, toate produsele se livrează cu HP Backup and Recovery Manager.

5 Actualizare ROM

BIOS-ul computerului este memorat într-o memorie programabilă flash ROM (Read Only Memory – memorie numai pentru citire). Prin stabilirea unei parole de setare în utilitarul Computer Setup (F10), aveți posibilitatea să protejați memoria ROM împotriva actualizării sau suprascrierii neintenționate. Acest lucru este important pentru asigurarea integrității funcționale a computerului. Dacă este necesar sau dacă doriți să efectuați upgrade de BIOS, aveți posibilitatea să descărcați cele mai recente imagini BIOS de la pagina HP pentru drivere și asistență, <http://www.hp.com/support/files>.

- △ **ATENȚIE:** Pentru protecția maximă a memoriei ROM, stabiliți o parolă de setare. Parola de setare împiedică actualizările neautorizate ale memoriei ROM. Managerul software-ului de sistem (SSM) permite administratorului de sistem să stabilească parola de setare pe unul sau pe mai multe PC-uri simultan. Pentru informații suplimentare, vizitați <http://www.hp.com/go/ssm>.

Actualizarea de la distanță a memoriei ROM

Actualizarea de la distanță a memoriei ROM permite administratorului de sistem să efectueze upgrade în siguranță al sistemului BIOS de la computere HP situate la distanță, direct de la consola de gestionare centralizată a rețelei. Faptul că administratorul de sistem poate să efectueze de la distanță această activitate, pe mai multe computere, are ca rezultat o desfășurare consistentă a imaginilor BIOS ale PC-urilor HP din rețea și un mai mare control asupra acestora. Un alt rezultat îl reprezintă creșterea productivității și reducerea costului total al proprietății.

- 📄 **NOTĂ:** SSM nu acceptă în prezent actualizarea ROM de la distanță pe sistemele la care este activat Windows Vista BitLocker și care utilizează măsurători TPM pentru a proteja cheile BitLocker, deoarece prin actualizarea BIOS-ului s-ar invalida semnătura de încredere pe care a creat-o BitLocker pentru platformă. Dezactivați BitLocker prin politica de grup pentru a actualiza BIOS-ul sistemului.

Pentru a beneficia de actualizarea memoriei ROM de la distanță, computerul trebuie pornit sau trebuie adus în stare de funcționare prin Remote Wakeup (Reactivare de la distanță).

Pentru mai multe informații despre actualizarea de la distanță a memoriei ROM, consultați software-ul HP Client Manager sau System Software Manager (Manager al software-ului de sistem) la adresa <http://www.hp.com/go/ssm/>.

HPQFlash

Utilitarul HPQFlash se utilizează pentru actualizarea sau restabilirea BIOS-ului sistemului de pe PC-uri individuale dintr-un sistem de operare Windows.

Pentru mai multe informații despre HPQFlash, vizitați <http://www.hp.com/support/files> și introduceți numărul de model al computerului când vi se solicită.

6 Boot Block Emergency Recovery Mode (Mod de recuperare de urgență a blocului de încărcare)

Boot Block Emergency Recovery Mode (Mod de recuperare de urgență a blocului de încărcare) permite recuperarea sistemului în situația neplăcută în care actualizarea memoriei ROM nu reușește. De exemplu, dacă a survenit o întrerupere a alimentării în timpul unui upgrade de BIOS, actualizarea memoriei ROM va fi incompletă. Acest lucru va face ca BIOS-ul sistemului să devină inutilizabil. Blocul de încărcare este o secțiune protejată la actualizare a memoriei ROM, care conține codul care verifică dacă imaginea BIOS pentru sistem este validă, la pornirea sistemului.

- Dacă imaginea BIOS a sistemului este validă, sistemul pornește normal.
- Dacă imaginea BIOS a sistemului nu este validă, un bloc de încărcare BIOS de siguranță în caz de eroare are o capacitate suficientă de căutare a fișierelor de imagine BIOS pe suporturi de stocare amovibile. Dacă se găsește un fișier imagine BIOS corespunzător, acesta actualizează automat memoria ROM.

Când se detectează o imagine BIOS nevalidă pentru sistem, LED-ul de alimentare a sistemului clipește de 8 ori cu culoare roșie, o dată pe secundă. Simultan, în difuzor se aud 8 semnale sonore. Dacă porțiunea din memoria ROM de sistem care conține imaginea ROM pentru componenta video nu este coruptă, pe ecran se afișează mesajul **Boot Block Emergency Recovery Mode** (Mod de recuperare de urgență a blocului de încărcare).

Pentru a recupera sistemul după ce acesta intră în Boot Block Emergency Recovery Mode (Mod de recuperare de urgență a blocului de încărcare), urmați toți pașii de mai jos:

1. Opriți alimentarea.
2. Introduceți un CD sau un dispozitiv flash USB care conține fișierul imagine BIOS dorit în directorul rădăcină.




NOTĂ: Suportul trebuie să fie formatat pentru un sistem de fișiere FAT12, FAT16 sau FAT32.

3. Porniți computerul.

Dacă nu se găsește nicio imagine BIOS corespunzătoare, vi se va solicita să introduceți suportul care conține un fișier de imagine BIOS.

Dacă sistemul reușește să programeze cu succes memoria ROM, sistemul se va opri automat.

4. Scoateți suportul amovibil utilizat pentru upgrade-ul de BIOS.
5. Activați alimentarea pentru a reporni computerul.

 **NOTĂ:** BitLocker împiedică Windows Vista să se încarce când un CD care conține fișierul de imagine BIOS este într-o unitate optică. Dacă BitLocker este activat, scoateți acest CD înainte de a încerca să încărcați sistemul din Windows Vista.

7 Multiplicarea instalării


Următoarele proceduri îi dau posibilitatea unui administrator să copieze cu ușurință o configurație de instalare pe alte computere de același model. Aceasta permite configurarea mai rapidă și mai consistentă pentru mai multe computere.

 **NOTĂ:** Ambele proceduri necesită o unitate de dischetă sau o unitate flash USB acceptată.

Copierea pe un singur computer

△ **ATENȚIE:** O configurație de instalare este specifică modelului. În cazul în care computerul sursă și cel de destinație nu sunt același model, poate să survină coruperea sistemului de fișiere. De exemplu, nu copiați configurația de instalare de pe un PC dc7xxx pe un PC dx7xxx.

1. Selectați o configurație de instalare pentru copiere. Opriți computerul. Dacă sunteți în Windows, faceți clic pe **Start > Închidere > Închidere**.
2. Dacă utilizați un dispozitiv de memorie flash USB, introduceți-l acum.
3. Porniți computerul.
4. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.

 **NOTĂ:** Dacă nu ați apăsăat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

5. Dacă utilizați o dischetă, introduceți-o acum.
6. Faceți clic pe **File (Fișier) > Replicated Setup (Instalare copiată) > Save to Removable Media (Salvare pe suport amovibil)**. Pentru a crea discheta sau dispozitivul de memorie flash USB de configurare, urmați instrucțiunile de pe ecran.
7. Opriți computerul care trebuie configurat și introduceți discheta sau dispozitivul de memorie flash USB de configurare.
8. Porniți computerul care se configurează.
9. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.

10. Faceți clic pe **File** (Fișier) > **Replicated Setup** (Instalare copiată) > **Restore from Removable Media** (Restaurare de pe suport amovibil) și urmați instrucțiunile de pe ecran.
11. Când configurația este completă, reporniți computerul.

Copierea pe mai multe computere

△ **ATENȚIE:** O configurație de instalare este specifică modelului. În cazul în care computerul sursă și cel de destinație nu sunt același model, poate să survină coruperea sistemului de fișiere. De exemplu, nu copiați configurația de instalare de pe un PC dc7xxx pe un PC dx7xxx.

Prin această metodă pregătirea dischetei sau a dispozitivului de memorie flash USB durează puțin mai mult, dar copierea configurației pe computerele sursă este substanțial mai rapidă.

📄 **NOTĂ:** Pentru această procedură sau pentru a crea un dispozitiv de memorie flash USB de încărcare, este necesară o dischetă de încărcare. Dacă Windows XP nu este disponibil pentru a fi utilizat la crearea unei dischete de încărcare, utilizați metoda copierii pe un singur computer (consultați [Copierea pe un singur computer, la pagina 18](#)).

1. Creați o dischetă de încărcare sau un dispozitiv de memorie flash USB de încărcare. Consultați [Dispozitive de memorie flash USB acceptate, la pagina 20](#) sau [Dispozitive de memorie flash USB neacceptate, la pagina 21](#).

△ **ATENȚIE:** Nu toate computerele pot fi încărcate de pe un dispozitiv de memorie flash USB. Dacă în ordinea implicită de încărcare din programul utilitar Computer Setup (F10) dispozitivul USB este listat înaintea unității de disc, computerul poate fi încărcat de pe un dispozitiv de memorie flash USB. În caz contrar, trebuie utilizată o dischetă de încărcare.

2. Selectați o configurație de instalare pentru copiere. Opriiți computerul. Dacă sunteți în Windows, faceți clic pe **Start** > **Închidere** > **Închidere**.
3. Dacă utilizați un dispozitiv de memorie flash USB, introduceți-l acum.
4. Porniți computerul.
5. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.

📄 **NOTĂ:** Dacă nu ați apăsat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

6. Dacă utilizați o dischetă, introduceți-o acum.
7. Faceți clic pe **File** (Fișier) > **Replicated Setup** (Instalare copiată) > **Save to Removable Media** (Salvare pe suport amovibil). Pentru a crea discheta sau dispozitivul de memorie flash USB de configurare, urmați instrucțiunile de pe ecran.
8. Descărcați un utilitar BIOS pentru copierea instalării (repset.exe) și copiați-l pe discheta sau pe dispozitivul de memorie flash USB de configurare. Pentru a obține acest utilitar, vizitați <http://welcome.hp.com/country/us/en/support.html> și introduceți numărul modelului computerului.
9. Pe discheta sau pe dispozitivul de memorie flash USB de configurare, creați un fișier autoexec.bat care să conțină următoarea comandă:

```
repset.exe
```

10. Opriți computerul care se configurează. Introduceți discheta sau dispozitivul de memorie flash USB de configurare și porniți computerul. Utilitarul de configurare se va executa automat.
11. Când configurația este completă, reporniți computerul.

Crearea unui dispozitiv de încărcare

Dispozitive de memorie flash USB acceptate

Dispozitivele acceptate au o imagine preinstalată, pentru a simplifica procesul de a le face dispozitive de încărcare. Toate dispozitivele de memorie flash USB marca HP, Compaq și majoritatea celor de la alți furnizori au încărcată în prealabil această imagine. Dacă dispozitivul de memorie flash USB utilizat nu are această imagine, utilizați procedura descrisă mai departe în această secțiune (consultați [Dispozitive de memorie flash USB neacceptate, la pagina 21](#)).

Pentru a crea un dispozitiv de memorie flash USB de încărcare, trebuie să aveți:

- un dispozitiv de memorie flash USB acceptat
- o dischetă DOS de încărcare cu programele FDISK și SYS (Dacă SYS nu este disponibil, se poate utiliza FORMAT, dar toate fișierele existente pe dispozitivul de memorie flash USB se vor pierde.)
- un PC care se poate încărca de pe un dispozitiv de memorie flash USB

△ **ATENȚIE:** Este posibil ca unele PC-uri mai vechi să nu se poată încărca de pe un dispozitiv de memorie flash USB. Dacă în ordinea implicită de încărcare din programul utilitar Computer Setup (F10) dispozitivul USB este listat înaintea unității de disc, computerul poate fi încărcat de pe un dispozitiv de memorie flash USB. În caz contrar, trebuie utilizată o dischetă de încărcare.

1. Opriți computerul.
2. Introduceți dispozitivul de memorie flash USB într-unul din porturile USB ale computerului și scoateți toate celelalte dispozitive USB de stocare, cu excepția unităților USB de dischetă.
3. Introduceți o dischetă DOS de încărcare cu FDISK.COM și SYS.COM sau FORMAT.COM într-o unitate de dischetă și porniți computerul pentru a încărca discheta DOS.
4. Executați FDISK de la promptul **A:** tastând **FDISK** și apăsând **Enter**. Dacă vi se solicită, faceți clic pe **Yes (Y)** pentru a activa suportul pentru discuri mari.
5. Introduceți opțiunea [5] pentru a afișa unitățile din sistem. Dispozitivul de memorie flash USB este unitatea cea mai apropiată ca dimensiuni de una dintre unitățile listate. De regulă, este ultima unitate din listă. Notați litera unității.

Unitatea dispozitivului de memorie flash USB: _____

△ **ATENȚIE:** Dacă nici o unitate nu corespunde cu dispozitivul de memorie flash USB, nu continuați. Pot surveni pierderi de date. Controlați toate port-urile USB pentru alte dispozitive de stocare. Dacă găsiți asemenea dispozitive, scoateți-le, reporniți computerul și continuați de la pasul 4. Dacă nu găsiți nici un astfel de dispozitiv, fie sistemul nu acceptă dispozitivul de memorie flash USB, fie dispozitivul de memorie flash USB este defect. NU încercați să faceți din dispozitivul de memorie flash USB un dispozitiv de încărcare.

6. Ieșiți din programul FDISK apăsând tasta **Esc** pentru a reveni la promptul **A:**.
7. Dacă discheta DOS de încărcare conține programul SYS.COM, mergeți la pasul 8. În caz contrar, mergeți la pasul 9.

8. La promptul **A:**, introduceți `SYS x :` unde **x** reprezintă litera de unitate notată mai sus.

△ **ATENȚIE:** Aveți grijă ca litera introdusă pentru dispozitivul de memorie flash USB să fie cea corectă.

După transferul fișierelor de sistem, SYS va reveni la promptul **A:**. Mergeți la pasul 13.

9. Copiați toate fișierele pe care doriți să le păstrați de pe dispozitivul de memorie flash USB într-un director temporar sau pe altă unitate (de exemplu, pe unitatea de disc internă a sistemului).

10. La promptul **A:**, introduceți `FORMAT /S X :` unde **X** reprezintă litera de unitate notată mai sus.

△ **ATENȚIE:** Aveți grijă ca litera introdusă pentru dispozitivul de memorie flash USB să fie cea corectă.

FORMAT va afișa unul sau mai multe mesaje și vă va întreba de fiecare dată dacă doriți să continuați. Introduceți **Y** de fiecare dată. FORMAT va formata dispozitivul de memorie flash USB, va adăuga fișierele de sistem și vă va solicita o etichetă de volum (Volume Label).

11. Apăsăți pe **Enter** sau introduceți eticheta dorită.

12. Copiați toate fișierele salvate la pasul 9 înapoi pe dispozitivul de memorie flash USB.

13. Scoateți discheta și reporniți computerul. Computerul se va încărca de pe dispozitivul de memorie flash USB, considerat ca unitatea C.

📝 **NOTĂ:** Ordinea implicită de încărcare diferă de la computer la computer și poate fi modificată din programul utilitar Computer Setup (F10).

Dacă ați utilizat o versiune DOS de pe Windows 9x, este posibil să apară un ecran cu sigla Windows. Dacă nu doriți să apară acest ecran, adăugați un fișier gol cu denumirea LOGO.SYS în directorul rădăcină al dispozitivului de memorie flash USB.

Reveniți la [Copierea pe mai multe computere, la pagina 19](#).

Dispozitive de memorie flash USB neacceptate

Pentru a crea un dispozitiv de memorie flash USB de încărcare, trebuie să aveți:

- un dispozitiv de memorie flash USB
- o dischetă DOS de încărcare cu programele FDISK și SYS (Dacă SYS nu este disponibil, se poate utiliza FORMAT, dar toate fișierele existente pe dispozitivul de memorie flash USB se vor pierde.)
- un PC care se poate încărca de pe un dispozitiv de memorie flash USB


△ **ATENȚIE:** Este posibil ca unele PC-uri mai vechi să nu se poată încărca de pe un dispozitiv de memorie flash USB. Dacă în ordinea implicită de încărcare din programul utilitar Computer Setup (F10) dispozitivul USB este listat înaintea unității de disc, computerul poate fi încărcat de pe un dispozitiv de memorie flash USB. În caz contrar, trebuie utilizată o dischetă de încărcare.

1. Dacă în sistem există plăci PCI care au atașate unități SCSI, ATA RAID sau SATA, opriți computerul și scoateți cablul de alimentare.

△ **ATENȚIE:** Cablul de alimentare TREBUIE să fie deconectat.

2. Deschideți computerul și scoateți plăcile PCI.


3. Introduceți dispozitivul de memorie flash USB într-unul din porturile USB ale computerului și scoateți toate celelalte dispozitive USB de stocare, cu excepția unităților USB de dischetă. Închideți capacul computerului.
4. Conectați cablul de alimentare și porniți computerul.
5. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.

 **NOTĂ:** Dacă nu ați apăsat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

6. Pentru a dezactiva controlerul PATA și SATA, mergeți la **Advanced (Complex) > PCI Devices (Dispozitive PCI)**. Când dezactivați controlerul SATA, notați IRQ-ul la care este asociat controlerul. Va fi necesar să reasociați acest IRQ mai târziu. Ieșiți din programul de instalare, confirmând modificările.

IRQ SATA: _____

7. Introduceți o dischetă DOS de încărcare cu FDISK.COM și SYS.COM sau FORMAT.COM într-o unitate de dischetă și porniți computerul pentru a încărca discheta DOS.
8. Executați programul FDISK și ștergeți toate partițiile existente pe dispozitivul de memorie flash USB. Creați o partiție nouă și marcați-o ca activă. Ieșiți din programul FDISK apăsând tasta **Esc**.
9. Dacă sistemul nu repornește automat când ieșiți din programul FDISK, apăsați pe **Ctrl+Alt+Del** pentru a se încărca de pe discheta DOS.
10. La promptul **A:**, tastați **FORMAT C: /S** și apăsați pe **Enter**. Programul FORMAT va formata dispozitivul de memorie flash USB, va adăuga fișierele de sistem și va solicita o etichetă de volum.
11. Apăsați pe **Enter** sau introduceți eticheta dorită.
12. Opriți computerul și scoateți cablul de alimentare. Deschideți computerul și montați la loc plăcile PCI pe care le-ați scos anterior. Închideți capacul computerului.
13. Conectați cablul de alimentare, scoateți discheta și porniți computerul.
14. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.
15. Mergeți la **Advanced (Complex) > PCI Devices (Dispozitive PCI)** și activați din nou controlerul PATA și SATA pe care le-ați dezactivat la pasul 6. Asociați controlerului SATA IRQ-ul inițial.
16. Ieșiți din program salvând modificările. Computerul se va încărca de pe dispozitivul de memorie flash USB, considerat ca unitatea C.

 **NOTĂ:** Ordinea implicită de încărcare diferă de la computer la computer și poate fi modificată din programul utilitar Computer Setup (F10). Pentru instrucțiuni, consultați *Computer Setup (F10) Utility* (Programul utilitar Computer Setup (F10)).

Dacă ați utilizat o versiune DOS de pe Windows 9x, este posibil să apară un ecran cu sigla Windows. Dacă nu doriți să apară acest ecran, adăugați un fișier gol cu denumirea LOGO.SYS în directorul rădăcină al dispozitivului de memorie flash USB.

Reveniți la [Copierea pe mai multe computere, la pagina 19](#).

8 Buton de alimentare cu două stări

Când Advanced Configuration (Configurație avansată) și interfața de putere (ACPI) sunt activate, butonul de alimentare poate să funcționeze fie ca un comutator pornit/oprit, fie ca buton de oprire temporară. Caracteristica de oprire temporară nu oprește complet alimentarea, ci provoacă intrarea computerului într-o stare de oprire temporară cu consum scăzut de energie. Acest lucru permite oprirea rapidă fără a închide aplicațiile și revenirea rapidă la aceeași stare de funcționare fără nici o pierdere de date.

Pentru modificarea configurației butonului de alimentare, urmați toți pașii de mai jos:

1. Faceți clic pe **butonul Start**, apoi selectați **Panou de control > Opțiuni de alimentare**.
2. În **Proprietăți opțiuni alimentare**, selectați fila **Complex**.
3. În secțiunea **Buton de alimentare**, selectați **Stare de veghe**.

După configurarea butonului de alimentare pentru a funcționa ca buton pentru oprire temporară, apăsați butonul de alimentare pentru a plasa sistemul într-o stare cu un consum foarte mic de energie (stare de veghe). Apăsați din nou butonul pentru a aduce înapoi sistemul din starea de oprire temporară în starea cu alimentare completă cu energie. Pentru a opri complet alimentarea sistemului, țineți apăsat butonul de alimentare timp de patru secunde.

△ **ATENȚIE:** Nu utilizați butonul de alimentare pentru a opri computerul decât dacă sistemul nu răspunde; oprirea alimentării fără interacțiunea sistemului de operare poate să provoace distrugerea sau pierderea unor date de pe unitatea de disc.

9 Asistență la site-ul Web HP

Specialiștii de la HP au testat și au depanat cu rigurozitate software-ul dezvoltat de HP și de alți furnizori și dezvoltă software specific de asistență pentru sistemul de operare, pentru a asigura performanțele, compatibilitatea și fiabilitatea computerelor HP.

Când realizați tranziția la sisteme de operare noi sau revizuite, este important să implementați software-ul de asistență proiectat pentru sistemul de operare respectiv. Dacă intenționați să executați o versiune de Microsoft Windows diferită de versiunea livrată împreună cu computerul, trebuie să instalați driverele și utilitarele corespunzătoare pentru unități pentru a fi sigur că toate caracteristicile sunt acceptate și funcționează corect.

HP a reușit să simplifice găsirea, accesarea, evaluarea și instalarea celui mai recent software de asistență. Software-ul poate fi descărcat de la adresa <http://www.hp.com/support>.

Site-ul Web conține cele mai recente drivere de dispozitive, utilitare și imagini de memorii flash ROM necesare pentru a executa cel mai recent sistem de operare Microsoft Windows pe computerul HP.

10 Standarde în domeniu


Soluțiile de management de la HP se integrează cu alte aplicații de management al sistemelor și se bazează pe standarde industriale precum:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Tehnologia Wake-On-LAN
- ACPI
- SMBIOS
- Suport PXE (Mediu de execuție înainte de încărcarea sistemului)

11 Urmărirea și securitatea activelor

Caracteristicile de urmărire a activelor încorporate în computer oferă date esențiale pentru urmărirea activelor, care se pot gestiona utilizând HP Systems Insight Manager (Manager inteligent sisteme HP), HP Client Manager (Manager client HP), HP Configuration Management Solution (Soluție de gestionare a configurației HP), HP Client Configuration Manager (Manager configurație client HP) sau alte aplicații de gestionare a sistemelor. Integrarea automată și nemijlocită între caracteristicile de urmărire a activelor și aceste produse vă permite să alegeți instrumentul de gestionare cel mai potrivit pentru mediu și să echilibrați investițiile în instrumentele existente.

De asemenea, HP oferă câteva soluții pentru controlul accesului la componentele și informațiile importante. HP Embedded Security for ProtectTools (Securitate încorporată HP pentru ProtectTools), dacă este instalat, împiedică accesul neautorizat la date, verifică integritatea sistemului și autentifică utilizatorii externi care încearcă accesarea sistemului. Pentru informații suplimentare, consultați *Ghidul managerului de securitate HP ProtectTools* de la adresa <http://www.hp.com/products/security>. Caracteristicile de securitate precum HP Embedded Security for ProtectTools, „Senzorul de capac inteligent și „Zăvorul de capac inteligent”, disponibile la unele modele, ajută la prevenirea accesului neautorizat la componentele interne ale computerului personal. Prin dezactivarea porturilor paralele, seriale sau USB sau prin dezactivarea posibilității de încărcare a sistemului de pe suporturi detașabile, aveți posibilitatea să protejați datele importante despre active. Alertele privind modificarea memoriei, precum și cele care provin de la senzorul de capac inteligent pot fi redirecționate automat către aplicațiile de gestionare a sistemului pentru a furniza notificări în timp real despre intervenții la componentele interne ale unui computer.

 **NOTĂ:** HP Embedded Security for ProtectTools (Securitate încorporată HP pentru ProtectTools), Smart Cover Sensor (Senzor capac inteligent) și Smart Cover Lock (Zăvor capac inteligent) sunt disponibile ca opțiuni pe anumite sisteme.

Pentru gestionarea setărilor de securitate de la computere HP, utilizați următoarele utilitare:

- Local, utilizând programele utilitare pentru setarea computerului. Pentru mai multe informații și instrucțiuni despre utilitarele de setare a computerului, consultați *Ghidul programului utilitar Computer Setup (F10)* care este livrat împreună cu computerul. Unele computere sunt dotate și cu HP BIOS Configuration for ProtectTools (Configurare BIOS HP pentru ProtectTools), o componentă ProtectTools bazată pe Windows care le permite administratorilor să configureze setări de securitate BIOS din sistemul de operare în execuție.
- De la distanță, prin utilizarea HP Client Manager from Symantec, HP Client Automation sau System Software Manager. Acest software permite desfășurarea sigură și consistentă și controlul setărilor de securitate.

Tabelul și secțiunile următoare se referă la gestionarea locală a caracteristicilor de securitate ale computerului prin intermediul programelor utilitare Computer Setup (F10).

Tabelul 11-1 Prezentare generală a caracteristicilor de securitate

Opțiune	Descriere
---------	-----------

Tabloul 11-1 Prezentare generală a caracteristicilor de securitate (Continuare)

Parolă de setare	Permite stabilirea și activarea unei parole de setare (de administrator). NOTĂ: Dacă se stabilește o parolă de setare, este necesar să modificați opțiunile programului Computer Setup, să curățați memoria ROM și să modificați anumite setări „plug and play” (conectare și redare) din Windows.
Power-On Password (Parolă de pornire)	Permite stabilirea și activarea unei parole de pornire. Promptul de parolă pentru pornire apare după un ciclu de alimentare. Dacă utilizatorul nu introduce parola corectă de pornire, unitatea nu va efectua secvența de încărcare. NOTĂ: Această parolă nu apare la încărcările la cald, precum Ctrl + Alt + Delete sau Restart from Windows (Repornire din Windows), dacă nu s-a activat din Password Options (Opțiuni parolă) (vezi mai jos).
Password Options (Opțiuni parolă) (Apare numai dacă s-a stabilit o parolă de pornire sau o parolă de setare.)	Permite: <ul style="list-style-type: none">• Blocarea variantelor vechi de resurse (apare dacă s-a stabilit o parolă de setare)• Activarea/dezactivarea modului server de rețea (apare dacă s-a stabilit o parolă de pornire)• Specificarea faptului că este necesară sau nu o parolă pentru încărcarea la cald (Ctrl+Alt+Delete) (apare dacă s-a stabilit o parolă de pornire)• Activarea/dezactivarea modului de răsfoire a configurației (apare dacă este setată o parolă de setare) (permite vizualizarea, dar nu și modificarea, opțiunilor de configurare F10, fără a introduce parola de setare)• Enable/disable Stringent Password (Activare/dezactivare parolă riguroasă) (apare dacă este setată o parolă de pornire) care, când este activată, ignoră jumperul de parolă de pe placă pentru a dezactiva parola de pornire <p>Pentru informații suplimentare, consultați <i>Ghid de gestionare a computerului</i>.</p>
Smart Cover (Capac inteligent) (la unele modele)	Permite: <ul style="list-style-type: none">• Blocarea/deblocarea dispozitivului Cover Lock (incuietoarea capacului).• Pentru Cover Removal Sensor (Senzor de scoatere a capacului) stabiliți Disable/Notify User/Setup Password (Dezactivare/Notificare utilizator/Parolă de setare). NOTĂ: <i>Notify User</i> (Notificare utilizator) informează utilizatorul atunci când senzorul a detectat că a fost scos capacul. <i>Setup Password</i> (Parolă de setare) solicită introducerea parolei de setare pentru a încărca sistemul în computer, dacă senzorul detectează că a fost scos capacul. Această caracteristică este acceptată numai la unele modele.
Device Security (Securitate dispozitiv)	Vă permite să setați Device Available/Device Hidden (Dispozitiv disponibil/Dispozitiv ascuns) pentru: <ul style="list-style-type: none">• Porturi seriale• Port paralel• Porturi USB din spate• Porturi USB frontale• Porturi USB interne• Sunet sistem• Controlere de rețea (la unele modele)• Dischetă• Dispozitiv de securitate încorporat (la unele modele)• SATA0

Tabelul 11-1 Prezentare generală a caracteristicilor de securitate (Continuare)

	<ul style="list-style-type: none">• SATA1 (la unele modele)• SATA2 (la unele modele)• SATA3 (la unele modele)• eSATA (la unele modele)
Network Service Boot (Încărcarea sistemului prin servicii de rețea)	Activează/dezactivează capacitatea computerului de a se încălca cu un sistem de operare instalat pe un server de rețea. (Caracteristică disponibilă numai la modelele dotate cu NIC; controlerul de rețea trebuie să fie ori o placă de extensie PCI, ori să fie încorporat pe placa de sistem.)
System IDs (ID-uri sistem)	Vă permit să stabiliți: <ul style="list-style-type: none">• Numărul de inventar (identificator pe 18 octeți), un număr de identificare atribuit de firmă acestui computer.• Eticheta proprietarului (identificator pe 80 de octeți), afișată în timpul testării POST.• Numărul de serie al șasiului sau numărul unic de identificare universal (UUID - Universal Unique Identifier). UUID poate fi actualizat numai dacă numărul de serie al șasiului nu este valid. (Aceste numere ID sunt stabilite, în mod normal, din fabrică și sunt utilizate pentru a identifica unic sistemul.)• Setarea locală pentru tastatură (de exemplu, Română sau Germană) pentru introducerea ID-ului de sistem.
DriveLock Security (Securitate DriveLock)	Permite stabilirea sau modificarea unor parole principale sau de utilizator pentru unitățile de disc. Când această caracteristică este activată, utilizatorului i se solicită să furnizeze una dintre parolele DriveLock în timpul testelor POST. Dacă nici o parolă nu este introdusă corect, unitatea de disc va rămâne inaccesibilă până când se furnizează o parolă corectă în timpul unei secvențe de încărcare la cald ulterioare. NOTĂ: Această opțiune va apărea numai atunci când la sistem este atașată cel puțin o unitate care acceptă caracteristica DriveLock.
System Security (Securitate sistem) (la unele modele: aceste opțiuni sunt dependente de hardware)	Data Execution Prevention (Împiedicarea execuției datelor) (la unele modele) (activare/dezactivare) - Contribuie la prevenirea apariției breșelor în securitate. Virtualization Technology (Tehnologie de virtualizare) (la anumite modele) (activare/dezactivare) - Controlează caracteristicile de virtualizare ale procesorului. Modificarea acestei setări necesită oprirea și repornirea computerului. Virtualization Technology Directed I/O (I/E direcționată prin tehnologie de virtualizare) (la anumite modele) (activare/dezactivare) - Controlează caracteristicile de remapare DMA de virtualizare pentru circuitele integrate. Modificarea acestei setări necesită oprirea și repornirea computerului. Trusted Execution Technology I/O (I/E cu tehnologie de execuție de încredere) (la anumite modele) (activare/dezactivare) - Controlează caracteristicile procesorului și circuitelor integrate principale necesare pentru suportul unui echipament virtual. Modificarea acestei setări necesită oprirea și repornirea computerului. Pentru a activa această caracteristică, trebuie să activați următoarele caracteristici: <ul style="list-style-type: none">• Suport de dispozitiv de securitate încorporat• Tehnologie de virtualizare• I/E direcționată prin tehnologie de virtualizare Embedded Security Device Support (Suport de dispozitiv de securitate încorporat) (la unele modele) (activare/dezactivare) - Permite activarea și dezactivarea dispozitivului de securitate încorporat. Modificarea acestei setări necesită oprirea și repornirea computerului.

Tabloul 11-1 Prezentare generală a caracteristicilor de securitate (Continuare)

NOTĂ: Pentru configurarea dispozitivului de securitate încorporat este necesară stabilirea unei parole de configurare.

- Reset to Factory Settings (Resetare la setările din fabrică) (la unele modele) (Fără resetare/Resetare) - Resetarea valorilor implicite din fabrică va șterge toate cheile de securitate. Modificarea acestei setări necesită oprirea și repornirea computerului.

ATENȚIE: Dispozitivul de securitate încorporat este o componentă critică a multor scheme de securitate. Ștergerea cheilor de securitate va preveni accesul la datele protejate de dispozitivul de securitate încorporat. Selectarea opțiunii Reset to Factory Settings (Resetare la setările din fabrică) poate avea ca rezultat o pierdere importantă a datelor.

- Power-on authentication support (Suport de autentificare la pornire) (la unele modele) (activare/dezactivare) - Controlează schema de autentificare prin parolă la pornire, care utilizează dispozitivul de securitate încorporat. Modificarea acestei setări necesită oprirea și repornirea computerului.
- Reset authentication credentials (Resetare acreditivă de autentificare) (la unele modele) (Fără resetare/Resetare) - Selectarea opțiunii de resetare conduce la dezactivarea suportului de autentificare la pornire și șterge informațiile de autentificare din dispozitivul de securitate încorporat. Modificarea acestei setări necesită oprirea și repornirea computerului.

OS management of Embedded Security Device (Gestionare prin SO a dispozitivului de securitate încorporat) (la unele modele) (activare/dezactivare) - Această opțiune permite utilizatorului să limiteze controlul sistemului de operare asupra dispozitivului de securitate încorporat. Modificarea acestei setări necesită oprirea și repornirea computerului. Această opțiune permite utilizatorului să limiteze controlul sistemului de operare asupra dispozitivului de securitate încorporat.

- Reset of Embedded Security Device through OS (Resetare prin SO a dispozitivului de securitate încorporat) (la unele modele) (activare/dezactivare) - Această opțiune permite utilizatorului să limiteze posibilitatea sistemului de operare de a solicita o resetare la setările din fabrică a dispozitivului de securitate încorporat. Modificarea acestei setări necesită oprirea și repornirea computerului.

NOTĂ: Pentru activarea acestei opțiuni este necesară stabilirea unei parole de configurare.

Smart Card BIOS Password Support (Suport parolă BIOS card inteligent) (la unele modele) (activare/dezactivare) - Permite utilizatorului să activeze/dezactiveze utilizarea cardului inteligent în loc de parolele de configurare și de pornire. Această setare necesită inițializare suplimentară în ProtectTools înainte ca această opțiune să aibă efect.

PAVP (la unele modele) (dezactivat/min/max) - PAVP activează Protected Audio Video Path (Cale audio-video protejată) din circuitul integrat. Aceasta poate permite vizualizarea conținutului de înaltă definiție protejat, a căror redare altfel ar fi interzisă. Prin selectarea Max se vor aloca 96 MO din memoria de sistem exclusiv pentru PAVP.

Setup Security Level (Nivel securitate configurație)

Furnizează o metodă de a permite accesul limitat al utilizatorilor finali la modificarea opțiunilor de configurare specificate, fără necesitatea de a se cunoaște parola de setare.

Această caracteristică acordă administratorului flexibilitatea de a proteja modificările asupra opțiunilor de configurare esențiale, în timp ce permite utilizatorului să vizualizeze setările de sistem și să configureze opțiuni neesențiale. Administratorul specifică drepturile de acces la opțiunile de configurare individuale pentru fiecare caz în parte, prin intermediul meniului Setup Security Level (Configurare nivel securitate). În mod implicit, toate opțiunile de configurare sunt asociate cu o parolă de setare, indicând faptul că utilizatorul trebuie să introducă parola de setare corectă în timpul testelor POST, pentru a efectua modificări asupra oricărei opțiuni. Administratorul poate seta None (Fără) pentru elemente individuale, indicând faptul că utilizatorul poate efectua modificări asupra opțiunii specificate, când programul de configurare a fost accesat cu parole incorecte. Opțiunea None (Fără) se înlocuiește cu parola de pornire, dacă este activată o parolă de pornire.

NOTĂ: Setup Browse Mode (Mod răsfoire configurație) trebuie să fie setat pe Enable (Activat) pentru ca utilizatorul să intre în programul de configurare fără să cunoască parola de setare.

Securitate prin parole


Parola de pornire împiedică utilizarea neautorizată a computerului prin solicitarea introducerii unei parole pentru a accesa aplicații sau date, de fiecare dată când computerul este pornit sau repornit. Parola de setare împiedică în special accesul neautorizat la programul Computer Setup și mai poate fi utilizată pentru a ignora parola de pornire. Cu alte cuvinte, când se solicită parola de pornire, introducerea în locul acesteia a parolei de setare va permite accesul la computer.

Se poate stabili o parolă de setare pentru întreaga rețea pentru a permite administratorului să se conecteze la toate sistemele din rețea în vederea efectuării operațiilor de întreținere fără a fi necesar ca acesta să cunoască parolele de pornire, chiar dacă au fost stabilite.

Stabilirea unei parole de setare prin intermediul utilitarului Computer Setup

Dacă sistemul este echipat cu un dispozitiv de securitate încorporat, consultați *Ghidul managerului de securitate HP ProtectTools* de la adresa <http://www.hp.com>. Stabilirea unei parole de setare prin Computer Setup împiedică reconfigurarea computerului (cu utilitarul Computer Setup (F10)) până când este introdusă parola.

1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start > Închidere > Repornire**.
2. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.


 **NOTĂ:** Dacă nu ați apăsat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

3. Selectați **Security** (Securitate), apoi selectați **Setup Password** (Parolă de setare) și urmați instrucțiunile de pe ecran.
4. Înainte de a ieși, faceți clic pe **File** (Fișier) > **Save Changes and Exit** (Salvare modificări și ieșire).

Stabilirea unei parole de pornire prin utilitarul Computer Setup

Stabilirea unei parole de pornire prin Computer Setup împiedică accesul la computer când acesta este pornit, cu excepția cazului în care este introdusă parola. Când este stabilită o parolă de pornire, programul Computer Setup prezintă **Password Options** (Opțiuni parolă) sub meniul **Security** (Securitate). Opțiunile pentru parolă includ **Password Prompt on Warm Boot** (Solicitare parolă la pornirea la cald). Când este activată opțiunea **Password Prompt on Warm Boot** (Solicitare parolă la pornirea la cald), parola trebuie introdusă de fiecare dată când computerul este reinițializat.

1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start > Închidere > Repornire**.
2. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.


 **NOTĂ:** Dacă nu ați apăsat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

3. Selectați **Security** (Securitate), apoi selectați **Power-On Password** (Parolă de pornire) și urmați instrucțiunile de pe ecran.
4. Înainte de a ieși, faceți clic pe **File** (Fișier) > **Save Changes and Exit** (Salvare modificări și ieșire).

Introducerea unei parole de pornire

Pentru a introduce o parolă de pornire, urmați toți pașii de mai jos:

1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start** > **Închidere** > **Repornire computer**.
2. Când pe monitor apare pictograma cheie, introduceți parola curentă, apoi apăsați tasta **Enter**.

 **NOTĂ:** Tastați cu atenție deoarece, din motive de securitate, caracterele tastate nu apar pe ecran.


Dacă introduceți incorect parola, va apărea o pictogramă sub formă de cheie ruptă. Încercați din nou. După trei încercări nereușite, trebuie să închideți computerul, apoi să îl reporniți pentru a avea posibilitatea să continuați.

Introducerea unei parole de setare


Dacă sistemul este echipat cu un dispozitiv de securitate încorporat, consultați *Ghidul managerului de securitate HP ProtectTools* de la adresa <http://www.hp.com>.

Dacă la computer a fost stabilită o parolă de setare, vi se va solicita să o introduceți de fiecare dată când executați Computer Setup.

1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start** > **Închidere** > **Repornire**.
2. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.

 **NOTĂ:** Dacă nu ați apăsasat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

3. Când pe monitor apare pictograma cheie, introduceți parola de setare, apoi apăsați tasta **Enter**.

 **NOTĂ:** Tastați cu atenție deoarece, din motive de securitate, caracterele tastate nu apar pe ecran.


Dacă introduceți incorect parola, va apărea o pictogramă sub formă de cheie ruptă. Încercați din nou. După trei încercări nereușite, trebuie să închideți computerul, apoi să îl reporniți pentru a avea posibilitatea să continuați.

Modificarea unei parole de pornire sau de setare


Dacă sistemul este echipat cu un dispozitiv de securitate încorporat, consultați *Ghidul managerului de securitate HP ProtectTools* de la adresa <http://www.hp.com>.

1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start > Închidere > Repornire computer**.
2. Pentru a modifica parola de pornire, mergeți la pasul 3.

Pentru a schimba parola de configurare, imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.


 **NOTĂ:** Dacă nu ați apăsăat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

3. Când apare pictograma cheie, tastați parola curentă, o bară oblică (/) sau un caracter alternativ de delimitare, parola nouă, încă o bară oblică (/) sau caracter alternativ de delimitare și iarăși parola nouă, după cum este prezentat mai jos: parolă curentă/parolă nouă/parolă nouă

 **NOTĂ:** Tastați cu atenție deoarece, din motive de securitate, caracterele tastate nu apar pe ecran.

4. Apăsați tasta **Enter**.

Parola nouă va avea efect la următoarea pornire a computerului.


 **NOTĂ:** Pentru informații despre caracterele alternative de delimitare, consultați [Caractere de delimitare pentru tastaturile naționale, la pagina 33](#). Parola de pornire și parola de setare se mai pot modifica utilizând opțiunea Security (Securitate) din programul Computer Setup.

Ștergerea unei parole de pornire sau de setare


Dacă sistemul este echipat cu un dispozitiv de securitate încorporat, consultați *Ghidul managerului de securitate HP ProtectTools* de la adresa <http://www.hp.com>.

1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start > Închidere > Repornire computer**.
2. Pentru a șterge parola de pornire, mergeți la pasul 3.

Pentru a șterge parola de configurare, imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.

 **NOTĂ:** Dacă nu ați apăsăat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

3. Când apare pictograma cheie, tastați parola curentă urmată de o bară oblică (/) sau de un caracter alternativ de delimitare, după cum este prezentat mai jos: parolă curentă/
4. Apăsați tasta **Enter**.

 **NOTĂ:** Pentru informații despre caracterele alternative de delimitare, consultați [Caractere de delimitare pentru tastaturile naționale, la pagina 33](#). Parola de pornire și parola de setare se mai pot modifica utilizând opțiunea Security (Securitate) din programul Computer Setup.

Caractere de delimitare pentru tastaturile naționale

Tastaturile sunt proiectate pentru a corespunde cerințelor specifice fiecărei țări. Sintaxa și tastele utilizate pentru modificarea sau ștergerea parolei depind de tastatura livrată împreună cu computerul.

Caractere de delimitare pentru tastaturile naționale					
/	Arabă	-	Greacă	/	Rusă
=	Belgiană	.	Ebraică	-	Slovacă
-	BHCMSS*	-	Maghiară	-	Spaniolă
/	Braziliană	-	Italiană	/	Suedează/Finlandeză
/	Chineză	/	Japoneză	-	Elvețiană
-	Cehă	/	Coreeană	/	Taiwaneză
-	Daneză	-	Latino-americană	/	Thai
!	Franceză	-	Norvegiană	.	Turcă
é	Franceză canadiană	-	Poloneză	/	Engleză americană
-	Germană	-	Portugheză		

* Pentru Bosnia-Herțegovina, Croația, Muntenegru, Serbia și Slovenia

Ștergerea parolelor

Dacă uitați parola, nu aveți posibilitatea să accesați computerul. Pentru instrucțiuni despre ștergerea parolelor, consultați *Ghid de depanare*.

Dacă sistemul este echipat cu un dispozitiv de securitate încorporat, consultați *Ghidul managerului de securitate HP ProtectTools* de la adresa <http://www.hp.com>.

DriveLock (Blocare unitate)

Caracteristica DriveLock, disponibilă pentru anumite modele, este o caracteristică de securitate de standard industrial care împiedică accesul neautorizat la datele de pe unitățile de disc ATA. Caracteristica DriveLock a fost implementată ca o extensie la Computer Setup. Ea este disponibilă numai când sunt detectate unități de disc care acceptă setul de comenzi ATA Security (Securitate ATA). Caracteristica DriveLock se adresează clienților HP pentru care securitatea datelor reprezintă o preocupare extremă. Pentru asemenea clienți, costul unității de disc și al pierderii datelor stocate pe acesta sunt nesemnificative în comparație cu pagubele care pot rezulta din accesul neautorizat la conținutul său. Pentru a echilibra acest nivel de securitate cu necesitatea practică de a introduce o parolă uitată, implementarea de către HP a caracteristicii DriveLock implică o schemă de securitate cu două parole. Una dintre parole este stabilită și utilizată de un administrator de sistem, în timp ce cealaltă este în mod obișnuit stabilită și întrebuințată de utilizatorul final. Nu există nici o „portiuță” care să se utilizeze pentru a debloca unitatea dacă se pierd ambele parole. De aceea, caracteristica DriveLock se utilizează fără nici un risc atunci când datele conținute pe unitatea de disc sunt copiate pe un sistem de informații al firmei sau li s-au făcut cu regularitate copii de rezervă. În cazul în care se pierd ambele

parole DriveLock, unitatea de disc devine inutilizabilă. Pentru utilizatorii care nu corespund profilului de client definit anterior, acesta poate să fie un risc inacceptabil. Pentru utilizatorii care corespund profilului de client, acesta poate să fie un risc tolerabil datorită datelor stocate pe unitatea de disc.

Utilizarea DriveLock

Când se detectează una sau mai multe unități de disc care acceptă setul de comenzi ATA Security (Securitate ATA), opțiunea DriveLock apare sub meniul Security (Securitate) din Computer Setup. Utilizatorului îi sunt prezentate opțiunile de a stabili parola principală sau de a activa caracteristica DriveLock. Pentru a activa caracteristica DriveLock, trebuie introdusă o parolă de utilizator. Deoarece configurarea inițială a caracteristicii DriveLock este în mod obișnuit efectuată de un administrator, trebuie mai întâi stabilită o parolă principală. HP încurajează administratorii de sistem să stabilească o parolă principală, indiferent dacă intenționează să activeze caracteristica DriveLock sau să o păstreze dezactivată. Această îi dă administratorului posibilitatea să modifice setările DriveLock în cazul blocării ulterioare a unității. După stabilirea parolei principale, administratorul de sistem poate să activeze caracteristica DriveLock sau să o mențină dezactivată.

Dacă este prezentă o unitate de disc blocată, testarea POST va solicita o parolă pentru a o debloca. Dacă parola de pornire stabilită corespunde cu parola utilizatorului unității, testarea POST nu va solicita utilizatorului să reintroducă parola. În caz contrar, utilizatorului i se va solicita să introducă o parolă DriveLock. La o pornire la cald, se pot utiliza atât parola principală, cât și parola utilizatorului. La o pornire la cald, introduceți aceeași parolă pe care ați utilizat-o pentru a debloca unitatea în timpul pornirii la cald precedente. Utilizatorii vor avea dreptul la două încercări pentru a introduce o parolă corectă. La o pornire la cald, dacă nici una din încercări nu este reușită, testarea POST va continua, dar unitatea va rămâne inaccesibilă. La o pornire la cald sau la repornirea din Windows, dacă nici una dintre încercări nu reușește, testele POST se vor opri și utilizatorul va primi instrucțiuni să oprească și să repornească alimentarea.

Aplicații DriveLock

Cea mai practică utilizare a caracteristicii de securitate DriveLock este într-un mediu de întreprindere. Administratorul de sistem va fi responsabil de configurarea unității de disc, care va implica, printre altele, stabilirea parolei principale DriveLock și a unei parole de utilizator temporare. În cazul în care utilizatorul uită parola de utilizator sau dacă echipamentul este transferat unui alt angajat, parola principală poate fi utilizată întotdeauna pentru a restabili parola de utilizator și pentru a recăpăta accesul la unitatea de disc.

HP recomandă administratorilor de sisteme de întreprindere care optează pentru activarea caracteristicii DriveLock să stabilească și o politică de întreprindere pentru stabilirea și întreținerea parolelor principale. Acest lucru trebuie făcut pentru a împiedica situația în care un angajat, intenționat sau nu, stabilește ambele parole DriveLock înainte de a părăsi firma. Într-un asemenea scenariu, unitatea de disc ar deveni inutilizabilă și ar necesita înlocuirea. De asemenea, dacă nu stabilesc o parolă principală, administratorii de sistem se pot descoperi blocați față de o unitate de disc, fără a avea posibilitatea să efectueze verificări de rutină pentru software neautorizat și alte funcții de control al activelor sau să acorde asistență.

Pentru utilizatori cu cerințe de securitate mai puțin stringente, HP nu recomandă să se activeze caracteristica DriveLock. Printre utilizatorii din această categorie sunt incluși utilizatorii individuali sau utilizatorii care în mod obișnuit nu păstrează date sensibile pe unitățile de disc. Pentru acești utilizatori, pierderea potențială a unității de disc rezultată ca urmare a uitării ambelor parole este mult mai mare decât valoarea datelor pentru protecția cărora a fost concepută caracteristica DriveLock. Accesul la programul Computer Setup și la caracteristica DriveLock poate fi restricționat prin parola de setare. Prin specificarea unei parole de setare necunoscută de utilizatorii finali, administratorii de sistem au posibilitatea să restricționeze activarea caracteristicii DriveLock de către utilizatori.

Smart Cover Sensor (Senzor capac inteligent)

Cover Removal Sensor (Senzor pentru scoaterea capacului), disponibil la unele modele, este o combinație de tehnologie hardware și software care vă poate avertiza dacă s-a scos capacul sau panoul lateral de la computer. Există trei niveluri de protecție, după cum este descris în tabelul următor.


Tabelul 11-2 Niveluri de protecție ale senzorului Smart Cover (Capac inteligent)

Nivel	Setare	Descriere
Nivel 0	Dezactivat	Senzorul Smart Cover este dezactivat (implicit).
Nivel 1	Notificare utilizator	Când computerul este repornit, pe ecran se afișează un mesaj care indică faptul că a fost scos capacul computerului sau panoul lateral.
Nivel 2	Setup Password (Parolă de setare)	Când computerul este repornit, pe ecran se afișează un mesaj care indică faptul că a fost scos capacul computerului sau panoul lateral. Pentru a continua, trebuie să introduceți parola de setare.

NOTĂ: Aceste setări se pot modifica prin intermediul utilitarului Computer Setup. Pentru informații suplimentare despre programul Computer Setup, consultați *Ghidul programului utilitar Computer Setup (F10)*.


Setarea nivelului de protecție pentru Smart Cover Sensor (Senzor capac inteligent)


Pentru a stabili nivelul de protecție pentru Smart Cover Sensor (Senzor capac inteligent), urmați toți pașii de mai jos:

1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start > Închidere > Repornire**.
2. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare, pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.
 **NOTĂ:** Dacă nu ați apăsat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.
3. Selectați **Security (Securitate) > Smart Cover (Capac inteligent) > Cover Removal Sensor (Senzor pentru scoaterea capacului)**, apoi selectați nivelul de securitate dorit.
4. Înainte de a ieși, faceți clic pe **File (Fișier) > Save Changes and Exit (Salvare modificări și ieșire)**.

Smart Cover Lock (Zăvor capac inteligent)

Smart Cover Lock (Zăvor capac inteligent) este un dispozitiv de blocare a capacului, controlabil prin software, disponibil pentru unele computere HP. Acest dispozitiv de blocare împiedică accesul neautorizat la componentele interne. Computerul este livrat cu dispozitivul Smart Cover Lock (Zăvor capac inteligent) în poziție deblocată.


 **ATENȚIE:** Pentru securitatea maximă a capacului, stabiliți o parolă de setare. Parola de setare împiedică accesul neautorizat la utilitarul Computer Setup.

 **NOTĂ:** Dispozitivul Smart Cover Lock (Zăvor capac inteligent) este disponibil ca opțiune pentru unele sisteme.

Blocarea dispozitivului Smart Cover Lock (Zăvor capac inteligent)

Pentru a activa și bloca dispozitivul Smart Cover Lock (Zăvor capac inteligent), urmați toți pașii de mai jos:


1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start > Închidere > Repornire**.
2. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.

 **NOTĂ:** Dacă nu ați apăsat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

3. Selectați **Security** (Securitate) > **Smart Cover** (Capac inteligent) > **Cover Lock** (Zăvor de capac) > **Lock option** (Opțiune blocare).
4. Înainte de a ieși, faceți clic pe **File** (Fișier) > **Save Changes and Exit** (Salvare modificări și ieșire).

Deblocarea dispozitivului Smart Cover Lock (Zăvor capac inteligent)

1. Porniți sau reporniți computerul. Dacă sunteți în Windows, faceți clic pe **Start > Închidere > Repornire**.
2. Imediat după pornirea computerului, apăsați **F10** înaintea încărcării de către computer a sistemului de operare pentru a intra în programul Computer Setup. Dacă este necesar, apăsați tasta **Enter** pentru a trece de ecranul de titlu.

 **NOTĂ:** Dacă nu ați apăsat **F10** la momentul potrivit, trebuie să reporniți computerul și, înaintea încărcării de către computer a sistemului de operare, să apăsați din nou **F10** pentru a accesa utilitarul.

3. Selectați **Security** (Securitate) > **Smart Cover** (Capac inteligent) > **Cover Lock** (Zăvor de capac) > **Unlock** (Deblocare).
4. Înainte de a ieși, faceți clic pe **File** (Fișier) > **Save Changes and Exit** (Salvare modificări și ieșire).

Utilizarea cheii Smart Cover FailSafe

Dacă ați activat dispozitivul Smart Cover Lock (Zăvor capac inteligent) și nu aveți posibilitatea să introduceți parola pentru dezactivarea blocării, pentru a deschide capacul computerului aveți nevoie de o cheie Smart Cover FailSafe. Această cheie este necesară în oricare dintre următoarele circumstanțe:

- Întreruperea alimentării
- Pornire nereușită
- Defectarea unei componente a PC-ului (de exemplu, procesorul sau sursa de alimentare)
- Uitarea parolei

△ **ATENȚIE:** Cheia Smart Cover FailSafe este o unealtă specializată, disponibilă de la HP. Fiți pregătit: comandați această cheie, înainte de a vă fi necesară, de la un distribuitor sau furnizor de servicii autorizat.

Pentru a obține cheia FailSafe, aveți următoarele posibilități:

- Contactați un distribuitor sau furnizor de servicii HP autorizat.
- Apelați numărul corespunzător listat în certificatul de garanție.

Pentru informații suplimentare despre utilizarea cheii Smart Cover FailSafe, consultați *Ghid de referință hardware*.

Disponibilitate pentru dispozitiv de blocare cu cablu

Pe panoul din spatele computerului (la unele modele) se poate monta un dispozitiv de blocare cu cablu, astfel încât computerul să fie fixat fizic la o zonă de lucru.

Pentru instrucțiuni ilustrate, consultați *Ghid de referință hardware*.

Tehnologie de identificare a amprentelor

Prin eliminarea cerinței de a introduce parole de utilizator, HP Fingerprint Identification Technology (Tehnologie de identificare a amprentelor) îmbunătățește securitatea rețelei, simplifică procesul de conectare și reduce costurile asociate cu gestionarea rețelelor de întreprindere. Fiind disponibilă la un preț convenabil, aceasta nu se mai adresează exclusiv instituțiilor dotate cu înaltă tehnologie și înaltă securitate.

 **NOTĂ:** Acceptarea tehnologiei de identificare a amprentelor diferă de la un model la altul.

Notificarea și remedierea defectelor

Caracteristicile de notificare și remediere a defectelor combină tehnologii inovatoare hardware și software pentru a împiedica pierderea de date importante și pentru a minimiza perioadele neplanificate de neutilizare.

În cazul în care computerul este conectat la o rețea gestionată de HP Client Manager, computerul trimite o notificare despre defecțiune spre aplicația de gestionare a rețelei. Cu software-ul HP Client Manager aveți, de asemenea, posibilitatea să programați de la distanță executarea automată a programelor de diagnosticare pe toate computerele gestionate și crearea unui raport succint despre testele eșuate.

Drive Protection System (Sistem de protecție a unităților)

Sistemul de protecție a unităților (DPS) este un instrument de diagnosticare încorporat în unitățile de disc instalate la unele computere HP. Sistemul DPS a fost conceput pentru a ajuta la diagnosticarea problemelor care pot avea ca rezultat înlocuirea nejustificată a unităților de disc.

Când sunt construite computerele HP, fiecare unitate de disc instalată este testată utilizând sistemul DPS, iar pe unitate se scrie o înregistrare permanentă cu informații esențiale. Rezultatele testării sunt scrise pe unitatea de disc de fiecare dată când se execută sistemul DPS. Furnizorul de servicii poate să utilizeze aceste informații pentru a determina condițiile care au impus executarea software-ului DPS. Pentru instrucțiuni despre utilizarea sistemului DPS, consultați *Ghid de depanare*.

Sursa de alimentare cu toleranță la supratensiune

O sursă integrată de alimentare cu toleranță la supratensiune oferă o mai mare siguranță în funcționare când la computer ajunge o supratensiune neprevăzută. Această sursă de alimentare este calculată pentru a rezista la o supratensiune de până la 2000 V, fără să rezulte opriri ale sistemului sau pierderi de date.

Senzor termic

Senzorul termic este o caracteristică hardware și software care urmărește temperatura internă a computerului. Această caracteristică afișează un mesaj de atenționare când s-a depășit intervalul normal, ceea ce vă permite să acționați în timp util, înaintea deteriorării componentelor interne sau a pierderii de date.

△ **ATENȚIE:** Temperatura ridicată poate avea ca rezultat deteriorarea sistemului sau pierderea de date.

Index

Simboluri/Numerice

ștergerea parolei 32
ștergerea parolelor 33

A

acces la computer, control 26
actualizare de la distanță a
memoriei ROM 15
actualizare ROM 15
adrese de Internet. *Vezi* site-uri
Web
Altiris
 AClient 3
 agentul soluției de
 desfășurare 3
 Client Management Suite 10

B

Backup and Recovery
Manager 11
BIOS
 actualizare de la distanță a
 memoriei ROM 15
 Boot Block Emergency
 Recovery Mode (Mod de
 recuperare de urgență a
 blocului de încărcare) 16
 HPQFlash 15
blocarea dispozitivului Smart Cover
Lock (Zăvor capac
inteligent) 36
blocare capac 35
Boot Block Emergency Recovery
Mode (Mod de recuperare de
urgență a blocului de
încărcare) 16
buton de alimentare cu două
stări 23

C

caractere de delimitare, tabel 33
caractere de delimitare pentru
tastaturile naționale 33
caractere de delimitare pe tastaturi,
naționale 33
cheie FailSafe, comandare 36
cheie Smart Cover FailSafe,
comandare 36
Client Management Interface
(Interfață pentru gestionarea
sistemelor client) 5
Client Manager from Symantec 9
comandare cheie FailSafe 36
configurare
 inițială 2
configurare buton de
alimentare 23
configurație buton de
alimentare 23
configurație inițială 2
configurații de instalare,
multiplicare 18
controlul accesului la
computer 26

D

deblocarea dispozitivului Smart
Cover Lock (Zăvor capac
inteligent) 36
disponibilitate pentru dispozitiv de
blocare cu cablu 37
dispozitiv de încărcare
 creare 20
 dispozitiv de memorie flash
 USB 20
dispozitiv de memorie flash USB, de
încărcare 20, 21
DriveLock (Blocare unitate) 33

H

HP
 Backup and Recovery
 Manager 11
 Client Automation, edițiile
 Starter, Standard și
 Enterprise 8
 Client Catalog pentru produse
 Microsoft System Center &
 SMS 10
 Client Management Interface
 (Interfață pentru gestionarea
 sistemelor client) 5
 Client Manager from
 Symantec 9
 ProtectTools Security Manager
 (Manager de securitate
 ProtectTools) 7
 System Software Manager
 (Manager al software-ului de
 sistem) 7
HPQFlash 15

I

image software preinstalat 2
instalare
 copierea pe un singur
 computer 18
 copiere pe mai multe
 computere 19
instalare de la distanță 4
instrument de diagnosticare pentru
unități de disc 37
instrumente de clonare,
software 2
instrumente de desfășurare,
software 2
introducere
 parolă de pornire 31
 parolă de setare 31

- M**
 mod de recuperare, urgență la
 blocul de încărcare 16
 mod de recuperare de urgență, bloc
 de încărcare 16
 modificarea parolei 32
- N**
 notificare a modificărilor 14
 notificare modificări 14
 notificare și remediere defecte 37
- P**
 parolă
 instalare 30, 31
 modificare 32
 pornire 30, 31
 securitate 30
 ștergere 32, 33
 parolă de pornire
 introducere 31
 modificare 32
 setare 30
 ștergere 32
 parolă de setare
 introducere 31
 modificare 32
 setare 30
 ștergere 32
 Proactive Change Notification
 (PCN) 14
 ProtectTools Security Manager
 (Manager de securitate
 ProtectTools) 7
 protejarea unității de disc 37
 PXE (Mediu de execuție înainte de
 încărcarea sistemului) 4
- R**
 recuperare, software 2
 Remote System Installation
 (Instalarea de la distanță a
 sistemului) 4
- S**
 schimbare sistem de operare,
 asistență 24
 securitate
 caracteristici, tabel 26
 dispozitiv de blocare cu
 cablu 37
 DriveLock (Blocare
 unitate) 33
 parolă 30
 ProtectTools Security Manager
 (Manager de securitate
 ProtectTools) 7
 setări 26
 Smart Cover Lock (Zăvor capac
 inteligent) 35
 Smart Cover Sensor (Senzor
 capac inteligent) 35
 tehnologie de identificare a
 amprentelor 37
 senzor termic 38
 sisteme de operare, asistență
 pentru schimbare 24
 site-uri Web
 actualizare de la distanță a
 memoriei ROM 15
 actualizare ROM 15
 Altiris Client Management
 Suite 10
 asistență HP 11, 12
 asistență software 24
 Configuration Management 3
 descărcare BIOS 15
 descărcări de software și
 drivere 19
 HP Business PC Security 8
 HP Client Automation
 Center 8
 HP Client Catalog for Microsoft
 SMS 10
 HP Client Management
 Interface 6
 HP Client Management
 Solutions 3
 HP Client Manager from
 Symantec 9
 HPQFlash 15
 HP Softpaq Download
 Manager 6
 HP System Software
 Manager 7
 Proactive Change
 Notification 14
 Subscriber's Choice 14
 tehnologie Intel vPro 12
 Smart Cover Lock
 cheie FailSafe 36
 Smart Cover Lock (Zăvor capac
 inteligent)
 blocare 36
 deblocare 36
 Smart Cover Sensor (Senzor capac
 inteligent)
 niveluri de protecție 35
 setare 35
 software
 agentul soluției de desfășurare
 Altiris 3
 Altiris AClient 3
 Altiris Client Management
 Suite 10
 desfășurare 2
 Drive Protection System (Sistem
 de protecție a unităților) 37
 HP Backup and Recovery
 Manager 11
 HP Client Automation, edițiile
 Starter, Standard și
 Enterprise 8
 HP Client Catalog pentru
 produse Microsoft System
 Center & SMS 10
 HP Client Management
 Interface 5
 HP Client Manager from
 Symantec 9
 HP ProtectTools Security
 Manager 7
 HP System Software
 Manager 7
 instrumente de actualizare și
 gestionare 5
 integrare 2
 Proactive Change Notification
 (PCN) 14
 recuperare 2
 Remote System Installation
 (Instalarea de la distanță a
 sistemului) 4
 Tehnologia de gestionare 12
 urmărire active 26
 Verdiem Surveyor 14
 soluții retrase 14
 standarde în domeniu 25
 Subscriber's Choice (Opțiunea
 abonatului) 14

Suport PXE (Mediu de execuție înainte de încărcarea sistemului) 4
sursă de alimentare, toleranță la supratensiune 38
sursă de alimentare cu toleranță la supratensiune 38
System Software Manager (Manager al software-ului de sistem) 7

T

tehnologia de gestionare 12
tehnologie de identificare a amprentelor 37
temperatura internă a computerului 38
temperatură, interiorul computerului 38

U

unitate, protejare 37
unități de disc, instrument de diagnosticare 37
urmărire active 26

V

Verdiem Surveyor 14