Guida di Desktop Management
Business Desktops

Numero di parte del documento: 361202-061

Maggio 2004

Contiene definizioni e istruzioni per l'uso delle caratteristiche di sicurezza e Intelligent Manageability preinstallate in alcuni modelli.

AVVERTENZA: Il testo presentato in questo modo indica che la mancata osservanza delle istruzioni potrebbe comportare lesioni fisiche o addirittura la perdita della vita.

ATTENZIONE: Il testo presentato in questo modo indica che la mancata osservanza delle relative istruzioni può causare danni alle apparecchiature o perdite di informazioni.

Guida di Desktop Management
Business Desktops
Prima edizione Maggio 2004
Numero di parte del documento: 361202-061

Sommario

Guida di Desktop Management

Configurazione iniziale e deployment 2
Installazione remota del sistema 2
Gestione e aggiornamento del software 3
HP Client Manager Software 3
Altiris Client Management Solutions 4
System Software Manager 5
Proactive Change Notification 5
Subscriber's Choice 6
Flash su ROM 6
Flash remoto della ROM 7
HPQFlash 7
ROM con blocco di avviamento FailSafe 7
Replica delle impostazioni 9
Pulsante d'accensione a doppio stato 19
Sito World Wide Web 20
Moduli e collaboratori 20
Controllo e sicurezza degli Asset 21
Sicurezza tramite password 27
Impostazione di una password di configurazione tramite Computer Setup 27
Immissione della password di accensione con Computer Setup 28
DriveLock 33
Sensore Smart Cover 35
Chiusura Smart Cover 36
Master Boot Record Security (Sicurezza MBR (Master Boot Record)) 39
Partizionamento e formattazione del disco avviabile corrente 41
Predisposizione per chiusura con cavo 41
Tecnologia per l'identificazione delle impronte digitali 42

Notifica guasti e ripristino 42
Drive Protection System (DPS) 42
Alimentatore protetto contro gli sbalzi di tensione 43
Sensore termico 43

Indice Analitico

Guida di Desktop Management

HP Intelligent Manageability fornisce soluzioni standard per la gestione ed il controllo di PC desktop, workstation e portatili in ambienti di rete. HP propone soluzioni per la gestione dei desktop fin dal 1995, con l'introduzione sul mercato dei primi personal computer completamente gestibili. HP dispone di una tecnologia di gestione brevettata, grazie alla quale ha condotto un incessante sforzo per sviluppare gli standard e le infrastrutture occorrenti per il deployment, la configurazione e la gestione efficaci di PC desktop, workstation e portatili. Intelligent Manageability è un elemento importante del grande impegno che HP ha posto nella realizzazione di soluzioni relative al ciclo vitale del PC, in grado di seguire l'utente nelle quattro fasi della pianificazione, deployment, gestione e transizioni.

Le funzioni e caratteristiche principali della gestione desktop sono:

- Configurazione iniziale e deployment
- Installazione remota del sistema
- Aggiornamento e gestione del software
- Flash della ROM
- Controllo e sicurezza asset
- Notifica e riparazione dei guasti

Il supporto di funzioni specifiche descritte in questa guida può variare in base al modello e alla versione del software.

Configurazione iniziale e deployment

Il computer viene fornito con un'immagine del software di sistema preinstallata. Dopo una veloce fase di "scompattamento" del software il computer è pronto per l'uso.

Potrebbe rivelarsi necessario sostituire l'immagine del software preinstallata con un set personalizzato di software applicativi e di sistema. In tal caso, esistono vari metodi per personalizzare il software. È possibile operare come segue:

- Installare il software applicativo aggiuntivo dopo aver scompattato l'immagine del software preinstallata.
- Utilizzare strumenti di deployment come Altiris Deployment Solution™ per sostituire il software preinstallato con un'immagine del software personalizzata.
- Eseguire una procedura di clonazione del disco per copiare il contenuto da un disco fisso ad un altro.

Il metodo di messa in uso da scegliere dipende dai processi e dagli ambienti informatici degli utenti. La sezione PC Deployment del sito Web HP Lifecycle Solutions (http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html) fornisce informazioni utili alla scelta del metodo di deployment migliore.

Il CD *Restore Plus!* l'installazione da ROM e l'hardware compatibile ACPI forniscono ulteriore assistenza per il ripristino del software di sistema, la gestione e la soluzione dei problemi di configurazione e la gestione dell'alimentazione.

Installazione remota del sistema

L'installazione remota del sistema consente di avviare e impostare il sistema utilizzando il software e le informazioni di configurazione situati in un server di rete tramite il Preboot Execution Environment (PXE). La funzione di installazione remota del sistema viene di solito utilizzata come strumento di impostazione e configurazione del sistema e può servire ai seguenti scopi:

- Formattazione di un disco fisso
- Deployment di una copia del software su uno o più PC nuovi
- Aggiornamento a distanza del BIOS nella flash ROM ("Flash remoto della ROM" a pagina 7)
- Configurazione dei parametri del BIOS

Per avviare l'installazione remota del sistema premere **F12** quando viene visualizzato il messaggio F12 = Avvio servizio di rete nell'angolo inferiore sinistro della schermata del logo HP. Per proseguire seguire le istruzioni sullo schermo. La sequenza di avvio predefinita viene configurata nel BIOS e può essere modificata in modo da provare ad avviare sempre da PXE.

HP e Altiris si sono associate per poter fornire strumenti progettati per facilitare il compito di unire installazione e gestione del PC con meno dispendio di tempo, riducendo infine i costi totali di proprietà e rendendo i PC HP i più gestibili PC client nell'ambiente aziendale.

Gestione e aggiornamento del software

HP ha dotato desktop e workstation di diversi strumenti per la gestione e l'aggiornamento del software: HP Client Manager Software, Client Management Solutions, System Software Manager; Proactive Change Notification e Subscriber's Choice.

HP Client Manager Software

HP Client Manager Software (HP CMS) assiste i clienti HP nella gestione degli aspetti hardware dei rispettivi client con le seguenti caratteristiche:

- Elenchi dettagliati dei componenti hardware per la gestione delle risorse
- Monitoraggio e diagnostica dello stato del PC
- Notifica proattiva di modifiche nell'ambiente hardware
- Report accessibile da Web di particolari di estrema importanza come macchine con sistemi di allarmi di temperatura, di memoria ed altro ancora
- Aggiornamento a distanza di software di sistema, ad esempio driver e BIOS della ROM
- Modifica a distanza della sequenza di avvio

Per ulteriori informazioni su HP Client Manager consultare http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Client Management Solutions

HP e Altiris si sono associate per fornire soluzioni di gestione dei sistemi esaustive e del tutto integrate per ridurre il costo di esercizio dei PC client HP. HP Client Manager Software costituisce la base per ulteriori Altiris Client Management Solutions per:

- Gestione componenti hardware e risorse
  - Verifica licenze software
  - Monitoraggio e reporting PC
  - Contratto di leasing, monitoraggio risorse
- Installazione e migrazione
  - Migrazione a Microsoft Windows XP Professional o Home Edition
  - Deployment del sistema
  - Migrazioni personalizzate
- Help Desk e risoluzione dei problemi
  - Gestione richieste di intervento help desk prepagate
  - Individuazione dei problemi a distanza
  - Risoluzione dei problemi a distanza
  - Recupero disastro client
- Gestione software e operativa
  - Gestione corrente desktop
  - Installazione software di sistema HP
  - Autoeliminazione dei guasti

Per ulteriori informazioni e particolari sulle modalità di download di una copia di valutazione valida 30 giorni completa di tutte le funzioni consultare http://h18000.www1.hp.com/im/prodinfo.html#deploy.

Su determinati modelli di computer desktop e notebook è previsto un agente di gestione Altiris che fa parte dell'immagine caricata di fabbrica. Questo agente consente la comunicazione con Altiris Development Solution, utilizzabile per completare l'installazione di nuovo hardware o migrazione personalizzata ad un nuovo sistema operativo tramite una semplice procedura guidata. Le soluzioni Altiris prevedono funzioni di distribuzione software di facile uso. In abbinamento a System Software Manager, o HP Client Manager Software, gli amministratori sono anche in grado di aggiornare il BIOS su ROM e i driver di periferica da una consolle centrale.

Per ulteriori informazioni consultare http://h18000.www1.hp.com/im/client_mgr.html.

System Software Manager

System Software Manager (SSM) è un'utility che consente di aggiornare il software a livello di sistema su più PC contemporaneamente. Se eseguita su un sistema client del PC, SSM rileva le versioni hardware e software, quindi aggiorna il software appropriato attingendo da un apposito archivio centrale. Le versioni dei driver supportati da SSM sono indicate con un'icona particolare nel sito Web dal quale scaricare i driver e sul CD del software di supporto. Per scaricare l'utility o per ulteriori informazioni su SSM consultare http://www.hp.com/go/ssm.

Proactive Change Notification

Il programma Proactive Change Notification utilizza il sito Web Subscriber's Choice per effettuare in modo proattivo ed automatico le seguenti operazioni:

- Invio di messaggi di posta elettronica PCN (Proactive Change Notification) contenenti informazioni sulle modifiche hardware e software alla maggior parte dei computer e server commerciali, con un preavviso massimo di 60 giorni.
- Invio di messaggi di posta elettronica Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins e Driver che segnalano problemi per la maggior parte dei computer e server commerciali.

Creazione di profili personalizzati per ricevere esclusivamente le informazioni relative ad uno specifico ambiente informatico. Per saperne di più sul programma Proactive Change Notification e creare un profilo personalizzato consultare http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn.

Subscriber's Choice

Il servizio Subscriber's Choice è un servizio HP riservati ai clienti. Sulla base del profilo del cliente, HP fornisce consigli personalizzati sui prodotti, articoli specialistici e/o driver e avvertenze/notifiche relative all'assistenza. Subscriber's Choice Driver and Support Alerts/Notifications invia un messaggio di posta elettronica che sono disponibili le nuove informazioni del tipo prescelto. Per saperne di più su Subscriber's Choice e creare un profilo personalizzato consultare http://h30046.www3.hp.com/subhub.php.

Flash su ROM

Il computer è dotato di una flash ROM programmabile. Con la definizione di una password di configurazione in Computer Setup (F10) è possibile proteggere la ROM in modo che non venga involontariamente aggiornata o sovrascritta. Si tratta di un aspetto importante per garantire l'integrità operativa del PC. Dovendo o volendo aggiornare la ROM, è possibile:

- Richiedere ad HP un dischetto con ROMPaq aggiornato.
- Scaricare le ultime immagini ROMPaq dalla pagina driver e supporto HP http://www.hp.com/support/files.

ATTENZIONE: Per garantire la massima protezione della ROM, è bene impostare una password di configurazione. La password di impostazione impedisce gli aggiornamenti non autorizzati della ROM. System Software Manager consente all'amministratore di sistema di impostare la password di impostazione su uno o più PC contemporaneamente. Per ulteriori informazioni consultare http://www.hp.com/go/ssm.

Flash remoto della ROM

Il flash remoto della ROM consente all'amministratore di sistema di aggiornare in condizioni di sicurezza la ROM dei PC HP remoti direttamente dalla consolle di gestione centralizzata della rete. La possibilità per l'amministratore di sistema di eseguire questa operazione a distanza su più PC si traduce in un deployment coerente ed in un maggior controllo delle immagini ROM dei PC HP in rete. Inoltre, ne derivano una maggiore produttività e una diminuzione del costo totale della proprietà.

Per l'esecuzione del flash remoto della ROM, il computer deve essere acceso o attivato tramite l'Apri sessione remoto.

Per ulteriori informazioni sul flash remoto della ROM vedere HP Client Manager Software o System Software Manager su http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

L'utility HPQFlash viene utilizzata per aggiornare localmente o ripristinare la ROM di sistema su singoli PC tramite un sistema operativo Windows.

Per ulteriori informazioni su HPQFlash consultare http://www.hp.com/support/files ed inserire il nome del computer quando viene richiesto.

ROM con blocco di avviamento FailSafe

La ROM con blocco di avvio FailSafe consente il ripristino del sistema nel caso, improbabile, che il flash della ROM non dovesse riuscire, ad esempio in seguito ad interruzione dell'alimentazione durante l'aggiornamento della ROM. Il blocco dell'avvio è una sezione della ROM con protezione flash che effettua un controllo di convalida della ROM ogni volta che il sistema viene acceso.

- Se la ROM di sistema è valida, il sistema parte normalmente.
- Se la ROM di sistema non supera il controllo di convalida, la ROM con blocco di avvio FailSafe fornisce supporto sufficiente per l'avvio del sistema da un dischetto ROMPaq che programmi la ROM con un'immagine valida.

Alcuni modelli supportano anche il ripristino da un CD ROMPaq. Le immagini ISO ROMPaq sono incluse con determinati modelli nei softpaq ROM scaricabili.

Quando il blocco di avvio rileva una ROM di sistema non valida, il LED di alimentazione di sistema emette una luce lampeggiante di colore ROSSO 8 volte, una al secondo, e fa una pausa di 2 secondi. Contemporaneamente vengono emessi 8 segnali acustici. A video appare un messaggio che indica la modalità di ripristino del blocco di avvio (in alcuni modelli).

Per ripristinare il sistema in modalità di ripristino blocco di avvio procedere come di seguito indicato:

1. In caso di presenza di dischetto nell'unità a dischetti o di CD nel lettore CD, togliere dischetto e CD e spegnere il computer.
2. Inserire un dischetto ROMPaq nell'unità a dischetti o, se consentito dal computer, un CD ROMPaq nel lettore CD.
3. Accendere il computer.

   Se non vengono rilevati dischetti o CD ROMPaq il sistema ne richiede l'introduzione ed il riavvio del computer.

   Se è stata impostata una password di configurazione, si accende la spia del blocco delle maiuscole e il sistema richiede l'inserimento della password.
4. Digitare la password di configurazione.

   Se il sistema riesce a a portare a termine l'avviamento dal dischetto e a riprogrammare la ROM, si accendono le tre spie della tastiera. Il successo dell'operazione viene inoltre segnalato da una serie di segnali acustici di tono crescente.
5. Togliere il dischetto o il CD e spegnere il computer.
6. Accendere o riavviare il computer.

La seguente tabella elenca le diverse combinazioni delle spie della tastiera utilizzate dalla ROM con blocco di avvio (quando al computer è collegata una tastiera PS/2) con i relativi significati e procedure.

Combinazioni delle spie della tastiera utilizzate dalla ROM con blocco di avvio

Modalità blocco di avvio FailSafe	Colore del LED della tastiera	Tastiera del LED della tastiera	Stato/Messaggio
Bloc Num	Verde	Acceso	Dischetto o CD ROMPaq non presente, danneggiato o non pronto.
Bloc Maiusc	Verde	Acceso	Immettere la password.
Bloc Num, Maiusc, Scorr	Verde	Emissione sequenziale di luce lampeggiante, una alla volta: N, C, SL	Tastiera bloccata in modalità rete.
Bloc Num, Maiusc, Scorr	Verde	Acceso	Flash della ROM con blocco dell'avvio eseguito con successo. Spegnere e riaccendere.

✎ Le spie diagnostiche non lampeggiano su tastiere USB.

Replica delle impostazioni

Le seguenti procedure offrono all'amministratore di sistema la possibilità di copiare facilmente le impostazioni di un computer su altri computer dello stesso modello. Ciò consente una configurazione più veloce e uniforme di più computer.

✎ In entrambe le procedure è necessaria un'unità a dischetti oppure un dispositivo flash media USB compatibile, come HP Drive Key.

Copia su computer singolo

ATTENZIONE: La configurazione è specifica per ogni modello. Se i computer d'origine e di destinazione non sono dello stesso modello il file system può subire danni. È sconsigliabile, ad esempio, la copia della configurazione di un dc7100 Ultra-slim Desktop su un dx6100 Slim Tower.

1. Selezionare una configurazione da copiare. Spegnere il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Arresta il sistema**.
2. Se si utilizza un dispositivo flash media USB, inserirlo.
3. Accendere il computer.
4. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

5. Se si utilizzano i dischetti, inserirne uno.
6. Fare clic su **File > Replicated Setup (Impostazioni replicate) > Save to Removable Media (Salva su supporti removibili)**. Per creare il dischetto di configurazione o il dispositivo flash media USB seguire le istruzioni a video.
7. Spegnere il computer da configurare ed inserire il dischetto di configurazione o il dispositivo flash media USB.
8. Accendere il computer.
9. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.
10. Fare clic su **File > Replicated Setup (Impostazioni replicate) > Restore from Removable Media (Ripristina da supporti removibili)**, e seguire le istruzioni a video.
11. Riavviare il computer al termine della configurazione.

Copia su più computer

ATTENZIONE: La configurazione è specifica per ogni modello. Se i computer d'origine e di destinazione non sono dello stesso modello il file system può subire danni. È sconsigliabile, ad esempio, la copia della configurazione di un dc7100 Ultra-slim Desktop su un dx6100 Slim Tower.

Questo metodo richiede un po'più di tempo per preparare il dischetto di configurazione o il dispositivo flash media USB, ma la copia della configurazione sui computer di destinazione avviene molto più rapidamente.

Per questa procedura o per creare un dispositivo flash media USB avviabile è necessario un dischetto avviabile. Se non è possibile utilizzare Windows XP per creare un dischetto avviabile, utilizzare il metodo di copiatura su un singolo computer (vedere "Copia su computer singolo" a pagina 10).

1. Creare un dischetto avviabile o un dispositivo flash media USB. Vedere "Dispositivi flash media USB supportati" a pagina 13, o "Dispositivi flash media USB non supportati" a pagina 16.

ATTENZIONE: Non tutti i computer possono essere avviati da un dispositivo flash media USB. Se nella sequenza d'avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, significa che è possibile avviare il computer dal dispositivo flash media USB. Altrimenti, si deve utilizzare un dischetto avviabile.

2. Selezionare una configurazione da copiare. Spegnere il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Arresta il sistema**.
3. Se si utilizza un dispositivo flash media USB, inserirlo.
4. Accendere il computer.

5. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

6. Se si utilizzano i dischetti, inserirne uno.
7. Fare clic su **File > Replicated Setup (Impostazioni replicate) > Save to Removable Media (Salva su supporti removibili)**. Per creare il dischetto di configurazione o il dispositivo flash media USB seguire le istruzioni a video.
8. Scaricare un'utility BIOS per la replica della configurazione (repset.exe) e copiarla nel dischetto di configurazione o nel dispositivo flash media USB. Per scaricare l'utility andare su http://welcome.hp.com/support/files ed inserire il numero di modello del computer.
9. Nel dischetto di configurazione o nel dispositivo flash media USB creare un file autoexec.bat contenente il comando seguente:

   repset.exe
10. Spegnere il computer da configurare. Inserire il dischetto di configurazione o il dispositivo flash media USB e riaccendere il computer. L'utility di configurazione si avvia automaticamente.
11. Al termine della configurazione riavviare il computer.

Creazione di un dispositivo avviabile

Dispositivi flash media USB supportati

Nei dispositivi supportati, ad esempio HP Drive Key o DiskOnKey, è preinstallata un'immagine che semplifica la procedura necessaria per renderli avviabili. Se nel dispositivo flash media USB in uso non è presente l'immagine, utilizzare la procedura descritta più avanti in questa sezione (vedere "Dispositivi flash media USB non supportati" a pagina 16).

ATTENZIONE: Non tutti i computer possono essere avviati da un dispositivo flash media USB. Se nella sequenza d'avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, significa che è possibile avviare il computer dal dispositivo flash media USB. Altrimenti, si deve utilizzare un dischetto avviabile.

Condizioni per la creazione di un dispositivo flash media USB avviabile:

- Uno dei seguenti sistemi:
  - HP Compaq Business Desktop dc7100 series
  - HP Compaq Business Desktop dx6100 series
  - HP Compaq Business Desktop d530 Series – Ultra-Slim Desktop, Small Form Factor o Convertible Minitower
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 Minitower convertibile/Small Form Factor

  A seconda del tipo di BIOS, è possibile che in futuro altri sistemi supportino l'avvio da un dispositivo flash media USB.

ATTENZIONE: Se si usa un computer non presente in elenco, verificare che nella sequenza di avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB sia elencato prima del disco fisso.

- Uno dei seguenti moduli di memoria:
  - HP Drive Key da 16 MB
  - HP Drive Key da 32 MB
  - DiskOnKey da 32 MB
  - HP Drive Key da 64 MB
  - DiskOnKey da 64 MB
  - HP Drive Key da 128 MB
  - DiskOnKey da 128 MB
  - HP Drive Key da 256 MB
  - DiskOnKey da 256 MB
- Un dischetto DOS avviabile con i programmi FDISK e SYS. Se SYS non è disponibile, si può utilizzare FORMAT, ma in questo caso tutti i file esistenti sul dispositivo flash media USB andranno perduti.

1. Spegnere il computer.
2. Inserire il dispositivo flash media USB in una delle porte USB del computer e togliere tutte le altre periferiche di memorizzazione USB tranne le unità a dischetti USB.
3. Inserire nell'unità a dischetti un dischetto DOS avviabile con FDISK.COM e SYS.COM o FORMAT.COM e accendere il computer per avviare il dischetto DOS.
4. Per eseguire FDISK da A:\ prompt digitare **FDISK** e premere Invio. Alla richiesta del sistema, fare clic su **Yes (Y)** per abilitare la compatibilità con dischi di grandi dimensioni.
5. Inserire l'opzione **[5]** per visualizzare le unità presenti nel sistema. L'unità più simile per dimensioni ad una di quelle elencate è il dispositivo flash media USB. Di solito è l'ultima dell'elenco. Annotare la lettera dell'unità.

   Unità dispositivo flash media USB: _____

ATTENZIONE: Se un'unità non corrisponde al dispositivo flash media USB, non proseguire, potrebbe verificarsi perdita di dati. Verificare su tutte le porte USB la presenza di ulteriori dispositivi di memorizzazione. Se ve ne sono, toglierli, riavviare il computer e procedere col punto 4. Se non se ne trovano, significa che il sistema non supporta i dispositivi flash media USB o che il dispositivo flash media USB è difettoso. NON proseguire tentare di rendere avviabile un dispositivo flash media USB.

6. Per uscire da FDISK premere il tasto **Esc** per ritornare al prompt A:\.
7. Se il dischetto DOS avviabile contiene SYS.COM, passare al punto 8. Altrimenti, passare al punto 9.
8. Al prompt A:\ digitare **SYS x:** dove x rappresenta la lettera dell'unità sopra annotata.

ATTENZIONE: Verificare di avere inserito la lettera di unità corretta per il dispositivo flash media USB.

Una volta trasferiti i file di sistema, SYS ritorna al prompt A:\. Passare al punto 13.

9. Copiare eventuali file da conservare dal dispositivo flash media USB su una directory temporanea di un'altra unità (ad esempio, il disco fisso interno del sistema).
10. Al prompt A:\ digitare **FORMAT /S X:** dove X rappresenta la lettera dell'unità sopra annotata.

ATTENZIONE: Verificare di avere inserito la lettera di unità corretta per il dispositivo flash media USB.

FORMAT visualizza uno o più messaggi di avvertenza e ogni volta chiede se si vuole procedere. Inserire **Y** ogni volta. FORMAT formatta il dispositivo flash media USB, aggiunge i file di sistema e chiede di inserire un'etichetta di volume.

11. Premere **Invio** per non inserire nessuna etichetta o digitarne l'eventuale testo.
12. Ricopiare sul dispositivo flash media USB gli eventuali file salvati al punto 9.
13. Togliere il dischetto e riavviare il computer. Il computer si avvia con il dispositivo flash media USB come unità C.

La sequenza d'avvio predefinita varia da computer a computer, e può essere modificata nell'utility Computer Setup (F10).

Se si è utilizzata una versione DOS di Windows 9x, è possibile che appaia una schermata con il logo di Windows. Per non far apparire questa schermata, aggiungere un file di zero byte con nome LOGO.SYS alla directory principale del dispositivo flash media USB.

Ritornare a "Copia su più computer" a pagina 11.

Dispositivi flash media USB non supportati

ATTENZIONE: Non tutti i computer possono essere avviati da un dispositivo flash media USB. Se nella sequenza d'avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, significa che è possibile avviare il computer dal dispositivo flash media USB. Altrimenti, si deve utilizzare un dischetto avviabile.

Per creare un dispositivo flash media USB avviabile è necessario avere:

- Uno dei seguenti sistemi:
  - HP Compaq Business Desktop dc7100 series
  - HP Compaq Business Desktop dx6100 series
  - HP Compaq Business Desktop d530 Series – Ultra-slim Desktop, Small Form Factor o Minitower convertibile
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 Minitower convertibile/Small Form Factor

  A seconda del tipo di BIOS, è possibile che in futuro altri sistemi supportino l'avvio da un dispositivo flash media USB.

ATTENZIONE: Se non si utilizza un computer presente nell'elenco sopra riportato, verificare che nella sequenza di avvio predefinita dell'utility Computer Setup (F10) il dispositivo USB si trovi prima dell'unità disco rigido.

- Un dischetto DOS avviabile con i programmi FDISK e SYS. Se SYS non è disponibile, si può utilizzare FORMAT, ma in questo caso tutti i file esistenti sul dispositivo flash media USB andranno perduti.

1. Se sul sistema sono installate schede PCI relative ad unità SCSI, ATA RAID o SATA, spegnere il computer e scollegare il cavo d'alimentazione.

ATTENZIONE: Il cavo d'alimentazione DEVE essere scollegato.

2. Aprire il computer e togliere le schede PCI.
3. Inserire il dispositivo flash media USB in una delle porte USB del computer e togliere tutti gli altri dispositivi di memorizzazione USB tranne l'unità a dischetti USB. Chiudere il coperchio del computer.
4. Ricollegare il computer ed accenderlo.
5. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

6. Andare su **Advanced (Avanzate) > PCI Devices (Periferiche PCI)** e disabilitare i controller PATA e SATA. Quando si disabilita il controller SATA, annotare l'IRQ al quale viene assegnato il controller, in quanto lo si dovrà riassegnare in seguito. Confermare le modifiche per uscire dalla procedura di configurazione.

   IRQ SATA: _____

7. Inserire nell'unità a dischetti un dischetto DOS avviabile con FDISK.COM e SYS.COM o FORMAT.COM e accendere il computer per avviare il dischetto DOS.
8. Eseguire FDISK e cancellare eventuali partizioni esistenti sul dispositivo flash media USB. Creare una nuova partizione e segnarla come attiva. Per uscire da FDISK premere il tasto **Esc**.
9. Se il sistema non si riavvia automaticamente all'uscita da FDISK, premere **Ctrl+Alt+Del** per riavviarlo dal dischetto DOS.

10. Al prompt A:\ digitare **FORMAT C: /S** e premere **Invio**. FORMAT formatta il dispositivo flash media USB, aggiunge i file di sistema e richiede l'immissione di un'etichetta di volume.
11. Premere **Invio** per non inserire nessuna etichetta o digitarne l'eventuale testo.
12. Spegnere il computer e scollegare il cavo d'alimentazione. Aprire il computer e reinstallare eventuali schede PCI tolte in precedenza. Chiudere il coperchio del computer.
13. Ricollegare il cavo d'alimentazione, togliere il dischetto e riaccendere il computer.
14. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.
15. Andare su **Advanced (Avanzate) > PCI Devices (Periferiche PCI)** e riabilitare i controller PATA e SATA disabilitati al punto 6. Riassegnare al controller SATA l'IRQ originale.
16. Salvare le modifiche e uscire. Il computer si avvia con il dispositivo flash media USB come unità C.

La sequenza d'avvio predefinita varia da computer a computer, e può essere modificata nell'utility Computer Setup (F10). Per istruzioni consultare la *Guida alle utility Computer Setup* sul *CD della documentazione*.

Se si è utilizzata una versione DOS di Windows 9x, è possibile che appaia una schermata con il logo di Windows. Per non far apparire questa schermata, aggiungere un file di zero byte con nome LOGO.SYS alla directory principale del dispositivo flash media USB.

Ritornare a "Copia su più computer" a pagina 11.

Pulsante d'accensione a doppio stato

Con la funzione ACPI (Advanced Configuration and Power Interface) abilitata, il pulsante di alimentazione può funzionare come interruttore on/off o come pulsante di standby. La funzione di standby non interrompe completamente l'alimentazione, ma fa entrare il computer in una modalità di minimo consumo energetico. In tal modo è possibile spegnere velocemente il computer senza chiudere le applicazioni e ritornare altrettanto velocemente allo stesso stato operativo senza alcuna perdita di dati.

Per cambiare la configurazione del pulsante di accensione procedere come segue:

1. Fare clic sul pulsante **Start** e selezionare **Pannello di controllo > Opzioni risparmio energia**.
2. In **Proprietà – Opzioni risparmio energia** selezionare la scheda **Avanzate**.
3. Nella sezione **Pulsante di alimentazione** selezionare **Stand by**.

Dopo aver configurato il pulsante di accensione in modalità standby, premerlo per portare il sistema ad uno stato di minimo consumo energetico (standby). Premere di nuovo il pulsante per riportare rapidamente il sistema fuori dalla modalità di standby allo stato di piena alimentazione. Per interrompere completamente l'alimentazione al sistema, premere e tenere premuto il pulsante di accensione per quattro secondi.

ATTENZIONE: Non utilizzare il pulsante di accensione per spegnere il computer a meno che il sistema non rispondi; lo spegnimento del computer senza interazione col sistema operativo può provocare danni al disco fisso o perdita di dati.

Sito World Wide Web

I tecnici HP controllano rigorosamente e mettono a punto il software prodotto da HP e da altri fornitori e sviluppano software di supporto specifici per i sistemi operativi, per garantire prestazioni, compatibilità e affidabilità dei personal computer HP.

Quando si passa a sistemi operativi nuovi o modificati, è importante implementare il software di supporto creato per il sistema operativo. Se si prevede di utilizzare una versione di Microsoft Windows diversa da quella preinstallata è necessario installare i driver corrispondenti e le utility necessarie per garantire il corretto funzionamento.

HP ha reso più facile il compito di localizzare, accedere, valutare e installare il software di supporto più recente. Scaricare il software da http://www.hp.com/support.

Il sito contiene gli aggiornamenti ai driver, alle utility ed alle immagini ROM aggiornabili mediante flash, occorrenti per eseguire i sistemi operativi Microsoft Windows sui computer HP.

Moduli e collaboratori

Le soluzioni di gestione HP si integrano con altre applicazioni di gestione sistemi e si basano su standard industriali quali:

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

Controllo e sicurezza degli Asset

Le funzioni di controllo Asset integrate nei PC forniscono dati di controllo sulle principali risorse gestibili con prodotti HP System Insight Manager, HP Client Manager o altre applicazioni di gestione sistemi. L'integrazione automatica e perfetta tra le funzioni di controllo asset e questi prodotti consente di scegliere lo strumento di gestione che meglio si adatta al proprio ambiente e che consente di sfruttare al massimo l'investimento in termini di strumenti già esistenti.

HP offre inoltre diverse soluzioni per il controllo dell'accesso ai componenti e ai dati critici del computer. La funzione di sicurezza integrata ProtectTools, se installata, impedisce l'accesso non autorizzato a dati, controlla l'integrità del sistema ed autentica eventuali utenti estranei che tentino di accedervi. (Per ulteriori informazioni consultare *Guida di HP ProtectTools Embedded Security,* sul *CD della documentazione*.) Le funzioni di sicurezza come ProtectTools, il sensore e la chiusura Smart Cover, disponibili su alcuni modelli, impediscono l'accesso non autorizzato ai componenti interni del personal computer. Disabilitando le porte parallela, seriale od USB, o disabilitando la funzione d'avvio da supporto rimovibile è possibile proteggere risorse dati preziose. Gli allarmi di modifica alla memoria e quelli trasmessi dal sensore Smart Cover possono essere inoltrati automaticamente alle applicazioni di gestione sistemi per fornire un'efficace segnalazione dei tentativi di manomissione dei componenti.

ProtectTools, il sensore e il dispositivo di chiusura Smart Cover sono disponibili come optional su alcuni sistemi.

Per gestire le impostazioni di sicurezza dei computer HP procedere come di seguito indicato:

- In loco, utilizzando le utility di Computer Setup. Per ulteriori informazioni e istruzioni sull'uso delle utility Computer Setup vedere la *Guida all'utility Computer Setup (F10)* sul *CD della documentazione* fornito con il computer.
- A distanza, utilizzare HP Client Manager Software o System Software Manager. Questo software consente un'installazione sicura e ottimizzata e di controllare le impostazioni di sicurezza con una semplice utility da eseguire dalla riga di comando.

La tabella e le sezioni seguenti si riferiscono alla gestione delle caratteristiche di sicurezza del computer a livello locale tramite le utility di Computer Setup (F10).

Descrizione generale delle funzioni di sicurezza

Opzione	Descrizione
Setup Password (Password di impostazione)	Consente di impostare ed abilitare la password di impostazione (password dell'amministratore). ✎ La password di impostazione è necessaria per modificare le opzioni di Computer Setup, effettuare il flash della ROM ed effettuare modifiche ad alcune impostazioni plug and play in Windows. Per ulteriori informazioni consultare la *Guida alla risoluzione dei problemi* sul *CD della documentazione*.
Password d'accensione	Consente di impostare ed abilitare la password di accensione. Per ulteriori informazioni consultare la *Guida alla risoluzione dei problemi* sul *CD della documentazione*.
Password Options (Opzioni della password) (Questa selezione appare solo se è stata impostata una password accensione.)	Consente di specificare se è richiesta la password per l'avvio a caldo **(CTRL+ALT+DEL)**. Per ulteriori informazioni consultare la *Guida di Desktop Management* sul *CD della documentazione*.
Autorizzazione preliminare all'avvio	Consente di abilitare/disabilitare la Smart Card da usare al posto della password di accensione.

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida dell'utility Computer Setup (F10)* nel *CD della documentazione*.

Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Opzione	Descrizione
Smart Cover	Consente di: • Abilitare/disabilitare la chiusura del coperchio. • Abilitare/disabilitare il sensore di assenza del coperchio. ✎ *Notify User (Notifica utente)* avverte l'utente che è stato rilevato il sensore alla rimozione del coperchio. *Setup Password (Password di impostazione)* richiede che venga inserita la password di impostazione per avviare il computer se il sensore rileva che il coperchio è stato tolto. (Funzione supportata solo su alcuni modelli). Per ulteriori informazioni consultare la *Guida di Desktop Management* sul *CD della documentazione*.
Sicurezza integrata	Consente di: • Abilitare/Disabilitare il dispositivo di sicurezza integrata. • Ripristinare sul dispositivo le impostazioni di fabbrica. (Funzione supportata solo su alcuni modelli). Per ulteriori informazioni consultare *Guida di HP ProtectTools Embedded Security,* sul *CD della documentazione*.
Device Security (Sicurezza dei dispositivi)	Abilita/disabilita le porte seriali, la porta parallela, le porte USB frontali, l'audio di sistema, i controller di rete (su alcuni modelli), i dispositivi Multibay (su alcuni modelli) e i controller SCSI (su alcuni modelli).
Network Service Boot (Avviamento servizio di rete)	Abilita/disabilita la capacità del computer di effettuare l'avvio da un sistema operativo installato su un server di rete. (Funzione disponibile solo su modelli NIC; il controller di rete deve risiedere sul bus PCI o essere integrato sulla scheda di sistema.)

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida dell'utility Computer Setup (F10)* nel *CD della documentazione*.

Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Opzione	Descrizione
System IDs (ID del sistema)	Consentono di impostare: • Contrassegno risorse (di 18 byte) e contrassegno di proprietà (identificativo di 80 byte visualizzato durante la fase POST). Per ulteriori informazioni consultare la *Guida di Desktop Management* sul *CD della documentazione*. • Numero di serie chassis o codice UUID (Universal Unique Identifier). Quest'ultimo può essere aggiornato solo se il numero di serie dello chassis non è valido. (Questi codici ID vengono di solito preimpostati in fabbrica e utilizzati esclusivamente per identificare il sistema.) Impostazione locale della tastiera (es. inglese o tedesco) per l'immissione dell'ID del sistema.
DriveLock	Consente di assegnare o modificare una password principale o utente per dischi fissi MultiBay (funzione non supportata su dischi fissi SCSI). Se la funzione è abilitata, all'utente viene richiesto di inserire una delle password DriveLock durante la fase di POST. Se le password non vengono inserite correttamente, non sarà possibile accedere al disco fisso fino al corretto inserimento della password durante una successiva fase di avvio a caldo. ✎ Questa selezione appare solo quando al sistema è collegata almeno un'unità MultiBay che supporta la funzione DriveLock. Per ulteriori informazioni consultare la *Guida di Desktop Management* sul *CD della documentazione*.

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida dell'utility Computer Setup (F10)* nel *CD della documentazione*.

Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Opzione	Descrizione
Master Boot Record Security (Sicurezza MBR (Master Boot Record))	Consente di abilitare o disabilitare la sicurezza MBR (Master Boot Record). Se la funzione è abilitata, il BIOS rifiuta tutte le richieste di scrivere sul Master Boot Record del disco d'avvio corrente. Ogni volta che il computer viene alimentato o riavviato, il BIOS confronta il MBR del disco d'avvio corrente con quello memorizzato in precedenza. Se vengono rilevate delle modifiche, è possibile scegliere di memorizzare il Master Boot Record sul disco d'avvio corrente, ripristinare l'MBR memorizzato in precedenza o disabilitare l'opzione di sicurezza MBR. È necessario conoscere la password di impostazione, se presente. ✎ Disabilitare la sicurezza MBR prima di modificare intenzionalmente la formattazione o la partizione del disco d'avvio corrente. Diverse utility disco (quali FDISK e FORMAT) cercano di aggiornare il Master Boot Record. Se l'opzione di sicurezza MBR è abilitata e gli accessi al disco sono gestiti dal BIOS, le richieste di scrittura sul Master Boot Record vengono respinte, provocando errori nel funzionamento delle utility. Se invece l'opzione è abilitata e gli accessi al disco sono gestiti dal sistema operativo, qualsiasi modifica MBR viene rilevata dal BIOS durante il riavvio successivo e viene visualizzato un messaggio d'avvertenza di sicurezza MBR.

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida dell'utility Computer Setup (F10)* nel *CD della documentazione*.

Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Opzione	Descrizione
Save Master Boot Record (Memorizza Master Boot Record)	Memorizza una copia di backup del Master Boot Record del disco d'avvio corrente. Questa opzione viene visualizzata solo se è abilitata l'opzione di sicurezza MBR.
Restore Master Boot Record (Ripristina Master Boot Record)	Ripristina il Master Boot Record di backup sul disco d'avvio corrente. ✎ Questa opzione viene visualizzata solo se si verificano tutte le condizioni seguenti: • La funzione MBR Security è abilitata. • Una copia di backup del Master Boot Record è stata memorizzata in precedenza. • Il disco d'avvio corrente è lo stesso dal quale viene memorizzata la copia di backup del Master Boot Record. ⚠ **ATTENZIONE:** Il ripristino di un MBR memorizzato in precedenza dopo l'esecuzione di un'utility del disco o dopo una modifica dell'MBR da parte del sistema operativo può impedire l'accesso ai dati presenti sul disco. Ripristinare un MBR memorizzato in precedenza solo se si è certi che l'MBR del disco d'avvio è corrotto o infettato da virus.

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida dell'utility Computer Setup (F10)* nel *CD della documentazione*.

Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Sicurezza tramite password

La password di accensione impedisce l'utilizzo non autorizzato del computer richiedendo l'immissione di una password per accedere alle applicazioni o ai dati ogni volta che il computer viene acceso o riavviato. La password di impostazione impedisce in modo specifico l'accesso non autorizzato a Computer Setup, e può anche essere utilizzata per escludere la password di accensione. Ciò significa che, quando viene richiesta la password di accensione, è possibile accedere al computer anche immettendo la password di configurazione.

È possibile impostare un'unica password per l'intera rete, al fine di consentire all'amministratore della rete di accedere a tutti i sistemi della rete per eseguire le operazioni di manutenzione senza conoscerne la password di accensione, nel caso ne sia stata attivata una.

Impostazione di una password di configurazione tramite Computer Setup

Se il sistema è dotato di un dispositivo di sicurezza integrato, consultare la *Guida di HP ProtectTools Embedded Security,* sul *CD della documentazione*. Se si imposta una password di configurazione tramite Computer Setup, si impedisce la riconfigurazione del computer (uso dell'utility di Computer Setup (F10)) finché non viene immessa la password.

1. Accendere o riavviare il computer. Se si è in Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

✎ Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

---

3. Selezionare **Sicurezza**, quindi **Password di configurazione** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Immissione della password di accensione con Computer Setup

Impostando una password di accensione in Computer Setup si impedisce l'accesso al computer all'accensione, finché non viene immessa la password. Se è stata impostata la password di accensione, Computer Setup presenta le opzioni disponibili (Password Options) nel menu Security (Sicurezza). Tra le opzioni della password figura Password Prompt on Warm Boot (Richiesta password al riavvio). Se l'opzione Password Prompt on Warm Boot è abilitata, la password dev'essere immessa ogni volta che il computer viene riavviato.

1. Accendere o riavviare il computer. Se si è in Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

---

3. Selezionare **Sicurezza**, quindi **Password di accensione** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Immissione della password di accensione

Per immettere la password di accensione procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando viene visualizzata sul monitor l'icona della chiave, digitare la password attuale e premere **Invio**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

Se si immette la password in modo errato, viene visualizzata un'icona di chiave spezzata. Tentare di nuovo. Dopo tre tentativi falliti, è necessario spegnere il computer e riaccenderlo, prima di poter continuare.

Immissione di una password di impostazione

Se il sistema è dotato di un dispositivo di sicurezza integrato, consultare la *Guida di HP ProtectTools Embedded Security,* sul *CD della documentazione*.

Se sul PC è stata impostata la password di configurazione, ne viene richiesta l'immissione ogni volta che viene eseguito Computer Setup.

1. Accendere o riavviare il computer. Se si è in Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

3. Quando viene visualizzata sul monitor l'icona della chiave, digitare la password di configurazione e premere **Invio**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

Se si immette la password in modo errato, viene visualizzata un'icona di chiave spezzata. Tentare di nuovo. Dopo tre tentativi falliti, è necessario spegnere il computer e riaccenderlo, prima di poter continuare.

Modifica delle password di accensione e di configurazione

Se il sistema è dotato di un dispositivo di sicurezza integrato, consultare la *Guida di HP ProtectTools Embedded Security,* sul *CD della documentazione*.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Per cancellare la password di accensione passare al punto 3.

   Per cancellare la password di impostazione, non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

---

3. Quando viene visualizzata l'icona della chiave, digitare la password, una barra (/) o un carattere delimitatore alternativo, la nuova password, un'altra barra (/) o un carattere delimitatore alternativo e ancora la nuova password, come di seguito precisato:
   password attuale/nuova password/nuova password

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

---

4. Premere **Invio**.

La nuova password sarà in vigore a partire dalla prossima volta che si accende il computer.

Per informazioni sui caratteri delimitatori alternativi consultare "Caratteri delimitatori delle tastiere nazionali" a pagina 32. È possibile modificare la password di accensione e di impostazione anche utilizzando le opzioni di sicurezza di Computer Setup.

Cancellazione delle password di accensione e di configurazione

Se il sistema è dotato di un dispositivo di sicurezza integrato, consultare la *Guida di HP ProtectTools Embedded Security,* sul *CD della documentazione*.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Per cancellare la password di accensione passare al punto 3.

   Per cancellare la password di impostazione, non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

---

3. Quando viene visualizzata l'icona della chiave, digitare la password attuale seguita da una barra (/) o da un carattere delimitatore alternativo, come qui illustrato:
   password attuale/
4. Premere **Invio**.

Per informazioni sui caratteri delimitatori alternativi consultare "Caratteri delimitatori delle tastiere nazionali". È possibile modificare la password di accensione e di impostazione anche utilizzando le opzioni di sicurezza di Computer Setup.

Caratteri delimitatori delle tastiere nazionali

Ciascuna tastiera è concepita per soddisfare i requisiti specifici dei singoli paesi. La sintassi e i tasti per la modifica o la cancellazione delle password dipendono dalla tastiera utilizzata.

Caratteri delimitatori delle tastiere nazionali

Araba	/	Greca	-	Russa	/
Belga	=	Ebraica	.	Slovacca	-
BHCSY*	-	Ungherese	-	Spagnola	-
Brasiliana	/	Italiana	-	Svedese/Finnica	/
Cinese	/	Giapponese	/	Svizzera	-
Ceca	-	Coreana	/	Taiwanese	/
Danese	-	Latino-americana	-	Tailandese	/
Francese	!	Norvegese	-	Turca	.
Canadese francofona	é	Polacca	-	Inglese del RU	/
Tedesca	-	Portoghese	-	Inglese degli USA	/

*Per Bosnia-Erzegovina, Croazia, Slovenia e Iugoslavia

Annullamento password

Se si dimentica la password, non è possibile accedere al computer. Per le istruzioni su come eliminare le password consultare la *Guida alla risoluzione dei problemi* sul *CD della documentazione*.

Se il sistema è dotato di un dispositivo di sicurezza integrato, consultare la *Guida di HP ProtectTools Embedded Security*, sul *CD della documentazione*.

DriveLock

DriveLock è una funzione di sicurezza di standard industriale che impedisce l'accesso non autorizzato ai dati memorizzati su dischi MultiBay. DriveLock è stato implementato come estensione di Computer Setup ed è disponibile quando vengono rilevate unità dischi rigidi compatibili con DriveLock.

DriveLock è destinato a clienti HP per i quali la sicurezza dei dati è fondamentale. Per tali clienti il costo del disco fisso e la perdita dei dati ivi memorizzati hanno un'importanza secondaria rispetto al danno provocato da un accesso non autorizzato al contenuto. Per bilanciare questo livello di sicurezza con l'esigenza pratica di consentire l'accesso in caso di smarrimento della password, l'implementazione HP di DriveLock utilizza uno schema di sicurezza a doppia password: una dev'essere impostata ed utilizzata da un amministratore di sistema, mentre l'altra viene normalmente impostata ed utilizzata dall'utente finale. Non sono previsti accorgimenti per sbloccare il disco se vengono smarrite entrambe le password. Pertanto, DriveLock risulta maggiormente indicato quando i dati contenuti sul disco fisso vengono replicati su un sistema informatico aziendale o quando ne viene effettuato il backup su base regolare.

Se entrambe le password di DriveLock vengono smarrite, il disco fisso viene reso inutilizzabile. Per gli utenti che non rispondono ai criteri sopra delineati questo può essere un rischio inaccettabile. Per quelli, invece, che rispondono a tali criteri, il rischio può essere tollerabile, data la natura dei dati memorizzati sul disco.

Uso di DriveLock

L'opzione DriveLock è disponibile nel menu Security (Sicurezza) di Computer Setup. L'utente ha la possibilità di impostare la password principale o di abilitare DriveLock. Per abilitare DriveLock dev'essere specificata una password utente. Dal momento che la configurazione iniziale di DriveLock viene normalmente eseguita da un amministratore di sistema, dev'essere prima di tutto impostata la password principale. HP invita gli amministratori di sistema ad impostare una password principale sia che prevedano di abilitare DriveLock, sia che prevedano di non abilitarlo. In tal modo gli amministratori avranno la possibilità di modificare le impostazioni di DriveLock se si deciderà di bloccare il disco in un secondo tempo. Una volta impostata la password principale l'amministratore di sistema potrà abilitare o meno DriveLock.

Se è presente un disco fisso bloccato, durante il POST chiede la password per sbloccarlo. Se viene impostata una password di accensione e la stessa coincide con quella dell'utente della periferica, durante il POST non viene richiesto all'utente di reimmettere la password. Altrimenti, all'utente viene richiesto di immettere la password per accedere a DriveLock. È possibile utilizzare a tal fine la password principale o quella dell'utente. Gli utenti hanno a disposizione due tentativi per immettere la password corretta. Se entrambi non riescono, il POST prosegue ma il disco resta inaccessibile.

Applicazioni di DriveLock

La condizione più indicata per la funzione di sicurezza DriveLock è in àmbito aziendale, quando un amministratore di sistema fornisce agli utenti dischi fissi MultiBay da utilizzare in alcuni computer desktop. L'amministratore di sistema è responsabile della configurazione del disco fisso MultiBay che comporta, tra l'altro, l'impostazione della password principale di DriveLock. Se l'utente dimentica la sua password o la macchina passa ad un altro impiegato, è possibile utilizzare la password principale per cambiare la password utente e riaccedere al disco.

HP consiglia agli amministratori dei sistemi aziendali che decidono di abilitare DriveLock di definire una politica aziendale per l'impostazione e il mantenimento delle password principali. Questa operazione ha lo scopo d'impedire che un dipendente, prima di lasciare l'azienda, imposti intenzionalmente o casualmente entrambe le password di DriveLock. In una simile eventualità il disco fisso non potrebbe più essere utilizzato e dovrebbe essere sostituito. Analogamente, non impostando la password principale gli amministratori di sistema potrebbero vedersi impedito l'accesso al disco per eseguire i controlli di routine del software non autorizzato, altre funzioni di controllo risorse e di supporto.

Per utenti con esigenze di sicurezza meno rigide HP sconsiglia di abilitare DriveLock. Appartengono a questa tipologia singoli utenti ed utenti che conservano dati non importanti sui dischi fissi. Per questi utenti il rischio di perdere il disco in caso di smarrimento di entrambe le password è decisamente superiore al valore dei dati che DriveLock dovrebbe proteggere. L'accesso a Computer Setup e a DriveLock può essere limitato tramite la password di configurazione. Specificando la password di configurazione senza comunicarla agli utenti, gli amministratori di sistema possono impedire loro di abilitare DriveLock.

Sensore Smart Cover

Il sensore di assenza coperchio, disponibile su alcuni modelli, è una combinazione di tecnologia hardware e software in grado di segnalare se il coperchio o il pannello laterale del computer sono stati tolti. Esistono tre livelli di protezione, come risulta dalla seguente tabella:

Livelli di protezione del sensore Smart Cover

Livello	Impostazione	Descrizione
Livello 0	Disattivato	Il sensore Smart Cover è disattivato (impostazione predefinita).
Livello 1	Notifica all'utente	Quando il computer viene riavviato, sullo schermo viene visualizzato un messaggio che avverte che il coperchio o il pannello laterale del computer sono stati rimossi.
Livello 2	Setup Password (Password di impostazione)	Quando il computer viene riavviato, sullo schermo viene visualizzato un messaggio che avverte che il coperchio o il pannello laterale del computer sono stati rimossi. Per continuare, è necessario immettere la password di impostazione.

✎ Le impostazioni possono essere modificate tramite Computer Setup. Per ulteriori informazioni su Computer Setup vedere la *Guida dell'utility Computer Setup (F10)* sul *CD della documentazione*.

Impostazione del livello di protezione del sensore Smart Cover

Per impostare il livello di protezione del sensore Smart Cover procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

3. Scegliere **Security (Sicurezza) > Smart Cover > Cover Removal Sensor (Sensore assenza coperchio)** e selezionare un livello di sicurezza.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Chiusura Smart Cover

La chiusura Smart Cover è un dispositivo di blocco a controllo informatizzato, presente su alcuni computer HP, Esso impedisce l'accesso non autorizzato ai componenti interni. Alla consegna, i computer hanno la chiusura Smart Cover sbloccata.

ATTENZIONE: Per garantire la massima sicurezza del blocco del coperchio, è bene stabilire una password di impostazione. La password impedisce l'accesso non autorizzato all'utility Computer Setup.

La chiusura Smart Cover è disponibile come optional su determinati modelli.

Blocco della chiusura Smart Cover

Per attivare e bloccare la chiusura Smart Cover procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

---

3. Selezionare **Security (Sicurezza) > Smart Cover > Cover Lock (Blocco coperchio) > Lock (Blocco)**.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Disattivazione del blocco di Smart Cover

1. Accendere o riavviare il computer. Se si è in Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

---

3. Selezionare **Security > (Sicurezza) > Smart Cover > Cover Lock (Blocco coperchio) > Unlock (Sblocco)**.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Uso della chiave FailSafe Smart Cover

Se la chiusura Smart Cover è abilitata e non è possibile immettere la password per disabilitarla, per aprire il coperchio del computer è necessaria la chiave Failsafe di Smart Cover. La chiave è necessaria in tutte le seguenti circostanze:

- Mancanza di corrente
- Guasto all'avvio
- Guasto dei componenti del PC (ad esempio, processore o alimentatore)
- Password dimenticata

ATTENZIONE: La chiave FailSafe di Smart Cover è uno strumento speciale disponibile presso HP. Per sicurezza si consiglia di ordinare la chiave prima che sia necessario utilizzarla presso un venditore o un centro assistenza autorizzati.

È possibile procurarsi la chiave FailSafe in diversi modi:

- Contattare un rivenditore o un centro assistenza autorizzati HP.
- Chiamare il numero di telefono appropriato, riportato nella garanzia.

Per ulteriori informazioni sull'utilizzo della chiave FailSafe di Smart Cover consultare la *Guida di riferimento hardware* sul *CD della documentazione*.

Master Boot Record Security (Sicurezza MBR (Master Boot Record))

Il Master Boot Record (MBR) contiene le informazioni necessarie per l'avvio da un disco e l'accesso ai dati ivi memorizzati. La sicurezza del Master Boot Record individua e registra modifiche involontarie o dolose al MBR, come quelle provocate da alcuni virus o dall'uso non corretto di alcune utility. Inoltre essa consente di ripristinare l'ultimo MBR valido nel caso in cui, in fase di riavvio del sistema, vengano rilevate modifiche al MBR.

Per abilitare la sicurezza MBR procedere come segue:

1. Accendere o riavviare il computer. Se si è in Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

3. Selezionare **Security** (**Sicurezza**) **> Master Boot Record Security** (**Sicurezza MBR**) **> Enabled** (**Abilitata**).
4. Selezionare **Security** (**Sicurezza**) **> Save Boot Record** (**Salva MBR**).
5. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Quando la sicurezza MBR è abilitata il BIOS impedisce qualsiasi modifica al MBR del disco avviabile corrente in MS-DOS o in Modalità provvisoria di Windows.

La maggior parte dei sistemi operativi controlla l'accesso al MBR del disco avviabile corrente; il BIOS non è in grado d'impedire che vengano apportate modifiche quando il sistema operativo è in funzione.

Ogni volta che il computer viene alimentato o riavviato, il BIOS confronta il MBR del disco d'avvio corrente con quello memorizzato in precedenza. Se vengono rilevate modifiche e se il disco avviabile corrente è lo stesso da cui è stato memorizzato il MBR, viene visualizzato il seguente messaggio:

1999 – Master Boot Record has changed (Il MBR è cambiato).

Premere un tasto per accedere a Computer Setup per configurare la sicurezza MBR.

Una volta in Computer Setup procedere come segue:

- Salvare il MBR del disco avviabile corrente;
- Ripristinare il MBR precedentemente memorizzato; oppure
- Disabilitare la funzione di sicurezza MBR.

È necessario conoscere l'eventuale password di configurazione.

Se vengono rilevate modifiche e se il disco avviabile corrente **non** è lo stesso da cui è stato memorizzato il MBR viene visualizzato il seguente messaggio:

2000 – Master Boot Record Hard Drive has changed (Il disco fisso con l'MBR è cambiato).

Premere un tasto per accedere a Computer Setup per configurare la sicurezza MBR.

Una volta in Computer Setup procedere come segue:

- Salvare il MBR del disco avviabile corrente; oppure
- Disabilitare la funzione di sicurezza MBR.

È necessario conoscere l'eventuale password di configurazione.

Nell'improbabile eventualità che il MBR precedentemente salvato si sia danneggiato viene visualizzato il seguente messaggio:

1998 – Master Boot Record has been lost (L'MBR è danneggiato).

Premere un tasto per accedere a Computer Setup per configurare la sicurezza MBR.

Una volta in Computer Setup procedere come segue:

- Salvare il MBR del disco avviabile corrente; oppure
- Disabilitare la funzione di sicurezza MBR.

È necessario conoscere l'eventuale password di configurazione.

Partizionamento e formattazione del disco avviabile corrente

Verificare che la sicurezza MBR sia disabilitata prima di modificare la partizione o prima di formattare il disco avviabile corrente. Alcune utility disco (FDISK e FORMAT) cercano di aggiornare il MBR. Se la sicurezza MBR è abilitata, quando si cambia la partizione o si formatta il disco è possibile che vengano visualizzati messaggi d'errore dall'utility o un avvertimento relativo alla sicurezza MBR in occasione del successivo riavvio del computer. Per disabilitare la sicurezza MBR procedere come segue:

1. Accendere o riavviare il computer. Se si è in Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

Con una tastiera PS/2 è possibile che appaia un messaggio di errore tastiera, che può essere tranquillamente ignorato.

3. Selezionare **Security (Sicurezza) > Master Boot Record Security (Sicurezza MBR) > Disabled (Disabilitata)**.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Predisposizione per chiusura con cavo

Sul retro del computer è presente la predisposizione per la chiusura con cavo in modo da bloccare fisicamente il computer al piano di lavoro.

Per le istruzioni consultare la *Guida di riferimento hardware* sul *CD della documentazione*.

Tecnologia per l'identificazione delle impronte digitali

Eliminando la necessità di immettere le password utente, la tecnologia per il riconoscimento delle impronte digitali di HP migliora la sicurezza della rete, semplificando il processo di accesso e riducendo i costi associati alla gestione delle reti aziendali. Grazie al prezzo accessibile, la funzione non è più appannaggio esclusivo delle organizzazioni high-tech con esigenze di sicurezza elevate.

Il supporto per la tecnologia d'identificazione delle impronte digitali varia da modello a modello.

Per ulteriori informazioni consultare:

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

Notifica guasti e ripristino

Le funzioni di notifica guasti e ripristino combinano hardware innovativo e tecnologia software al fine di prevenire la perdita di dati critici e ridurre al minimo i periodi di inattività non programmati.

Se è collegato ad una rete gestita da HP Client Manager, il computer invia un avviso di guasto all'applicazione di gestione della rete. Con HP Client Manager Software è possibile programmare a distanza operazioni diagnostiche da eseguire automaticamente su tutti i PC gestiti e creare un report riepilogativo dei test non andati a buon fine.

Drive Protection System (DPS)

Il Drive Protection System (DPS) è uno strumento di diagnostica incorporato nei dischi fissi installati su alcuni computer HP, Il DPS è stato progettato per consentire la diagnosi di problemi che potrebbero provocare la sostituzione di unità disco rigido non in garanzia.

In fase di produzione dei PC HP, i dischi fissi installati vengono collaudati uno per uno tramite DPS e su di essi viene registrato un record permanente di dati chiave. Ogni volta che viene eseguito il DPS, gli esiti del test vengono memorizzati nell'unità disco rigido. Il fornitore di servizi potrà servirsi di queste informazioni per diagnosticare le condizioni che hanno indotto l'utente ad eseguire il software DPS. Per le istruzioni su come utilizzare il DPS consultare la *Guida alla risoluzione dei problemi* sul *CD della documentazione*.

Alimentatore protetto contro gli sbalzi di tensione

Un alimentatore integrato protetto contro gli sbalzi di tensione garantisce maggiore affidabilità in presenza di instabilità nell'alimentazione. L'alimentatore è concepito per tollerare sbalzi di tensione fino a 2000 volt, senza esporre il sistema periodi di inattività o perdita di dati.

Sensore termico

Il sensore termico è una funzione hardware e software che controlla la temperatura interna del computer. Quando la temperatura supera i valori normali, questa funzione visualizza un messaggio di allarme che consente di intervenire prima che vengano danneggiati i componenti interni o che si verifichi una perdita di dati.

Indice Analitico

A

accesso al computer, controllo 21
aggiornamento della ROM 6
alimentatore protetto contro gli sbalzi di tensione 43
alimentatore, protetto contro gli sbalzi di tensione 43
Altiris 4
annullamento password 32
attenzione
  protezione ROM 6
avvertenze
  chiave FailSafe 38
  sicurezza chiusura coperchio 36

B

blocco della chiusura Smart Cover 37

C

cancellazione password 31
caratteri delimitatori tastiere nazionali 32
caratteri delimitatori tastiere, nazionali 32
caratteri delimitatori, tabella 32
chiave FailSafe
  avvertenza 38
  ordinazione 38
chiave FailSafe di Smart Cover, ordinazione 38
chiusura Smart Cover
  blocco 37
  sblocco 37
configurazione
  iniziale 2
configurazione iniziale 2
configurazione pulsante di accensione 19
controllo asset 21
controllo dell'accesso al computer 21

D

dischi, clonazione 2
disco avviabile, informazioni importanti 41
DiskOnKey
  vedere anche HP Drive Key
  avviabile 13 a 18
dispositivo avviabile
  creazione 13 a 18
  DiskOnKey 13 a 18
  dispositivo flash media USB 13 a 18
  HP Drive Key 13 a 18
dispositivo flash media USB, avviabile 13 a 18
Drivelock 33 a 34

F

flash ROM remoto 7
formattazione disco, informazioni importanti 41

H

HP Client Manager 3
HP Drive Key
  vedere anche DiskOnKey
  avviabile 13 a 18

I

immagine del software preinstallato 2
immissione
  password di accensione 28
  password di configurazione 29
impostazioni
  replica 9
indirizzi Internet, vedere siti Web
installazione remota 2
installazione remota del sistema, accesso 3

M

modifica dei sistemi operativi, informazioni importanti 20
modifica password 30

N

notifica di modifiche 5
notifica guasti 42
notifica modifica 5

O

ordinazione chiave FailSafe 38

P

partizione disco, informazioni importanti 41
password
  accensione 28
  annullamento 32
  cancellazione 31
  configurazione 27, 29
  modifica 30
  sicurezza 27
password di accensione
  cancellazione 31
  immissione 28
  modifica 30
password di configurazione
  cancellazione 31
  immissione 29
  impostazione 27
  modifica 30
PCN (Proactive Change Notification) 5
personalizzazione del software 2
Preboot Execution Environment (PXE) 2
predisposizione per chiusura con cavo 41
Proactive Change Notification (PCN) 5
protezione ROM, attenzione 6
protezione unità disco rigido 42
pulsante di accensione
  bistabile 19
  configurazione 19
pulsante di accensione bistabile 19
PXE (Preboot Execution Environment) 2

R

replica 9
ripristino del sistema 7
ripristino, software 2
ROM
  flash remoto 7
  non valida 8
ROM con blocco di avviamento FailSafe 8
ROM di sistema non valida 8
ROM, aggiornamento 6

S

sblocco chiusura Smart Cover 37
sensore Smart Cover 35
  impostazione 36
  livelli di protezione 35
sensore termico 43
sicurezza
  DriveLock 33 a 34
  funzioni, tabella 22
  impostazioni, configurazione 21
  Master Boot Record 39 a 40
  MultiBay 33 a 34
  password 27
  sensore Smart Cover 35
  Smart Cover Lock 36 a 38

sicurezza chiusura coperchio, avvertenza 36
sicurezza Master Boot Record 39 a 40
sicurezza Multibay 33 a 34
sistemi operativi, informazioni importanti 20
siti Web
  Altiris 4, 5
  deployment PC 2
  flash ROM remoto 7
  Flash su ROM 6
  HP Client Manager 3
  HPQFlash 7
  immagini ROMPaq 6
  Proactive Change Notification 6
  replica della configurazione 12, 13
  Subscriber's Choice 6
  supporto software 20
  System Software Manager (SSM) 5
  tecnologia per l'identificazione delle impronte digitali 42
Smart Cover Lock 36 a 38
smart cover, chiusura 36
software
  aggiornamento contemporaneo di più macchine 5
  controllo asset 21
  Drive Protection System (DPS) 42
  flash ROM remoto 7
  installazione remota del sistema 2
  integrazione 2
  notifica guasti e ripristino 42
  ripristino 2
  ROM con blocco di avviamento FailSafe 8
  sicurezza Master Boot Record 39 a 40
  System Software Manager 5
  utility Computer Setup 9
spie della tastiera ROM, tabella 9
spie della tastiera, ROM, tabella 9
SSM (System Software Manager) 5
strumenti di clonazione, software 2
strumenti di deployment, software 2
strumento diagnostico per unità disco rigido 42
System Software Manager (SSM) 5

T

tecnologia per l'identificazione delle impronte digitali 42
temperatura interna del computer 43
temperatura, interna del computer 43

U

unità disco rigido, strumento diagnostico 42
unità, protezione 42
URL (siti Web). Vedere Siti Web
utility Computer Setup 9