

# Guida di Desktop Management Business PC

© Copyright 2007 Hewlett-Packard Development Company, L.P. Le informazioni qui contenute sono soggette a modifiche senza preavviso.

Windows e Windows Vista sono entrambi marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi.

Intel e vPro sono marchi di Intel Corporation negli Stati Uniti e in altri paesi.

Le uniche garanzie su prodotti e servizi HP sono definite nei certificati di garanzia allegati a prodotti e servizi. Nulla di quanto qui contenuto potrà essere interpretato nel senso della costituzione di garanzie accessorie. HP declina ogni responsabilità per errori od omissioni tecniche o editoriali contenuti nella presente guida.

Questo documento contiene informazioni proprietarie protette da copyright. Nessuna parte del documento può essere fotocopiata, riprodotta o tradotta in altra lingua senza la preventiva autorizzazione scritta di Hewlett-Packard Company.

Guida di Desktop Management

Business PC

Seconda edizione (ottobre 2007)

Numero di parte del documento: 451272-062

## Informazioni su questa guida

contiene definizioni e istruzioni per l'uso delle caratteristiche di sicurezza e gestibilità preinstallate su 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.
- 📝 **NOTA:** Il testo presentato in questo modo indica che vengono fornite importanti informazioni supplementari.



---

# Sommario

## 1 Panoramica di Desktop Management

## 2 Configurazione iniziale e deployment

HP Software Agent .....	3
Altiris Deployment Solution Agent .....	3

## 3 Installazione remota del sistema

## 4 Aggiornamento e gestione del software

HP Client Management Interface .....	5
HP SoftPaq Download Manager .....	6
HP System Software Manager .....	7
HP ProtectTools Security Manager .....	7
HP Client Configuration Manager .....	8
HP Configuration Management Solution .....	9
HP Client Manager for Altiris .....	10
Altiris Client Management Suite .....	11
HP Client Catalog for SMS .....	11
HP Backup and Recovery Manager .....	12
PC Intel vPro con Active Management Technology .....	13
Verdiem Surveyor .....	15
HP Proactive Change Notification .....	15
Subscriber's Choice .....	15
Soluzioni sospese .....	16

## 5 Flash della ROM

Flash remoto della ROM .....	17
HPQFlash .....	17

## 6 Boot Block Emergency Recovery Mode

## 7 Replica delle impostazioni

Copia su computer singolo .....	19
Copia su più computer .....	20
Creazione di un dispositivo d'avvio .....	21
Dispositivo USB flash media compatibile .....	21
Dispositivi USB flash media non compatibili .....	22

## 8 Pulsante d'accensione a doppio stato

## 9 Assistenza sul sito Web HP

## 10 Standard di settore

## 11 Controllo e sicurezza degli asset

Sicurezza tramite password .....	29
Impostazione di una password di configurazione tramite Computer Setup .....	29
Impostazione di una password di accensione tramite Computer Setup .....	29
Immissione della password di accensione .....	30
Immissione di una password di configurazione .....	30
Modifica delle password di accensione e di configurazione .....	31
Cancellazione delle password di accensione e di configurazione .....	31
Caratteri delimitatori delle tastiere nazionali .....	32
Annullamento password .....	32
DriveLock .....	32
Uso di DriveLock .....	32
Applicazioni di DriveLock .....	33
Sensore Smart Cover .....	33
Impostazione del livello di protezione del sensore Smart Cover .....	34
Chiusura Smart Cover .....	34
Blocco della chiusura Smart Cover .....	34
Disattivazione del blocco della chiusura Smart Cover .....	35
Uso della chiave FailSafe Smart Cover .....	35
Predisposizione per fissaggio con cavo .....	35
Tecnologia per l'identificazione delle impronte digitali .....	35
Notifica guasti e ripristino .....	37
Drive Protection System (DPS) .....	37
Alimentatore protetto contro gli sbalzi di tensione .....	37
Sensore termico .....	37
<b>Indice analitico .....</b>	<b>38</b>

---


# 1 Panoramica di Desktop Management

HP Client Management Solutions fornisce soluzioni standard per la gestione e 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. HP sviluppa un proprio software di gestione e collabora strettamente con le principali aziende produttrici di soluzioni per la gestione, allo scopo di garantirne la compatibilità con HP Client Management Solutions. Il software Client Management Solutions è un aspetto importante del grande impegno di HP nel proporre soluzioni che aiutino l'utente a ridurre il costo totale della proprietà e la manutenzione dei PC nel corso dell'intero ciclo vitale.

Le principali capacità e funzioni della gestione desktop sono:

- Configurazione iniziale e deployment
- Installazione remota del sistema
- Aggiornamento e gestione del software
- Flash della ROM
- Configurazione delle opzioni hardware
- Asset tracking and security (Controllo e sicurezza asset)
- Notifica e riparazione dei guasti

---

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

---

---

## 2 Configurazione iniziale e deployment


Il computer include 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 del software, come HP Client Configuration Manager, HP Configuration Management Solution (basato su tecnologia Radia) o 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 deployment da preferire dipende dai processi e dagli ambienti informatici degli utenti. La sezione PC Deployment del sito HP Lifecycle Service (<http://h20219.www2.hp.com/services/cache/80906-0-0-225-121.html>) fornisce informazioni che aiutano a selezionare il metodo di deployment più adatto.

Il CD *Restore Plus!*, l'installazione da CD-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.

 **NOTA:** Per informazioni sulla creazione del CD *Restore Plus!*, consultare [HP Backup and Recovery Manager a pagina 12](#).

---



## HP Software Agent

L'agente di gestione utilizzato sia da HP Client Configuration Manager sia da HP Configuration Management Solution è preinstallato sul computer. Quando installato, consente la comunicazione con la console di gestione HP.

Per installare HP Software Agent:

1. Fare clic su **Start**.
2. Fare clic su **Tutti i programmi**.
3. Fare clic su **HP Manageability**.
4. Fare clic su **Radia Management Agent Readme**.
5. Leggere e seguire le istruzioni contenute nel file Readme per installare HP Software Agent:

HP Software Agent è un componente di infrastruttura chiave per l'abilitazione di tutte le soluzioni di gestione HP Configuration Management Solution. Per informazioni sugli altri componenti di infrastruttura necessari per l'implementazione di HP Configuration Management Solution, visitare il sito <http://h20229.www2.hp.com/solutions/ascm/index.html>.

## Altiris Deployment Solution Agent

Questo programma è preinstallato sul computer. Quando installato, consente la comunicazione con la console di amministrazione di Deployment Solution.

Per installare Altiris Deployment Solution Agent:

1. Fare clic su **Start/Avvio**.
2. Fare clic su **Tutti i programmi**.
3. Per Windows Vista, fare clic su **Install Altiris DAgent**. Per Windows XP, fare clic su **Install Altiris AClient**.
4. Seguire le istruzioni a video per installare e configurare il client Altiris.

Questo agente è un componente di infrastruttura chiave per l'abilitazione di Altiris Deployment Solution, che fa parte di Altiris Client Management Suite. Per informazioni sugli altri componenti di infrastruttura necessari per l'implementazione di Altiris Client Management Suite, visitare il sito <http://www.hp.com/go/easydeploy>.

---

## 3 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'unità disco rigido
- Installazione di una copia del software su uno o più PC nuovi
- Aggiornamento remoto del BIOS di sistema nella ROM flash ([Flash remoto della ROM a pagina 17](#))
- Configurazione delle impostazioni del BIOS di sistema

Per avviare l'installazione remota del sistema, premere **F12** quando il messaggio **F12=Avvio servizi di rete** appare nell'angolo in basso a destra dello schermo del logo HP all'avvio del computer. Per continuare il processo, seguire le istruzioni sullo schermo. La sequenza di avvio predefinita è un'impostazione di configurazione del BIOS che è possibile modificare in modo che venga sempre eseguito prima l'avvio PXE.

---

## 4 Aggiornamento e gestione del software

HP fornisce diversi strumenti per la gestione e l'aggiornamento del software su PC desktop, workstation e notebook:

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Configuration Manager
- HP Configuration Management Solution
- HP Client Manager for Altiris
- Altiris Client Management Suite
- HP Client Catalog for SMS
- HP Backup and Recovery Manager
- PC Intel vPro con Active Management Technology
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

### HP Client Management Interface

Indipendentemente dagli strumenti di gestione utilizzati dai responsabili dei sistemi informatici, le risorse hardware e software sono importanti in ugual misura per contenere i costi IT e garantire la flessibilità dell'azienda. L'amministratore IP può accedere a HP Client Management Interface redigendo semplici script e integrandoli nella soluzione di gestione di sua scelta.

Con HP Client Management Interface (HP CMI), i nuovi computer aziendali HP si integrano perfettamente nell'ambiente IT gestito. HP CMI offre un'interfaccia che semplifica l'integrazione dei computer aziendali HP con gli strumenti di gestione del sistema più comuni del settore (inclusi Microsoft Systems Management Server, IBM Tivoli Software e HP Operations) e le applicazioni di gestione personalizzate sviluppate in azienda. Grazie a HP CMI, gli strumenti e le applicazioni di gestione del sistema possono richiedere un inventario approfondito del client, ricevere informazioni sulle relative condizioni e gestire le impostazioni del BIOS di sistema comunicando direttamente con il computer client, in modo che non sia necessario che il software agente o di connessione ottenga l'integrazione.

HP Client Management Interface si basa su standard del settore, tra cui Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) e Advanced Configuration and Power Interface (ACPI). HP CMI è una tecnologia di

base utilizzata in HP Client Management Solutions. Grazie ad HP CMI, HP offre la flessibilità di scegliere la modalità di gestione dei computer client HP.

Utilizzata unitamente al software di gestione del sistema, l'interfaccia di gestione client HP può:

- Richiedere un inventario approfondito del client - Acquisire informazioni dettagliate su processori, unità disco rigido, memoria, BIOS, driver, comprese le informazioni sui sensori (velocità della ventola, tensione e temperatura).
- Ricevere informazioni sulle condizioni del client - Attivare l'invio di una vasta gamma di allarmi hardware del client (surriscaldamento, arresto della ventola e modifiche alla configurazione dell'hardware) alla console di gestione del sistema, all'applicazione o al computer client locale. Gli allarmi vengono inviati in tempo reale quando sono attivati da eventi hardware.
- Gestire le impostazioni del BIOS di sistema - Eseguire funzioni F10, incluse l'impostazione e la modifica delle password del BIOS e la sequenza di avvio del computer, in remoto dalla console di gestione del sistema su qualsiasi sistema client, senza doversi recare personalmente alla macchina.

Per ulteriori informazioni su HP Client Management Interface, visitare il sito <http://www.hp.com/go/hpcmi/>.

## HP SoftPaq Download Manager


HP SoftPaq Download Manager è un'interfaccia gratuita di facile utilizzo che consente di individuare e scaricare gli aggiornamenti del software per i modelli di PC client HP nel proprio ambiente. Specificando i modelli, il sistema operativo e la lingua, è possibile individuare, ordinare e selezionare rapidamente i softpaq necessari. Per scaricare HP SoftPaq Download Manager, visitare il sito <http://h20331.www2.hp.com/Hpsub/cache/509658-0-0-225-121.html>.

# HP System Software Manager

HP System Software Manager (SSM) è una utility gratuita che rende automatico il deployment remoto dei driver e degli aggiornamenti del BIOS per i PC aziendali HP in rete. Quando l'utility SSM è in esecuzione, determina automaticamente (senza intervento dell'utente) i livelli di revisione dei driver e del BIOS installati su ciascun sistema client in rete e confronta tale inventario con i SoftPaq del software di sistema che sono stati verificati e memorizzati in un archivio centrale. L'utility SSM esegue quindi l'aggiornamento automatico delle eventuali versioni precedenti del software di sistema sui PC in rete con le versioni più recenti disponibili nell'archivio file. Poiché l'utility SSM consente la distribuzione degli aggiornamenti SoftPaq ai modelli di sistema del client corretti, gli amministratori possono utilizzarla in tutta fiducia e in modo efficace per mantenere aggiornato il software di sistema.

System Software Manager si integra con gli strumenti di distribuzione software aziendali come HP Configuration Management Solution, HP Client Manager for Altiris e Microsoft Systems Management Server (SMS). Grazie all'utility SSM, è possibile distribuire aggiornamenti creati dal cliente o da terze parti e forniti nel formato SSM.

L'utility SSM è scaricabile gratuitamente sul sito <http://www.hp.com/go/ssm>.

 **NOTA:** L'utility SSM attualmente non supporta il flash remoto della ROM su sistemi in cui Windows Vista BitLocker è abilitato e che utilizzano moduli TPM per proteggere le chiavi BitLocker poiché il flashing del BIOS potrebbe invalidare la firma attendibile creata da BitLocker per la piattaforma. Disattivare BitLocker tramite Criteri di gruppo per effettuare il flashing del BIOS di sistema.

È possibile abilitare il supporto per BitLocker senza misurazioni TMP del BIOS per evitare l'invalidazione delle chiavi di BitLocker. HP consiglia di conservare un backup protetto delle credenziali di BitLocker in caso di ripristino di emergenza.


# HP ProtectTools Security Manager

HP ProtectTools Security Manager è un software che fornisce funzioni di protezione create per salvaguardare il computer, le reti e i dati critici dall'accesso non autorizzato. I seguenti moduli software forniscono una funzionalità di protezione potenziata:

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

La disponibilità dei moduli software può variare a seconda del modello di computer. Ad esempio, Embedded Security for HP ProtectTools è disponibile solo per i computer che installano il chip TPM di protezione incorporata.

I moduli software HP ProtectTools possono essere preinstallati, preinstallati oppure disponibili per il download dal sito Web HP. Per determinati computer HP Compaq Desktop, HP ProtectTools è disponibile come opzione post-vendita. Per ulteriori informazioni, visitare il sito <http://www.hp.com>.

 **NOTA:** Le istruzioni presenti in questa guida sono state redatte presupponendo che l'utente abbia già installato i moduli software HP ProtectTools applicabili.

## HP Client Configuration Manager

HP Client Configuration Manager è una soluzione per la gestione hardware e software per gli ambienti Windows Vista, Windows XP e HP Thin Client semplice da utilizzare e installare e fornisce una base solida per i requisiti futuri. Viene offerta in due edizioni:

- La Basic Edition (edizione base) è un prodotto gratuito per la gestione di PC desktop, notebook e workstation HP e fornisce inventario hardware e software, controllo remoto, HP alert monitoring (monitoraggio allarmi HP), BIOS HP e aggiornamenti del driver, integrazione con HP Protect Tools e assistenza aggiuntiva per Intel AMT. La Basic Edition (edizione base) supporta anche deployment e gestione di HP Thin Client.
- La Premium Edition (edizione premium), disponibile per l'acquisto, include tutte le funzionalità della Basic Edition (edizione base) e inoltre aggiunge le funzionalità di deployment e migrazione Windows, capacità di gestione patch, distribuzione del software e misurazione dell'utilizzo del software.

HP Client Configuration Manager fornisce un percorso di migrazione verso HP Configuration Management Solution (basato sulla tecnologia Radia) per la gestione automatica di ambienti IT di grandi dimensioni, eterogenei e in continuo mutamento.

Per ulteriori informazioni su HP Client Configuration Manager, visitare il sito <http://www.managementsoftware.hp.com/products/ccm/index.html>.

# HP Configuration Management Solution

HP PC Configuration Management Solution è una soluzione basata su criteri che consente agli amministratori di inventariare, installare, applicare patch e gestire continuamente software e contenuti di piattaforme desktop eterogenee. Grazie a HP PC Configuration Management Solution i professionisti IT potranno:

- automatizzare il processo di gestione dell'intero ciclo di vita a partire dal rilevamento, al deployment e alla gestione continua attraverso migrazione e sospensione
- installare automaticamente e gestire continuamente un intero stack software (sistemi operativi, applicazioni, patch, impostazioni e contenuti)
- gestire virtualmente i software di ogni dispositivo, inclusi PC desktop, workstation e notebook, in una struttura eterogenea e standalone
- gestire software sulla maggior parte dei sistemi operativi

Grazie ad una gestione continua delle operazioni di configurazione i clienti HP riportano un notevole risparmio dei costi IT, la rapida introduzione sul mercato di software e contenuti e maggiore produttività e soddisfazione dell'utente.

Per ulteriori informazioni su HP PC Configuration Management Solution, visitare il sito <http://h20229.www2.hp.com/solutions/ascm/index.html>.

## HP Client Manager for Altiris

HP Client Manager, sviluppato in collaborazione con Altiris, è disponibile gratuitamente per tutti i modelli di PC desktop, notebook e workstation aziendali di HP. L'utility SSM è integrata in HP Client Manager e permette di eseguire la ricerca, il monitoraggio e la gestione centralizzati degli aspetti hardware dei sistemi client HP.

Utilizzare HP Client Manager per:

- Ottenere utili informazioni sull'hardware, come le impostazioni relative a CPU, memoria, video e protezione
- Monitorare le condizioni del sistema per prevenire i problemi
- Acquisire e installare automaticamente gli aggiornamenti dei driver e del BIOS senza recarsi personalmente presso ogni PC
- Configurare in remoto le impostazioni di BIOS e protezione
- Automatizzare i processi per risolvere rapidamente i problemi di hardware

La solida integrazione con gli strumenti di HP Instant Support riduce i tempi di risoluzione dei problemi di hardware.

- Diagnostica: eseguire e visualizzare in remoto i rapporti sui modelli PC desktop, notebook e workstation HP
- Scansione delle condizioni del sistema: rilevare i problemi dell'hardware noti nel database installato di sistemi client HP
- Chat attiva: connessione diretta con l'assistenza tecnica HP per risolvere i problemi.
- HP Knowledgebase: database delle conoscenze degli esperti
- Procedura di raccolta e consegna automatizzata dei SoftPak per una rapida risoluzione dei problemi di hardware
- Identificazione, gestione e inizializzazione dei sistemi con il chip di protezione incorporato di HP ProtectTools
- Visualizzazione locale opzionale degli allarmi sullo stato del sistema client
- Rapporto delle informazioni di inventario di base per i client non HP
- Installazione e configurazione del chip di protezione TPM
- Pianificazione a livello centrale del backup e del ripristino del client
- Aggiunta del supporto per la gestione di Intel AMT

Per ulteriori informazioni su HP Client Manager, visitare il sito <http://www.hp.com/go/clientmanager>.



## Altiris Client Management Suite

Altiris Client Management Suite è una soluzione facile da utilizzare per la gestione del ciclo di vita completo del software per PC desktop, notebook e workstation. Client Management Suite Level 1 include i seguenti prodotti Altiris:

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

Per ulteriori informazioni su Altiris Client Management Suite, visitare il sito <http://www.altiris.com/Products/ClientManagementSuite.aspx>.

## HP Client Catalog for SMS

La gestione degli aggiornamenti è una funzione importante per la manutenzione di un gruppo di computer, da un unico PC a un centro dati aziendale. La capacità di identificare gli aggiornamenti esistenti e implementarli selettivamente in maniera tempestiva e automatizzata contribuisce a salvaguardare la protezione e la produttività dell'organizzazione gestita. HP offre al momento un meccanismo che consente di semplificare gli aggiornamenti dei sistemi HP nell'ambito di un'infrastruttura di gestione Microsoft System Management Server. HP Client Catalog for SMS contiene driver di software e informazioni sulle patch per piattaforme desktop, notebook e workstation. Grazie a SMS 2003 R2 and Inventory Tool for Custom Updates, le aziende possono integrare e implementare gli aggiornamenti del software HP in modo semplice e rapido, in base alle caratteristiche dettagliate della piattaforma che HP Client Catalog for SMS offre ai sistemi client appropriati di destinazione all'interno dell'impresa gestita.

Per ulteriori informazioni su HP Client Catalog for SMS, visitare il sito <http://www.hp.com/go/easydeploy/>.

## HP Backup and Recovery Manager

L'applicazione HP Backup and Recovery Manager, versatile e facile da utilizzare, consente di eseguire il backup e ripristino dell'unità disco rigido principale sul PC. L'applicazione consente di creare backup del sistema operativo Windows, di tutte le applicazioni e di tutti i file di dati in ambiente Windows. È possibile pianificare l'esecuzione automatica del backup a intervalli prestabiliti, oppure avviarla manualmente. È possibile archiviare i file importanti separatamente dai normali backup.

L'applicazione HP Backup and Recovery Manager è preinstallata sulla partizione di ripristino dell'unità disco rigido.


È possibile copiare i punti di ripristino e i backup dei file su dischi CD o DVD, mentre tutti i backup possono essere copiati sulla rete o su unità disco rigido secondarie.

HP consiglia vivamente di creare un set di dischi di ripristino immediatamente prima di utilizzare il computer e di pianificare regolari backup automatici dei punti di ripristino.

Per creare un set di dischi di ripristino:

1. Selezionare **Start > HP Backup and Recovery > HP Backup and Recovery Manager** per aprire la procedura guidata Backup and Recovery Wizard, quindi selezionare **Avanti**.
2. Selezionare **Create a set of recovery discs (Recommended)** (Creare un set di dischi di ripristino (Consigliato)) e fare clic su **Avanti**.
3. Seguire le istruzioni visualizzate nella procedura guidata.

Per ulteriori informazioni sull'uso di HP Backup and Recovery Manager, consultare la *Guida dell'utente di HP Backup and Recovery Manager* selezionando **Start > HP Backup and Recovery > HP Backup and Recovery Manager Manual**.

 **NOTA:** È possibile ordinare un set di dischi di ripristino contattando l'assistenza clienti HP. Visitare il sito Web di seguito indicato, selezionare il paese e fare clic sul collegamento **Technical support after you buy (Assistenza tecnica dopo l'acquisto)** dal menu **Call HP (Contattare HP)** per ottenere il numero telefonico del centro assistenza del paese.

[http://welcome.hp.com/country/us/en/wwcontact\\_us.html](http://welcome.hp.com/country/us/en/wwcontact_us.html)


# PC Intel vPro con Active Management Technology

Intel Active Management Technology (AMT) consente di migliorare le procedure di rilevamento, risoluzione e protezione dei computer in rete. Grazie alla tecnologia AMT, è possibile gestire i PC indipendentemente dallo stato del sistema operativo (acceso, spento o bloccato).

Le caratteristiche di Intel vPro includono:

- Informazioni sull'inventario hardware
- Allarmi
- Gestione dell'alimentazione - accensione/spegnimento, ciclo di spegnimento e riaccensione
- Diagnosi e riparazione remota
  - Serial-over-LAN - consente il controllo del PC remoto mediante console nella fase di avvio
  - IDE-Redirect - permette di avviare il sistema da un'unità o da un disco di avvio remoto o da un'immagine ISO
- Isolamento e ripristino basato su hardware - limitare o interrompere l'accesso alla rete di PC al rilevamento di un'attività simile a un virus

---

 **NOTA:** Per una panoramica della tecnologia Intel vPro, visitare il sito <http://www.intel.com/vpro>.

Per informazioni specifiche di HP sulla tecnologia Intel vPro, consultare i white paper disponibili sul sito <http://www.hp.com/support>. Selezionare il paese e la lingua, scegliere **Visualizzazione delle informazioni sul supporto e la risoluzione dei problemi**, immettere il numero di modello del computer e premere **Invio**. Nella categoria **Risorse**, fare clic su **Manuali (guide, supplementi, addendum, ecc.)**. In **Accesso rapido alle guide per categoria**, fare clic su **White paper**.

---

Di seguito sono elencate alcune tra le tecnologie di gestione disponibili sui PC Intel vPro:


- AMT
- ASF
- Virtualization Technology (VT)

Benché siano entrambe supportate, può non essere possibile configurare contemporaneamente le tecnologie ASF e AMT.

Per configurare le tecnologie AMT o ASF sui sistemi Intel vPro:

1. Accendere o riavviare il computer. In Microsoft Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer si accende, premere i tasti di scelta rapida **Ctrl+P** quando la spia del monitor diventa verde.

---

 **NOTA:** Se al momento opportuno non viene premuta la combinazione di tasti **Ctrl+P**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **Ctrl+P** quando la spia del monitor diventa verde.

---

Questi tasti di scelta rapida consentono di accedere all'utility di setup Intel Management Engine BIOS Execution (MEBx). Questa utility consente di configurare vari aspetti della tecnologia di gestione. Le opzioni di configurazione includono:

- ME Platform Configuration
  - ME Platform State Control - abilitazione/disabilitazione del motore di gestione
  - ME Firmware Local Update - abilitazione/disabilitazione locale della gestione degli aggiornamenti del firmware
  - LAN Controller - abilitazione/disabilitazione del controller di rete integrato
  - ME Features Control - abilitazione della tecnologia AMT, ASF o di nessuna delle due
  - ME Power Control - configurazione dei criteri di alimentazione del motore di gestione
- Intel AMT Configuration
  - Change AMT Password - modifica della password richiesta per configurare AMT (la password predefinita è **admin**)
  - Host Name - consente all'amministratore di assegnare un nome al client
  - TCP/IP - consente all'amministratore di assegnare un indirizzo IP o di abilitare il protocollo DHCP
  - Provisioning Server - consente all'amministratore di assegnare l'indirizzo IP del provisioning server
  - Provision Model - consente all'amministratore di configurare la modalità aziendale o SMB
  - Set PID and PPS - consente all'amministratore di fornire la pre-provisioning key (consultare il white paper HP *Intel vPro Provisioning*)
  - Un-Provision - consente all'amministrazione di reimpostare i valori predefiniti della configurazione AMT
  - VLAN - consente all'amministratore di abilitare il supporto Virtual LAN
  - SOL/IDE-R - consente all'amministratore di abilitare l'avvio remoto e le sessioni di controllo
- Change MEBx Password (HP consiglia vivamente di modificare questa password. La password predefinita è **admin**).

Per gestire in remoto i sistemi AMT l'amministratore deve utilizzare una console remota che supporti AMT. Le console di gestione aziendale sono disponibili presso fornitori come HP, Altiris e Microsoft SMS. In modalità SMB, il client prevede un'interfaccia di browser Web. Per accedere a questa funzione, aprire un browser da qualsiasi sistema in rete e immettere `http://nome_host:16992`, dove `nome_host` è il nome assegnato al sistema. In alternativa, utilizzare l'indirizzo IP al posto del nome `host`.

## Verdiem Surveyor

Verdiem Surveyor è una soluzione software che contribuisce alla gestione dei costi energetici del PC. Surveyor calcola e riporta il consumo energetico di ogni computer. Inoltre, consente agli amministratori di controllare le impostazioni di alimentazione del PC, in modo che sia possibile implementare facilmente strategie di risparmio energetico su tutte le reti. È possibile scaricare dal sito Web di supporto HP un HP SoftPaq contenente l'agente Surveyor e installarlo sui modelli di PC desktop commerciali supportati. È possibile acquistare le licenze Surveyor per la gestione dei PC tramite il proprio rappresentante HP.

## HP Proactive Change Notification

Il programma Proactive Change Notification utilizza il sito Web Subscriber's Choice per effettuare in modo preventivo 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 a uno specifico ambiente informatico. Per saperne di più sul programma Proactive Change Notification e creare un profilo personalizzato, visitare il sito <http://h30046.www3.hp.com/subhub.php>

## Subscriber's Choice

Subscriber's Choice è un servizio HP basato su client.

In base al profilo dell'utente, HP fornirà suggerimenti personalizzati sui prodotti, articoli specialistici e/o avvisi/notifiche su driver e assistenza.

Il servizio Subscriber's Choice Driver and Support Alerts/Notifications invierà notifiche tramite posta elettronica per avvisare l'utente che le informazioni per le quali ha indicato interesse nel proprio profilo sono disponibili per la lettura e il download. Per saperne di più su Subscriber's Choice e creare un profilo personalizzato, visitare il sito <http://h30046.www3.hp.com/subhub.php>.

## Soluzioni sospese

Due pacchetti software, Altiris Local Recovery e Dantz Retrospect, non verranno più forniti su PC desktop, notebook o workstation aziendali HP. A cominciare dai prodotti distribuiti nel 2006, tutti i nuovi PC desktop, notebook e workstation saranno dotati di HP Backup and Recovery Manager.

---

## 5 Flash della ROM

Il BIOS del computer è memorizzato in una ROM flash programmabile (memoria di sola lettura). 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. Nel caso fosse necessario oppure opportuno aggiornare il BIOS, scaricare le immagini del BIOS più recenti dalla pagina Supporto e Driver di HP sul sito <http://www.hp.com/support/files>.

- △ **ATTENZIONE:** Per garantire la massima protezione della ROM, è bene impostare una password di configurazione. La password di configurazione impedisce gli aggiornamenti non autorizzati della ROM. System Software Manager consente all'amministratore di sistema di impostare la password di configurazione su uno o più PC contemporaneamente. Per ulteriori informazioni, visitare il sito <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 il BIOS dei computer HP remoti direttamente dalla console di gestione centralizzata della rete. Se si consente all'amministratore del sistema di eseguire tale operazione a distanza e su più computer, la distribuzione delle immagini BIOS dei PC HP in rete sarà più uniforme e sarà possibile un maggior controllo su di esse. Inoltre, ne derivano una maggiore produttività e una diminuzione dei costi totali di gestione.

- 📄 **NOTA:** L'utility SSM attualmente non supporta il flash remoto della ROM su sistemi in cui Windows Vista BitLocker è abilitato e che utilizzano moduli TPM per proteggere le chiavi BitLocker poiché il flashing del BIOS potrebbe invalidare la firma attendibile creata da BitLocker per la piattaforma. Disattivare BitLocker tramite Criteri di gruppo per effettuare il flashing del BIOS di sistema.

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

Per ulteriori informazioni sul flash remoto della ROM vedere HP Client Manager Software o System Software Manager sul sito <http://www.hp.com/go/ssm/>.

### HPQFlash

L'utility HPQFlash permette di aggiornare o ripristinare localmente il BIOS di sistema di singoli PC da un unico sistema operativo Windows.

Per ulteriori informazioni su HPQFlash, visitare il sito <http://www.hp.com/support/files> e immettere il numero del modello di computer quando richiesto.

## 6 Boot Block Emergency Recovery Mode

Boot Block Emergency Recovery Mode (modalità di ripristino di emergenza con blocco di avvio) consente il ripristino del sistema nel caso, improbabile, che il flash della ROM non abbia avuto esito positivo. Ad esempio, in caso di interruzione dell'energia elettrica durante l'aggiornamento del BIOS, il flash della ROM sarebbe incompleto, rendendo inutilizzabile il BIOS di sistema. Il blocco dell'avvio è una sezione della ROM con protezione flash contenente un codice che effettua un controllo di convalida dell'immagine BIOS ogni volta che il sistema viene acceso.


- Se l'immagine del BIOS di sistema è valida, il sistema parte normalmente.
- Se l'immagine del BIOS di sistema non è valida, il BIOS del blocco di avvio FailSafe fornisce un supporto sufficiente a cercare supporti rimovibili per i file di immagine BIOS. Se viene rilevato un file immagine BIOS adeguato, viene automaticamente eseguito il flash nella ROM.

Quando viene rilevata un'immagine del BIOS di sistema non valida, il LED di alimentazione di sistema diventa di colore rosso e lampeggia 8 volte, una al secondo. Contemporaneamente, l'altoparlante emetterà un segnale acustico per 8 volte. Se la parte della ROM di sistema contenente l'immagine ROM dell'opzione video non è danneggiata, sullo schermo verrà visualizzato **Boot Block Emergency Recovery Mode** (Modalità di ripristino di emergenza blocco di avvio).

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

1. Spegnerne il computer.
2. Inserire un CD o un dispositivo flash USB contenente il file di immagine BIOS desiderato nella directory principale.

---

 **NOTA:** Il supporto deve essere formattato mediante il file system FAT12, FAT16 o FAT32.

---


3. Accendere il computer.

Se non è stato rilevato un file di immagine BIOS appropriato, verrà richiesto di inserire un supporto contenente un file di immagine BIOS.

Se la ROM è stata correttamente riprogrammata, il sistema verrà automaticamente spento.

4. Estrarre il supporto rimovibile utilizzato per aggiornare il BIOS.
5. Accendere il computer per riavviarlo.

---


 **NOTA:** BitLocker impedisce l'avvio di Windows Vista quando nell'unità ottica è inserito un CD contenente un file di immagine BIOS. Se BitLocker è abilitato, rimuovere il CD prima di riavviare Windows Vista.

---



# 7 Replica delle impostazioni


Queste procedure consentono all'amministratore di copiare facilmente la configurazione di un computer su altri dello stesso modello. Ciò consente una configurazione più veloce e uniforme di più computer.

 **NOTA:** Per 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 di 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 computer dc7xxx su un modello dx7xxx.

1. Selezionare una configurazione del setup da copiare. Spegnerne il computer. In Microsoft Windows fare clic su **Start > Chiudi sessione > Arresta il sistema**.
2. Se si utilizza un supporto USB flash media, inserirlo.
3. Accendere il computer.
4. Non appena il computer è acceso, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per escludere la schermata del titolo.

 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.

5. Se si utilizza un dischetto, inserirlo ora.
6. Selezionare **File > Replicated Setup** (Impostazioni replicate) > **Save to Removable Media** (Salva su supporti rimovibili). Seguire le istruzioni visualizzate sullo schermo per creare il dischetto o il dispositivo USB flash media di configurazione.
7. Spegnerne il computer da configurare e inserire il dischetto o il dispositivo USB flash media di configurazione.
8. Accendere il computer da configurare.
9. Non appena il computer è acceso, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per escludere la schermata del titolo.
10. Selezionare **File > Replicated Setup** (Impostazioni replicate) > **Restore from Removable Media** (Ripristina da supporti rimovibili) e seguire le istruzioni visualizzate sullo schermo.
11. Riavviare il computer al termine della configurazione.

## Copia su più computer

- △ **ATTENZIONE:** La configurazione è specifica per ogni modello. Se i computer di 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 computer dc7xxx su un modello dx7xxx.

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

- 📝 **NOTA:** Per questa procedura, è necessario un dischetto di avvio oppure creare un dispositivo flash media USB di avvio. Se non è possibile utilizzare Windows XP per creare un dischetto di avvio, utilizzare il metodo per la copia su un singolo computer (vedere [Copia su computer singolo a pagina 19](#)).

1. Creare un dischetto di avvio o un dispositivo USB flash media. Vedere [Dispositivo USB flash media compatibile a pagina 21](#) o [Dispositivi USB flash media non compatibili a pagina 22](#).

- △ **ATTENZIONE:** Non è possibile avviare tutti i computer da un dispositivo USB flash media. Se nella sequenza di avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, è possibile avviare il computer dal dispositivo USB flash media. Altrimenti, utilizzare esclusivamente un dischetto di avvio.

2. Selezionare una configurazione del setup da copiare. Spegnerne il computer. In Microsoft Windows fare clic su **Start > Chiudi sessione > Arresta il sistema**.
3. Se si utilizza un supporto USB flash media, inserirlo ora.
4. Accendere il computer.
5. Non appena il computer è acceso, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

- 📝 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.

6. Se si utilizza un dischetto, inserirlo.
7. Selezionare **File > Replicated Setup** (Impostazioni replicate) > **Save to Removable Media** (Salva su supporti rimovibili). Seguire le istruzioni visualizzate sullo schermo per creare il dischetto o il dispositivo USB flash media di configurazione.
8. Scaricare una utility BIOS per replicare il setup (repset.exe) e copiarla sul dischetto o sul dispositivo USB flash media di configurazione. Per scaricare questa utility, accedere al sito <http://welcome.hp.com/country/us/en/support.html> e immettere il numero del modello del computer.
9. Sul dischetto o sul dispositivo USB flash media di configurazione, creare un file autoexec.bat contenente il seguente comando:

```
repset.exe
```

10. Spegnerne il computer da configurare. Inserire il dischetto o il dispositivo USB flash media di configurazione e accendere il computer. L'utility di configurazione verrà eseguita automaticamente.
11. Riavviare il computer al termine della configurazione.

# Creazione di un dispositivo d'avvio

## Dispositivo USB flash media compatibile

I dispositivi compatibili sono dotati di un'immagine preinstallata che ne semplifica l'avvio. Tutti i dispositivi USB flash media HP o Compaq e molti altri sono dotati di questa immagine preinstallata. Se il dispositivo USB flash media in uso non è dotato di questa immagine, utilizzare la procedura descritta più avanti in questa sezione (vedere [Dispositivi USB flash media non compatibili a pagina 22](#)).

Per creare un dispositivo USB flash media di avvio è necessario disporre di quanto segue:

- Un dispositivo USB flash media compatibile
- Un dischetto DOS avviabile con i programmi FDISK e SYS. Se SYS non è disponibile, utilizzare FORMAT, che però comporta la cancellazione di tutti i file esistenti sul dispositivo USB flash media.
- Un PC avviabile mediante un dispositivo USB flash media

△ **ATTENZIONE:** Non è possibile avviare alcuni PC più obsoleti da un dispositivo USB flash media. Se nella sequenza di avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, è possibile avviare il computer da un dispositivo USB flash media. Altrimenti, utilizzare esclusivamente un dischetto di avvio.

1. Spegnerne il computer.
2. Inserire il dispositivo USB flash media in una delle porte USB del computer e rimuovere tutti gli altri dispositivi di memorizzazione USB, tranne le unità a dischetti USB.
3. Inserire un dischetto DOS di avvio con FDISK.COM e un programma a scelta tra SYS.COM o FORMAT.COM in un'unità a dischetti, quindi accendere il computer per avviare il dischetto DOS.
4. Per eseguire FDISK dal prompt **A:\** digitare `FDISK` e premere Invio. Alla richiesta del sistema, fare clic su **Yes (Y)** per abilitare la compatibilità con dischi di grandi dimensioni.
5. Immettere l'opzione [5] per visualizzare le unità del sistema. L'unità più simile per dimensioni a una di quelle elencate è il dispositivo USB flash media. Di solito è l'ultima dell'elenco. Annotare la lettera dell'unità.

Unità dispositivo USB flash media: \_\_\_\_\_

△ **ATTENZIONE:** Se un'unità non corrisponde al dispositivo USB flash media, non procedere: potrebbe verificarsi una perdita di dati. Verificare su tutte le porte USB la presenza di ulteriori dispositivi di memorizzazione. Se presenti, rimuoverli, riavviare il computer e procedere dal punto 4. Se non viene rilevato alcun dispositivo, il sistema non supporta il dispositivo USB flash media oppure quest'ultimo è difettoso. **NON tentare di rendere avviabile il dispositivo USB flash media.**

6. Uscire da FDISK premendo il tasto **Esc** per tornare al prompt **A:\**.
7. Se il dischetto DOS di avvio 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 annotata in precedenza.

△ **ATTENZIONE:** Assicurarsi di immettere correttamente la lettera dell'unità corrispondente al dispositivo USB flash media.

Al termine del trasferimento dei file di sistema, verrà nuovamente visualizzato il prompt **A:\**. Passare al punto 13.

9. Copiare i file desiderati dal dispositivo USB flash media in una directory temporanea su un'altra unità (ad esempio, l'unità disco rigido interna del sistema).

10. Al prompt **A:\**, digitare `FORMAT /S X:` dove X rappresenta la lettera dell'unità annotata in precedenza.

△ **ATTENZIONE:** Assicurarsi di immettere correttamente la lettera dell'unità corrispondente al dispositivo USB flash media.

FORMAT visualizza uno o più avvisi, chiedendo ogni volta la conferma a procedere. Digitare **Y** ogni volta. FORMAT formatta il dispositivo USB flash media, aggiunge i file di sistema e chiede di immettere un'etichetta di volume.

11. Immettere un'etichetta oppure premere **Invio** se non si desidera immettere alcuna etichetta.
12. Copiare gli eventuali file salvati al punto 9 sul dispositivo USB flash media.
13. Togliere il dischetto e riavviare il computer. Il computer verrà riavviato con il dispositivo USB flash media come unità C.

📝 **NOTA:** La sequenza di 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. Se non si desidera visualizzare questa schermata, aggiungere un file di zero byte denominato LOGO.SYS alla directory principale del dispositivo USB flash media.

Tornare a [Copia su più computer a pagina 20](#).

## Dispositivi USB flash media non compatibili

Per creare un dispositivo USB flash media di avvio è necessario disporre di quanto segue:

- Un dispositivo USB flash media
- Un dischetto DOS di avvio con i programmi FDISK e SYS. Se SYS non è disponibile, utilizzare FORMAT, che però comporta la cancellazione di tutti i file esistenti sul dispositivo USB flash media.
- Un PC avviabile mediante un dispositivo USB flash media

△ **ATTENZIONE:** Non è possibile avviare alcuni PC più obsoleti da un dispositivo USB flash media. Se nella sequenza di avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, è possibile avviare il computer da un dispositivo USB flash media. Altrimenti, utilizzare esclusivamente un dischetto di avvio.

1. Se nel sistema sono presenti schede PCI a cui sono collegate unità SCSI, ATA RAID o SATA, spegnere il computer e scollegare il cavo di alimentazione.

△ **ATTENZIONE:** Il cavo di alimentazione DEVE essere scollegato.

2. Aprire il computer e rimuovere le schede PCI.
3. Inserire il dispositivo USB flash media in una delle porte USB del computer e rimuovere tutti gli altri dispositivi di memorizzazione USB, tranne le unità a dischetti USB. Chiudere il coperchio del computer.
4. Collegare il cavo di alimentazione e accendere il computer.
5. Non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per escludere la schermata del titolo.


📝 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.

- Scegliere **Advanced** (Avanzate) > **PCI Devices** (Dispositivi PCI) per disabilitare i controller PATA e SATA. Nel disabilitare il controller SATA, annotare l'IRQ al quale è stato assegnato. In seguito sarà necessario rassegnare questo IRQ. Confermare le modifiche e uscire dal setup.

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

- Inserire un dischetto DOS di avvio con FDISK.COM e un programma a scelta tra SYS.COM o FORMAT.COM in un'unità a dischetti, quindi accendere il computer per avviare il dischetto DOS.
- Eeguire FDISK ed eliminare eventuali partizioni esistenti sul dispositivo USB flash media. Creare una nuova partizione e contrassegnarla come attiva. Premere il tasto **esc** per uscire da FDISK.
- Se il sistema non è stato automaticamente riavviato all'uscita da FDISK, premere **Ctrl+Alt+Canc** per riavviare il dischetto DOS.
- Al prompt di **A:\**, digitare `FORMAT C: /S` e premere **Invio**. FORMAT formatterà il dispositivo USB flash media, aggiungerà i file di sistema e chiederà di immettere l'etichetta di volume.
- Immettere un'etichetta oppure premere **Invio** se non si desidera immettere alcuna etichetta.
- Spegnere il computer e scollegare il cavo di alimentazione. Aprire il computer e reinstallare le schede PCI precedentemente rimosse. Chiudere il coperchio del computer.
- Collegare il cavo di alimentazione, rimuovere il dischetto e accendere il computer.
- Non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.
- Selezionare **Advanced** (Avanzate) > **PCI Devices** (Dispositivi PCI) e riabilitare i controller PATA e SATA che erano stati disabilitati al punto 6. Assegnare il controller SATA all'IRQ originale.
- Salvare le modifiche e uscire. Il computer verrà riavviato con il dispositivo USB flash media come unità C.

---

 **NOTA:** La sequenza di avvio predefinita varia da computer a computer e può essere modificata nell'utility Computer Setup (F10). Per ottenere le istruzioni, consultare la *Guida dell'utility Computer Setup (F10)*.

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

---

Tornare a [Copia su più computer a pagina 20](#).

---

## 8 Pulsante d'accensione a doppio stato

Con le funzioni Advanced Configuration and Power Interface (ACPI) abilitate, il pulsante di alimentazione può funzionare come interruttore di accensione o come pulsante di standby. La funzione di standby non spegne completamente il computer, ma fa entrare il computer in una modalità a basso consumo energetico. In tal modo sarà possibile spegnere velocemente il computer senza chiudere le applicazioni e tornare altrettanto velocemente allo stesso stato operativo senza alcuna perdita di dati.

Per cambiare la configurazione del pulsante d'accensione procedere come segue:

1. Fare clic su **Start** e selezionare **Pannello di controllo > Opzioni risparmio energia**.
2. In **Proprietà - Opzioni risparmio energia** selezionare la scheda **Avanzate**.
3. Nella sezione **Pulsanti di alimentazione**, selezionare **Standby**.

Dopo aver configurato il pulsante di accensione come pulsante di standby, premerlo per attivare lo stato di alimentazione ridotta del sistema (standby). Premere di nuovo il pulsante per riportare rapidamente il sistema dallo 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 risponda; lo spegnimento del computer senza interazione con il sistema operativo può provocare danni al disco fisso o perdita di dati.

---

---

## 9 Assistenza sul sito Web HP

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. È possibile scaricare il software dal sito <http://www.hp.com/support>.

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

---

## 10 Standard di settore

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


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



# 11 Controllo e sicurezza degli asset

Le funzioni di controllo asset integrate nei PC forniscono dati di controllo sulle principali risorse gestibili con soluzioni HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration 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. Se installato, HP Embedded Security for ProtectTools impedisce l'accesso non autorizzato ai dati e verifica l'integrità del sistema, autenticando gli utenti di terze parti che tentino l'accesso al sistema (per ulteriori informazioni consultare la guida *HP ProtectTools Security Manager Guide* sul sito <http://www.hp.com>). Le funzioni di sicurezza come HP Embedded Security for 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 o 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.

 **NOTA:** HP Embedded Security for ProtectTools, il sensore e la chiusura Smart Cover sono disponibili come opzione su alcuni sistemi.

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

- Localmente, utilizzando le utility Computer Setup. Per ulteriori informazioni sull'uso delle utility Computer Setup vedere la *Guida all'utility Computer Setup (F10)* in dotazione al computer. Alcuni computer dispongono inoltre del componente HP BIOS Configuration for ProtectTools, basato su Windows, che consente agli amministratori di configurare le impostazioni di protezione del BIOS dal sistema operativo in esecuzione.
- In remoto, utilizzare HP Client Manager, HP Client Configuration Manager o System Software Manager. Questo software consente un'installazione sicura e ottimizzata e permette di controllare le impostazioni di sicurezza.

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

**Tabella 11-1** Panoramica delle funzioni di sicurezza

Opzione	Descrizione
Password di configurazione	Consente di impostare e abilitare la password di configurazione (amministratore).  <b>NOTA:</b> Se la password di configurazione è impostata, è necessario modificare le opzioni Computer Setup, eseguire il flash della ROM ed eseguire le modifiche ad alcune impostazioni plug and play in Windows.  Per ulteriori informazioni consultare la <i>Guida alla risoluzione dei problemi</i> .

**Tabella 11-1 Panoramica delle funzioni di sicurezza (continuazione)**

Opzione	Descrizione
Password di accensione)	<p>Consente di impostare ed abilitare la password di configurazione (password dell'amministratore). Dopo aver spento e riacceso il computer, appare il prompt per la password di accensione. Se l'utente non immette la password di accensione corretta, l'unità non viene avviata.</p> <p><b>NOTA:</b> Questa password non appare quando si riavvia premendo la combinazione di tasti <b>Ctrl+Alt+Canc</b> o si seleziona il pulsante <b>Riavvia da Windows</b>, a meno che non sia stata abilitata nella sezione <b>Password Options</b> (Opzioni password).</p> <p>Per ulteriori informazioni consultare la <i>Guida alla risoluzione dei problemi</i>.</p>
Password Options (Opzioni password)	<p>Consente di specificare se la password è richiesta per l'avvio a caldo (<b>Ctrl+Alt+Canc</b>).</p> <p>Questa selezione appare solo se è stata impostata una password di accensione.</p> <p>Per ulteriori informazioni consultare la <i>Guida alla risoluzione dei problemi</i>.</p>
Pre-Boot Authorization (Autorizzazione preliminare all'avvio)	<p>Consente di abilitare/disabilitare la Smart Card da usare al posto della password di accensione.</p>
Smart Cover (alcuni modelli)	<p>Consente di:</p> <ul style="list-style-type: none"> <li>• Abilitare/disabilitare il dispositivo di chiusura del coperchio.</li> <li>• Abilitare/disabilitare il sensore di assenza coperchio.</li> </ul> <p><b>NOTA:</b> <i>(Please insert SW in English first and then IT translation in brackets, as per above suggestions) Notify User</i> avverte l'utente che è stato rilevato il sensore di assenza coperchio. <i>Setup Password</i> (Password di configurazione) richiede che venga inserita la password di configurazione per avviare il computer se il sensore rileva l'assenza del coperchio.</p>
Embedded Security (Sicurezza integrata)	<p>Consente di:</p> <ul style="list-style-type: none"> <li>• Abilitare/disabilitare il dispositivo di sicurezza integrata.</li> <li>• Ripristinare le impostazioni di fabbrica.</li> </ul> <p>Questa funzione è supportata solo su alcuni modelli. Vedere la guida <i>HP ProtectTools Security Manager Guide</i> sul sito <a href="http://www.hp.com">http://www.hp.com</a></p>
Device Security (Sicurezza periferiche)	<p>Abilita/disabilita le porte seriali, le porte parallele, le porte USB frontali, l'audio di sistema, i controller di rete (alcuni modelli) e i controller SCSI (alcuni modelli).</p>
Avvio servizio di rete)	<p>Attiva/disattiva la capacità del computer di avviarsi da un sistema operativo installato su un server di rete (funzione disponibile solo su modelli di schede di rete; il controller di rete deve essere una scheda di espansione PCI o essere integrato sulla scheda di sistema).</p>
System Ids (ID di sistema)	<p>Consente di impostare:</p> <ul style="list-style-type: none"> <li>• Contrassegno risorse (di 18 byte) e contrassegno di proprietà (identificativo di 80 byte visualizzato durante la fase POST) Per ulteriori informazioni consultare la <i>Guida dell'utility Computer Setup (F10)</i>.</li> <li>• 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.)</li> </ul>
DriveLockSecurity (alcuni modelli)	<p>Consente di assegnare o modificare una password principale o utente per le unità disco fisso. 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.</p>

**Tabella 11-1** Panoramica delle funzioni di sicurezza (continuazione)

Opzione	Descrizione
	<b>NOTA:</b> Questa selezione appare solo quando al sistema è collegata almeno un'unità che supporta la funzione DriveLock.
	Per ulteriori informazioni su Computer Setup, consultare la <i>Guida dell'utility Computer Setup (F10)</i> .
	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 configurazione impedisce in modo specifico l'accesso non autorizzato a Computer Setup, ma può essere anche utilizzata per bypassare 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 protezione incorporato, consultare la guida *HP ProtectTools Security Manager Guide* sul sito <http://www.hp.com>. 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. In Microsoft Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per escludere la schermata del titolo.


 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.

3. Selezionare **Security** (Sicurezza), quindi **Password di configurazione** e seguire le istruzioni visualizzate sullo schermo.
4. Prima di uscire, scegliere **File > Save Changes and Exit** (Salva modifiche ed esci).

### Impostazione di una password di accensione tramite 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 in **Password Options** (Opzioni password) nel menu **Security** (Protezione). 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 deve essere immessa ogni volta che il computer viene riavviato.

1. Accendere o riavviare il computer. In Microsoft Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.


3. Selezionare **Security** (Protezione), quindi **Power-On Password** (Password di accensione) e seguire le istruzioni visualizzate sullo schermo.
4. Prima di uscire, scegliere **File > Save Changes and Exit** (Salva modifiche ed esci).

## Immissione della password di accensione

Per immettere la password d'accensione, seguire questa procedura:

1. Accendere o riavviare il computer. In ambiente 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**.

---

 **NOTA:** 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 configurazione

Se il sistema è dotato di un dispositivo di protezione incorporato, consultare la guida *HP ProtectTools Security Manager Guide* sul sito <http://www.hp.com>.

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. In Microsoft Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.


---

 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.

---

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

---

 **NOTA:** 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 protezione incorporato, consultare la guida *HP ProtectTools Security Manager Guide* sul sito <http://www.hp.com>.

1. Accendere o riavviare il computer. In ambiente Windows, scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Per modificare la password di accensione, passare al punto 3.

Per modificare la password di configurazione, non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.


 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.

3. Quando viene visualizzata l'icona della chiave, digitare la password corrente, una barra (/) o un carattere delimitatore alternativo, la nuova password, un'altra barra (/) o un carattere delimitatore alternativo e ancora la nuova password, nel modo seguente: `password attuale/nuova password/nuova password`

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

4. Premere **Invio**.

La nuova password sarà valida a partire dalla successiva accensione del computer.


 **NOTA:** Per informazioni sui caratteri delimitatori alternativi, consultare [Caratteri delimitatori delle tastiere nazionali a pagina 32](#). È possibile modificare le password di accensione e di configurazione 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 protezione incorporato, consultare la guida *HP ProtectTools Security Manager Guide* sul sito <http://www.hp.com>.


1. Accendere o riavviare il computer. In ambiente Windows, scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Per eliminare la password di accensione, passare al punto 3.

Per eliminare la password di configurazione, non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.

 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.

3. Quando viene visualizzata l'icona della chiave, digitare la password attuale seguita da una barra (/) o da un carattere delimitatore alternativo, nel modo seguente: `password attuale/`

4. Premere **Invio**.

 **NOTA:** Per informazioni sui caratteri delimitatori alternativi, consultare [Caratteri delimitatori delle tastiere nazionali a pagina 32](#). È possibile modificare le password di accensione e di configurazione anche utilizzando le opzioni di sicurezza di Computer Setup.

## Caratteri delimitatori delle tastiere nazionali

Le singole tastiere sono progettate per soddisfare i requisiti specifici dei rispettivi paesi. La sintassi e i tasti utilizzati per modificare o eliminare la password dipendono dalla tastiera fornita con il computer.

Caratteri delimitatori delle tastiere nazionali					
/	Araba	-	Greca	/	Russa
=	Belga	.	Ebraica	-	Slovacca
-	BECSI*	-	Ungherese	-	Spagnola
/	Brasiliana	-	Italiana	/	Svedese/Finnica
/	Cinese	/	Giapponese	-	Svizzera
-	Ceca	/	Coreana	/	Taiwanese
-	Danese	-	Latino-americana	/	Tailandese
!	Francese	-	Norvegese	.	Turca
é	Canadese francofona	-	Polacca	/	Inglese
-	Tedesca	-	Portoghese		

\* Per Bosnia-Erzegovina, Croazia, Slovenia e Jugoslavia

## Annullamento password

Se si dimentica la password, non è possibile accedere al computer. Per istruzioni sull'annullamento delle password, consultare la *Guida alla risoluzione dei problemi*.

Se il sistema è dotato di un dispositivo di protezione incorporato, consultare la guida *HP ProtectTools Security Manager Guide* sul sito <http://www.hp.com>.

## DriveLock

DriveLock è una funzione di sicurezza di standard industriale che impedisce l'accesso non autorizzato ai dati memorizzati su unità disco rigido ATA. DriveLock è stato implementato come estensione di Computer Setup ed è disponibile solo se vengono rilevate unità disco rigido che supportano il set di comandi di protezione ATA. 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 deve 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 l'unità 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 presentano questo tipo di esigenza, questo può essere un rischio inaccettabile. Per quelli, invece, che presentano questo tipo di esigenza, il rischio può essere tollerabile, data la natura dei dati memorizzati sul disco.

## Uso di DriveLock

Quando vengono rilevate una o più unità disco rigido che supportano il set di comandi di protezione ATA, l'opzione DriveLock compare nel menu Security di Computer Setup. L'utente ha la possibilità di impostare la password principale o di abilitare DriveLock. Per abilitare DriveLock deve essere specificata una password utente. Dal momento che la configurazione iniziale di DriveLock viene

normalmente eseguita da un amministratore di sistema, deve 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, verrà chiesta la password per sbloccarlo durante il POST. Se viene impostata una password di accensione e quest'ultima coincide con quella dell'utente della periferica, durante il POST non viene richiesto all'utente di reimmettere la password. Diversamente, all'utente viene richiesto di immettere la password per accedere a DriveLock. Dopo un avvio a freddo, è possibile utilizzare la password principale o quella dell'utente. Dopo un avvio a caldo, immettere la stessa password utilizzata per sbloccare l'unità durante il precedente avvio a freddo. Gli utenti hanno a disposizione due tentativi per immettere la password corretta. Se dopo l'avvio a freddo nessun tentativo ha esito positivo, il POST prosegue, ma i dati sull'unità restano inaccessibili. Se dopo l'avvio a freddo o il riavvio da Windows nessun tentativo ha esito positivo, il POST si interromperà e verrà richiesto di spegnere e riaccendere il computer.

## Applicazioni di DriveLock

L'utilizzo più pratico della funzione di protezione DriveLock è negli ambienti aziendali. L'amministratore di sistema è responsabile della configurazione dell'unità disco rigido che comporta, tra l'altro, l'impostazione della password principale di DriveLock e una password utente temporanea. Se l'utente dimentica la sua password o la macchina viene ceduta 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 utenti singoli 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:

**Tabella 11-2 Livelli di protezione del sensore Smart Cover**

Livello	Impostazione	Descrizione
Livello 0	Disabilitata	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	Password di configurazione	Quando il computer viene riavviato, sullo schermo viene visualizzato un messaggio che avverte che il coperchio o il pannello laterale del


**Tabella 11-2 Livelli di protezione del sensore Smart Cover (continuazione)**

Livello	Impostazione	Descrizione
		computer sono stati rimossi. Per continuare, è necessario immettere la password di configurazione.

**NOTA:** Le impostazioni possono essere modificate tramite Computer Setup. Per ulteriori informazioni su Computer Setup, consultare la *Guida dell'utility Computer Setup (F10)*.


## Impostazione del livello di protezione del sensore Smart Cover

Per impostare il livello di protezione del sensore Smart Cover, seguire questa procedura:

1. Accendere o riavviare il computer. In Microsoft Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.  
 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.
3. Selezionare **Security (Protezione) > Smart Cover > Cover Removal Sensor** (Sensore di assenza coperchio) e selezionare il livello di sicurezza desiderato.
4. Prima di uscire, scegliere **File > Save Changes and Exit** (Salva modifiche ed esci).

## Chiusura Smart Cover


La chiusura Smart Cover è un dispositivo di blocco controllato da software, presente su alcuni computer HP. Essa impedisce l'accesso non autorizzato ai componenti interni. I computer vengono consegnati con la chiusura Smart Cover sbloccata.

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

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

## Blocco della chiusura Smart Cover

Per attivare la chiusura Smart Cover, seguire questa procedura:


1. Accendere o riavviare il computer. In Microsoft Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.  
 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.
3. Selezionare **Security (Protezione) > Smart Cover > Cover Lock (Blocco coperchio) > Lock (Blocca)**.
4. Prima di uscire, scegliere **File > Save Changes and Exit** (Salva modifiche ed esci).



## Disattivazione del blocco della chiusura Smart Cover

1. Accendere o riavviare il computer. In Microsoft Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer si accende, premere **F10** quando la spia del monitor diventa verde per accedere a Computer Setup. Se necessario, premere **Invio** per saltare la schermata del titolo.  

---

 **NOTA:** Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario riavviare il computer e premere di nuovo **F10** quando la spia del monitor diventa verde.
3. Selezionare **Security (Protezione) > Smart Cover > Cover Lock (Blocco coperchio) > Unlock (Sblocca)**.
4. Prima di uscire, scegliere **File > Save Changes and Exit (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 rivenditore o un centro assistenza autorizzato.

Per ottenere la chiave FailSafe, è possibile agire in uno dei due modi seguenti:

- Contattare il rivenditore o un centro assistenza autorizzato 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*.


## Predisposizione per fissaggio con cavo

Sul pannello posteriore è presente una fessura per l'inserimento di un cavo in modo che il computer possa essere fisicamente fissato ad un posto di lavoro (solo in alcuni modelli).

Per le istruzioni consultare la *Guida di riferimento hardware*.

## 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.

 **NOTA:** 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

La notifica dei guasti e le funzioni di ripristino combinano hardware innovativo e tecnologia software al fine di prevenire la perdita di dati critici e minimizzare i periodi di inattività non programmati.

Se il computer è collegato a 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 inoltre possibile pianificare in remoto l'esecuzione automatica della diagnostica su tutti i PC gestiti e la creazione di un rapporto riepilogativo dei test non riusciti.

## Drive Protection System (DPS)

Il Drive Protection System (DPS) è uno strumento di diagnostica incorporato nelle unità disco rigido installate 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, le unità disco rigido installate vengono collaudate una per una tramite DPS e in esse viene registrato un record permanente di dati chiave. Ogni volta che viene eseguito il DPS, gli esiti del test vengono scritti sull'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 istruzioni sull'utilizzo del DPS, consultare la *Guida alla risoluzione dei problemi*.

## Alimentatore protetto contro gli sbalzi di tensione

Un alimentatore con tolleranza degli sbalzi integrato assicura maggiore affidabilità quando il computer è sottoposto a improvvisi sbalzi di corrente. L'alimentatore è concepito per tollerare sbalzi di tensione fino a 2000 volt, senza esporre il sistema a 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, viene visualizzato un messaggio di avvertimento che consente di disporre del tempo necessario per intervenire prima che vengano danneggiati i componenti interni o si verifichi una perdita di dati.

# Indice analitico

- A**  
accesso al computer,  
controllo 27  
Active Management Technology,  
PC Intel vPro 13  
alimentatore protetto contro gli  
sbalzi di tensione 37  
Altiris  
AClient 3  
Deployment Solution Agent 3  
asset, controllo 27  
attenzione  
chiave FailSafe 35  
protezione della ROM 17  
sicurezza chiusura  
coperchio 34  
avviabile, dispositivo  
creazione 21  
DiskOnKey 21, 22  
HP Drive Key 22  
USB flash media,  
dispositivo 21
- B**  
BIOS  
Boot Block Emergency  
Recovery Mode 18  
Flash remoto della ROM 17  
HPQFlash 17  
blocco della chiusura Smart  
Cover 34  
Boot Block Emergency Recovery  
Mode 18
- C**  
cambiamento password 31  
cancellazione password 31  
caratteri delimitatori delle tastiere  
nazionali 32  
caratteri delimitatori, tabella 32  
chiave FailSafe  
attenzione 35  
ordinazione 35  
chiave FailSafe di Smart Cover,  
ordinazione 35  
chiusura Smart Cover  
blocco 34  
chiave FailSafe 35  
sblocco 35  
Client Management Interface 5  
Client Manager 10  
Configuration Management  
Solution 9  
configurazione iniziale 2  
configurazione pulsante di  
accensione 24  
controllo dell'accesso al  
computer 27  
coperchio, chiusura 34
- D**  
dischi fissi, strumenti  
diagnostici 37  
dischi, protezione 37  
disco, clonazione 2  
DiskOnKey  
avviabile 21, 22  
HP Drive Key 21  
dispositivo di avvio  
HP Drive Key 21  
dispositivo USB flash media,  
avviabile 21, 22  
DriveLock  
applicazioni 33  
utilizzo 32
- E**  
eliminazione password 32  
Emergency Recovery Mode, Boot  
Block 18
- F**  
fissaggio con cavo 35  
Flash remoto della ROM 17
- H**  
HP  
Client Management  
Interface 5  
Client Manager for Altiris 10  
Configuration Management  
Solution 9  
ProtectTools Security  
Manager 7  
System Software Manager 7  
HP Client Catalog for SMS 11  
HP Drive Key  
avviabile 21, 22  
DiskOnKey 21  
HP Lifecycle solutions 2  
HPQFlash 17
- I**  
immagine software  
preinstallata 2  
immissione  
Password di accensione 30  
password di  
configurazione 30  
industriali, standard 26  
installazione remota 4  
Installazione remota del  
sistema 4  
Internet, indirizzi. *Vedere siti Web*
- M**  
modifiche ai sistemi operativi,  
informazioni importanti 25  
modifiche, notifica 15
- N**  
notifica di modifiche 15  
notifica guasti e ripristino  
HP Client Manager 37
- O**  
ordinazione Chiave FailSafe 35

## P

password  
accensione 29, 30  
cancellazione 31  
eliminazione 32  
modifica 31  
Setup 29, 30  
sicurezza 29

password di accensione  
cancellazione 31  
immissione 30  
impostazione 29  
modifica 31

Password di configurazione  
impostazione 29

password di configurazione  
cancellazione 31  
immissione 30  
modifica 31

PC Intel vPro con Active Management Technology 13

PC, deployment 2

PCN (Proactive Change Notification) 15

personalizzazione software 2

Preboot Execution Environment (PXE) 4

Proactive Change Notification (PCN) 15

ProtectTools Security Manager 7

protezione dei dischi fissi 37

protezione della ROM, avvertenza 17

pulsante d'accensione  
configurazione 24  
doppio stato 24

pulsante di accensione a due stati 24

PXE (Preboot Execution Environment) 4

## R

Recovery Mode, Boot Block Emergency 18

ripristino software 2

ROM  
flash 17  
remoto, flash 17

## S

sblocco della chiusura Smart Cover 35

sensore Smart Cover  
impostazione 34  
protezione, livelli 33

sensore termico 37

Setup  
copia su computer singolo 19  
copia su più computer 20  
replica 19

setup  
iniziale 2

sicurezza  
caratteristiche, tabella 27  
chiusura con cavo 35  
chiusura Smart Cover 34  
DriveLock 32  
impostazioni 27  
password 29  
ProtectTools Security Manager 7  
Sensore Smart Cover 33  
tecnologia per l'identificazione delle impronte digitali 35

sicurezza chiusura coperchio, avvertenza 34

sistemi operativi, informazioni importanti sulla modifica 25

siti Web  
BIOS, download 17  
Flash della ROM 17  
flash remoto della ROM 17  
HP Client Configuration Manager 8  
HP Client Manager 10  
HP Configuration Management Solution 3, 9  
HP, white paper 13  
HPQFlash 17  
Intel vPro, tecnologia 13  
PC, deployment 2  
Proactive Change Notification 15  
replica, impostazioni 20  
Subscriber's Choice 15  
Subscriber's Choice 15  
supporto software 25  
System Software Manager, download 7  
Tecnologia per l'identificazione delle impronte digitali 36

software  
Active Management Technology 13  
aggiornamento e gestione, strumenti 5

Altiris AClient 3

Altiris Deployment Solution Agent 3

asset, controllo 27

Configuration Management Solution 9

Drive Protection System (DPS) 37

HP Client Catalog for SMS 11

HP Client Management Interface 5

HP Client Manager per Altiris 10

HP ProtectTools Security Manager 7

HP System Software Manager 7

Installazione remota del sistema 4

integrazione 2

ripristino 2

sospese, soluzioni 16

strumenti di clonazione, software 2

strumenti di deployment, software 2

strumenti diagnostici per dischi fissi 37

Subscriber's Choice 15

System Software Manager 7

## T

tecnologia per l'identificazione delle impronte digitali 35

temperatura interna del computer 37

## U

utility Computer Setup 19

## W

white paper 13