Guida di Desktop Management
PC aziendali HP

Guida di Desktop Management

PC aziendali HP

Quarta edizione (settembre 2009)

Numero di parte del documento: 581009-061

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 e deployment iniziale

HP Client Automation Agent 2
HP Client Manager 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 6
HP ProtectTools Security Manager 7
HP Client Automation Starter e Standard Edition 8
HP Client Automation Enterprise Edition 8
HP Client Manager from Symantec 8
Altiris Client Management Suite 9
HP Client Catalog for Microsoft System Center & SMS Products 10
Tecnologia di gestione remota 10
Configurazione di Intel Management Engine 11
Verdiem Surveyor 13
HP Proactive Change Notification 13
Subscriber's Choice 13
Soluzioni sospese 13

5 Flash della ROM

Flash remoto della ROM 14
HPQFlash 14

6 Boot Block Emergency Recovery Mode

7 Replica della configurazione

Copia su computer singolo 16

Copia su più computer 17
Creazione di un dispositivo avviabile 18
Dispositivo flash media USB supportato 18
Dispositivo flash media USB non supportato 19

8 Pulsante d'accensione a doppio stato

9 Sito Web di supporto HP

10 Standard di settore

11 Controllo e sicurezza degli asset
Sicurezza tramite password 27
Impostazione di una password di configurazione tramite Computer Setup 28
Impostazione di una password di accensione tramite Computer Setup 28
Immissione della password di accensione 29
Immissione di una password di configurazione 29
Modifica delle password di accensione e di configurazione 30
Cancellazione delle password di accensione e di configurazione 30
Caratteri delimitatori delle tastiere nazionali 31
Annullamento password 31
DriveLock 31
Utilizzo di DriveLock 32
Applicazioni DriveLock 32
Sensore Smart Cover 33
Impostazione del livello di protezione del sensore Smart Cover 33
Chiusura Smart Cover 33
Blocco della chiusura Smart Cover 34
Disattivazione del blocco della chiusura Smart Cover 34
Utilizzo della chiave di sicurezza FailSafe Smart Cover 34
Predisposizione per fissaggio con cavo 35
Tecnologia per l'identificazione delle impronte digitali 35
Notifica guasto e ripristino 35
Drive Protection System (DPS) 35
Alimentatore protetto contro gli sbalzi di tensione 35
Sensore termico 35

Indice analitico 37

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 e deployment iniziale

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 Automation Standard Edition o HP Client Automation Enterprise Edition (basato sulla tecnologia Radia) per sostituire il software preinstallato con un'immagine 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.

Il setup basato su ROM e l'hardware ACPI forniscono ulteriore assistenza per il ripristino del software del sistema operativo, la gestione della configurazione e la risoluzione dei problemi e la gestione del risparmio energetico.

HP Client Automation Agent

L'agente di gestione utilizzato da HP Client Automation Standard ed Enterprise Edition è precaricato sul computer. Quando installato, consente la comunicazione con la console di gestione HP.

Per installare HP Client Automation Agent:

1. Fare clic su **Start**.
2. Fare clic su **Tutti i programmi**.
3. Fare clic su **HP Manageability**.
4. Fare clic sul **HP Management Agent Readme** relativo al linguaggio desiderato.
5. Leggere e seguire le istruzioni contenute nel file Readme (Leggimi) per installare HP Client Automation Agent.

HP Client Automation Agent è un componente di infrastruttura chiave per l'abilitazione di tutte le soluzioni di gestione HP Client Automation. Per informazioni sugli altri componenti di infrastruttura necessari per l'implementazione delle soluzioni di gestione della configurazione HP, visitare il sito Web http://h20229.www2.hp.com/solutions/ascm/index.html.

HP Client Manager

HP Client Manager (HPCM) è una soluzione sviluppata da Symantec disponibile gratuitamente per tutti i modelli di desktop, notebook e workstation aziendali HP e HP Blade supportati. HPCM integra strumenti HP specifici quali System Software Manager, HP Instant Support Professional Edition e HP Client Management Interface per fornire un modello centralizzato di gestione, identificazione e monitoraggio di tutto l'hardware HP supportato.

HP Client Manager 7.0 è dotato di un nuovissimo portale che fornisce agli amministratori un singolo punto di gestione in cui eseguire le seguenti attività:

- Inventario
- Avvisi
- Gestione BIOS
- Aggiornamento driver
- Esecuzione di HP Instant Support Health Scan and Diagnostics
- Esecuzione di attività di sicurezza integrata
- Visualizzazione riassuntiva delle tendenze degli avvisi relativi all'integrità del sistema degli ultimi 3-6 mesi
- Visualizzare la conformità complessiva dei computer supportati tramite HP Instant Support Health Scan and Diagnostics
- Visualizzare il riepilogo dei computer HP: un'analisi dei diversi computer desktop, notebook, workstation e HP Blade
- Visualizzazione di avvisi: risorse, soglia, stato di salute hardware
- Rapporti
- Attività amministrative per aggiornare specifici strumenti HP

HPCM è scaricabile da http://www.symantec.com/business/theme.jsp; fare clic su **HP Client Manager** in **Strategic Partner Products**. Nella pagine di download è inoltre possibile scaricare una licenza permanente gratuita.

I video di esercitazione di HPCM sono inoltre disponibili all'indirizzo http://www.symantec.com/connect. Ricercare **HP Client Manager 7.0** per visualizzare i video che illustrano le procedure relative alle diverse attività in HPCM.

3 Installazione remota del sistema

Con l'installazione remota del sistema è possibile avviare e configurare il sistema, utilizzando le informazioni su software e configurazione archiviate su un server della rete mediante l'avvio del PXE (Preboot Execution Environment). La funzione di installazione remota del sistema viene in genere utilizzata come strumento di installazione e configurazione del sistema e consente di portare a termine le seguenti attività:

- 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 14)

  NOTA: sono disponibili funzionalità per eseguire il flash del BIOS del sistema dal sistema operativo Microsoft Windows.

- 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 Automation Starter, Standard ed Enterprise Edition
- HP Client Manager from Symantec
- Altiris Client Management Suite
- HP Client Catalog for Microsoft System Center & SMS Products
- 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 senza problemi nell'ambiente IT gestito della società. HP CMI offre un'interfaccia che semplifica l'integrazione dei computer aziendali HP con gli strumenti di gestione dei sistemi più diffusi (tra cui Microsoft Systems Management Server, IBM Tivoli Software e HP Operations) e con le applicazioni di gestione proprietarie sviluppate in azienda. Quando si utilizza HP CMI, gli strumenti e le applicazioni di gestione dei sistemi possono richiedere un inventario approfondito dei client, ricevere informazioni sullo stato di integrità e gestire le impostazioni dei sistemi comunicando direttamente con i computer client, riducendo così l'impiego di software agenti o di connessione per ottenere 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 e di semplice utilizzo per l'individuazione e il download degli aggiornamenti software per i modelli di PC client HP presenti nell'ambiente. È sufficiente specificare modelli, sistema operativo e lingua, per individuare, ordinare e selezionare rapidamente i softpaq necessari. Per scaricare HP SoftPaq Download Manager, visitare il sito Web http://www.hp.com/go/sdm.

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 le soluzioni HP Client Automation, HP Client Manager from Symantec 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 non supporta al momento il flash della memoria ROM remota sui sistemi su cui è attivato Windows BitLocker Drive Encryption e che utilizzano le misure TPM per proteggere le chiavi BitLocker in quanto il flash del BIOS rende non valida la firma attendibile che BitLocker ha creato per la piattaforma. Disabilitare BitLocker tramite i Criteri di gruppo per eseguire il flash del BIOS del 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

Il software di protezione HP ProtectTools offre funzionalità di sicurezza che consentono di proteggere computer, reti e dati importanti contro l'accesso non autorizzato. La funzionalità potenziata di protezione viene fornita dai seguenti moduli software ed è accessibile attraverso HP ProtectTools Security Manager:

HP ProtectTools Security Manager è la console unica dalla quale è possibile accedere a tutti gli altri moduli.

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro per HP ProtectTools

HP ProtectTools fornisce due versioni che è possibile utilizzare: HP ProtectTools Security Manager e HP ProtectTools Administrative Console. Entrambe le versioni, per amministratori e utenti, sono disponibili tramite il menu **Start** > **Tutti i programmi**.

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, precaricati oppure sono disponibili per il download dal sito Web HP. Per alcuni modelli di desktop HP Pro, HP ProtectTools è disponibile come opzione da acquistare a parte. Per ulteriori informazioni, visitare il sito http://www.hp.com/products/security.

HP Client Automation Starter e Standard Edition

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

- La Starter 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, monitoraggio allarmi HP, BIOS HP e aggiornamenti del driver, integrazione con HP Protect Tools e assistenza aggiuntiva per Intel AMT. La Starter Edition supporta anche deployment e gestione di HP Thin Client.
- La Standard Edition (edizione standard), disponibile per l'acquisto, include tutte le funzionalità della Starter Edition con inoltre le funzionalità di deployment e migrazione Windows, capacità di gestione patch, distribuzione del software e misurazione dell'utilizzo del software.

HP Client Automation Starter and Standard Editions offrono un percorso di migrazione verso HP Client Automation Enterprise Edition (basato sulla tecnologia Radia) per la gestione automatica di ambienti IT di grandi dimensioni, eterogenei e in continuo mutamento.

Per ulteriori informazioni sulle soluzioni HP Client Automation, visitare il sito Web http://www.hp.com/go/client.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition è una soluzione basata su criteri che consente agli amministratori di inventariare, installare, applicare patch e gestire continuativamente software e contenuti di piattaforme desktop eterogenee. Grazie a HP Client Automation Enterprise Edition 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 continuativamente un intero stack software (sistemi operatici, 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 sulle soluzioni HP Client Automation, visitare il sito Web http://www.hp.com/go/client.

HP Client Manager from Symantec

HP Client Manager from Symantec, sviluppato in collaborazione con Altiris, è disponibile gratuitamente per tutti i modelli desktop, notebook e workstation aziendali HP supportati. SSM è integrato in HP Client Manager e consente di controllare, monitorare e gestire in modo centralizzato gli aspetti hardware dei sistemi client HP.

Utilizzare HP Client Manager from Symantec 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 SoftPaq 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 from Symantec, visitare il sito Web http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite è una soluzione di semplice utilizzo per la gestione completa del ciclo di vita di computer desktop, notebook e workstation. Client Management Suite 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 Web http://www.symantec.com/business/client-management-suite.

HP Client Catalog for Microsoft System Center & SMS Products

HP Client Catalog consente ai professionisti IT di utilizzare i prodotti Microsoft per automatizzare il deployment degli aggiornamenti software HP (Softpaq) ai PC aziendali HP. Il file del catalogo contiene informazioni di piattaforma dettagliate su desktop, notebook e workstation aziendali HP. È possibile utilizzarlo insieme all'inventario personalizzato e alle funzionalità di aggiornamento dei prodotti Microsoft per fornire aggiornamenti di driver e patch automatizzati ai computer client HP gestiti.

I prodotti Microsoft supportati da HP Client Catalog sono:

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

Per ulteriori informazioni su HP Client Catalog for SMS, visitare il sito Web http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

Tecnologia di gestione remota

Nei modelli è integrata la tecnologia vPro o la tecnologia standard. Entrambe consentono di implementare il rilevamento, la riparazione e la protezione dei computer connessi in rete. Entrambe le tecnologie, inoltre, consentono di gestire i PC con il sistema acceso, spento o con il sistema operativo bloccato.

Le tre forme di gestione remota disponibili nei computer desktop aziendali sono Alert Standard Format (ASF), Intel Active Management Technology (AMT) e Desktop and mobile Architecture for Systems Hardware (DASH).

Le funzionalità della tecnologia di gestione remota includono:

- Individuazione rete
- Informazioni sull'inventario hardware
- Monitoraggio stato di salute della piattaforma
- Gestione dell'alimentazione - accensione/spegnimento, ciclo di spegnimento e riaccensione

- Diagnosi e riparazione remota
  - Reindirizzamento console testo: consente il controllo tramite console del PC remoto durante la fase di avvio
  - Reindirizzamento supporti: consente l'avvio del sistema da un'unità, disco o immagine ISO di avvio remoti (le due varianti sono IDE-Redirect (IDE-R) sulle piattaforme AMT e USB Media Redirection)
- Isolamento e ripristino basato su hardware - limitare o interrompere l'accesso alla rete di PC al rilevamento di un'attività simile a un virus
- Controllo e monitoraggio degli eventi della piattaforma
- Portale di gestione server Web integrato per l'accesso e la configurazione remote
- Le tecnologie di gestione remota sono integrate con i partner della console di gestione HP

NOTA: tutte le funzionalità sopra indicate non sono disponibili su tutte le piattaforme.

Configurazione di Intel Management Engine

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**.

Le tecnologie di gestione disponibili sono le seguenti:

- AMT (con DASH 1.0)
- ASF
- DASH 1.1 (utilizzando un NIC di Broadcom)

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. Subito dopo l'accensione del computer, premere Ctrl+P prima dell'avvio del sistema operativo.

   NOTA: se non si preme Ctrl+P al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo Ctrl+P prima dell'avvio del sistema operativo.

I 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. Alcune delle opzioni di configurazione sono riportate di seguito:

- Menu principale
  - Intel ® ME Configuration
  - Intel ® AMT Configuration
  - Change Intel ® ME Password
  - Exit (Esci)
- Intel ® ME Platform Configuration
  - Intel ® ME State Control (enable/disable)
  - Intel ® ME Firmware Local Update (enable/disable)
  - Intel ® ME Features Control
  - Intel ® ME Power Control
- Intel ® AMT Configuration
  - Host Name
  - TCP/IP
  - Provision Model (Enterprise, SMB)
  - Setup and Configuration
  - Un-Provision
  - SOL/IDE-R (enable/disable)
  - Password Policy
  - Secure Firmware Update (enable/disable)
  - Set PRTC
  - Idle Timeout
- Change Intel ® ME Password (HP consiglia 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.

Per configurare i sistemi con un NIC che supporta Broadcom DASH:

Consultare la documentazione più recente sul sito http://www.hp.com nella sezione **Support & Troubleshooting**, selezionare il modello specifico, quindi selezionare **Manuals**, **White papers** facendo riferimento a DASH o al NIC di Broadcom.

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 ulteriori informazioni su Subscriber's Choice e creare un profilo personalizzato, visitare il sito Web http://h30046.www3.hp.com/subhub.php.

Soluzioni sospese

Due pacchetti software, Altiris Local Recovery e Dantz Retrospect, non verranno più forniti con i desktop aziendali, notebook o workstation HP.

5 Flash della ROM

Il BIOS del computer è memorizzato in una memoria ROM flash programmabile (memoria di sola lettura). Impostando una password di configurazione nell'utility Computer Setup (F10), è possibile proteggere la memoria ROM dall'aggiornamento o dalla sovrascrittura involontari. L'impostazione della password è importante per assicurare l'integrità operativa del computer. Se si desidera aggiornare il BIOS, scaricare le più recenti immagini BIOS dalla pagina di supporto e driver HP all'indirizzo http://www.hp.com/.

△ **ATTENZIONE:** per garantire la massima protezione della memoria ROM, è bene impostare una password di configurazione. La password di configurazione impedisce aggiornamenti non autorizzati alla memoria 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 non supporta al momento il flash della memoria ROM remota sui sistemi su cui è attivato Windows BitLocker Drive Encryption e che utilizzano le misure TPM per proteggere le chiavi BitLocker in quanto il flash del BIOS rende non valida la firma attendibile che BitLocker ha creato per la piattaforma. Disabilitare BitLocker tramite i Criteri di gruppo per eseguire il flash del BIOS del 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, fare riferimento al software HP Client Manager o System Software Manager all'indirizzo 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 su HPQFlash, visitare l'indirizzo http://www.hp.com/support/files e, quando richiesto, immettere il numero del modello del computer.

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. Spegnere 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 della configurazione

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 necessario un'unità a dischetti o un'unità flash USB supportata.

NOTA: System Software Manager (SSM) può essere utilizzato per replicare le informazioni di configurazione del computer nel sistema operativo Windows. Per ulteriori informazioni, consultare la guida per l'utente di SSM all'indirizzo http://www.hp.com/go/ssm.

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. Spegnere 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. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.
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. Spegnere il computer da configurare e inserire il dischetto o il dispositivo USB flash media di configurazione.
8. Accendere il computer da configurare.
9. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare 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 16).

1. Creare un dischetto di avvio o un dispositivo USB flash media. Vedere Dispositivo flash media USB supportato a pagina 18 o Dispositivo flash media USB non supportato a pagina 19.

   △ **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. Spegnere 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. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.

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. Spegnere 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 avviabile

Dispositivo flash media USB supportato

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 Dispositivo flash media USB non supportato a pagina 19).

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. Spegnere 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. Eseguire FDISK dal prompt **A:** digitando `FDISK` e premendo Invio. Se richiesto, fare clic su **Yes** (**Y**) per attivare il supporto dei dischi di grande capacità.
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.

Durante l'esecuzione di FORMAT verranno visualizzati uno o più messaggi di conferma con cui si chiede se si intende procedere. Digitare `Y` a ogni richiesta. FORMAT formatterà il dispositivo flash media USB, aggiungerà i file di sistema e chiederà di digitare un'etichetta del 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 17.

Dispositivo flash media USB non supportato

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. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.

6. 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: _____

7. 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.

8. Eseguire 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.

9. Se il sistema non è stato automaticamente riavviato all'uscita da FDISK, premere Ctrl+Alt+Canc per riavviare il dischetto DOS.

10. 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.

11. Immettere un'etichetta oppure premere Invio se non si desidera immettere alcuna etichetta.

12. Spegnere il computer e scollegare il cavo di alimentazione. Aprire il computer e reinstallare le schede PCI precedentemente rimosse. Chiudere il coperchio del computer.

13. Collegare il cavo di alimentazione, rimuovere il dischetto e accendere il computer.

14. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

15. 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.

16. 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 è può essere modificata nell'utility Computer Setup (F10). Per istruzioni, consultare *Computer Setup (F10) Utility* .

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 17.

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 Sito Web di supporto 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 semplificato le attività di individuazione, accesso, valutazione e installazione del software di supporto più recente. Il software è scaricabile all'indirizzo 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 tentano l'accesso al sistema (per ulteriori informazioni, consultare la guida *HP ProtectTools Security Manager* all'indirizzo Web http://www.hp.com/products/security). 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 parallele, seriali 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:

- In locale, utilizzando le utility Computer Setup. Consultare la *Guida dell'utility Computer Setup (F10)* inclusa con il computer per ulteriori informazioni e istruzioni sull'utilizzo delle utility Computer Setup.
- In remoto, utilizzare HP Client Manager from Symantec, HP Client Automation 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
Setup Password (Password di configurazione)	Consente di impostare e abilitare la password di configurazione (amministratore). **NOTA:** Se la password di configurazione è impostata, è necessario modificare le opzioni di Computer Setup, eseguire il flash della ROM ed eseguire le modifiche ad alcune impostazioni plug and play in Windows.

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

Power-On Password (Password di accensione)	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. **NOTA:** questa password non viene richiesta al riavvio "a caldo" del sistema, ad esempio quando viene premuta la combinazione di tasti Ctrl+Alt+Canc oppure quando si seleziona **Restart from Windows** (Riavvia da Windows), a meno che l'opzione non sia abilitata in **Password Options** (Opzioni password) (vedere di seguito).
Password Options (Opzioni password) (Questa selezione appare solo se è stata impostata una password di accensione o di configurazione).	Consente di: • Bloccare le risorse di vecchio tipo (appare se è stata impostata una password di configurazione) • Abilitare/disabilitare la modalità server di rete (appare se è stata impostata una password di accensione). • Specificare se la password è richiesta per il riavvio (Ctrl+Alt+Canc) (appare se è stata impostata una password di accensione) • Abilitare/disabilitare la modalità di esplorazione del setup (appare se è stata impostata una password di configurazione; consente la visualizzazione, ma non la modifica, delle opzioni di Computer Setup (F10) senza immettere la password di configurazione) • Abilitare/disabilitare la password rigida (visualizzata quando si imposta una password di accensione) che, quando abilitata, ignora il ponticello della password integrato per disabilitare la password di accensione Per ulteriori informazioni consultare la *Guida di Desktop Management*.
Smart Cover (alcuni modelli)	Consente di: • Bloccare/sbloccare il dispositivo di chiusura del coperchio. • Impostare il sensore di assenza coperchio su Disable/Notify User/Setup Password (Disabilita/Notifica utente/Password di configurazione). **NOTA:** *Notify User* avverte l'utente che è stato rilevato il sensore alla rimozione del coperchio. *Setup Password* (Password di configurazione) richiede che venga inserita la password di configurazione per avviare il computer se il sensore rileva l'assenza del coperchio. Questa funzione è supportata solo su alcuni modelli.
Device Security (Sicurezza periferiche)	Consente di impostare le opzioni Dispositivo disponibile o Dispositivo nascosto per: • Porte seriali • Porta parallela • Porte USB posteriori • Porte USB frontali • Porte USB interne • Audio di sistema • Controller di rete (alcuni modelli) • Legacy diskette (Dischetto di vecchio tipo) • Dispositivo di sicurezza integrata (alcuni modelli) • SATA0 • SATA1 (alcuni modelli) • SATA2 (alcuni modelli)

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

	• SATA3 (alcuni modelli) • eSATA (alcuni modelli)
LoJack per HP ProtectTools	Consente di monitorare, gestire e controllare in remoto il computer. Una volta attivato, LoJack Pro per HP ProtectTools viene configurato dal centro clienti di Absolute Software. Dal centro clienti, l'amministratore può configurare LoJack per HP ProtectTools per monitorare o gestire il computer. Se il sistema viene smarrito o rubato, il centro clienti è in grado di assistere le autorità locali nell'individuazione e nel recupero del computer. Se configurato, LoJack Pro può continuare a funzionare anche se l'unità disco rigido viene cancellata o sostituita.
Network Service Boot (Avvio servizio di rete)	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).
System Ids (ID di sistema)	Consente di impostare: • Contrassegno risorsa (di 18 byte), un numero di identificazione della proprietà assegnato al computer dalla casa produttrice. • Contrassegno di proprietà (identificativo di 80 byte) visualizzato durante la fase POST. • 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 Security (Funzione di sicurezza DriveLock)	Consente di assegnare o modificare una password principale o utente per le unità 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. **NOTA:** questa selezione viene visualizzata solo quando al sistema è collegata almeno un'unità che supporta la funzione DriveLock.
Setup Security Level (Livello sicurezza setup)	Fornisce un metodo per consentire agli utenti finali l'accesso limitato per modificare le opzioni di configurazione specificate, senza dover conoscere la password di configurazione. Questa funzione offre agli amministratori la flessibilità necessaria per proteggere le modifiche apportate alle opzioni di configurazione essenziali, pur permettendo agli utenti di visualizzare le impostazioni di sistema e di configurare le opzioni non essenziali. L'amministratore specifica i diritti di accesso alle singole opzioni di configurazione caso per caso tramite il menu Setup Security Level (Livello sicurezza setup). Per impostazione predefinita, a tutte le opzioni di configurazione è assegnata una password, che l'utente deve immettere correttamente durante il POST per modificare qualsiasi opzione. L'amministratore può impostare il valore None per singole voci, di modo che l'utente possa apportare modifiche alle opzioni specificate quando è stato eseguito l'accesso con password non valide. L'opzione None viene sostituita dalla password di accensione, se abilitata. **NOTA:** affinché l'utente possa accedere senza conoscere la password, impostare Setup Browse Mode su Enable.
System Security (Sicurezza sistema) (alcuni modelli: queste opzioni dipendono dall'hardware)	La modalità Data Execution Prevention (Blocco esecuzione dati) (in alcuni modelli) (abilitazione/disabilitazione) aiuta a evitare la violazione della sicurezza del sistema operativo. Virtualization Technology (Tecnologia di virtualizzazione) (alcuni modelli) (abilitazione/disabilitazione) controlla le funzionalità di virtualizzazione del processore. La modifica di questa impostazione richiede lo spegnimento e la riaccensione del computer. Virtualization Technology Directed I/O (I/O diretto tecnologia di virtualizzazione) (alcuni modelli) (abilitazione/disabilitazione) controlla le funzionalità di rimappatura DMA del chipset. La modifica di questa impostazione richiede lo spegnimento e la riaccensione del computer. Trusted Execution Technology (Tecnologia esecuzione attendibile) (alcuni modelli) (abilitazione/disabilitazione) controlla le funzionalità di base del processore e del chipset necessarie per

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

	supportare un'appliance virtuale. La modifica di questa impostazione richiede lo spegnimento e la riaccensione del computer. Per abilitare questa funzione è necessario abilitare anche: • Supporto per Embedded Security Device (alcuni modelli) • Virtualization Technology • Virtualization Technology Directed I/O Il supporto per Embedded Security Device (Dispositivo di sicurezza integrata) (alcuni modelli) (abilitazione/disabilitazione) consente l'attivazione e la disattivazione di Embedded Security Device. La modifica di questa impostazione richiede lo spegnimento e la riaccensione del computer. **NOTA:** per la configurazione di Embedded Security Device, è richiesta l'impostazione di una password. • Reset to Factory Settings (Ripristina impostazioni predefinite) (alcuni modelli) (Non ripristinare/Ripristina) - Con il ripristino delle impostazioni predefinite, vengono cancellate tutte le chiavi di protezione. La modifica di questa impostazione richiede lo spegnimento e la riaccensione del computer. **ATTENZIONE:** Embedded Security Device è un componente di importanza critica di molti schemi di sicurezza. Con la cancellazione delle chiavi di protezione, verrà impedito l'accesso ai dati protetti da Embedded Security Device. L'utilizzo dell'opzione Reset to Factory Settings (Ripristina impostazioni predefinite) può comportare la perdita di dati importanti. • Reset authentication credentials (Ripristina credenziali di autenticazione) (alcuni modelli) (Non ripristinare/Ripristina) - Selezionando Reset (Ripristina), il supporto di autenticazione password all'accensione viene disabilitato e le informazioni di autenticazione ricevute da Embedded Security Device vengono cancellate. La modifica di questa impostazione richiede lo spegnimento e la riaccensione del computer OS Management of Embedded Security Device (Gestione SO del dispositivo di sicurezza integrata) (alcuni modelli) (abilitazione/disabilitazione) - Consente all'utente di limitare il controllo del sistema operativo su Embedded Security Device. La modifica di questa impostazione richiede lo spegnimento e la riaccensione del computer. Questa opzione consente all'utente di limitare il controllo del sistema operativo su Embedded Security Device. • Reset of Embedded Security Device through OS (Ripristino dispositivo di sicurezza integrata mediante sistema operativo) (alcuni modelli) (abilitazione/disabilitazione) - Consente all'utente di limitare le possibilità del sistema operativo di richiedere il ripristino delle impostazioni predefinite di Embedded Security Device. La modifica di questa impostazione richiede lo spegnimento e la riaccensione del computer. **NOTA:** per l'abilitazione di questa opzione, è richiesta l'impostazione di una password di configurazione. PAVP (alcuni modelli) (disabilitazione/min/max) - Abilita Protected Audio Video Path (Percorso audio video protetto) nel chipset. Consente di visualizzare alcuni contenuti ad alta definizione protetti la cui riproduzione sarebbe altrimenti vietata. Se si seleziona Max, si assegnano 96 Megabyte della memoria di sistema a PAVP in modo esclusivo.

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.

NOTA: System Software Manager (SSM) può essere utilizzato per creare e gestire le password del BIOS nel sistema operativo Windows. Per ulteriori informazioni, consultare la guida per l'utente di SSM all'indirizzo http://www.hp.com/go/ssm.

NOTA: HP Client Management Interface (HP CMI) fornisce accesso alla gestione delle impostazioni del BIOS, incluse le password del BIOS, dal sistema operativo Windows. Per ulteriori informazioni, consultare il white paper tecnico di HP Client Management Interface all'indirizzo http://www.hp.com/go/hpcmi.

Impostazione di una password di configurazione tramite Computer Setup

Se il sistema è dotato di un dispositivo di protezione integrato, consultare la *Guida di HP ProtectTools Security Manager* all'indirizzo http://www.hp.com. L'impostazione di una password di configurazione in Computer Setup impedisce la riconfigurazione del computer (ovvero l'utilizzo dell'utility Computer Setup (F10)) fino a quando non viene immessa la password.

1. Accendere o riavviare il computer. In Microsoft Windows fare clic su **Start** > **Chiudi sessione** > **Riavvia il sistema**.
2. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.
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. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.
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 integrato, consultare la *Guida di HP ProtectTools Security Manager* all'indirizzo 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. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.

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 integrato, consultare la *Guida di HP ProtectTools Security Manager* all'indirizzo 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, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo per accedere a Computer Setup. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.
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 31. 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 integrato, consultare la *Guida di HP ProtectTools Security Manager* all'indirizzo 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, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo per accedere a Computer Setup. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.
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 31. 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
-	BECMSS*	-	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 ed Erzegovina, Croazia, Montenegro, Serbia e Slovenia

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 integrato, consultare la *Guida di HP ProtectTools Security Manager* all'indirizzo 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.

Utilizzo 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 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 rimozione del coperchio, disponibile su alcuni modelli, è una combinazione di tecnologie hardware e software in grado di avvisare l'amministratore quando viene rimosso il coperchio o il pannello laterale. Esistono tre livelli di protezione, come illustrato nella tabella che segue.

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 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. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.
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 protezione del blocco del coperchio, è bene impostare una password di configurazione. La password di configurazione impedisce gli accessi non autorizzati alla 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. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.
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. Per accedere a Computer Setup, subito dopo l'accensione del computer, premere F10 prima dell'avvio del sistema operativo. Se necessario, premere Invio per ignorare la schermata del titolo.

   NOTA: se non si preme F10 al momento opportuno, per accedere all'utility sarà necessario riavviare il computer e premere di nuovo F10 prima dell'avvio del sistema operativo.
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).

Utilizzo della chiave di sicurezza 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 Smart Cover FailSafe è uno strumento speciale da ordinare a HP. È opportuno ordinare la chiave prima che sia necessario utilizzarla, contattando 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.

Notifica guasto 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 tiene sotto controllo la temperatura interna del computer. Questa funzione consente di visualizzare un messaggio di avviso quando l'intervallo

normale delle temperature viene superato, in modo da offrire all'utente la possibilità di agire prima che i componenti interni vengano danneggiati o che i dati vadano perduti.

△ **ATTENZIONE:** quando le temperature si alzano, il sistema può restare danneggiato o i dati possono andare perduti.

Indice analitico

A

Accesso al computer, controllo 24
Alimentatore protetto contro gli sbalzi di tensione 35
Altiris
  Client Management Suite 9
Asset, controllo 24

B

BIOS
  Boot Block Emergency Recovery Mode 15
  flash remoto della ROM 14
  HPQFlash 14
Blocco della chiusura Smart Cover 34
Blocco Smart Cover
  chiave FailSafe 34
Boot Block Emergency Recovery Mode 15

C

Cambiamento di sistema operativo, supporto 22
Cambiamento password 30
Cancellazione password 30
Caratteri delimitatori delle tastiere nazionali 31
Caratteri delimitatori, tabella 31
Chiave FailSafe Smart Cover, ordinazione 34
Chiave FailSafe, ordinazione 34
Chiusura Smart Cover
  blocco 34
  sblocco 34
Client Management Interface 5
Client Manager from Symantec 8
Configurazione
  iniziale 2
Configurazione del pulsante d'accensione 21
Configurazione iniziale 2
Configurazioni, replica 16
Controllo dell'accesso al computer 24
Coperchio, chiusura 33

D

Dischi fissi, strumenti diagnostici 35
Dischi, protezione 35
Dispositivo avviabile
  creazione 18
  dispositivo flash media USB 18
Dispositivo flash media USB, avviabile 18, 19
DriveLock 31

E

Eliminazione password 31
Emergency Recovery Mode, Boot Block 15

F

Fissaggio con cavo 35
Flash della ROM 14
Flash remoto della ROM 14

H

HP
  Client Automation Starter, Standard ed Enterprise Edition 8
  Client Catalog for Microsoft System Center & SMS Products 10
  Client Management Interface 5
  Client Manager from Symantec 8
  ProtectTools Security Manager 7
  System Software Manager 6
HP Client Automation Enterprise Edition 8
HP Client Manager 3
HPQFlash 14

I

Immagine software precaricata 2
Immissione
  Password di accensione 29
  password di configurazione 29
Indirizzi Internet. *Vedere* siti Web
Industriali, standard 23
Installazione remota 4
Installazione remota del sistema 4

M

Modifiche, notifica 13

N

Notifica di modifiche 13
Notifica guasto e ripristino 35

O

Ordinazione della chiave FailSafe 34

P

Password
  accensione 28, 29
  cancellazione 30
  eliminazione 31
  modifica 30

Setup 28, 29
sicurezza 27
Password di accensione
cancellazione 30
immissione 29
impostazione 28
modifica 30
Password di configurazione
cancellazione 30
immissione 29
impostazione 28
modifica 30
Preboot Execution Environment (PXE) 4
Proactive Change Notification (PCN) 13
ProtectTools Security Manager 7
Protezione dei dischi fissi 35
Pulsante d'accensione a doppio stato 21
Pulsante d'accensione, configurazione 21
PXE (Preboot Execution Environment) 4

R
Recovery Mode, Boot Block Emergency 15
Ripristino, software 2

S
Sblocco della chiusura Smart Cover 34
Sensore Smart Cover
impostazione 33
protezione, livelli 33
Sensore termico 35
Setup
copia su computer singolo 16
copia su più computer 17
Sicurezza
caratteristiche, tabella 24
chiusura con cavo 35
chiusura Smart Cover 33
DriveLock 31
impostazioni 24
password 27
ProtectTools Security Manager 7
Sensore Smart Cover 33
tecnologia per l'identificazione delle impronte digitali 35
Sistemi operativi, supporto per il cambiamento 22
siti Web
Altiris Client Management Suite 10
Download del BIOS 14
Flash della ROM 14
flash remoto della ROM 14
HP Client Automation Agent 2
HP Client Automation Center 8
HP Client Catalog for Microsoft SMS 10
HP Client Management Interface 6
HP Client Manager 3
HP Client Manager from Symantec 9
HP Softpaq Download Manager 6
HP System Software Manager 6
HPQFlash 14
Intel vPro, tecnologia 11
Proactive Change Notification 13
protezione dei PC aziendali HP 7
Software & Driver Downloads 17
Subscriber’s Choice 13
supporto HP 11
supporto software 22
Software
aggiornamento e gestione, strumenti 5
Altiris Client Management Suite 9
asset, controllo 24
deployment 2
Drive Protection System (DPS) 35
HP Client Automation Starter, Standard ed Enterprise Edition 8
HP Client Catalog for Microsoft System Center & SMS Products 10
HP Client Management Interface 5
HP Client Manager from Symantec 8
HP ProtectTools Security Manager 7
HP System Software Manager 6
Installazione remota del sistema 4
integrazione 2
Proactive Change Notification (PCN) 13
ripristino 2
Verdiem Surveyor 13
software
tecnologia di gestione remota 10
Sospese, soluzioni 13
Strumenti di clonazione, software 2
Strumenti di deployment, software 2
Strumenti diagnostici per dischi fissi 35
Subscriber's Choice 13
System Software Manager 6

T
Tecnologia di gestione remota 10
Tecnologia per l'identificazione delle impronte digitali 35
Temperatura interna del computer 35

V
Verdiem Surveyor 13