Guida di Desktop Management
Business Desktop

Numero di parte del documento: 312947-061

Marzo 2003

La presente guida fornisce definizioni ed istruzioni delle funzioni di sicurezza d'uso e Intelligent Manageability 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.

Guida di Desktop Management
Business Desktop

Prima Edizione (Marzo 2003)
Numero di parte del documento: 312947-061

Sommario

Guida di Desktop Management

Indice Analitico

Guida di Desktop Management

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

Questa guida riassume le capacità e le caratteristiche dei sette componenti chiave della Gestione del desktop:

- Configurazione iniziale e deployment
- Installazione remota del sistema
- Software updating and management (Aggiornamento e gestione del software)
- Flash della ROM
- Moduli e collaboratori
- Controllo e sicurezza degli Asset
- Fault notification and recovery (Notifica guasti e ripristino)

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

Configurazione iniziale e deployment

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

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

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

Il metodo di deployment dipende dai processi e dagli ambienti informatici degli utenti. La sezione PC Deployment (Installazione del PC) del sito Web Solutions and Services (Soluzioni e Servizi) site (http://www.compaq.com/solutions/pcsolutions) fornisce informazioni utili per la scelta del metodo migliore di deployment.

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

Installazione remota del sistema

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

- Formattazione di un'unità disco rigido.
- Installazione di una copia del software su uno o più PC nuovi.
- Installazione di software applicativo o di driver per applicazioni.
- Aggiornamento del sistema operativo, del software di applicazione o dei driver.

Per avviare l'installazione remota del sistema premere **F12** quando viene visualizzato il messaggio F12=Avvio servizio di rete nell'angolo inferiore sinistro della schermata del logo HP. Per proseguire seguire le istruzioni sullo schermo.

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

Gestione e aggiornamento del software

HP ha dotato desktop e workstation di diversi strumenti per la gestione e l'aggiornamento del software, Altiris eXpress; Altiris eXpress PC Transplant Pro; HP Client Manager Software, una soluzione Altiris eXpress; System Software Manager; HP Proactive Notification e ActiveUpdate.

Altiris eXpress

HP ed Altiris hanno esteso la partnership a soluzioni leader a livello industriale che riducono la complessità di gestione hardware e software per desktop, portatili, dispositivi palmari e server per tutto la loro durata. Altiris eXpress consentono all'amministratore del sistema di creare e di installare in poco tempo un'immagine del software standard aziendale e personalizzata su uno o più PC client in rete con un interfaccia semplice da utilizzare come Windows Explorer. Altiris eXpress supporta Preboot Execution Environment (PXE). Con Altiris eXpress e le funzioni d'installazione remota del sistema del computer HP non è necessario che l'amministratore si rechi personalmente presso ogni nuovo PC per scompattare la copia del software.

Le soluzioni Altiris eXpress costituiscono un modo efficace e funzionale per automatizzare i processi esistenti e risolvere le zone problematiche nell'ambiente informatico in uso. Con un'infrastruttura di tipo Web Altiris eXpress è in grado di gestire i sistemi da qualunque luogo e in qualsiasi momento, anche da un PC iPAQ Pocket.

Le soluzioni Altiris eXpress sono modulari ed estendibili per soddisfare le esigenze a livello di workgroup e di aziende e si integrano con altri strumenti di gestione client, fornendo estensioni a Microsoft BackOffice/SMS.

Le soluzioni Altiris eXpress espanse riguardano quattro aree informatiche fondamentali:

- Deployment e migrazione
- Gestione software e operativa
- Gestione componenti hardware e risorse
- Help Desk e risoluzione dei problemi

Nel giro di pochi minuti dall'installazione Altiris eXpress è in grado d'installare un'immagine disco contenente il sistema operativo, il software applicativo ed il client Altiris eXpress, senza bisogno di dischetti d'avvio. Con Altiris eXpress gli amministratori di rete possono:

- Creare una nuova immagine o modificarne una esistente, oppure clonare un PC in rete contenente l'immagine ideale.
- Creare qualsiasi numero d'immagini disco personalizzate per numerosi gruppi di lavoro.
- Modificare i file d'immagine senza dover ripartire da zero. Ciò è reso possibile dal fatto che Altiris eXpress memorizza i file nel loro formato nativo: NTFS, FAT16 o FAT32.
- Stabilire un "New PC Event" (Nuovo evento PC), ovvero uno script da eseguire automaticamente quando viene aggiunto un PC in rete. Lo script può, ad esempio, formattare il disco fisso, effettuare il flash del BIOS su ROM ed installare un'immagine software standard completa.
- Programmare l'esecuzione d'un evento su un gruppo di computer.

Altiris eXpress è anche dotato di funzioni di distribuzione software di facile uso. Altiris eXpress può essere utilizzato per aggiornare i sistemi operativi e il software di applicazione da una console centrale. In abbinamento a SSM, o HP Client Manager, Altiris eXpress è anche in grado di aggiornare il BIOS su ROM e i driver di periferica.

Per ulteriori informazioni consultare http://www.compaq.com/easydeploy.

Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Pro garantisce una migrazione indolore del PC mantenendo le vecchie impostazioni e preferenze e i vecchi dati e trasportandoli in modo semplice e rapido nel nuovo ambiente. L'upgrade richiede solo alcuni minuti, anziché ore o giorni, e il desktop ha l'aspetto e le funzioni previste.

Per ulteriori informazioni e particolari sulle modalità di download di una copia di valutazione valida 30 giorni completa di tutte le funzioni consultare http://www.compaq.com/easydeploy.

HP Client Manager Software

HP Client Manager Software (HP CMS) integra a fondo la tecnologia HP Intelligent Manageability in Altiris eXpress per fornire funzioni di gestione hardware superiori per dispositivi d'accesso HP, fra cui:

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

Per ulteriori informazioni su HP Client Manager consultare http://www.compaq.com/easydeploy.

System Software Manager

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

HP Proactive Notification (HPPN)

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

- Invio di messaggi di posta elettronica PCN (Product 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 all'ambiente informatico in uso. Per saperne di più su HPPN e la creazione dei profili consultare: http://www.hp.com/united-states/subscribe/

ActiveUpdate

ActiveUpdate è un'applicazione HP di tipo client, che funziona sul sistema locale e utilizza profili definiti dall'utente per scaricare in modo proattivo ed automatico aggiornamenti software per la maggior parte dei computer e server HP disponibili in commercio.

Per saperne di più su ActiveUpdate, scaricare l'applicazione e creare un profilo consultare: http://www.compaq.com/activeupdate.

Flash della ROM

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

- Richiedere ad HP un dischetto con *ROMPaq*™ aggiornato.
- Scaricare le ultime immagini ROMPaq da http://www.hp.com/support.

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

Flash remoto della ROM

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

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

Per ulteriori informazioni sul flash remoto della ROM vedere HP Client Manager Software o System Software Manager su http://www.compaq.com/easydeploy.

ROM con blocco di avviamento FailSafe

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

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

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

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

1. Se nell'unità a dischetti è inserito un dischetto, toglierlo e spegnere il computer.
2. Inserire un dischetto ROMPaq nel lettore.
3. Accendere il sistema.
4. Se non viene rilevato alcun dischetto ROMPaq il sistema ne richiede l'introduzione ed il riavvio del computer.
5. Se è stata impostata una password di configurazione la spia del blocco delle maiuscole si accende ed il sistema richiede l'inserimento della password.
6. Digitare la password di configurazione.
7. Se il sistema riesce ad avviarsi dal dischetto e a riprogrammare la ROM, le tre spie della tastiera si accendono. Il successo dell'operazione viene segnalata inoltre da una serie di segnali acustici di tono crescente.
8. Togliere il dischetto e spegnere il computer.
9. Accendere o riavviare il computer.

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

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

Modalità blocco di avvio FailSafe	Colore del LED della tastiera	Attività del LED della tastiera	Stato/Messaggio
BlocNum	Verde	Acceso	Dischetto ROMPaq non presente, danneggiato o non pronto.
BlocMaiusc	Verde	Acceso	Immettere la password.
BlocNum, Maiusc, Scorr	Verde	Si accendono e si spengono 2 volte (accompagnati da 1 segnale acustico lungo e 3 brevi)	Il flash della ROM è fallito.
BlocNum, Maiusc, Scorr	Verde	Acceso	Flash della ROM con blocco dell'avvio eseguito con successo. Spegnere e riaccendere.

✎ Le spie diagnostiche non lampeggiano su tastiere USB.

Replica delle impostazioni

Questa procedura offre all'amministratore di sistema la possibilità di copiare facilmente le impostazioni di un computer su altri computer dello stesso modello. Ciò consente una configurazione più veloce e uniforme di più computer. Per replicare le impostazioni:

1. Accedere al menu Utility di Computer Setup (F10).
2. Dal menu **File** scegliere **Salva su dischetto**. Seguire le istruzioni visualizzate sullo schermo.

È necessaria un'unità a dischetti oppure un dispositivo flash media USB compatibile, come DiskOnKey.

3. Per duplicare la configurazione, dal menu **File** scegliere **Ripristina da dischetto** e seguire le istruzioni a video.

Altiris eXpress, System Software Manager e PC Transplant facilitano la replicazione della configurazione e delle impostazioni personalizzate di un PC copiandole su uno o più PC. Per ulteriori informazioni consultare http://www.compaq.com/easydeploy.

Pulsante d'accensione bistabile

Con le funzioni Advanced Configuration and Power Interface (ACPI) abilitate in Windows 98, Windows 2000 e Windows XP, il pulsante può funzionare come interruttore di accensione o come interruttore di sospensione. La funzione di sospensione non interrompe completamente l'alimentazione, ma fa entrare il computer in una modalità di minimo consumo energetico. In tal modo è possibile spegnere velocemente il computer senza chiudere le applicazioni e ritornare altrettanto velocemente allo stesso stato operativo senza alcuna perdita di dati.

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

1. In Windows 2000, fare clic su **Start** e selezionare **Impostazioni > Pannello di controllo > Opzioni risparmio energia**.

   In Windows XP, fare clic su **Start** e selezionare **Pannello di controllo > Prestazioni e manutenzione > Opzioni risparmio energia**.

2. In **Proprietà – Opzioni risparmio energia** selezionare la scheda **Avanzate**.

3. Nella sezione **Pulsanti di alimentazione** selezionare l'impostazione preferita.

Dopo aver configurato il pulsante di accensione come pulsante di standby, premerlo per portare il sistema ad uno stato di alimentazione ridotta (Sospendi). 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 rispondi; lo spegnimento del computer senza interazione col sistema operativo può provocare danni al disco fisso o perdita di dati.

Gestione alimentazione

La funzione di Gestione dell'alimentazione interrompe l'alimentazione a determinati componenti del computer quando questi non vengono utilizzati, in modo da risparmiare energia senza che sia necessario spegnere il computer.

Con le funzioni Advanced Configuration and Power Interface (ACPI) abilitate in Windows 98, Windows 2000, Windows Millennium e Windows XP, è possibile abilitare, personalizzare o disabilitare i timeout (periodi di inattività consentiti prima che i componenti vengano spenti) tramite il sistema operativo.

1. In Windows 2000, fare clic su **Start** e selezionare **Impostazioni > Pannello di controllo > Opzioni risparmio energia**.

   In Windows XP, fare clic su **Start** e selezionare **Pannello di controllo > Prestazioni e manutenzione > Opzioni risparmio energia**.

2. In **Proprietà – Opzioni risparmio energia** selezionare la scheda **Combinazioni risparmio energia**.

3. Selezionare l'impostazione preferita.

Per definire, modificare o disattivare le impostazioni della Gestione dell'alimentazione per quanto riguarda il monitor, occorre utilizzare Proprietà schermo. Per accedervi, è sufficiente fare clic con il pulsante destro del mouse sul **desktop di Windows** e scegliere **Proprietà**.

Sito World Wide Web

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

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

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

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

Moduli e collaboratori

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

- Desktop Management Interface (DMI) 2.0
- Tecnologia WON (Wake on LAN)
- ACPI
- SMBIOS
- Support PXE (Pre-boot Execution)

Controllo e sicurezza degli Asset

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

HP offre inoltre diverse soluzioni per il controllo dell'accesso ai componenti e ai dati critici del computer. Le funzioni di sicurezza come il sensore e la chiusura Smart Cover, disponibili su alcuni modelli, impediscono l'accesso non autorizzato ai componenti interni del personal computer. Disabilitando le porte parallela, seriale od USB, o disabilitando la funzione d'avvio da supporto rimovibile è possibile proteggere risorse dati preziose. Gli allarmi di modifica alla memoria e quelli trasmessi dal sensore Smart Cover possono essere inoltrati automaticamente alle applicazioni di gestione sistemi per fornire un'efficace segnalazione dei tentativi di manomissione dei componenti.

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

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

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

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

Descrizione generale delle funzioni di sicurezza

Funzione	Scopo	Come viene attivata
Controllo avvio dispositivi removibili	Impedisce l'avviamento da unità a supporti rimovibili.	Dal menu Utility di Computer Setup (F10).
Serial, Parallel, USB, or Infrared Interface Control (Controllo inferfaccia seriale, parallela, USB o infrarossi)	Impedisce il trasferimento di dati tramite le interfacce seriali, parallele, USB (universal serial bus) o a infrarossi.	Dal menu Utility di Computer Setup (F10).
Password di accensione	Impedisce l'uso del computer finché non viene immessa la password. Ciò vale sia per l'avvio iniziale che per le operazioni di riavvio.	Dal menu Utility di Computer Setup (F10).
Password di impostazione	Impedisce la riconfigurazione del computer (uso delle utility di Computer Setup) finché non viene immessa la password.	Dal menu Utility di Computer Setup (F10).
DriveLock	Impedisce l'accesso non autorizzato ai dati su dischi fissi specifici. Questa funzione è disponibile solo su alcuni modelli.	Dal menu Utility di Computer Setup (F10).

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida all'utility Computer Setup (F10)*.
Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Funzione	Scopo	Come viene attivata
Sensore Smart Cover	Indica che il coperchio o il pannello laterale del computer sono stati rimossi. È possibile impostarlo in modo che venga richiesta la password di configurazione per il riavvio del computer, dopo la rimozione del coperchio o del pannello laterale. Per ulteriori informazioni su questa funzione consultare la *Guida di riferimento hardware* sul CD *Documentation Library.* Questa funzione è disponibile solo su alcuni modelli.	Dal menu Utility di Computer Setup (F10).
Sicurezza MBR (Master Boot Record)	Serve per impedire che il Master Boot Record del disco d'avvio venga modificato inavvertitamente o dolosamente e per ripristinare l'ultimo MBR valido.	Dal menu Utility di Computer Setup (F10).
Allarmi di variazione memoria	Rileva l'aggiunta, lo spostamento o la rimozione di moduli di memoria, informandone l'utente finale e l'amministratore del sistema.	Per informazioni sull'abilitazione degli allarmi di modifica alla memoria consultare la guida in linea *Intelligent Manageability Guide*.

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida all'utility Computer Setup (F10)*. Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Funzione	Scopo	Come viene attivata
Ownership Tag (Contrassegno proprietà)	Durante l'avvio del sistema (protetto da password di configurazione), visualizza le informazioni relative alla proprietà, come definite dall'amministratore del sistema.	Dal menu Utility di Computer Setup (F10).
Predisposizione per chiusura con cavo	Impedisce l'accesso all'interno del computer per impedire modifiche non autorizzate della configurazione o la rimozione di componenti. È possibile utilizzarla anche per fissare il computer ad un oggetto immobile, in modo da impedirne il furto.	Utilizzare una chiusura con cavo per assicurare il computer ad un oggetto fisso.
Chiusura di sicurezza	Impedisce l'accesso all'interno del computer per impedire modifiche non autorizzate della configurazione o la rimozione di componenti.	Installare un lucchetto nella chiusura di sicurezza per impedire modifiche non autorizzate della configurazione o la rimozione di componenti.

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida all'utility Computer Setup (F10)*. Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Sicurezza tramite password

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

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

Impostazione di una password di configurazione tramite Computer Setup

Se si imposta una password di configurazione tramite Computer Setup, si impedisce la riconfigurazione del computer (uso dell'utility di Computer Setup (F10)) finché non viene immessa la password.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Sicurezza**, quindi **Password di configurazione** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > 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 (Password Options) nel menu Security (Sicurezza). Tra le opzioni della password figura Password Prompt on Warm Boot (Richiesta password al riavvio). Se l'opzione Password Prompt on Warm Boot è abilitata, la password dev'essere immessa ogni volta che il computer viene riavviato.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

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

Immissione della password di accensione

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

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

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

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

Immissione di una password di impostazione

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

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio F10 = Setup, premere il tasto **F10**.

Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

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

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

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

Modifica delle password di accensione e di configurazione

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**. Per cambiare la password di configurazione, eseguire **Computer Setup**.
2. Quando viene visualizzata l'icona della chiave, digitare la password, una barra (/) o un carattere delimitatore alternativo, la nuova password, un'altra barra (/) o un carattere delimitatore alternativo e ancora la nuova password, come di seguito precisato: **password attuale/nuova password/ nuova password**

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

3. Premere **Invio**.

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

Per informazioni sui caratteri delimitatori alternativi consultare la sezione di questo capitolo "Caratteri delimitatori delle tastiere nazionali". Le password d'accensione e di configurazione possono essere modificate anche con le opzioni di sicurezza di Computer Setup.

Cancellazione delle password di accensione e di configurazione

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**. Per cancellare la password di configurazione, eseguire **Computer Setup**.
2. Quando viene visualizzata l'icona della chiave, digitare la password attuale seguita da una barra (/) o da un carattere delimitatore alternativo, come qui illustrato:
   password attuale/
3. Premere **Invio**.

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

Caratteri delimitatori delle tastiere nazionali

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

Caratteri delimitatori delle tastiere nazionali

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

*Per Bosnia-Erzegovina, Croazia, Slovenia e Iugoslavia

Annullamento password

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

DriveLock

DriveLock è una funzione di sicurezza di standard industriale che impedisce l'accesso non autorizzato ai dati memorizzati su determinati dischi fissi. DriveLock è stato implementato come estensione di Computer Setup ed è disponibile solo su alcuni sistemi a condizione che utilizzino dischi fissi compatibili.

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

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

Uso di DriveLock

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

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

Applicazioni di DriveLock

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

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

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

Sensore Smart Cover

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

Livelli di protezione del sensore Smart Cover

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

✎ Le impostazioni possono essere modificate tramite Computer Setup. Per ulteriori informazioni su Computer Setup vedere la *Guida all'utility Computer Setup (F10)*.

Impostazione del livello di protezione del sensore Smart Cover

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

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza)**, quindi **Smart Cover** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Chiusura Smart Cover

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

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

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

Blocco della chiusura Smart Cover

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

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza)**, quindi **Smart Cover** e l'opzione **Bloccata**.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Disattivazione della chiusura Smart Cover

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

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

Uso della chiave FailSafe Smart Cover

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

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

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

È possibile procurarsi la chiave FailSafe in diversi modi:

- Contattare il rivenditore o il centro di assistenza autorizzato HP di fiducia.
- 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.*

Sicurezza MBR (Master Boot Record)

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

Per abilitare la sicurezza MBR procedere come segue:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

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

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

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

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

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

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

Una volta in Computer Setup procedere come segue:

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

È necessario conoscere l'eventuale password di configurazione.

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

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

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

Una volta in Computer Setup procedere come segue:

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

È necessario conoscere l'eventuale password di configurazione.

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

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

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

Una volta in Computer Setup procedere come segue:

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

È necessario conoscere l'eventuale password di configurazione.

Partizionamento e formattazione del disco avviabile corrente

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

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

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

Predisposizione per chiusura con cavo

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

Per le istruzioni consultare la *Guida di riferimento hardware* nel CD *Documentation Library.*

Tecnologia per l'identificazione delle impronte digitali

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

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

Per ulteriori informazioni consultare:
http://www.compaq.com/solutions/security

Notifica guasti e ripristino

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

Quando si verifica un guasto, il computer visualizza un messaggio di avviso locale che contiene una descrizione del guasto e le procedure consigliate. Tramite HP Client Manager, è possibile visualizzare lo stato attuale di integrità del sistema. Se è collegato ad una rete gestita da un prodotto HP Insight Manager, HP Client Manager o da altre applicazioni di gestione sistemi, il computer invia anche un avviso di guasto all'applicazione di gestione della rete.

Drive Protection System (DPS)

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

In fase di produzione dei PC HP, i dischi fissi installati vengono collaudati uno per uno tramite DPS ed in essi 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 le istruzioni sull'uso del DPS consultare la *Guida alla soluzione dei problemi*.

Alimentatore protetto contro gli sbalzi di tensione

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

Sensore termico

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

Indice Analitico

T

U