HP ProtectTools

Guida introduttiva

Prima edizione: Agosto 2012

Numero parte documento: 702113-061

Sommario

1 Informazioni introduttive sulle funzioni di protezione

HP ProtectTools Security Manager è un software che fornisce funzioni di protezione rivolte a salvaguardare il computer, le reti e i dati critici dall'accesso non autorizzato.

Applicazione	Caratteristiche
Console amministrativa di HP ProtectTools Security Manager (per gli amministratori)	• Richiede i diritti di amministratore® Microsoft Windows per accedere. • Fornisce accesso ai moduli configurati da un amministratore e non disponibili agli utenti. • Consente di eseguire la configurazione iniziale delle funzionalità di protezione e di definire le opzioni o i requisiti per tutti gli utenti.
Console utente HP ProtectTools Security Manager (per gli utenti)	• Consente agli utenti di configurare le opzioni rese disponibili da un amministratore. • Consente agli amministratori di fornire agli utenti il controllo limitato di alcuni moduli HP ProtectTools.

I moduli software disponibili variano in base al modello di computer in uso.

I moduli software HP ProtectTools possono essere preinstallati o precaricati nel computer in uso oppure possono essere scaricati dal sito Web HP. Per ulteriori informazioni, consultare http://www.hp.com.

NOTA: Le istruzioni riportate nella presente guida presumono che i moduli software HP ProtectTools pertinenti siano già installati nel computer in uso.

Funzioni di HP ProtectTools

Nella tabella riportata di seguito vengono indicate le funzioni principali dei moduli HP ProtectTools.

Modulo	Funzioni principali
Console amministrativa di HP ProtectTools Security Manager	Gli amministratori possono eseguire le seguenti attività: • Impostazione e configurazione dei livelli di protezione e dei metodi di accesso protetti tramite l'installazione guidata di Security Manager. • Configurazione delle opzioni non visibili dagli utenti. • Attivazione di Drive Encryption e configurazione dell'accesso utente. • Configurazione dei criteri di Device Access Manager e dell'accesso utente. • Utilizzo degli strumenti amministrativi per aggiungere e rimuovere gli utenti HP ProtectTools e visualizzarne lo stato.

Modulo	Funzioni principali
Console utente di HP ProtectTools Security Manager	Gli utenti di base possono eseguire le seguenti attività: • Visualizzazione delle impostazioni relative allo stato della crittografia e a Device Access Manager. • Attivazione di Computrace for HP ProtectTools. • Configurazione delle preferenze e delle opzioni di backup e ripristino.
Credential Manager	Gli utenti di base possono eseguire le seguenti attività: • Modifica dei nomi e delle password utente. • Configurazione e modifica delle credenziali dell'utente, ad esempio password di Windows, impronte digitali, immagini del viso, smart card, schede di prossimità o schede senza contatti.
Password Manager	Gli utenti di base possono eseguire le seguenti attività: • Organizzazione e impostazione delle password e dei nomi utente. • Creazione di password più sicure per livelli superiori di protezione dell'account. Gestore password compila le informazioni e le invia in modo automatico. • Semplificazione della procedura di accesso con la funzione Single Sign On, che consente di salvare e applicare automaticamente le credenziali dell'utente.
Drive Encryption for HP ProtectTools (solo in determinati modelli)	• Crittografia completa dell'unità disco rigido. • Forzatura dell'autenticazione di preavvio per la decrittografia dei dati e il loro utilizzo. • Possibilità di attivazione delle unità che supportano la crittografia automatica (solo in determinati modelli).
Device Access Manager for HP ProtectTools (solo in determinati modelli)	• Consente ai responsabili IT di controllare l'accesso ai dispositivi in base ai profili utente. • Impedisce agli utenti non autorizzati di rimuovere i dati tramite supporti di archiviazione esterni e di introdurre virus nel sistema da supporti simili. • Consente agli amministratori di impedire a utenti o gruppi di utenti specifici di accedere ai dispositivi di comunicazione.
Ritrovamento di PC rubati (Computrace for HP ProtectTools, da acquistare separatamente)	• L'attivazione richiede l'acquisto a parte di sottoscrizioni per il monitoraggio e il tracciamento. • Offre il monitoraggio sicuro delle risorse. • Esegue il monitoraggio dell'attività dell'utente e delle modifiche apportate all'hardware e al software. • Rimane attivo anche in caso di riformattazione o sostituzione del disco rigido.

Descrizione del prodotto di protezione HP ProtectTools ed esempi di uso comune

La maggior parte dei prodotti di protezione HP ProtectTools utilizza sia l'autenticazione utente (in genere una password) che il supporto amministrativo per ottenere l'accesso qualora si dimentichino o

smarriscano le password, o in tutte le situazioni in cui le operazioni di protezione aziendali richiedono l'accesso.

NOTA: alcuni dei prodotti di protezione HP ProtectTools sono progettati per limitare l'accesso ai dati. I dati devono essere crittografati quando la loro importanza è tale da preferirne la perdita alla compromissione. Si consiglia di eseguire il backup di tutti i dati in una posizione protetta.

Password Manager

Password Manager è un archivio per nomi utente e password, e può essere utilizzato per:

- Salvare i nomi e le password di accesso a Internet o alla posta elettronica.
- Eseguire automaticamente l'accesso dell'utente a un sito Web o alla posta.
- Gestire e organizzare le autenticazioni.
- Selezionare una risorsa Web o di rete ed accedere direttamente al link.
- Visualizzare nomi e password se necessario.

Esempio 1: Un addetto agli acquisti di una grande società manifatturiera effettua la maggior parte delle transazioni aziendali su Internet e visita spesso anche diversi siti Web che richiedono credenziali di accesso. L'addetto è consapevole dei rischi alla protezione correlati a queste attività, pertanto utilizza password diverse per ogni account. Decide quindi di utilizzare Password Manager per associare nomi utenti e password diverse ai link Web. Quando visita un sito Web che richiede autenticazione, Password Manager propone in modo automatico le credenziali di accesso. Se desidera visualizzare il nome utente e la password, può configurare Password Manager affinché li renda visibili.

Password Manager può anche essere utilizzato per gestire e organizzare le autenticazioni. Questo strumento consente a un utente di selezionare la risorsa Web o di rete desiderata e di accedere direttamente al link, nonché visualizzare i nomi utente e le password qualora necessario.

Esempio 2:A un dinamico addetto alla contabilità è stata assegnata la gestione dell'intero ufficio contabile. Il team deve accedere a molti account Web client, ciascuno con credenziali diverse. Questi dati di accesso devono essere condivisi con altri utenti, pertanto la riservatezza è un aspetto critico. Il contabile decide quindi di organizzare tutti i link Web, i nomi utente e le password aziendali in Password Manager. Al termine, applica Password Manager ai computer dei dipendenti affinché possano lavorare negli account Web senza mai conoscere le credenziali di accesso in uso.

Drive Encryption for HP ProtectTools (solo in determinati modelli)

Drive Encryption viene utilizzato per limitare l'accesso ai dati di tutta l'unità disco fisso del computer o di un'unità esterna, nonché gestire le unità che supportano la crittografia automatica.

Esempio 1: un medico desidera avere accesso esclusivo ai dati presenti sull'unità disco rigido del suo computer, pertanto attiva Drive Encryption, che richiede l'autenticazione di preavvio prima dell'accesso a Windows. Terminata la configurazione, l'unità disco rigido non può essere aperta senza una password persino prima dell'avvio del sistema operativo. Il medico potrebbe aumentare ulteriormente il livello di protezione dell'unità scegliendo di crittografare i dati con l'opzione delle unità che supportano la crittografia automatica.

Drive Encryption for HP ProtectTools non concede l'accesso ai dati crittografati nemmeno quando il disco viene rimosso, perché sono entrambi legati alla scheda del sistema originale.

Esempio 2: un amministratore ospedaliero desidera garantire che solo i dottori e il personale autorizzato possano accedere a tutti i dati nei loro computer locali senza condividere le loro password personali. Gli addetti del reparto IT aggiungono l'amministratore, i dottori e tutto il personale

autorizzato come utenti di Drive Encryption. A questo punto, solo il personale autorizzato può avviare il computer utilizzando il nome utente e la password personali.

Device Access Manager for HP ProtectTools (solo in determinati modelli)

Device Access Manager for HP ProtectTools consente agli amministratori di limitare e gestire l'accesso all'hardware. Device Access Manager for HP ProtectTools può essere utilizzato per bloccare l'accesso non autorizzato alle unità flash USB su cui possono essere copiati i dati, nonché limitare l'accesso alle unità CD/DVD, il controllo dei dispositivi USB, delle connessioni di rete e così via. Si pensi ad esempio ai fornitori esterni che devono accedere ai computer aziendali, ma che non devono essere in grado di copiare i dati in un'unità USB.

Esempio 1: il manager di un'azienda di fornitura di prodotti medicali lavora spesso con record medici personali e informazioni aziendali. I dipendenti devono accedere a questi dati, tuttavia è estremamente importante che non vengano rimossi dal computer tramite unità USB o altri supporti di archiviazione esterni. La rete è protetta, ma i computer dispongono di masterizzatori di CD e porte USB che potrebbero consentire la copia o il furto dei dati. Il manager usa quindi Device Access Manager per disabilitare le porte USB e i masterizzatori di CD in modo che non possano essere utilizzati. Anche se le porte USB sono bloccate, il mouse e le tastiere continuano a funzionare.

Esempio 2: un'agenzia di assicurazioni non vuole che i dipendenti installino o carichino software o dati personali da casa. Alcuni di essi necessitano dell'accesso alla porta USB su tutti i computer. Il responsabile IT utilizza quindi Device Access Manager per abilitare l'accesso per alcuni dipendenti, bloccando quello esterno ad altri.

Computrace for HP ProtectTools (in precedenza LoJack Pro) (da acquistare separatamente)

Computrace for HP ProtectTools (da acquistare separatamente) è un servizio che consente di rintracciare un computer rubato nel momento in cui viene utilizzato per eseguire l'accesso a Internet. Computrace for HP ProtectTools può anche consentire la gestione e l'individuazione remota dei computer, nonché il monitoraggio dell'uso del computer e delle applicazioni.

Esempio 1: il preside di una scuola ha richiesto al reparto IT di tenere traccia di tutti i computer scolastici. Dopo l'inventario dei PC, l'amministratore IT registra tutti i computer con Computrace per consentire di rintracciarli in caso di furto. Di recente, la scuola ha rilevato la mancanza di diversi computer, pertanto l'amministratore IT ha avvertito le autorità e gli ufficiali Computrace. I computer sono stati individuati e restituiti alla scuola dalle autorità.

Esempio 2: un'agenzia immobiliare deve gestire e aggiornare i computer in tutto il mondo. Si affida quindi a Computrace per monitorare e aggiornare i computer senza dover inviare un addetto IT per ogni computer.

Conseguimento degli obiettivi principali in materia di protezione

I moduli HP ProtectTools possono agire in sinergia per consentire la risoluzione di problemi di protezione di diverso tipo; di seguito vengono riportati alcuni degli obiettivi principali conseguibili:

- Protezione da furto mirato
- Restrizione dell'accesso ai dati riservati
- Blocco dell'accesso non autorizzato da posizioni esterne o interne
- Creazione di criteri per password complesse

Protezione da furto mirato

Un esempio di furto mirato è la sottrazione di un computer contenente informazioni sui clienti e dati riservati presso un checkpoint di sicurezza aeroportuale. Le seguenti funzioni consentono di proteggere dal furto mirato:

- La funzionalità di autenticazione di preavvio, se abilitata, consente di impedire l'accesso al sistema operativo.
  - Security Manager for HP ProtectTools—Vedi HP ProtectTools Security Manager a pagina 25.
  - Drive Encryption for HP ProtectTools—Vedi Drive Encryption for HP ProtectTools (solo in determinati modelli) a pagina 41.
- La crittografia consente di impedire l'accesso ai dati anche in caso di rimozione dell'unità disco rigido e installazione in un sistema non protetto.
- Computrace consente di individuare la posizione di un computer rubato.
  - Computrace for HP ProtectTools—Vedi Ritrovamento in seguito a furto (solo in determinati modelli) a pagina 61.

Restrizione dell'accesso ai dati riservati

Si supponga che un revisore contabile esterno lavori presso la sede di un'azienda e che sia autorizzato ad accedere ai computer per rivedere dati finanziari riservati; non si desidera però che stampi i file o li salvi in un dispositivo riscrivibile, ad esempio un CD. La seguente funzionalità consente di limitare l'accesso ai dati:

- Device Access Manager for HP ProtectTools consente ai responsabili IT di limitare l'accesso ai dispositivi di comunicazione, in modo da impedire la stampa o la copia di informazioni riservate contenute nell'unità disco rigido. Vedere Configurazione delle classi di periferiche a pagina 52.

Blocco dell'accesso non autorizzato da posizioni esterne o interne

L'accesso non autorizzato a un computer aziendale non protetto rappresenta un rischio reale per le risorse di rete dell'organizzazione, ad esempio le informazioni dei servizi finanziari, di un executive o di un team di ricerca e sviluppo, nonché informazioni private ad esempio record di pazienti o record finanziari personali. Le seguenti funzionalità consentono di impedire l'accesso non autorizzato:

- La funzionalità di autenticazione di preavvio, se abilitata, consente di impedire l'accesso al sistema operativo.
  - Security Manager for HP ProtectTools—Vedi HP ProtectTools Security Manager a pagina 25.
  - Drive Encryption for HP ProtectTools—Vedi Drive Encryption for HP ProtectTools (solo in determinati modelli) a pagina 41.
- Security Manager consente di garantire che solo un utente autorizzato possa ottenere le password o l'accesso alle applicazioni protette da password. Vedere HP ProtectTools Security Manager a pagina 25.
- Device Access Manager for HP ProtectTools consente ai responsabili IT di limitare l'accesso ai dispositivi riscrivibili, in modo da impedire la stampa o la copia di informazioni riservate dall'unità disco rigido. Vedere Device Access Manager for HP ProtectTools (solo in determinati modelli) a pagina 50.

Creazione di criteri per password complesse

Se i criteri di un'azienda richiedono l'utilizzo di password complesse per dozzine di database e applicazioni basate sul Web, Security Manager offre un archivio protetto per le password e per la funzione Single Sign On. Vedere HP ProtectTools Security Manager a pagina 25.

Elementi per protezione aggiuntiva

Assegnazione di ruoli di protezione

Una prassi importante nell'ambito della gestione della protezione informatica, soprattutto delle organizzazioni di grandi dimensioni, consiste nell'assegnazione di responsabilità e diritti a diversi tipi di amministratori e utenti.

NOTA: Per singoli individui o organizzazioni di piccole dimensioni, questi ruoli possono essere assegnati alla stessa persona.

In HP ProtectTools, le responsabilità e i privilegi correlati alla protezione possono essere classificati nei seguenti ruoli:

- Responsabile della protezione—Definisce il livello di protezione dell'azienda o della rete, e determina le funzionalità di protezione da distribuire, ad esempio Drive Encryption.

  NOTA: Molte funzioni di HP ProtectTools possono essere personalizzate dal responsabile della protezione in collaborazione con HP. Per ulteriori informazioni, consultare http://www.hp.com.

- Amministratore IT—Applica e gestisce le funzionalità di protezione definite dal responsabile della protezione, e può anche abilitare o disabilitare alcune funzionalità. Ad esempio, se il responsabile della protezione ha deciso di implementare l'impiego delle smart card, l'amministratore IT può abilitare sia la modalità password che la modalità smart card.
- Utente—Utilizza le funzioni di protezione. Ad esempio, se il responsabile della protezione e l'amministratore IT hanno abilitato le smart card per il sistema, l'utente può impostare il PIN della smart card e utilizzare quest'ultima per l'autenticazione.

ATTENZIONE: Gli amministratori sono esortati a seguire le “strategie” di restrizione dei privilegi e di limitazione dell'accesso per gli utenti finali.

I privilegi amministrativi non devono essere assegnati agli utenti non autorizzati.

Gestione delle password di HP ProtectTools

Molte funzioni di HP ProtectTools Security Manager sono protette da password. Nella tabella riportata di seguito vengono indicati i tipi di password utilizzati più spesso, la loro funzione e il modulo software in cui vengono impostate.

Nella tabella vengono anche indicate le password impostate e utilizzate soltanto dagli amministratori IT. Tutte le altre password possono essere impostate da amministratori o utenti senza privilegi.

Password di HP ProtectTools	Modulo di impostazione	Funzione
Password di accesso Windows	Pannello di controllo Windows o HP ProtectTools Security Manager	Può essere utilizzata per eseguire l'accesso manuale e l'autenticazione al fine di accedere a diverse funzioni di Security Manager.

Password di HP ProtectTools	Modulo di impostazione	Funzione
Password di backup e ripristino di Security Manager	Security Manager, da singolo utente	Protegge l'accesso al file di backup e ripristino di Security Manager.
PIN della Smart Card	Credential Manager	Può essere utilizzato come autenticazione a più fattori. Può essere utilizzato come autenticazione Windows. Se è selezionata la smart card, autentica gli utenti di Drive Encryption.

Creazione di una password sicura

Quando si creano le password, occorre innanzitutto attenersi a tutte le eventuali specifiche previste dal programma. In generale, tuttavia, è possibile attenersi alle seguenti linee guida per creare password sicure e ridurne la probabilità di compromissione:

- Utilizzare password con più di 6 caratteri, preferibilmente più di 8.
- Utilizzare sia lettere maiuscole che minuscole.
- Quando possibile, utilizzare caratteri alfanumerici e includere caratteri speciali e segni di punteggiatura.
- Sostituire i caratteri speciali o i numeri con le lettere, ad esempio utilizzare il numero 1 per le lettere I o L.
- Combinare parole di 2 o più lingue.
- Dividere a metà una parola o una frase con numeri o caratteri speciali, ad esempio “Mary2-2Cat45.”
- Non utilizzare come password una parola che potrebbe essere presente in un dizionario.
- Non utilizzare il proprio nome come password o qualsiasi altra informazione personale quale data di nascita, nomi di animali domestici o nome da nubile della madre, anche se utilizzati al contrario.
- Cambiare le password periodicamente. È possibile cambiare anche soltanto un paio di caratteri per aumentarne la sicurezza.
- Se si trascrive la password, non tenerla vicino al computer.
- Non salvare la password in un file, ad esempio in un'e-mail sul computer.
- Non condividere gli account o comunicare la password a terzi.

Backup delle credenziali e delle impostazioni

È possibile eseguire il backup delle credenziali nei seguenti modi:

- Utilizzare Drive Encryption for HP ProtectTools per selezionare le credenziali di HP ProtectTools ed eseguirne il backup.
- Utilizzare lo strumento di backup e ripristino in HP ProtectTools Security Manager come posizione centrale da cui eseguire il backup e il ripristino delle credenziali di protezione da alcuni dei moduli di HP ProtectTools installati.

2 Guida

Per configurare le impostazioni di HP ProtectTools, utilizzare l'Installazione gudiata di HP Client Security o di HP ProtectTools Security Manager.

Al termine dell'Installazione guidata di HP Client Security, lo stato dell'applicazione è visualizzato sul pannello di controllo di HP Client Security.

Installazione guidata HP Client Security

NOTA: Per poter amministrare HP ProtectTools è necessario disporre dei privilegi di amministratore.

L'Installazione guidata di HP Client Security assiste l'utente in tutte le fasi della configurazione delle funzioni più comuni dell'applicazione. Se l'Installazione guidata di HP Client Security non è stata completata in precedenza, è possibile avviarla con una di queste modalità:

▲ Dal menu Avvio, fare clic su o toccare l'applicazione **HP Client Security**.

– oppure –

Dal desktop di Windows, fare clic su o toccare il gadget **HP ProtectTools**.

Le pagine vengono visualizzate nel seguente ordine:

1. **Dominio Windows**—Inserire la password di Windows.

   Ciò consente di proteggere l'account di Windows utilizzando un'autenticazione complessa.

2. **SpareKey**—Per registrare l'opzione SpareKey, selezionare tre domande di sicurezza.

3. **Registrare le impronte digitali**—Nel caso un lettore di impronte digitali e relativo driver siano installati, è possibile registrare le impronte digitali. È necessario selezionare e registrare almeno 2 impronte digitali.

4. **Drive Encryption**—Se Drive Encryption for HP ProtectTools è installato è possibile attivare la crittografia sul disco primario:

   - Crittografia software per un disco rigido tradizionale.
   - Crittografia hardware se viene rilevato un disco autocrittografante.

   È necessario salvare una o più delle seguenti chiavi di crittografia prima di abilitare la crittografia:

   NOTA: Se l'Installazione guidata viene interrotta, non sarà possibile attivare l'autenticazione Windows e Drive Encryption.

   - **Dispositivi rimovibili**, come supporti USB in formato FAT32.
     - Questa opzione è selezionata per default se viene rilevato un dispositivo rimovibile prima che venga visualizzata la pagina Drive Encryption.
     - Se vengono rilevati 2 o più dispositivi mobili, selezionarne uno tra quelli visualizzati.
   - **SkyDrive**—Questa opzione è disponibile se viene rilevata una connessione Internet.

Un Live ID® Windows è necessario. Inserire ID e password, o richiederne una.

5. La pagina Fine visualizza la notifica dell'avvenuta operazione, dopo la quale viene richiesto di riavviare il computer per completare l'attivazione di Drive Encryption.

Installazione guidata di HP ProtectTools Security

NOTA: Per poter amministrare HP ProtectTools è necessario disporre dei privilegi di amministratore.

L'installazione guidata di HP ProtectTools Security Manager assiste l'utente in tutte le fasi dell'impostazione di HP ProtectTools Security Manager. Oltre alle impostazioni nella procedura di installazione guidata, gli amministratori possono configurare molte altre funzioni aggiuntive dalla Console amministrativa. Queste impostazioni vengono applicate al computer e a tutti gli utenti che lo condividono.

Per avviare l'Installazione guidata di HP ProtectTools Security Manager:

▲ Fare clic su **Installazione guidata** nel riquadro a sinistra della Console amministrativa, poi seguire le istruzioni a schermo fino al completamento dell'installazione.

Gli amministratori possono avviare la Console amministrativa dalla Console utente HP ProtectTools Security Manager. Per ulteriori informazioni, vedere Console amministrativa HP ProtectTools Security Manager a pagina 14.

Security Manager e le sue applicazioni sono disponibili a tutti gli utenti che condividono il computer.

Pannello di controllo HP Client Security

Per avviare HP Client Security dopo averne completato l'installazione guidata:

▲ Dal menu Avvio digitare `hp`, poi selezionare **HP Client Security**.

Il pannello di controllo mostra una rapida panoramica delle funzioni e relativo stato per ciascuna applicazione.

▲ Fare clic su o toccare un'applicazione per visualizzare più informazioni sull'applicazione selezionata:

- Il tasto **Configura ora** indica un'applicazione non ancora configurata. Fare clic su o toccare il pulsante per aprire la pagina dell'applicazione per configurare l'applicazione.
- Il pulsante **Impostazioni** indica un'applicazione con stato OK. Fare clic su o toccare il pulsante per accedere alle impostazioni per l'applicazione.
- La **Console utente** è avviata per la configurazione utente.
- La **Console utente** è avviata per una configurazione che richiede privilegi di amministrazione.
- Il **Dashboard stato** rimane aperto dopo l'avvio di Console utente o Console amministrativa, e una volta configurate le impostazioni e chiusa la Console, lo stato viene aggiornato.

3 Guida rapida all'installazione per piccole aziende

In questo capitolo vengono descritti i passaggi di base per l'attivazione delle opzioni più utili e comuni di HP ProtectTools for Small Business. Questo software offre numerosi strumenti e opzioni che consentono di regolare le preferenze e impostare il controllo dell'accesso. La presente guida rapida all'installazione descrive i passaggi necessari per rendere operativo ciascun modulo nel minor tempo possibile e con i minori sforzi. Selezionare il modulo desiderato e fare clic sul pulsante **?** o della Guida nell'angolo superiore destro per leggere ulteriori informazioni sulla finestra attualmente visualizzata.

Guida introduttiva

1. Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.
2. Immettere la password di Windows o crearne una.
3. Completare l'installazione guidata.

NOTA: Per default, HP ProtectTools Security Manager è impostato su Autenticazione complessa.

Questa impostazione è progettata per impedire l'accesso non autorizzato mentre si è in Windows e deve essere utilizzata quando occorre protezione avanzata o quando si lasciano spesso i computer incustoditi. Per modificare questa impostazione, fare clic sulla scheda Criterio sessione ed effettuare le selezioni desiderate.

Per fare in modo che HP ProtectTools Security Manager richieda l'autenticazione solo una volta durante l'accesso a Windows, seguire questa procedura.

1. Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.
2. Nel riquadro sinistro di Security Manager, fare clic su **Amministrazione**, quindi su **Console amministrativa**.
3. Nel riquadro sinistro, sotto la voce **Sistema**, selezionare **Autenticazione** dal gruppo **Sicurezza**.
4. Fare clic sulla scheda **Criterio di sessione** e selezionare i requisiti di login per la sessione. Per annullare queste selezioni fare clic su **Ripristina impostazioni predefinite**.
5. Al termine, fare clic sul pulsante **Applica**.

Password Manager

Password! Ne abbiamo tutti molte, specie per quei siti o quelle applicazioni a cui accediamo regolarmente e che richiedono una password. L'utente normale di solito utilizza la stessa password per tutti i siti e le applicazioni, o ne sceglie sempre una diversa, dimenticando regolarmente quale password si abbina a quale applicazione.

Password Manager può ricordare automaticamente le password o dare la possibilità di scegliere quali siti ricordare e quali no. Una volta effettuato l'accesso al computer, Password Manager fornirà le password o le credenziali per accedere ai diversi siti e applicazioni.

Quando si accede a un'applicazione o a un sito Web che richiede le credenziali, Password Manager riconoscerà automaticamente il sito e chiederà se si desidera salvare tali dati. Se si desidera escludere determinati siti, è possibile declinare la richiesta.

Per avviare il salvataggio dei siti Web, dei nomi utente e delle password, procedere come segue:

1. Ad esempio, provate ad accedere a un sito o un'applicazione ad accesso ristretto, poi fate clic sull'icona di Password Manager nell'angolo in alto a sinistra della pagina Web.
2. Assegnare un nome al collegamento (facoltativo) e immettere un nome utente e una password in Password Manager.

NOTA: Vengono evidenziate le aree che Password Manager utilizzerà ora e durante le visite successive.

3. Al termine, fare clic sul pulsante **OK**.
4. Password Manager può anche salvare il nome utente e le password per le condivisioni di rete o per le unità di rete mappate.

Visualizzazione e gestione delle autenticazioni salvate in Password Manager

Password Manager consente di visualizzare, gestire, eseguire il backup e avviare le autenticazioni da una posizione centrale. Password Manager supporta anche l'avvio dei siti salvati da Windows.

Per aprire Password Manager, utilizzare uno dei due seguenti metodi:

- Utilizzare la combinazione dei tasti ctrl+tasto con il logo di Windows+h per aprire Password Manager, quindi fare clic su **Apri** per avviare e autenticare il collegamento salvato.

  – oppure –

- Selezionare la scheda **Gestione** in Password Manager per aprire HP ProtectTools Security Manager e modificare le credenziali.

Le opzioni di modifica di Password Manager consentono di visualizzare e modificare il nome, il nome di login e le password.

HP ProtectTools for Small Business consente di eseguire un backup e/o una copia su un altro computer di tutte le credenziali e le impostazioni.

Device Access Manager for HP ProtectTools

Device Access Manager consente di limitare l'utilizzo di diversi dispositivi di archiviazione esterni e interni in modo da garantire la protezione dei dati sull'unità disco rigido. Ad esempio, un utente potrebbe consentire l'accesso ai suoi dati a un altro utente, ma potrebbe impedirne la copia su un CD, un lettore di musica personale o un dispositivo di memoria USB. Di seguito viene illustrato un modo rapido per eseguire la configurazione.

1. Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.
2. Nel riquadro sinistro di HP ProtectTools Security Manager, fare clic su **Amministrazione**, quindi su **Console amministrativa**.
3. Fare clic su **Device Access Manager**, poi su **Device Class Configuration**.
4. Il passaggio successivo è la selezione degli utenti che avranno accesso mentre tutti gli altri saranno bloccati.
5. Selezionare i dispositivi hardware da limitare, quindi fare clic sul pulsante **Applica** per terminare la procedura.
6. Selezionare **Aggiungi**, fare clic su **Avanzate**, poi su **Trova ora**.
7. Selezionare l'utente desiderato, poi fare clic su **OK > OK > Applica**.

   La selezione è visualizzata nel riquadro **Utenti/Gruppi**.
8. Selezionare la **Classe di periferiche** che si desidera utilizzare, selezionare **Consenti** o **Nega**, poi **Applica**.

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools viene utilizzato per proteggere i dati mediante la crittografia di tutta l'unità disco rigido. I dati presenti nell'unità disco rigido rimarranno protetti in caso di furto del PC o di rimozione dell'unità disco rigido e di installazione in un computer diverso da quello originale.

Un vantaggio ulteriore dal punto di vista della sicurezza è che Drive Encryption richiede di autenticarsi usando i propri nome utente e password prima dell'avvio del sistema operativo. Questo processo è chiamato autenticazione preavvio.

Per semplicità, più moduli software sincronizzano le password automaticamente, tra cui gli account utenti di Windows, i domini, Drive Encryption for HP ProtectTools, Password Manager e HP ProtectTools Security Manager.

Per attivare Drive Encryption for HP ProtectTools, utilizzare i semplici passaggi riportati di seguito:

1. Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.
2. Nel riquadro sinistro di Security Manager, fare clic su **Amministrazione**, quindi su **Console amministrativa**.
3. Nel riquadro di sinistra, fare clic su **Installazione guidata**.
4. Nella schermata di benvenuto, selezionare **Avanti**.
5. Per avviare la procedura guidata di attivazione, immettere la password di Windows e fare clic su **Avanti**.
6. Ignorare la SpareKey se non si desidera utilizzarla.

7. Selezionare la casella **Drive Encryption**, quindi fare clic su **Avanti**.
8. Selezionare l'unità da crittografare, quindi fare clic su **Avanti**.
9. La finestra di configurazione di Drive Encryption richiede un dispositivo USB o altri dispositivi esterni per memorizzare la chiave di ripristino. Conservare al sicuro questa chiave, poiché è necessaria per ripristinare i dati o accedere al disco in caso di smarrimento o errore della password di preavvio.
10. Fare clic su **Avanti**, completare la procedura, quindi fare clic su **Fine**. Rimuovere l'unità flash USB, quindi riavviare il computer.
11. All'avvio del sistema, Drive Encryption richiederà la password di Windows. Immetterla, quindi fare clic su **OK**.

NOTA: Il computer può rallentare durante il processo di crittografia del disco. Al termine del processo il funzionamento tornerà normale. A ogni accesso del disco i dati vengono crittografati o decrittografati a seconda delle impostazioni stabilite dall'amministratore.

L'autenticazione di Drive Encryption è legata al login di Windows e consente di accedere direttamente al desktop Windows, senza necessità di inserire la password due volte.

4 Console amministrativa HP ProtectTools Security Manager

HP ProtectTools Security Manager è un software che fornisce funzioni di protezione rivolte a salvaguardare il computer, le reti e i dati critici dall'accesso non autorizzato. Le operazioni di amministrazione di HP ProtectTools Security Manager vengono eseguite tramite la Console amministrativa.

Nella Console utente di Security Manager sono disponibili applicazioni aggiuntive (solo in determinati modelli) che assistono l'utente nel ritrovamento del computer in caso di perdita o furto.

L'amministratore locale può utilizzare la Console amministrativa per eseguire le seguenti attività:

- Abilitazione o disabilitazione delle funzioni di protezione
- Definizione delle credenziali di autenticazione obbligatorie
- Gestione degli utenti del computer
- Modifica dei parametri specifici del dispositivo
- Configurazione delle applicazioni di Security Manager installate

Guida introduttiva

Per configurare le impostazioni di HP ProtectTools, utilizzare l'Installazione gudiata di HP Client Security o di HP ProtectTools Security Manager.

Al termine dell'Installazione guidata di HP Client Security, lo stato dell'applicazione è visualizzato sul pannello di controllo di HP Client Security.

Installazione guidata HP Client Security

NOTA: Per poter amministrare HP ProtectTools è necessario disporre dei privilegi di amministratore.

L'Installazione guidata di HP Client Security assiste l'utente in tutte le fasi della configurazione delle funzioni più comuni dell'applicazione. Se l'Installazione guidata di HP Client Security non è stata completata in precedenza, è possibile avviarla con una di queste modalità:

▲ Dal menu Avvio, fare clic su o toccare l'applicazione **HP Client Security**.

– oppure –

Dal desktop di Windows, fare clic su o toccare il gadget **HP ProtectTools**.

Le pagine vengono visualizzate nel seguente ordine:

1. **Dominio Windows**—Inserire la password di Windows.

   Ciò consente di proteggere l'account di Windows utilizzando un'autenticazione complessa.

2. **SpareKey**—Per registrare l'opzione SpareKey, selezionare tre domande di sicurezza.

3. **Registrare le impronte digitali**—Nel caso un lettore di impronte digitali e relativo driver siano installati, è possibile registrare le impronte digitali. È necessario selezionare e registrare almeno 2 impronte digitali.

4. **Drive Encryption**—Se Drive Encryption for HP ProtectTools è installato è possibile attivare la crittografia sul disco primario:

   - Crittografia software per un disco rigido tradizionale
   - Crittografia hardware se viene rilevato un disco autocrittografante.

   È necessario salvare una o più delle seguenti chiavi di crittografia prima di abilitare la crittografia:

   NOTA: Se l'Installazione guidata viene interrotta, non sarà possibile attivare l'autenticazione Windows e Drive Encryption.

   - **Dispositivi rimovibili**, come supporti USB in formato FAT32.
     - Questa opzione è selezionata per default se viene rilevato un dispositivo rimovibile prima che venga visualizzata la pagina Drive Encryption.
     - Se vengono rilevati 2 o più dispositivi mobili, selezionarne uno tra quelli visualizzati.
   - **SkyDrive**—Questa opzione è disponibile se viene rilevata una connessione Internet.

     Un Live ID® Windows è necessario. Inserire ID e password, o richiederne una.

5. La pagina Fine visualizza la notifica dell'avvenuta operazione, dopo la quale viene richiesto di riavviare il computer per completare l'attivazione di Drive Encryption.

Installazione guidata di HP ProtectTools Security

NOTA: Per poter amministrare HP ProtectTools è necessario disporre dei privilegi di amministratore.

L'installazione guidata di HP ProtectTools Security Manager assiste l'utente in tutte le fasi dell'impostazione di HP ProtectTools Security Manager. Oltre alle impostazioni nella procedura di installazione guidata, gli amministratori possono configurare molte altre funzioni aggiuntive dalla Console amministrativa. Queste impostazioni vengono applicate al computer e a tutti gli utenti che lo condividono.

Per avviare l'Installazione guidata di HP ProtectTools Security Manager:

▲ Fare clic su **Installazione guidata** nel riquadro a sinistra della Console amministrativa, poi seguire le istruzioni a schermo fino al completamento dell'installazione.

Gli amministratori possono avviare la Console amministrativa dalla Console utente HP ProtectTools Security Manager. Per ulteriori informazioni, vedere Console amministrativa HP ProtectTools Security Manager a pagina 14.

Security Manager e le sue applicazioni sono disponibili a tutti gli utenti che condividono il computer.

Pannello di controllo HP Client Security

Per avviare HP Client Security dopo averne completato l'installazione guidata:

▲ Dal menu Avvio digitare `hp`, poi selezionare **HP Client Security**.

Il pannello di controllo mostra una rapida panoramica delle funzioni e relativo stato per ciascuna applicazione.

▲ Fare clic su o toccare un'applicazione per visualizzare più informazioni sull'applicazione selezionata:

- Il tasto **Configura ora** indica un'applicazione non ancora configurata. Fare clic su o toccare il pulsante per aprire la pagina dell'applicazione per configurare l'applicazione.
- Il pulsante **Impostazioni** indica un'applicazione con stato OK. Fare clic su o toccare il pulsante per accedere alle impostazioni per l'applicazione.
- La **Console utente** è avviata per la configurazione utente.
- La **Console utente** è avviata per una configurazione che richiede privilegi di amministrazione.
- Il **Dashboard stato** rimane aperto dopo l'avvio di Console utente o Console amministrativa, e una volta configurate le impostazioni e chiusa la Console, lo stato viene aggiornato.

Apertura della Console amministrativa di HP ProtectTools

Utilizzare la Console amministrativa HP ProtectTools per attività amministrative, come impostare i criteri di sistema o configurare un software. Per accedere alla Console amministrativa, aprire HP ProtectTools Security Manager:

1. Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.

   – oppure –

   Da **Pannello di controllo**, selezionare **Sistema e sicurezza**, poi **HP ProtectTools Security Manager**.

2. Nel riquadro sinistro della Console utente di Security Manager, fare clic su **Amministrazione**, quindi su **Console amministrativa**.

Utilizzo della Console amministrativa

La Console amministrativa di HP ProtectTools è la posizione centrale per l'amministrazione delle funzioni e delle applicazioni di HP ProtectTools Security Manager.

1. Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.

   – oppure –

   Da **Pannello di controllo**, selezionare **Sistema e sicurezza**, poi **HP ProtectTools Security Manager**.

2. Nel riquadro sinistro della Console utente di Security Manager, fare clic su **Amministrazione**, quindi su **Console amministrativa**.

Nel riquadro sinistro della Console amministrativa, in Home, vengono visualizzate le seguenti opzioni:

- **Sistema**—Consente di configurare le seguenti funzioni di protezione e l'autenticazione per utenti e dispositivi.
  - **Protezione**
  - **Utenti**
  - **Credenziali**
- **Applicazioni**—Consente di configurare le impostazioni generali di HP ProtectTools Security Manager e delle applicazioni di Security Manager.
- **Dati**—consente di configurare le impostazioni per Drive Encryption (solo per modelli selezionati).
- **Computer**—Consente di configurare le impostazioni per Device Access Manager.
- **Installazione guidata**—Assiste l'utente in tutte le fasi dell'impostazione di HP ProtectTools Security Manager.
- **Informazioni su**—Visualizza le informazioni su HP ProtectTools Security Manager, ad esempio il numero di versione e l'informativa sul copyright.
- **Area principale**—Visualizza le schermate specifiche dell'applicazione.

  ?—Consente di visualizzare la guida della Console amministrativa. Questa icona si trova nell'angolo superiore destro della finestra, accanto alle icone per la riduzione e l'ingrandimento.

Configurazione del sistema

Il gruppo **Sistema** è accessibile dal riquadro del menu Strumenti a sinistra della schermata della Console amministrativa di HP ProtectTools. È possibile utilizzare le applicazioni in questo gruppo per gestire i criteri e le impostazioni del computer, i suoi utenti e i suoi dispositivi.

Le applicazioni riportate di seguito sono incluse nel gruppo **Sistema**:

- **Protezione**—Consente di gestire le funzioni, l'autenticazione e le impostazioni che regolano la modalità di interazione degli utenti con il computer.
- **Utenti**—Consente di configurare, gestire e registrare gli utenti del computer.
- **Credenziali**—Consente di gestire le impostazioni dei dispositivi di protezione integrati o collegati al computer.

Impostazione dell'autenticazione del computer

All'interno dell'applicazione di autenticazione, è possibile impostare i criteri che disciplinano l'accesso al computer. È possibile specificare le credenziali richieste per eseguire l'autenticazione di ogni classe di utente durante l'accesso a Windows o ai siti Web e ai programmi durante una sessione utente.

Per impostare l'autenticazione del computer:

1. Nel riquadro sinistro della Console amministrativa, fare clic su **Protezione**, quindi su **Autenticazione**.
2. Per configurare l'autenticazione dell'accesso, fare clic sulla scheda **Criterio di accesso**, apportare le modifiche, quindi fare clic su **Applica**.
3. Per configurare l'autenticazione della sessione, fare clic sulla scheda **Criterio di sessione**, apportare le modifiche, quindi fare clic su **Applica**.

Criterio di accesso

Per definire i criteri che regolano le credenziali richieste per autenticare un utente quando esegue l'accesso a Windows:

1. Nel riquadro sinistro della Console amministrativa, fare clic su **Protezione**, quindi su **Autenticazione**.
2. Nella scheda **Criteri di accesso**, selezionare una categoria di utenti, come Amministratori o Utenti standard.
3. Fare clic su una credenziale di autenticazione per visualizzare la finestra di modifica.
4. Per richiedere una combinazione di due credenziali di autenticazione, fare clic sulla freccia rivolta verso il basso per selezionare ciascuna credenziale, quindi fare clic su **OK**.
5. Per rimuovere una credenziale, fare clic sulla **X** oppure fare clic con il pulsante destro del mouse sulla credenziale, quindi fare clic su **Elimina**.
6. Nella finestra di dialogo di configurazione, fare clic su **Sì**.
7. Per verificare che gli utenti possano accedere, fare clic su **Controlla che gli utenti di HP ProtectTools possano eseguire l'accesso**.
8. Per ripristinare i valori originali delle impostazioni, fare clic su **Ripristina impostazioni predefinite**.
9. Fare clic su **Applica**.

Criterio di sessione

Per definire i criteri che regolano le credenziali richieste per l'autenticazione durante una sessione di Windows:

1. Nel riquadro sinistro della Console amministrativa, fare clic su **Protezione**, quindi su **Autenticazione**.
2. Nella scheda **Criteri di sessione**, selezionare una categoria di utenti, come Amministratori o Utenti standard.
3. Fare clic su una credenziale di autenticazione per visualizzare la finestra di modifica.
4. Per richiedere una combinazione di due credenziali di autenticazione, fare clic sulla freccia rivolta verso il basso per selezionare ciascuna credenziale, quindi fare clic su **OK**.
5. Per rimuovere una credenziale, fare clic sulla **X** oppure fare clic con il pulsante destro del mouse sulla credenziale, quindi fare clic su **Elimina**.
6. Nella finestra di dialogo di configurazione, fare clic su **Sì**.
7. Per verificare che gli utenti possano accedere, fare clic su **Controlla che gli utenti di HP ProtectTools possano eseguire l'accesso**.

8. Per ripristinare i valori originali delle impostazioni, fare clic su **Ripristina impostazioni predefinite**.
9. Fare clic su **Applica**.

Impostazioni

Per consentire agli utenti del computer di ignorare l'accesso di Windows se l'autenticazione è stata già eseguita a livello di BIOS o di Drive Encryption, procedere come segue:

1. Nel riquadro sinistro della Console amministrativa, fare clic su **Protezione**, quindi su **Impostazioni**.
2. **Consenti accesso One Step logon**—Selezionare la casella di controllo per abilitare l'accesso One Step logon oppure deselezionarla per disabilitarlo.
3. Fare clic su **Applica**.

Gestione degli utenti

All'interno dell'applicazione Utenti, è possibile monitorare e gestire gli utenti di HP ProtectTools del computer.

Tutti gli utenti di HP ProtectTools sono elencati e verificati a fronte dei criteri impostati tramite Security Manager e in base al fatto che abbiano eseguito o meno la registrazione delle credenziali appropriate che consentono di soddisfare questi criteri.

Per gestire gli utenti, scegliere tra le seguenti impostazioni:

- Per aggiungere utenti, fare clic su **Aggiungi**.
- Per eliminare un utente, selezionare l'utente desiderato, quindi fare clic su **Elimina**.
- Per impostare credenziali aggiuntive per l'utente, fare clic sull'utente desiderato, quindi su **Registra**.
- Per visualizzare i criteri per un utente specifico, selezionare l'utente desiderato e visualizzare i criteri nella finestra in basso.

Credenziali

All'interno dell'applicazione Credenziali, è possibile configurare le impostazioni disponibili per tutti i dispositivi di protezione integrati o collegati riconosciuti da HP ProtectTools Security Manager.

SpareKey

È possibile scegliere se consentire l'autenticazione SpareKey all'avvio di Windows e gestire le domande di protezione che verranno visualizzate dagli utenti durante la loro registrazione a SpareKey.

1. Selezionare le domande di protezione che verranno visualizzate dagli utenti durante la loro registrazione a SpareKey.

   È possibile specificare fino a tre domande personalizzate oppure è possibile consentire agli utenti di digitare passphrase personalizzate.
2. Per consentire il ripristino SpareKey per l'accesso a Windows, selezionare la casella di controllo.
3. Fare clic su **Applica**.

Impronte digitali

Se un lettore di impronte digitali è installato o collegato al computer, la pagina Impronte digitali visualizza le seguenti schede:

- **Registrazione**—Consente di scegliere il numero minimo e massimo di impronte digitali che un utente può registrare.

  È inoltre possibile cancellare tutti i dati dal lettore di impronte digitali.

  ⚠ **ATTENZIONE:** la cancellazione di tutti i dati dal lettore di impronte digitali comporta la cancellazione di tutti i dati di tutti gli utenti, inclusi gli amministratori. Se il criterio di accesso richiede soltanto le impronte digitali, a tutti gli utenti può essere impedito l'accesso al computer.

- **Sensibilità**—Spostare il dispositivo di scorrimento per regolare la sensibilità di scansione del lettore di impronte digitali al passaggio del dito.

  Se l'impronta digitale non viene riconosciuta in modo coerente, potrebbe essere necessario selezionare un livello di sensibilità inferiore. Un livello superiore aumenta la sensibilità alle varianti nelle scansioni delle impronte digitali, diminuendo di conseguenza la possibilità di una falsa accettazione. L'impostazione **medio-alta** offre una buona combinazione di protezione e praticità.

- **Avanzate**—Selezionare una delle seguenti opzioni per configurare il lettore di impronte digitali in modo da risparmiare energia e migliorare il feedback visivo:

  - **Ottimizzato**—Il lettore di impronte digitali viene attivato all'occorrenza. Al primo utilizzo, si potrebbe notare un leggero ritardo nella risposta del lettore.
  - **Risparmia energia**—Il lettore di impronte digitali risponde più lentamente, ma consuma molto meno.
  - **Modalità a consumo normale**—Il lettore di impronte digitali è sempre pronto per essere utilizzato, ma consuma più energia.

Viso

Se il computer ha una webcam installata o collegata, e se il programma Face Recognition è installato, è possibile impostare il livello di protezione di Face Recognition in modo da ottenere un buon compromesso tra facilità d'uso e protezione del computer.

1. Selezionare **Credenziali**, quindi fare clic su **Viso**.
2. Spostare il dispositivo di scorrimento verso sinistra se si desidera maggior praticità, spostarlo verso destra se invece si preferisce una maggiore precisione.

   - **Praticità**—Per semplificare l'accesso agli utenti registrati in situazioni marginali, spostare il dispositivo di scorrimento nella posizione **Praticità**.
   - **Bilanciamento**—Se si desidera un buon compromesso tra protezione e usabilità oppure se si hanno informazioni riservate o se il computer viene utilizzato in un luogo dove possono verificarsi tentativi di accesso non autorizzati, spostare il dispositivo di scorrimento nella posizione **Bilanciamento**.
   - **Precisione**—Per rendere più difficile l'accesso di un utente se le scene registrate o le condizioni di luce correnti sono al di sotto del normale, nonché rendere meno probabile una falsa accettazione, spostare il dispositivo di scorrimento nella posizione **Precisione**.

3. Per ripristinare i valori originali delle impostazioni, fare clic su **Ripristina impostazioni predefinite**.
4. Fare clic su **Applica**.

Smart card

Per poter essere utilizzata, la smart card deve essere prima inizializzata dagli amministratori. La maggior parte delle smart card standard CSP e PKCS11 sono supportate in Windows.

Inizializzazione della smart card

HP ProtectTools Security Manager supporta un certo numero di smart card diverse. Il numero e il tipo di caratteri usati come numeri PIN possono variare. Il produttore della smart card deve fornire gli strumenti necessari per installare un certificato di protezione e un PIN di gestione da utilizzare negli algoritmi di protezione di HP ProtectTools.

NOTA: è necessario che sia installata un'applicazione middleware per le smart card.

1. Scaricare e installare l'applicazione middleware per la smart card in uso (ad esempio ActivClient 6.x per una smart card ActivIdentity).
2. Inserire la smart card nel lettore.
3. Inizializzare (formattare) la smart card.
   a. Lo strumento di inizializzazione della smart card può essere avviato manualmente oppure visualizzato all'inserimento della smart card nel lettore.
   b. Seguire le istruzioni visualizzate per impostare un PIN.
   c. Prendere nota del codice di sblocco per riferimento futuro.
4. Creare una coppia di chiavi e un certificato.
   a. Aprire la Console amministrativa di **HP ProtectTools**.
   b. Fare clic su **Credenziali**, **Smart Card**, quindi fare clic sulla scheda **Amministrazione**.
   c. Controllare che sia selezionata l'opzione **Inizializza smart smart**.
   d. Immettere il PIN, fare clic su **Applica**, quindi seguire le istruzioni visualizzate.

      Dopo aver inizializzato la smart card, è necessario eseguirne la registrazione.

Registrazione della smart card

Dopo aver inizializzato la smart card, gli amministratori possono eseguirne la registrazione come metodo di autenticazione nella Console amministrativa di HP ProtectTools.

1. Fare clic su **Configurazione guidata**.
2. Nella **schermata di benvenuto**, fare clic su **Avanti**.
3. Immettere la propria password di Windows, quindi fare clic su **Avanti**.
4. Nella pagina **SpareKey**, fare clic su **Salta l'impostazione di SpareKey** (a meno che non si desideri aggiornare le informazioni relative alla SpareKey), quindi fare clic su **Avanti**.
5. Nella pagina **Attiva funzioni di protezione**, fare clic su **Avanti**.
6. Nella pagina **Scegliere le credenziali**, verificare che sia selezionata l'opzione **Smart card**, quindi fare clic su **Avanti**.
7. Nella pagina **Smart card**, immettere il PIN, quindi fare clic su **Avanti**.
8. Fare clic su **Fine**.

Gli utenti possono anche registrare la smart card nella Console utente di Security Manager. Per ulteriori informazioni consultare la guida del software Security Manager for HP ProtectTools, facendo clic sull'icona **?** blu in alto a destra della pagina per l'accesso tramite smart card.

Configurazione della smart card

Se il computer ha un lettore di smart card collegato o installato, la pagina Smart card presenterà due schede:

- **Impostazioni**—Selezionare la casella di controllo **Blocca computer alla rimozione della smart card**— per configurare il blocco automatico del computer alla rimozione di una smart card, quindi fare clic su **Applica**.

NOTA: il computer si bloccherà solo se la smart card è stata utilizzata come credenziale di autenticazione per l'accesso a Windows. La rimozione di una smart card non utilizzata per eseguire l'accesso a Windows non determinerà il blocco del computer.

- **Amministrazione**—Selezionare una delle seguenti opzioni:
  - **Inizializza la smart card**—Prepara una smart card all'utilizzo con HP ProtectTools. Se una smart card è stata inizializzata in precedenza al di fuori di HP ProtectTools (contiene una coppia di chiavi asimmetrica e un certificato associato), non è necessario eseguire di nuovo questa operazione, a meno che si desideri inizializzarla con un certificato specifico.
  - **Modifica PIN smart card**—Consente di modificare il PIN utilizzato con la smart card.
  - **Cancella soltanto i dati di HP ProtectTools**—Consente di cancellare soltanto il certificato di HP ProtectTools creato durante l'inizializzazione della scheda. Nessun altro dato viene cancellato dalla scheda.
  - **Cancella tutti i dati dalla smart card**—Consente di cancellare tutti i dati sulla smart card specificata. La scheda non può più essere utilizzata con HP ProtectTools o qualsiasi altra applicazione.

NOTA: Le funzioni che non sono supportate dalla smart card o altri dispositivi associati non sono disponibili.

▲ Fare clic su **Applica**.

Scheda senza contatti

La scheda senza contatti è una piccola scheda di plastica contenente un chip di computer. È possibile utilizzare una scheda senza contatti se al computer è collegato il lettore appropriato, se è stato installato il driver associato del relativo produttore e se è stata selezionata la scheda senza contatti come credenziale di autenticazione. In HP ProtectTools, sono supportati i seguenti tipi di schede senza contatti:

- Schede di memoria HID iCLASS senza contatti
- Schede di memoria MiFare Classic 1k, 4k e mini senza contatti

▲ Per impostare la scheda senza contatti, avvicinarla al lettore, seguire le istruzioni visualizzate, quindi fare clic su **Applica**.

Scheda di prossimità

La scheda di prossimità è una piccola scheda di plastica contenente un chip di computer. Se al computer è collegato un lettore di schede di prossimità, se è stato installato il driver associato del relativo produttore e se è stata selezionata la scheda di prossimità come credenziale di

autenticazione, è possibile utilizzare una scheda di prossimità insieme ad altre credenziali per protezione aggiuntiva.

▲ Per impostare la scheda di prossimità, avvicinarla al lettore, quindi fare clic su **Applica**.

Bluetooth

Se il computer è dotato della funzionalità Bluetooth,® se è stata selezionata come credenziale di autenticazione e se un telefono Bluetooth è abbinato con il computer, è possibile utilizzare il telefono Bluetooth insieme ad altre credenziali per protezione aggiuntiva. Specificare le impostazioni Bluetooth:

▲ Per consentire l'autenticazione automatica, selezionare la casella di controllo, quindi fare clic su **Applica**.

PIN

Se si è selezionato il PIN come credenziale di autenticazione, è possibile utilizzarne uno insieme ad altre credenziali per protezione aggiuntiva. Specificare le impostazioni del PIN:

1. Fare clic sulla freccia rivolta verso l'alto o il basso per selezionare la lunghezza minima del PIN.

   Il numero massimo di cifre consentito è 8.

2. Fare clic su **Applica**.

Applicazioni

La pagina Impostazioni di Applicazioni nel riquadro sinistro della Console amministrativa contiene due schede che consentono di personalizzare il comportamento delle applicazioni HP ProtectTools Security Manager attualmente installate.

▲ Nel riquadro sinistro della Console amministrativa, in **Applicazioni**, fare clic su **Impostazioni**.

Scheda Generale

Nella scheda **Generale**, sono disponibili le seguenti impostazioni:

- **Non avviare automaticamente l'impostazione guidata per gli amministratori**—Selezionare questa opzione per impedire l'apertura automatica della procedura guidata al momento dell'accesso.
- **Non avviare automaticamente l'introduzione guidata per gli utenti**—Selezionare questa opzione per impedire l'apertura automatica della configurazione utente al momento dell'accesso.

1. Selezionare o deselezionare le caselle di controllo corrispondenti alle specifiche impostazioni che si desidera abilitare o disabilitare.
2. Fare clic su **Applica**.

Scheda Applicazioni

Gli amministratori possono abilitare o disabilitare le seguenti applicazioni:

- **Stato**—Selezionare la casella di controllo per abilitare tutte le applicazioni oppure deselezionarla per disabilitarle tutte.
- **Password Manager**—Consente di attivare Password Manager per tutti gli utenti del computer.

1. Selezionare o deselezionare le caselle di controllo corrispondenti alle specifiche impostazioni che si desidera abilitare o disabilitare.
2. Fare clic su **Applica**.

Per ripristinare le impostazioni predefinite delle applicazioni, fare clic su **Ripristina impostazioni predefinite**.

Dati

La sezione Dati del riquadro sinistro della Console amministrativa consente di configurare le impostazioni per le seguenti applicazioni:

- **Drive Encryption**—Consente di configurare le impostazioni e di visualizzare lo stato delle unità. Per ulteriori informazioni consultare la guida del software Drive Encryption, facendo clic sull'icona **?** blu in alto a destra della pagina Drive Encryption.

Computer

La sezione Computer del riquadro sinistro della Console amministrativa consente di configurare le impostazioni per l'applicazione Device Access Manager:

- Configurazione semplice
- Configurazione delle classi di periferiche
- Configurazione dell'autenticazione Just-in-Time (JITA)
- Impostazioni avanzate

Per ulteriori informazioni, consultare la guida del software Device Access Manager, facendo clic sull'icona **?** blu in alto a destra della pagina Device Access Manager.

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager consente di aumentare sensibilmente la protezione del computer.

È possibile utilizzare le applicazioni di Security Manager preinstallate, nonché le applicazioni aggiuntive disponibili per il download immediato dal Web:

- Gestione dell'accesso e delle password.
- Modifica semplificata della password del sistema operativo Windows®.
- Impostazione delle preferenze di programma.
- Utilizzo delle impronte digitali per maggior protezione e praticità.
- Registrazione di una o più scene per l'autenticazione.
- Configurazione di una smart card per l'autenticazione.
- Backup e ripristino dei dati di programma.
- Aggiunta di applicazioni.

Avvio di Security Manager

Security Manager può essere aperto in uno dei seguenti modi:

▲ Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.

– oppure –

Da **Pannello di controllo**, selezionare **Sistema e sicurezza**, poi **HP ProtectTools Security Manager**.

Utilizzare la Console utente Security Manager

La Console utente di Security Manager è la posizione centrale da cui si accede facilmente alle funzioni, alle applicazioni e alle impostazioni di Security Manager. La Console utente mostra i seguenti componenti:

- **ID Card**—Visualizza il nome utente Windows e l'icona che identifica l'utente che ha effettuato l'accesso.
- **Applicazioni di protezione**—Visualizza un menu espandibile di collegamenti per la configurazione delle seguenti categorie di protezione:
  - **Home**—Consente di gestire le password, impostare le credenziali di autenticazione e verificare lo stato delle applicazioni di protezione.
  - **Ritrovamento di PC rubati**—Computrace for HP ProtectTools (da acquistare separatamente)
- **Accessi personali**—Consente di gestire le credenziali di autenticazione con Password Manager e Credential Manager.

- **My Data**— (Miei dati) Consente di gestire la protezione dei dati con Drive Encryption e File Sanitizer.

NOTA: Questo elemento non viene visualizzato se l'applicazione non è installata.

- **My Computer**— (Mio computer) Consente di gestire la protezione del computer in uso con Device Access Manager.

NOTA: Questo elemento non viene visualizzato se l'applicazione non è installata.

- **Amministrazione**—Consente agli amministratori di accedere alla **Console amministrativa** per gestire la protezione e gli utenti.
- **Avanzate**—Vsualizza i comandi di accesso ad ulteriori funzionalità, tra cui:
  - **Preferenze**—Consente di personalizzare le impostazioni di Security Manager.
  - **Backup e ripristino**—Consente di eseguire il backup o il ripristino dei dati.
  - **Informazioni su**—Visualizza le informazioni su HP ProtectTools Security Manager, ad esempio il numero di versione e l'informativa sul copyright.
- **Area principale**—Visualizza le schermate specifiche dell'applicazione.
- **?**—Visualizza la Guida della Console utente di Security Manager. Questa icona si trova nell'angolo superiore destro della finestra, accanto alle icone per la riduzione e l'ingrandimento.

Scheda ID personale

La scheda ID identifica in modo univoco l'utente come proprietario dell'account Windows, mostrandone il nome e un'immagine di sua scelta. Viene visualizzata in modo prominente nell'angolo superiore sinistro delle pagine di Security Manager.

È possibile modificare l'immagine e il modo in cui viene visualizzato il nome. Per impostazione predefinita, vengono mostrati il nome utente di Windows completo e l'immagine selezionata durante la configurazione di Windows.

Per modificare il nome visualizzato:

1. Aprire la Console utente di Security Manager. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
2. Fare clic sulla scheda ID nell'angolo superiore sinistro della Console utente.
3. Fare clic nella casella che visualizza il nome utente Windows per l'account in uso, digitare il nuovo nome quindi fare clic su **Salva**.

My Logons (Miei accessi)

Le applicazioni incluse in questo gruppo assistono l'utente nella gestione di diversi aspetti della sua identità digitale.

- **Password Manager**—Consente di creare e gestire i collegamenti rapidi tramite cui eseguire l'avvio e l'accesso ai siti Web e ai programmi mediante l'autenticazione della password di Windows, l'impronta digitale, una smart card, una scheda di prossimità o senza contatti, un telefono Bluetooth o un PIN.
- **Credential Manager**—Consente di modificare facilmente la password di Windows, registrare le impronte digitali e le scene del viso, configurare una smart card, una scheda senza contatti o di prossimità, un telefono Bluetooth o un PIN.

Gli amministratori possono accedere alle informazioni relative alle applicazioni di protezione aggiuntiva disponibili facendo clic su **Amministrazione**, quindi su **Gestione centrale** nell'angolo inferiore sinistro del dashboard.

Password Manager

Accedere a Windows, ai siti Web e alle applicazioni è più semplice e sicuro quando si utilizza Password Manager. È possibile utilizzare questo programma per creare password più sicure che non richiedono di essere memorizzate o annotate, quindi accedere facilmente e velocemente autenticandosi tramite impronta digitale, riconoscimento del viso, smart card, scheda di prossimità o senza contatti, PIN o password di Windows.

Password Manager offre le seguenti opzioni:

Scheda Gestisci

- Aggiunta, modifica o eliminazione degli accessi.
- Utilizzo dei collegamenti rapidi per avviare il browser predefinito e accedere a qualsiasi sito Web o programma una volta impostato.
- Trascinamento della selezione per organizzare i collegamenti rapidi in categorie.
- Visualizzazione rapida delle eventuali password che presentano un rischio per la protezione.

Scheda Complessità password

- Controllare la complessità delle singole password utilizzate per i siti Web e le applicazioni, nonché la complessità generale della password.
- La complessità della password è illustrata da indicatori di stato di color rosso, giallo o verde.

L'icona del programma **Password Manager** è visualizzata nell'angolo superiore sinistro di una pagina Web o della schermata di accesso a un'applicazione. Quando occorre ancora configurare l'accesso a tale sito Web o applicazione, l'icona riporta il segno +.

▲ Fare clic sull'icona di **Password Manager** per visualizzare un menu contestuale da cui è possibile scegliere le opzioni riportate di seguito:

- Aggiungi [qualchedominio.com] a Password Manager
- Apri Password Manager
- Impostazioni icone
- Assistenza

Per pagine Web o programmi senza accesso disponibile

Nel menu contestuale vengono visualizzate le seguenti opzioni:

- **Aggiungi [qualchedominio.com] a Password Manager**—Consente di aggiungere un accesso alla schermata di accesso corrente.
- **Apri Password Manager**—Avvia Password Manager.
- **Impostazioni icona**—Consente di specificare quali condizioni determinano la visualizzazione dell'icona di **Password Manager**.
- **Guida**—Visualizza la Guida di Security Manager.

Per pagine Web o programmi con accesso disponibile

Nel menu contestuale vengono visualizzate le seguenti opzioni:

- **Immetti i dati di accesso**—Visualizza una pagina per la verifica dell'identità. Se l'autenticazione viene eseguita correttamente, i dati di accesso vengono immessi negli appositi campi e la pagina viene inviata (se l'invio è stato specificato al momento della creazione dell'accesso o della sua ultima modifica).
- **Modifica accesso**—Consente di modificare i dati di accesso al sito Web.
- **Aggiungi accesso**—Consente di aggiungere un account a Password Manager.
- **Apri Password Manager**—Avvia Password Manager.
- **Guida**—Visualizza la Guida di Security Manager.

NOTA: l'amministratore di questo computer potrebbe avere impostato Security Manager affinché richieda più di una credenziale durante la verifica dell'identità.

Aggiunta di accessi

È possibile aggiungere facilmente un accesso a un sito Web o programma immettendo i dati di accesso una volta, dopodiché la loro immissione avverrà in modo automatico. È possibile riutilizzare questi accessi dopo la navigazione al sito Web o al programma, altrimenti è possibile selezionare la voce desiderata nel menu **Collegamenti rapidi Password Manager** affinché Password Manager esegua l'accesso automatico dell'utente al sito Web o al programma.

Per aggiungere un accesso:

1. Aprire la schermata di accesso a un sito Web o programma.
2. Fare clic sulla freccia dell'icona **Password Manager**, quindi fare clic su una delle seguenti opzioni a seconda che la schermata di accesso sia relativa a un sito Web o a un programma:
   - Per un sito Web, fare clic su **Aggiungi [nome dominio] a Password Manager**.
   - Per un programma, fare clic su **Aggiungi schermata accesso a Password Manager**.
3. Immettere i dati di accesso. I campi di accesso nella schermata e i campi corrispondenti nella finestra di dialogo sono identificati con un bordo arancione in grassetto. È inoltre possibile visualizzare questa finestra di dialogo facendo clic su **Aggiungi accesso** dalla scheda **Gestisci Password Manager**, utilizzando ctrl+tasto logo di Windows+h o passando il dito.
   a. Per compilare un campo di accesso con una delle opzioni preformattate, fare clic sulle frecce a destra del campo.
   b. Per visualizzare la password di accesso, fare clic su **Mostra password**.

c. Per compilare i campi di accesso, ma non inviarli, deselezionare la casella di controllo **Invia automaticamente i dati di accesso**.

d. Fare clic su **OK** per selezionare il metodo di autenticazione desiderato (impronte digitali, riconoscimento del viso, smart card, scheda di prossimità o senza contatti, telefono Bluetooth, PIN o password), quindi eseguire l'accesso con tale metodo.

   Il segno "+" viene rimosso dall'icona di **Password Manager** per indicare che l'accesso è stato creato.

e. Se Password Manager non rileva i campi di accesso, fare clic su **Altri campi**.

   - Selezionare la casella di controllo di ciascun campo obbligatorio per l'accesso oppure deselezionarla per eventuali campi facoltativi.
   - Fare clic su **Chiudi**.

Ogni volta che si accede a tale sito Web o programma, viene visualizzata l'icona **Password Manager** nell'angolo superiore sinistro della relativa schermata di accesso, per indicare che è consentito l'accesso con le credenziali registrate.

Modifica degli accessi

Per modificare un accesso, procedere come segue:

1. Aprire la schermata di accesso a un sito Web o programma.
2. Per visualizzare una finestra di dialogo in cui è possibile modificare i dati di accesso, fare clic sulla freccia dell'icona **Password Manager**, quindi fare clic su **Modifica accesso**. I campi di accesso nella schermata e i campi corrispondenti nella finestra di dialogo sono identificati con un bordo arancione in grassetto.

   È possibile inoltre visualizzare questa finestra di dialogo facendo clic su **Modifica per accesso desiderato** nella scheda **Gestisci** di **Password Manager**.
3. Modificare le informazioni di accesso.

   - Per compilare un campo di accesso **Nome utente** con una delle scelte preformattate, fare clic sulla freccia in giù a destra del campo.
   - Per compilare un campo di accesso **Password** con una delle scelte preformattate, fare clic sulla freccia in giù a destra del campo.
   - Per aggiungere altri campi dalla schermata all'accesso, fare clic su **Altri campi**.
   - Per visualizzare la password di accesso, fare clic su **Mostra password**.
   - Per compilare i campi di accesso, ma non inviarli, deselezionare la casella di controllo **Invia automaticamente i dati di accesso**.
4. Fare clic su **OK**.

Utilizzo del menu Collegamenti rapidi Password Manager

Password Manager offre un modo semplice e veloce per avviare i siti Web e i programmi per i quali sono stati creati gli accessi. Fare doppio clic in corrispondenza dell'accesso a un programma o a un sito Web dal menu **Collegamenti rapidi Password Manager** oppure dalla scheda **Gestisci** in Password Manager per aprire la schermata in cui immettere i dati di accesso.

Quando si crea un accesso, questo viene automaticamente aggiunto al menu **Collegamenti rapidi** di Password Manager.

Per visualizzare il menu **Collegamenti rapidi**, procedere come segue:

1. Premere la combinazione di tasti di scelta rapida per **Password Manager** (ctrl+tasto del logo Windows+h è la combinazione predefinita). Per cambiare la combinazione di tasti, nella Console utente di Security Manager fare clic su **Password Manager**, quindi su **Impostazioni**.
2. Eseguire la scansione dell'impronta digitale (sui computer con un lettore di impronte digitali integrato o collegato) oppure immettere la password Windows.

Organizzazione degli accessi in categorie

Creare una o più categorie per mantenere in ordine gli accessi. Quindi, trascinare e rilasciare gli accessi nelle categorie desiderate.

Per aggiungere una categoria:

1. Dalla Console utente di Security Manager, fare clic su **Password Manager**.
2. Fare clic sulla scheda **Gestisci**, quindi su **Aggiungi categoria**.
3. Inserire un nome per la categoria.
4. Fare clic su **OK**.

Per aggiungere un accesso a una categoria:

1. Posizionare il puntatore del mouse sull'accesso desiderato.
2. Tenere premuto il pulsante sinistro del mouse.
3. Trascinare l'accesso nell'elenco di categorie. Le categorie vengono evidenziate quando si posiziona il puntatore del mouse su di esse.
4. Rilasciare il pulsante del mouse quando viene evidenziata la categoria desiderata.

Gli accessi non vengono spostati ma solo copiati nella categoria selezionata. È possibile aggiungere lo stesso accesso a più categorie ed è possibile visualizzare tutti gli accessi facendo clic su **Tutti**.

Gestione degli accessi

Password Manager semplifica la gestione delle informazioni di accesso per i nomi utente, le password e gli account di accesso multipli da una posizione centrale.

Gli accessi vengono elencati nella scheda **Gestisci**. Se sono stati creati più accessi per lo stesso sito Web, tutti vengono riportati in corrispondenza del nome del sito Web e inclusi nell'elenco degli accessi.

Per gestire gli accessi:

▲ Dalla Console utente di Security Manager, fare clic su **Password Manager**, quindi selezionare la scheda **Gestisci**.

- **Aggiungi un accesso**—Fare clic su **Aggiungi accesso** e seguire le istruzioni visualizzate.
- **Accessi personali**—Fare clic su un accesso esistente, selezionare una delle seguenti opzioni, quindi seguire le istruzioni visualizzate:
  - **Apri**—Apre un sito web o un programma per cui è stato impostato un login.
  - **Aggiungi**—Aggiunge un accesso. Per ulteriori informazioni, vedere Aggiunta di accessi a pagina 28.

- **Modifica**—Modifica un accesso. Per ulteriori informazioni, vedere Modifica degli accessi a pagina 29.
- **Apri**—Apre un sito web o un programma per cui è stato impostato un login.

- **Aggiungi categoria**—Fare clic su **Aggiungi categoria**, quindi seguire le istruzioni visualizzate. Per ulteriori informazioni, vedere Organizzazione degli accessi in categorie a pagina 30.

Per aggiungere un altro accesso per un sito Web o un programma:

1. Aprire la schermata di accesso al sito Web o programma.
2. Fare clic sull'icona **Password Manager** per visualizzare il relativo menu contestuale.
3. Fare clic su **Aggiungi ad accesso**, quindi seguire le istruzioni visualizzate.

Verifica della complessità della password

L'utilizzo di password complesse per l'accesso ai siti Web e ai programmi è un aspetto importante della protezione dell'identità personale.

Password Manager semplifica il monitoraggio e il miglioramento del livello di protezione grazie all'analisi immediata e automatica della complessità di tutte le password utilizzate per accedere ai siti Web e ai programmi.

Nella scheda **Complessità password**, gli indicatori di stato di color rosso, giallo o verde segnalano la complessità di ciascuna password utilizzata per i siti Web e le applicazioni, nonché la complessità generale della password.

Impostazioni dell'icona di Gestore password

Password Manager esegue l'identificazione delle schermate di accesso ai siti Web e programmi. Quando rileva una schermata che non dispone di un accesso, **Password Manager** la contrassegna aggiungendo alla propria icona il segno "+" per indicare che occorre crearne uno.

1. Fare clic sull'icona, quindi fare clic su **Impostazioni icona** per personalizzare il modo in cui Password Manager gestisce i possibili siti di accesso.
   - **Richiedi l'aggiunta di accessi per le schermate di accesso**—Fare clic su questa opzione se si desidera che Password Manager richieda di aggiungere una voce quando viene visualizzata una schermata per la quale non è stato ancora configurato un accesso.
   - **Escludi questa schermata**—Selezionare questa casella di controllo se non si desidera che Password Manager richieda di nuovo di aggiungere un accesso per questa schermata.

     Per aggiungere un accesso per una schermata esclusa in precedenza, procedere come segue:

     - Durante la visualizzazione della pagina di accesso al sito Web o del programma escluso in precedenza, aprire la Console utente di Security Manager, quindi fare clic su **Password Manager**.
     - Fare clic su **Aggiungi accesso**.

       Si apre la finestra di dialogo Aggiungi accesso in cui è presente il campo **Schermata corrente** che riporta in elenco la schermata di accesso al sito Web oppure il programma.
     - Fare clic su **Continua**.

       Viene visualizzata la schermata Aggiungi accesso a Password Manager.

- Seguire le istruzioni visualizzate. Per ulteriori informazioni, vedere Aggiunta di accessi a pagina 28.
- Ogni volta che si apre la schermata di accesso al sito Web o al programma, viene visualizzata l'icona di **Password Manager**.

Non richiedere l'aggiunta di accessi per la schermata di accesso—Selezionare il pulsante di opzione.

2. Per accedere alle altre impostazioni di Password Manager, fare clic su **Password Manager**, quindi su **Impostazioni** nella Console utente di Security Manager.

Impostazioni

È possibile specificare le impostazioni per la personalizzazione di Password Manager:

1. **Richiedi di aggiungere gli accessi per le schermate di accesso**—L'icona di **Password Manager** con il segno "+" viene visualizzata ogni volta che viene rilevata una schermata di accesso di un sito Web o di un programma. Ciò indica che è possibile aggiungere un accesso per tale schermata nel menu **Accessi**. Per disabilitare questa funzione, deselezionare la casella di controllo accanto a **Richiedi di aggiungere gli accessi per le schermate di accesso**.
2. **Apri Password Manager con ctrl+win+h**—La combinazione predefinita di tasti di scelta rapida che apre il menu **Collegamenti rapidi Password Manager** è ctrl+tasto logo di Windows+h. Per modificarla, fare clic su questa opzione e immettere una nuova combinazione. Le combinazioni possono includere uno o più tasti seguenti: ctrl, alt o maiusc e qualsiasi tasto alfabetico o numerico.
3. Per salvare le modifiche apportate, fare clic su **Applica**.

Credential Manager

Utilizzare le credenziali Security Manager per verificare la propria identità. L'amministratore del computer in uso può impostare le credenziali da utilizzare per verificare l'identità durante l'accesso all'account Windows, ai siti Web o ai programmi.

Le credenziali disponibili possono variare in base ai dispositivi di protezione integrati o collegati al computer in uso. Le credenziali supportate, i requisiti e lo stato attuale sono visualizzati quando si fa clic su **Credential Manager** in **My Logons** (Miei accessi). I dati disponibili possono essere i seguenti:

- Password
- SpareKey
- Impronte digitali
- Viso
- Smart card
- Scheda senza contatti
- Scheda di prossimità
- Bluetooth
- PIN

Per registrare o modificare una credenziale, fare clic sul collegamento e seguire le istruzioni visualizzate.

Modifica della password di Windows

La procedura di modifica della password con Security Manager è più semplice e veloce rispetto a quando la si esegue nel Pannello di controllo di Windows.

Per modificare la password di Windows, procedere come segue:

1. Dalla Console utente di Security Manager, fare clic su **Credential Manager**, quindi su **Password**.
2. Immettere la password corrente nella casella di testo **Password di Windows corrente**.
3. Digitare la nuova password nella casella di testo **Nuova password di Windows**, quindi immetterla di nuovo nella casella di testo **Conferma nuova password**.
4. Fare clic su **Modifica** per sostituire immediatamente la password corrente con quella nuova appena immessa.

Impostazione della SpareKey

La SpareKey consente di accedere al computer in uso (su piattaforme supportate) fornendo la risposta alle tre domande per la protezione riportate in un elenco che l'amministratore ha definito in precedenza.

HP ProtectTools Security Manager richiede di configurare la SpareKey personale durante l'installazione guidata di HP ProtectTools Security Manager.

Per configurare la SpareKey, procedere come segue:

1. Nella pagina SpareKey della procedura guidata selezionare le tre domande di protezione, quindi immettere la risposta per ciascuna risposta.
2. Fare clic su **Crea**.

È possibile selezionare domande diverse oppure cambiare le risposte nella pagina SpareKey in **Credential Manager**.

Una volta configurata la SpareKey, è possibile utilizzarla per accedere al computer dalla schermata di accesso di preavvio oppure dalla schermata di benvenuto di Windows.

Registrazione delle impronte digitali

Se l'amministratore ha selezionato le impronte digitali nella schermata **Scegliere le credenziali** e se il computer in uso ha un lettore di impronte digitali integrato o collegato, l'installazione guidata di HP ProtectTools Security Manager includerà tutti i passaggi per l'impostazione o la "registrazione" delle impronte digitali: È anche possibile registrare le impronte digitali nell'apposita pagina Impronte digitali in **Credential Manager** nella Console utente di Security Manager.

1. Nella pagina Impronte digitali della procedura guidata, viene visualizzata una sagoma con due mani. Le dita che sono state già registrate sono evidenziate. Fare clic su un dito della sagoma.

NOTA: per eliminare un'impronta digitale registrata in precedenza, fare clic sul dito corrispondente.

2. Viene richiesto di passare il dito finché l'impronta digitale corrispondente non risulta registrata correttamente. Un dito registrato viene evidenziato nella sagoma.
3. È necessario registrare almeno due dita, preferibilmente l'indice o il medio. Ripetere i passaggi 1 e 2 per un altro dito.
4. Fare clic su **Avanti**, quindi seguire le istruzioni visualizzate.

ATTENZIONE: quando si registrano le impronte digitali tramite la procedura guidata, le relative informazioni non vengono salvate fino a quando non si fa clic su **Avanti**. Se si lascia il computer inattivo per qualche tempo o si chiude il programma, le modifiche apportate **non** verranno salvate.

Registrazione di scene per l'accesso tramite riconoscimento del viso

Se si sceglie l'accesso tramite il riconoscimento del viso e il computer in uso ha una webcam integrata o collegata, l'installazione guidata di HP ProtectTools Security Manager richiede di eseguire la registrazione delle scene. È anche possibile registrare le scene nell'apposita pagina per l'accesso tramite il riconoscimento del viso presente in **Credential Manager** nella Console utente di Security Manager.

È necessario registrare una o più scene per poter utilizzare l'accesso tramite il riconoscimento del viso. Dopo aver eseguito la registrazione, è anche possibile registrare una nuova scena se si sono riscontrate difficoltà durante l'accesso, perché una o più delle seguenti condizioni sono cambiate:

- L'aspetto del viso dell'utente è cambiato in modo significativo dall'ultima registrazione.
- La luce è molto diversa da quella delle registrazioni precedenti.
- Durante l'ultima registrazione si indossavano o non si indossavano gli occhiali.

NOTA: nel caso di difficoltà con la registrazione delle scene, provare ad avvicinare la webcam.

Per registrare una nuova scena dall'installazione guidata di HP ProtectTools Security Manager, procedere come indicato di seguito:

1. Nella pagina di accesso tramite il riconoscimento del viso della procedura guidata, fare clic su **Avanzate**, quindi configurare le opzioni aggiuntive. Per ulteriori informazioni, vedere Impostazioni utente avanzate a pagina 36.
2. Fare clic su **OK**.
3. Fare clic su **Avvia**, altrimenti se sono già state registrate delle scene, fare clic su **Registra una nuova scena**.
4. Durante la registrazione della scena è possibile guardare una dimostrazione facendo clic su **Riproduci video**.

   Se si tratta della registrazione iniziale, viene visualizzata una finestra di dialogo in cui viene chiesto se si desidera guardare un video dimostrativo. Fare clic su **Sì** o su **No**.
5. In condizioni di luce scarsa, il software regola la luminosità dello schermo automaticamente oppure è possibile modificare la luce di sfondo facendo clic sull'icona della **lampadina blu**.
6. Fare clic sull'icona **Camera** (Fotocamera), quindi seguire le istruzioni visualizzate per registrare la scena.

   NOTA: durante la fase di acquisizione delle scene, non distogliere gli occhi dalla propria immagine.
7. Fare clic su **Avanti**.

È anche possibile registrare le scene dalla Console utente di Security Manager:

1. Aprire la Console utente di Security Manager. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
2. In **My Logons** (Miei accessi) fare clic su **Credential Manager**, quindi su **Face** (Viso).
3. Fare clic su **Avanzate**, quindi configurare le opzioni aggiuntive. Per ulteriori informazioni, vedere Impostazioni utente avanzate a pagina 36.

4. Fare clic su **OK**.
5. Fare clic su **Avvia**, altrimenti se sono già state registrate delle scene, fare clic su **Registra una nuova scena**.
6. Se viene richiesto di immettere la password di Windows, immetterla, quindi fare clic su **Avanti**.
7. Durante la registrazione della scena è possibile guardare una dimostrazione facendo clic su **Riproduci video**.

   Se si tratta della registrazione iniziale, viene visualizzata una finestra di dialogo in cui viene chiesto se si desidera guardare un video dimostrativo. Fare clic su **Sì** o su **No**.
8. In condizioni di luce scarsa, il software regola la luminosità dello schermo automaticamente oppure è possibile modificare la luce di sfondo facendo clic sull'icona della **lampadina blu**.
9. Fare clic sull'icona **Camera** (Fotocamera), quindi seguire le istruzioni visualizzate per registrare la scena.

NOTA: durante la fase di acquisizione delle scene, non distogliere gli occhi dalla propria immagine.

Per ulteriori informazioni, consultare la guida del software Face Recognition, facendo clic sull'icona **?** blu nella parte superiore destra della pagina di registrazione delle scene del viso.

Autenticazione

Dopo aver registrato una o più scene, l'utente può utilizzare il viso per l'autenticazione quando accede al computer o avvia una nuova sessione di Windows.

1. Quando viene avviata la schermata di autenticazione e viene rilevato il viso dell'utente, si hanno a disposizione 5 secondi per iniziare la procedura di accesso. Se il viso viene autenticato correttamente, è possibile accedere al computer.
2. Allo scadere del tempo a disposizione per l'accesso tramite il riconoscimento del viso, Face Recognition viene messo in pausa. Fare clic sull'icona della **fotocamera** per ripristinare la procedura di autenticazione.

NOTA: se l'illuminazione non è sufficiente e non si è in grado di eseguire l'accesso utilizzando Face Recognition, è possibile immettere la password di Windows per accedere al computer.

3. Una volta eseguito l'accesso al computer, se Face Recognition richiede di aggiungere nuove scene per aumentare le probabilità di accesso durante le sessioni future, fare clic su **Sì**.

Modalità scura

Se il processo di accesso tramite il riconoscimento del viso avviene in condizioni di luce troppo scura, viene automaticamente utilizzata una schermata bianca come sfondo, che illumina meglio il viso dell'utente.

Per cambiare il colore dello sfondo in modo manuale, fare clic sull'icona della **lampadina blu**.

Informazioni

Se l'accesso tramite il riconoscimento del viso ha esito negativo ma si immette la password correttamente, viene richiesto di salvare una serie di immagini per aumentare le probabilità di accesso tramite il riconoscimento del viso in futuro.

Eliminazione di una scena

Per eliminare una scena attualmente registrata:

1. Aprire la Console utente di Security Manager. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
2. In **Miei accessi**, fare clic su **Credential Manager**, quindi su **Viso**.
3. Fare clic sulla scena da eliminare, quindi sull'icona del **cestino**.
4. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **OK**.

Impostazioni utente avanzate

1. Aprire la Console utente di Security Manager. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
2. In **My Logons** (Miei accessi) fare clic su **Credential Manager**, quindi su **Face** (Viso).
3. Fare clic su **Avanzate** per configurare le seguenti opzioni:

   Scheda **Altre impostazioni**—Selezionare o deselezionare le caselle di controllo corrispondenti a una o più opzioni che si desidera abilitare o disabilitare. Queste impostazioni risultano valide solo per l'utente corrente.

   - **Riproduci un suono in corrispondenza di eventi di riconoscimento del viso**—Viene riprodotto un suono quando il riconoscimento del viso viene completato, con esito sia positivo che negativo.
   - **Richiedi l'aggiornamento delle scene quando l'accesso non riesce**—Se l'accesso tramite il riconoscimento del viso ha esito negativo ma la password viene digitata correttamente, all'utente viene richiesto di salvare una serie di immagini acquisite per aumentare le probabilità di accesso tramite riconoscimento del viso la volta successiva.
   - **Richiedi la registrazione di una nuova scena quando l'accesso non riesce**—Se l'accesso tramite il riconoscimento del viso ha esito negativo ma la password viene digitata correttamente, può essere richiesto di registrare una nuova scena per aumentare le probabilità di accesso tramite riconoscimento del viso la volta successiva.
4. Per ripristinare i valori originali delle impostazioni, fare clic su **Ripristina impostazioni predefinite**.
5. Fare clic su **OK**.

Configurazione di una smart card

Se un lettore di smart card è integrato o collegato al computer in uso, se l'amministratore ha abilitato una smart card come credenziale di autenticazione ed eseguito i passaggi descritti nella Guida di Console amministrativa di HP ProtectTools, la procedura di installazione guidata di HP ProtectTools Security Manager richiederà di inserire e impostare una smart card. È anche possibile configurare la smart card nell'apposita pagina di **Credential Manager** nella Console utente di Security Manager.

NOTA: Per poter essere utilizzata, la smart card deve essere prima inizializzata dagli amministratori.

Inizializzazione della smart card

HP ProtectTools Security Manager supporta un certo numero di smart card diverse. Il numero e il tipo di caratteri usati come numeri PIN possono variare. Il produttore della smart card in genere fornisce

gli strumenti necessari per l'installazione di un certificato di protezione e la gestione del PIN che HP ProtectTools userà nei suoi algoritmi di protezione.

Gli amministratori possono inizializzare la smart card utilizzando il software del produttore e la Console amministrativa di HP ProtectTools. Per ulteriori informazioni, vedere la Guida del software della Console amministrativa di HP ProtectTools.

Registrazione della smart card

Dopo aver inizializzato la smart card, gli utenti possono registrarla in Security Manager:

1. Aprire la Console utente di Security Manager. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
2. Fare clic su **Credential Manager**, quindi su **Smart card**.
3. Controllare che sia selezionata l'opzione **Imposta**.
4. Immettere la password di Windows e il PIN, quindi fare clic su **Salva**.

Per registrare le scene, gli amministratori possono anche utilizzare l'impostazione guidata della Console amministrativa di HP ProtectTools. Per ulteriori informazioni, vedere la Guida del software della Console amministrativa di HP ProtectTools.

Modifica del PIN della smart card

Per cambiare il codice PIN della smart card, procedere come segue:

1. Inserire una smart card già formattata e inizializzata.
2. Selezionare **Modifica il PIN della smart card**.
3. Immettere il PIN precedente, quindi immettere e confermare un nuovo PIN.

Scheda senza contatti

La scheda senza contatti è una piccola scheda di plastica contenente un chip di computer. È possibile utilizzare una scheda senza contatti se al computer è collegato il lettore appropriato, se l'amministratore ha installato il driver associato del relativo produttore e se ha selezionato la scheda senza contatti come credenziale di autenticazione. In HP ProtectTools, sono supportati i seguenti tipi di schede senza contatti:

- Schede di memoria HID iCLASS senza contatti
- Schede di memoria MiFare Classic 1k, 4k e mini senza contatti

▲ Per impostare la scheda senza contatti, avvicinarla al lettore, seguire le istruzioni visualizzate, quindi fare clic su **Applica**.

Scheda di prossimità

La scheda di prossimità è una piccola scheda di plastica contenente un chip di computer. Se al computer è collegato un lettore di schede di prossimità, se l'amministratore ha installato il driver associato del relativo produttore e se ha selezionato la scheda di prossimità come credenziale di autenticazione, è possibile utilizzare la scheda di prossimità insieme ad altre credenziali per protezione aggiuntiva.

▲ Per impostare la scheda senza contatti, avvicinarla al lettore, seguire le istruzioni visualizzate, quindi fare clic su **Applica**.

Bluetooth

Se l'amministratore ha abilitato Bluetooth come credenziale di autenticazione, è possibile impostare un telefono Bluetooth da utilizzare con altre credenziali per protezione aggiuntiva.

NOTA: sono supportati soltanto i telefoni Bluetooth.

1. Verificare che la funzionalità Bluetooth sia abilitata nel computer e che il telefono Bluetooth sia impostato sulla modalità di individuazione. Per collegare il telefono, è possibile che venga richiesto di digitare un codice generato automaticamente nel dispositivo Bluetooth. Se il dispositivo Bluetooth è configurato per il confronto dei codici di abbinamento tra il computer e il telefono, sarà richiesto di eseguire tale operazione.
2. Per eseguire la registrazione del telefono, selezionarlo e fare clic su **Registra**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **OK**.

PIN

Se l'amministratore ha abilitato il PIN come credenziale di autenticazione, è possibile impostare un PIN da utilizzare insieme ad altre credenziali per protezione aggiuntiva.

▲ Per impostare un nuovo PIN, immetterlo e confermarlo digitandolo nuovamente.

Amministrazione

Gli amministratori possono accedere alla Console amministrativa e Gestione centrale facendo clic su **Amministrazione**, poi selezionando **Console amministrativa** nel riquadro in basso a sinistra della Console utente di HP ProtectTools Security Manager.

Per ulteriori informazioni, vedere la Guida del software della Console amministrativa di HP ProtectTools.

Avanzate

È possibile accedere alle seguenti opzioni facendo clic su **Avanzate** nel riquadro inferiore sinistro della Console utente:

- **Preferenze**—Consente di personalizzare le impostazioni di Security Manager.
- **Backup e ripristino**—Consente di eseguire il backup e il ripristino dei dati.
- **Informazioni su**—Consente di visualizzare le informazioni sulla versione di Security Manager.

Impostazione delle preferenze

È possibile personalizzare le impostazioni di HP ProtectTools Security Manager. Dalla Console utente di Security Manager, fare clic su **Avanzate**, quindi su **Preferenze**. Le impostazioni disponibili vengono visualizzate in due schede: **Generale** e **Impronte digitali**.

Scheda Generale

Aspetto—Mostra l'icona nell'area di notifica della barra delle applicazioni

- Per abilitare la visualizzazione dell'icona nella barra delle applicazioni, selezionare la casella di controllo.
- Per disabilitare la visualizzazione dell'icona nella barra delle applicazioni, deselezionare la casella di controllo.

Scheda Impronta digitale

NOTA: la scheda **Impronta digitale** è disponibile solo se al computer è collegato un apposito lettore con il relativo driver installato.

- **Azioni rapide**—Consente di selezionare l'attività di Security Manager che deve essere eseguita quando si preme un tasto designato durante la scansione dell'impronta digitale.

  Per assegnare un'azione rapida a uno dei tasti elencati, fare clic sull'opzione **(Tasto)+Impronta digitale**, quindi selezionare una delle attività disponibili nel menu.

- **Feedback scansione impronte digitali**—Viene visualizzata solo quando è disponibile un lettore di impronte digitali. Utilizzare questa impostazione per modificare il feedback ottenuto quando si esegue la scansione dell'impronta digitale.

  - **Attiva feedback audio**—Quando è stata eseguita la scansione di un'impronta digitale, in Security Manager viene riprodotto un feedback audio con suoni diversi in corrispondenza di eventi di programma specifici. È possibile assegnare nuovi suoni a questi eventi tramite la scheda **Suoni** nel Pannello di controllo di Windows oppure disabilitare il feedback audio deselezionando questa opzione.

  - **Mostra il feedback sulla qualità della scansione**

    Selezionare la casella di controllo per visualizzare tutte le scansioni, a prescindere dalla qualità.

    Deselezionare la casella di controllo per visualizzare solo le scansioni di buona qualità.

Backup e ripristino dei dati

Si consiglia di eseguire backup regolari dei dati di Security Manager. La frequenza dei backup dipende dalla frequenza con cui si modificano i dati. Ad esempio, se ogni giorno si aggiungono nuovi accessi, è consigliabile eseguire questa operazione quotidianamente.

I backup possono anche essere utilizzati per eseguire le importazioni e le esportazioni tra un computer e l'altro.

NOTA: Questa funzione esegue il backup delle sole informazioni relative a Password Manager e Face Recognition. Drive Encryption ha un metodo di backup indipendente. Non viene eseguito il backup delle informazioni di autenticazione tramite impronte digitali e di Device Access Manager.

È necessario che HP ProtectTools Security Manager sia installato sui computer di destinazione dei dati di backup prima che questi possano essere ripristinati dal relativo file.

Per eseguire il backup dei dati:

1. Aprire la Console utente di Security Manager. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
2. Nel riquadro sinistro della Console utente, fare clic su **Avanzate**, quindi su **Backup e ripristino**.
3. Fare clic su **Backup dei dati**.
4. Selezionare i moduli da includere nel backup. In genere, si selezionano tutti i moduli.
5. Verificare l'identità.
6. Inserire un nome per il file di archiviazione. Per impostazione predefinita, il file viene salvato nella cartella Documenti. Fare clic su **Sfoglia** per specificare un'altra cartella.
7. Immettere una password per proteggere il file.
8. Fare clic su **Fine**.

Per ripristinare i dati:

1. Aprire la Console utente di Security Manager. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
2. Nel riquadro sinistro della Console utente, fare clic su **Avanzate**, quindi su **Backup e ripristino**.
3. Fare clic su **Ripristina dati**.
4. Selezionare il file di archiviazione creato in precedenza. Specificare il percorso nell'apposito campo oppure fare clic su **Sfoglia**.
5. Immettere la password utilizzata per proteggere il file.
6. Selezionare i moduli di cui ripristinare i dati. In genere, si selezionano tutti i moduli riportati in elenco.
7. Verificare la password di Windows.
8. Fare clic su **Fine**.

6 Drive Encryption for HP ProtectTools (solo in determinati modelli)

Drive Encryption for HP ProtectTools garantisce la protezione completa dei dati del computer tramite crittografia. Una volta attivato Drive Encryption, è necessario accedere tramite la relativa schermata di accesso che viene visualizzata prima® dell'avvio di Windows.

HP ProtectTools Security Manager (Installazione guidata di HP Client Security, Installazione guidata avanzata o Console amministrativa) consente agli amministratori di Windows di attivare Drive Encryption, eseguire il backup della chiave di crittografia, selezionare o deselezionare le unità o le partizioni per la crittografia. Per ulteriori informazioni, vedere la Guida del software HP ProtectTools Security Manager.

Con Drive Encryption è possibile eseguire le attività riportate di seguito:

- Selezione delle impostazioni di Drive Encryption:
  - Attivazione di una password protetta da TPM
  - Crittografia o decrittografia di singole unità o partizioni tramite crittografia basata sul software
  - Crittografia o decrittografia di singole unità che supportano la crittografia automatica mediante la crittografia basata sull'hardware
  - Potenziamento della protezione mediante la disabilitazione delle modalità di sospensione o standby per garantire la richiesta di autenticazione di preavvio di Drive Encryption

NOTA: solo le unità disco rigido eSATA esterne e SATA interne possono essere crittografate.

- Creazione di chiavi di backup
- Ripristino dell'accesso a un computer crittografato tramite chiavi di backup ed HP SpareKey
- Abilitazione dell'autenticazione di preavvio di Drive Encryption mediante una password, un'impronta digitale registrata o il PIN di una smart card

Apertura di Drive Encryption

Gli amministratori possono accedere a Drive Encryption aprendo la Console utente di HP ProtectTools Security Manager.

1. Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.

   – oppure –

   Da **Pannello di controllo**, selezionare **Sistema e sicurezza**, poi **HP ProtectTools Security Manager**.

2. Nel riquadro sinistro della Console utente di HP ProtectTools Security Manager fare clic su **Amministrazione**, quindi su **Console amministrativa**.

3. Nel riquadro sinistro della Console amministrativa di HP ProtectTools selezionare **Drive Encryption**.

Attività generali

Attivazione di Drive Encryption per le unità disco rigido standard

Le unità disco rigido standard vengono crittografate mediante la crittografia basata sul software. Per attivare Drive Encryption, attenersi ai passaggi riportati di seguito:

1. Aprire la Console amministrativa di **HP ProtectTools**. Per ulteriori informazioni, vedere Apertura della Console amministrativa di HP ProtectTools a pagina 16.

2. Nel riquadro di sinistra, fare clic su **Installazione guidata**.

3. Selezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.

4. Per eseguire il backup della chiave di crittografia, collegare un dispositivo esterno per registrare questa chiave. Questa chiave è utilizzata per accedere ai dati in caso di errore con altri metodi.

5. In **Back up Drive Encryption keys** (Backup delle chiavi di Drive Encryption), selezionare la casella di controllo corrispondente al dispositivo di archiviazione in cui salvare la chiave di crittografia.

6. Fare clic su **Avanti**.

NOTA: Viene richiesto di riavviare il computer. Dopo il riavvio, viene visualizzata la schermata di preavvio di Drive Encryption che richiede di eseguire l'autenticazione per poter avviare Windows.

Drive Encryption è stato attivato. La crittografia delle partizioni dell'unità selezionate potrebbe richiedere diverse ore, a seconda del numero e delle dimensioni delle partizioni.

Per ulteriori informazioni, vedere la Guida del software HP ProtectTools Security Manager.

Attivazione di Drive Encryption per le unità disco rigido che supportano la crittografia automatica

Le unità che supportano la crittografia automatica e che soddisfano le specifiche OPAL del Trusted Computing Group in materia di gestione delle stesse, possono essere crittografate utilizzando la crittografia basata sull'hardware o sul software. Seguire questi passaggi per attivare Drive Encryption per le unità disco rigido che supportano la crittografia automatica:

NOTA: la crittografia basata sull'hardware è disponibile solo se TUTTE le unità del computer supportano la crittografia automatica conforme alle specifiche OPAL del Trusted Computing Group in materia di gestione delle unità SED (Self-encrypting Drive). In tal caso, l'opzione **Utilizza crittografia dell'unità hardware** è disponibile ed è possibile utilizzare tanto la crittografia basata sul software quanto la crittografia basata sull'hardware.

Se nel computer sono presenti sia unità che supportano la crittografia automatica che unità disco rigido standard, l'opzione **Utilizza crittografia dell'unità hardware** non è disponibile ed è possibile utilizzare solo la crittografia basata sul software. Per ulteriori informazioni, vedere Attivazione di Drive Encryption per le unità disco rigido standard a pagina 42.

- Utilizzare l'Installazione guidata di HP ProtectTools Security Manager per attivare Drive Encryption.

– oppure –

Crittografia basata sul software

1. Aprire la Console amministrativa di **HP ProtectTools**. Per ulteriori informazioni, vedere Apertura della Console amministrativa di HP ProtectTools a pagina 16.
2. Nel riquadro di sinistra, fare clic su **Installazione guidata**.
3. Selezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.

   NOTA: se l'opzione **Utilizza crittografia dell'unità hardware** è disponibile nella parte inferiore dello schermo, deselezionare la casella di controllo.
4. In **Unità da crittografare**, selezionare la casella di controllo corrispondente all'unità disco rigido che si desidera crittografare, quindi fare clic su **Avanti**.
5. Per eseguire il backup della chiave di crittografia, inserire il dispositivo di archiviazione nello slot appropriato.
6. In **Back up Drive Encryption keys** (Backup delle chiavi di Drive Encryption), selezionare la casella di controllo corrispondente al dispositivo di archiviazione in cui salvare la chiave di crittografia.
7. Fare clic su **Applica**.

   NOTA: Il computer verrà riavviato.

   Drive Encryption è stato attivato. La crittografia dell'unità potrebbe richiedere diverse ore, a seconda delle dimensioni dell'unità.

Crittografia basata sull'hardware

1. Aprire la Console amministrativa di **HP ProtectTools**. Per ulteriori informazioni, vedere Apertura della Console amministrativa di HP ProtectTools a pagina 16.
2. Nel riquadro di sinistra, fare clic su **Installazione guidata**.
3. Selezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.
4. Se la casella di controllo **Utilizza crittografia dell'unità hardware** è disponibile nella parte inferiore della schermata, assicurarsi che sia selezionata.

   Se la casella di controllo è deselezionata o non è disponibile, viene applicata la crittografia basata sul software. Per ulteriori informazioni, vedere Attivazione di Drive Encryption per le unità disco rigido standard a pagina 42.

5. In **Unità da crittografare**, selezionare la casella di controllo corrispondente all'unità disco rigido che si desidera crittografare, quindi fare clic su **Avanti**.

NOTA: se viene mostrata soltanto un'unità, la casella di controllo corrispondente viene automaticamente selezionata e disattivata.

Se il computer include più unità, anche il disco 0 verrà automaticamente selezionato e disattivato, ma risulterà disponibile l'opzione di selezione di unità disco rigido aggiuntive per la crittografia basata sull'hardware.

Il pulsante **Avanti** non è disponibile finché non è stata selezionata almeno un'unità.

6. Per eseguire il backup della chiave di crittografia, inserire il dispositivo di archiviazione nello slot appropriato.
7. In **Back up Drive Encryption keys** (Backup delle chiavi di Drive Encryption), selezionare la casella di controllo corrispondente al dispositivo di archiviazione in cui salvare la chiave di crittografia.
8. Fare clic su **Applica**.

NOTA: Viene richiesto di riavviare il computer. Viene visualizzata la schermata di preavvio di Drive Encryption, che richiede di eseguire l'autenticazione prima di avviare Windows.

Drive Encryption è stato attivato. La crittografia dell'unità potrebbe richiedere diversi minuti.

Per ulteriori informazioni, vedere la Guida del software HP ProtectTools Security Manager.

Disattivazione di Drive Encryption

Gli amministratori possono utilizzare l'installazione guidata di HP ProtectTools Security Manager per attivare Drive Encryption. Per ulteriori informazioni, vedere la Guida del software HP ProtectTools Security Manager.

1. Aprire la Console amministrativa di **HP ProtectTools**. Per ulteriori informazioni, vedere Apertura della Console amministrativa di HP ProtectTools a pagina 16.
2. Nel riquadro di sinistra, fare clic su **Installazione guidata**.
3. Deselezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.

Ha inizio la disattivazione di Drive Encryption.

NOTA: se è stata utilizzata la crittografia basata sul software, viene avviata la decrittografia. L'operazione potrebbe richiedere diverse ore, a seconda delle dimensioni delle partizioni dell'unità disco rigido crittografate. Al completamento della decrittografia, Drive Encryption viene disattivato.

Se è stata utilizzata la crittografia basata sull'hardware, l'unità viene immediatamente decrittografata e, dopo alcuni minuti, viene disattivato Drive Encryption.

Una volta disattivato Drive Encryption, verrà richiesto di spegnere il computer, se viene applicata la crittografia basata sull'hardware, oppure di riavviare il computer, se viene applicata la crittografia sul software.

Accesso dopo l'attivazione di Drive Encryption

Quando il computer viene acceso dopo l'attivazione di Drive Encryption e la registrazione del proprio account, è necessario effettuare l'accesso tramite Drive Encryption:

NOTA: durante la disattivazione delle modalità Sospensione o Standby, l'autenticazione di preavvio di Drive Encryption non viene visualizzata per la crittografia basata sul software o sull'hardware. Con la crittografia basata sull'hardware, è disponibile l'opzione **Disabilita modalità Sospensione per maggiore protezione** che impedisce l'attivazione delle modalità Sospensione o Standby se sono abilitate.

Durante la disattivazione della modalità Ibernazione, l'autenticazione di preavvio di Drive Encryption viene visualizzata per la crittografia basata sul software e sull'hardware.

NOTA: se l'amministratore Windows ha abilitato la protezione di preavvio del BIOS in HP ProtectTools Security Manager e se l'accesso One Step Logon è abilitato (impostazione predefinita), è possibile accedere al computer subito dopo aver eseguito l'autenticazione al preavvio del BIOS, senza doverla eseguire di nuovo nella schermata di accesso di Drive Encryption.

Accesso utente singolo:

- ▲ Nella pagina **Accesso**, immettere la password di Windows, il PIN della smart card, Sparekey, Face o passare un dito registrato.

Accesso multi-utente:

1. Nella pagina **Seleziona utente per accesso**, effettuare la propria selezione dall'elenco a discesa, quindi fare clic su **Avanti**.
2. Nella pagina **Accesso**, immettere la password di Windows oppure il PIN della smart card o ancora passare il dito registrato.

NOTA: consultare l'elenco seguenti per le smart card supportate.

Smart card supportate

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

NOTA: se si utilizza una chiave di ripristino per accedere alla schermata di accesso di Drive Encryption, all'accesso di Windows vengono richieste credenziali aggiuntive per poter accedere agli account degli utenti.

Protezione dei dati tramite la crittografia dell'unità disco rigido

Si consiglia di utilizzare l'Installazione guidata di HP ProtectTools Security Manager per proteggere i dati mediante la crittografia dell'unità disco rigido. Dopo l'attivazione, è possibile crittografare qualsiasi unità disco rigido aggiunta attenendosi alla seguente procedura:

1. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra della voce **Drive Encryption** per visualizzare le opzioni disponibili.
2. Fare clic su **Impostazioni**.
3. Per le unità crittografate tramite software, selezionare le partizioni da crittografare.

   NOTA: questa operazione è valida anche in uno scenario di unità miste dove sono presenti una o più unità disco rigido standard e una o più unità che supportano la crittografia automatica.

– oppure –

- ▲ Per le unità crittografate tramite hardware, selezionare le unità aggiuntive desiderate.

Attività avanzate

Gestione di Drive Encryption (attività dell'amministratore)

Nella pagina Impostazioni di Drive Encryption, gli amministratori possono visualizzare e modificare lo stato di Drive Encryption (abilitato, disabilitato o crittografia basata sull'hardware attivata), nonché visualizzare lo stato di crittografia di tutte le unità disco rigido del computer.

NOTA: solo le unità disco rigido aggiuntive possono essere selezionate o deselezionate per la crittografia basata sull'hardware nella pagina Impostazioni di Drive Encryption.

- Se lo stato è disabilitato, Drive Encryption non è stato ancora attivato dall'amministratore Windows e pertanto non protegge l'unità disco rigido. Utilizzare l'Installazione guidata di HP ProtectTools Security Manager per attivare Drive Encryption.
- Se lo stato è abilitato, Drive Encryption è stato attivato e configurato. L'unità si trova in uno dei seguenti stati:

Crittografia basata sul software

- Non crittografata
- Crittografata
- Crittografia in corso
- Decrittografia in corso

Crittografia basata sull'hardware

- Crittografata
- Non crittografate (per unità aggiuntive)

Utilizzo di protezione avanzata con TPM (solo in determinati modelli)

Se il modulo Trusted Platform Module (TPM) è attivo e la protezione avanzata di Drive Encryption è selezionata, la password di Drive Encryption verrà protetta dal chip di di sicurezza TPM. Se l'unità disco rigido viene rimossa e installata in un altro computer, l'accesso a tale unità verrà negato.

ATTENZIONE: La proprietà di TPM non può essere condivisa con Windows TPM.msc.

NOTA: poiché la password è protetta da un chip di protezione TPM, se l'unità disco rigido viene spostata su un altro computer, per poter accedere ai dati sarà necessario effettuare la migrazione delle impostazioni TPM sul nuovo computer.

NOTA: è necessario che l'opzione TPM sia abilitata in BIOS Setup (Impostazione BIOS).

Crittografia o decrittografia di singole partizioni di unità (solo crittografia basata sul software)

Gli amministratori possono utilizzare la pagina Impostazioni di Drive Encryption per crittografare una o più partizioni dell'unità disco rigido presenti nel computer o per decrittografare partizioni di unità già crittografate.

1. Aprire la Console amministrativa di **HP ProtectTools**. Per ulteriori informazioni, vedere Apertura della Console amministrativa di HP ProtectTools a pagina 16.
2. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra della voce **Drive Encryption** per visualizzare le opzioni disponibili.

3. Fare clic su **Impostazioni**.
4. In **Stato unità**, selezionare o deselezionare la casella di controllo corrispondente a ogni unità disco rigido che si desidera crittografare o decrittografare, quindi fare clic su **Applica**.

NOTA: durante le operazioni di crittografia o decrittografia di una partizione, una barra di avanzamento visualizza la percentuale di completamento e il tempo rimanente alla fine del processo.

NOTA: sono supportate le partizioni dinamiche. Per partizione dinamica si intende una partizione che viene visualizzata come disponibile, ma che non può essere crittografata una volta selezionata. Una partizione dinamica è il risultato della riduzione di una partizione per crearne una nuova all'interno di Gestione disco.

Quando una partizione sta per essere convertita in una partizione dinamica, viene visualizzato un messaggio di avvertenza.

Backup e ripristino (attività dell'amministratore)

Quando Drive Encryption è attivato, gli amministratori possono utilizzare la pagina di backup delle chiavi di crittografia per eseguire il backup su un supporto rimovibile e un ripristino.

Backup delle chiavi di crittografia

Gli amministratori possono eseguire il backup della chiave di crittografia per un'unità crittografata su un dispositivo di archiviazione rimovibile.

ATTENZIONE: conservare il dispositivo di archiviazione contenente la chiave di backup in un luogo sicuro, perché, se si dimentica la password, se si perde la smart card o se non si è effettuata la registrazione di un dito, questo dispositivo è l'unico modo per poter accedere al computer. Anche il luogo di archiviazione deve essere sicuro, perché il dispositivo di archiviazione consente l'accesso a Windows.

NOTA: per salvare la chiave di crittografia, è necessario utilizzare un dispositivo di archiviazione USB in formato FAT32 o FAT16. Per il backup è possibile utilizzare memory stick USB, schede di memoria SD (Secure Digital) o MMC (MultiMedia Card).

1. Aprire la Console amministrativa di **HP ProtectTools**. Per ulteriori informazioni, vedere Apertura della Console amministrativa di HP ProtectTools a pagina 16.
2. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra della voce **Drive Encryption** per visualizzare le opzioni disponibili.
3. Fare clic su **Backup delle chiavi di crittografia**.
4. Inserire il dispositivo di archiviazione utilizzato per eseguire il backup della chiave di crittografia.

   NOTA: per salvare la chiave di crittografia, è necessario utilizzare un dispositivo di archiviazione USB formattato FAT32. Per il backup è possibile utilizzare memory stick USB, schede di memoria SD (Secure Digital) o MMC (MultiMedia Card). In alcuni casi è possibile utilizzare SkyDrive.

5. In **Unità**, selezionare la casella di controllo corrispondente al dispositivo in cui si desidera eseguire il backup della chiave di crittografia.
6. Fare clic su **Esegui backup chiavi**.
7. Leggere le informazioni nella pagina che viene visualizzata, quindi fare clic su **OK**. La chiave di crittografia viene salvata nel dispositivo di archiviazione selezionato.

Ripristino dell'accesso a un computer attivato tramite le chiavi di backup

Gli amministratori possono eseguire un ripristino utilizzando la chiave di Drive Encryption di cui si è eseguito il backup su un dispositivo di archiviazione rimovibile al momento dell'attivazione o selezionando l'opzione **Backup delle chiavi di crittografia dell'unità** in Security Manager.

1. Inserire il dispositivo di archiviazione rimovibile in cui è memorizzata la chiave di backup.
2. Accendere il computer.
3. Quando si apre la finestra di dialogo di accesso a Drive Encryption for HP ProtectTools, fare clic su **Opzioni**.
4. Fare clic su **Ripristino**.
5. Immettere il nome o il percorso del file contenente la chiave di backup, quindi fare clic su **Ripristina**.

   – oppure –

   Fare clic su **Sfoglia** per cercare il file di backup richiesto, fare clic su **OK**, quindi su **Ripristina**.
6. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **OK**.

   La finestra di accesso di Windows è visualizzata.

NOTA: se si utilizza una chiave di ripristino per accedere alla schermata di accesso di Drive Encryption, all'accesso di Windows vengono richieste credenziali aggiuntive per poter accedere agli account degli utenti. si consiglia di reimpostare la password dopo aver eseguito un ripristino.

Eseguire un recupero di HP SpareKey Recovery

Il ripristino con la SpareKey all'interno del preavvio di Drive Encryption richiede di rispondere correttamente alle domande di protezione prima di poter accedere al computer. Per ulteriori informazioni sull'impostazione del ripristino con la SpareKey, vedere la Guida del software Security Manager.

Per eseguire un ripristino con la SpareKey se si è dimenticata la password, procedere come segue:

1. Accendere il computer.
2. Quando viene visualizzata la pagina Drive Encryption for HP ProtectTools, spostarsi alla pagina di accesso.
3. Fare clic su **SpareKey**.

   NOTA: se la SpareKey non è stata inizializzata in Security Manager, il pulsante **SpareKey** non è disponibile.
4. Digitare le risposte corrette alle domande visualizzate, quindi fare clic su **Accesso**.

   La finestra di accesso di Windows è visualizzata.

NOTA: se la SpareKey viene utilizzata per accedere alla schermata di accesso di Drive Encryption, all'accesso di Windows vengono richieste credenziali aggiuntive per poter accedere agli account degli utenti. si consiglia di reimpostare la password dopo aver eseguito un ripristino.

Visualizzazione stato crittografia

Gli utenti possono visualizzare lo stato della crittografia da HP ProtectTools Security Manager.

NOTA: Gli amministratori possono cambiare lo stato di Drive Encryption utilizzando la Console amministrativa di HP ProtectTools.

1. Aprire la Console utente di **HP ProtectTools**. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
2. In **Dati personali**, fare clic su **Drive Encryption**.

   In uno scenario di crittografia basata sul software o sull'hardware, lo stato della crittografia dell'unità viene visualizzato in uno dei seguenti modi:

   - Attivata
   - Disattivata

   In uno scenario di crittografia basata sul software, lo stato della crittografia dell'unità viene visualizzato in uno dei seguenti modi per ogni unità disco rigido o partizione di unità disco rigido:

   - Non crittografata
   - Crittografato
   - Crittografia in corso
   - Decrittografia in corso

   In uno scenario di crittografia basata sull'hardware, lo stato della crittografia dell'unità viene visualizzato in uno dei seguenti modi:

   - Non crittografata
   - Crittografato

   Durante le operazioni di crittografia o decrittografia dell'unità disco rigido, una barra di avanzamento visualizza la percentuale di completamento e il tempo rimanente alla fine del processo.

7 Device Access Manager for HP ProtectTools (solo in determinati modelli)

HP ProtectTools Device Access Manager controlla l'accesso ai dati disabilitando le periferiche di trasferimento dei dati.

NOTA: alcune periferiche di input/HID (Human Interface Input), ad esempio mouse, tastiere, touchpad e lettori di impronte digitali, non sono controllate da Device Access Manager. Per ulteriori informazioni, vedere Classi di periferiche non gestite a pagina 59.

Gli amministratori dei sistemi operativi Windows® utilizzano HP ProtectTools Device Access Manager per controllare l'accesso alle periferiche di un sistema e per proteggerle dall'accesso non autorizzato:

- Per tutti gli utenti vengono creati profili che definiscono le periferiche a cui possono o non possono accedere.
- L'autenticazione Just-in-time (JITA, Just-in-time authentication) consente a utenti predefiniti di autenticarsi per poter accedere a periferiche altrimenti non accessibili.
- Per escludere gli amministratori e gli utenti attendibili dalle restrizioni relative all'accesso alle periferiche stabilite da Device Access Manager, aggiungerli al gruppo Amministratori di periferiche. L'appartenenza a questo gruppo è gestita tramite le Impostazioni avanzate.
- L'accesso alle periferiche può essere concesso o negato in base all'appartenenza al gruppo o a singoli utenti.
- Per le classi di periferiche, ad esempio le unità CD-ROM e DVD, gli accessi in lettura e scrittura possono essere concessi o negati separatamente.

Apertura di Device Access Manager

1. Eseguire l'accesso come amministratore.
2. Aprire **HP ProtectTools Security Manager** da **HP Client Security Dashboard**.

   – oppure –

   Dal desktop di Windows, fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.

   – oppure –

   Da **Pannello di controllo**, selezionare **Sistema e sicurezza**, poi **HP ProtectTools Security Manager**.
3. Nel riquadro sinistro della Console utente di HP ProtectTools Security Manager fare clic su **Amministrazione**, quindi su **Console amministrativa**.
4. Nel riquadro di sinistra della Console amministrativa, fare clic su **Device Access Manager**.

Un utente standard può visualizzare i criteri di HP ProtectTools Device Access Manager utilizzando HP ProtectTools Security Manager. La console visualizza una schermata di sola lettura.

Procedure di installazione

Configurazione dell'accesso ai dispositivi

HP ProtectTools Device Access Manager presenta quattro schermate:

- **Configurazione semplice**—Consente di concedere o negare l'accesso alle classi di periferiche in base all'appartenenza al gruppo Amministratori di periferiche.
- **Configurazione delle classi di periferiche**—Consente di concedere o negare a utenti o gruppi selezionati l'accesso a tipi di periferiche o periferiche specifiche.
- **JITA Configuration**—Consente di configurare l'autenticazione Just-in-time (JITA, Just-in-time configuration) per concedere agli utenti selezionati l'accesso alle unità DVD/CD-ROM o ai supporti rimovibili mediante l'autenticazione.
- **Impostazioni avanzate**—Consente di configurare un elenco di lettere di unità a cui Device Access Manager non limiterà l'accesso, ad esempio C: o l'unità di sistema. Da questa schermata è anche possibile gestire l'appartenenza al gruppo Amministratori di periferiche.

Configurazione semplice

Gli amministratori possono utilizzare la schermata **Configurazione semplice** per consentire o negare l'accesso alle seguenti classi di periferiche per tutti gli amministratori–non di periferiche:

- Tutti i supporti rimovibili (dischetti, unità flash USB e così via)
- Tutte le unità DVD/CD-ROM
- Tutte le porte seriali e parallele
- Tutti i dispositivi Bluetooth

NOTA: se i dispositivi Bluetooth vengono utilizzati come credenziali di autenticazione, il relativo accesso non deve essere limitato nei criteri di Device Access Manager.

- Tutti i dispositivi modem
- Tutte le periferiche PCMCIA/ExpressCard
- Tutte le periferiche 1394

Per consentire o negare a tutti gli amministratori non di periferiche l'accesso a una classe di periferiche, procedere come segue:

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, and then click **Simple Configuration**.
2. Per negare l'accesso, nel riquadro di destra, selezionare la casella di controllo corrispondente a una classe di periferiche o a una periferica specifica. Deselezionare la casella di controllo per consentire l'accesso a tale classe di periferiche o periferica specifica.

   Se una casella di controllo è disattivata, i valori che interessano lo scenario di accesso sono stati modificati nella schermata **Configurazione delle classi di periferiche**. Per ripristinare i valori predefiniti, fare clic su **Reimposta** nella schermata **Configurazione delle classi di periferiche**.

3. Fare clic su **Applica**.

NOTA: se il servizio in background non è in esecuzione, viene aperta una finestra di dialogo che richiede se si desidera avviarlo. Fare clic su **Sì**.

4. Fare clic su **OK**.

Avvio del servizio in background

La prima volta che si definisce e applica un nuovo criterio, il servizio in background Controllo/blocco dispositivi HP ProtectTools viene avviato automaticamente e tale comportamento viene impostato in corrispondenza di ogni avvio del sistema.

NOTA: è necessario definire un profilo di periferiche prima che venga visualizzato il prompt del servizio in background.

Gli amministratori possono inoltre avviare o arrestare questo servizio.

L'arresto di questo servizio non comporta l'interruzione del blocco della periferica. Due componenti sono responsabili del blocco della periferica:

- Servizio di controllo/blocco dispositivi
- Driver DAMDrv.sys

L'avvio del servizio comporta l'avvio del driver della periferica, mentre il suo arresto non comporta l'interruzione del driver.

Per determinare se il servizio in background è in esecuzione, aprire una finestra del prompt dei comandi e digitare`sc query flcdlock`.

Per determinare se il driver del dispositivo è in esecuzione, aprire una finestra del prompt dei comandi e digitare`sc query damdrv`.

Configurazione delle classi di periferiche

Gli amministratori possono visualizzare e modificare gli elenchi degli utenti e dei gruppi a cui è consentito o negato l'accesso alle classi di periferiche o a periferiche specifiche.

La schermata **Configurazione delle classi di periferiche** è costituita dalle seguenti sezioni:

- **Elenco periferiche**—Mostra tutte le classi di periferiche e tutte le periferiche installate sul sistema o che sono state installate sul sistema in precedenza.
  - La protezione viene in genere applicata a una classe di periferiche. Un utente o gruppo selezionato sarà in grado di accedere a qualsiasi periferica inclusa in tale classe.
  - La protezione potrebbe essere anche applicata a periferiche specifiche.
- **Elenco utenti**—Mostra tutti gli utenti e gruppi a cui è consentito o negato l'accesso alla classe di periferiche selezionata o a una periferica specifica.
  - La voce Elenco utenti può essere associata a un utente specifico o a un gruppo di cui l'utente è membro.
  - Quando una voce di utente o gruppo in Elenco utenti non è disponibile, l'impostazione è stata ereditata dalla classe delle periferiche in Elenco periferiche o dalla cartella Classe.
  - Alcune classi di periferiche, ad esempio, DVD e CD-ROM, possono essere controllate ulteriormente consentendo o negando l'accesso separatamente per le operazioni di lettura e scrittura.

Per quanto riguarda le altre periferiche e classi, i diritti di accesso in lettura e scrittura possono essere ereditati. Ad esempio, l'accesso in lettura può essere ereditato da una classe superiore, ma l'accesso in scrittura può essere specificamente negato per un utente o un gruppo.

NOTA: se la casella di controllo **Lettura** è deselezionata, la voce di controllo dell'accesso non influisce sull'accesso in lettura alla periferica, ma l'accesso in lettura non è negato.

NOTA: il gruppo Amministratori non può essere aggiunto all'elenco utenti. Utilizzare piuttosto il gruppo Amministratori di periferiche.

Esempio 1—Se a un utente o a un gruppo è negato l'accesso in scrittura a una periferica o classe di periferiche:

Allo stesso utente, stesso gruppo o a un membro dello stesso gruppo può essere concesso l'accesso in scrittura o in lettura e scrittura solo per una periferica che si trova a un livello inferiore rispetto a questa nella gerarchia delle periferiche.

Esempio 2—Se a un utente o a un gruppo è consentito l'accesso in scrittura a una periferica o classe di periferiche:

Allo stesso utente, stesso gruppo o a un membro dello stesso gruppo può essere negato l'accesso in scrittura o in lettura e scrittura solo per la stessa periferica o per una periferica che si trova a un livello inferiore rispetto a questa nella gerarchia delle periferiche.

Esempio 3—Se a un utente o a un gruppo è consentito l'accesso in lettura a una periferica o classe di periferiche:

Allo stesso utente, stesso gruppo o a un membro dello stesso gruppo può essere negato l'accesso in lettura o in lettura e scrittura solo per la stessa periferica o per una periferica che si trova a un livello inferiore rispetto a questa nella gerarchia delle periferiche.

Esempio 4—Se a un utente o a un gruppo è negato l'accesso in lettura a una periferica o classe di periferiche:

Allo stesso utente, stesso gruppo o a un membro dello stesso gruppo può essere concesso l'accesso in lettura o in lettura e scrittura solo per una periferica che si trova a un livello inferiore rispetto a questa nella gerarchia delle periferiche.

Esempio 5—Se a un utente o a un gruppo è consentito l'accesso in scrittura e lettura a una periferica o classe di periferiche:

Allo stesso utente, stesso gruppo o a un membro dello stesso gruppo può essere negato l'accesso in scrittura o in lettura e scrittura solo per la stessa periferica o per una periferica che si trova a un livello inferiore rispetto a questa nella gerarchia delle periferiche.

Esempio 6—Se a un utente o a un gruppo è negato l'accesso in lettura e scrittura a una periferica o classe di periferiche:

Allo stesso utente, stesso gruppo o a un membro dello stesso gruppo può essere concesso l'accesso in lettura o in lettura e scrittura solo per una periferica che si trova a un livello inferiore rispetto a questa nella gerarchia delle periferiche.

Negazione dell'accesso a un utente o gruppo

Per impedire a un utente o a un gruppo di accedere a una periferica o a una classe di periferiche, procedere come segue:

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, and then click **Device Class Configuration**.
2. Nell'elenco delle periferiche, fare clic sulla classe che si desidera configurare.
   - **Classe di periferiche**
   - **Tutte le periferiche**
   - **Singola periferica**
3. In **Utente/Gruppi**, fare clic sull'utente o sul gruppo cui negare l'accesso, quindi fare clic su **Nega**.
4. Fare clic su **Applica**.

NOTA: se le impostazioni Nega e Consenti sono definite a livello della stessa periferica per un utente, la negazione dell'accesso avrà la precedenza sulla concessione.

Concessione dell'accesso a un utente o gruppo

Per autorizzare un utente o un gruppo ad accedere a una periferica o classe di periferiche, procedere come segue:

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, and then click **Device Class Configuration**.
2. Nell'elenco delle periferiche, fare clic su una delle seguenti opzioni:
   - **Classe di periferiche**
   - **Tutte le periferiche**
   - **Singola periferica**
3. Fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo **Seleziona utenti o gruppi**.
4. Fare clic su **Avanzate**, quindi su **Trova** per cercare gli utenti o i gruppi da aggiungere.
5. Fare clic su un utente o su un gruppo da aggiungere all'elenco di utenti e gruppi disponibili, quindi fare clic su **OK**.
6. Fare clic di nuovo su **OK**.
7. Per concedere l'accesso all'utente selezionato, fare clic su **Consenti**.
8. Fare clic su **Applica**.

Concessione a un utente di un gruppo dell'accesso a una classe di periferiche

Per concedere a un utente l'accesso a una classe di periferiche negandolo a tutti gli altri membri del suo gruppo, procedere come segue:

1. Nel riquadro di sinistra della **Console amministrativa di HP ProtectTools**, fare clic su **Device Access Manager**, quindi su **Configurazione delle classi di periferiche**.
2. Nell'elenco delle periferiche, fare clic sulla classe che si desidera configurare.
   - **Classe di periferiche**
   - **Tutte le periferiche**
   - **Singola periferica**
3. In **Utente/Gruppi**, selezionare il gruppo cui negare l'accesso, quindi fare clic su **Nega**.
4. Spostarsi alla cartella sotto quella della classe richiesta, quindi aggiungere l'utente specifico.
5. Per concedere l'accesso all'utente selezionato, fare clic su **Consenti**.
6. Fare clic su **Applica**.

Concessione a un utente di un gruppo dell'accesso a una periferica specifica

Gli amministratori possono concedere a un utente l'accesso a una periferica specifica negando contemporaneamente a tutti gli altri membri del gruppo di tale utente l'accesso a tutte le periferiche nella classe:

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, and then click **Device Class Configuration**.
2. Nell'elenco delle periferiche, fare clic sulla classe che si desidera configurare, quindi spostarsi alla cartella al di sotto di questa.
3. In **Utente/Gruppi**, fare clic su **Consenti** accanto al gruppo cui concedere l'accesso.
4. Fare clic su **Nega** accanto al gruppo cui negare l'accesso.
5. Spostarsi alla periferica specifica presente nell'elenco delle periferiche a cui si desidera che l'utente abbia accesso.
6. Fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo **Seleziona utenti o gruppi**.
7. Fare clic su **Avanzate**, quindi su **Trova** per cercare gli utenti o i gruppi da aggiungere.
8. Fare clic su un utente cui consentire l'accesso, quindi su **OK**.
9. Per concedere l'accesso all'utente selezionato, fare clic su **Consenti**.
10. Fare clic su **Applica**.

Rimozione delle impostazioni per un utente o gruppo

Per rimuovere da un utente o gruppo l'autorizzazione di accesso a una periferica o classe di periferiche, procedere come segue:

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, and then click **Device Class Configuration**.
2. Nell'elenco delle periferiche, fare clic sulla classe che si desidera configurare.
   - **Classe di periferiche**
   - **Tutte le periferiche**
   - **Singola periferica**
3. In **Utente/Gruppi**, fare clic sull'utente o sul gruppo desiderato, quindi fare clic su **Rimuovi**.
4. Fare clic su **Applica**.

Reimpostazione della configurazione

ATTENZIONE: quando si reimposta la configurazione, vengono eliminate tutte le modifiche di configurazione apportate alle periferiche e vengono ripristinate tutte le impostazioni predefinite.

NOTA: La pagina Impostazioni avanzate non viene reimpostata.

Per ripristinare i valori predefiniti, procedere come segue:

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, and then click **Device Class Configuration**.
2. Fare clic su **Reimposta**.
3. Fare clic su **Sì** per confermare la richiesta.
4. Fare clic su **Applica**.

Configurazione JITA (Just-in-time authentication)

La configurazione JITA consente agli amministratori di visualizzare e modificare gli elenchi degli utenti e dei gruppi che possono accedere alle periferiche mediante l'autenticazione Just-in-time (JITA).

Gli utenti abilitati all'autenticazione JITA saranno in grado di accedere ad alcune periferiche i cui criteri creati nelle schermate **Configurazione delle classi di periferiche** e **Configurazione semplice** sono stati limitati.

- **Scenario**—Un criterio di configurazione semplice viene configurato per negare l'accesso alle unità DVD/CD-ROM per tutti gli amministratori non di periferiche.
- **Risultato**—Un utente abilitato all'autenticazione JITA che tenta di accedere all'unità DVD/CD-ROM visualizza lo stesso messaggio di “accesso negato” di un utente non abilitato all'autenticazione JITA. Viene visualizzato un messaggio che chiede se l'utente desidera l'accesso JITA. Se si fa clic sul messaggio, viene visualizzata la finestra di dialogo di autenticazione dell'utente. Con l'immissione delle credenziali, all'utente viene concesso l'accesso all'unità DVD/CD-ROM.

È possibile autorizzare la durata della sessione JITA in base a un numero di minuti definito o per 0 minuti. Una durata di 0 minuti non avrà scadenza. Gli utenti avranno accesso alla periferica dal momento in cui si autenticano fino a quando si disconnettono dal sistema.

La durata JITA può anche essere estesa, se opportunamente configurata. In questo scenario, 1 minuto prima della scadenza della sessione JITA, gli utenti possono selezionare il prompt per estendere l'accesso senza dover eseguire di nuovo l'autenticazione.

A prescindere dalla durata della sessione JITA, limitata o illimitata, non appena l'utente esegue la disconnessione dal sistema o un altro utente esegue l'accesso, la sessione JITA scade. Al successivo accesso, quando l'utente tenta di accedere a una periferica abilitata all'autenticazione JITA, viene visualizzato un messaggio che richiede di immettere le credenziali.

JITA è disponibile per le seguenti classi di periferiche:

- Unità DVD/CD-ROM
- Supporti rimovibili

Creazione di un'autenticazione Just-in-time per un utente o gruppo

Gli amministratori possono consentire agli utenti o ai gruppi di accedere alle periferiche utilizzando l'autenticazione Just-in-time.

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, quindi su **JITA Configuration** (Configurazione JITA).
2. Dal menu a discesa della periferica', selezionare **Supporti rimovibili** o **Unità DVD/CD-ROM**.
3. Fare clic su **+** per aggiungere un utente o un gruppo alla configurazione JITA.
4. Selezionare la casella di controllo **Abilitata**.
5. Impostare la durata della sessione JITA desiderata.
6. Fare clic su **Applica**.

Per applicare la nuova impostazione JITA, è necessario che l'utente si disconnetta e riconnetta.

Creazione di una sessione di Just-in-time prorogabile per un utente o gruppo

Gli amministratori possono consentire all'utente o al gruppo di accedere alle periferiche utilizzando l'autenticazione Just-in-time prorogabile prima della sua scadenza.

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, quindi su **JITA Configuration** (Configurazione JITA).
2. Dal menu a discesa della periferica', selezionare **Supporti rimovibili** o **Unità DVD/CD-ROM**.
3. Fare clic su **+** per aggiungere un utente o un gruppo alla configurazione JITA.
4. Selezionare la casella di controllo **Abilitata**.
5. Impostare la durata della sessione JITA desiderata.
6. Selezionare la casella di controllo **Estendibile**.
7. Fare clic su **Applica**.

Per applicare la nuova impostazione JITA, è necessario che l'utente si disconnetta e riconnetta.

Disattivazione di un'autenticazione Just-in-time per un utente o gruppo

Gli amministratori possono negare agli utenti o ai gruppi l'accesso alle periferiche utilizzando l'autenticazione Just-in-time.

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, quindi su **JITA Configuration** (Configurazione JITA).
2. Dal menu a discesa della periferica', selezionare **Supporti rimovibili** o **Unità DVD/CD-ROM**.
3. Selezionare l'utente o un gruppo di cui si desidera disattivare l'autenticazione Just-in-time.
4. Deselezionare la casella di controllo **Abilitata**.
5. Fare clic su **Applica**.

L'utente non può accedere quando esegue l'accesso e tenta di utilizzare la periferica.

Impostazioni avanzate

Le impostazioni avanzate offrono le seguenti funzioni:

- Gestione del gruppo Amministratori di periferiche
- Gestione delle lettere di unità a cui Device Access Manager non nega mai l'accesso.

Il gruppo Amministratori di periferiche viene utilizzato per escludere gli utenti attendibili (attendibili in termini di accesso alle periferiche) dalle restrizioni imposte da un criterio di Device Access Manager. Gli utenti attendibili in genere includono gli amministratori di sistema. Per ulteriori informazioni, vedere Gruppo Amministratori di periferiche a pagina 58.

La schermata **Impostazioni avanzate** consente anche all'amministratore di configurare un elenco di lettere di unità il cui accesso da parte di tutti gli utenti non verrà mai limitato da Device Access Manager.

NOTA: i servizi in background di Device Access Manager devono essere in esecuzione durante la configurazione dell'elenco delle lettere di unità.

Per avviare questi servizi, procedere come segue:

1. Applicare un criterio di configurazione semplice, ad esempio negare l'accesso ai supporti rimovibili per tutti gli amministratori non di periferiche.

   – oppure –

   Aprire una finestra del prompt dei comandi con privilegi di amministratore, quindi digitare:

   ```
   sc start flcdlock
   ```

   Premere invio.

2. All'avvio dei servizi, è possibile modificare l'elenco delle unità. Immettere le lettere di unità corrispondenti alle periferiche da escludere dal controllo di Device Access Manager.

   Le lettere di unità vengono visualizzate per le partizioni o i dischi rigidi fisici.

NOTA: tutti gli utenti avranno sempre accesso all'unità di sistema (in genere indicata dalla lettera C) a prescindere dalla sua presenza in questo elenco.

Gruppo Amministratori di periferiche

Quando viene installato Device Access Manager, viene creato un gruppo denominato Amministratori di periferiche.

Il gruppo Amministratori di periferiche viene utilizzato per escludere gli utenti attendibili (attendibili in termini di accesso alle periferiche) dalle restrizioni imposte da un criterio di Device Access Manager. Gli utenti attendibili in genere includono gli amministratori di sistema.

NOTA: l'aggiunta di un utente al gruppo Amministratori di periferiche non consente automaticamente all'utente di accedere alle periferiche. Nella schermata **Configurazione delle classi di periferiche**, se al gruppo Utenti è negato l'accesso a una periferica, il gruppo Amministratori di periferiche deve disporre dell'accesso per fare in modo che i membri del gruppo abbiano accesso alla periferica. Tuttavia, la schermata **Configurazione semplice** può essere utilizzata per negare l'accesso alle classi di periferiche per tutti gli utenti che non sono appartengono al gruppo Amministratori di periferiche.

Per aggiungere utenti al gruppo Amministratori di periferiche, procedere come segue:

1. Nella schermata **Impostazioni avanzate**, fare clic su **+**.
2. Immettere il nome dell'utente attendibile.
3. Fare clic su **OK**.
4. Fare clic su **Applica**.

Supporto dispositivi eSATA

Per poter consentire a Device Access Manager di controllare le periferiche eSATA, è necessario configurare quanto riportato di seguito:

1. L'unità deve essere collegata all'avvio del sistema.
2. Utilizzando la schermata **Impostazioni avanzate**, controllare che la lettera di unità corrispondente a eSATA non sia nell'elenco delle unità a cui Device Access Manager non negherà l'accesso. Se la lettera di unità corrispondente a eSATA è presente nell'elenco, eliminarla, quindi fare clic su **Applica**.
3. La periferica può essere controllata utilizzando la classe di periferiche Supporti rimovibili, la schermata **Configurazione semplice** o la schermata **Configurazione delle classi di periferiche**.

Classi di periferiche non gestite

HP ProtectTools Device Access Manager non gestisce le seguenti classi di periferiche:

- Dispositivi di input/output
  - Biometrici
  - Mouse
  - Tastiera
  - Stampante
  - Stampanti Plug and play (PnP)
  - Aggiornamento stampante
  - Human Interface Device (HID) a infrarossi
  - Lettore di smart card
  - Dispositivi seriali multi-porta
  - Unità disco

- Controller floppy disk (FDC, Floppy Disk Controller)
- Controller unità disco rigido (HDC, Hard Disk Controller)
- Classe Human Interface Device (HID)

- Alimentazione
  - Batteria
  - Supporto Advanced power management (APM)
- Varie
  - Computer
  - Decodificatore
  - Display
  - Elaboratore
  - Sistema
  - Sconosciuto
  - Volume
  - Istantanea volume
  - Dispositivi di protezione
  - Acceleratori di protezione
  - Driver display unificato Intel®
  - Driver multimediale
  - Dispositivi juke-box
  - Multifunzione
  - Legacard
  - Client di rete
  - Servizio di rete
  - Trasporto di rete
  - Scheda SCSI

8 Ritrovamento in seguito a furto (solo in determinati modelli)

Computrace for HP ProtectTools (da acquistare a parte) consente il monitoraggio, la gestione e l'individuazione del computer da remoto.

Una volta attivato, Computrace for HP ProtectTools viene configurato dal centro assistenza clienti di Absolute Software Customer Center. Dal centro assistenza clienti, l'amministratore può configurare Computrace for HP ProtectTools per monitorare o gestire il computer. In caso di furto o smarrimento del computer, il centro assistenza clienti collabora con le autorità locali al suo ritrovamento. Se configurato, Computrace può continuare a funzionare anche se l'unità disco rigido viene cancellata o sostituita.

Per attivare Computrace for HP ProtectTools, procedere come segue:

1. Connettersi a Internet.
2. Aprire la Console utente di Security Manager. Per ulteriori informazioni, vedere Avvio di Security Manager a pagina 25.
3. Nel riquadro di sinistra di Security Manager, fare clic su **Ritrovamento in seguito a furto**.
4. Per avviare l'attivazione guidata di Computrace, fare clic sul pulsante **Inizio**.
5. Inserire le proprie informazioni di contatto e i dati della carta di credito, oppure immettere un codice prodotto preacquistato.

La procedura guidata di attivazione elabora in modo sicuro la transazione e configura l'account utente sul sito Web del centro assistenza clienti di Absolute Software. Una volta completata l'operazione, si riceve un'e-mail di conferma contenente i dati dell'account del centro assistenza clienti.

Se in passato si è eseguita la procedura guidata di attivazione di Computrace e l'account utente del centro assistenza clienti è già esistente, è possibile comprare licenze aggiuntive contattando un addetto dell'account HP.

Per accedere al centro assistenza clienti:

1. Andare a https://cc.absolute.com/.
2. Nei campi **ID accesso** e **Password** immettere le credenziali contenute nell'e-mail di conferma, quindi fare clic su **Accedi**.

Nel Centro assistenza clienti è possibile:

- Monitorare i computer.
- Proteggere i dati remoti.
- Segnalare il furto dei computer protetti da Computrace.

▲ Fare clic su **Ulteriori informazioni** per maggiori dettagli su Computrace for HP ProtectTools.

9 Eccezioni relative alle password localizzate

A livello di protezione di preavvio e di HP Drive Encryption, il supporto della localizzazione della password è limitato, come descritto nelle seguenti sezioni.

Operazioni da eseguire quando una password viene rifiutata

Le password possono essere rifiutate per i seguenti motivi:

- Un utente usa un editor IME non supportato. Si tratta di un problema comune con le lingue a doppio byte (coreano, giapponese e cinese). Per risolverlo, procedere come segue:

  1. Tramite **Pannello di controllo**, aggiungere un layout della tastiera supportato (aggiungere le tastiere US/Inglese sotto la lingua di input Cinese).
  2. Impostare la tastiera supportata per l'input predefinito.
  3. Riavviare HP ProtectTools, quindi immettere di nuovo la password.

- Un utente usa un carattere non supportato. Per risolvere questo problema, procedere come segue:

  1. Modificare la password di Windows utilizzando solo caratteri supportati. Per ulteriori informazioni sui caratteri non supportati, vedere la Guida del software della Console amministrativa di HP ProtectTools.
  2. Eseguire di nuovo l'installazione guidata di HP ProtectTools Security Manager, quindi immettere la nuova password di Windows.

IME di Windows non supportati a livello di protezione di preavvio o di HP Drive Encryption

In Windows, l'utente può scegliere un editor IME per immettere caratteri e simboli complessi, ad esempio quelli del giapponese o cinese, utilizzando una tastiera occidentale standard.

Gli editor IME non sono supportati a livello di protezione di preavvio o di HP Drive Encryption. Non è possibile immettere una password di Windows con un editor IME nella schermata di accesso alla protezione di preavvio o a HP Drive Encryption, in quanto ciò potrebbe causare una situazione di blocco. In alcuni casi, Microsoft® Windows non visualizza l'editor IME quando l'utente immette la password.

La soluzione è passare a uno dei seguenti layout di tastiera supportati che esegue la conversione in layout di tastiera 00000411:

- IME Microsoft per il giapponese
- Layout della tastiera giapponese
- IME per Office 2007 per il giapponese— se Microsoft o una terza parte utilizza il termine IME o Editor del metodo di input, è possibile che il metodo non sia effettivamente un IME. Ciò può

causare confusione, ma il software legge la rappresentazione del codice esadecimale. Pertanto, se un IME esegue l'associazione a un layout di tastiera supportato, HP ProtectTools può supportare la configurazione.

AVVERTENZA! Quando viene distribuito HP ProtectTools, le password immesse con un editor IME Windows verranno rifiutate.

Modifiche della password con layout di tastiera supportato

Se la password viene inizialmente impostata con un layout di tastiera, ad esempio U.S. English (409), e viene quindi modificata utilizzando un layout diverso che è anche supportato, ad esempio Latin American (080A), la modifica della password avrà esito positivo in HP Drive Encryption, ma non riuscirà nel BIOS se vengono utilizzati caratteri presenti in quest'ultimo layout ma non nel primo (ad esempio, ē).

NOTA: Gli amministratori possono risolvere questo problema utilizzando la funzionalità di gestione degli utenti di HP ProtectTools, selezionando il layout di tastiera desiderato nel sistema operativo, quindi eseguendo di nuovo l'installazione guidata di HP Security Manager per lo stesso utente. Nel BIOS è memorizzato il layout di tastiera desiderato e le password che possono essere digitate con questo layout verranno correttamente impostate nel BIOS.

Un altro problema potenziale è l'utilizzo di layout di tastiera diversi, ma tutti in grado di produrre gli stessi caratteri. Ad esempio, entrambi i layout di tastiera U.S. International (20409) e Latin American (080A) possono produrre il carattere é, benché la sua digitazione richieda sequenze di tasti diverse. Se una password viene inizialmente impostata con il layout di tastiera Latin American, questo layout viene impostato nel BIOS, anche se la password viene successivamente modificata utilizzando il layout U.S. International.

Gestione tasti speciali

- Cinese, slovacco, francese canadese e ceco

  Quando si seleziona uno dei layout di tastiera precedenti e si immette una password (ad esempio, abcdef), è necessario immettere la stessa password premendo il tasto maiusc per il carattere minuscolo e i tasti maiusc e bloc maiusc per il carattere maiuscolo a livello di protezione di preavvio del BIOS e di HP Drive Encryption. Le password numeriche devono essere immesse utilizzando il tastierino numerico.

- Coreano

  Quando si seleziona un layout di tastiera coreano supportato e si immette una password, è necessario immettere la stessa password premendo il tasto destro alt per il carattere minuscolo e il tasto destro alt e bloc maiusc per il carattere maiuscolo a livello di protezione di preavvio del BIOS e di HP Drive Encryption.

- Nella tabella seguente vengono elencati i caratteri non supportati:

Lingua	Windows	BIOS	Drive Encryption
Arabo	I tasti ﻻ, ﻷ e ﻹ generano due caratteri.	I tasti ﻻ, ﻷ e ﻹ generano un carattere.	I tasti ﻻ, ﻷ e ﻹ generano un carattere.
Francese canadese	ç, è, à, e é con caps lock sono Ç, È, À, e É in Windows.	ç, è, à, e é con caps lock sono ç, è, à, e é in BIOS Pre-boot Security.	ç, è, à, e é con caps lock sono ç, è, à, e é in HP Drive Encryption.

Lingua	Windows	BIOS	Drive Encryption
Spagnolo	40a non è supportato, ma funziona comunque perché il software lo converte in c0a. Tuttavia, a causa delle differenze minime tra i layout di tastiera, si consiglia agli utenti di lingua spagnola di passare al layout Windows in 1040a (Spagnolo (varianti)) o 080a (latino americano).	n/a	n/a
USA internazionale	◦ I tasti ¡, ¤, ‘, ’, ¥, e × nella prima fila vengono rifiutati. ◦ I tasti å, ®, e Þ nella seconda fila vengono rifiutati. ◦ I tasti á, ð, e ø nella terza fila vengono rifiutati. ◦ Il tasto æ nell'ultima fila viene rifiutato.	n/a	n/a
Ceco	◦ Il tasto ğ viene rifiutato. ◦ Il tasto į viene rifiutato. ◦ Il tasto ų viene rifiutato. ◦ I tasti ė, ı, e ż vengono rifiutati. ◦ I tasti ġ, ķ, ļ, ņ, e ŗ vengono rifiutati.	n/a	n/a
Slovacco	Il tasto ż viene rifiutato.	◦ I tasti š, ś, e ş; vengono rifiutati al momento della digitazione, ma vengono accettati quando immessi con la tastiera software. ◦ Il tasto ţ senza funzione associata genera due caratteri.	n/a
Ungherese	Il tasto ż viene rifiutato.	Il tasto ţ senza funzione associata genera due caratteri.	n/a

Lingua	Windows	BIOS	Drive Encryption
Sloveno	Il tasto żŻ viene rifiutato in Windows e il tasto alt genera un tasto senza funzione associata nel BIOS.	I tasti ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, e Š vengono rifiutati nel BIOS.	n/a
Giapponese	Se disponibile, si consiglia di preferire IME per Microsoft Office 2007. Nonostante il nome IME, si tratta effettivamente di un layout di tastiera 411, che è supportato.	n/a	n/a

Glossario

accesso al sistema
Oggetto di Security Manager che consiste in un nome utente e una password (e possibilmente altre informazioni selezionate) utilizzabili per eseguire l'accesso ai siti Web o ad altri programmi.

account di rete
Account amministratore o utente Windows in un computer locale, in un gruppo di lavoro o in un dominio.

account utente di Windows
Profilo di un utente autorizzato ad accedere a una rete o a un singolo computer.

amministratore
Vedere *Amministratore Windows*.

amministratore Windows
Utente che dispone di privilegi completi per la modifica delle autorizzazioni e la gestione di altri utenti.

archivio per il ripristino di emergenza
Area di memorizzazione protetta che consente di ricrittografare le chiavi utente di base da una chiave di proprietario di piattaforma all'altra.

attivazione
Questa operazione deve essere eseguita per poter accedere a qualsiasi funzione di Drive Encryption. Drive Encryption viene attivato utilizzando l'installazione guidata di HP ProtectTools. L'attivazione di Drive Encryption può essere eseguita esclusivamente da un amministratore. Il processo di attivazione comprende l'attivazione del software, la crittografia dell'unità disco, la creazione di un account utente e la creazione della chiave di crittografia di backup iniziale su un dispositivo di archiviazione rimovibile.

autenticazione
Processo che verifica se un utente è autorizzato a eseguire un'attività, ad esempio l'accesso al computer, la modifica delle impostazioni per un determinato programma o la visualizzazione di dati protetti.

autenticazione di accensione
Funzionalità di protezione che richiede alcune forme di autenticazione, ad esempio una smart card, un chip di protezione o la password all'accensione del computer.

Autorità di certificazione (CA)
Servizio che rilascia i certificati richiesti per eseguire un'infrastruttura di chiavi pubbliche.

backup
Utilizzare la funzione di backup per salvare una copia di informazioni importanti del programma in un'ubicazione esterna al programma. Utilizzarla quindi per ripristinare le informazioni in un secondo momento sullo stesso o un altro computer.

biometrica
Categoria delle credenziali di autenticazione che prevede l'utilizzo di una funzionalità fisica, come l'impronta digitale, per identificare un utente.

chip di protezione integrato TPM (Trusted Platform Module)
Termine generico per il chip di HP ProtectTools Embedded Security. Un chip TPM esegue l'autenticazione di un computer anziché di un utente memorizzando specifiche informazioni sul sistema host, ad esempio chiavi di crittografia, certificati digitali e password. Un TPM minimizza il rischio di compromissione delle informazioni sul computer in caso di furto o di un attacco da parte di un hacker esterno.

classe periferica

Tutte le periferiche di un tipo particolare, ad esempio le unità.

Console amministrativa
Posizione centrale da cui gli amministratori possono accedere e gestire le funzioni e le impostazioni in HP ProtectTools.

credenziali
Mezzi attraverso cui un utente dimostra la propria idoneità all'esecuzione di una determinata attività nel processo di autenticazione.

criterio di controllo di accesso alla periferica
Elenco di periferiche a cui l'utente può o non può accedere.

crittografia
Modalità di crittografia e decrittografia dei dati che ne contente la decodifica soltanto da parte di individui specifici.

crittografia
Procedura, ad esempio l'utilizzo di un algoritmo, impiegata nella crittografia per convertire testo semplice in testo cifrato per impedirne la lettura a destinatari non autorizzati. La crittografia dei dati è alla base della protezione di rete ed è disponibile in diversi tipi, i più comuni dei quali includono Data Encryption Standard e la crittografia a chiave pubblica.

cryptographic service provider (CSP)
Fornitore di algoritmi crittografici che può essere utilizzato in un'interfaccia ben definita per eseguire determinate funzioni crittografiche.

decrittografia
Procedura utilizzata nella crittografia per convertire i dati crittografati in testo semplice.

dominio
Gruppo di computer appartenenti alla rete che condividono un database di directory comune. I domini sono denominati in modo univoco e ciascuno di essi dispone di un set di regole e procedure comuni.

Drive Encryption
Protegge i dati crittografando i dischi rigidi, rendendo illeggibili i dati da coloro che non dispongono dell'adeguata autorizzazione.

DriveLock
Funzionalità di protezione che collega l'unità disco rigido a un utente, a cui richiede di digitare correttamente la password DriveLock all'accensione del computer.

Encryption File System (EFS)
Sistema che esegue la crittografia di tutti i file e di tutte le sottocartelle all'interno della cartella selezionata.

gruppo
Gruppo di utenti con lo stesso livello di accesso o divieto di accesso a una classe di periferiche o a una periferica specifica.

identità
In HP ProtectTools Security Manager, un gruppo di credenziali e impostazioni gestito come un account o un profilo per un determinato utente.

impronta digitale
Un'estrazione digitale dell'immagine dell'impronta digitale. L'immagine effettiva dell'impronta digitale non viene mai memorizzata da Security Manager.

JITA
autenticazione Just-in-time.

metodo di accesso di protezione

Il metodo utilizzato per accedere al computer.

modalità periferica SATA
Modalità di trasferimento dei dati tra un computer e dispositivi di archiviazione di massa, ad esempio unità disco rigido e ottiche.

password revocata
Password creata quando un utente richiede un certificato digitale. La password viene richiesta quando un utente desidera revocare un certificato digitale e assicura che solo l'utente sia in grado di revocare il certificato.

PIN
Numero identificativo personale.

PKI
Standard di infrastruttura di chiave pubblica che definisce l'interfaccia per la creazione, l'utilizzo e l'amministrazione dei certificati e delle chiavi di crittografia.

protezione di accesso Windows
Protegge gli account Windows mediante richiesta dell'uso di credenziali specifiche per l'accesso.

riavvio
Processo di riavvio del computer.

ripristino
Processo che copia i dati di programma da un file di backup salvato in precedenza in questo programma.

Ripristino con HP SpareKey
Funzione di accesso al computer mediante risposta corretta a domande di sicurezza.

risorsa
Componente dati situato sull'unità disco rigido e costituito da informazioni o file personali, dati cronologici e relativi al Web, e così via.

scena
Immagine di un utente registrato da utilizzare per l'autenticazione.

scheda ID
Gadget di Windows che serve a identificare visivamente il desktop con il nome utente e l'immagine selezionata.

schermata di accesso di Drive Encryption
Schermata di accesso che viene visualizzata prima dell'avvio di Windows. Gli utenti devono immettere il nome utente e la password Windows oppure il PIN della smart card. Nella maggior parte dei casi, l'immissione delle informazioni corrette nella finestra di accesso di Drive Encryption consente l'accesso diretto a Windows, senza dover ripetere la procedura nella relativa schermata.

servizio in backgroung
servizio in background Controllo/blocco dispositivi HP ProtectTools che deve essere in esecuzione per poter applicare i criteri di controllo dell'accesso alle periferiche. Questo servizio può essere visualizzato dall'applicazione Servizi sotto l'opzione Strumenti di amministrazione nel Pannello di controllo. Se il servizio non è attivo, HP Protect Tools Security Manager tenterà di avviarlo durante l'applicazione dei criteri di controllo dell'accesso alle periferiche.

Single Sign-on
Funzionalità che memorizza le informazioni di autenticazione e consente all'utente di utilizzare Security Manager per accedere a Internet e alle applicazioni Windows che richiedono l'autenticazione tramite password.

smart card
Piccolo componente hardware, simile per dimensione e forma a una carta di credito, in cui sono memorizzate le informazioni di identificazione relative al proprietario. Viene utilizzata per l'autenticazione del proprietario su un computer.

TXT
Trusted Execution Technology.

utente
Per utente si intende chiunque sia registrato in Drive Encryption. Gli utenti non in possesso dei privilegi di amministratore dispongono di diritti limitati in Drive Encryption. Possono solo registrarsi (con l'approvazione dell'amministratore) ed effettuare l'accesso.

Indice analitico

T

U

V