Software di protezione HP ProtectTools per le piccole imprese, versione 5.10

Guida per l'utente

Guida per l'utente del software di protezione HP ProtectTools per le piccole imprese, versione 5.10

PC aziendali HP

Seconda edizione: maggio 2010

Numero di parte del documento: 610663-062

Informazioni su questa guida

Questa guida contiene informazioni sul software di protezione HP ProtectTools per le piccole imprese.

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

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

NOTA: il testo presentato in questo modo indica che vengono fornite importanti informazioni supplementari.

Sommario

1 Introduzione alle modalità di protezione

HP sa bene che per le aziende il tempo è una risorsa preziosa da investire concentrandosi sul business e sulla sua crescita, anziché preoccupandosi del software adeguato alla protezione dell'organizzazione, dei computer e dei dati aziendali.

È importante che le aziende considerino in modo proattivo l'impiego di soluzioni di sicurezza che siano facili da usare e al tempo stesso efficaci nel proteggere le risorse aziendali. La sicurezza è una componente essenziale del business e non un'opzione facoltativa.

HP ProtectTools per le piccole imprese è la soluzione software per la protezione con cui HP risponde alle esigenze di facilità d'implementazione e d'uso.

HP ProtectTools per le piccole imprese offre funzionalità di sicurezza rivolte a proteggere i computer e i dati critici dall'accesso non autorizzato. La funzionalità di protezione avanzata viene garantita dai diversi moduli software di HP ProtectTools.

L'offerta di HP ProtectTools per le piccole imprese prevede due versioni: Console amministrativa di HP ProtectTools Security Manager e HP ProtectTools Security Manager (per tutti gli utenti). Entrambe le versioni sono accessibili dal menu **Start** > **Tutti i programmi**.

Funzione	Caratteristiche
Console amministrativa di HP ProtectTools Security Manager	• Richiede i diritti di accesso di amministratore di Microsoft Windows • Accesso ai moduli configurato da un amministratore e non disponibile per gli utenti • Consente di eseguire le impostazioni iniziali di protezione e di configurare le opzioni o i requisiti per tutti gli utenti
HP ProtectTools Security Manager (per tutti gli utenti)	• Consente agli utenti di configurare le opzioni fornite da un amministratore • Consente di limitare l'accesso e di consentire solo un accesso limitato ad alcuni moduli di HP ProtectTools

I moduli software di HP ProtectTools possono essere preinstallati, precaricati oppure sono disponibili come opzione configurabile o opzione da acquistare a parte. Per ulteriori informazioni, visitare il sito http://www.hp.com.

Funzioni di HP ProtectTools

Nella seguente tabella vengono riportate le funzioni principali dei moduli HP ProtectTools per le piccole imprese:

Modulo	Funzioni principali
Console amministrativa di HP ProtectTools Security Manager	• La procedura di configurazione guidata di Security Manager consente agli amministratori di impostare e configurare i livelli di sicurezza e i metodi di accesso di sicurezza. • Configurazione di opzioni non accessibili agli utenti di base. • Configurazione di Device Access Manager e dell'accesso utente. • Gli strumenti di amministrazione consentono di aggiungere e rimuovere gli utenti di HP ProtectTools, nonché di visualizzare lo stato degli utenti.
HP ProtectTools Security Manager (per tutti gli utenti)	• Organizzazione, impostazione e modifica di nomi utente e password. • Configurazione e modifica di credenziali utente quali password di Windows e smart card. • Configurazione e modifica delle impostazioni e della distruzione e pulizia dei file in File Sanitizer. • Visualizzazione delle impostazioni di Device Access Manager. • Configurazione di opzioni relative a preferenze, backup e ripristino.
Credential Manager for HP ProtectTools (Gestore password)	• Progettato per salvare, organizzare e proteggere i nomi utente e le password. • Consente di impostare le schermate di accesso dei siti Web e dei programmi per accedervi in maniera più rapida e sicura. • Grazie a Gestore password, è possibile salvare il nome utente e le password utilizzate di volta in volta per accedere ai diversi siti Web ed evitare così di doverle ricordare. La prossima volta che si accede a un sito Web, Gestore password completerà i campi e invierà i dati in modo automatico. • Consente di creare password più sicure che non sarà necessario annotare o ricordare, e di aumentare la protezione dei propri account.
Drive Encryption for HP ProtectTools	• Fornisce la crittografia completa di tutto il volume dell'unità. • Forza l'autenticazione prima dell'avvio al fine di decrittografare e accedere ai dati sul disco rigido. • Consente di conformarsi ai requisiti legali o di settore relativi alla protezione dei dati riservati. • Protegge i dati dall'accesso non autorizzato mediante la crittografia di tutta l'unità disco rigido. Se il PC viene rubato e l'unità viene rimossa dal sistema originale e installata in un altro sistema, i dati non verranno compromessi.

Modulo	Funzioni principali
File Sanitizer for HP ProtectTools	• L'eliminazione dei dati in Windows non comporta la rimozione completa dei contenuti dall'unità disco rigido. Windows cancella soltanto il riferimento ai dati, i quali rimangono nell'unità disco rigido finché non vengono sovrascritti da altri file con nuove informazioni. Tuttavia, con File Sanitizer è possibile cancellare completamente e automaticamente documenti, cronologia del browser Web, file temporanei e così via. • Consente di cancellare (o distruggere) in modo sicuro i file e le cartelle critici (informazioni o file personali, dati cronologici o relativi al Web o altri componenti di dati) presenti sul computer ed eseguire la pulizia periodica del disco rigido (sovrascrittura dei dati eliminati in precedenza).
Device Access Manager for HP ProtectTools	• Può essere utilizzato per controllare l'accesso alle unità multimediali, USB e altri dispositivi hardware in base a profili utente. • Consente di limitare la capacità di un utente di memorizzare dati critici. • Impedisce agli utenti di utilizzare dispositivi di archiviazione esterni, ad esempio i lettori musicali personali, per copiare i dati da un computer o dalla rete. • Impedisce agli utenti di introdurre virus nel sistema da supporti esterni. • Consente di disattivare in modo selettivo un gruppo di dispositivi (ad esempio chiavi USB, dispositivi scrivibili, lettori musicali personali e così via) in base all'utente o al gruppo di utenti. Solo l'utente che dispone di una password di amministratore può eseguire l'accesso e copiare le informazioni dal computer.

2 Guida all'impostazione semplificata delle opzioni più utili

In questa guida vengono illustrati i passaggi di base per l'attivazione delle opzioni più utili e comuni presenti in HP ProtectTools per le piccole imprese. Il software include numerosi strumenti e opzioni rivolti a ottimizzare le preferenze personali e impostare il controllo dell'accesso. La guida descrive le procedure per rendere operativo ciascun modulo nel minor tempo possibile e con il minor numero di passaggi di configurazione. Per ulteriori informazioni, selezionare il modulo desiderato e fare clic sul pulsante "?" o Guida nell'angolo superiore destro. Questo pulsante consente di mostrare in modo automatico le informazioni relative alla finestra attualmente visualizzata.

Informazioni preliminari

1. Aprire HP ProtectTools Security Manager dall'icona Gadget, dall'icona della barra delle applicazioni (scudo dorato) oppure fare clic su **Start** > **Tutti i programmi** > **HP**.

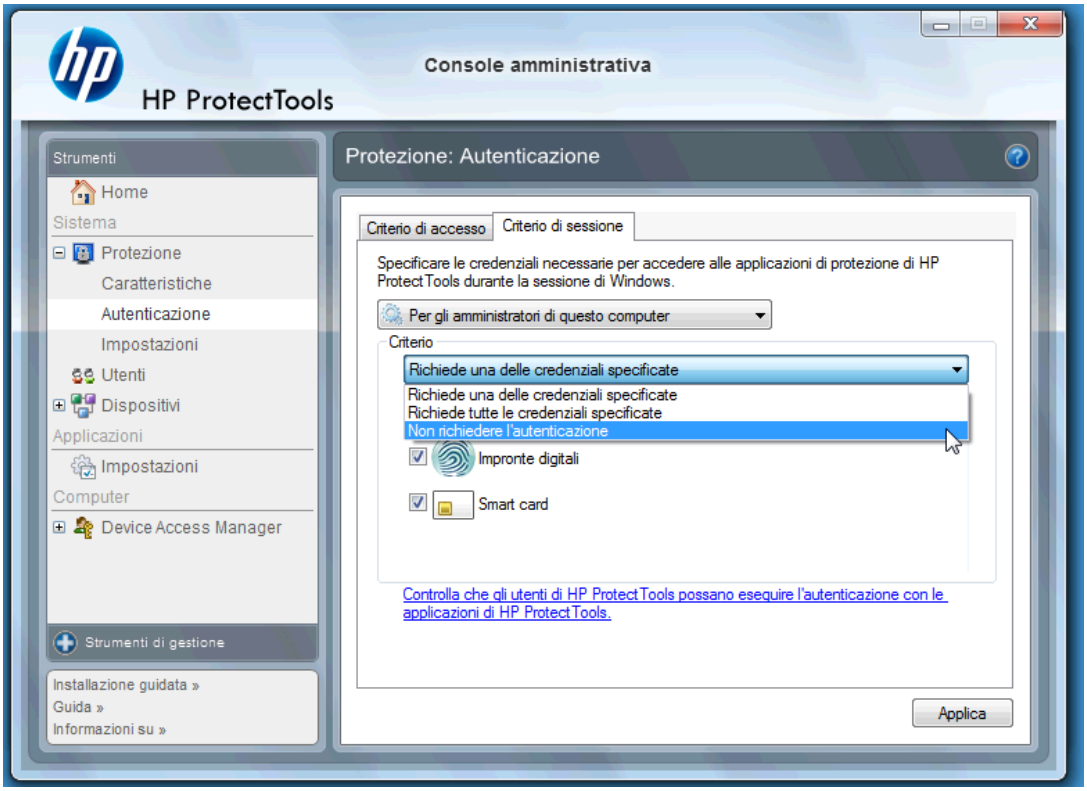
2. Immettere la password di Windows oppure crearne una.

3. Completare la configurazione guidata.

NOTA: per impostazione predefinita, HP ProtectTools Security Manager è impostato sul criterio di autenticazione avanzata.

Questa impostazione è progettata per impedire l'accesso non autorizzato mentre si è connessi a Windows e deve essere utilizzata quando è richiesto un livello di protezione elevato o quando gli utenti si allontanano spesso dai loro sistemi durante la giornata. Per modificare questa impostazione, fare clic sulla scheda Criterio di sessione, quindi effettuare la propria selezione.

Per configurare HP ProtectTools Security Manager in modo da utilizzare soltanto l'accesso a Windows iniziale per tutta la sessione, modificare la seguente configurazione.



Per eseguire l'autenticazione di HP ProtectTools Security Manager soltanto una volta durante la sessione di Windows:

1. Fare clic su **Start** > **Tutti i programmi** > **HP** > **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro **Strumenti**, selezionare **Autenticazione** dal gruppo **Protezione**.
3. Fare clic sulla scheda **Criterio di sessione** e selezionare **Non richiedere l'autenticazione** dall'elenco a discesa **Criterio**.
4. Al termine, fare clic sul pulsante **Applica**.

Credential Manager for HP ProtectTools (Gestore password)

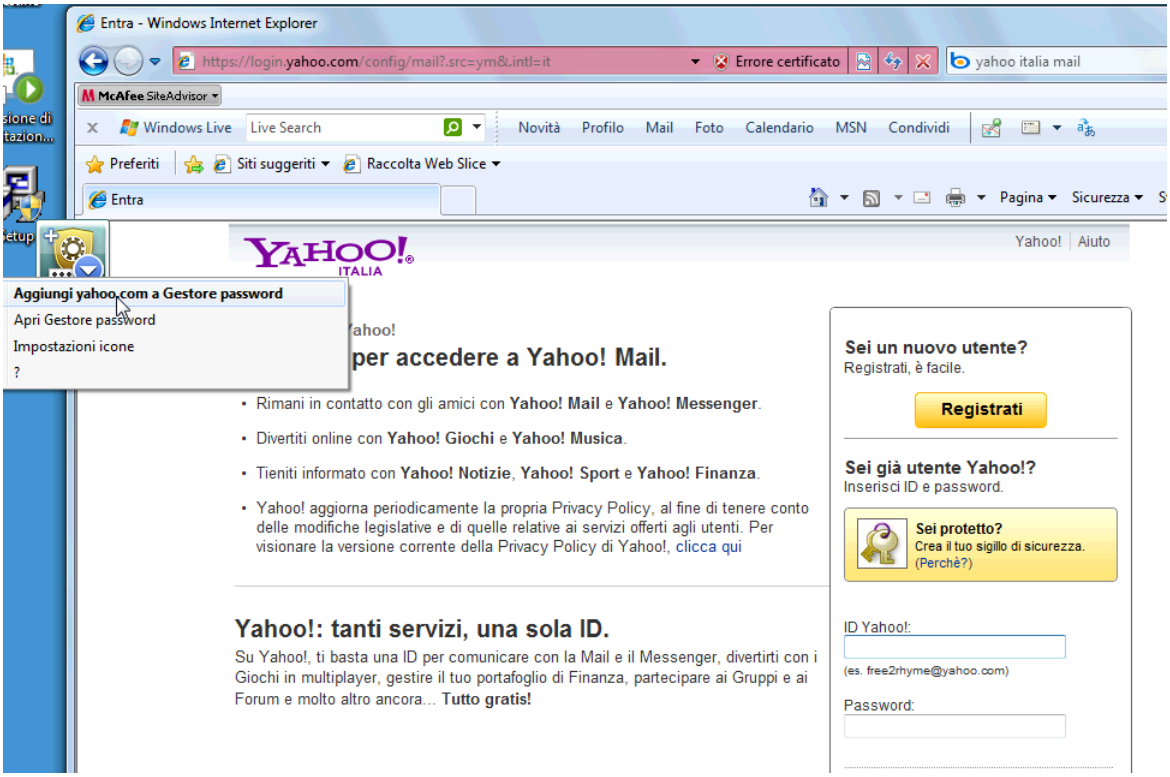
Gli utenti di computer dispongono di un numero elevato di password, soprattutto se accedono regolarmente a siti Web o ad applicazioni che richiedono di eseguire la procedura di accesso. Gli utenti si distinguono in due categorie: quelli che utilizzano la stessa password in tutte le situazioni e quelli più creativi che impiegano password diverse e che prontamente dimenticano a quali applicazioni o siti Web sono associate.

Un software che consente di ricordare automaticamente le password per i siti non critici o di individuare i siti da ricordare e ignorare è Credential Manager for HP ProtectTools. Credential Manager è il gestore delle password che offre questa funzionalità. Una volta eseguito l'accesso al PC, Credential Manager fornisce le password o le credenziali in base a necessità.

Quando si accede a un'applicazione o a un sito Web che richiede l'immissione di credenziali, Credential Manager riconoscerà automaticamente tale sito e chiederà se si desidera memorizzare i dati. Se si accetta, non sarà più necessario ricordare la password. È possibile rifiutare la richiesta di ricordare le credenziali se si desidera escludere determinati siti.

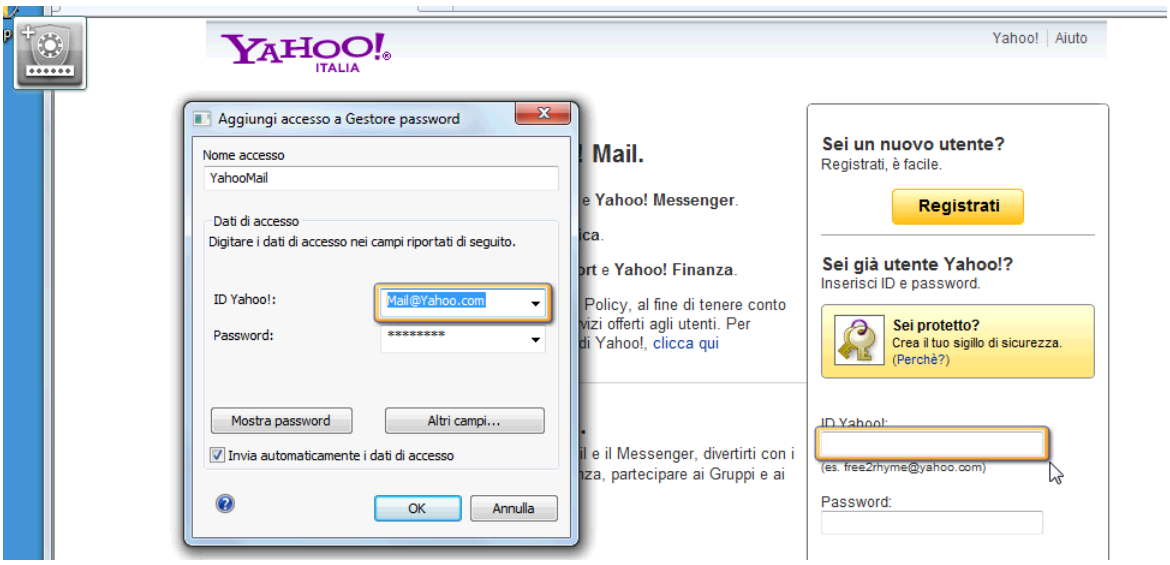
Per iniziare a salvare i siti Web, i nomi utente e le password:

1. Spostarsi ad esempio al proprio account di posta sul Web e fare clic sull'icona di Credential Manager per aggiungere l'autenticazione Web.



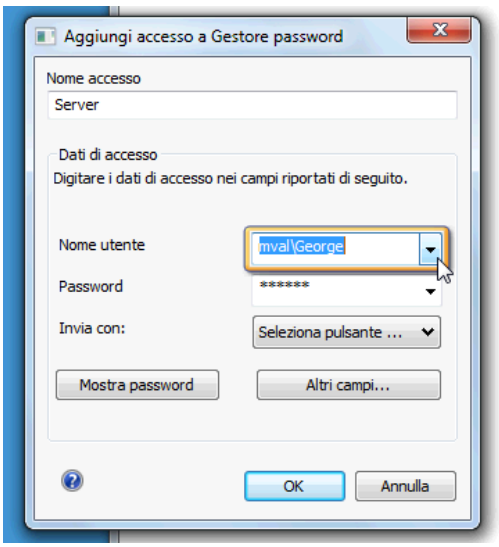
2. Assegnare un nome al collegamento (facoltativo) e immettere un nome utente e una password in Credential Manager.

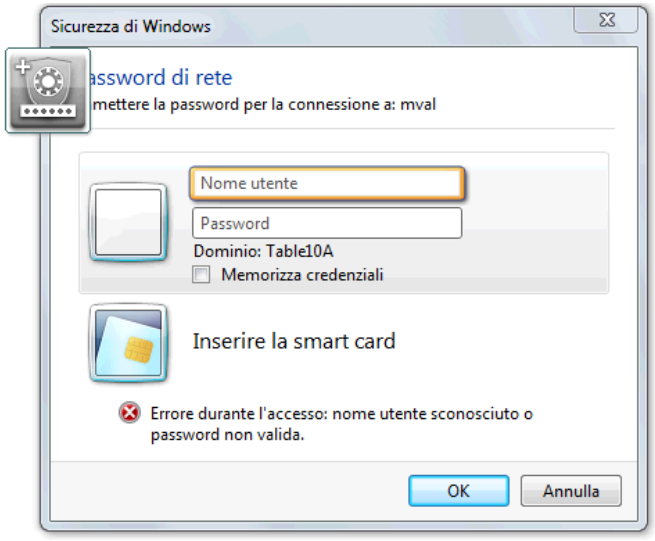
NOTA: nella pagina Web verranno evidenziate le aree che Credential Manager utilizzerà in occasione di questa visita e di quelle successive.



3. Al termine, fare clic sul pulsante **OK**.

4. Credential Manager può anche salvare il nome utente e le password per le condivisioni di rete o la mappatura delle unità di rete.





Visualizzazione e gestione delle autenticazioni salvate in Credential Manager

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

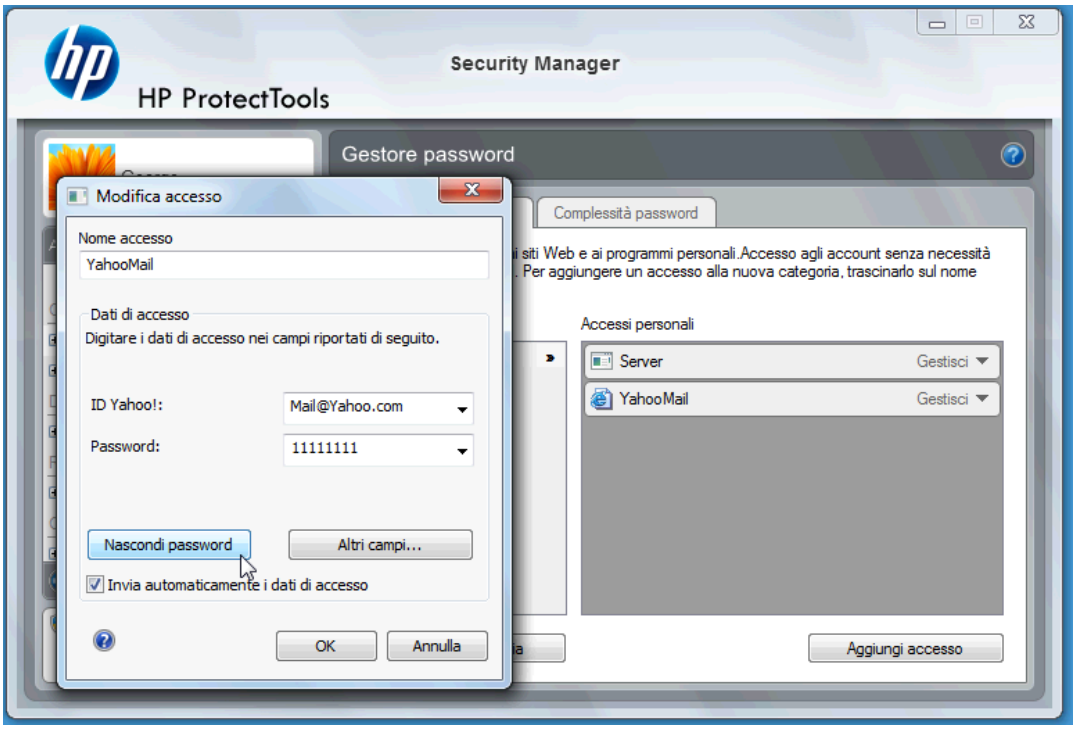
Per aprire Gestore password, utilizzare uno dei due seguenti metodi:

- Utilizzare la combinazione di tasti Ctrl + Windows + H per aprire Gestore password. Selezionare **Apri** per avviare e autenticare il collegamento in modo rapido.

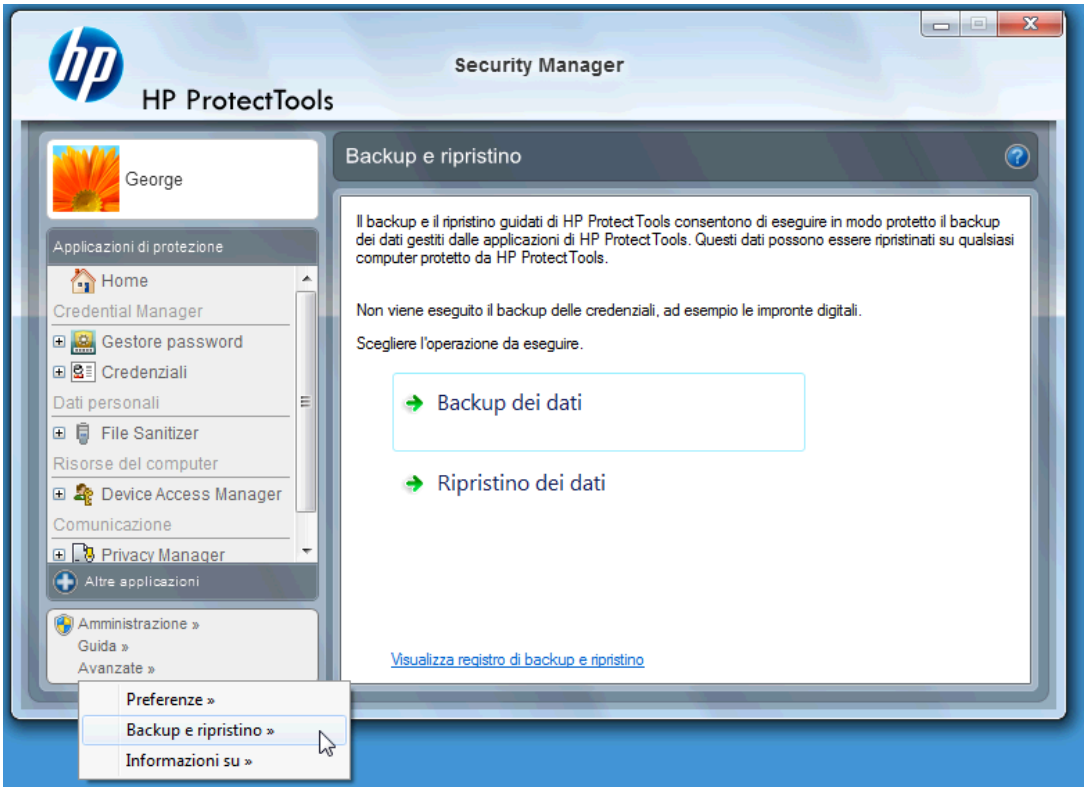
OPPURE

- Selezionare la scheda **Gestisci** in Gestore password per aprire HP ProtectTools Security Manager e modificare le credenziali.

L'opzione **Modifica** di Credential Manager consente di visualizzare e modificare il nome e il nome di accesso, nonché di mostrare le password.



HP ProtectTools per le piccole imprese consente di eseguire il backup e/o la copia di tutte le credenziali e impostazioni in un altro computer.


Security Manager
HP ProtectTools
George
Backup e ripristino
Applicazioni di protezione
Home
Credential Manager
Gestore password
Credenziali
Dati personali
File Sanitizer
Risorse del computer
Device Access Manager
Comunicazione
Privacy Manager
Altre applicazioni
Amministrazione »
Guida »
Avanzate »
Preferenze »
Backup e ripristino »
Informazioni su »
Il backup e il ripristino guidati di HP ProtectTools consentono di eseguire in modo protetto il backup dei dati gestiti dalle applicazioni di HP ProtectTools. Questi dati possono essere ripristinati su qualsiasi computer protetto da HP ProtectTools.
Non viene eseguito il backup delle credenziali, ad esempio le impronte digitali.
Scegliere l'operazione da eseguire.
Backup dei dati
Ripristino dei dati
Visualizza registro di backup e ripristino

File Sanitizer for HP ProtectTools

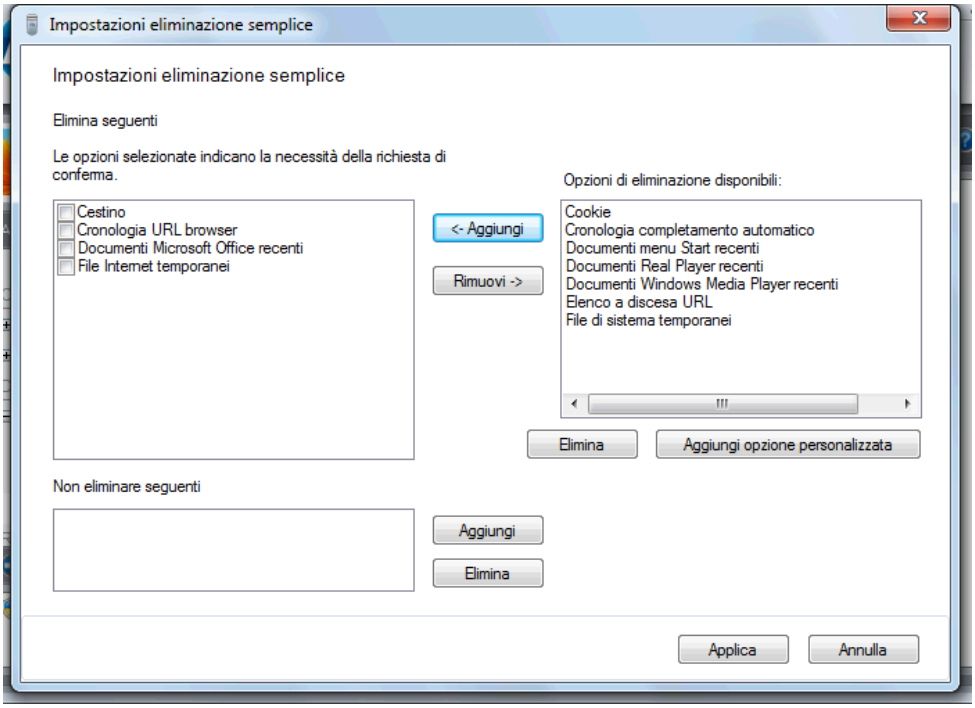
File Sanitizer è progettato per impedire a un utente non autorizzato di recuperare i dati eliminati. Sono disponibili diverse opzioni che consentono di eliminare, sia manualmente che in base a una pianificazione periodica, file e cartelle selezionati, inclusa la cronologia del browser.

Di seguito sono riportate alcune impostazioni di configurazione di base.

Per avviare l'eliminazione permanente dei dati eliminati, selezionare il file o le cartelle non più necessarie.

1. Spostarsi a **Security Manager** > **File Sanitizer** > **Impostazioni**. Selezionare **Impostazioni eliminazione semplice** e fare clic sul pulsante **Visualizza dettagli**.

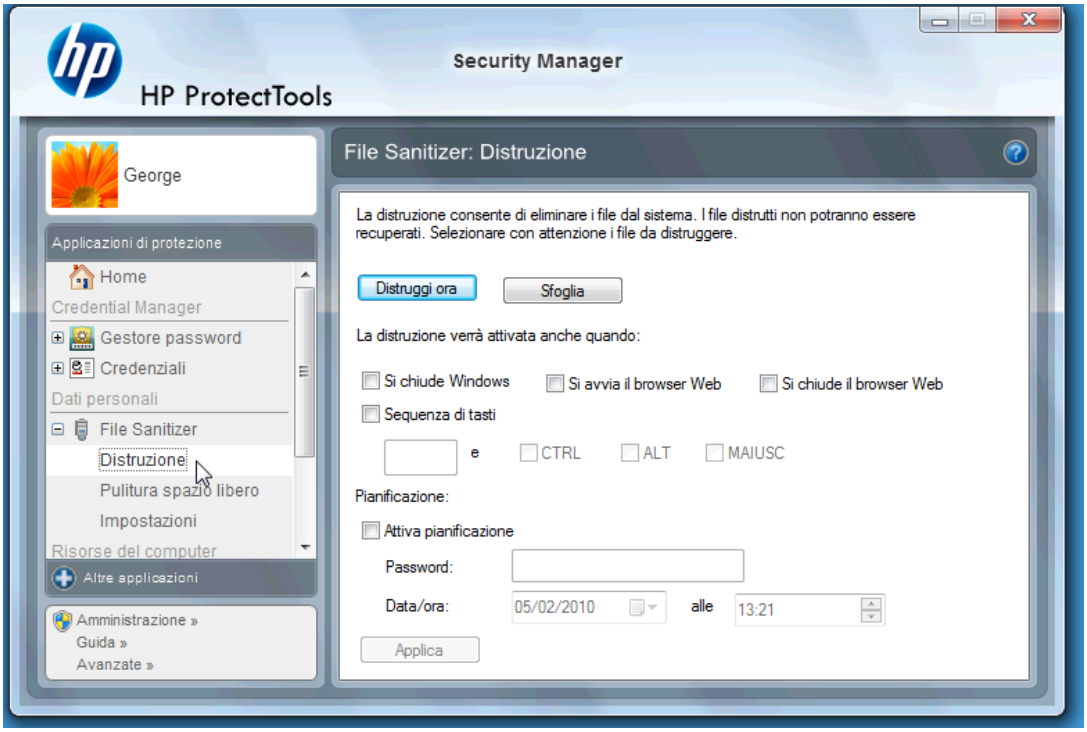
2. Selezionare gli elementi a destra della finestra Impostazioni eliminazione semplice che si desidera eliminare in modo permanente su base regolare, quindi fare clic sul pulsante **<-Aggiungi** per spostare gli elementi selezionati in Elimina seguenti.



3. Avviare il Cestino e aggiungere altri elementi da eliminare tramite la distruzione.

4. Fare clic sul pulsante **Applica** dopo aver selezionato tutti gli elementi da eliminare in modo permanente.

5. Spostarsi all'opzione **Distruzione** e configurare la data e l'ora di esecuzione dell'operazione. Il pulsante **Distruggi ora** cancellerà immediatamente gli elementi selezionati nella finestra Impostazioni eliminazione semplice appena configurata.



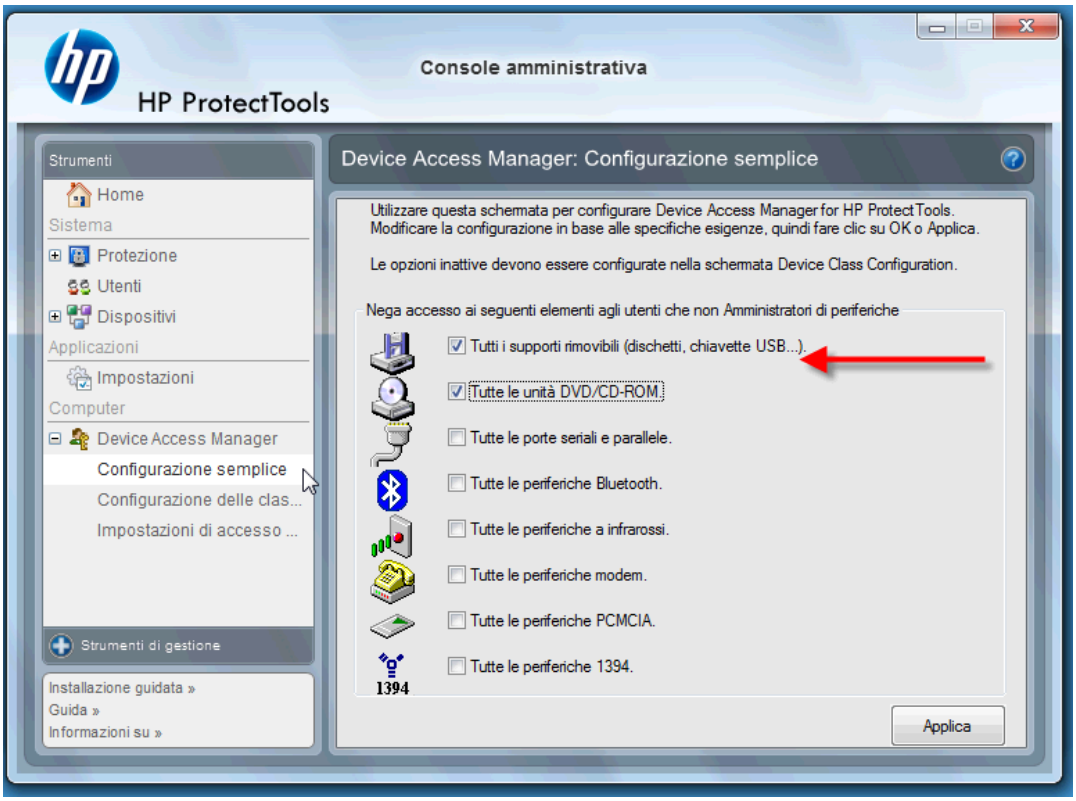
6. Nella barra delle applicazioni verrà visualizzato un piccolo popup ogni volta che viene avviata e completata la procedura di distruzione.

Device Access Manager for HP ProtectTools

Device Access Manager può essere utilizzato per limitare l'utilizzo di diversi dispositivi di archiviazione esterni e interni e quindi proteggere i dati, che rimarranno al sicuro sull'unità disco rigido e all'interno dell'azienda. Ad esempio, si potrebbe consentire a un utente di accedere ai dati, ma impedirgli di copiarli su un CD, lettore musicale personale o dispositivo di archiviazione USB. Di seguito vengono descritti i pochi passaggi di questa configurazione.

1. Fare clic su **Start** > **Tutti i programmi** > **HP** > **Console amministrativa** > **Device Access Manager** > **Configurazione semplice**.

2. Selezionare i dispositivi hardware da bloccare e fare clic sul pulsante **Applica** per terminare il processo.

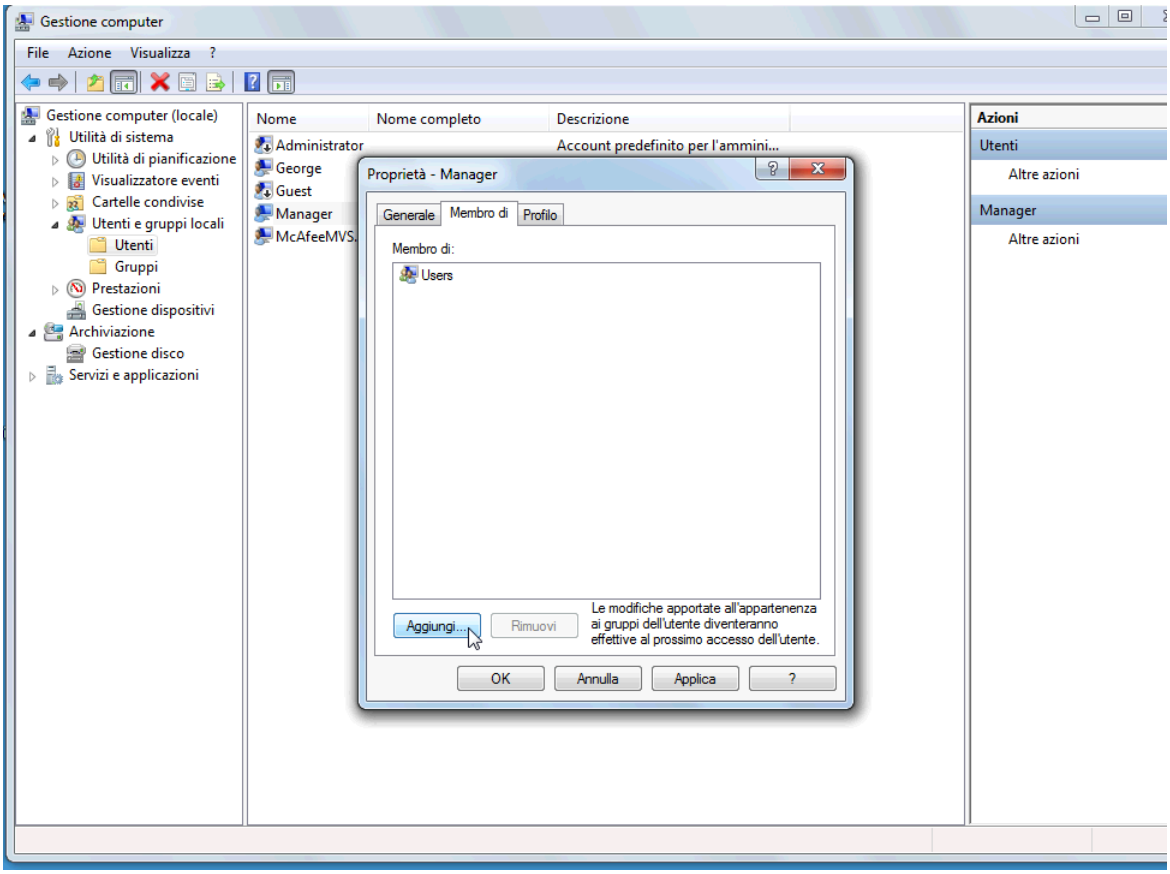


3. Il passo successivo prevede la selezione degli utenti che continueranno a poter accedere ai dispositivi bloccati.

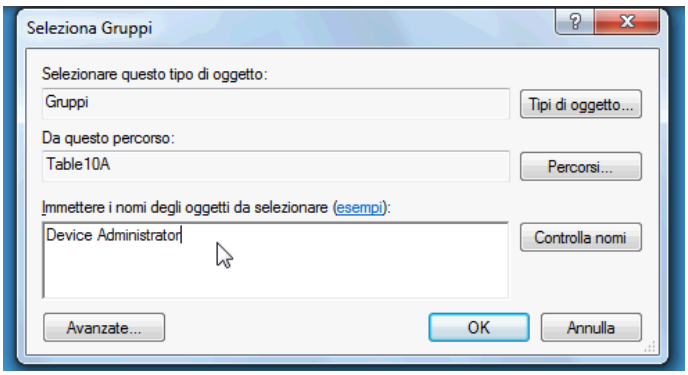
4. Selezionare **Risorse del computer**, fare clic con il pulsante destro del mouse su **Gestisci** > **Gestione computer** > **Utilità di sistema** > **Utenti e gruppi locali** > **Utenti**.

5. Fare doppio clic sull'utente (in questo esempio "Manager") a cui consentire l'accesso all'hardware bloccato.

6. Nella scheda **Membro di**, fare clic sul pulsante **Aggiungi**.



7. Nella finestra **Seleziona Gruppi** è possibile utilizzare l'opzione **Avanzate** o semplicemente digitare "Device Administrator". Fare clic sul pulsante **OK**, quindi su tutti i pulsanti OK che vengono visualizzati fino alla chiusura delle finestre. Per ottenere le autorizzazioni, è necessario disconnettersi e connettersi di nuovo.



A questo punto, tutte le unità di archiviazione esterne e interne, inclusi le unità CD e USB, i lettori musicali personali e così via, funzioneranno solo per gli utenti inclusi nel gruppo "Device Administrator".

Drive Encryption for HP ProtectTools

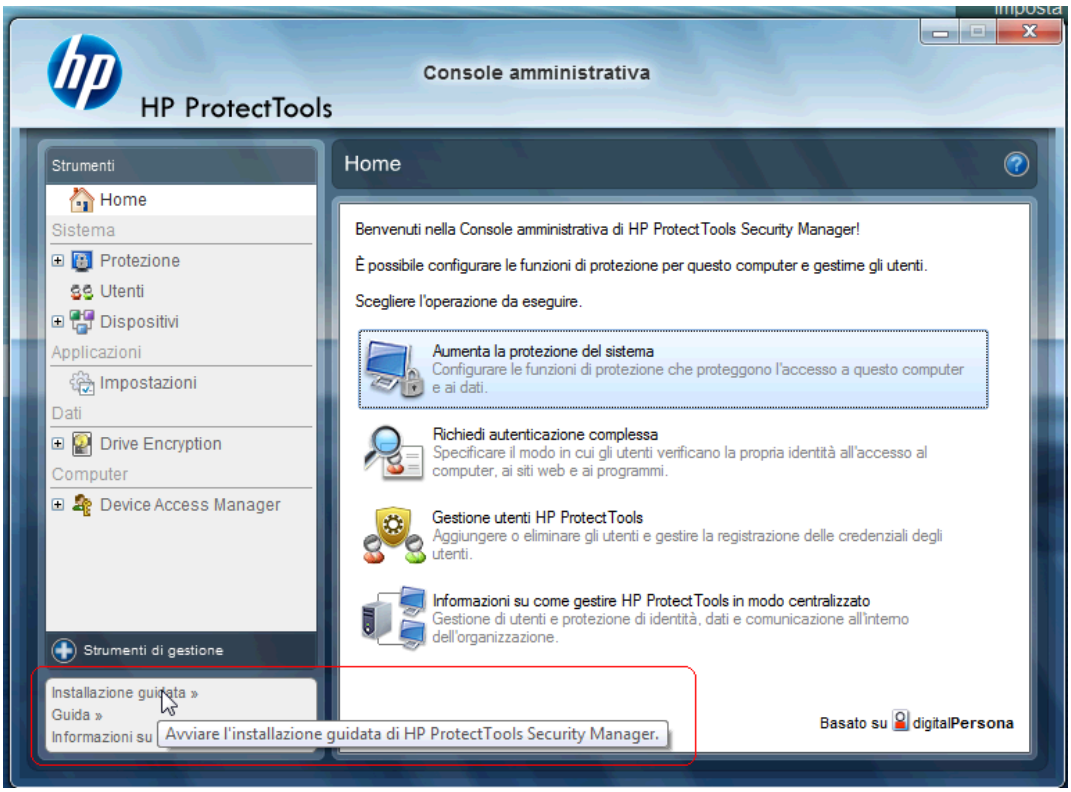
Drive Encryption for HP ProtectTools è un software che viene utilizzato per proteggere i dati mediante la crittografia dell'intera unità disco rigido. I dati sull'unità disco rigido rimarranno protetti in caso di furto del PC e/o di rimozione dell'unità disco rigido dal sistema originale e installazione in un altro sistema.

Per proteggere ulteriormente i dati, Drive Encryption richiede all'utente di eseguire l'opportuna procedura di autenticazione tramite l'immissione del nome utente e della password prima dell'avvio del sistema. Questo processo è chiamato Autenticazione di preavvio.

Un altro aspetto vantaggioso è che gli utenti di Windows, i domini, Credential Manager for HP ProtectTools e HP ProtectTools Security Manager si interfacciano tutti con Drive Encryption per consentire la sincronizzazione semplificata delle password.

Per attivare Drive Encryption for HP ProtectTools, eseguire questi semplici passaggi.

1. Fare clic su **Start** > **Tutti i programmi** > **HP** > **Console amministrativa di HP ProtectTools** > **Strumenti di gestione** > **Impostazione guidata**. Viene visualizzata la seguente schermata.



2. Scegliere **Avanti** nella schermata iniziale.
3. Per avviare l'attivazione guidata, è necessaria la password di Windows. Fare clic su **Avanti**.
4. Selezionare la casella **Drive Encryption**, quindi **Avanti**.

5. Nella finestra di configurazione di Drive Encryption riportata di seguito vengono visualizzate le unità disponibili per la crittografia e viene richiesta un'unità flash USB in cui memorizzare la chiave di ripristino della crittografia. Conservare la chiave in un luogo sicuro, in quanto viene utilizzata per ripristinare i dati o accedere all'unità in caso di perdita o errore della password di preavvio.

6. Selezionare **Avanti**, completare la procedura e selezionare **Fine**. Quando richiesto, rimuovere l'unità flash USB e riavviare il sistema non appena si è pronti.

7. Quando il sistema viene avviato dall'unità disco rigido, Drive Encryption richiederà la password di Windows. Immettere la password, quindi fare clic su **OK**.

NOTA: durante la crittografia dell'unità, le prestazioni del computer possono risultare rallentate. Una volta completata la crittografia, il sistema tornerà a funzionare normalmente. I dati presenti sull'unità verranno crittografati o decrittografati in base a necessità man mano che vi si accede.

Inoltre, tenere presente che l'autenticazione di Drive Encryption "collegherà" attraverso l'accesso di Windows di Credential Manager direttamente al desktop senza dover immettere la password due volte.

3 Vantaggi di HP ProtectTools per le piccole imprese

Accesso a HP ProtectTools per le piccole imprese

Per accedere a HP ProtectTools Security Manager dal menu Start di Windows:

- In Windows, fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **HP ProtectTools Security Manager**.

Per accedere alla Console amministrativa di HP ProtectTools Security Manager dal menu Start di Windows:

- In Windows, fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.

Raggiungimento degli obiettivi chiave relativi alla protezione

I moduli di HP ProtectTools possono lavorare in combinazione per fornire soluzioni in grado di soddisfare varie problematiche relative alla protezione, inclusi i seguenti obiettivi chiave:

- Limitazione dell'accesso ai dati sensibili
- Blocco degli accessi non autorizzati dall'interno o dall'esterno della sede
- Creazione di criteri per password sicure

Limitazione dell'accesso ai dati sensibili

Si supponga che un revisore esterno lavori in sede e abbia ricevuto l'accesso ai computer per analizzare dati finanziari sensibili; non si desidera che il revisore possa stampare i file o salvarli su un dispositivo di scrittura quale ad esempio un CD. La funzione seguente consente di limitare l'accesso ai dati:

Device Access Manager for HP ProtectTools consente agli amministratori di limitare l'accesso ai dispositivi scrivibili per impedire la stampa o la copia dei dati riservati dal disco rigido a supporti rimovibili. Vedere Configurazione delle classi di periferiche (avanzata) a pagina 49.

Blocco degli accessi non autorizzati dall'interno o dall'esterno della sede

L'accesso non autorizzato a un PC aziendale non protetto rappresenta un rischio molto tangibile per dati critici quali informazioni di servizi finanziari, dirigenti o del team di ricerca e sviluppo o per dati

personali quali cartelle mediche o dati finanziari personali. Le funzioni seguenti consentono di impedire l'accesso non autorizzato:

- La funzione di autenticazione prima dell'avvio, se abilitata, consente di impedire l'accesso al sistema operativo. Vedere i seguenti capitoli:
  - Credential Manager for HP ProtectTools (Gestore password) a pagina 36
  - Drive Encryption for HP ProtectTools a pagina 33
- Credential Manager for HP ProtectTools consente di impedire che un utente non autorizzato possa ottenere le password o l'accesso ad applicazioni protette da password. Vedere il seguente capitolo:
  - Credential Manager for HP ProtectTools (Gestore password) a pagina 36
- Device Access Manager for HP ProtectTools consente agli amministratori di limitare l'accesso ai dispositivi scrivibili per impedire la copia dei dati riservati dal disco rigido. Vedere il seguente capitolo:
  - Device Access Manager for HP ProtectTools a pagina 48
- File Sanitizer consente di eliminare i dati in modo sicuro distruggendo i file e le cartelle critici o ripulendo il disco rigido (sovrascrivendo i dati eliminati in precedenza ma che sono ancora presenti sul disco, in modo da renderne più difficile il recupero). Vedere il seguente capitolo:
  - File Sanitizer for HP ProtectTools a pagina 41

Creazione di criteri per password sicure

Se si richiede un criterio che prescrive l'utilizzo di password sicure (password difficili da indovinare) per decine di applicazioni e database basati sul Web, Credential Manager for HP ProtectTools fornisce un archivio protetto per le password e la funzione Single Sign On. Vedere il seguente capitolo:

- Credential Manager for HP ProtectTools (Gestore password) a pagina 36

Ulteriori elementi protettivi

Assegnazione dei ruoli di protezione

Per proteggere adeguatamente i dati, è buona prassi suddividere responsabilità e diritti tra i diversi tipi di amministratori e utenti.

NOTA: nel caso di una piccola impresa o di un singolo utente, questi ruoli possono essere ricoperti dalla stessa persona.

In HP ProtectTools per le piccole imprese, le responsabilità e le autorizzazioni di protezione possono essere suddivise nei seguenti ruoli:

- Amministratore: applica e gestisce le funzioni di protezione. Può anche attivare e disattivare alcune funzioni.
- Utente: utilizza le funzioni di protezione.

Gestione delle password di HP ProtectTools

Le funzioni di HP ProtectTools Security Manager sono nella maggior parte dei casi protette da password. La tabella seguente elenca le password comunemente usate, il modulo software in cui la password è impostata e la funzione della password.

In questa tabella vengono anche riportate le password impostate e utilizzate soltanto dagli amministratori. Tutte le altre password possono essere impostate dagli utenti normali.

Password di HP ProtectTools	Modulo di HP ProtectTools in cui è impostata	Funzione
Password di accesso di Gestore password	Gestore password	Questa password è disponibile per 2 opzioni: • Può essere utilizzata separatamente per accedere a Gestore password dopo l'accesso a Windows. • Può essere utilizzata al posto della procedura di accesso a Windows, consentendo di accedere simultaneamente a Windows e a Gestore password.
Password di Impostazione del computer **NOTA:** denominata anche password amministratore del BIOS, password di configurazione F10 o password di configurazione di protezione	BIOS, dall'amministratore	Protegge l'accesso all'utility Impostazione del computer.
Password di accensione	BIOS	Protegge l'accesso al contenuto del computer, quando il computer viene acceso, riavviato o viene disattivato lo stato di sospensione.
Password di accesso a Windows	Pannello di controllo di Windows	Può essere utilizzato per l'accesso manuale.

Creazione di una password di protezione

Quando si creano password, occorre innanzitutto rispettare le specifiche tecniche stabilite dal programma. In linea generale, comunque, considerare quanto segue per creare password complesse e ridurre le possibilità che la password venga compromessa:

- Scegliere password che contengano più di 6 caratteri, preferibilmente più di 8.
- Scegliere una password che contenga sia maiuscole che minuscole.
- Se possibile, usare una combinazione di caratteri alfanumerici e aggiungere caratteri speciali e segni di punteggiatura.
- Sostituire alcune lettere di una parola chiave con caratteri speciali o numeri. Ad esempio, è possibile sostituire la lettera I o L con il numero 1.
- Usare una combinazione di parole appartenenti a 2 o più lingue diverse.
- Inserire numeri o caratteri speciali all'interno di una parola o frase. Ad esempio, “Maria2-2Gatto45”.

- Scegliere una password non elencata nel dizionario.
- Non utilizzare il proprio nome o altre informazioni personali, come la data di nascita, il nome dei propri animali domestici, o il cognome da nubile della propria madre, nemmeno se digitato in senso inverso.
- Modificare le password regolarmente. È possibile modificare solo un paio di caratteri, ad esempio incrementandoli.
- Se si annota la password, non conservarla in un luogo facilmente visibile in prossimità del computer.
- Non salvare la password in un file, come ad esempio un messaggio di posta elettronica, nel computer.
- Non condividere account e non rivelare a nessuno la password.

Backup di credenziali e impostazioni

Utilizzare lo strumento Backup e ripristino in HP ProtectTools Security Manager come posizione centralizzata da cui eseguire backup e ripristini delle credenziali dai moduli di HP ProtectTools installati.

4 Console amministrativa di HP ProtectTools Security Manager

Informazioni sulla Console amministrativa di HP ProtectTools

HP ProtectTools Security Manager viene amministrato attraverso la Console amministrativa.

Utilizzando la console, l'amministratore locale è in grado di:

- Attivare o disattivare funzioni di protezione
- Gestire gli utenti del computer
- Configurare parametri specifici dei dispositivi
- Configurare le applicazioni di Security Manager
- Aggiungere ulteriori applicazioni di Security Manager

Utilizzo della Console amministrativa

La Console amministrativa di Security Manager è il punto di gestione centrale per l'amministrazione di HP ProtectTools Security Manager.

Per aprire la console:

- Selezionare **Start** > **Tutti i programmi** > **Console amministrativa di HP ProtectTools**, oppure
- Fare clic sul collegamento **Amministrazione** nell'angolo inferiore sinistro della console di Security Manager.

La Console amministrativa è costituita da due riquadri: un riquadro sinistro e un riquadro destro. Il riquadro sinistro contiene gli strumenti di amministrazione. Il riquadro destro contiene l'area di lavoro per la configurazione degli strumenti.

Il riquadro sinistro della Console amministrativa è costituito da:

- **Home**: fornisce un facile accesso alle attività più comunemente utilizzate, quali l'attivazione di funzioni di protezione, la richiesta di credenziali di sicurezza e la gestione degli utenti.
- **Sistema**: consente di gestire la configurazione di funzioni di protezione del sistema, utenti e dispositivi di autenticazione quali lettori di smart card.

- **Applicazioni**: include strumenti per la configurazione del comportamento di Security Manager e relative applicazioni.
- **Dati**: fornisce gli strumenti per il backup e il ripristino delle chiavi di crittografia.
- **Computer**: fornisce opzioni di protezione avanzate per disabilitare selettivamente diversi tipi di dispositivi che potrebbero compromettere la sicurezza del PC e impostare le autorizzazioni di accesso per diversi utenti e gruppi.
- **Strumenti di gestione**: consente di aprire il browser predefinito su una pagina Web dalla quale è possibile utilizzare ulteriori applicazioni e strumenti di gestione che estendono le funzionalità di Security Manager; consente inoltre di ricevere una notifica quando sono disponibili nuove applicazioni e aggiornamenti.
- **Collegamenti**: consente di accedere a:
  - **Installazione guidata**: consente di avviare la configurazione guidata iniziale di Security Manager.
  - **?**: apre il file della Guida che fornisce informazioni su Security Manager e relative applicazioni.
  - **Informazioni su**: visualizza le informazioni su Security Manager, inclusi il numero di versione e l'avviso sul copyright.

Informazioni preliminari sulla Configurazione guidata

L'amministrazione di HP ProtectTools Security Manager richiede privilegi di amministratore.

La configurazione guidata di HP ProtectTools Security Manager consente di impostare tutte le funzioni di protezione di HP ProtectTools. Tuttavia, tramite la console di HP ProtectTools Security Manager è possibile accedere a diverse altre funzioni. Dalla console è possibile configurare le stesse impostazioni presenti nella configurazione guidata, oltre a funzioni di protezione aggiuntive, accessibili dal menu Start di Windows o da un collegamento disponibile all'interno della Console amministrativa. Queste impostazioni vengono applicate al computer e a tutti gli utenti che lo condividono.

Al primo accesso a Windows, verrà richiesto di configurare HP ProtectTools Security Manager. Fare clic su **OK** per avviare l'installazione guidata di Security Manager e seguire la procedura di configurazione del programma.

NOTA: per avviare la configurazione guidata è inoltre possibile fare clic su **Impostazione guidata di protezione** nella sezione inferiore del riquadro sinistro della Console amministrativa.

Seguire le istruzioni visualizzate sullo schermo fino a quando la procedura guidata non viene completata.

Se la procedura guidata non viene completata, verrà avviata automaticamente fino a quando non si fa clic su **Non mostrare più questa procedura guidata**.

Per utilizzare le applicazioni di HP ProtectTools Security Manager, avviare HP ProtectTools Security Manager dal menu **Start** oppure fare clic con il pulsante destro del mouse sull'icona **Security Manager** nell'area di notifica (barra delle applicazioni). La console di Security Manager e le relative applicazioni sono a disposizione di tutti gli utenti che condividono il computer.

Configurazione del sistema

Il gruppo di applicazioni **Sistema** è accessibile dal menu **Strumenti** sul lato sinistro della Console amministrativa.

Utilizzando le applicazioni incluse in questo gruppo, è possibile configurare e gestire i criteri e le impostazioni del computer, dei suoi utenti e dispositivi.

Le seguenti applicazioni sono incluse nel gruppo Sistema.

- **Protezione**: per gestire le funzioni di protezione, i criteri di autenticazione e altre impostazioni che definiscono la modalità di autenticazione dell'accesso utenti al computer o alle applicazioni HP ProtectTools.
- **Utenti**: per impostare, gestire e registrare gli utenti del computer.
- **Dispositivi**: per gestire le impostazioni dei dispositivi di protezione integrati o collegati al computer.

Abilitazione delle funzioni di protezione

Le funzioni di protezione qui abilitate vengono applicate a tutti gli utenti del computer.

1. Nel riquadro sinistro della Console amministrativa, espandere **Protezione** e fare clic su **Caratteristiche**.
2. Per abilitare una funzione di protezione, fare clic sulla casella di controllo corrispondente accanto a **Protezione di accesso a Windows** e/o a **Drive Encryption**.
   - **Protezione di accesso a Windows**: protegge gli account Windows richiedendo l'utilizzo di credenziali specifiche per l'accesso.
   - **Drive Encryption**: protegge i dati tramite la crittografia del disco rigido, rendendo i dati illeggibili per chi non dispone di un'autorizzazione appropriata.
3. Fare clic sul pulsante **Avanti**.
4. Fare clic sul pulsante **Applica**.

Definizione dei criteri di autenticazione di Security Manager

I criteri di autenticazione di Security Manager per il computer vengono definiti in due schede, Accesso e Sessione, che specificano le credenziali richieste per autenticare ogni classe di utenti all'accesso al computer e alle applicazioni di HP ProtectTools durante una sessione utente.

Scheda Accesso

Per specificare le credenziali richieste per l'accesso al computer e accedere a Windows:

1. Nel riquadro sinistro della Console amministrativa, espandere **Protezione** e fare clic su **Autenticazione**.
2. Nella scheda **Accesso**, selezionare una categoria di utenti dall'elenco a discesa.
3. Nella sezione **Criterio**, specificare le credenziali di autenticazione richieste per la categoria di utenti selezionata facendo clic sulle caselle di controllo appropriate accanto alle credenziali elencate. Specificare almeno una credenziale.

4. Nell'elenco a discesa della sezione **Criterio**, scegliere se è necessaria una sola delle credenziali specificate oppure se tutte le credenziali specificate sono necessarie per autenticare un utente.

5. Fare clic sul pulsante **Applica**.

Scheda Sessione

Per definire i criteri che stabiliscono le credenziali richieste per autenticare un utente per l'accesso alle applicazioni di HP ProtectTools durante una sessione Windows:

1. Nel riquadro sinistro della Console amministrativa, espandere **Protezione** e fare clic su **Autenticazione**.

2. Nella scheda **Sessione**, selezionare una categoria di utenti.

3. Nella sezione **Criterio**, specificare le credenziali di autenticazione richieste per la categoria di utenti selezionata facendo clic sulle caselle di controllo appropriate accanto alle credenziali elencate. Specificare almeno una credenziale.

4. Nell'elenco a discesa della sezione **Criterio**, scegliere se è necessaria una sola delle credenziali specificate oppure se tutte le credenziali specificate sono necessarie per autenticare un utente.

5. Fare clic sul pulsante **Applica**.

Definizione delle impostazioni

È possibile specificare quali impostazioni di protezione avanzate consentire. Per modificare le impostazioni:

1. Nel riquadro sinistro della Console amministrativa, espandere **Protezione** e fare clic su **Impostazioni**.

2. Fare clic sulla casella di controllo appropriata per abilitare o disabilitare una impostazione specifica.

3. Fare clic sul pulsante **Applica** per salvare le modifiche.

NOTA: l'impostazione **Consenti One Step Logon** consente agli utenti del computer di ignorare la procedura di accesso a Windows se l'autenticazione è stata eseguita a livello di BIOS.

Gestione degli utenti

All'interno dell'applicazione Utenti, l'amministratore Windows può gestire gli utenti del computer e i criteri ad essi applicati. Per accedere all'applicazione Utenti nella Console amministrativa, fare clic su **Utenti**.

Gli utenti di HP ProtectTools sono elencati e verificati a fronte dei criteri di autenticazione impostati mediante Security Manager e a fronte delle credenziali richieste per soddisfarli.

Per visualizzare i criteri applicati a uno specifico utente, selezionare l'utente dall'elenco e fare clic sul pulsante **Visualizza criteri**.

Per controllare un utente mentre registra le credenziali, selezionare l'utente dall'elenco e fare clic sul pulsante **Registra**.

Aggiunta di un utente

Questo processo consente di aggiungere utenti all'elenco di accesso. È possibile aggiungere solo utenti che già dispongano di un account utente Windows sul computer e che siano presenti per digitare la password durante la procedura riportata di seguito.

Per aggiungere un utente all'elenco:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro della Console amministrativa, fare clic su **Utente**.
3. Fare clic sul pulsante **Aggiungi**. Viene visualizzata la finestra **Seleziona utenti**
4. Fare clic sul pulsante **Avanzate**, quindi fare clic sul pulsante **Trova ora** per ricercare gli utenti da aggiungere.
5. Fare clic su un utente da aggiungere all'elenco e quindi fare clic su **OK**.
6. Fare clic su **OK** nella finestra di dialogo **Seleziona utenti**.
7. Digitare la password di Windows per l'account selezionato e quindi fare clic su **Fine**.

NOTA: è necessario utilizzare un account Windows esistente e digitarlo in modo corretto. In questa finestra di dialogo non è possibile modificare o aggiungere un account utente Windows.

Rimozione di un utente

NOTA: con questa procedura non si elimina l'account utente di Windows, ma solo l'account da Security Manager. Per rimuovere del tutto l'utente, è necessario effettuare la rimozione sia da Security Manager che da Windows.

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro della Console amministrativa, fare clic su **Utente**.
3. Fare clic sul nome utente dell'account che si desidera rimuovere, quindi scegliere **Elimina**.
4. Nella finestra di dialogo di conferma, fare clic su **Sì**.

Verifica dello stato dell'utente

La sezione Utente della Console amministrativa indica lo stato corrente di ogni utente:

- **Segno di spunta verde**: indica che l'utente ha configurato i metodi di accesso di sicurezza richiesti.
- **X rossa**: indica che l'utente non ha configurato un metodo di accesso di sicurezza richiesto e non gli verrà consentito l'accesso al computer. L'utente deve eseguire la configurazione guidata per configurare i metodi di accesso richiesti.
- **Vuoto**: indica che non è richiesto alcun metodo di accesso di sicurezza.

Configurazione delle impostazioni delle applicazioni

La finestra Impostazioni include strumenti per la configurazione del comportamento di Security Manager e relative applicazioni. Per modificare le impostazioni:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro della Console amministrativa, fare clic su **Impostazioni**.
3. Nella scheda **Generale**, scegliere le impostazioni generali per HP ProtectTools Security Manager, quindi fare clic sul pulsante **Applica**.
4. Nella scheda **Applicazioni**, selezionare le applicazioni da abilitare o disabilitare, quindi fare clic sul pulsante **Applica**.

NOTA: l'abilitazione o la disabilitazione di un'applicazione può non avere effetto fino a quando non viene riavviato il computer.

Crittografia delle unità

Drive Encryption for HP ProtectTools consente di crittografare le unità disco rigido del computer rendendole illeggibili e inaccessibili a persone non autorizzate che potrebbero provare ad accedere al computer anche se l'unità è stata rimossa dal computer o inviata a un servizio di ripristino dei dati.

Per abilitare o disabilitare Drive Encryption, fare clic sulla configurazione guidata nella Console amministrativa.

ATTENZIONE: è importante che si esegua il backup delle chiavi di crittografia in un'unità flash USB e che si custodisca quest'ultima in un luogo sicuro. Se si dimentica la password, sarà possibile accedere all'unità disco rigido solo grazie a questo dispositivo.

Per ulteriori informazioni sull'utilizzo di Drive Encryption for HP ProtectTools, vedere Drive Encryption for HP ProtectTools a pagina 33.

Gestione dell'accesso ai dispositivi

Device Access Manager for HP ProtectTools fornisce opzioni di protezione avanzate per disabilitare selettivamente diversi tipi di dispositivi che potrebbero compromettere la sicurezza del PC. Per ulteriori informazioni sull'utilizzo di Device Access Manager for HP ProtectTools, vedere Device Access Manager for HP ProtectTools a pagina 48.

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager consente di accrescere sensibilmente la protezione del computer. Utilizzando le applicazioni di Security Manager è possibile:

- Gestire l'accesso e le password
- Modificare con facilità la password di Windows
- Impostare credenziali di autenticazione, inclusa una smart card
- Distruggere o pulire l'unità disco rigido
- Visualizzare lo stato della crittografia dell'unità
- Visualizzare le impostazioni dell'accesso ai dispositivi
- Eseguire il backup e il ripristino dei dati di Security Manager

Gestione delle password

Credential Manager for HP ProtectTools (Gestore password) consente di creare e gestire gli accessi in modo da avviare e accedere ai siti Web e ai programmi eseguendo l'autenticazione con le credenziali registrate.

Per ulteriori informazioni sulla gestione delle password, vedere Credential Manager for HP ProtectTools (Gestore password) a pagina 36.

Impostazione delle credenziali

Le credenziali di Security Manager sono utilizzate per verificare l'identità dell'utente. L'amministratore del computer può stabilire le credenziali da utilizzare per dimostrare l'identità dell'utente durante l'accesso all'account Windows, ai siti web o ai programmi.

Le credenziali disponibili possono variare in base al dispositivo di protezione integrato o collegato al computer. Ogni credenziale supportata viene indicata dalla relativa voce nel gruppo Credenziali.

Modifica della password Windows

In Security Manager l'operazione di modifica della password Windows è più semplice e rapida dell'analoga operazione eseguita nel Pannello di controllo di Windows.

Per modificare la password di Windows:

1. In HP ProtectTools Security Manager, fare clic su **Credenziali** nel riquadro sinistro.
2. Fare clic su **Password di Windows**.
3. Digitare la password corrente nella casella **Password di Windows corrente**.
4. Digitare la nuova password corrente nelle caselle **Nuova password di Windows** e **Conferma nuova password**.
5. Fare clic su **Modifica**.

Distruzione o pulizia dei file

File Sanitizer for HP ProtectTools elimina i file sovrascrivendoli con dati non significativi. Questo processo di “distruzione” potenzia significativamente la protezione dei dati rendendo molto difficile il ripristino dei file eliminati. File Sanitizer migliora inoltre la protezione dei dati sovrascrivendo lo spazio precedentemente utilizzato sul disco rigido mediante un processo di “pulizia”. Il sistema operativo o altri software di ripristino file comunemente utilizzati non sono in grado di ripristinare i file eliminati utilizzando File Sanitizer.

Per ulteriori informazioni sull'utilizzo di File Sanitizer for HP ProtectTools, vedere File Sanitizer for HP ProtectTools a pagina 41.

Visualizzazione dello stato della crittografia dell'unità

Drive Encryption viene impostato dall'amministratore di Windows nella Console amministrativa. Gli utenti sono in grado di visualizzare lo stato della crittografia in Security Manager.

Per visualizzare lo stato della crittografia dell'unità:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **HP ProtectTools Security Manager**.
2. Nel riquadro sinistro di Security Manager, fare clic su **Stato crittografia**. La pagina Stato crittografia viene visualizzata se la crittografia dell'unità è attiva o inattiva e se vi sono unità crittografate o non crittografate.

Visualizzazione dell'accesso ai dispositivi

L'accesso ai dispositivi viene impostato dall'amministratore di Windows nella Console amministrativa. Gli utenti sono in grado di visualizzare l'impostazione di accesso ai dispositivi in Security Manager.

Per visualizzare le impostazioni di accesso ai dispositivi:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **HP ProtectTools Security Manager**.
2. Nel riquadro sinistro di Security Manager, espandere **Device Access Manager**.
3. Per visualizzare i dispositivi ai quali è negato l'accesso, fare clic su **Configurazione semplice**. Un segno di spunta contrassegna i dispositivi ai quali è negato l'accesso.

4. Per visualizzare gli utenti o i gruppi ai quali è negato l'accesso, fare clic su **Configurazione delle classi di periferiche**.

5. Fare clic su un dispositivo per visualizzare gli utenti o i gruppi ai quali è negato o consentito l'accesso a un dispositivo.

Aggiunta di applicazioni

Ulteriori applicazioni possono essere disponibili per aggiungere nuove funzioni al programma.

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **HP ProtectTools Security Manager**.

2. Nel riquadro sinistro di Security Manager, fare clic su **Altre applicazioni**.

NOTA: il collegamento **Altre applicazioni** potrebbe non essere disponibile se è stato disabilitato dall'amministratore del computer.

3. Nella scheda **Aggiungi applicazioni**, cercare le applicazioni aggiuntive.

4. Per rimanere al passo con le novità, fare clic sulla casella di controllo **Invia informazioni su nuove applicazioni e aggiornamenti** nella scheda **Aggiornamenti e messaggi** e impostare il numero di giorni desiderato oppure fare clic sul pulsante **Verifica ora** per controllare immediatamente la disponibilità di aggiornamenti.

Impostazione delle preferenze

Nella pagina Preferenze è possibile selezionare la casella di controllo **Mostra l'icona nella barra delle applicazioni** per visualizzare l'icona di Security Manager nell'area di notifica della barra delle applicazioni.

Per accedere alla pagina Preferenze:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **HP ProtectTools Security Manager**.

2. Nel riquadro sinistro di Security Manager, fare clic su **Avanzate**, quindi fare clic su **Preferenze**.

3. Selezionare o deselezionare la casella di controllo **Mostra l'icona nella barra delle applicazioni** e fare clic su **Applica**.

Backup e ripristino

Si consiglia di eseguire regolarmente il backup dei dati di Security Manager. La frequenza di esecuzione del backup dipende dalla cadenza con cui si modificano i dati. Ad esempio, se si aggiungono nuovi accessi ogni giorno, è opportuno eseguire il backup con frequenza giornaliera.

I backup possono essere inoltre utilizzati per eseguire la migrazione dei dati da un computer a un altro (operazione talvolta nota come importazione ed esportazione). Ricordare, tuttavia, che questa funzione esegue il backup dei soli dati.

Se viene ripristinato il file di backup su un altro computer, oppure sullo stesso computer dopo avere reinstallato il sistema operativo, HP ProtectTools Security Manager deve essere già installato nel sistema prima di ripristinare i dati dal file di backup.

Backup dei dati

Quando si esegue il backup dei dati, i dati relativi ad accessi e credenziali vengono salvati in un file crittografato, protetto dalla password specificata.

Per eseguire il backup dei dati:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **HP ProtectTools Security Manager**.
2. Nel riquadro sinistro di Security Manager, fare clic su **Avanzate**, quindi fare clic su **Backup e ripristino**.
3. Fare clic su **Backup dei dati**.
4. Selezionare i moduli da includere nel backup. Nella maggior parte dei casi, è opportuno selezionarli tutti. Fare clic su **Avanti**.
5. Immettere la password per verificare la propria identità, quindi fare clic sul pulsante a freccia.
6. Specificare il percorso e il nome del file di archiviazione. Per impostazione predefinita, il file viene salvato nella cartella Documenti. Fare clic su **Sfoglia** per specificare un percorso differente. Fare clic su **Avanti**.
7. Specificare e confermare la password per proteggere il file.
8. Fare clic su **Fine**.

Ripristino dei dati

I dati vengono ripristinati da un file crittografato protetto da password precedentemente creato mediante la funzione di Backup e ripristino di Security Manager.

Per eseguire il ripristino dei dati:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **HP ProtectTools Security Manager**.
2. Nel riquadro sinistro di Security Manager, fare clic su **Avanzate**, quindi fare clic su **Backup e ripristino**.
3. Fare clic su **Ripristino dei dati**.
4. Immettere il percorso e il nome del file di archiviazione oppure fare clic su **Sfoglia** e selezionare il file.
5. Immettere la password utilizzata per proteggere il file e fare clic su **Avanti**.
6. Selezionare i moduli con i dati da ripristinare. Nella maggior parte dei casi, si tratterà di tutti i moduli elencati. Fare clic su **Avanti**.
7. Fare clic su **Fine**.

Modifica del nome utente e dell'immagine di Windows

Il nome utente e l'immagine di Windows sono visualizzati nell'angolo superiore sinistro di Security Manager.

Per modificare il nome utente e/o l'immagine:

1. Fare clic sulla sezione superiore sinistra di Security Manager in cui sono presenti il nome utente e l'immagine.
2. Per modificare il nome utente, digitare un nome nella casella **Nome utente di Windows**.
3. Per cambiare l'immagine, fare clic sul pulsante **Scegli immagine** e cercare un'immagine.
4. Fare clic sul pulsante **Salva** per salvare le modifiche.

6 Drive Encryption for HP ProtectTools

NOTA: Drive Encryption for HP ProtectTools è disponibile solo su alcuni modelli.

Oggi, i dati critici di un'organizzazione potrebbero essere seriamente compromessi a seguito dell'eventuale furto di un computer aziendale. La crittografia dei dati salvati sull'unità disco rigido del computer consente di rendere tali dati illeggibili e inaccessibili a persone non autorizzate che potrebbero provare ad accedere al computer anche se l'unità è stata rimossa dal computer o inviata a un servizio di ripristino dei dati.

Il software Drive Encryption for HP ProtectTools offre protezione completa dei dati mediante la crittografia dell'unità disco rigido. Quando Drive Encryption è attivato, è necessario eseguire l'accesso nell'opportuna schermata di Drive Encryption, visualizzata prima dell'avvio di Windows.

Drive Encryption non impedisce l'accesso non autorizzato durante la stessa sessione di Windows. Una volta avviato il PC e immessi il nome utente e la password, i dati sull'unità disco rigido sono sempre crittografati, ma sono disponibili a tutti gli utenti del sistema. Accertarsi di proteggere la sessione di Windows con la password quando ci si allontana dal computer.

NOTA: Drive Encryption for HP ProtectTools può essere abilitato solo attraverso la configurazione guidata della Console amministrativa di HP ProtectTools.

NOTA: Drive Encryption non è supportato dai sistemi operativi a 64 bit se configurati con RAID su sistemi che utilizzano un processore AMD.

NOTA: Drive Encryption non supporta la prevenzione degli attacchi con dizionario.

Drive Encryption:

- Consente di crittografare tutti i dati delle unità disco rigido interne
- Fornisce un accesso protetto da password e un'autenticazione degli utenti Preboot di facile utilizzo
- Supporta Microsoft Windows XP, Windows Vista e Windows 7

In Drive Encryption for HP ProtectTools è possibile eseguire diverse attività:

- Gestione della crittografia dell'unità
  - Crittografia o decrittografia di singole unità
- Backup e ripristino
  - Creazione di chiavi di backup
  - Esecuzione del ripristino

△ **ATTENZIONE:** è importante che si esegua il backup delle chiavi di crittografia in un'unità flash USB e che si custodisca quest'ultima in un luogo sicuro. Se si dimentica la password, sarà possibile accedere all'unità disco rigido solo grazie a questo dispositivo.

ATTENZIONE: se si decide di disinstallare il modulo Drive Encryption oppure se si utilizza una soluzione di backup e ripristino, sarà prima necessario decrittografare tutte le unità crittografate. In caso contrario, non si sarà in grado di accedere ai dati sulle unità crittografate. La reinstallazione del modulo Drive Encryption non consente di accedere alle unità crittografate.

Procedure di configurazione

Avvio di Drive Encryption

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Fare clic su **Drive Encryption**.

Attività generali

Attivazione di Drive Encryption

Utilizzare la configurazione guidata della Console amministrativa di HP ProtectTools per attivare Drive Encryption.

Disattivazione di Drive Encryption

Utilizzare la configurazione guidata della Console amministrativa di HP ProtectTools per disattivare Drive Encryption.

Accesso dopo l'attivazione di Drive Encryption

Una volta attivato Drive Encryption e registrato l'account utente, all'accensione del computer sarà necessario accedere tramite la schermata di accesso di Drive Encryption:

NOTA: se l'amministratore di Windows ha abilitato la Sicurezza prima dell'avvio nella Console amministrativa di HP ProtectTools, si accederà al computer subito dopo l'accensione del computer, invece che dalla schermata di accesso di Drive Encryption.

NOTA: se si utilizza una chiave di ripristino per l'accesso tramite la schermata di accesso di Drive Encryption, verrà inoltre richiesto di selezionare il proprio nome utente e immettere la password nella schermata di accesso a Windows.

Attività avanzate

Gestione di Drive Encryption (attività dell'amministratore)

La finestra di Drive Encryption consente agli amministratori di Windows di visualizzare e modificare lo stato di Drive Encryption (attivo o inattivo) e di visualizzare lo stato della crittografia di tutte le unità disco rigido del computer.

Crittografia o decrittografia di singole unità disco

1. Nel riquadro sinistro della Console amministrativa, espandere **Drive Encryption** e fare clic su **Gestione crittografia**.
2. Fare clic sul pulsante **Cambia crittografia**.
3. Nella finestra di dialogo Cambia crittografia, selezionare o deselezionare la casella di controllo accanto a ciascuna unità disco da crittografare o decrittografare, quindi fare clic su **OK**.

NOTA: durante le operazioni di crittografia o decrittografia delle unità disco, una barra di avanzamento mostra il tempo rimanente per il completamento del processo nella sessione corrente. Se durante il processo di crittografia il computer viene spento (o si attiva lo stato di sospensione o ibernazione) e poi riavviato, la crittografia riprende da dove era stata interrotta, anche se per l'indicazione del tempo residuo viene ripristinato il valore iniziale. Le indicazioni del tempo residuo e dell'avanzamento cambieranno più velocemente, a riflettere l'avanzamento precedente.

Backup e ripristino (attività dell'amministratore)

La finestra Drive Encryption: Backup and Recovery consente agli amministratori di Windows di eseguire il backup e il ripristino delle chiavi di crittografia.

Creazione delle chiavi di backup

ATTENZIONE: conservare il dispositivo di archiviazione contenente la chiave di backup in un luogo sicuro, perché, se si dimentica la password, sarà possibile accedere all'unità disco rigido solo grazie ad esso.

1. Nel riquadro sinistro della Console amministrativa, espandere **Drive Encryption** e fare clic su **Backup and Recovery**.
2. Fare clic sul pulsante **Esegui backup chiavi**.
3. Nella pagina “Selezionare il disco di backup”, fare clic sul dispositivo sul quale si desidera eseguire il backup della chiave di crittografia, quindi fare clic su **Avanti**.
4. Leggere le informazioni visualizzate sulla pagina successiva, quindi fare clic su **Avanti**.

   La chiave di crittografia viene salvata sul dispositivo di archiviazione selezionato.
5. Fare clic su **OK** quando viene visualizzata la finestra di dialogo di conferma.

NOTA: consultare il file della Guida di Drive Encryption for HP ProtectTools per informazioni sulla gestione e l'esecuzione di un ripristino.

7 Credential Manager for HP ProtectTools (Gestore password)

Gestore password rende più semplice e sicuro l'accesso a Windows, ai siti Web e ai programmi.

Gestore password consente di impostare le schermate di accesso dei siti Web e dei programmi per accedervi in maniera più rapida e sicura. Innanzitutto, Gestore password rileva i dati di accesso e le informazioni specifiche digitate nelle caselle di immissione di ogni schermata di accesso. Quindi, dopo aver visualizzato una schermata di accesso e aver verificato l'identità, Gestore password completa e invia automaticamente i dati.

Per un accesso ancora più rapido, è possibile visualizzare un menu di accessi utilizzando una semplice combinazione di tasti di scelta rapida configurabile (Ctrl+Windows+H è la combinazione predefinita). Nel menu, è sufficiente selezionare un accesso per fare in modo che Gestore password avvii il sito Web o il programma desiderato, visualizzi la schermata di accesso ed esegua l'accesso in modo automatico.

Per verificare la propria identità, l'utente utilizza le credenziali di HP ProtectTools per le piccole imprese, ad esempio la password di Windows. Questo significa che verranno utilizzate le stesse credenziali per eseguire l'accesso in tutte le schermate impostate. È quindi possibile creare password più sicure che non sarà necessario annotare o ricordare e mantenere i propri account più protetti.

Gestore password consente di vedere subito se una delle password rappresenta un rischio per la protezione e può generare automaticamente una password sicura e complessa da utilizzare per i nuovi siti.

Con Gestore password è possibile visualizzare i dati di accesso e le password, e modificarli in qualsiasi momento. Molte delle sue funzioni sono anche disponibili tramite l'icona Gestore password visualizzata ogni volta che è attiva la schermata di accesso di un programma impostato o la schermata di accesso di un sito Web. Fare clic sull'icona per visualizzare un menu di scelta rapida in cui scegliere tra le seguenti opzioni.

Per pagine Web o programmi per i quali non è stato ancora creato un accesso:

Le seguenti opzioni sono indicate nel menu di scelta rapida.

- Aggiungi [nomedominio.com] a Gestore password: utilizzare per aggiungere un accesso per la schermata di accesso corrente.
- Apri Gestore password: avvia Security Manager nella pagina di Gestore password.
- Impostazioni dell'icona di Password Manager: consente di specificare le condizioni in cui viene visualizzata l'icona di Gestore password.
- ?: visualizza la Guida in linea dell'applicazione Gestore password.

Per pagine Web o programmi per i quali non è già stato creato un accesso:

Le seguenti opzioni sono indicate nel menu di scelta rapida.

- Immetti i dati di accesso: immette i dati di accesso nei relativi campi e quindi invia la pagina (se l'invio è stato specificato quando l'accesso è stato creato o modificato l'ultima volta).
- Modifica accesso: consente di modificare i dati di accesso per il sito Web.
- Aggiungi accesso: utilizzare per aggiungere un altro accesso per lo stesso sito Web o programma.
- Apri Gestore password: avvia l'applicazione Security Manager nella pagina di Gestore password.
- ?: visualizza la Guida in linea dell'applicazione Gestore password.

Aggiunta di accessi

Per aggiungere un accesso:

1. Aprire la schermata di accesso di un sito Web o di un programma.
2. Fare clic sulla freccia dell'icona di Gestore password e quindi selezionare una delle seguenti opzioni, per la schermata di accesso di un sito Web oppure di un programma.
   - Per un sito Web: selezionare **Aggiungi [nome dominio] a Gestore password**.
   - Per un programma: selezionare **Aggiungi questa schermata di accesso a Gestore password**.
3. Immettere i dati di accesso. I campi di accesso della schermata e i campi corrispondenti nella finestra di dialogo sono identificati da un bordo arancione doppio. Sono disponibili altre opzioni per la visualizzazione di questa finestra di dialogo, quali Aggiungi accesso nella scheda **Gestisci** di Gestore password. Alcune opzioni dipendono dai dispositivi di protezione collegati al computer; ad esempio, l'uso della combinazione di tasti Ctrl-H o l'inserimento di una smart card.
   - Fare clic sulle frecce a destra del campo di accesso per compilarlo con una delle selezioni preformattate.
   - Facoltativamente, fare clic su **Scegli altri campi** per aggiungere ulteriori campi della schermata all'accesso.
   - Deselezionare **Invia dati di accesso** se si desidera compilare i campi di accesso ma non inviarli.
   - Se si desidera visualizzare la password per questo accesso, fare clic su **Mostra password**.
4. Fare clic su **OK**. Il segno “più” viene rimosso dall'icona di Gestore password, indicando in tal modo che l'accesso è stato creato.

Successivamente, a ogni visita al sito o avvio del programma, l'icona di gestore password viene visualizzata, indicando che è possibile utilizzare le credenziali registrate per eseguire l'accesso.

Modifica degli accessi

Per modificare un accesso:

1. Aprire la schermata di accesso di un sito Web o di un programma.
2. Fare clic sulla freccia dell'icona di Gestore password e selezionare **Modifica accesso** per visualizzare una finestra di dialogo che consente di modificare i dati di accesso. I campi di accesso della schermata e i campi corrispondenti nella finestra di dialogo sono identificati da un bordo arancione doppio.
3. Modificare i dati di accesso.
   - Fare clic sulle frecce a destra del campo di accesso per compilarlo con una delle selezioni preformattate.
   - Facoltativamente, fare clic su **Scegli altri campi** per aggiungere ulteriori campi della schermata all'accesso.
   - Deselezionare **Invia dati account** se si desidera compilare i campi di accesso ma non inviarli.
   - Se si desidera visualizzare la password per questo accesso, fare clic su Mostra password.
4. Fare clic su **OK**.

Utilizzo del menu Accessi

Password Manager fornisce un metodo semplice e rapido per avviare siti Web e programmi per i quali sono stati creati accessi. È sufficiente fare doppio clic sull'accesso a un programma o a un sito Web dal menu Accessi, oppure nella scheda **Gestisci** di Gestore password, per avviare la schermata degli accessi e immettere i relativi dati di accesso. Per impostazione predefinita, vengono immediatamente inviati anche i dati al sito Web, sebbene sia possibile scegliere di non inviarli deselezionando **Invia dati account** quando si imposta o si modifica l'accesso.

Quando viene creato, l'accesso viene automaticamente aggiunto al menu Accessi di Gestore password.

Per visualizzare il menu Accessi, premere la combinazione di tasti di Gestore password. Ctrl-H è la combinazione predefinita, ma è possibile modificarla in **Gestore password** > **Impostazioni**.

Organizzazione degli accessi in categorie

Utilizzare le categorie per organizzare gli accessi. Creare una o più categorie e selezionare e trascinare gli accessi nelle categorie desiderate.

Per aggiungere una categoria:

1. Nel riquadro sinistro di Security Manager, selezionare **Gestore password**.
2. Selezionare la scheda **Gestisci** e fare clic su **Aggiungi categoria**.
3. Specificare il nome della categoria.
4. Fare clic su **OK**.

Per aggiungere un accesso:

1. Posizionare il puntatore del mouse sull'accesso desiderato.
2. Premere senza rilasciare il pulsante sinistro del mouse.
3. Trascinare l'accesso nell'elenco di categorie. Le categorie vengono evidenziate passandovi sopra il mouse.
4. Rilasciare il pulsante del mouse quando è evidenziata la categoria desiderata.

Gli accessi non vengono spostati nella categoria, ma solo copiati nella categoria selezionata. Questo significa che è possibile aggiungere lo stesso accesso a più di una categoria. Per visualizzare tutti gli accessi, fare clic su **Tutti**.

Gestione degli accessi

Gestore password assicura una semplice e intuitiva gestione centralizzata dei dati di accesso quali nomi utente, password e account di accesso multipli.

Gli accessi sono elencati nella scheda **Gestisci**. Quando vengono creati più accessi per lo stesso sito Web, ogni accesso viene elencato sotto il nome del sito Web, indicato da un rientro nell'elenco degli accessi.

Per gestire gli accessi:

Nel riquadro sinistro di Security Manager, selezionare **Gestore password** e fare clic sulla scheda **Gestisci**.

- Aggiunta di un accesso: fare clic su **Aggiungi accesso** e seguire le istruzioni visualizzate.
- Modifica di un accesso: selezionare un accesso e fare clic su **Modifica**. Modificare quindi i dati di accesso come desiderato.
- Eliminazione di un accesso: selezionare un accesso e fare clic su **Elimina**.

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

1. Aprire la schermata di accesso di un sito Web o di un programma.
2. Fare clic sull'icona di Gestore password per visualizzare il relativo menu di scelta rapida.
3. Selezionare **Aggiungi accesso aggiuntivo** e seguire le istruzioni visualizzate.

Valutazione 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.

Gestore password semplifica il monitoraggio e il miglioramento della protezione mediante l'analisi immediata e automatica della complessità di ogni singola password utilizzata per accedere a siti Web e programmi. È possibile verificare la complessità delle password utilizzate per gli accessi nella scheda **Complessità password** di Gestore password.

Impostazioni dell'icona di Gestore password

Gestore password tenta di identificare le schermate di accesso di siti Web e programmi. Quando rileva una schermata di accesso per la quale non è stato creato un accesso, Gestore password richiede di aggiungere un accesso per la schermata visualizzando l'icona di Gestore password con il segno “+”.

Sono disponibili le seguenti impostazioni:

- Richiedi sempre: selezionare questa opzione per richiedere di aggiungere un accesso ogni volta che viene visualizzata una schermata di accesso per la quale non è stato impostato un accesso.
- Non mostrare la richiesta per questa schermata: selezionare questa opzione per non richiedere di aggiungere nuovamente un accesso per questa specifica schermata di accesso.
- Non richiedere: selezionare questa opzione per assicurarsi che Gestore password non richieda mai schermate di accesso che non sono state impostate.

8 File Sanitizer for HP ProtectTools

File Sanitizer è uno strumento che consente di distruggere in modo sicuro i file e le cartelle critici (informazioni o file personali, dati cronologici o relativi al Web o altri componenti di dati) presenti sul computer ed eseguire la pulizia periodica del disco rigido.

NOTA: File Sanitizer funziona correntemente solo sull'unità disco rigido.

Informazioni sulla distruzione

L'eliminazione dei file e/o delle cartelle in Windows non comporta la rimozione di tutti i contenuti dell'unità disco rigido. Windows cancella soltanto il riferimento a tali dati, che rimangono sul disco rigido finché non vengono sovrascritti da altri file con nuove informazioni.

La distruzione si distingue dall'eliminazione standard di Windows (nota anche come eliminazione semplice in File Sanitizer) per il fatto che, una volta distrutti i dati, è virtualmente impossibile recuperarli.

Quando si sceglie un profilo di distruzione (Protezione alta, Protezione media o Protezione bassa), viene automaticamente selezionato un elenco predefinito di file e/o cartelle e un metodo per l'operazione di distruzione. È anche possibile personalizzare un profilo di distruzione al fine di specificare il numero di cicli di distruzione, i file da includere ed escludere dall'operazione e quelli da confermare prima della distruzione.

È possibile impostare una pianificazione di distruzione automatica, nonché distruggere file e/o cartelle in modo manuale in qualsiasi momento.

Informazioni sulla pulizia dello spazio libero

La pulizia dello spazio libero consente di scrivere dati casuali sui file eliminati in modo sicuro, impedendo agli utenti di visualizzare i contenuti originali dei file eliminati.

NOTA: la pulizia dello spazio libero è adatta per i file eliminati utilizzando il Cestino di Windows o manualmente. La pulizia dello spazio libero non offre protezione aggiuntiva ai file eliminati.

È possibile impostare un programma di pulizia automatica dello spazio libero oppure attivare manualmente la pulizia dello spazio libero mediante l'icona HP ProtectTools nell'area di notifica all'estrema destra della barra delle applicazioni.

Procedure di configurazione

Avvio di File Sanitizer

Per avviare File Sanitizer:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **HP ProtectTools Security Manager**.
2. Nel riquadro sinistro di Security Manager, fare clic su **File Sanitizer**.

   – oppure –

- Fare doppio clic sull'icona di **File Sanitizer**.

  – oppure –

- Fare clic con il pulsante destro del mouse sull'icona di HP ProtectTools nell'area di notifica all'estrema destra della barra delle applicazioni, evidenziare **File Sanitizer**, quindi fare clic su **Avvia File Sanitizer**.

Impostazione di un piano di pulizia dello spazio libero

Per impostare un programma di pulizia dello spazio libero

1. Nel riquadro sinistro di Security Manager, espandere **File Sanitizer**, quindi fare clic su **Pulizia**.
2. Selezionare la casella di controllo **Attiva pianificazione**, immettere la password di Windows, quindi specificare giorno e ora in cui eseguire la pulizia del disco rigido.
3. Fare clic sull'icona **Salva**.

NOTA: l'operazione di pulizia del disco rigido può richiedere tempi lunghi. Anche se la pulizia dello spazio libero viene eseguita in background, il computer potrebbe risultare più lento a causa del maggior utilizzo del processore.

Impostazione di un piano di distruzione

1. Nel riquadro sinistro di Security Manager, espandere **File Sanitizer**, quindi fare clic su **Distruzione**.
2. Selezionare un'opzione di distruzione:

   - **Si chiude Windows**: scegliere questa opzione per distruggere tutti i file selezionati alla chiusura di Windows.

     NOTA: se si seleziona questa opzione, all'arresto del computer viene visualizzata una finestra di dialogo in cui viene richiesto se continuare la distruzione dei file selezionati oppure ignorare la procedura. Fare clic su Sì per ignorare la procedura di distruzione oppure fare clic su No per continuare la procedura di distruzione. L'opzione Sì o No deve essere selezionata rapidamente perché Windows chiuderà il software in preparazione dell'arresto e genererà un errore. Se si seleziona No per continuare la distruzione, Windows genererà un errore indicante che File Sanitizer non risponde. Lasciare che File Sanitizer completi la distruzione, quindi avviare di nuovo l'arresto.

   - **Si avvia il browser Web**: scegliere questa opzione per distruggere tutti i file correlati al Web selezionati, ad esempio la cronologia URL del browser, all'apertura del browser.

- **Si chiude il browser Web**: scegliere questa opzione per distruggere tutti i file correlati al Web selezionati, ad esempio la cronologia URL del browser, alla chiusura del browser.
- **Sequenza di tasti**: scegliere questa opzione per avviare la distruzione utilizzando una sequenza di tasti.
- **Pianificazione**: selezionare la casella di controllo Attiva pianificazione e immettere la password di Windows, quindi specificare un giorno e un orario in cui distruggere i file selezionati.

3. Fare clic sull'icona **Salva**.

Selezione o creazione di un profilo di distruzione

È possibile specificare un metodo di eliminazione e selezionare i file e/o le cartelle da distruggere selezionando un profilo predefinito o creandone uno personalizzato.

Selezione di un profilo di distruzione predefinito

Quando si sceglie un profilo di distruzione predefinito (Protezione alta, Protezione media o Protezione bassa), vengono automaticamente selezionati un metodo di eliminazione e un elenco di file. Per visualizzare l'elenco predefinito dei file selezionati per la distruzione, fare clic sul pulsante Visualizza dettagli.

Per selezionare un profilo di distruzione predefinito:

1. Nel riquadro sinistro di Security Manager, espandere **File Sanitizer**, quindi fare clic su **Impostazioni**.
2. Fare clic su un profilo di distruzione predefinito.
3. Fare clic su **Visualizza dettagli** per visualizzare l'elenco di file selezionati per la distruzione.
4. In **Elimina seguenti**, selezionare la casella di controllo accanto a ciascun file che deve essere confermato prima della distruzione.
5. Fare clic su **Applica**.

Personalizzazione di un profilo di distruzione di sicurezza avanzato

Quando si crea un profilo di distruzione, è possibile specificare il numero di cicli di distruzione, i file da includere ed escludere dall'operazione, e i file da confermare prima della distruzione:

1. Nel riquadro sinistro di Security Manager, espandere **File Sanitizer**, fare clic su **Impostazioni**, selezionare **Impostazioni di protezione avanzate**, quindi fare clic su **Visualizza dettagli**.
2. Specificare il numero di cicli di distruzione.

NOTA: per ciascun file verrà eseguito il numero di cicli di distruzione selezionato. Ad esempio, se si scelgono 3 cicli di distruzione, un algoritmo che elimina i dati viene eseguito 3 volte diverse. Se si scelgono i cicli di protezione più alta, la distruzione potrebbe richiedere parecchio tempo. Tuttavia, maggiore è il numero dei cicli di distruzione specificati, più protetto sarà il computer.

3. Selezionare le risorse che si desidera distruggere:

   a. In **Opzioni di distruzione disponibili**, fare clic su un file, quindi su **Aggiungi**.

   b. Per aggiungere un file personalizzato, fare clic su **Aggiungi opzione personalizzata**, cercare o immettere il nome del file o della cartella, quindi fare clic su **OK**. Fare clic sul file personalizzato, quindi scegliere **Aggiungi**.

   NOTA: per eliminare un file dalle opzioni di distruzione disponibili, fare clic sul file, quindi su **Elimina**.

4. In **Elimina seguenti**, selezionare la casella di controllo accanto a ciascun file che deve essere confermato prima della distruzione.

NOTA: per rimuovere un file dall'elenco di distruzione, fare clic sul file desiderato, quindi su **Rimuovi**.

5. In **Non distruggere seguenti**, fare clic su **Aggiungi** per selezionare i file specifici da escludere dalla distruzione.

6. Al termine della configurazione del profilo di distruzione, fare clic su **Applica**.

Personalizzazione di un profilo di eliminazione semplice

Il profilo di eliminazione semplice consente di eseguire un'eliminazione standard dei file senza distruzione. Quando si personalizza un profilo di eliminazione semplice, è possibile specificare i file da includere ed escludere da una eliminazione semplice, e i file da confermare prima dell'operazione:

NOTA: è consigliabile eseguire regolarmente la pulizia dello spazio libero se si utilizza l'opzione di eliminazione semplice.

1. Nel riquadro sinistro di Security Manager, espandere **File Sanitizer**, fare clic su **Impostazioni**, selezionare **Impostazioni eliminazione semplice**, quindi fare clic su **Visualizza dettagli**.

2. Scegliere i file da eliminare:

   a. In **Opzioni di eliminazione disponibili**, fare clic su un file, quindi su **Aggiungi**.

   b. Per aggiungere un file personalizzato, fare clic su **Aggiungi opzione personalizzata**, cercare o immettere il nome del file o della cartella, quindi fare clic su **OK**. Fare clic sul file personalizzato, quindi scegliere **Aggiungi**.

   NOTA: per eliminare un file dalle opzioni di eliminazione disponibili, fare clic sul file, quindi su **Elimina**.

3. In **Elimina seguenti**, selezionare la casella di controllo accanto a ciascun file da confermare prima della eliminazione.

NOTA: per rimuovere un file dall'elenco di eliminazione, fare clic sul file desiderato, quindi su **Rimuovi**.

4. In **Non eliminare seguenti**, fare clic su **Aggiungi** per selezionare i file specifici da escludere dalla distruzione.

5. Al termine della configurazione del profilo di eliminazione semplice, fare clic su **Applica**.

Attività generali

Uso di una sequenza di tasti per avviare la distruzione

Per specificare una sequenza di tasti, procedere come segue:

1. Nel riquadro sinistro di Security Manager, espandere **File Sanitizer**, quindi fare clic su **Distruzione**.
2. Selezionare la casella di controllo **Sequenza di tasti**.
3. Immettere un carattere nella casella disponibile, quindi selezionare la casella **CTRL**, **ALT** o **MAIUSC** o tutte e tre.

   Ad esempio, per avviare la distruzione automatica utilizzando il tasto S e Ctrl+Maiusc, immettere S nella casella, quindi selezionare le opzioni **CTRL** e **MAIUSC**.

NOTA: accertarsi di selezionare una sequenza di tasti diversa da altre sequenze di tasti configurate.

Per avviare la distruzione mediante una sequenza di tasti.

1. Tenere premuti il tasto Ctrl, Alt o Maiusc (o una qualsiasi combinazione specificata) mentre si preme il tasto del carattere prescelto.
2. Se viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

Uso dell'icona File Sanitizer

△ **ATTENZIONE:** i file distrutti non possono essere ripristinati, pertanto selezionare con attenzione gli elementi da eliminare manualmente.

1. Passare al documento o alla cartella che si desidera distruggere.
2. Trascinare il file sull'icona File Sanitizer sul desktop.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

Distruzione manuale di una risorsa

△ **ATTENZIONE:** i file distrutti non possono essere ripristinati, pertanto selezionare con attenzione gli elementi da eliminare manualmente.

1. Fare clic con il pulsante destro del mouse sull'icona di **HP ProtectTools** nell'area di notifica all'estrema destra della barra delle applicazioni, evidenziare **File Sanitizer**, quindi fare clic su **Distruggi uno**.
2. Quando viene visualizzata la finestra di dialogo Sfoglia, spostarsi al file da distruggere, quindi scegliere **Apri**.

   NOTA: il file selezionato può essere un singolo file o una singola cartella.

3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

– oppure –

1. Fare clic con il pulsante destro del mouse sull'icona **File Sanitizer** sul desktop, quindi scegliere **Distruggi uno**.
2. Quando viene visualizzata la finestra di dialogo Sfoglia, spostarsi al file da distruggere, quindi scegliere **OK**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

– oppure –

1. Nel riquadro sinistro di Security Manager, espandere **File Sanitizer**, quindi fare clic su **Distruzione**.
2. Fare clic sul pulsante **Sfoglia**.
3. Quando viene visualizzata la finestra di dialogo Sfoglia, spostarsi al file da distruggere, quindi scegliere **Apri**.
4. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

Distruzione manuale di tutti gli elementi selezionati

1. Fare clic con il pulsante destro del mouse sull'icona di **HP ProtectTools** nell'area di notifica all'estrema destra della barra delle applicazioni, evidenziare **File Sanitizer**, quindi fare clic su **Distruggi ora**.
2. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

– oppure –

1. Fare clic con il pulsante destro del mouse sull'icona **File Sanitizer** sul desktop, quindi scegliere **Distruggi ora**.
2. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

Attivazione manuale della pulizia dello spazio libero

1. Fare clic con il pulsante destro del mouse sull'icona di **HP ProtectTools** nell'area di notifica all'estrema destra della barra delle applicazioni, evidenziare **File Sanitizer**, quindi fare clic su **Pulisci ora**.
2. Viene visualizzato un fumetto di notifica in cui viene indicato che l'operazione di pulizia è iniziata.

– oppure –

1. Nel riquadro sinistro di Security Manager, espandere **File Sanitizer**, quindi fare clic su **Pulizia**.
2. Fare clic su **Pulisci ora**
3. Viene visualizzato un fumetto di notifica in cui viene indicato che l'operazione di pulizia è iniziata.

Interruzione di un'operazione di distruzione o di pulizia dello spazio libero

Durante un'operazione di distruzione o di pulizia dello spazio libero, viene visualizzato un messaggio sull'icona di HP ProtectTools Security Manager nell'area di notifica. Nel messaggio sono riportate informazioni dettagliate sul processo di distruzione o di pulizia dello spazio libero (avanzamento) e viene offerta la possibilità di interrompere l'operazione.

Per interrompere l'operazione:

▲ Fare clic sul messaggio, quindi scegliere **Stop** per annullare l'operazione.

Visualizzazione dei file di registro

Ogni volta che viene eseguita un'operazione di distruzione o di pulizia dello spazio libero, vengono generati dei file di registro degli eventuali errori. I file di registro vengono sempre aggiornati in base all'ultima operazione di distruzione o di pulizia dello spazio libero.

NOTA: i file distrutti o puliti correttamente non vengono visualizzati nei file di registro.

Un file di registro viene creato per le operazioni di distruzione e un altro file di registro viene creato per le operazioni di pulizia dello spazio libero. Entrambi i file di registro sono archiviati sull'unità disco rigido in:

- C:\Programmi\Hewlett-Packard\File Sanitizer\`[Nome utente]`_ShredderLog.txt
- C:\Programmi\Hewlett-Packard\File Sanitizer\`[Nome utente]`_DiskBleachLog.txt

9 Device Access Manager for HP ProtectTools

Questo strumento di protezione è accessibile solo agli amministratori. Device Access Manager for HP ProtectTools include le seguenti funzioni che forniscono protezione dall'accesso non autorizzato a dispositivi collegati al computer:

- Vengono creati dei profili dei dispositivi per definire l'accesso ai dispositivi di ciascun utente
- L'accesso ai dispositivi viene concesso o negato in base all'appartenenza a un gruppo

NOTA: Device Access Manager utilizza l'opzione Utenti e gruppi locali di Windows per gestire l'accesso. Le versioni Home di Windows non supportano l'opzione Utenti e gruppi locali, pertanto Device Access Manager non funzionerà correttamente. Tuttavia, Device Access Manager funziona in Microsoft Windows Vista Home se si utilizzano i comandi DOS per l'impostazione utente. Per le istruzioni, consultare il file della Guida di Device Access Manager.

Avvio del servizio in background

Perché vengano applicati i profili dispositivo, deve essere in esecuzione il servizio in background HP ProtectTools Device Locking/Auditing. Quando si tenta di applicare i profili dispositivo per la prima volta, nella Console amministrativa di HP ProtectTools viene visualizzata una finestra di dialogo dove viene richiesto se si desidera avviare il servizio in background. Fare clic su **Sì** per avviare il servizio in background e impostarlo in modo che si avvii automaticamente all'avvio del sistema.

Configurazione semplice

Device Access Manager crea un nuovo gruppo di utenti durante l'inizializzazione denominato Device Administrators per accedere o visualizzare le funzioni dei dispositivi con i diritti di amministratore. Inserire in questo gruppo i nomi degli utenti a cui consentire l'accesso con privilegi amministrativi al dispositivo controllato con la configurazione semplice di Device Access Manager.

Con questa funzione si nega l'accesso alle seguenti classi di dispositivi:

- Dispositivi USB per tutti gli utenti non amministratori
- Tutti i supporti rimovibili (dischetti, lettori musicali, chiavette USB ecc) per tutti gli utenti non amministratori
- Tutte le unità DVD/CD-ROM per tutti gli utenti non amministratori
- Tutte le porte seriali e parallele per tutti gli utenti non amministratori

Per negare l'accesso a una classe di dispositivi per tutti gli utenti non amministratori:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro di sinistra fare clic su **Device Access Manager**, quindi selezionare **Configurazione semplice**.
3. Nel riquadro di destra selezionare la casella di controllo corrispondente al dispositivo di cui negare l'accesso.
4. Fare clic sull'icona **Salva**.

   NOTA: se il servizio di background non è in esecuzione, a questo punto si tenterà l'avvio. Fare clic su **Sì** per consentirne l'avvio.

5. Fare clic su **OK**.

Configurazione delle classi di periferiche (avanzata)

Sono disponibili ulteriori selezioni per consentire a utenti specifici o a gruppi di utenti di ottenere o meno l'accesso a determinati tipi di dispositivi.

Aggiunta di un utente o di un gruppo

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, espandere **Device Access Manager** e quindi fare clic su **Configurazione delle classi di periferiche**.
3. Nell'elenco dei dispositivi fare clic sulla classe del dispositivo da configurare.
4. Fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo **Seleziona utenti o gruppi**.
5. Fare clic su **Avanzate** e successivamente su **Trova ora** per cercare utenti o gruppi da aggiungere.
6. Fare clic su un utente o su un gruppo da aggiungere all'elenco degli utenti/gruppi disponibili e fare clic su **OK**.
7. Fare clic su **OK**.

Rimozione di un utente o di un gruppo

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, espandere **Device Access Manager** e quindi fare clic su **Configurazione delle classi di periferiche**.
3. Nell'elenco dei dispositivi fare clic sulla classe del dispositivo da configurare.
4. Fare clic sull'utente o sul gruppo che si desidera rimuovere, quindi fare clic su **Rimuovi**.

Negare o consentire l'accesso a un utente o a un gruppo

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, espandere **Device Access Manager** e quindi fare clic su **Configurazione delle classi di periferiche**.
3. Nell'elenco dei dispositivi fare clic sulla classe del dispositivo da configurare.
4. In **Utente/Gruppi** selezionare l'utente o il gruppo a cui negare l'accesso.
5. Fare clic su **Nega** accanto all'utente o al gruppo a cui negare l'accesso.
6. Fare clic sull'icona **Salva** e quindi fare clic su **OK**.

Impostazioni di accesso utente (avanzate)

Le impostazioni di accesso utente consentono agli amministratori di utilizzare le visualizzazioni Configurazione semplice e Configurazione delle classi di periferiche.

All'utente o al gruppo deve essere concesso l'accesso **Visualizza (sola lettura) impostazioni di configurazione** per potere visualizzare i dati in Configurazione semplice e Configurazione delle classi di periferiche.

All'utente o al gruppo deve essere concesso l'accesso **Cambia impostazioni di configurazione** per potere modificare i dati in Configurazione semplice e Configurazione delle classi di periferiche.

All'utente o al gruppo deve essere concesso l'accesso **Diritti amministratore utente completi** per potere modificare le impostazioni nelle visualizzazioni Configurazione semplice e Configurazione delle classi di periferiche.

Aggiunta di un utente o di un gruppo

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, espandere **Device Access Manager** e quindi fare clic su **Impostazioni di accesso utente**.
3. Fare clic su **Aggiungi**. Viene visualizzata la finestra **Seleziona utenti o gruppi**.
4. Fare clic sul pulsante **Avanzate** e quindi fare clic sul pulsante **Trova ora** per ricercare gli utenti o i gruppi da aggiungere.
5. Fare clic su un utente o un gruppo da aggiungere all'elenco di utenti e gruppi disponibili e quindi fare clic su **OK**.
6. Fare clic su **OK**.
7. Fare clic sull'icona **Salva**.

Rimozione di un utente o di un gruppo

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, espandere **Device Access Manager** e quindi fare clic su **Impostazioni di accesso utente**.
3. Fare clic sull'utente o il gruppo da rimuovere, quindi scegliere **Rimuovi**.
4. Fare clic sull'icona **Salva**.

Consentire o rifiutare autorizzazioni

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi fare clic su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, espandere **Device Access Manager** e quindi fare clic su **Impostazioni di accesso utente**.
3. Nella casella **Nomi utente o gruppo**, selezionare un nome utente o gruppo.

4. Nella casella **Autorizzazioni**, selezionare la casella di controllo **Consenti** oppure **Nega** come appropriato per le autorizzazioni.

5. Fare clic sull'icona **Salva**.

Glossario

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

Account utente di Windows.
Profilo di un utente autorizzato all'accesso a una rete o a un singolo computer.

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

Amministratore.
Vedere amministratore di Windows.

Autenticazione di accensione.
Funzione di protezione che, all'accensione del computer, richiede un tipo di credenziale di autenticazione, ad esempio una password.

Autenticazione.
Processo che consente di verificare se un utente è autorizzato a eseguire una determinata attività, come accedere a un computer, modificare uno specifico programma o visualizzare dati protetti.

Automatic Technology Manager (ATM).
Consente agli amministratori di rete di gestire in remoto i sistemi a livello di BIOS.

Ciclo di distruzione.
Il numero di volte in cui l'algoritmo di distruzione viene eseguito su ciascuna risorsa. Maggiore è il numero di cicli di distruzione che viene selezionato, più protetto risulterà il computer.

Credenziali.
Metodo con cui un utente prova la sua idoneità all'esecuzione di una determinata attività nel processo di autenticazione, ad esempio tramite l'immissione del nome utente e della password.

Distruzione automatica.
Distruzione programmata che l'utente imposta in File Sanitizer for HP ProtectTools.

Distruzione manuale.
Distruzione immediata di una o più risorse selezionate, che elude il programma di distruzione automatica.

Distruzione.
Esecuzione di un algoritmo che nasconde i dati contenuti in una risorsa.

Dominio.
Gruppo di computer che fanno parte di una rete e condividono un database di directory comune. A ciascun dominio è assegnato un nome univoco ed è associato un insieme di regole e procedure comuni.

Eliminazione semplice.
Eliminazione protetta dei dati riservati, tra cui file, contenuti correlati al Web o cronologici o altre informazioni confidenziali.

Metodo di accesso di sicurezza.
Il metodo utilizzato per accedere al computer.

Profilo di distruzione.
Un metodo di cancellazione e un elenco di risorse specifico.

Pulizia dello spazio libero.
Scrittura protetta di dati casuali sui file eliminati sull'unità disco rigido al fine di occultarne il contenuto, rendendo più difficoltoso il recupero dei dati precedenti.

Pulizia.
vedere **pulizia dello spazio libero**.

Riavvio.
Processo di riavvio del computer.

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

Sequenza di tasti:
Una combinazione di tasti specifici che, premuti, avviano una distruzione automatica, ad esempio, Ctrl+Alt+S.

Indice analitico