HP ProtectTools
Guida per l'utente

Guida dell'utente di HP ProtectTools

HP Compaq Business PC

Prima edizione: Luglio 2008

Numero di parte del documento: 491163-061

Informazioni su questa guida

Il presente manuale fornisce informazioni di base per l'aggiornamento del computer.

⚠ **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

Il software HP ProtectTools Security Manager for Administrators offre funzionalità di sicurezza che consentono di proteggere computer, reti e dati importanti contro l'accesso non autorizzato. La funzionalità di sicurezza avanzata viene garantita dai seguenti moduli software:

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

NOTA: Credential Manager, Java Card Security e Drive Encryption vengono configurati mediante la procedura di configurazione guidata di Security Manager.

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.

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

Funzioni di HP ProtectTools

Nella tabella riportata di seguito vengono elencate le funzioni principali dei moduli HP ProtectTools:

Modulo	Funzioni principali
HP ProtectTools Security Manager for Administrators	• 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. • La configurazione guidata può essere utilizzata anche dagli utenti per configurare i propri metodi di accesso. • Per aggiungere e rimuovere gli utenti di ProtectTools e per visualizzare lo stato degli utenti, si utilizzano gli strumenti di amministrazione. • Esegue il backup e il ripristino dei moduli di sicurezza dai moduli di HP ProtectTools installati.
Credential Manager for HP ProtectTools	• Credential Manager funge da archivio password personale, semplificando l'accesso grazie alla funzione di accesso “Single Sign On” che memorizza e applica automaticamente le credenziali dell'utente. • Questa funzione offre inoltre un livello di protezione aggiuntivo, poiché per l'autenticazione utente richiede combinazioni di tecnologie di sicurezza diverse, quali le Java™ Card e la biometrica. • La protezione dell'archivio delle password viene effettuata mediante crittografia software e può essere potenziata mediante l'uso di un chip di sicurezza incorporato TPM e/o dell'autenticazione mediante un dispositivo di sicurezza, quali le Java Card o la biometrica.
Drive Encryption for HP ProtectTools	• Drive Encryption fornisce una crittografia completa e integrale dei dischi rigidi. • Drive Encryption forza l'autenticazione prima dell'avvio al fine di decrittografare e accedere ai dati sul disco rigido.
Privacy Manager for HP ProtectTools	• Privacy Manager è uno strumento che consente di ottenere i certificati di autenticità, con cui verificare l'origine, l'integrità e la sicurezza delle comunicazioni quando si utilizzano la posta elettronica di Microsoft, i documenti di Microsoft Office e Live Messenger.
File Sanitizer for HP ProtectTools	• File Sanitizer consente di distruggere in modo definitivo e sicuro i dati digitali (ovvero di eliminare dati riservati, compresi i file delle applicazioni, i contenuti delle cronologie o correlati all'attività sul Web o altri dati da non divulgare) presenti nei computer e di ripulire periodicamente il disco rigido (scrivendo sui dati eliminati in precedenza ma che sono ancora presenti sul disco, in modo da rendere più difficile il recupero dei dati).

Modulo	Funzioni principali
Java Card Security for HP ProtectTools	• Java Card Security è un'interfaccia di gestione software per Java Card. Java Card è un dispositivo di protezione personale che protegge i dati di autenticazione che richiedono sia la scheda sia un numero PIN per concedere l'accesso. Java Card può essere utilizzata per accedere a Credential Manager, Drive Encryption, HP BIOS o a qualsiasi numero di punti di accesso di terze parti. • Java Card Security configura la Java Card for HP ProtectTools per l'autenticazione utente prima dell'avvio dell'unità disco rigido. È possibile accedere a Java Card Security tramite Embedded Security, Java Card e le password. • Java Card Security configura Java Card separate per amministratore e utente.
BIOS Configuration for HP ProtectTools	• BIOS Configuration fornisce l'accesso alla gestione delle password utente e amministratore necessarie per l'accensione. • Rappresenta un'alternativa all'utility di configurazione pre-avvio del BIOS nota come Impostazione del computer. • L'abilitazione tramite BIOS Configuration del supporto DriveLock automatico, reso ancora più potente dal chip di sicurezza incorporato, aiuta a proteggere il disco rigido dagli accessi non autorizzati (anche se viene rimosso da un sistema), senza che all'utente venga richiesto di ricordare password aggiuntive oltre alla password utente del chip di sicurezza incorporato.
Embedded Security for HP ProtectTools	• Embedded Security sfrutta un chip di protezione incorporata TPM (Trusted Platform Module) per accrescere il livello di protezione dagli accessi non autorizzati ai dati sensibili degli utenti o alle credenziali memorizzate a livello locale in un PC. • Embedded Security consente la creazione di un'unità PSD (Personal Secure Drive), utile per proteggere le informazioni relative a file e cartelle. • Supporta inoltre applicazioni di terzi, quali Microsoft Outlook e Internet Explorer, per le operazioni protette da certificato digitale.
Device Access Manager for HP ProtectTools	• Device Access Manager consente ai professionisti IT di controllare l'accesso ai dispositivi come le porte USB, le unità ottiche e così via, in base ai profili utente. • Device Access Manager impedisce agli utenti non autorizzati di usare supporti di memorizzazione esterna per rimuovere dati introdurre virus nel sistema. • L'amministratore può disattivare l'accesso ai dispositivi scrivibili a singoli utenti o a gruppi.

Accesso a HP ProtectTools Security

Per accedere a HP ProtectTools Security Manager for Administrators dal Pannello di controllo di Windows®:

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

  – oppure –

  In Windows XP, fare clic su **Start**, quindi selezionare **Tutti i programmi** e successivamente **HP ProtectTools Security Manager**.

NOTA: Se non si è un amministratore di HP ProtectTools, è possibile eseguire HP ProtectTools in modalità non amministratore per poter visualizzare (ma non modificare) le informazioni.

NOTA: Dopo aver configurato il modulo Credential Manager, è inoltre possibile aprire HP ProtectTools accedendo a Credential Manager direttamente dalla schermata di accesso di Windows. Per ulteriori informazioni, consultare Accesso a Windows con Credential Manager a pagina 29.

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:

- Protezione contro furti mirati
- Limitazione dell'accesso ai dati sensibili
- Blocco degli accessi non autorizzati dall'interno o dall'esterno della sede
- Creazione di criteri per password sicure
- Mandati di sicurezza per la conformità normativa

Protezione contro furti mirati

Un esempio di questo tipo di incidente è il furto mirato di un computer o dei dati riservati oppure delle informazioni sui clienti. È un evenienza relativamente frequente in uffici aperti al pubblico o in aree poco

protette. Le seguenti funzioni contribuiscono a proteggere i dati presenti nei computer che vengono rubati:

- Se abilitata, la funzione di autenticazione al preavvio impedisce l'accesso al sistema operativo. Vedere le seguenti procedure:
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- DriveLock garantisce che non sia possibile accedere ai dati anche se il disco rigido viene rimosso e installato su un sistema non protetto.
- La funzione Personal Secure Drive, inclusa nel modulo Embedded Security for HP ProtectTools, consente di crittografare i dati sensibili per impedirne l'accesso senza autenticazione. Vedere le seguenti procedure:
  - Embedded Security “Procedure di installazione a pagina 81”
  - “Uso dell'unità personale protetta (PSD) a pagina 83”

Limitazione dell'accesso ai dati sensibili

Se, ad esempio, un consulente a contratto sta temporaneamente lavorando nella sede del cliente e ha ricevuto accesso ai computer per effettuare la revisione dei dati finanziari sensibili, potrebbe essere utile impedirgli l'accesso a funzioni quali la stampa dei file o il loro salvataggio su dispositivi scrivibili, come ad esempio un CD. Le funzioni indicate di seguito consentono di limitare l'accesso ai dati:

- Device Access Manager for HP ProtectTools consente ai professionisti IT di limitare l'accesso ai dispositivi di scrittura, in modo che non sia possibile stampare dati riservati o copiarli dal disco rigido su un supporto rimovibile. Vedere Configurazione delle classi di periferiche (avanzata) a pagina 89.
- DriveLock garantisce che non sia possibile accedere ai dati anche se il disco rigido viene rimosso e installato su un sistema non protetto.

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

L'accesso non autorizzato a un PC di lavoro non protetto presenta un rischio molto tangibile per le risorse presenti nella rete aziendale, quali le informazioni provenienti da servizi finanziari, da un dirigente o da

un team R&D, e per informazioni private come i record personali dei pazienti o finanziari. Le funzioni seguenti aiutano a impedire gli accessi non autorizzati:

- Se abilitata, la funzione di autenticazione al preavvio impedisce l'accesso al sistema operativo. Vedere le seguenti procedure:
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- Embedded Security for HP ProtectTools protegge i dati sensibili le credenziali memorizzate a livello locale in un PC utilizzando le seguenti procedure.
  - Embedded Security “Procedure di installazione a pagina 81”
  - “Uso dell'unità personale protetta (PSD) a pagina 83”
- Credential Manager for HP ProtectTools aiuta a impedire che utenti non autorizzati possano ottenere le password o accedere alle applicazioni protette da password. A tale scopo, utilizza le seguenti procedure:
  - Credential Manager “Procedure di installazione a pagina 24”
  - “Uso di Single Sign-on a pagina 29”
- Device Access Manager for HP ProtectTools consente ai professionisti IT di limitare l'accesso ai dispositivi di scrittura, in modo che non sia possibile copiare i dati riservati dal disco rigido. Vedere Configurazione semplice a pagina 87.
- La funzione Personal Secure Drive utilizza le seguenti procedure per crittografare i dati sensibili in modo da impedirne l'accesso senza autenticazione.
  - Embedded Security “Procedure di installazione a pagina 81”
  - “Uso dell'unità personale protetta (PSD) a pagina 83”
- File Sanitizer consente di eliminare i dati in modo sicuro distruggendo definitivamente i file o ripulendo periodicamente il disco rigido (con la scrittura sui dati eliminati in precedenza ma che sono ancora presenti sul disco, in modo da rendere più difficile il recupero dei dati).
- Privacy Manager consente di ottenere i certificati di autenticità quando si utilizzano la posta elettronica di Microsoft, i documenti di Microsoft Office e Live Messenger, rendendo il processo di invio e salvataggio dei dati più importanti semplice e sicuro.

Creazione di criteri per password sicure

Se l'azienda decide di implementare criteri di protezione che prevedono l'uso di password sicure per decine di applicazioni Web e database, Credential Manager for HP ProtectTools potrà essere utilizzato come deposito protetto per password e Single Sign On. A tale scopo vengono usate le seguenti procedure:

- Credential Manager “Procedure di installazione a pagina 24”
- “Uso di Single Sign-on a pagina 29”

Per una maggiore sicurezza, Embedded Security for HP ProtectTools protegge il deposito di nomi utente e password. In tal modo gli utenti possono gestire più password complesse senza doverle annotare o ricordare. Vedere Embedded Security Procedure di installazione a pagina 81.

Ulteriori elementi protettivi

Assegnazione dei ruoli di protezione

Nella gestione della protezione dei computer (soprattutto per le grandi imprese), una pratica importante è quella di distribuire responsabilità e diritti tra vari 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.

Nel caso di HP ProtectTools, gli obblighi e i privilegi di protezione possono essere suddivisi tra i seguenti ruoli:

- Responsabile per la protezione: stabilisce il livello di protezione per l'azienda o la rete e decide quali funzioni di protezione utilizzare, come Java™ Card, lettori biometrici o token USB.
- Amministratore IT: applica e gestisce le funzioni di protezione decise dal responsabile per la protezione. Può anche attivare e disattivare alcune funzioni. Ad esempio, se il responsabile per la protezione ha deciso di utilizzare le Java Card, l'amministratore IT può attivare la modalità di protezione del BIOS con Java Card.
- Utente: utilizza le funzioni di protezione. Ad esempio, se il responsabile per la protezione e l'amministratore IT hanno attivato le Java Card per il sistema, l'utente può impostare il PIN della Java Card e utilizzare quest'ultima per l'autenticazione.

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 sono elencate anche le password impostate e utilizzate solo dagli amministratori IT. Tutte le altre password possono essere impostate da utenti abituali o da amministratori.

Password di HP ProtectTools	Modulo di HP ProtectTools in cui è impostata	Funzione
Password di accesso a Credential Manager	Credential Manager	Questa password è disponibile per 2 opzioni: • Può essere utilizzata per accedere separatamente a Credential Manager dopo aver effettuato l'accesso a Windows. • Può essere utilizzata per accedere contemporaneamente a Windows e a Credential Manager, in sostituzione della procedura di accesso a Microsoft Windows.
Password del file di ripristino di Credential Manager	Credential Manager, da amministratore IT	Protegge l'accesso al file di ripristino di Credential Manager.
Password chiave utente di base **NOTA:** Denominata anche: password di protezione incorporata	Embedded Security	Viene utilizzata per accedere alle funzioni di protezione incorporata, come la posta elettronica protetta e la crittografia di file e cartelle. Quando utilizzata per l'autenticazione dell'accensione, protegge anche l'accesso al contenuto del computer,

Password di HP ProtectTools	Modulo di HP ProtectTools in cui è impostata	Funzione
		quando il computer viene acceso, riavviato o viene disattivato lo stato di sospensione.
Password token per il ripristino di emergenza **NOTA:** Denominata anche: password chiave token per il ripristino di emergenza	Embedded Security, da amministratore IT	Protegge l'accesso al token per il ripristino di emergenza, che è un file di backup per il chip di protezione incorporata.
Password proprietario	Embedded Security, da amministratore IT	Protegge il sistema e il chip TPM dall'accesso non autorizzato a tutte le funzioni del proprietario di Embedded Security.
PIN Java™ Card	Java Card Security	Protegge l'accesso al contenuto della Java Card e permette l'autenticazione degli utenti della Java Card. Quando utilizzato per l'autenticazione dell'accensione, il PIN Java Card protegge anche l'accesso all'utility Impostazione del computer e al contenuto del computer. Permette l'autenticazione degli utenti di Drive Encryption se il token della Java Card è stato selezionato.
Password di Impostazione del computer **NOTA:** Denominata anche password amministratore del BIOS, password di configurazione F10 o password di configurazione di protezione	BIOS Configuration, da amministratore IT	Protegge l'accesso all'utility Impostazione del computer.
Password di accensione	BIOS Configuration	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 utilizzata per l'accesso manuale o salvata nella Java Card.

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 e ripristino delle credenziali di HP ProtectTools

Per effettuare il backup e il ripristino delle credenziali di tutti i moduli HP ProtectTools supportati, fare riferimento alle procedure descritte di seguito:

Backup di credenziali e impostazioni

È possibile effettuare il backup delle credenziali in uno dei seguenti modi:

- Utilizzando Drive Encryption for HP ProtectTools per selezionare le credenziali di HP ProtectTools ed effettuarne il backup.

  È anche possibile registrarsi per il servizio di recupero online delle chiave di crittografia delle unità Online Drive Encryption Key Recovery Service per memorizzare una copia di backup della chiave di crittografia, che consente di accedere al computer se si è dimenticata la password e non è possibile accedere al backup locale.

  NOTA: È necessario essere collegati a Internet e disporre di un indirizzo e-mail valido per registrarsi e recuperare la password mediante questo servizio.

- Utilizzando Embedded Security for HP ProtectTools per effettuare il backup delle credenziali di HP ProtectTools.

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

2 HP ProtectTools Security Manager for Administrators

Informazioni su HP ProtectTools Security Manager for Administrators

HP ProtectTools Security Manager for Administrators offre funzionalità di sicurezza che consentono di proteggere computer, reti e dati importanti contro l'accesso non autorizzato. Security Manager è scalabile e può quindi essere ampliato per gestire le nuove minacce emergenti e offrire le nuove tecnologie che si rendono disponibili.

Utilizzare i moduli di HP ProtectTools Security Manager for Administrators per la configurazione iniziale della sicurezza. L'interfaccia centralizzata di Security Manager contiene le seguenti funzioni:

- **Getting Started** (Configurazione iniziale): configurazione guidata che consente agli amministratori del sistema operativo Windows di configurare i livelli di sicurezza e i metodi di accesso utilizzati per l'ambiente di pre-avvio, Credential Manager e Drive Encryption. La configurazione guidata può essere utilizzata anche dagli utenti per configurare i metodi di accesso di sicurezza. Per ulteriori informazioni, consultare Getting Started (Configurazione iniziale): configurazione di HP ProtectTools Security Manager for Administrators a pagina 13 e Getting Started (Configurazione iniziale): configurazione dei metodi di accesso di sicurezza a pagina 15.
- **Administrators Tools** (Strumenti di amministrazione): consente agli amministratori di Windows di aggiungere e rimuovere gli utenti di ProtectTools e visualizzare lo stato degli utenti. Per ulteriori informazioni consultare Strumenti di amministrazione: gestione degli utenti (attività dell'amministratore) a pagina 17.
- **Backup and Restore** (Backup e ripristino): esegue il backup e il ripristino delle credenziali di sicurezza dai moduli di HP ProtectTools installati. Per ulteriori informazioni consultare Backup e ripristino a pagina 19.
- **Settings** (Impostazioni): consente di personalizzare il comportamento di alcune funzionalità. Per ulteriori informazioni consultare Impostazioni a pagina 23.

L'interfaccia utente centralizzata di Security Manager contiene inoltre un elenco di moduli software aggiuntivi progettati per incrementare ulteriormente la sicurezza dei computer. È possibile scegliere e configurare tutti i moduli desiderati.

Getting Started (Configurazione iniziale): configurazione di HP ProtectTools Security Manager for Administrators

La procedura di configurazione guidata consente agli amministratori di Windows di definire e/o aggiornare i livelli di sicurezza e i metodi di accesso di sicurezza.

La procedura può anche essere utilizzata dagli utenti per configurare i metodi di accesso protetti.

NOTA: Un amministratore di Windows può eseguire la configurazione guidata ogni volta che è necessario modificare i livelli di sicurezza o i metodi di accesso di sicurezza.

La configurazione guidata facilita le operazioni di configurazione di Security Manager:

1. In HP ProtectTools Security Manager for Administrators fare clic su **Getting Started** (Configurazione iniziale), quindi fare clic sul pulsante **Security Manager Setup** (Configurazione di Security Manager). È possibile che venga avviata una dimostrazione che descrive le funzioni di Security Manager.
2. Nella pagina di benvenuto, se visualizzata, deselezionare la casella di controllo **Automatically play video when wizard starts** (Riproduci automaticamente il video all'avvio della configurazione guidata), se si desidera evitare che la dimostrazione venga avviata al successivo avvio della configurazione guidata.
3. Leggere la pagina, quindi fare clic su **Avanti**.
4. Scegliere i livelli di sicurezza nella pagina “Set Levels of Security” (Impostazione livelli di sicurezza). È possibile scegliere uno o più dei seguenti livelli:
   - HP Credential Manager: protegge l'account Windows.
   - Pre-boot Security (Sicurezza prima dell'avvio) (alcuni modelli): protegge il computer prima dell'avvio di Windows.
   - HP Drive Encryption: protegge i dati del computer crittografando il contenuto del disco rigido. Quando si sceglie questa opzione, è necessario eseguire il backup della chiave crittografica univoca su un dispositivo di memorizzazione rimovibile.

   NOTA: Il valore indicato dal misuratore della sicurezza cambia in base alle opzioni selezionate. A un maggior numero di livelli selezionati corrisponde una maggiore sicurezza del computer.

   Dopo aver selezionato i livelli di sicurezza, scegliere **Avanti**.

5. Verrà visualizzata una o più delle seguenti pagine, in base ai livelli di sicurezza scelti al punto 4.

   - Protect your Windows account (Protezione dell'account Windows): la password di Windows è necessaria perché Security Manager deve sincronizzare la password per ciascuno dei livelli di sicurezza.

     Immettere e confermare una password di Windows oppure immettere la password già specificata, quindi scegliere **Avanti**.

   - Protect your system before Windows start-up (Protezione del sistema prima dell'avvio di Windows) (opzionale): se l'amministratore o l'utente conoscono la password amministratore BIOS, è possibile immettere tale password. Se si immette la password amministratore BIOS, l'amministratore o l'utente di Windows diventa un amministratore BIOS.

     NOTA: Se la password amministratore BIOS non esiste, è necessario specificarne una prima di procedere. Quando si immette una password amministratore BIOS, si diventa un amministratore BIOS.

     Immettere e confermare una password amministratore BIOS oppure immettere la password già specificata. Quindi fare clic su **Avanti**.

   - Protect your data by encrypting your hard drive (Protezione dei dati mediante crittografia del disco rigido): per salvare la chiave di crittografia, è necessario utilizzare un dispositivo di memorizzazione USB. Scegliere le unità da crittografare (almeno una), inserire il dispositivo di memorizzazione nell'alloggiamento appropriato, selezionare il dispositivo di memorizzazione in cui salvare la chiave, quindi scegliere **Avanti**.

6. Scegliere uno o più metodi di accesso di sicurezza nella pagina “Set Security Login Methods” (Impostazione metodi di accesso di sicurezza).

   a. Al punto 1, scegliere uno o più metodi di accesso di sicurezza.

   NOTA: Le selezioni vengono applicate a utenti e amministratori.

   b. Al punto 2, per aumentare il livello di sicurezza, selezionare la casella di controllo per richiedere *tutti* i metodi di accesso di sicurezza del punto 1 per l'accesso al computer.

   Se invece si desidera che *qualcuno* dei metodi di accesso di sicurezza venga ignorato durante l'accesso al computer, deselezionare la casella di controllo corrispondente.

   ATTENZIONE: Se si seleziona una casella di controllo ma un utente non ha ancora configurato i propri metodi di accesso (password di Windows, identificazione delle impronte digitali e/o HP ProtectTools Java™ Card), tale utente non sarà in grado di accedere al computer. Prima di selezionare l'opzione, è consigliabile che tutti gli utenti configurino i propri metodi di accesso.

   c. Fare clic su **Avanti**. Viene visualizzata una pagina di riepilogo, che consente di esaminare le opzioni selezionate.

7. Fare clic su **Enable** (Abilita) nella pagina “Riepilogo e abilitazione delle impostazioni di sicurezza”.

   Quando si fa clic su **Enable** (Abilita), il computer imposta le opzioni selezionate. Non sarà possibile tornare ad alcuna delle precedenti pagine della configurazione guidata prima della fine della configurazione. Al termine della configurazione guidata, sarà possibile modificare le impostazioni eseguendo di nuovo la configurazione guidata.

8. In base ai metodi di accesso di sicurezza selezionati al punto 6, verrà visualizzata una o più delle pagine riportate di seguito. Seguire le istruzioni visualizzate, quindi fare clic su **Avanti**.

   - “Enroll your fingerprints” (Registrazione delle impronte digitali): fare clic sul dito visualizzato sullo schermo corrispondente all'impronta che si desidera registrare (è necessario registrare almeno 2 impronte digitali), passare lentamente il dito sul sensore di impronte digitali, quindi continuare a passare lo stesso dito sul sensore fino a completare i passaggi necessari. Ripetere il processo per registrare un secondo dito, quindi scegliere **Fine**.
   - “Register an HP ProtectTools Java Card” (Registrazione di una HP ProtectTools Java Card): inserire la HP ProtectTools Java Card, immettere il PIN della Java Card, quindi scegliere **Fine**.

9. Nella pagina di conferma dell'esito della configurazione, esaminare le opzioni selezionate, quindi scegliere **Fine**.

Getting Started (Configurazione iniziale): configurazione dei metodi di accesso di sicurezza

Dopo che l'amministratore di Windows ha configurato i livelli di sicurezza e i metodi di accesso di sicurezza, gli utenti eseguono la configurazione guidata per aggiungersi come utenti di HP ProtectTools sul computer.

NOTA: Durante l'esecuzione della configurazione guidata, gli utenti visualizzano molte delle pagine della procedura guidata. Tuttavia le pagine “Set Levels of Security” (Impostazione livelli di sicurezza) e “Set Security Login Methods” (Impostazione metodi di accesso di sicurezza) non sono configurabili perché riservate agli amministratori.

1. Eseguire l'accesso sul computer.
2. In Security Manager fare clic su **Getting Started** (Configurazione iniziale), quindi fare clic sul pulsante **Security Manager Setup** (Configurazione di Security Manager).
3. Nella pagina di benvenuto deselezionare la casella di controllo **Automatically play video when wizard starts** (Riproduci automaticamente il video all'avvio della configurazione guidata), se si desidera evitare che la dimostrazione venga avviata al successivo avvio della configurazione guidata.
4. Leggere la pagina, quindi fare clic su **Avanti**.
5. Nella pagina “Set Levels of Security” (Impostazione livelli di sicurezza) fare clic su **Avanti**.

6. In base al livello di sicurezza impostato dall'amministratore, verrà visualizzata una o entrambe le pagine riportate di seguito.

   - Protect your Windows account (Protezione dell'account Windows): la password di Windows è necessaria perché Security Manager deve sincronizzare la password per ciascuno dei livelli di sicurezza.

     NOTA: Se HP Credential Manager è l'unico livello di sicurezza selezionato, la password di Windows non verrà richiesta perché Credential Manager già dispone della password di Windows.

     Immettere e confermare una password di Windows oppure immettere la password già specificata, quindi scegliere **Avanti**.

   - Protect your system before Windows start-up (Protezione del sistema prima dell'avvio di Windows) (opzionale): se si conosce la password amministratore BIOS, è possibile immetterla. Se si immette la password amministratore BIOS, l'amministratore o l'utente di Windows diventa un amministratore BIOS.

     NOTA: Se la password amministratore BIOS non esiste, è necessario specificarne una prima di procedere. Quando si immette una password amministratore BIOS, si diventa un amministratore BIOS.

     Immettere e confermare una password amministratore BIOS oppure immettere la password già specificata. Quindi fare clic su **Avanti**.

7. Nella pagina “Set Levels of Security” (Impostazione metodi di accesso di sicurezza) fare clic su **Avanti**.

8. Fare clic su **Enable** (Abilita) nella pagina “Riepilogo e abilitazione delle impostazioni di sicurezza”.

9. In base ai metodi di accesso di sicurezza impostati dall'amministratore, verrà visualizzata una o entrambe le pagine riportate di seguito. Seguire le istruzioni visualizzate, quindi fare clic su **Avanti**.

   - “Enroll your fingerprints” (Registrazione delle impronte digitali): fare clic sul dito visualizzato sullo schermo corrispondente all'impronta che si desidera registrare (è necessario registrare almeno 2 impronte digitali), passare lentamente il dito sul sensore di impronte digitali, quindi continuare a passare lo stesso dito sul sensore fino a completare i passaggi necessari. Ripetere il processo per registrare un secondo dito, quindi scegliere **Fine**.

   - “Register an HP ProtectTools Java Card” (Registrazione di una HP ProtectTools Java Card): inserire la HP ProtectTools Java Card, immettere il PIN della Java Card, quindi scegliere **Fine**.

10. Nella pagina di conferma dell'esito della configurazione, esaminare le opzioni selezionate, quindi scegliere **Fine**.

Accesso dopo la configurazione di Security Manager

Gli scenari di accesso variano in base ai livelli di sicurezza e ai metodi di accesso di sicurezza scelti dall'amministratore di Windows durante la configurazione. Di seguito sono descritti alcuni dei possibili scenari:

- Se sono stati configurati tutti e tre i livelli di sicurezza e sono richiesti *tutti* i metodi di accesso di sicurezza, gli utenti devono eseguire l'accesso utilizzando tutti i metodi configurati alla prima accensione del computer. Questa azione consente all'utente di accedere a Windows.
- Se sono stati configurati tutti e tre i livelli di sicurezza ed è richiesto solo *qualcuno* dei metodi di accesso di sicurezza, gli utenti possono eseguire l'accesso utilizzando i metodi configurati alla prima accensione del computer. Questa azione consente all'utente di accedere a Windows.
- Se sono stati configurati i livelli di sicurezza HP Drive Encryption e HP Credential Manager e sono richiesti *tutti* i metodi di accesso di sicurezza, gli utenti devono accedere utilizzando tutti i metodi configurati alla visualizzazione della schermata di accesso di HP Drive Encryption. Questa azione consente all'utente di accedere a Windows.
- Se sono stati configurati i livelli di sicurezza HP Drive Encryption e HP Credential Manager ed è richiesto *qualcuno* dei metodi di accesso di sicurezza, gli utenti possono accedere utilizzando i metodi configurati alla visualizzazione della schermata di accesso di HP Drive Encryption. Questa azione consente all'utente di accedere a Windows.
- Se è stato configurato il livello di sicurezza HP Credential Manager e sono richiesti *tutti* i metodi di accesso di sicurezza, gli utenti devono accedere utilizzando tutti i metodi configurati alla visualizzazione della schermata di accesso di HP Credential Manager. Questa azione consente all'utente di accedere a Windows.
- Se è stato configurato il livello di sicurezza HP Credential Manager ed è richiesto *qualcuno* dei metodi di accesso di sicurezza, gli utenti possono accedere utilizzando i metodi configurati alla visualizzazione della schermata di accesso di HP Credential Manager. Questa azione consente all'utente di accedere a Windows.

NOTA: Se il livello di sicurezza HP Credential Manager non è stato configurato, gli utenti devono comunque immettere la password di Windows nella schermata di accesso di Windows, indipendentemente dai metodi di accesso di sicurezza richiesti da altri livelli di sicurezza.

Strumenti di amministrazione: gestione degli utenti (attività dell'amministratore)

Gli amministratori di Windows possono aggiungere e rimuovere gli utenti di HP ProtectTools e visualizzare lo stato degli utenti utilizzando gli strumenti di amministrazione.

Nelle schede Administrator (Amministratore) e User (Utente) di Administrator Tools (Strumenti di amministrazione) vengono visualizzati i metodi di accesso di sicurezza selezionati e la possibilità dell'utente di scegliere se utilizzare solo alcuni o tutti i metodi. Per modificare i livelli di sicurezza o i metodi di accesso di sicurezza, eseguire la configurazione guidata.

Aggiunta di un utente

L'amministratore di Windows può aggiungere ulteriori amministratori o normali utenti all'elenco degli utenti esistenti. La procedura è la stessa per entrambi i tipi di utenti.

NOTA: 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 **HP ProtectTools Security Manager for Administrators**.
2. Fare clic su **Administrator Tools** (Strumenti di amministrazione).
3. Fare clic sul pulsante **Manage Users** (Gestisci utenti).
4. Scegliere la scheda **Administrator** (Amministratore) o **User** (Utente).
5. Fare clic su **Add** (Aggiungi).
6. Fare clic sul nome utente dell'account che si desidera aggiungere oppure digitarlo nella casella **User Name** (Nome utente), quindi scegliere **Avanti**.

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

7. Digitare la password Windows per l'account selezionato, quindi fare clic su **OK**.

   NOTA: Se esegue l'accesso con le impronte digitali e/o con il metodo di accesso di sicurezza HP ProtectTools Java Card, l'utente ora deve accedere al computer ed eseguire la configurazione guidata per configurare tali metodi di accesso di sicurezza.

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.

Per rimuovere un utente dall'elenco:

1. Fare clic su **Start**, scegliere **Tutti i programmi**, quindi **HP ProtectTools Security Manager for Administrators**.
2. Fare clic su **Administrator Tools** (Strumenti di amministrazione).
3. Fare clic sul pulsante **Manage Users** (Gestisci utenti).
4. Scegliere la scheda **Administrator** (Amministratore) o **User** (Utente).
5. Fare clic sul nome utente dell'account che si desidera rimuovere, quindi scegliere **Remove** (Rimuovi).

   NOTA: Se nell'elenco degli amministratori è presente un solo amministratore, non sarà possibile rimuoverlo.

6. Nella finestra di dialogo di conferma, fare clic su **Sì**.

Verifica dello stato dell'utente

Nelle schede Administrator (Amministratore) e User (Utente) di Administrator Tools (Strumenti di amministrazione) è riportato lo stato di ciascun utente:

- **Segno di spunta verde**: indica che l'utente ha configurato i metodi di accesso di sicurezza richiesti.
- **Punto esclamativo giallo**: indica che un utente non ha configurato uno o più dei metodi di accesso di sicurezza richiesti o consentiti. Se l'amministratore di Windows, ad esempio, configura almeno due metodi di accesso di sicurezza richiesti e specifica che è possibile utilizzare uno qualsiasi dei due per l'accesso al computer, un utente che ha già configurato uno di tali metodi può eseguire l'accesso utilizzando il metodo configurato. Il punto esclamativo giallo indica all'amministratore di Windows che l'utente non ha configurato l'altro metodo di accesso di sicurezza.
- **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.

Backup e ripristino

Lo strumento di backup e ripristino di HP ProtectTools costituisce una posizione centralizzata da cui eseguire backup e ripristini delle credenziali dai moduli di HP ProtectTools installati.

In Security Manager fare clic su **Backup and Restore** (Backup e ripristino), quindi fare clic su uno dei seguenti pulsanti:

- **Backup Options** (Opzioni di backup): consente di configurare le impostazioni per il backup. Per ulteriori informazioni, vedere Utilizzo della procedura guidata di backup a pagina 20.
- **Backup**: consente di eseguire un backup immediato di tutte le credenziali di sicurezza.

NOTA: Prima di eseguire un backup, è necessario configurare le impostazioni per il backup con **Backup Options** (Opzioni di backup).

- **Schedule Backups** (Pianificazione backup): consente di configurare i backup pianificati. Per ulteriori informazioni sulla pianificazione, cercare l'argomento “pianificazione attività” nella Guida di Windows.

NOTA: Prima di pianificare un backup, è necessario configurare le impostazioni per il backup con **Backup Options** (Opzioni di backup).

- **Restore** (Ripristino): consente di ripristinare le credenziali di sicurezza sottoposte a backup in precedenza. Per ulteriori informazioni, vedere Utilizzo della procedura guidata di ripristino a pagina 21.

△ **ATTENZIONE:** I file di backup non creati con HP ProtectTools Backup and Restore (ad esempio, i file creati in precedenza da un modulo di sicurezza specifico) non sono compatibili con HP ProtectTools Backup and Restore, quindi non è possibile ripristinarli con HP ProtectTools Backup and Restore o con le nuove versioni degli stessi moduli di sicurezza. È consigliabile creare un nuovo file di backup con HP ProtectTools Backup and Restore.

Utilizzo della procedura guidata di backup

1. In Security Manager fare clic su **Backup and Restore** (Backup e ripristino), quindi fare clic su **Backup Options** (Opzioni di backup) per avviare la procedura guidata di backup.
2. Deselezionare la casella di controllo **Show Welcome Screen** (Mostra schermata iniziale) per evitare che al prossimo accesso alla procedura guidata di backup venga visualizzata di nuovo la pagina di benvenuto.
3. Fare clic su **Avanti**. Viene visualizzata la pagina “Security Modules” (Moduli di sicurezza).
4. Per procedere, consultare i paragrafi che seguono.

Security Modules (Moduli di sicurezza)

Per selezionare i moduli di cui eseguire il backup, attenersi alla seguente procedura:

1. Selezionare la casella di controllo all'inizio di una riga per aggiungere il modulo associato all'elenco del backup. Fare clic sui pulsanti **Select All** (Seleziona tutto) o su **Clear All** (Deseleziona tutto) per aggiungere o rimuovere rapidamente tutti i moduli all'elenco di backup. Perché sia possibile selezionare un modulo, è necessario che lo stato riportato nell'apposita colonna sia “Ready” (Pronto) o “Needs Authentication” (Autenticazione necessaria).

NOTA: Se il modulo non è in stato pronto, non sarà possibile selezionare la casella di controllo. Dopo aver aggiornato lo stato di un modulo, fare clic sul pulsante **Refresh** (Aggiorna) alla destra della riga per aggiornare il campo Status (Stato). Per aggiornare lo stato di tutti i moduli, fare clic sul pulsante **Refresh All** (Aggiorna tutti).

2. Se necessario, digitare il valore richiesto nella colonna Authentication (Autenticazione) per ciascuno dei moduli selezionati. È possibile che il dispositivo di sicurezza richieda l'immissione dei valori di autenticazione per accedere ai dati delle credenziali del dispositivo. I valori possono essere password, PIN e così via.
3. Fare clic su **Avanti**. Viene visualizzata la pagina “File Location” (Percorso file).

File Location (Percorso file)

Nella pagina “File Location” (Percorso file) è possibile specificare la posizione del file di archiviazione di backup e del file del token di sicurezza.

Nel file del token di sicurezza viene archiviata e protetta la chiave utilizzata per la crittografia del file di backup. Una password crittografa il contenuto del file del token di sicurezza. Se si salva il file del token di sicurezza in un percorso non in linea (unità flash USB, disco o altro supporto), si ottiene una sicurezza su due livelli, poiché per accedere ai dati sottoposti a backup nel file di archiviazione, è necessario *disporre* del file del token di sicurezza e *conoscere* la password. È quindi consigliabile memorizzare file di archiviazione e file del token in due diversi supporti rimovibili conservati in luoghi diversi.

Per configurare il percorso dei file:

1. Confermare o modificare il nome del file e il percorso in cui si desidera salvare il file di archiviazione e il file del token di sicurezza. Per modificare il percorso, fare clic sul pulsante **Edit** (Modifica), quindi digitare il nuovo nome del file oppure fare clic su **Browse** (Sfoglia) per specificare una nuova posizione. Al nome del file viene automaticamente aggiunta l'estensione .ptb.

   NOTA: In ogni file di archiviazione è consentita una sola istanza di dati di backup per ciascun modulo. Se si specifica un file di archiviazione esistente, sarà possibile scegliere se sovrascrivere i dati del modulo selezionato all'interno del file di archiviazione o specificare un altro file di archiviazione. Se si specifica un file di archiviazione esistente, non verrà sovrascritto l'intero file, ma solo i dati di backup del modulo selezionato.

2. Per crittografare e proteggere il file di archiviazione con token di sicurezza e password, fare clic su **Password protect the storage file** (Proteggi file di archiviazione con password). Quindi, digitare e confermare la password da utilizzare per la crittografia del file del token di sicurezza.

3. Per configurare il sistema in modo da effettuare il salvataggio sicuro delle password nella cache (per consentire i backup automatici), fare clic su **Remember all passwords and authentication values** (Ricorda tutte le password e i valori di autenticazione). Se si abilita questa funzione, verranno memorizzati nella cache anche gli eventuali valori di autenticazione immessi nei moduli di sicurezza.

4. Fare clic su **Backup Now** (Esegui backup) per avviare il backup oppure scegliere **Avanti** per salvare la configurazione di backup senza eseguire subito un backup.

   Se si avvia il backup, al termine dell'operazione verrà visualizzata la pagina “Backup Complete” (Backup completato).

Backup Complete (Backup completato)

Nella pagina “Backup Complete” (Backup completato) viene indicato lo stato dell'operazione di backup.

1. Per visualizzare ulteriori informazioni sull'operazione di backup, compresi gli eventuali errori, fare clic su **View Log** (Visualizza registro).

2. Per uscire dalla procedura guidata, scegliere **Finish** (Fine).

Utilizzo della procedura guidata di ripristino

1. In Security Manager fare clic su **Backup and Restore** (Backup e ripristino), quindi fare clic su **Restore** (Ripristino) per avviare la procedura guidata di ripristino.

2. Deselezionare la casella di controllo **Show Welcome Screen** (Mostra schermata iniziale) per evitare che al prossimo accesso alla procedura guidata di ripristino venga visualizzata di nuovo la pagina di benvenuto.

3. Fare clic su **Avanti**. Viene visualizzata la pagina “File Location” (Percorso file).

4. Per procedere, consultare i paragrafi che seguono.

File Location (Percorso file)

Nella pagina “File Location” (Percorso file) è possibile specificare i file di archiviazione di backup e del token di sicurezza (se presente) che contengono le credenziali di sicurezza da ripristinare.

Per selezionare il percorso dei file di backup, attenersi alla seguente procedura:

1. Se il file non è presente nella pagina, fare clic sul pulsante **Edit** (Modifica), quindi fare clic su **Browse** (Sfoglia) per individuare il file.
2. Se il file del token di sicurezza non è presente nella pagina, fare clic sul pulsante **Edit** (Modifica), quindi fare clic su **Browse** (Sfoglia) per individuare il file del token di sicurezza.
3. Se necessario, digitare la password per il file.
4. Fare clic su **Avanti**. Viene visualizzata la pagina “Security Modules” (Moduli di sicurezza).

Security Modules (Moduli di sicurezza)

In questa pagina vengono visualizzati tutti i moduli installati per cui esistono dati di backup nel file selezionato nella pagina “File Location” (Percorso file).

Per selezionare i moduli da ripristinare:

1. Selezionare la casella di controllo all'inizio di ciascuna riga per aggiungere il modulo associato all'elenco di ripristino. Fare clic sul pulsante **Select All** (Seleziona tutto) o **Clear All** (Deseleziona tutto) per aggiungere o rimuovere rapidamente tutti i moduli all'elenco di ripristino. Perché sia possibile selezionare un modulo, è necessario che lo stato riportato nell'apposita colonna sia “Ready” (Pronto) o “Needs Authentication” (Autenticazione necessaria).

NOTA: Se il modulo non è in stato pronto, non sarà possibile selezionare la casella di controllo. Dopo aver aggiornato lo stato di un modulo, fare clic sul pulsante **Refresh** (Aggiorna) alla destra della riga per aggiornare il campo Status (Stato). Per aggiornare lo stato di tutti i moduli, fare clic sul pulsante **Refresh All** (Aggiorna tutti).

2. Se necessario, digitare il valore richiesto nella colonna Authentication (Autenticazione) per ciascuno dei moduli selezionati. I valori di autenticazione possono essere necessari per accedere al dispositivo di sicurezza da ripristinare. I valori possono essere password, PIN e così via. I valori digitati in questi campi vengono immediatamente convalidati.
3. Fare clic su **Avanti**. Viene visualizzata la pagina “Confirmation” (Conferma).

Confirmation (Conferma)

1. Per modificare le impostazioni di ripristino, scegliere **Previous** (Precedente) per tornare alle schermate di configurazione del ripristino.
2. Confermare l'intenzione di ripristinare le credenziali per i moduli elencati, quindi fare clic su **Restore Now** (Esegui ripristino) per avviare il ripristino.
3. Scegliere i file da ripristinare e fare clic su **Finish** (Fine).
4. Nella finestra di dialogo di conferma, fare clic su **Sì**.

△ **ATTENZIONE:** Il ripristino delle credenziali comporta la sovrascrittura delle credenziali correnti, con possibili blocchi del sistema o perdite di dati.

Restore Complete (Ripristino completato)

Nella pagina “Restore Complete” (Ripristino completato) viene indicato lo stato dell'operazione di ripristino.

- Per visualizzare ulteriori informazioni sull'operazione di ripristino, compresi gli eventuali errori, fare clic su **View Log** (Visualizza registro).
- Per uscire dalla procedura guidata, scegliere **Finish** (Fine).

Impostazioni

In HP ProtectTools Security Manager for Administrators fare clic su **Settings** (Impostazioni) per modificare le opzioni di impostazione.

Le impostazioni di Security Manager disponibili sono le seguenti:

- Selezionare la casella di controllo **Show icon on the taskbar** (Mostra l'icona sulla barra delle applicazioni) per visualizzare nella barra delle applicazioni un'icona che consente di avviare l'host e attivare una pagina specifica e/o avviare un'applicazione specifica.
- Selezionare la casella di controllo **Show Security Desktop Notifications** (Mostra notifiche desktop di sicurezza) per visualizzare le notifiche generate dai moduli installati.
- Visualizzare o meno la pagina iniziale della procedura guidata di backup.
- Visualizzare o meno la pagina iniziale della procedura guidata di ripristino.

3 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools utilizza le seguenti funzioni per proteggere il computer dagli accessi non autorizzati.

- Alternative alle password per l'accesso a Windows, come l'utilizzo di una Java Card o un lettore biometrico. Per ulteriori informazioni, consultare Registrazione delle credenziali a pagina 25.
- Funzione Single Sign-on che ricorda automaticamente le credenziali per i siti Web, le applicazioni e le risorse di rete protette.
- Supporto per dispositivi di protezione opzionali, come ad esempio le Java Card e i lettori biometrici.
- Supporto per impostazioni di protezione aggiuntive, come la richiesta di autenticazione mediante un dispositivo di protezione opzionale per sbloccare il computer.

Procedure di installazione

Accesso a Credential Manager

A seconda della configurazione, è possibile accedere a Credential Manager con uno dei seguenti metodi:

- Icona di HP ProtectTools Security Manager for Administrators nell'area di notifica
- In Windows Vista® fare clic su **Start**, scegliere **Tutti i programmi**, quindi **HP ProtectTools Security Manager for Administrators**.
- In Windows XP fare clic su **Start**, scegliere **Tutti i programmi**, quindi **HP ProtectTools Security Manager for Administrators**.

NOTA: In Windows Vista, per apportare le modifiche è necessario eseguire HP ProtectTools Security Manager.

Dopo l'accesso a Credential Manager, è possibile registrare ulteriori credenziali, come impronte digitali o Java Card. Per ulteriori informazioni, consultare Registrazione delle credenziali a pagina 25.

All'accesso successivo è possibile selezionare i criteri di accesso e utilizzare una delle combinazioni delle credenziali registrate.

Uso della procedura di accesso guidato a Credential Manager

Per accedere a Credential Manager utilizzando la relativa procedura di accesso guidato, attenersi alla procedura seguente:

1. Aprire la procedura di accesso guidato a Credential Manager con uno dei seguenti metodi:
   - Dalla schermata di accesso a Windows
   - Doppio clic nell'area di notifica sull'icona di **HP ProtectTools Security Manager for Administrators**
   - Nella pagina di Credential Manager di HP ProtectTools Security Manager for Administrators, clic sul collegamento **Log On** (Acceso) nell'angolo superiore destro della finestra
2. Seguire le istruzioni visualizzate per accedere a Credential Manager.

Registrazione delle credenziali

Dalla pagina “Identità personale” è possibile registrare vari metodi di autenticazione o credenziali. Dopo la registrazione di questi metodi, è possibile utilizzarli per accedere a Credential Manager.

Registrazione delle impronte digitali

Il lettore di impronte digitali consente di accedere a Windows utilizzando un'impronta digitale per l'autenticazione, invece di una password di Windows.

Configurazione del lettore di impronte digitali

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **My Identity** (Identità personale) e successivamente su **Register Fingerprints** (Registra impronte).
3. Seguire le istruzioni visualizzate sullo schermo per completare la registrazione delle impronte digitali e configurare il lettore di impronte digitali.
4. Per configurare il lettore di impronte digitali per un utente Windows diverso, accedere a Windows come tale utente e ripetere la procedura descritta.

Utilizzo dell'impronta digitale registrata per accedere a Windows

1. Subito dopo aver registrato le impronte digitali, riavviare Windows.
2. Nella schermata di benvenuto di Windows, passare una delle dita registrate per accedere a Windows.

Registrazione di una smart card o di un token

Una smart card è una scheda in plastica della dimensione di una carta di credito e dotata di un microchip incorporato su cui è possibile caricare delle informazioni. Le smart card offrono la protezione dei dati e l'autenticazione per i singoli utenti. L'accesso a una rete mediante una smart card può fornire una solida forma di autenticazione quando utilizza l'identificazione basata su crittografia e fungere da attestato di proprietà quando si effettua l'autenticazione di un utente in un dominio.

Un token USB è semplicemente una smart card con un formato diverso. Anziché su un supporto a carta di credito, lo smart chip viene inserito in un token in plastica, noto anche come chiavetta USB. La differenza principale tra una smart card e un token è costituita dall'interfaccia di accesso. Una card richiede un apposito lettore, mentre un token viene inserito direttamente in una porta USB. Per quanto riguarda invece la funzionalità di base di memorizzazione e accesso delle credenziali non esistono differenze.

Il token USB viene utilizzato per l'autenticazione di livello elevato, poiché fornisce un livello potenziato di sicurezza e garantisce un accesso protetto alle informazioni.

NOTA: Per eseguire questa procedura, è necessario disporre di un lettore di schede configurato. Se non si dispone di un lettore, è possibile registrare un token virtuale come descritto in Creazione di un token virtuale a pagina 27.

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **My Identity** (Identità personale) e successivamente su **Register Fingerprints** (Registra impronte).
3. Nella finestra **Device Type** (Tipo dispositivo), fare clic sul tipo di dispositivo desiderato, quindi su **Next** (Avanti).
4. Se come tipo di dispositivo è stata selezionata una smart card o un token USB, assicurarsi che la smart card sia inserita o che il token sia connesso a una porta USB.

   NOTA: Se la smart card non è inserita o il token USB non è connesso, nella finestra Select Token (Selezione token) il pulsante Next (Avanti) è disabilitato.

5. Nella finestra Device Type, selezionare **Next**.

   Viene visualizzata la finestra di dialogo Token Properties (Proprietà token).

6. Digitare il PIN utente nel campo appropriato, selezionare **Register smart card or token for authentication** (Registra smart card o token per l'autenticazione), quindi fare clic su **Finish** (Fine).

Registrazione di altre credenziali

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager**.
2. Fare clic su **My Identity** (Identità personale) e successivamente su **Register Credentials** (Registra credenziali).

   Viene aperta la registrazione guidata di Credential Manager.

3. Seguire le istruzioni visualizzate.

Attività generali

La pagina “Identità personale” in Credential Manager è accessibile a tutti gli utenti. Dalla pagina “Identità personale” è possibile effettuare le seguenti operazioni:

- Modifica della password di accesso a Windows
- Modifica del PIN di un token
- Blocco di una workstation

NOTA: Questa opzione è disponibile solo quando è abilitato il prompt di accesso classico di Credential Manager. Vedere Esempio 1: uso della pagina “Advanced Settings” (Impostazioni avanzate) per consentire l'accesso a Windows da Credential Manager a pagina 35.

Creazione di un token virtuale

Un token virtuale funziona in modo molto simile a una Java Card o a un token USB. Il token viene salvato sul disco rigido del computer o nel registro di Windows. Quando si effettua l'accesso con un token virtuale, per completare l'autenticazione viene richiesto un PIN utente.

Per creare un nuovo token virtuale:

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **My Identity** (Identità personale) e successivamente su **Register Fingerprints** (Registra impronte).
3. Nella finestra di dialogo **Device Type** (Tipo di dispositivo), fare clic su **Virtual Token** (Token virtuale) e successivamente selezionare **Next** (Avanti).
4. Specificare il nome e la posizione del token, quindi fare clic su **Next**.

   Un nuovo token virtuale può essere archiviato in un file o nel database del registro di Windows.
5. Nella finestra di dialogo Token Properties (Proprietà token), specificare il PIN principale (Master PIN) e il PIN utente (User PIN) per il token virtuale appena creato, selezionare **Register smart card or token for authentication** (Registra smart card o token per l'autenticazione), quindi fare clic su **Finish** (Fine).

   Viene visualizzata la finestra di dialogo Token Properties (Proprietà token).
6. Digitare il PIN utente nel campo appropriato, selezionare **Register smart card or token for authentication** (Registra smart card o token per l'autenticazione), quindi fare clic su **Finish** (Fine).

Modifica della password di accesso a Windows

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **My Identity** (Identità personale) e successivamente su **Change Windows Password** (Cambia password di Windows).
3. Immettere la vecchia password nel campo **Password vecchia**.

4. Digitare la nuova password nei campi **Nuova password** e **Conferma password**.
5. Fare clic su **Fine**.

Modifica di un PIN del token

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **My Identity** (Identità personale) e successivamente su **Change Token PIN** (Cambia PIN token).
3. Nella finestra Device Type (Tipo dispositivo), fare clic sul tipo di dispositivo desiderato, quindi su **Next** (Avanti).
4. Selezionare il token del quale si desidera modificare il PIN, quindi fare clic su **Avanti**.
5. Seguire le istruzioni visualizzate per completare la modifica del PIN.

NOTA: Se si immette un PIN non corretto per il token diverse volte in sequenza, il token viene bloccato e non sarà possibile utilizzarlo fino a quando non viene sbloccato.

Blocco del computer (workstation)

La funzione è disponibile quando si accede a Windows mediante Credential Manager. Per proteggere il computer mentre si è lontani dalla postazione, utilizzare la funzione Lock Workstation (Blocca workstation). Questa funzione impedisce a utenti non autorizzati di accedere al computer. Solo l'utente e i membri del gruppo di amministratori del computer possono sbloccarlo.

NOTA: Questa opzione è disponibile solo quando è abilitato il prompt di accesso classico di Credential Manager. Vedere Esempio 1: uso della pagina “Advanced Settings” (Impostazioni avanzate) per consentire l'accesso a Windows da Credential Manager a pagina 35.

Per migliorare la sicurezza, è possibile configurare la funzione di blocco della workstation in modo da richiedere una Java Card, un lettore biometrico o un token per sbloccare il computer. Per ulteriori informazioni, vedere Configurazione delle impostazioni di Credential Manager a pagina 35.

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **My Identity** (Identità personale).
3. Fare clic su **Lock Workstation** (Blocca workstation) per bloccare immediatamente il computer.

   Per sbloccare il computer sarà necessario utilizzare una password di Windows o la procedura guidata di accesso di Credential Manager.

Utilizzo dell'accesso a Windows

Per accedere a Windows, da un computer locale o un dominio di rete, è possibile utilizzare Credential Manager. Quando si accede a Credential Manager per la prima volta, il sistema aggiunge automaticamente l'account utente Windows locale come account per il servizio di accesso a Windows.

Accesso a Windows con Credential Manager

Per accedere a una rete Windows o a un account locale, è possibile utilizzare Credential Manager.

1. Se per accedere a Windows sono state registrate le impronte digitali, passare il dito per effettuare l'accesso.
2. In Windows XP, se non è stata registrata un'impronta digitale per l'accesso a Windows, fare clic sull'icona della tastiera nell'angolo superiore sinistro della schermata accanto all'icona dell'impronta digitale. Viene aperta la procedura guidata di accesso di Credential Manager.

   In Windows Vista, se non è stata registrata un'impronta digitale per l'accesso a Windows, fare clic sull'icona di **Credential Manager** nella schermata di accesso. Viene aperta la procedura guidata di accesso di Credential Manager.
3. Fare clic sulla freccia **User name** (Nome utente) e fare clic sul nome dell'utente.
4. Digitare la password nella casella **Password**, quindi fare clic su **Avanti**.
5. Selezionare **More** (Altro), quindi fare clic su **Wizard Options** (Opzioni procedura guidata).

   a. Se si desidera che il nome utente venga impostato come default per il successivo accesso al computer, selezionare la casella di controllo **Use last user name on next logon** (Utilizza l'ultimo nome al prossimo accesso).

   b. Se si desidera che questo criterio di accesso venga impostato come default, selezionare la casella di controllo **Use last policy on next logon** (Utilizza l'ultimo criterio al prossimo accesso).
6. Seguire le istruzioni visualizzate. Se le informazioni di autenticazione sono corrette, si effettua l'accesso all'account Windows e a Credential Manager.

Uso di Single Sign-on

Credential Manager ha una funzione Single Sign-On che memorizza i nomi utente e le password per più programmi Internet e Windows, e immette automaticamente le credenziali di accesso quando si accede a un programma registrato.

NOTA: Protezione e riservatezza dei dati sono funzioni importanti di Single Sign-On. Tutte le credenziali sono crittografate e accessibili solo dopo l'accesso riuscito a Credential Manager.

NOTA: È inoltre possibile configurare Single Sign On in modo da convalidare le credenziali di autenticazione con una Java Card, un lettore di impronte digitali o un token prima di accedere a un sito o programma sicuro. Questa funzione è particolarmente utile per l'accesso a programmi o siti Web che contengono informazioni personali, come numeri di conti bancari. Per ulteriori informazioni, consultare Configurazione delle impostazioni di Credential Manager a pagina 35.

Registrazione di una nuova applicazione

In Credential Manager viene richiesto di registrare qualsiasi applicazione avviata con collegamento a Credential Manager. È anche possibile registrare un'applicazione manualmente.

Uso della registrazione automatica

1. Aprire un'applicazione che richieda l'accesso.
2. Fare clic sull'icona Credential Manager SSO nella finestra di dialogo della password per il programma o il sito Web.

3. Digitare la password per il programma o il sito Web e fare clic su **OK**. Viene visualizzata la finestra di dialogo **Credential Manager Single Sign On**.
4. Fare clic su **More** (Altro) e scegliere tra le opzioni di seguito:
   - Non utilizzare SSO (Single Sign-On) con questo sito o applicazione.
   - Richiedere di selezionare l'account per questa applicazione.
   - Inserire le credenziali senza inviarle.
   - Autenticare l'utente prima di immettere le credenziali.
   - Visualizzare il collegamento SSO per questa applicazione.
5. Fare clic su **Sì** per completare la registrazione.

Uso della registrazione manuale (trascinamento)

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager**, quindi fare clic su **Services and Applications** (Servizi e applicazioni) nel riquadro a sinistra.
2. Fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).

   Viene visualizzata la finestra di dialogo Credential Manager Single Sign On (Accesso Single Sign On di Credential Manager).
3. Per modificare o rimuovere un sito Web o un'applicazione registrata in precedenza, selezionare il record corrispondente nell'elenco.
4. Seguire le istruzioni visualizzate.

Gestione di applicazioni e credenziali

Modifica delle proprietà dell'applicazione

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager**, quindi fare clic su **Services and Applications** (Servizi e applicazioni) nel riquadro a sinistra.
2. Fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).

   Viene visualizzata la finestra di dialogo Credential Manager Single Sign On (Accesso Single Sign On di Credential Manager).
3. Fare clic sulla voce dell'applicazione che si desidera modificare, quindi fare clic su **Proprietà**.
4. Fare clic sulla scheda **Generale** per modificare il nome e la descrizione dell'applicazione. Modificare le impostazioni selezionando o deselezionando le caselle di controllo corrispondenti alle impostazioni appropriate.
5. Fare clic sulla scheda **Script** per visualizzare e modificare lo script dell'applicazione SSO.
6. Fare clic su **OK**.

Rimozione di un'applicazione da Single Sign-On

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager**, quindi fare clic su **Services and Applications** (Servizi e applicazioni) nel riquadro a sinistra.
2. Fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).

   Viene visualizzata la finestra di dialogo Credential Manager Single Sign On (Accesso Single Sign On di Credential Manager).
3. Fare clic sulla voce corrispondente all'applicazione che si desidera rimuovere, quindi fare clic su **Remove** (Rimuovi).
4. Fare clic su **Sì** nella finestra di dialogo di conferma.
5. Fare clic su **OK**.

Esportazione di un'applicazione

È possibile esportare applicazioni per creare una copia di backup dello script dell'applicazione Single Sign-On. Sarà possibile utilizzare questo file per ripristinare i dati di Single Sign-On. Sarà un supplemento al file di backup dell'identità, che contiene solo le credenziali.

Per esportare un'applicazione:

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager**, quindi fare clic su **Services and Applications** (Servizi e applicazioni) nel riquadro a sinistra.
2. Fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).

   Viene visualizzata la finestra di dialogo Credential Manager Single Sign On (Accesso Single Sign On di Credential Manager).
3. Fare clic sulla voce corrispondente all'applicazione che si desidera esportare, quindi fare clic su **More** (Altro).
4. Seguire le istruzioni visualizzate per completare l'esportazione.
5. Fare clic su **OK**.

Importazione di un'applicazione

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager**, quindi fare clic su **Services and Applications** (Servizi e applicazioni) nel riquadro a sinistra.
2. Fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).

   Viene visualizzata la finestra di dialogo Credential Manager Single Sign On (Accesso Single Sign On di Credential Manager).
3. Fare clic sulla voce corrispondente all'applicazione che si desidera importare, quindi fare clic su **More** (Altro).
4. Seguire le istruzioni visualizzate per completare l'importazione.
5. Fare clic su **OK**.

Modifica delle credenziali

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager**, quindi fare clic su **Services and Applications** (Servizi e applicazioni).
2. Fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).

   Viene visualizzata la finestra di dialogo Credential Manager Single Sign On (Accesso Single Sign On di Credential Manager).
3. Fare clic sulla voce dell'applicazione che si desidera modificare, quindi fare clic su **More** (Altro).
4. Ecco alcune delle opzioni che è possibile selezionare:
   - Applicazioni
     - Add New (Aggiungi nuova)
     - Rimuovi
     - Proprietà
     - Import Script (Importa script)
     - Export Script (Esporta script)
   - Credenziali
     - Create New (Crea nuova)
   - View Password (Visualizza password)

   NOTA: È necessario autenticare l'identità prima di visualizzare la password.
5. Seguire le istruzioni visualizzate.
6. Fare clic su **OK**.

Utilizzo della protezione applicazioni

Con questa funzione è possibile configurare l'accesso alle applicazioni. È possibile limitare l'accesso in base ai criteri di seguito:

- Categoria dell'utente
- Ora di utilizzo
- Inattività dell'utente

Limitazione dell'accesso a un'applicazione

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra, quindi fare clic su **Services and Applications** (Servizi e applicazioni).
2. Fare clic su **Application Protection** (Protezione applicazioni), quindi scegliere **Manage Protected Applications** (Gestisci applicazioni protette).
3. Selezionare una categoria di utente per cui si desidera gestire l'accesso.

NOTA: Se la categoria non è Everyone (Tutti), potrebbe essere necessario selezionare **Override default settings** (Sovrascrivi impostazioni predefinite) per sovrascrivere le impostazioni della categoria Everyone (Tutti).

4. Fare clic su **Add** (Aggiungi).

   Viene visualizzata la procedura guidata di aggiunta programmi (Add a Program Wizard).

5. Seguire le istruzioni visualizzate.

Rimozione della protezione da un'applicazione

Per rimuovere le limitazioni da un'applicazione:

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **Services and Applications** (Servizi e applicazioni).
3. Fare clic su **Application Protection** (Protezione applicazioni), quindi scegliere **Manage Protected Applications** (Gestisci applicazioni protette).
4. Selezionare una categoria di utente per cui si desidera gestire l'accesso.

NOTA: Se la categoria non è Everyone (Tutti), potrebbe essere necessario fare clic su **Override default settings** (Sovrascrivi impostazioni predefinite) per sovrascrivere le impostazioni della categoria Everyone (Tutti).

5. Fare clic sulla voce dell'applicazione che si desidera rimuovere, quindi fare clic su **Rimuovi**.
6. Fare clic su **OK**.

Modifica delle impostazioni di limitazione per un'applicazione protetta

1. Fare clic su **Application Protection** (Protezione applicazioni), quindi scegliere **Manage Protected Applications** (Gestisci applicazioni protette).
2. Selezionare una categoria di utente per cui si desidera gestire l'accesso.

NOTA: Se la categoria non è Everyone (Tutti), potrebbe essere necessario fare clic su **Override default settings** (Sovrascrivi impostazioni predefinite) per sovrascrivere le impostazioni della categoria Everyone (Tutti).

3. Fare clic sull'applicazione da modificare, quindi fare clic su **Proprietà**. Viene visualizzata la finestra di dialogo **Proprietà** relativa all'applicazione selezionata.
4. Fare clic sulla scheda **Generale**. Selezionare una delle seguenti impostazioni:
   - Disabled (Cannot be used) (Disabilitato – Non utilizzabile)
   - Enabled (Can be used without restrictions) (Abilitato - Utilizzabile senza limitazioni))
   - Restricted (Usage depends on settings) (Limitato- L'utilizzo dipende dalle impostazioni)

5. Se si seleziona l'utilizzo limitato, sono disponibili le seguenti impostazioni:

   a. Per limitare l'utilizzo in base all'ora, al giorno o alla data, fare clic sulla scheda **Programma** e configurare le impostazioni.

   b. Per limitare l'accesso in base all'inattività, fare clic sulla scheda **Avanzate** e selezionare il periodo di inattività.

6. Per chiudere la finestra di dialogo **Proprietà** dell'applicazione, fare clic su **OK**.

7. Fare clic su **OK**.

Attività avanzate (riservate all'amministratore)

Le pagine “Multifactor Authentication” (Autenticazione a più fattori) e “Settings” (Impostazioni) di Credential Manager sono disponibili solo per gli utenti con diritti di amministrazione. In queste pagine è possibile eseguire le seguenti operazioni:

- Configurazione delle proprietà delle credenziali
- Configurazione delle impostazioni di Credential Manager

Configurazione delle proprietà delle credenziali

Nella scheda Credentials (Credenziali) della pagina “Multifactor Authentication” (Autenticazione a più fattori) è possibile visualizzare l'elenco dei metodi di autenticazione disponibili e modificare le impostazioni.

Per configurare le credenziali:

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.

2. Fare clic su **Multifactor Authentication** (Autenticazione multifattore).

3. Fare clic sulla scheda **Credentials** (Credenziali).

4. Fare clic sul tipo di credenziale da modificare. Per modificare le credenziali è possibile utilizzare una delle seguenti opzioni:

   - Per registrare la credenziale, fare clic su **Register** (Registra) e seguire le istruzioni visualizzate.
   - Per eliminare la credenziale, fare clic su **Clear** (Cancella), quindi fare clic su **Sì** nella finestra di dialogo di conferma.
   - Per modificare le proprietà della credenziale, fare clic su **Proprietà** e seguire le istruzioni visualizzate.

5. Fare clic su **Applica**, quindi su **OK**.

Configurazione delle impostazioni di Credential Manager

Nella pagina “Settings” (Impostazioni) è possibile visualizzare e modificare alcune impostazioni nelle schede seguenti:

- Generale: consente di modificare le impostazioni per la configurazione di base.
- Single Sign-On: consente di modificare le impostazioni di funzionamento di Single Sign-On per l'utente corrente, come la gestione del rilevamento di schermate di accesso, l'accesso automatico a finestre di dialogo registrate per l'accesso e la visualizzazione della password.
- Services and Applications (Servizi e applicazioni): consente di visualizzare i servizi disponibili e modificarne le impostazioni.
- Sicurezza: consente di selezionare il software del lettore di impronte digitali e regolare il livello di protezione del lettore stesso.
- Smart Cards and Tokens (Smart card e token): consente di visualizzare e modificare le proprietà di tutte le Java Card e i token disponibili.

Per modificare le impostazioni di Credential Manager:

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **Impostazioni**.
3. Fare clic sulla scheda appropriata per le impostazioni che si desidera modificare.
4. Seguire le istruzioni visualizzate per modificare le impostazioni.
5. Fare clic su **Applica**, quindi su **OK**.

Esempio 1: uso della pagina “Advanced Settings” (Impostazioni avanzate) per consentire l'accesso a Windows da Credential Manager

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager** nel riquadro a sinistra.
2. Fare clic su **Impostazioni**.
3. Fare clic sulla scheda **Generale**.
4. Sotto **Select the way users log on to Windows** (Scegli modalità di accesso a Windows degli utenti) selezionare la casella di controllo **Use Credential Manager to log on to Windows** (Usa Credential Manager per accedere a Windows).
5. Fare clic su **Applica**, quindi su **OK**.
6. Riavviare il computer.

NOTA: Se si seleziona la casella di controllo **Use Credential Manager to log on to Windows** (Usa Credential Manager per accedere a Windows), è possibile bloccare il computer. Vedere Blocco del computer (workstation) a pagina 28.

NOTA: La procedura precedente è leggermente diversa per Windows XP.

Esempio 2: uso della pagina “Advanced Settings” (Impostazioni avanzate) per richiedere la verifica utente prima dell'operazione Single Sign-on

1. In HP ProtectTools Security Manager for Administrators fare clic su **Credential Manager**, quindi fare clic su **Settings** (Impostazioni).
2. Fare clic sulla scheda **Single Sign On**.
3. In **When registered logon dialog or Web page is visited** (In caso di accesso a una finestra di dialogo o a una pagina Web registrata), selezionare la casella di controllo **Authenticate user before submitting credentials** (Autentica utente prima di immettere credenziali).
4. Fare clic su **Applica**, quindi su **OK**.
5. Riavviare il computer.

4 Drive Encryption for HP ProtectTools

△ **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 sarà possibile accedere ai dati delle unità crittografate a meno di non aver eseguito la registrazione con il servizio di ripristino di Drive Encryption. 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**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Fare clic su **Drive Encryption**.

Attività generali

Attivazione di Drive Encryption

Utilizzare la configurazione guidata di HP ProtectTools Security Manager for Administrators per attivare Drive Encryption.

Disattivazione di Drive Encryption

Utilizzare la configurazione guidata di HP ProtectTools Security Manager for Administrators 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 Pre-boot Security (Sicurezza prima dell'avvio) in HP ProtectTools Security Manager for Administrators, si accederà al computer subito dopo l'accensione del computer, invece che dalla schermata di accesso di Drive Encryption.

1. Selezionare il nome utente e immettere la password di Windows o il PIN della Java™ Card, oppure far scorrere il dito registrato.
2. Fare clic su **OK**.

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 pagina Encryption Management (Gestione crittografia) consente agli amministratori di Windows di visualizzare e modificare lo stato di Drive Encryption (attivo o inattivo), nonché di visualizzare lo stato di crittografia di tutti i dischi rigidi del computer.

Attivazione di una password TPM

Per attivare la protezione TPM, utilizzare Embedded Security for HP ProtectTools. Dopo l'attivazione, per l'accesso alla schermata di Drive Encryption saranno necessari il nome utente e la password di Windows.

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

1. Per attivare la protezione TPM, utilizzare Embedded Security for HP ProtectTools.
2. Aprire Drive Encryption e fare clic su **Gestione crittografia**.
3. Selezionare la casella di controllo **Password protetta da TPM**.

Crittografia o decrittografia di singole unità disco

1. Aprire Drive Encryption e fare clic su **Gestione crittografia**.
2. Fare clic su **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 pagina Ripristino consente agli amministratori di eseguire le operazioni di backup e 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: se si dimentica la password o si perde la Java Card, la chiave di backup rappresenta l'unica possibilità di accedere al disco rigido.

1. Aprire Drive Encryption e fare clic su **Ripristino**.
2. Fare clic su **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.

Registrazione per il recupero online

Il servizio di recupero online delle chiavi di Drive Encryption memorizza una copia di backup della chiave di crittografia, che consentirà l'accesso al computer qualora la password venga dimenticata e non si abbia accesso al backup locale.

NOTA: È necessario essere collegati a Internet e disporre di un indirizzo e-mail valido per registrarsi e recuperare la password mediante questo servizio.

1. Aprire Drive Encryption e fare clic su **Ripristino**.
2. Fare clic su **Registra**.
3. Fare clic su una delle seguenti opzioni:
   - I want to create a new recovery account for this PC. (Desidero creare un account di ripristino per questo PC.) Se si sceglie questa opzione, digitare il proprio indirizzo e-mail e altri dati, quindi fare clic su **Avanti**.
   - I want to add this PC to my existing web recovery account. (Desidero aggiungere questo PC al mio account di ripristino via Web esistente)
4. Creare e confermare una password, selezionare le domande di sicurezza immettendo le relative risposte, quindi fare clic su **Avanti**.

   NOTA: Il codice di attivazione dell'account verrà inviato all'indirizzo di posta elettronica fornito.
5. Immettere il codice di attivazione e fare clic su **Avanti**.
6. Immettere il numero di serie del computer e fare clic su **Avanti**.

   NOTA: Per individuare il numero di serie del computer, fare clic su **Start**, quindi su **Guida in linea e supporto tecnico**.
7. Se non si dispone di un coupon di iscrizione, fare clic sul collegamento **Fare clic qui per acquistare i coupon**.

   Facendo clic sul collegamento si verrà reindirizzati al sito Web del servizio di recupero SafeBoot. Non chiudere la procedura guidata.
8. Fare clic su **Purchase Coupon Codes** (Acquista codici coupon).

9. Selezionare il paese, il tipo di computer e fare clic su **Start**.
10. Fare clic su **Buy** (Acquista) accanto all'opzione di iscrizione per 1 anno o per 3 anni.
11. Fare clic su **Checkout** (Pagamento).
12. Leggere i termini e le condizioni, quindi fare clic su **Accept** (Accetto).
13. Immettere i dati di fatturazione, quindi fare clic su **Continue** (Continua).
14. Immettere i dati della propria carta di credito, quindi fare clic su **Make Payment** (Effettua pagamento).
15. Annotare il codice di coupon, quindi tornare alla pagina Attivazione account della procedura guidata.
16. Immettere il proprio codice di attivazione dell'account e fare clic su **Avanti**.
17. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **OK**.

Gestione di un account di ripristino online esistente

Dopo aver creato un account di ripristino online, sarà possibile accedere al sito Web del servizio di recupero SafeBoot per ripristinare l'accesso al computer nel caso si sia persa la password, modificare le proprie impostazioni personali, reimpostare la password utilizzata per l'account di ripristino online e visualizzare o rinnovare l'account.

1. Aprire Drive Encryption e fare clic su **Ripristino**.
2. Fare clic su **Manage** (Gestisci).
3. Quando viene visualizzata la pagina Web “SafeBoot Recovery Service”, fare clic su **Recovery Service Account** (Account del servizio di recupero) oppure su **Processo di recupero**.
4. Nella pagina di accesso al servizio di recupero, immettere il proprio indirizzo di posta elettronica e la password, quindi immettere i numeri e le lettere visualizzati nel riquadro.
5. Fare clic su **Logon** (Accedi).
6. Fare clic su **Profilo** per aggiornare le informazioni personali, ad esempio il numero telefonico o l'indirizzo di fatturazione.

   – oppure –

   Fare clic su **Reimposta password** per reimpostare o modificare la password.

   – oppure –

   Fare clic su **My Subscriptions** (Iscrizioni personali) per visualizzare le informazioni sulle attuali iscrizioni.

NOTA: In questa pagina è inoltre possibile rinnovare la propria iscrizione. A tale scopo, fare clic su **Renew Subscription** (Rinnova iscrizione).

Esecuzione di un ripristino

Esecuzione di un ripristino locale

1. Accendere il computer.
2. Inserire il dispositivo di archiviazione rimovibile in cui è memorizzata la chiave di backup.
3. Nella finestra di dialogo di accesso a Drive Encryption for HP ProtectTools visualizzata, fare clic su **Annulla**.
4. Fare clic su **Opzioni** nell'angolo inferiore sinistro dello schermo, quindi fare clic su **Ripristino**.
5. Selezionare **Ripristino locale**, quindi fare clic su **Avanti**.
6. Selezionare il file contenente la chiave di backup oppure fare clic su **Sfoglia** per cercarlo, quindi fare clic su **Avanti**.
7. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **OK**.

   Il processo di ripristino è stato completato e il computer viene avviato.

NOTA: Si consiglia di reimpostare la password dopo aver eseguito un ripristino.

Esecuzione di un ripristino online

NOTA: In questa sezione viene descritta l'esecuzione di un ripristino online quando si dispone dell'accesso a un diverso computer con una connessione a Internet. Se non si dispone dell'accesso a un computer simile, contattare l'assistenza tecnica HP.

1. Accendere il computer.
2. Nella finestra di dialogo di accesso a Drive Encryption for HP ProtectTools visualizzata, fare clic su **Annulla**.
3. Fare clic su **Opzioni** nell'angolo inferiore a sinistra dello schermo, quindi fare clic su **Ripristino**.
4. Selezionare **Ripristino via Web**, quindi fare clic su **Avanti**.
5. Annotare il codice del client e fare clic su **Avanti**.
6. Su un computer diverso con una connessione a Internet, accedere al sito Web del servizio di recupero SafeBoot all'indirizzo http://www.safeboot-hp.com.
7. Fare clic su **Processo di recupero**.
8. Nella pagina di accesso al servizio di recupero, immettere il proprio indirizzo di posta elettronica e la password, quindi immettere i numeri e le lettere visualizzati nel riquadro.
9. Fare clic su **Logon** (Accedi).
10. Fare clic su **Processo di recupero**.
11. Immettere il codice client annotato per il computer in corso di recupero, quindi immettere i numeri e le lettere visualizzati nel riquadro.
12. Fare clic su **Submit** (Inoltra).
13. Annotare tutte le righe della chiave di risposta.

14. Sul computer in fase di ripristino, immettere la riga 1 della chiave di risposta annotata dal sito Web SafeBoot Recovery Service, quindi fare clic su **Invio**.
15. Immettere la riga 2 della chiave di risposta, quindi fare clic su **Invio**.
16. Immettere la riga 3 della chiave di risposta, quindi fare clic su **Invio**.
17. Immettere la riga 4 della chiave di risposta, quindi fare clic su **Invio**.

    NOTA: La riga 4 della chiave di risposta è più breve delle prime 3 righe.

18. Fare clic su **Fine**.

NOTA: Si consiglia di reimpostare la password dopo aver eseguito un ripristino.

5 Privacy Manager for HP ProtectTools

Privacy Manager è uno strumento che consente di ottenere i certificati di autenticità, con cui verificare l'origine, l'integrità e la sicurezza delle comunicazioni quando si utilizzano la posta elettronica di Microsoft, i documenti di Microsoft Office e Live Messenger.

Privacy Manager sfrutta l'infrastruttura di sicurezza fornita da HP ProtectTools Security Manager for Administrators, che comprende i seguenti metodi di accesso di sicurezza:

- Autenticazione delle impronte digitali
- Password di Windows®
- HP ProtectTools Java™ Card
- Token virtuale
- Chiave utente di base di Embedded Security for HP ProtectTools

In Privacy Manager è possibile utilizzare uno dei metodi di accesso di sicurezza riportati sopra.

Avvio di Privacy Manager

Per avviare Privacy Manager:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Fare clic su **Privacy Manager: Sign and Chat**.

– oppure –

Fare clic con il pulsante destro del mouse sull'icona **HP ProtectTools** nell'area di notifica nella parte destra della barra delle applicazioni, selezionare **Privacy Manager: Sign and Chat**, quindi fare clic su **Configuration** (Configurazione).

– oppure –

Sulla barra degli strumenti di un messaggio e-mail di Microsoft Outlook, fare clic sulla freccia giù accanto a **Send Securely** (Invia in modalità protetta) e fare clic su **Gestione certificati** o su **Trusted Contact Manager** (Gestione contatti attendibili).

– oppure –

Sulla barra degli strumenti di un documento di Microsoft Office, fare clic sulla freccia giù accanto a **Sign and Encrypt** (Firma e crittografa) e fare clic su **Gestione certificati** o su **Trusted Contact Manager** (Gestione contatti attendibili).

Procedure di configurazione

Gestione dei certificati di Privacy Manager

I certificati di Privacy Manager proteggono dati e messaggi mediante una tecnologia di crittografia denominata infrastruttura a chiave pubblica (PKI). PKI richiede che gli utenti ottengano chiavi di crittografia e un certificato di Privacy Manager emesso da un'autorità di certificazione (CA). A differenza della maggior parte delle applicazioni software di crittografia e autenticazione che richiedono di autenticarsi solo periodicamente, Privacy Manager richiede l'autenticazione ogni volta che si firma un messaggio e-mail o un documento di Microsoft Office mediante una chiave di crittografia. Privacy Manager rende il processo di salvataggio e invio dei dati importanti sicuro e protetto.

Richiesta e installazione di un certificato di Privacy Manager

Prima di poter utilizzare le funzioni di protezione di Privacy Manager è necessario richiedere e installare un certificato di Privacy Manager (dall'interno di Privacy Manager) utilizzando un indirizzo e-mail valido. L'indirizzo e-mail deve essere configurato come account in Microsoft Outlook sullo stesso computer dal quale si richiede il certificato di Privacy Manager.

Richiesta di un certificato di Privacy Manager

1. Avviare Privacy Manager e fare clic su **Gestione certificati**.
2. Selezionare **Request a Privacy Manager Certificate** (Richiedi un certificato di Privacy Manager).
3. Leggere il testo presente nella pagina di benvenuto e fare clic su **Avanti**.
4. Leggere il contratto di licenza presente nella pagina License Agreement (Contratto di licenza).
5. Assicurarsi che la casella di controllo accanto a **Check here to accept the terms of this license agreement** (Fare clic qui per accettare i termini del contratto di licenza) sia selezionata e fare clic su **Avanti**.
6. Immettere le informazioni richieste nella pagina Your Certificate Details (Dettagli certificato), quindi fare clic su **Avanti**.
7. Nella pagina Certificate Request Accepted (Richiesta di certificato accettata), fare clic su **Fine**.

   Si riceverà un messaggio e-mail in Microsoft Outlook con allegato il certificato di Privacy Manager.

Installazione di un certificato di Privacy Manager

1. Quando si riceve il messaggio e-mail con il certificato di Privacy Manager Certificate allegato, aprire l'e-mail e fare clic sul pulsante **Setup** (Installa), nell'angolo inferiore destro del messaggio.
2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
3. Nella pagina Certificate Installed (Certificato installato) fare clic su **Avanti**.
4. Nella pagina Certificate Backup (Backup certificato) immettere il nome e il percorso per il file di backup oppure fare clic su **Sfoglia** per cercare un percorso.

   △ **ATTENZIONE:** Assicurarsi di salvare il file in un percorso diverso dall'unità disco rigido e conservarlo in un posto sicuro. Il file dovrà essere riservato all'uso personale e sarà richiesto nel caso in cui risulti necessario ripristinare il certificato di Privacy Manager e le chiavi associate.

5. Immettere e confermare una password, quindi fare clic su **Avanti**.

6. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

7. Se si decide di iniziare il processo di invito di contatti attendibili, seguire le istruzioni visualizzate.

   – oppure –

   Se si sceglie Annulla, per informazioni sull'aggiunta di contatti attendibili in un secondo momento, fare riferimento alla sezione Gestione di contatti attendibili.

Visualizzazione dei dettagli del certificato di Privacy Manager

1. Avviare Privacy Manager e fare clic su **Gestione certificati**.
2. Fare clic su un **Privacy Manager Certificate** (Certificato Privacy Manager).
3. Selezionare **Certificate details** (Dettagli certificato).
4. Dopo aver terminato la visualizzazione dei dettagli, fare clic su **OK**.

Rinnovo di un certificato di Privacy Manager

Quando si avvicina la scadenza del certificato di Privacy Manager, si riceverà la notifica della necessità di rinnovo:

1. Avviare Privacy Manager e fare clic su **Gestione certificati**.
2. Fare clic su un **Privacy Manager Certificate** (Certificato Privacy Manager).
3. Selezionare **Renew certificate** (Rinnova certificato).
4. Seguire le istruzioni visualizzate per acquistare un nuovo certificato di Privacy Manager.

NOTA: Il processo di rinnovo del certificato di Privacy Manager non sostituisce il precedente certificato di Privacy Manager. Sarà necessario acquistare un nuovo certificato di Privacy Manager e installarlo mediante le stesse procedure illustrate in Richiesta e installazione di un certificato di Privacy Manager.

Impostazione di un certificato predefinito di Privacy Manager

Dall'interno di Privacy Manager sono visibili solo i certificati di Privacy Manager, anche se nel computer sono installati altri certificati di diverse autorità di certificazione.

Per eliminare un certificato di Privacy Manager:

1. Avviare Privacy Manager e fare clic su **Gestione certificati**.
2. Fare clic sul certificato di Privacy Manager che si desidera impostare come predefinito, quindi fare clic su **Set default** (Imposta predefinito).
3. Fare clic su **OK**.

NOTA: Non è obbligatorio utilizzare il certificato predefinito di Privacy Manager. Dalle varie funzioni di Privacy Manager è possibile selezionare uno dei certificati di Privacy Manager da utilizzare.

Eliminazione di un certificato di Privacy Manager

Se si elimina un certificato di Privacy Manager, non sarà possibile aprire i file o visualizzare i dati crittografati con quel certificato. Se si è eliminato per errore un certificato di Privacy Manager, sarà possibile ripristinarlo utilizzando il file di backup creato quando è stato installato il certificato.

Per eliminare un certificato di Privacy Manager:

1. Avviare Privacy Manager e fare clic su **Gestione certificati**.
2. Fare clic sul certificato di Privacy Manager che si desidera eliminare, quindi fare clic su **Avanzate**.
3. Fare clic su **Elimina**.
4. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.
5. Fare clic su **Chiudi**, quindi scegliere **OK**.

Ripristino di un certificato di Privacy Manager

Se si è eliminato per errore un certificato di Privacy Manager, sarà possibile ripristinarlo utilizzando il file di backup creato quando è stato installato o esportato il certificato:

1. Avviare Privacy Manager e fare clic su **Migrazione**.
2. Fare clic su **Import migration file** (Importa file di migrazione).
3. Nella pagina del file di migrazione, fare clic su **Browse** (Sfoglia) per cercare il file .dppsm creato quando è stato installato o esportato il certificato di Privacy Manager, quindi fare clic su **Next** (Avanti).
4. Nella pagina Migration File Import (Importazione file di migrazione), fare clic su **Finish** (Fine).
5. Fare clic su **Chiudi**, quindi scegliere **OK**.

NOTA: Per maggiori informazioni, consultare le sezioni Installazione di un certificato di Privacy Manager o Esportazione dei certificati di Privacy Manager e dei contatti attendibili.

Revoca di un certificato di Privacy Manager

Se si teme che la sicurezza del certificato di Privacy Manager sia stata messa in pericolo, è possibile revocare il certificato:

NOTA: Un certificato di Privacy Manager revocato non viene eliminato. Il certificato può ancora essere utilizzato per visualizzare i file crittografati.

1. Avviare Privacy Manager e fare clic su **Gestione certificati**.
2. Fare clic su **Avanzate**.
3. Fare clic sul certificato di Privacy Manager che si desidera revocare, quindi fare clic su **Revoke** (Revoca).
4. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.
5. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
6. Seguire le istruzioni visualizzate.

Gestione di contatti attendibili

I contatti attendibili sono utenti con i quali si sono scambiati certificati di Privacy Manager, il che consente la comunicazione reciproca protetta.

Aggiunta di contatti attendibili

1. Si invia un messaggio e-mail di invito a un destinatario di contatto attendibile.
2. Il destinatario di contatto attendibile risponde all'e-mail.
3. Si riceve l'e-mail di risposta del destinatario di contatto attendibile e si fa clic su Accetto.

È possibile inviare messaggi e-mail di invito a singoli destinatari dei contatti attendibili oppure è possibile inviarli a tutti i contatti della rubrica di Microsoft Outlook.

NOTA: Per rispondere all'invito di diventare un contatto attendibile, i destinatari dei contatti attendibili devono avere Privacy Manager o il client alternativo installato nel computer. Per informazioni sull'installazione del client alternativo, accedere al sito Web DigitalPersona all'indirizzo http://DigitalPersona.com/PrivacyManager.

Aggiunta di un contatto attendibile

1. Avviare Privacy Manager, fare clic su **Trusted Contacts Manager** (Gestione contatti attendibili) e quindi scegliere **Invite Contacts** (Invita contatti).

   – oppure –

   In Microsoft Outlook, fare clic sulla freccia giù accanto a **Send Securely** (Invia in modalità protetta) sulla barra degli strumenti, quindi fare clic su **Invite Contacts** (Invita contatti).

2. Se viene visualizzata la finestra di dialogo di Privacy Manager, fare clic sul certificato di Privacy Manager che si desidera utilizzare e scegliere **OK**.
3. Quando viene visualizzata la finestra di dialogo Trusted Contact Invitation (Invito contatti attendibili), leggere il testo, quindi scegliere **OK**.

   Verrà generato automaticamente un messaggio e-mail.

4. Immettere uno o più indirizzi e-mail dei destinatari che si desidera aggiungere come contatti attendibili.
5. Modificare il testo e firmare con il proprio nome (opzionale).
6. Fare clic su **Invio**.

   NOTA: Se non si è ottenuto un certificato di Privacy Manager, un messaggio informerà che è necessario disporre di un certificato di Privacy Manager per inviare una richiesta di contatto attendibile. Fare clic su OK per avviare la richiesta guidata dei certificati (Certificate Request Wizard).

7. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
8. Quando si riceve il messaggio e-mail di risposta dal destinatario che accetta l'invito a diventare un contatto attendibile, fare clic su Accetto nell'angolo inferiore destro dell'e-mail.

Viene visualizzata una finestra di dialogo a conferma che il destinatario è stato correttamente aggiunto all'elenco di contatti attendibili.

9. Fare clic su **OK**.

Aggiunta di contatti attendibili mediante la rubrica di Microsoft Outlook

1. Avviare Privacy Manager, fare clic su **Trusted Contacts Manager** (Gestione contatti attendibili), quindi fare clic su **Invite Contacts** (Invita contatti).

   – oppure –

   In Microsoft Outlook, fare clic sulla freccia giù accanto a **Send Securely** (Invia in modalità protetta) sulla barra degli strumenti, quindi fare clic su **Invite All My Outlook Contacts** (Invita tutti i contatti di Outlook).

2. Quando viene visualizzata la pagina Trusted Contact Invitation (Invito contatti attendibili), selezionare gli indirizzi e-mail dei destinatari che si desidera aggiungere come contatti attendibili e fare clic su **Avanti**.

3. Quando viene visualizzata la pagina Sending Invitation (Invio invito), fare clic su **Fine**.

   Verrà generato automaticamente un messaggio e-mail che riporta l'indirizzo e-mail di Microsoft Outlook selezionato.

4. Modificare il testo e firmare con il proprio nome (opzionale).

5. Fare clic su **Invio**.

NOTA: Se non si è ottenuto un certificato di Privacy Manager, un messaggio informerà che è necessario disporre di un certificato di Privacy Manager per inviare una richiesta di contatto attendibile. Fare clic su **OK** per avviare la Certificate Request Wizard (Richiesta guidata certificati).

6. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

NOTA: Quando il messaggio e-mail viene ricevuto dal destinatario di contatto attendibile, il destinatario deve aprire il messaggio e fare clic su Accetto nell'angolo inferiore destro dell'e-mail, quindi scegliere OK quando viene visualizzata la finestra di dialogo di conferma.

7. Quando si riceve il messaggio e-mail di risposta dal destinatario che accetta l'invito a diventare un contatto attendibile, fare clic su Accetto nell'angolo inferiore destro dell'e-mail.

   Viene visualizzata una finestra di dialogo a conferma che il destinatario è stato correttamente aggiunto all'elenco di contatti attendibili.

8. Fare clic su **OK**.

Visualizzazione dei dettagli dei contatti attendibili

1. Avviare Privacy Manager e fare clic su **Trusted Contacts Manager** (Gestione contatti attendibili).

2. Fare clic su un contatto attendibile.

3. Fare clic su **Contact details** (Dettagli contatto).

4. Dopo aver terminato la visualizzazione dei dettagli, fare clic su **OK**.

Eliminazione di un contatto attendibile

1. Avviare Privacy Manager e fare clic su **Trusted Contacts Manager** (Gestione contatti attendibili).
2. Fare clic sul contatto attendibile che si desidera eliminare.
3. Fare clic su **Delete contact** (Elimina contatto).
4. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

Verifica dello stato della revoca per un contatto attendibile

1. Avviare Privacy Manager e fare clic su **Trusted Contacts Manager** (Gestione contatti attendibili).
2. Fare clic su un contatto attendibile.
3. Fare clic sul pulsante **Avanzate**.

   Viene visualizzata la finestra di dialogo Advanced Trusted Contact Management (Gestione avanzata contatti attendibili).
4. Fare clic su **Check Revocation** (Verifica revoca).
5. Fare clic su **Chiudi**.

Attività generali

Uso di Privacy Manager in Microsoft Office

Dopo aver installato il certificato di Privacy Manager, sul lato destro della barra degli strumenti di tutti i documenti di Microsoft Word, Microsoft Excel e Microsoft PowerPoint viene visualizzato il pulsante Sign and Encrypt (Firma e crittografa).

Configurazione di Privacy Manager in un documento di Microsoft Office

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

– oppure –

1. Avviare Privacy Manager, fare clic su **Impostazioni** e quindi selezionare la scheda **Documenti**.

   – oppure –

   Sulla barra degli strumenti di un documento di Microsoft Office, fare clic sulla freccia giù accanto a **Sign and Encrypt** (Firma e crittografa), quindi fare clic su **Impostazioni**.
2. Selezionare le azioni che si desidera configurare, quindi fare clic su **OK**.

Firma di un documento di Microsoft Office

1. In Microsoft Word, Microsoft Excel o Microsoft PowerPoint, creare e salvare un documento.
2. Fare clic sulla freccia giù accanto a **Sign and Encrypt** (Firma e crittografa), quindi scegliere **Sign Document** (Firma documento).

3. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

4. Quando viene visualizzata la finestra di dialogo di conferma, leggere il testo, quindi scegliere **OK**.

Se in seguito si desidera modificare il documento, procedere come segue:

1. Fare clic sul pulsante **Office** nell'angolo superiore sinistro della schermata.

2. Fare clic su **Prepare** (Prepara) quindi su **Mark as Final** (Contrassegna come finale).

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

4. Una volta completata la modifica, firmare di nuovo il documento.

Aggiunta di una riga per la firma di un documento Microsoft Word o Microsoft Excel

Privacy Manager consente di aggiungere una riga per la firma quando si firma un documento di Microsoft Word o Microsoft Excel:

1. In Microsoft Word o Microsoft Excel creare e salvare un documento.

2. Fare clic sul menu **Home**.

3. Fare clic sulla freccia giù accanto a **Sign and Encrypt** (Firma e crittografa) quindi scegliere **Add Signature Line Before Signing** (Aggiungi riga prima di firmare).

NOTA: Viene visualizzato un segno di spunta accanto alla voce Add Signature Line Before Signing (Aggiungi riga prima di firmare) quando questa opzione è selezionata. Per impostazione predefinita, questa opzione è attivata.

4. Fare clic sulla freccia giù accanto a **Sign and Encrypt** (Firma e crittografa), quindi scegliere **Sign Document** (Firma documento).

5. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

Aggiunta di firmatari suggeriti a un documento Microsoft Word o Microsoft Excel

È possibile aggiungere più righe per la firma nel documento indicando i firmatari suggeriti. Un firmatario suggerito è un utente designato dal proprietario di un documento Microsoft Word o Microsoft Excel per l'aggiunta di una riga per la firma all'interno del documento. I firmatari suggeriti possono essere l'utente stesso o una persona a cui si desidera far firmare il documento. Ad esempio, se si prepara un documento che deve essere firmato da tutti i membri di un reparto, è possibile includere le righe per la firma degli utenti nella parte inferiore dell'ultima pagina del documento con le istruzioni per firmare in una data specifica.

Per aggiungere un firmatario suggerito in un documento Microsoft Word o Microsoft Excel:

1. In Microsoft Word o Microsoft Excel, creare e salvare un documento.

2. Fare clic sul menu **Insert** (Inserisci).

3. Nel gruppo **Testo** sulla barra degli strumenti, fare clic sulla freccia accanto a **Signature Line** (Riga per la firma) e scegliere **Privacy Manager Signature Provider** (Provider di firme di Privacy Manager).

   Viene visualizzata la finestra di dialogo Signature Setup (Impostazione firme).

4. Nella casella sotto **Suggested signer** (Firmatario suggerito), immettere il nome del firmatario suggerito.

5. Nella casella sotto **Instructions to the signer** (Istruzioni per il firmatario), immettere un messaggio per questo firmatario suggerito.

NOTA: Il messaggio verrà visualizzato al posto di un titolo e verrà eliminato o sostituito dal titolo dell'utente quando il documento viene firmato.

6. Selezionare la casella di controllo **Show sign date in signature line** (Visualizza data della firma sulla riga della firma).

7. Selezionare la casella di controllo **Show signer's title in signature line** (Visualizza titolo del firmatario sulla riga della firma) per visualizzare il titolo.

NOTA: Poiché il proprietario del documento assegna i firmatari suggeriti al documento, se le caselle di controllo **Show sign date in signature line** (Visualizza data della firma sulla riga della firma) e/o **Show signer's title in signature line** (Visualizza titolo del firmatario sulla riga della firma) non vengono selezionate, il firmatario suggerito non sarà in grado di visualizzare la data e/o il titolo sulla riga della firma anche se le impostazioni del relativo documento sono configurate in tal senso.

8. Fare clic su **OK**.

Aggiunta di una riga per la firma dei firmatari suggeriti

Quando i firmatari suggeriti aprono il documento, verrà visualizzato il loro nome in parentesi, il che indica che è richiesta la firma.

Per firmare il documento:

1. Fare doppio clic sulla riga per la firma appropriata.

2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

   La riga per la firma verrà visualizzata secondo le impostazioni specificate dal proprietario del documento.

Crittografia di un documento di Microsoft Office

È possibile crittografare un documento di Microsoft Office per un utente e per i relativi contatti attendibili. Quando un documento viene crittografato e poi chiuso, l'utente e i relativi contatti attendibili selezionati dall'elenco devono autenticarsi prima di poter aprire il documento.

Per crittografare un documento di Microsoft Office:

1. In Microsoft Word, Microsoft Excel o Microsoft PowerPoint, creare e salvare un documento.

2. Fare clic sul menu **Home**.

3. Fare clic sulla freccia giù accanto a **Sign and Encrypt** (Firma e crittografa), quindi fare clic su **Encrypt Document** (Crittografa documento).

   Viene visualizzata la finestra di dialogo Select Trusted Contacts (Seleziona contatti attendibili).

4. Fare clic sul nome di un contatto attendibile che potrà aprire il documento e visualizzarne il contenuto.

NOTA: Per selezionare più nomi di contatti attendibili, tenere premuto il tasto Ctrl e fare clic sui singoli nomi.

5. Fare clic su **OK**.

6. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

Se in seguito si desidera modificare il documento, seguire i passaggi riportati in **Firma di un documento di Microsoft Office**. Quando la crittografia viene rimossa, è possibile modificare il documento. Seguire i passaggi riportati in questa sezione per crittografare di nuovo il documento.

Rimozione della crittografia da un documento di Microsoft Office

Quando si rimuove la crittografia da un documento di Microsoft Office, l'utente e i relativi contatti attendibili non devono più autenticarsi per aprire e visualizzare il contenuto del documento.

Per rimuovere la crittografia da un documento di Microsoft Office:

1. Aprire un documento crittografato di Microsoft Word, Microsoft Excel o Microsoft PowerPoint.

2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

3. Fare clic sul menu **Home**.

4. Fare clic sulla freccia giù accanto a **Sign and Encrypt** (Firma e crittografa) quindi fare clic su **Remove Encryption** (Rimuovi crittografia).

Invio di un documento crittografato di Microsoft Office

È possibile allegare un documento crittografato di Microsoft Office a un messaggio e-mail senza firmare o crittografare il messaggio stesso. A tal fine, creare e inviare un messaggio e-mail con un documento firmato o crittografato, come si fa normalmente per un messaggio e-mail contenente un allegato.

Per una protezione ottimale, tuttavia, è consigliabile crittografare il messaggio e-mail quando si allega un documento crittografato o firmato di Microsoft Office.

Per inviare un messaggio e-mail crittografato con un documento allegato firmato o crittografato di Microsoft Office, procedere come segue:

1. In Microsoft Outlook, fare clic su **Nuovo** o **Rispondi**.

2. Digitare il messaggio e-mail.

3. Allegare il documento di Microsoft Office.

4. Per ulteriori istruzioni, fare riferimento alla sezione Crittografia e invio di un messaggio e-mail.

Visualizzazione di un documento firmato di Microsoft Office

NOTA: Non è necessario disporre di un certificato di Privacy Manager per poter visualizzare un documento firmato di Microsoft Office.

Quando si apre un documento firmato di Microsoft Office, viene visualizzata una finestra di dialogo Signatures (Firme) accanto al documento, che contiene il nome dell'utente che ha firmato il documento e la data della firma. È possibile fare clic con il pulsante destro del mouse sul nome per visualizzare ulteriori dettagli.

Visualizzazione di un documento crittografato di Microsoft Office

Per visualizzare un documento crittografato di Microsoft Office da un altro computer, è necessario che Privacy Manager sia installato su quel computer. Inoltre, è necessario importare il certificato di Privacy Manager utilizzato per crittografare il file.

Un contatto attendibile che desidera visualizzare un documento crittografato di Microsoft Office dovrà disporre di un certificato di Privacy Manager e di Privacy Manager installato nel computer. Inoltre, il contatto attendibile deve essere selezionato dal proprietario del documento crittografato di Microsoft Office.

Uso di Privacy Manager in Microsoft Outlook

Quando si installa Privacy Manager, viene visualizzato un pulsante Privacy sulla barra degli strumenti di Microsoft Outlook e un pulsante Send Securely (Invia in modalità protetta) viene visualizzato sulla barra degli strumenti di ciascun messaggio e-mail di Microsoft Outlook.

Configurazione di Privacy Manager per Microsoft Outlook

1. Avviare **Privacy Manager**, fare clic su **Impostazioni** e quindi selezionare la scheda **E-mail**.

   – oppure –

   Sulla barra degli strumenti principale di Microsoft Outlook, fare clic sulla freccia giù accanto a **Privacy**, quindi fare clic su **Impostazioni**.

   – oppure –

   Sulla barra degli strumenti di un messaggio e-mail di Microsoft Outlook, fare clic sulla freccia giù accanto a **Send Securely** (Invia in modalità protetta), quindi fare clic su **Impostazioni**.

2. Selezionare le azioni che si desidera eseguire quando si invia un messaggio e-mail protetto e scegliere **OK**.

Firma e invio di un messaggio e-mail

- In Microsoft Outlook, fare clic su **Nuovo** o **Rispondi**.
- Digitare il messaggio e-mail.
- Fare clic sulla freccia giù accanto a **Send Securely** (Invia in modalità protetta), quindi fare clic su **Sign and Send** (Firma e invia).
- Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

Crittografia e invio di un messaggio e-mail

I messaggi e-mail cui viene applicata la firma digitale e la crittografia possono essere visualizzati solo dalle persone selezionate dell'elenco dei contatti attendibili.

Per crittografare e inviare un messaggio e-mail a un contatto attendibile:

1. In Microsoft Outlook, fare clic su **Nuovo** o **Rispondi**.
2. Digitare il messaggio e-mail.
3. Fare clic sulla freccia giù accanto a **Send Securely** (Invia in modalità protetta), quindi fare clic su **Seal for Trusted Contacts and Send** (Crittografa per contatti attendibili e invia).
4. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

Visualizzazione di un messaggio e-mail crittografato

Quando si apre un messaggio e-mail crittografato, viene visualizzata l'etichetta di protezione nell'intestazione dell'e-mail. L'etichetta di protezione fornisce le seguenti informazioni:

- Le credenziali utilizzate per verificare l'identità della persona che ha firmato l'e-mail
- Il prodotto utilizzato per verificare le credenziali della persona che ha firmato l'e-mail

Uso di Privacy Manager in Windows Live Messenger

Aggiunta dell'attività Privacy Manager Chat

Per aggiungere la funzione Privacy Manager Chat in Windows Live Messenger, procedere come segue:

1. Accedere a Windows Live Home.
2. Fare clic sull'icona **Windows Live**, quindi su **Servizi Windows Live**.
3. Selezionare **Gallery**, quindi fare clic su **Messenger**.
4. Fare clic su **Attività**, quindi scegliere **Sicurezza**.
5. Fare clic su **Privacy Manager Chat** e seguire le istruzioni visualizzate.

Avvio di Privacy Manager Chat

NOTA: Per poter utilizzare Privacy Manager Chat, entrambe le parti devono disporre di Privacy Manager e di un certificato di Privacy Manager installati nel computer. Per maggiori dettagli sull'installazione di un certificato di Privacy Manager, vedere Richiesta e installazione di un certificato di Privacy Manager a pagina 5.

1. Per avviare Privacy Manager Chat in Windows Live Messenger, eseguire una delle seguenti procedure:

   a. Fare clic con il pulsante destro del mouse su un contatto online in Live Messenger, quindi scegliere **Start an Activity** (Avvia un'attività).

   b. Fare clic su **Start Privacy Manager Chat** (Avvia Privacy Manage Chat).

   – oppure –

   a. Fare doppio clic su un contatto online in Live Messenger, quindi fare clic sul menu **Conversation** (Conversazione).

   b. Fare clic su **Operazione**, quindi su **Start Privacy Manager Chat** (Avvia Privacy Manager Chat).

   Privacy Manager invia al contatto un invito ad avviare Privacy Manager Chat. Quando il contatto invitato accetta, viene aperta la finestra Privacy Manager Chat. Se il contatto invitato non dispone di Privacy Manager, gli verrà offerto di scaricarlo.

2. Fare clic su **Avvio** per iniziare una chat protetta.

Configurazione di Privacy Manager Chat per Windows Live Messenger

1. In Privacy Manager Chat, fare clic sul pulsante **Impostazioni**.

   – oppure –

   In Privacy Manager, fare clic su **Impostazioni** e quindi selezionare la scheda **Chat**.

   – oppure –

   Nel Visualizzatore cronologia di Privacy Manager, fare clic sul pulsante **Impostazioni**.

2. Per specificare il tempo di attesa di Privacy Manager Chat prima del blocco della sessione, selezionare un numero dalla casella **Lock session after _ minutes of inactivity** (Blocca sessione dopo _ minuti di inattività).

3. Per indicare una cartella per la cronologia delle sessioni di chat, fare clic su **Sfoglia** per cercarla, quindi fare clic su **OK**.

4. Per crittografare e salvare automaticamente le sessioni quando le si chiude, selezionare la casella di controllo **Automatically save secure chat history** (Salva automaticamente cronologia delle chat protette).

5. Fare clic su **OK**.

Chat nella finestra Privacy Manager Chat

Una volta avviato Privacy Manager Chat, verrà aperta una finestra Privacy Manager Chat in Windows Live Messenger. L'uso di Privacy Manager Chat è fondamentalmente simile a quello di Windows Live Messenger, tranne per il fatto che nella finestra Privacy Manager Chat sono disponibili le seguenti funzioni aggiuntive:

- **Salva**: fare clic su questo pulsante per salvare la sessione di chat nella cartella indicata nelle impostazioni di configurazione. È anche possibile configurare Privacy Manager Chat per il salvataggio automatico di ogni sessione quando la si chiude.
- **Nascondi tutto** e **Mostra tutto**: fare clic sul pulsante appropriato per espandere o comprimere i messaggi riportati nella finestra Secure Communications (Comunicazioni protette). È inoltre possibile nascondere o mostrare singoli messaggi facendo clic sulla relativa intestazione.
- **Trillo**: fare clic su questo pulsante per richiedere l'autenticazione dal contatto.
- **Blocca**: fare clic su questo pulsante per chiudere la finestra Privacy Manager Chat e tornare alla finestra Chat Entry (Apertura chat). Per visualizzare di nuovo la finestra Secure Communications (Comunicazioni protette), fare clic su **Riprendi sessione**, quindi autenticarsi utilizzando il metodo di accesso di sicurezza selezionato.
- **Invio**: fare clic su questo pulsante per inviare un messaggio crittografato al contatto.
- **Invia messaggio firmato**: selezionare questa casella di controllo per firmare e crittografare elettronicamente i messaggi. Quindi, se il messaggio viene alterato, verrà contrassegnato come non valido quando il destinatario lo riceve. È necessario autenticarsi ogni volta che si invia un messaggio firmato.
- **Invia messaggio nascosto**: selezionare questa casella di controllo per crittografare e inviare un messaggio mostrando solo l'intestazione. Il contatto deve autenticarsi per poter leggere il contenuto del messaggio.

Visualizzazione della cronologia chat

Nel Chat History Viewer di Privacy Manager Chat vengono riportati i file di sessione crittografati di Privacy Manager Chat. È possibile salvare le sessioni facendo clic su Salva nella finestra Privacy Manager Chat oppure configurando il salvataggio automatico nella scheda Chat di Privacy Manager. Nel visualizzatore, ciascuna sessione riporta il nome (crittografato) del contatto, con data e ora di inizio e fine della sessione. Per impostazione predefinita, vengono riportate le sessioni per tutti gli account e-mail impostati dall'utente. È possibile utilizzare il menu **Display history for** (Visualizza cronologia per) per selezionare solo account specifici da visualizzare.

Avvio di Chat History Viewer:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Fare clic su **Privacy Manager: Sign and Chat**, quindi fare clic su **Chat History Viewer**.

   – oppure –

   ▲ In una sessione di chat, fare clic su **Visualizzatore cronologia** o su **History** (Cronologia).

   – oppure –

   ▲ Nella pagina Chat Configuration (Configurazione chat), fare clic su **Start Live Messenger History Viewer** (Avvia il Visualizzatore cronologia di Live Messenger).

Rivelazione di tutte le sessioni

La rivelazione di tutte le sessioni consente di visualizzare il nome del contatto decrittografato per le sessioni selezionate e per tutte le sessioni dello stesso account.

1. In Chat History Viewer, fare clic con il pulsante del mouse su una sessione qualsiasi e selezionare **Reveal All Sessions** (Rivela tutte le sessioni).
2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

   I nomi dei contatti vengono decrittografati.
3. Fare doppio clic su una sessione per visualizzarne il contenuto.

Rivelazione delle sessioni di un account specifico

La rivelazione di una sessione consente di visualizzare il nome del contatto decrittografato per la sessione selezionata.

1. In Chat History Viewer, fare clic con il pulsante del mouse su una sessione qualsiasi e selezionare **Reveal Session** (Rivela sessione).
2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

   I nomi dei contatti vengono decrittografati.
3. Fare doppio clic sulla sessione rivelata per visualizzarne il contenuto.

NOTA: Le altre sessioni crittografate con lo stesso certificato riporteranno un'icona con lucchetto aperto, per indicare che è possibile visualizzarle facendo doppio clic su una di esse senza un'ulteriore autenticazione. Le sessioni crittografate con un certificato diverso riporteranno un'icona con lucchetto chiuso, per indicare che per queste sessioni è richiesta un'ulteriore autenticazione per visualizzarne il contenuto o i nomi dei contatti.

Visualizzazione di un ID sessione

▲ Nel Visualizzatore cronologia Chat, fare clic con il pulsante del mouse su una sessione rivelata e selezionare **View session ID** (Visualizza ID sessione).

Visualizzazione di una sessione

Quando si visualizza una sessione viene aperto il relativo file da visualizzare. Se la sessione non è stata rivelata (con la visualizzazione del nome del contatto decrittografato) in precedenza, viene rivelata contemporaneamente.

1. In Chat History Viewer, fare clic con il pulsante del mouse su una sessione rivelata e scegliere **View** (Visualizza).
2. Se richiesto, autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

   Il contenuto della sessione viene decrittografato.

Ricerca di testo specifico nelle sessioni

È possibile cercare testo solo nelle sessioni rivelate (decrittografate) visualizzate nella finestra del visualizzatore. Si tratta delle sessioni in cui il nome del contatto viene visualizzato in testo normale.

1. In Chat History Viewer, fare clic sul pulsante **Search** (Cerca).
2. Immettere il testo da cercare, configurare eventuali parametri di ricerca desiderati, infine scegliere **OK**.

   Le sessioni contenenti il testo vengono evidenziate nella finestra del visualizzatore.

Eliminazione di una sessione

1. Selezionare una sessione di cronologia chat.
2. Fare clic su **Elimina**.

Aggiunta o rimozione di colonne

Per impostazione predefinita, in Chat History Viewer vengono visualizzate le 3 colonne più utilizzate. È possibile aggiungere o rimuovere colonne dalla visualizzazione.

Per aggiungere colonne alla visualizzazione:

1. Fare clic con il pulsante destro del mouse su un'intestazione di colonna e selezionare **Add/Remove Columns** (Aggiungi/Rimuovi colonne).
2. Selezionare un'intestazione di colonna nel pannello di sinistra, quindi fare clic su **Aggiungi** per spostarla nel pannello di destra.

Per rimuovere colonne dalla visualizzazione:

1. Fare clic con il pulsante destro del mouse su un'intestazione di colonna e selezionare **Add/Remove Columns** (Aggiungi/Rimuovi colonne).
2. Selezionare un'intestazione di colonna nel pannello di destra, quindi fare clic su **Rimuovi** per spostarla nel pannello di sinistra.

Filtro delle sessioni visualizzate

In Chat History Viewer viene riportato un elenco delle sessioni di tutti gli account.

Visualizzazione delle sessioni di un account specifico

- In Chat History Viewer, selezionare un account dal menu **Display history for** (Visualizza cronologia per).

Visualizzazione delle sessioni per un intervallo di date

1. Nel Visualizzatore cronologia Chat, fare clic sull'icona **Advanced Filter** (Filtro avanzato).

   Viene visualizzata la finestra di dialogo Advanced Filter (Filtro avanzato).

2. Selezionare la casella di controllo **Display only sessions within specified date range** (Visualizza solo le sessioni entro l'intervallo di date specificato).

3. Nelle caselle **From date** (Da) e **To date** (A), immettere giorno, mese e/o anno oppure fare clic sulla freccia accanto al calendario per selezionare le date.

4. Fare clic su **OK**.

Visualizzazione delle sessioni salvate in una cartella diversa da quella predefinita

1. Nel Visualizzatore cronologia Chat, fare clic sull'icona **Advanced Filter** (Filtro avanzato).

2. Selezionare la casella di controllo **Use an alternate history files folder** (Utilizza una cartella diversa per i file di cronologia).

3. Immettere il percorso della cartella o scegliere **Sfoglia** per cercare una cartella.

4. Fare clic su **OK**.

Attività avanzate

Migrazione dei certificati di Privacy Manager e dei contatti attendibili su un altro computer

È possibile migrare in modo protetto i certificati di Privacy Manager e i contatti attendibili su un altro computer. A tal fine, esportarli come file protetto da password in un percorso di rete o in un dispositivo di archiviazione rimovibile, quindi importare il file nel nuovo computer.

Esportazione dei certificati di Privacy Manager e dei contatti attendibili

Per esportare i certificati di Privacy Manager e i contatti attendibili in un file protetto da password, procedere come segue:

1. Avviare Privacy Manager e fare clic su **Migrazione**.

2. Fare clic su **Export migration file** (Esporta file di migrazione).

3. Nella pagina Select Data (Selezione dati), selezionare le categorie di dati da inserire nel file di migrazione, quindi fare clic su **Avanti**.

4. Nella pagina Migration File (File di migrazione), immettere un nome file o fare clic su **Sfoglia** per cercare un percorso, quindi fare clic su **Avanti**.

5. Immettere e confermare una password, quindi fare clic su **Avanti**.

NOTA: Memorizzare questa password in un posto sicuro, perché servirà per importare il file di migrazione.

6. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
7. Nella pagina Migration File Saved (File di migrazione salvato), fare clic su **Fine**.

Importazione dei certificati di Privacy Manager e dei contatti attendibili

Per importare i certificati di Privacy Manager e i contatti attendibili in un file protetto da password, procedere come segue:

1. Avviare Privacy Manager e fare clic su **Migrazione**.
2. Fare clic su **Import migration file** (Importa file di migrazione).
3. Nella pagina Select Data (Selezione dati), selezionare le categorie di dati da inserire nel file di migrazione, quindi fare clic su **Avanti**.
4. Nella pagina Migration File (File di migrazione), immettere un nome file o fare clic su **Sfoglia** per cercare un percorso, quindi fare clic su **Avanti**.
5. Nella pagina Migration File Import (Importazione file di migrazione), fare clic su **Finish** (Fine).

6 File Sanitizer for HP ProtectTools

File Sanitizer è uno strumento che consente di distruggere in modo sicuro risorse quali informazioni o file personali, dati cronologici o relativi al Web o altri componenti di dati presenti nel computer e di eseguire una pulizia periodica dell'unità disco rigido.

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

Informazioni sulla distruzione

L'eliminazione di una risorsa in Windows non rimuove completamente il contenuto della risorsa dall'unità disco rigido. Windows elimina soltanto il riferimento alla risorsa. Il contenuto della risorsa rimane ancora sull'unità disco rigido fino a quando una nuova risorsa sovrascrive la stessa area dell'unità disco rigido con nuove informazioni.

La distruzione differisce da un'operazione di eliminazione standard di Windows® (denominata anche eliminazione semplice in File Sanitizer) poiché quando si distrugge una risorsa, viene richiamato un algoritmo che nasconde i dati rendendone potenzialmente impossibile il recupero.

Quando si sceglie un profilo di distruzione tra High Security (Protezione alta), Medium Security (Protezione media) o Low Security (Protezione bassa), vengono automaticamente selezionati un elenco predefinito di risorse e un metodo di cancellazione per la distruzione. È inoltre possibile personalizzare un profilo di distruzione, il che consente di specificare il numero di cicli di distruzione, quali risorse includere nella distruzione, quali risorse confermare prima della distruzione e quali escludere.

È possibile impostare un programma di distruzione automatico ed è inoltre possibile distruggere le risorse manualmente quando lo si desidera.

Informazioni sulla pulizia dello spazio libero

La pulizia dello spazio libero consente di scrivere in modo sicuro dati casuali sulle risorse eliminate, impedendo agli utenti la visualizzazione del contenuto originale della risorsa eliminata.

NOTA: La pulizia dello spazio libero è riservata alle risorse eliminate utilizzando il Cestino di Windows o alle risorse eliminate manualmente. La pulizia dello spazio libero non fornisce protezione aggiuntiva alle risorse distrutte.

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**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. 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 HP ProtectTools nell'area di notifica all'estrema destra della barra delle applicazioni, fare clic su File Sanitizer, quindi scegliere Open File Sanitizer (Avvia File Sanitizer).

Impostazione di un programma di pulizia dello spazio libero

NOTA: La pulizia dello spazio libero è riservata alle risorse eliminate utilizzando il Cestino di Windows o alle risorse eliminate manualmente. La pulizia dello spazio libero non fornisce protezione aggiuntiva alle risorse distrutte.

Per impostare un programma di pulizia dello spazio libero

1. Avviare File Sanitizer e fare clic su **Free Space Bleaching** (Pulizia dello spazio libero).
2. Selezionare la casella di controllo **Activate Scheduler** (Attiva pianificazione), immettere la password di Windows, quindi specificare giorno e ora in cui eseguire la pulizia del disco rigido.
3. Fare clic su **Applica**, quindi su **OK**.

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.

Selezione o creazione di un profilo di distruzione

È possibile specificare un metodo di cancellazione e selezionare le risorse da distruggere scegliendo un profilo predefinito o creando un profilo personalizzato.

Selezione di un profilo di distruzione predefinito

Quando si sceglie un profilo di distruzione predefinito tra High Security (Protezione alta), Medium Security (Protezione media) o Low Security (Protezione bassa), vengono automaticamente selezionati un metodo di cancellazione predefinito e un elenco di risorse. È possibile fare clic sul pulsante View Details (Visualizza dettagli) per visualizzare l'elenco predefinito delle risorse selezionate per la distruzione.

Per selezionare un profilo di distruzione predefinito:

1. Avviare **File Sanitizer** e fare clic su **Impostazioni**.
2. Fare clic su un profilo di distruzione predefinito.
3. Fare clic su **View Details** (Visualizza dettagli) per visualizzare l'elenco delle risorse selezionate per la distruzione.
4. In **Shred the following** (Distruggi seguenti), selezionare la casella di controllo accanto a ciascuna risorsa che si desidera confermare prima della distruzione.
5. Fare clic su **Apply** (Applica), quindi su **OK**.

Personalizzazione di un profilo di distruzione

Durante la creazione di un profilo di distruzione, viene specificato il numero di cicli di distruzione, quali risorse si desidera includere nella distruzione, quali risorse confermare prima della distruzione e quali escludere:

1. Avviare File Sanitizer e scegliere **Impostazioni**, fare clic su **Advanced Security Settings** (Impostazioni di sicurezza avanzate), quindi scegliere **View Details** (Visualizza dettagli).
2. Specificare il numero di cicli di distruzione.

NOTA: Il numero selezionato di cicli di distruzione verrà eseguito per ciascuna risorsa. Se ad esempio si scelgono 3 cicli di distruzione, viene eseguito 3 volte un algoritmo che nasconde i dati. Se si scelgono cicli di distruzione a più alta protezione, la distruzione potrebbe richiedere molto tempo; tuttavia, maggiore è il numero di cicli di distruzione specificato, più protetto risulterà il computer.

3. Selezionare le risorse che si desidera distruggere:
   a. In **Available shred options** (Opzioni di distruzione disponibili), fare clic su una risorsa, quindi scegliere **Aggiungi**.
   b. Per aggiungere una risorsa personalizzata, fare clic su Add Custom Option (Aggiungi opzione personalizzata), immettere il nome del file o della cartella, quindi scegliere **OK**. Fare clic sulla risorsa personalizzata, quindi scegliere **Aggiungi**.

   NOTA: Per eliminare una risorsa dalle opzioni di distruzione disponibili, fare clic sulla risorsa, quindi scegliere **Elimina**.

4. In **Shred the following** (Distruggi seguenti), selezionare la casella di controllo accanto a ciascuna risorsa che si desidera confermare prima della distruzione.

NOTA: Per rimuovere una risorsa dall'elenco di distruzione, fare clic sulla risorsa, quindi scegliere **Rimuovi**.

5. In **Do not shred the following** (Non distruggere seguenti), fare clic su **Aggiungi** per selezionare le risorse specifiche che si desidera escludere dalla distruzione.

NOTA: È possibile escludere dalla distruzione solo estensioni di file. Se ad esempio si aggiunge l'estensione .BMP, tutti i file con estensione .BMP verranno esclusi dalla distruzione.

Per rimuovere una risorsa dall'elenco delle esclusioni, fare clic sulla risorsa, quindi scegliere **Elimina**.

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

Personalizzazione di un profilo di eliminazione semplice

Il profilo di eliminazione semplice esegue un'eliminazione standard della risorsa senza distruzione. Quando si personalizza un profilo di eliminazione semplice, è possibile specificare quali risorse includere in un'eliminazione semplice, quali risorse confermare prima che venga eseguita un'eliminazione semplice e quali risorse escludere dall'eliminazione semplice:

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

1. Avviare **File Sanitizer**, fare clic su **Impostazioni**, scegliere **Simple Delete Setting** (Impostazioni di eliminazione semplice), quindi fare clic su **View Details** (Visualizza dettagli).
2. Selezionare le risorse che si desidera eliminare:
   a. In **Available delete options** (Opzioni di eliminazione disponibili), fare clic sulla risorsa, quindi scegliere **Aggiungi**.
   b. Per aggiungere una risorsa personalizzata, fare clic su **Add Custom Option** (Aggiungi opzione personalizzata), immettere il nome del file o della cartella, quindi scegliere **OK**. Fare clic sulla risorsa personalizzata, quindi scegliere **Aggiungi**.

   NOTA: Per eliminare una risorsa dalle opzioni di eliminazione disponibili, fare clic sulla risorsa, quindi scegliere **Elimina**.
3. In **Delete the following** (Elimina seguenti), selezionare la casella di controllo accanto a ciascuna risorsa che si desidera confermare prima dell'eliminazione.

NOTA: Per rimuovere una risorsa dall'elenco di eliminazione, fare clic sulla risorsa, quindi scegliere **Rimuovi**.

4. In **Do not shred the following** (Non distruggere seguenti), fare clic su **Aggiungi** per selezionare le risorse specifiche che si desidera escludere dalla distruzione.

NOTA: È possibile escludere dalla distruzione solo estensioni di file. Se ad esempio si aggiunge l'estensione .BMP, tutti i file con estensione .BMP verranno esclusi dall'eliminazione.

Per rimuovere una risorsa dall'elenco delle esclusioni, fare clic sulla risorsa, quindi scegliere **Elimina**.

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

Impostazione di un piano di distruzione

1. Avviare File Sanitizer e fare clic su **Shred** (Distruggi).
2. Selezionare un'opzione di distruzione:
   - **Windows startup** (Avvio di Windows): scegliere questa opzione per distruggere tutte le risorse selezionate all'avvio di Windows.
   - **Windows shutdown** (Arresto di Windows): scegliere questa opzione per distruggere tutte le risorse selezionate all'arresto di Windows.

     NOTA: Quando questa opzione è selezionata, al momento dell'arresto verrà visualizzata una finestra di dialogo che chiede se si desidera continuare con la distruzione delle risorse selezionate o se si desidera annullare la procedura. Fare clic su Sì per annullare la procedura di distruzione oppure su No per procedere con la distruzione.
   - **Web browser open** (Avvio del browser Web): scegliere questa opzione per distruggere tutte le risorse selezionate relative al Web, come la cronologia URL del browser, quando si avvia un browser Web.
   - **Web browser quit** (Uscita dal browser Web): scegliere questa opzione per distruggere tutte le risorse selezionate relative al Web, come la cronologia URL del browser, quando si chiude un browser Web.
   - **Scheduler** (Pianificazione): selezionare la casella di controllo Activate Scheduler (Attiva pianificazione), immettere la password di Windows, quindi specificare giorno e ora in cui distruggere le risorse selezionate.
3. Fare clic su **Applica**, quindi su **OK**.

Impostazione di un programma di pulizia dello spazio libero

NOTA: La pulizia dello spazio libero è riservata alle risorse eliminate utilizzando il Cestino di Windows o alle risorse eliminate manualmente. La pulizia dello spazio libero non fornisce protezione aggiuntiva alle risorse distrutte.

Per impostare un programma di pulizia dello spazio libero

1. Avviare File Sanitizer e fare clic su **Free Space Bleaching** (Pulizia dello spazio libero).
2. Selezionare la casella di controllo **Activate Scheduler** (Attiva pianificazione), immettere la password di Windows, quindi specificare giorno e ora in cui eseguire la pulizia del disco rigido.
3. Fare clic su **Applica**, quindi su **OK**.

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.

Selezione o creazione di un profilo di distruzione

Selezione di un profilo di distruzione predefinito

Quando si sceglie un profilo di distruzione predefinito tra High Security (Protezione alta), Medium Security (Protezione media) o Low Security (Protezione bassa), vengono automaticamente selezionati un metodo di cancellazione predefinito e un elenco di risorse. È possibile fare clic sul pulsante View

Details (Visualizza dettagli) per visualizzare l'elenco predefinito delle risorse selezionate per la distruzione.

Per selezionare un profilo di distruzione predefinito:

1. Avviare **File Sanitizer** e fare clic su **Impostazioni**.
2. Fare clic su un profilo di distruzione predefinito.
3. Fare clic su **View Details** (Visualizza dettagli) per visualizzare l'elenco delle risorse selezionate per la distruzione.
4. In **Shred the following** (Distruggi seguenti), selezionare la casella di controllo accanto a ciascuna risorsa che si desidera confermare prima della distruzione.
5. Fare clic su **Annulla**, quindi su **OK**.

Personalizzazione di un profilo di distruzione

Durante la creazione di un profilo di distruzione, viene specificato il numero di cicli di distruzione, quali risorse si desidera includere nella distruzione, quali risorse confermare prima della distruzione e quali escludere:

1. Avviare File Sanitizer e scegliere **Impostazioni**, fare clic su **Advanced Security Settings** (Impostazioni di sicurezza avanzate), quindi scegliere **View Details** (Visualizza dettagli).
2. Specificare il numero di cicli di distruzione.

NOTA: Il numero selezionato di cicli di distruzione verrà eseguito per ciascuna risorsa. Se ad esempio si scelgono 3 cicli di distruzione, viene eseguito 3 volte un algoritmo che nasconde i dati. Se si scelgono cicli di distruzione a più alta protezione, la distruzione potrebbe richiedere molto tempo; tuttavia, maggiore è il numero di cicli di distruzione specificato, più protetto risulterà il computer.

3. Selezionare le risorse che si desidera distruggere:
   a. In **Available shred options** (Opzioni di distruzione disponibili), fare clic su una risorsa, quindi scegliere **Aggiungi**.
   b. Per aggiungere una risorsa personalizzata, fare clic su Add Custom Option (Aggiungi opzione personalizzata), immettere il nome del file o della cartella, quindi scegliere **OK**. Fare clic sulla risorsa personalizzata, quindi scegliere **Aggiungi**.

   NOTA: Per eliminare una risorsa dalle opzioni di distruzione disponibili, fare clic sulla risorsa, quindi scegliere **Elimina**.

4. In **Shred the following** (Distruggi seguenti), selezionare la casella di controllo accanto a ciascuna risorsa che si desidera confermare prima della distruzione.

NOTA: Per rimuovere una risorsa dall'elenco di distruzione, fare clic sulla risorsa, quindi scegliere **Rimuovi**.

5. In **Do not shred the following** (Non distruggere seguenti), fare clic su **Aggiungi** per selezionare le risorse specifiche che si desidera escludere dalla distruzione.

NOTA: È possibile escludere dalla distruzione solo estensioni di file. Se ad esempio si aggiunge l'estensione .BMP, tutti i file con estensione .BMP verranno esclusi dalla distruzione.

Per rimuovere una risorsa dall'elenco delle esclusioni, fare clic sulla risorsa, quindi scegliere **Elimina**.

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

Personalizzazione di un profilo di eliminazione semplice

Il profilo di eliminazione semplice esegue un'eliminazione standard della risorsa senza distruzione. Quando si personalizza un profilo di eliminazione semplice, è possibile specificare quali risorse includere in un'eliminazione semplice, quali risorse confermare prima che venga eseguita un'eliminazione semplice e quali risorse escludere dall'eliminazione semplice:

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

1. Avviare **File Sanitizer**, fare clic su **Impostazioni**, scegliere **Simple Delete Setting** (Impostazioni di eliminazione semplice), quindi fare clic su **View Details** (Visualizza dettagli).
2. Selezionare le risorse che si desidera eliminare:
   - In **Available delete options** (Opzioni di eliminazione disponibili), fare clic sulla risorsa, quindi scegliere **Aggiungi**.
   - Per aggiungere una risorsa personalizzata, fare clic su **Add Custom Option** (Aggiungi opzione personalizzata), immettere il nome del file o della cartella, quindi scegliere **OK**. Fare clic sulla risorsa personalizzata, quindi scegliere **Aggiungi**.

     NOTA: Per eliminare una risorsa dalle opzioni di eliminazione disponibili, fare clic sulla risorsa, quindi scegliere **Elimina**.
3. In **Delete the following** (Elimina seguenti), selezionare la casella di controllo accanto a ciascuna risorsa che si desidera confermare prima dell'eliminazione.

NOTA: Per rimuovere una risorsa dall'elenco di eliminazione, fare clic sulla risorsa, quindi scegliere **Rimuovi**.

4. In **Do not delete the following** (Non eliminare seguenti), fare clic su **Aggiungi** per selezionare le risorse specifiche che si desidera escludere dalla distruzione.

NOTA: È possibile escludere dalla distruzione solo estensioni di file. Se ad esempio si aggiunge l'estensione .BMP, tutti i file con estensione .BMP verranno esclusi dall'eliminazione.

Per rimuovere una risorsa dall'elenco delle esclusioni, fare clic sulla risorsa, quindi scegliere **Elimina**.

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

Attività generali

Uso di una sequenza di tasti per avviare la distruzione

Per specificare una sequenza di tasti, procedere come segue:

1. Avviare **File Sanitizer** e fare clic su **Shred** (Distruggi).
2. Selezionare la casella di controllo **Key sequence** (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:** Le risorse distrutte non possono essere ripristinate. Considerare attentamente quali elementi selezionare per la distruzione manuale.

1. Passare al documento o alla cartella che si desidera distruggere.
2. Trascinare la risorsa sull'icona File Sanitizer sul desktop.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.
4. Fare clic su **Sì** per confermare la rimozione dell'utente selezionato.

Distruzione manuale di una risorsa

△ **ATTENZIONE:** Le risorse distrutte non possono essere ripristinate. Considerare attentamente quali elementi selezionare per la distruzione manuale.

1. Fare clic con il pulsante destro del mouse sull'icona **HP ProtectTools** nell'area di notifica all'estrema destra della barra delle applicazioni, fare clic su **File Sanitizer**, quindi scegliere **Shred One** (Distruggi uno).
2. Quando viene visualizzata la finestra di dialogo Sfoglia, spostarsi sulla risorsa che si desidera distruggere, quindi scegliere **OK**.

   NOTA: La risorsa selezionata può essere un singolo file o una 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 **Shred One** (Distruggi uno).
2. Quando viene visualizzata la finestra di dialogo Sfoglia, spostarsi sulla risorsa che si desidera distruggere, quindi scegliere **OK**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

– oppure –

1. Avviare File Sanitizer e fare clic su **Shred** (Distruggi).
2. Fare clic sul pulsante **Sfoglia**.
3. Quando viene visualizzata la finestra di dialogo Sfoglia, spostarsi sulla risorsa che si desidera distruggere, quindi scegliere **OK**.
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 **HP ProtectTools** nell'area di notifica all'estrema destra della barra delle applicazioni, fare clic su **File Sanitizer**, quindi scegliere **Shred Now** (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 **Shred Now** (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 **HP ProtectTools** nell'area di notifica all'estrema destra della barra delle applicazioni, fare clic su **File Sanitizer**, quindi scegliere **Bleach Now** (Pulisci ora).
2. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

– oppure –

1. Avviare File Sanitizer e fare clic su **Free Space Bleaching** (Pulizia dello spazio libero).
2. Fare clic su **Bleach Now** (Pulisci ora)
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì**.

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 for Administrators 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

7 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools gestisce l'impostazione e la configurazione della Java Card per l'utilizzo con la tastiera HP Smart Card. Java Card di HP è un dispositivo di protezione personale che protegge i dati di autenticazione che richiedono sia la scheda sia un numero PIN per concedere l'accesso (come accade per il PIN della carta Bancomat). Java Card può essere utilizzata per accedere a Credential Manager, Drive Encryption, HP BIOS o a qualsiasi numero di punti di accesso di terze parti.

Con Java Card Security sono disponibili le seguenti funzioni:

- Accesso alle funzioni di Java Card Security.
- Utilizzo congiunto con l'utility Impostazione del computer per attivare l'autenticazione delle Java Card al momento dell'accensione.
- Configurazione di Java Card separate per amministratore e utente. Per consentire il caricamento del sistema, l'utente dovrà quindi inserire la Java card e un PIN.
- Impostazione e modifica del PIN utilizzato per autenticare gli utenti della Java card.

Attività generali

La pagina “Generale” consente di effettuare le seguenti attività:

- Modificare un PIN Java Card
- Selezionare il lettore di schede o la tastiera Smart Card

NOTA: Il lettore utilizza sia Java Card sia smart card. Questa funzione è disponibile se il computer dispone di più di un lettore.

Modifica di un PIN Java Card

Per modificare un PIN Java Card:

NOTA: Il PIN Java Card deve comprendere da 4 a 8 caratteri numerici.

1. Fare clic su **Start** > **Tutti i programmi** > **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Generale**.
3. Inserire una Java Card (con un PIN esistente) nel lettore.
4. Nel riquadro di destra, fare clic su **Change** (Modifica).
5. Nella finestra di dialogo **Modifica PIN**, digitare il PIN corrente nella casella **PIN attuale**.

6. Digitare un nuovo PIN nella casella **Nuovo PIN** e digitarlo nuovamente nella casella **Conferma nuovo PIN**.

7. Fare clic su **OK**.

Selezione del lettore

Prima di usare la Java Card, verificare che in Java Card Security sia selezionato il lettore corretto. In caso contrario, alcune delle funzioni potrebbero non essere disponibili o visualizzate in modo corretto. Inoltre, i driver del lettore devono essere correttamente installati, come indicato in Gestione periferiche di Windows.

Per selezionare il lettore:

1. Fare clic su **Start** > **Tutti i programmi** > **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.

2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Generale**.

3. Inserire la Java card nel lettore.

4. Nel riquadro di destra, sotto **Selected card reader** (Lettore selezionato), fare clic sul lettore desiderato.

Attività avanzate (solo per amministratori)

La pagina “Avanzate” consente di eseguire le seguenti attività:

- Assegnazione di un PIN Java card
- Assegnazione di un nome a una Java card
- Impostazione di autenticazione di accensione
- Backup e ripristino di Java card

NOTA: Per visualizzare la pagina “Avanzate” è necessario disporre dei diritti di amministratore per Windows.

Assegnazione di un PIN Java card

Per poterla utilizzare in Java Card Security, è necessario che alla Java card vengano assegnati un nome e un PIN.

Per assegnare un PIN a una Java card:

NOTA: Il PIN Java card deve comprendere da 4 a 8 caratteri numerici.

1. Fare clic su **Start** > **Tutti i programmi** > **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.

2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Avanzate**.

3. Inserire una nuova Java card nel lettore.

4. Quando viene visualizzata la finestra di dialogo **New Card** (Nuova scheda), digitare un nuovo nome nella casella **New display name** (Nuovo nome visualizzato), digitare un nuovo PIN nella casella **Nuovo PIN** e immettere nuovamente il PIN nella casella **Conferma nuovo PIN**.

5. Fare clic su **OK**.

Assegnazione di un nome a una Java card

Per poterla utilizzare per l'autenticazione di accensione, è necessario che alla Java card venga assegnato un nome.

Per assegnare un nome a una Java card:

1. Fare clic su **Start** > **Tutti i programmi** > **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Avanzate**.
3. Inserire la Java card nel lettore.

NOTA: Se a questa scheda non è stato assegnato un PIN, verrà visualizzata la finestra di dialogo **New Card** (Nuova scheda), che consente l'immissione di un nuovo nome e di un nuovo PIN.

4. Nel riquadro di destra, in **Nome visualizzato**, fare clic su **Change** (Cambia).
5. Digitare il nome della Java Card nella casella **Name** (Nome).
6. Digitare il PIN corrente della Java Card nella casella **PIN**.
7. Fare clic su **OK**.

Impostazione di autenticazione di accensione

L'attivazione di questa opzione richiede l'uso di una Java card per avviare il computer.

Il processo di abilitazione della Java card per l'autenticazione di accensione comprende la seguente procedura:

1. Abilitazione del supporto di autenticazione all'accensione di Java Card in BIOS Configuration o in Computer Setup.
2. Abilitare la Java card per l'autenticazione di accensione in Java Card Security.
3. Creazione e abilitazione della Java card dell'amministratore.

Attivazione della Java card per l'autenticazione di accensione e creazione di una Java card amministratore

Per attivare la Java card per l'autenticazione di accensione:

1. Fare clic su **Start** > **Tutti i programmi** > **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Avanzate**.
3. Inserire la Java card nel lettore.

NOTA: Se a questa scheda non sono stati assegnati un nome e un PIN, verrà visualizzata la finestra di dialogo **New Card** (Nuova scheda), che consente l'immissione di un nuovo nome e di un nuovo PIN.

4. Nel riquadro di destra, sotto **Autenticazione all'accensione**, selezionare la casella di controllo **Abilita**.
5. Nella finestra di dialogo **Password di Impostazione del computer** immettere la password di Impostazione del computer, quindi fare clic su **OK**.
6. Se DriveLock non è abilitato, digitare il PIN Java Card e fare clic su **OK**.

   – oppure –

   Se DriveLock è abilitato:

   a. Fare clic su **Rendi univoca l'identità della Java card**.

      – oppure –

      Fare clic su **Rendi l'identità della Java Card uguale alla password DriveLock**.

   NOTA: Se DriveLock è abilitato, è possibile uniformare l'identità Java card alla password utente DriveLock; in tal modo, è possibile convalidare sia DriveLock che la Java card utilizzando solo quest'ultima all'avvio del computer.

   b. Se possibile, digitare la password utente di DriveLock nella casella **Password DriveLock** quindi immetterla nuovamente nella casella **Conferma password**.

   c. Digitare il PIN Java card.

   d. Fare clic su **OK**.

7. Alla richiesta di creazione di un file di ripristino, fare clic su **Annulla** per creare un file di ripristino in un secondo momento oppure fare clic su **OK** e seguire le istruzioni visualizzate in Backup guidato di HP ProtectTools per creare immediatamente un file di ripristino.

NOTA: Per ulteriori informazioni, vedere Backup e ripristino delle credenziali di HP ProtectTools a pagina 10.

Creazione di una Java card utente

NOTA: Per la creazione di una Java card utente, sono necessari l'autenticazione di accensione e una scheda amministratore.

Per creare una Java card utente:

1. Fare clic su **Start** > **Tutti i programmi** > **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Avanzate**.
3. Inserire una Java card che verrà utilizzata come scheda utente.
4. Nel riquadro di destra, sotto **Autenticazione all'accensione**, fare su **Create** (Crea), accanto a **Identità scheda utente**.
5. Digitare un PIN per la Java card utente e fare clic su **OK**.

Disabilitazione di una Java card per l'autenticazione di accensione

Quando la Java card per l'autenticazione di accensione viene disabilitata, non è più necessario utilizzare una Java card per accedere al computer.

1. Fare clic su **Start** > **Tutti i programmi** > **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Avanzate**.
3. Inserire la Java Card dell'amministratore.
4. Nel riquadro di destra, sotto **Autenticazione all'accensione**, deselezionare la casella di controllo **Enable** (Abilita).
5. Digitare un PIN per la Java Card e fare clic su **OK**.

8 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools permette di accedere alle impostazioni di configurazione e sicurezza della Computer Setup Utility, in modo che gli utenti Windows possano accedere alle funzioni di sicurezza di sistema gestite da Computer Setup. Le opzioni contenute in BIOS Configuration for HP ProtectTools sono elencate di seguito.

- File
- Storage (Memorizzazione)
- Security (Sicurezza)
- Power (Alimentazione)
- Advanced (Avanzata)

NOTA: Il supporto per opzioni specifiche di Computer Setup può variare a seconda della configurazione hardware.

BIOS Configuration consente di gestire diverse impostazioni del computer che sarebbero altrimenti accessibili solo premendo F10 all'avvio e accedendo all'utility Computer Setup. Con BIOS Configuration, è possibile conseguire i seguenti obiettivi:

- Gestire le password di accensione e dell'amministratore.
- Configurare altre funzioni di autenticazione all'accensione, come l'attivazione del supporto per l'autenticazione della protezione incorporata.
- Attivazione e disattivazione delle funzioni hardware, quali avvio da supporto rimovibile o da diverse porte hardware.
- Configurare le opzioni di avvio, tra cui l'attivazione di MultiBoot e la modifica dell'ordine di avvio.

NOTA: Tutte le funzioni di configurazione del BIOS per HP ProtectTools sono disponibili anche in F10 Setup. Per istruzioni dettagliate sull'utilizzo di F10 Setup, consultare la *Guida dell'utility Computer Setup (F10)* fornita con il computer o con l'aggiornamento del BIOS.

Attività generali

BIOS Configuration consente di gestire varie impostazioni del computer che altrimenti sarebbero accessibili solo premendo F10 all'avvio per accedere all'utility Impostazione del computer.

Accesso alla configurazione del BIOS

Per accedere a BIOS Configuration:

1. Fare clic su **Start**, quindi selezionare **Impostazioni** e **Pannello di controllo**.
2. Fare clic su **HP ProtectTools Security Manager for Administrators**, quindi su **BIOS Configuration** (Configurazione BIOS).

   È inoltre possibile accedere a BIOS Configuration nell'area di notifica posta all'estrema destra della barra delle applicazioni.

   NOTA: Per visualizzare l'icona di HP ProtectTools Security Manager for Administrators, è possibile che sia necessario fare clic sull'icona **Mostra icone nascoste** (**<** o **<<**) nell'area di notifica.

   - Fare clic con il pulsante destro del mouse sull'icona di **HP ProtectTools Security Manager for Administrators** nell'area di notifica.
   - Fare clic su **BIOS Configuration**.
3. Gli utenti di HP ProtectTools devono immettere la password di Windows.
   - Se si immette la password corretta di Windows, ma non si è amministratori BIOS, la possibilità di apportare modifiche varia in base alle impostazioni del livello di sicurezza.

     NOTA: Gli utenti di HP ProtectTools possono anche non essere amministratori BIOS.
   - Se la password di Windows viene immessa in modo non corretto, le impostazioni di BIOS Configuration risulteranno visibili, ma non potranno essere modificate.
4. Se non si è un utente di HP ProtectTools, verrà effettuato un controllo per verificare se è stata impostata una password dell'amministratore BIOS.
   - Se è stata impostata una password amministratore del BIOS, è necessario immetterla.
     - Se la password dell'amministratore BIOS viene immessa in modo corretto, le impostazioni di BIOS Configuration risulteranno visibili e potranno essere modificate.
     - Se la password dell'amministratore BIOS è stata impostata, ma non viene immessa oppure viene immessa in modo non corretto, le impostazioni di BIOS Configuration risulteranno visibili, ma non potranno essere modificate.
   - Se la password dell'amministratore BIOS non è stata impostata, le impostazioni di BIOS Configuration risulteranno visibili e potranno essere modificate.

Visualizzazione o modifica delle impostazioni

Per visualizzare o modificare le impostazioni di configurazione:

1. Fare clic su una delle pagine di configurazione del BIOS.
2. Apportare le modifiche desiderate, quindi fare clic su **Apply** (Applica) per applicare le modifiche.
3. Uscire e riavviare il computer.

   Le modifiche diventeranno effettive al successivo riavvio del computer.

NOTA: Le modifiche apportate alle password diventano attive immediatamente senza che sia necessario riavviare il computer.

File

L'opzione File all'interno di BIOS Configuration for HP ProtectTools fornisce informazioni sul sistema, quali il tipo di processore, il nome e la versione del BIOS di sistema, il numero di serie, ecc. Gli unici dati File che possono essere modificati sono i numeri di controllo asset. Gli altri dati sono accessibili in sola lettura.

NOTA: Per ulteriori informazioni sulle opzioni per i file, consultare la *Guida dell'utility Computer Setup (F10)*.

Storage (Memorizzazione)

L'opzione Storage (Memorizzazione) all'interno di BIOS Configuration for HP ProtectTools fornisce informazioni su tutti i dispositivi avviabili configurati nel sistema del computer e consente di specificare le impostazioni per tali dispositivi. Le impostazioni accessibili in Storage includono:

- Device Configuration (Configurazione periferiche)
- Storage Options (Opzioni di memorizzazione)
- DPS Self-Test (Autotest DPS)
- Boot Order (Sequenza di avvio)

NOTA: Per ulteriori informazioni sulle opzioni di memorizzazione, consultare la *Guida dell'utility Computer Setup (F10)*.

Security (Sicurezza)

L'opzione Security (Sicurezza) all'interno di BIOS Configuration for HP ProtectTools rappresenta il centro di configurazione di tutte le impostazioni correlate alla sicurezza e alle password. Le impostazioni disponibili sono le seguenti:

- Setup Password (Password di configurazione)
- Power-On Password (Password di accensione)
- Password Options (Opzioni password)
- Smart Cover (alcuni modelli)

- Device Security (Sicurezza periferiche)
- Network Service Boot (Avvio servizio di rete)
- System Ids (ID di sistema)
- DriveLock Security (Funzione di sicurezza DriveLock)
- System Security (Sicurezza sistema) (alcuni modelli)
- Setup Security Level (Livello sicurezza setup)

NOTA: Per ulteriori informazioni sulle opzioni di sicurezza, consultare la *Guida dell'utility Computer Setup (F10)*.

Power (Alimentazione)

L'opzione Power (Alimentazione) all'interno di BIOS Configuration for HP ProtectTools fornisce le impostazioni che controllano la gestione dell'alimentazione a livello di hardware. Le impostazioni disponibili sono le seguenti:

- OS Power Management (Gestione alimentazione SO)
- Hardware Power Management (Gestione alimentazione hardware)
- Thermal (Termico)

NOTA: Per ulteriori informazioni sulle opzioni di alimentazione, consultare la *Guida dell'utility Computer Setup (F10)*.

Advanced (Avanzata)

Le impostazioni disponibili nell'opzione Advanced di BIOS Configuration for HP ProtectTools sono destinate agli utenti esperti. Le impostazioni sono le seguenti:

- Power-On Options (Opzioni di accensione)
- Execute Memory Test (Esegui test di memoria) (alcuni modelli)
- BIOS Power-On (Accensione da BIOS)
- Onboard Devices (Periferiche incorporate)
- PCI Devices (Periferiche PCI)
- PCI VGA Configuration (Configurazione VGA PCI)
- Bus Options (Opzioni bus)
- Device Options (Opzioni periferiche)
- Management Devices (Gestione dispositivi)
- Management Operations (Operazioni di gestione)

NOTA: Per ulteriori informazioni sulle opzioni avanzate, consultare la *Guida dell'utility Computer Setup (F10)*.

9 Embedded Security for HP ProtectTools

NOTA: Per utilizzare Embedded Security for HP ProtectTools è necessario che il chip TPM di protezione incorporata sia installato nel computer.

Embedded Security for HP ProtectTools protegge i dati o le credenziali utente dall'accesso non autorizzato. Questo modulo software offre le seguenti funzioni di protezione:

- Crittografia di file e cartelle con Enhanced Microsoft® Encryption File System (EFS) (Servizio potenziato di crittografia del file system (EFS) di Microsoft®
- Creazione di una personal secure drive (PSD) per la protezione dei dati utente
- Funzioni di gestione dei dati, quali il backup e il ripristino della gerarchia delle chiavi
- Supporto per applicazioni di terzi, quali Microsoft Outlook e Internet Explorer, per le operazioni protette da certificato digitale quando si utilizza il software Embedded Security

Il chip di protezione TPM integrato migliora e abilita altre funzioni di sicurezza di HP ProtectTools Security Manager for Administrators. Credential Manager for HP ProtectTools, ad esempio, può utilizzare il chip integrato come fattore di autenticazione quando l'utente accede a Windows. In alcuni modelli, il chip di protezione TPM integrato abilita anche le funzioni di sicurezza avanzate del BIOS a cui si accede mediante BIOS Configuration for HP ProtectTools.

Procedure di installazione

△ **ATTENZIONE:** Per ridurre i rischi in termini di protezione, si consiglia all'amministratore IT di inizializzare immediatamente il chip di protezione incorporata. In caso di mancata inizializzazione del chip di protezione incorporata, un utente non autorizzato, un worm o un virus potrebbero assumere la proprietà del computer e ottenere il controllo delle attività del proprietario, quali la gestione dell'archivio per il ripristino di emergenza e la configurazione delle impostazioni di accesso dell'utente.

Seguire la procedura riportata nelle 2 sezioni successive e inizializzare il chip di protezione incorporata.

Abilitazione del chip di protezione integrato in Computer Setup

È possibile abilitare il chip di protezione integrato nella procedura guidata di inizializzazione rapida o nell'utility Computer Setup, come descritto di seguito. Non è possibile seguire la procedura in BIOS Configuration for HP ProtectTools.

Per abilitare il chip di protezione integrato in Computer Setup:

1. Aprire Impostazione del computer accendendo o riavviando il computer e premendo il tasto F10 quando nell'angolo inferiore sinistro dello schermo viene visualizzato il messaggio “F10 = ROM Based Setup” (F10 = Impostazione da ROM).
2. Se non è stata impostata una password dell'amministratore, utilizzare i tasti freccia per selezionare **Security** (Sicurezza), quindi **Setup password** (Password di configurazione), e premere Invio.
3. Immettere la password nelle caselle **Password nuova** e **Verifica la nuova password**, quindi premere F10.
4. Nel menu **Protezione**, utilizzare i tasti freccia per selezionare **TPM protezione integrata**, quindi premere invio.
5. Se la periferica è nascosta, in **Protezione integrata** selezionare **Available** (Disponibile).
6. Selezionare **Embedded security device state** (Stato della periferica di protezione incorporata) e modificarlo in **Enable** (Attivo).
7. Premere F10 per accettare le modifiche alla configurazione di protezione incorporata.
8. Per salvare le preferenze e uscire da Impostazione del computer, utilizzare i tasti freccia per selezionare **File**, quindi fare clic su **Save Changes and Exit** (Salva le modifiche ed esci). Seguire le istruzioni visualizzate.

Inizializzazione del chip di protezione incorporata

Durante il processo di inizializzazione di Embedded Security, è possibile eseguire le seguenti operazioni:

- Impostare una password proprietario per il chip di protezione incorporata, che protegga l'accesso a tutte le funzioni del titolare sul chip di protezione incorporata.
- Configurare l'archivio per il ripristino di emergenza, un'area di memorizzazione protetta che consente la nuova crittografia di chiavi utente di base per tutti gli utenti.

Per inizializzare il chip di protezione incorporata:

1. Fare clic con il pulsante destro del mouse sull'icona HP ProtectTools Security Manager for Administrators nell'area di notifica, all'estrema destra della barra delle applicazioni, quindi selezionare **Embedded Security Initialization** (Inizializzazione protezione integrata).

   Viene visualizzata l'Inizializzazione guidata di HP ProtectTools Embedded Security.

2. Seguire le istruzioni visualizzate.

Impostazione dell'account utente di base

L'impostazione di un account utente di base in Embedded Security consente di effettuare le seguenti attività:

- Generare una chiave utente di base per la protezione delle informazioni crittografate, e impostare una password per la protezione della chiave utente di base.
- Impostare un'unità personale protetta (PSD) per la memorizzazione di file e cartelle crittografate.

△ **ATTENZIONE:** Salvaguardare la password chiave utente di base. In mancanza di questa password, non è possibile accedere alle informazioni crittografate né ripristinarle.

Per impostare un account utente di base ed attivare le funzioni di protezione dell'utente:

1. Se la procedura guidata di inizializzazione non viene avviata, fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **User Settings** (Impostazioni utente).
3. Nel riquadro di destra, in **Embedded Security Features** (Funzioni di Protezione incorporata), fare clic su **Configura**.

   Viene visualizzata l'Inizializzazione guidata di Protezione integrata.

4. Seguire le istruzioni visualizzate.

NOTA: Per utilizzare l'e-mail protetta, come prima cosa è necessario configurare il client e-mail in modo che usi un certificato digitale creato con Embedded Security. Se non è disponibile un certificato digitale, è necessario ottenerne uno da un'autorità di certificazione. Per istruzioni sulla configurazione dell'e-mail e su come ottenere un certificato digitale, fare riferimento alla guida in linea del software del client e-mail.

Attività generali

Dopo aver impostato l'account utente di base, è possibile effettuare le seguenti attività:

- Crittografia di file e cartelle
- Invio e ricezione di posta elettronica crittografata

Uso dell'unità personale protetta (PSD)

Al termine dell'impostazione della PSD, viene richiesto di digitare la password chiave utente di base all'accesso successivo. Se la password chiave utente di base viene immessa correttamente, è possibile accedere alla PSD direttamente da Esplora risorse.

Crittografia di file e cartelle

Se si lavora con file crittografati, considerare le seguenti regole:

- Solo file e cartelle in partizioni NTFS possono essere crittografati. File e cartelle in partizioni FAT non possono essere crittografati.
- I file di sistema e i file compressi non possono essere crittografati e i file crittografati non possono essere compressi.
- Le cartelle temporanee devono essere crittografate, perché sono un potenziale bersaglio per i pirati informatici.
- Quando si crittografa un file o una cartella per la prima volta, viene automaticamente impostato un criterio di ripristino. Quest'ultimo garantisce la possibilità di utilizzare un agente di recupero dati per decrittografare le informazioni in caso di perdita del certificato di crittografia e delle chiavi private.

Per crittografare file e cartelle:

1. Fare clic con il pulsante destro del mouse sul file o sulla cartella che si desidera crittografare.
2. Fare clic su **Encrypt** (Crittografa).
3. Fare clic su una delle seguenti opzioni:
   - **Applica cambiamenti solo a questa cartella**.
   - **Applica cambiamenti a questa cartella, a tutte le sottocartelle e a tutti i file**.
4. Fare clic su **OK**.

Invio e ricezione di posta elettronica crittografata

Embedded Security consente di inviare e ricevere messaggi e-mail crittografati, ma le procedure variano a seconda del programma che si utilizza per accedere all'e-mail. Per maggiori informazioni, fare riferimento alla guida in linea di Embedded Security e a quella del programma di gestione e-mail in uso.

Modifica della password chiave utente di base

Per modificare la password chiave utente di base:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **User Settings** (Impostazioni utente).
3. Nel riquadro di destra, in **Basic User Key password** (Password chiave utente di base), fare clic su **Change** (Cambia).
4. Immettere la vecchia password, quindi impostare e confermare la nuova password.
5. Fare clic su **OK**.

Attività avanzate

Backup e ripristino

La funzionalità di backup di Protezione integrata crea un archivio che contiene informazioni sulla certificazione da ripristinare in caso di emergenza.

Creazione di un file di backup

Per creare un file di backup:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Backup**.
3. Nel riquadro di destra, fare clic su **Backup**. Viene visualizzato il programma Backup guidato di HP ProtectTools Embedded Security.
4. Seguire le istruzioni visualizzate.

Ripristino dei dati relativi alla certificazione dal file di backup

Per ripristinare dati dal file di backup:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Backup**.
3. Nel riquadro di destra, fare clic su **Restore** (Ripristina). Viene visualizzato il programma di Backup guidato di HP ProtectTools Embedded Security.
4. Seguire le istruzioni visualizzate.

Modifica della password proprietario

Per modificare la password proprietario:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Avanzate**.
3. Nel riquadro di destra, in **Owner Password** (Password proprietario), fare clic su **Change** (Cambia).
4. Immettere la vecchia password proprietario, quindi impostare e confermare la nuova.
5. Fare clic su **OK**.

Ripristino di una password utente

Un amministratore può assistere un utente nel ripristino di una password dimenticata. Per maggiori informazioni, consultare la guida in linea del programma.

Attivazione e disattivazione di Protezione integrata

Se si desidera usare il computer senza la funzione di protezione, è possibile disattivare le funzioni di Protezione integrata.

Sono possibili due livelli di attivazione o disattivazione delle funzioni di Protezione integrata:

- Disattivazione temporanea: questa opzione consente la riattivazione automatica della protezione integrata al riavvio di Windows. Questa opzione è accessibile a tutti gli utenti per default.
- Disattivazione definitiva: con questa opzione, per riattivare la funzione Protezione integrata, è necessario immettere la password proprietario. Questa opzione è accessibile solo agli amministratori.

Disattivazione definitiva di Protezione integrata

Per disattivare definitivamente Protezione integrata:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Avanzate**.
3. Nel riquadro di destra, in **Protezione integrata**, fare clic su **Disable** (Disattiva).
4. Alla richiesta, immettere la password proprietario, quindi fare clic su **OK**.

Attivazione di Protezione integrata dopo la disattivazione definitiva

Per attivare Protezione integrata dopo la disattivazione definitiva:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Avanzate**.
3. Nel riquadro di destra, in **Protezione integrata**, fare clic su **Enable** (Attiva).
4. Alla richiesta, immettere la password proprietario, quindi fare clic su **OK**.

Migrazione delle chiavi con Migrazione guidata

La migrazione è un'attività avanzata riservata all'amministratore, che consente la gestione, il ripristino e il trasferimento di chiavi e certificati.

Per maggiori dettagli sulla migrazione, fare riferimento alla guida in linea di Embedded Security.

10 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

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, in HP ProtectTools Security Manager for Administrators 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

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

- Dispositivi USB per tutti gli utenti non amministratori
- Tutti i supporti rimovibili (floppy disk, pen drive e così via) 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 dispositivo per tutti gli utenti non amministratori:

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
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 di un dispositivo per negare l'accesso.
4. Fare clic su **Applica**.

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**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Device Access Manager**, quindi selezionare **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 **Select Users or Groups** (Seleziona utenti o gruppi).
5. Fare clic su **Advanced** (Avanzate) e successivamente su **Find Now** (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**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Device Access Manager**, quindi selezionare **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**.
5. Fare clic su **Applica**, quindi su **OK**.

Negazione dell'accesso a un utente o gruppo

1. Fare clic su **Start**, quindi su **Tutti i programmi** e su **HP ProtectTools Security Manager for Administrators** in Windows Vista oppure su **HP ProtectTools Security Manager** in Windows XP.
2. Nel riquadro di sinistra, fare clic su **Device Access Manager**, quindi selezionare **Configurazione delle classi di periferiche**.
3. Nell'elenco dei dispositivi fare clic sulla classe del dispositivo da configurare.
4. In **User/Groups** (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 su **Applica**, quindi su **OK**.

11 Risoluzione dei problemi

Credential Manager for HP ProtectTools

Breve descrizione	Dettagli	Soluzione
L'opzione Network Accounts (Account di rete) di Credential Manager consente a un utente di selezionare l'account di dominio a cui connettersi. Questa opzione non è disponibile se si utilizza l'autenticazione TPM. Funziona regolarmente con tutti gli altri metodi.	Quando si utilizza l'autenticazione TPM, la connessione avviene solo con il computer locale.	Utilizzando gli strumenti Single Sign On di Credential Manager, l'utente è in grado di autenticare altri account.
Le smart card e i token USB non sono disponibili in Credential Manager se installati dopo Credential Manager.	Per poter utilizzare le smart card o i token USB in Credential Manager, il software di supporto (driver, PKCS#11 provider, e così via) deve essere installato prima di Credential Manager. Se Credential Manager è già stato installato, attenersi alla procedura seguente dopo aver installato il software di supporto della smart card o del token:	Accedere a Credential Manager. In HP ProtectTools Security Manager, fare clic su **Credential Manager**, successivamente su **Advanced Settings** (Impostazioni avanzate) e infine sulla scheda **Smart Cards and Tokens** (Smart card e token). Sotto Local Tokens (Token locali) viene visualizzato un elenco dei token disponibili. Accedere a un menu a comparsa facendo clic con il pulsante destro del mouse sul nodo Local Tokens e selezionando Scan for New Smart Cards and Tokens (Scansione nuove smart card e token). Riavviare il computer, se richiesto.
Le pagine Web di alcune applicazioni creano errori che impediscono agli utenti di eseguire o completare le attività.	Alcune applicazioni Web cessano di funzionare e producono errori a causa dello schema di disabilitazione di Single Sign On. Ad esempio, in Internet Explorer verrà visualizzato un **!** racchiuso in un triangolo giallo a indicare la presenza di un errore.	La modalità Single Sign On di Credential Manager non supporta tutte le interfacce Web software. Disabilitare il supporto Single Sign On per la pagina Web specifica. Consultare la documentazione completa sull'accesso di tipo Single Sign On disponibile nella guida in linea di Credential Manager. Se non fosse possibile disabilitare uno specifico Single Sign per una determinata applicazione, chiamare il servizio di assistenza tecnica di HP e richiedere, tramite il proprio contatto, un intervento di assistenza di terzo livello.
L'opzione **Browse for Virtual Token** (Cerca token virtuale) non viene visualizzata durante il processo di connessione.	L'utente non può spostare la posizione di un token virtuale registrato in Credential Manager in quanto l'opzione “Sfoglia” è stata eliminata per aumentare il livello di protezione.	Tale opzione consentiva ai non utenti di eliminare e rinominare i file e di assumere il controllo di Windows.

Breve descrizione	Dettagli	Soluzione
L'amministratore di dominio non può modificare la password di Windows anche con l'autorizzazione.	Questa situazione si verifica dopo che un amministratore di dominio ha effettuato l'accesso a un dominio e ne ha registrato l'identità con Credential Manager utilizzando un account con diritti di amministratore su dominio e PC locale. Quando l'amministratore di dominio prova a modificare la password di Windows da Credential Manager, ottiene un errore di accesso non riuscito: **User account restriction** (Restrizione account utente).	Credential Manager non può modificare la password di un account utente del dominio mediante l'opzione **Change Windows Password** (Cambia password di Windows). Credential Manager può cambiare solo le password degli account del PC locale. L'utente del dominio può modificare la propria password mediante l'opzione **Cambia password** di **Protezione di Windows** ma, poiché l'utente del dominio non dispone di un account fisico sul PC locale, Credential Manager può modificare solo la password utilizzata per l'accesso ma, poiché l'utente del dominio non dispone di un account fisico sul PC locale, Credential Manager può modificare solo la password utilizzata per l'accesso.
Credential Manager mostra problemi di incompatibilità con il GINA delle password di Corel WordPerfect 12.	Se l'utente si connette a Credential Manager, crea un documento in WordPerfect e lo salva proteggendolo con password, Credential Manager non sarà in grado di rilevare o riconoscere, né in modo manuale né in modo automatico, il GINA della password.	HP sta cercando una soluzione per migliorare il prodotto nel futuro.
Credential Manager non riconosce il pulsante **Connect** (Connetti) sullo schermo.	Se le credenziali Single Sign On per Remote Desktop Connection (RDP) sono impostate su **Connect** (Connetti), quando Single Sign On viene riavviato, immette sempre **Save As** (Salva con nome) al posto di **Connect** (Connetti).	HP sta cercando una soluzione per migliorare il prodotto nel futuro.
Gli utenti potrebbero perdere tutte le credenziali di Credential Manager protette dal TPM.	Se il modulo TPM viene rimosso o è danneggiato, gli utenti perdono tutte le credenziali protette dal TPM.	Come da progettazione. Il modulo TPM è stato progettato per proteggere le credenziali di Credential Manager. HP consiglia di effettuare il backup della propria identità da Credential Manager prima di rimuovere il modulo TPM.
Solo se si utilizza Windows XP Service Pack 1, dopo la transizione dalla modalità di sospensione a quella di ibernazione, l'utente non è in grado di connettersi a Credential Manager.	Dopo avere consentito al sistema di entrare in modalità di sospensione o di ibernazione, l'amministratore o l'utente non è in grado di connettersi a Credential Manager e la schermata di accesso a Windows rimane visualizzata a prescindere dalla credenziale di accesso (password, impronta digitale o Java Card) selezionata.	Effettuare l'aggiornamento al Service Pack 2 di Windows mediante Windows Update. Per maggiori informazioni sulla causa del problema, fare riferimento all'articolo 813301 della knowledge base Microsoft all'indirizzo http://www.microsoft.com. Per ottenere la connessione, l'utente deve selezionare Credential Manager e accedere. Dopo la connessione a Credential Manager, viene richiesto di accedere a Windows (potrebbe essere necessario selezionare l'opzione di accesso a Windows) per completare il processo di connessione. Se l'utente si connette prima a Windows, dovrà successivamente connettersi a Credential Manager in modo manuale.
Il ripristino di Embedded Security impedisce a Credential Manager di andare a buon fine.	Credential Manager non riesce a registrare le credenziali in seguito al ripristino delle impostazioni predefinite della ROM.	Credential Manager non riesce ad accedere al TPM se la ROM viene reimpostata ai valori di fabbrica dopo l'installazione di Credential Manager. Il chip di protezione incorporata TPM può essere abilitato con l'utility Impostazione del computer F10, con BIOS Configuration o con HP Client Manager. Per attivare il chip di protezione incorporata TPM

Breve descrizione	Dettagli	Soluzione
		utilizzando Impostazione computer, procedere come indicato di seguito: 1. Aprire Impostazione del computer accendendo o riavviando il computer e premendo il tasto F10 quando nell'angolo inferiore sinistro dello schermo viene visualizzato il messaggio **F10 = ROM Based Setup** (F10= impostazione da ROM) 2. Utilizzare i tasti freccia per selezionare **Security** (Sicurezza), quindi selezionare **Setup Password** (Password di configurazione). Impostare una password. 3. Selezionare **Embedded Security Device** (Dispositivo di sicurezza integrata). 4. Utilizzare i tasti freccia per selezionare **Embedded Security Device–Disable** (Dispositivo di sicurezza integrata - Disabilita). Utilizzare i tasti freccia per modificarlo in **Embedded Security Device–Enable** (Dispositivo di sicurezza integrata - Abilita). 5. Fare clic su **Enable** (Abilita) e successivamente su **Save changes and exit** (Salva le modifiche ed esci). HP sta valutando alcune soluzioni per le future release.
Il processo di protezione **Restore Identity** (Ripristina identità) perde l'associazione con il token virtuale.	Quando l'utente ripristina l'identità, Credential Manager può perdere l'associazione con la posizione del token virtuale nella schermata di accesso. Anche se Credential Manager registra il token virtuale, l'utente deve ripetere la registrazione per ripristinare l'associazione.	Attualmente secondo progettazione. Quando si disinstalla Credential Manager senza mantenere le identità, la parte sistemica (server) del token viene distrutta per impedire che possa essere riutilizzato per l'accesso, anche se la parte client viene recuperata tramite il ripristino dell'identità. HP sta valutando opzioni a lungo termine per risolvere il problema.

Embedded Security for HP ProtectTools

Breve descrizione	Dettagli	Soluzione
La crittografia di cartelle, sottocartelle e file su PSD produce un messaggio di errore.	Se l'utente copia file e cartelle nel PSD e tenta di crittografare cartelle/file o cartelle/sottocartelle, viene visualizzato il messaggio **Error Applying Attributes** (Errore nell'applicazione degli attributi). Gli stessi file possono essere crittografati nell'unità C:\ o in un disco rigido aggiuntivo.	Come da progettazione. Se spostati nel PSD, file e cartelle vengono automaticamente crittografati. La doppia crittografia di file/cartelle risulta superflua. Il tentativo di doppia crittografia nel PSD tramite EFS produce questo messaggio di errore.
Non è possibile assumere la proprietà con un altro SO in piattaforma multi-avvio.	Se un'unità è configurata per l'avvio di più SO, la proprietà può essere assunta solo con la procedura di inizializzazione della piattaforma in un solo sistema operativo.	Come da progettazione, per motivi di sicurezza.
Un amministratore non autorizzato potrebbe visualizzare, eliminare, rinominare o spostare il contenuto dei file EFS crittografati.	La crittografia di una cartella non impedisce ad utenti non autorizzati in possesso di diritti amministrativi di visualizzare, cancellare o spostare il contenuto della cartella.	Come da progettazione. Si tratta di una funzione EFS, e non Embedded Security TPM. Embedded Security utilizza il software Microsoft EFS ed EFS mantiene i diritti di accesso a file/cartelle per tutti gli amministratori.
L'utente non ottiene opzioni di crittografia quando tenta di ripristinare il disco rigido utilizzando FAT32.	Se l'utente cerca di ripristinare il disco fisso mediante FAT32, non vi saranno opzioni di crittografia per i file/le cartelle che utilizzano EFS.	È il funzionamento previsto. Il software non deve essere installato su un disco formattato con partizione FAT32. Microsoft EFS è supportato solo da NTFS e non funziona con FAT32. Si tratta di una caratteristica di Microsoft EFS non correlata al software HP ProtectTools.
L'utente è in grado di crittografare o eliminare il file XML dell'archivio di ripristino.	Per design, le ACL di questa cartella non sono impostate. Pertanto, un utente potrebbe accidentalmente o volontariamente crittografare o eliminare il file, rendendolo inaccessibile. Se il file viene crittografato o eliminato, nessuno potrà utilizzare il software TPM.	Come da progettazione. Gli utenti hanno diritti di accesso a un archivio di emergenza per salvare/aggiornare la copia di backup della loro chiave utente di base. Gli utenti devono essere informati che i file dell'archivio di ripristino non possono essere crittografati o eliminati.
L'interazione del sistema EFS di Embedded Security con Symantec Antivirus o McAfee Total Protection comporta tempi di crittografia/ decrittografia e scansione più lunghi.	I file crittografati interferiscono con la scansione virus di Symantec Antivirus o McAfee Total Protection. La crittografia dei file mediante il sistema EFS di Embedded Security richiede più tempo se è in esecuzione Symantec Antivirus o McAfee Total Protection.	Per ridurre i tempi per la scansione dei file dell'EFS di Embedded Security, l'utente può digitare la password di crittografia prima della scansione oppure eseguire la decrittazione prima della scansione. Per ridurre il tempo richiesto per crittografare/ decrittografare i dati mediante il sistema EFS di Embedded Security, l'utente deve disabilitare la funzione di protezione automatica di Symantec Antivirus o McAfee Total Protection.
L'archivio di ripristino di emergenza non può essere salvato su un supporto estraibile.	Se al momento di creare il percorso per l'archivio di ripristino di emergenza, durante l'inizializzazione di Embedded Security, l'utente inserisce una scheda di memoria Secure Digital (SD) o MultiMediaCard, viene prodotto un messaggio di errore.	Come da progettazione. L'archivio di ripristino non può essere salvato su un supporto estraibile. È tuttavia possibile salvarlo su un'unità di rete o su un disco locale, diverso da C.
Se l'inizializzazione di Embedded Security si interrompe a causa di una	In caso di interruzione dell'alimentazione durante l'inizializzazione del chip di	Per il ripristino successivamente ad una perdita di alimentazione, eseguire la procedura seguente:

Breve descrizione	Dettagli	Soluzione
mancata alimentazione, viene prodotto un errore.	Embedded Security, si verificano i seguenti problemi: • Quando si tenta di eseguire l'inizializzazione guidata di Embedded Security, viene visualizzato il seguente messaggio di errore: **The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner** (Embedded Security non può essere inizializzato perché il chip ha già un proprietario Embedded Security). • Quando si tenta di eseguire l'inizializzazione guidata utente, viene visualizzato il seguente messaggio di errore: **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first** (Embedded security non è inizializzato. Prima di usare il programma guidato, è necessario inizializzarlo).	**NOTA:** Utilizzare i tasti freccia per selezionare i menu e le voci di menu e per modificare i valori (a meno che non sia specificato diversamente). 1. Avviare o riavviare il computer. 2. Premere F10 quando viene visualizzato il messaggio **F10=Setup**. 3. Selezionare l'opzione della lingua. 4. Premere invio. 5. Selezionare **Security** (Sicurezza), quindi fare clic su **Embedded Security**. 6. Impostare l'opzione **Embedded Security Device** (Dispositivo di sicurezza integrata) su **Enable** (Abilita). 7. Premere F10 per confermare le modifiche. 8. Fare clic su **File** e successivamente su **Save changes and exit** (Salva le modifiche ed esci). 9. Premere invio. 10. Premere F10 per salvare le modifiche e uscire dall'utility.
Dopo l'abilitazione del modulo TPM, la password dell'utility Impostazione computer (F10) può essere eliminata.	Per l'abilitazione del modulo TPM è necessaria una password per l'utility Impostazione computer (F10). Dopo che il modulo è stato abilitato, la password può essere eliminata. In questo modo, chiunque abbia accesso diretto al sistema avrà la possibilità di reimpostare il modulo TPM e causare una perdita di dati.	Come da progettazione. La password dell'utility Impostazione computer (F10) può essere eliminata solo da un utente a conoscenza della password stessa. In ogni caso, HP consiglia vivamente di mantenere sempre una password a protezione dell'utility Impostazione computer (F10).
La casella della password PSD non viene visualizzata dopo che il sistema torna attivo a seguito di uno stato di standby.	Quando un utente si connette al sistema dopo avere creato un PSD, il TPM richiede la password utente di base. Se l'utente non digita la password e il sistema entra in standby, la casella della password non risulterà più disponibile.	Secondo progettazione. L'utente deve uscire dal sistema e riaccedere per visualizzare di nuovo la finestra della password PSD.
Per la modifica dei criteri della piattaforma di protezione non è richiesta alcuna password.	L'accesso alle Security Platform Policies (Politiche piattaforma di sicurezza) (per macchina e utente) non richiede una password TPM per gli utenti in possesso di diritti amministrativi sul sistema.	Secondo progettazione. Qualunque amministratore può modificare le politiche della piattaforma di sicurezza con o senza inizializzazione utente TPM.
I certificati visualizzati sono indicati come “non affidabili”.	Dopo avere impostato HP ProtectTools e avere eseguito l'inizializzazione guidata, l'utente ha la possibilità di visualizzare il certificato emesso. Tuttavia, una volta visualizzato, il certificato appare come “non affidabile”. Il certificato può essere installato facendo clic sul relativo pulsante, ma tale operazione non lo rende affidabile.	I certificati autofirmati non vengono considerati affidabili. In un ambiente aziendale configurato correttamente, i certificati EFS vengono rilasciati da autorità di certificazione online e vengono considerati affidabili.

Breve descrizione	Dettagli	Soluzione
Si verifica un errore intermittente di crittografia e decrittografia: **Il processo non riesce ad accedere al file perché questo è già utilizzato da un altro processo.**	Si tratta di un errore a intermittenza frequente durante la crittografia o la decrittografia e si verifica perché il file viene utilizzato da un altro processo, anche se il file o la cartella in questione non viene elaborato dal sistema operativo o da altre applicazioni.	Per correggere l'errore: 1. Riavviare il sistema. 2. Disconnettersi. 3. Riconnettersi.
Si verifica una perdita di dati nel supporto estraibile se questo viene rimosso prima che la generazione dei nuovi dati o il trasferimento sia stato completato.	Dopo la rimozione, un dispositivo di archiviazione come, ad esempio, un disco rigido MultiBay continua a mostrare una disponibilità PSD e non genera errori durante l'aggiunta/modifica di dati nel PSD. Dopo il riavvio del sistema, il PSD non riflette le modifiche apportate al file mentre il supporto estraibile non era disponibile.	Non rimuovere un PSD prima di avere completato la generazione o il trasferimento dei dati. Questo problema si verifica solo se l'utente accede al PSD e quindi rimuove il disco rigido prima che il processo di generazione o di trasferimento dei dati sia stato completato. Se l'utente cerca di accedere al PSD quando il disco rigido non è presente, viene visualizzato il messaggio di errore **the device is not ready** (dispositivo non pronto).
Durante la disinstallazione, se l'utente non ha inizializzato l'utente di base e apre lo strumento di amministrazione, l'opzione **Disabilita** non risulterà disponibile e il programma di disinstallazione si interrompe fino a quando lo strumento di amministrazione non viene chiuso.	L'utente ha la possibilità di effettuare la disinstallazione senza disabilitare il TPM oppure disattivandolo prima della disinstallazione (tramite lo strumento di amministrazione). Per accedere allo strumento di amministrazione è necessaria l'inizializzazione della chiave utente di base. Se l'inizializzazione di base non è stata eseguita, tutte le opzioni risulteranno inaccessibili all'utente. Dato che l'utente ha esplicitamente scelto di aprire lo strumento di amministrazione, facendo clic su **Sì** nel prompt della finestra di dialogo **Click Yes to open Embedded Security Administration tool** (Fare clic su Sì per aprire lo strumento di amministrazione di Embedded Security), il programma di disinstallazione si interrompe in attesa che lo strumento di amministrazione venga chiuso. Se nella finestra di dialogo l'utente seleziona **No**, lo strumento di amministrazione non viene aperto e la disinstallazione prosegue normalmente.	Lo strumento di amministrazione viene utilizzato per disabilitare il chip TPM, ma l'opzione non risulterà a meno che la chiave utente di base non sia stata inizializzata. In caso contrario, selezionare **OK** o **Annulla** per procedere con la disinstallazione.
Dopo la creazione del PSD su account per 2 utenti e se si utilizzano commutazioni rapide in configurazioni di sistema a 128 MB, si verificano blocchi intermittenti del sistema.	Se si utilizza la commutazione rapida con una RAM minima, il sistema potrebbe bloccarsi producendo una schermata nera al posto di quella introduttiva e il mouse e la tastiera potrebbero diventare inattivi.	Tale comportamento è probabilmente dovuto a un problema di temporizzazione nelle configurazioni con memoria scarsa. La grafica integrata utilizza un'architettura UMA che richiede 8 MB di memoria, lasciando solo 120 MB a disposizione dell'utente. L'errore viene generato quando questi 120 MB vengono condivisi dai due utenti connessi, che utilizzano la commutazione rapida. Per risolvere il problema, riavviare il sistema e aumentare la configurazione di memoria (HP non fornisce configurazioni da 128 MB con i moduli di protezione).
L'autenticazione utente EFS (è richiesta la	La password di autenticazione utente EFS viene riaperta dopo che l'utente fa	Come da progettazione. Per evitare problemi con Microsoft EFS, è stato creato un timer watchdog di 30 secondi per generare il messaggio d'errore.

Breve descrizione	Dettagli	Soluzione
password) scade con **accesso negato**.	clic su **OK** o quando il sistema esce dallo stato di standby.	
Durante l'impostazione del giapponese si osservano tagli minimi nelle descrizioni funzionali.	Durante la configurazione personalizzata della procedura di installazione guidata le descrizioni funzionali vengono tagliate.	HP si occuperà del problema in una release futura.
La crittografia EFS funziona senza bisogno di digitare una password alla richiesta.	Se si lascia scadere il tempo di immissione della password utente, sarà comunque possibile crittografare un file o una cartella.	La crittografia non richiede l'autenticazione della password, perché è una funzione di Microsoft EFS. Al contrario, per la decrittografia è necessario fornire la password utente.
La funzione di posta elettronica protetta è supportata anche se non viene specificata nell'inizializzazione guidata utente o quando la configurazione della posta elettronica protetta viene disabilitata nei criteri utente.	Il software Embedded Security e il programma guidato non controllano le impostazione dei client di posta elettronica (Outlook, Outlook Express o Netscape).	È il funzionamento previsto. La configurazione delle impostazioni di posta elettronica TPM non impedisce la modifica delle impostazioni di decrittazione direttamente all'interno di un client di posta elettronica. L'utilizzo della posta elettronica protetta viene impostato e controllato tramite applicazioni di terze parti. Il programma guidato di HP consente di effettuare collegamenti alle tre applicazioni di riferimento, per una personalizzazione immediata.
Eseguendo una seconda volta una distribuzione su larga scala sullo stesso PC o su un PC inizializzato in precedenza vengono sovrascritti i file Emergency Recovery e Emergency Token. I nuovi file non possono essere utilizzati per il recupero.	Una distribuzione su larga scala su un sistema HP ProtectTools Embedded Security precedentemente inizializzato, rende inutili Recovery Archives e Recovery Tokens in quanto sovrascrive i relativi file XML.	HP si sta occupando di risolvere il problema relativo alla sovrascrittura dei file XML e fornirà una soluzione in un prossimo SoftPaq.
Gli script di accesso automatico non funzionano durante il ripristino utente in Embedded Security.	L'errore si presenta quando l'utente svolge le seguenti azioni: • inizializza proprietario e utente in Embedded Security (utilizzando le posizioni predefinite: **Documenti**). • Ripristina le impostazioni predefinite del chip nel BIOS. • Riavvia il computer. • Inizia a ripristinare Embedded Security. Durante il processo di ripristino, Credential Manager chiede se il sistema è in grado di automatizzare l'accesso all'autenticazione utente TPM Infineon. Se l'utente seleziona **Sì**, la posizione di SPEmRecToken viene automaticamente visualizzata nella casella di testo. Anche se questa posizione è corretta, viene visualizzato il seguente messaggio d'errore: **No Emergency Recovery Token is provided. Select the token location the Emergency Recovery**	Fare clic sul pulsante **Browse** (Sfoglia) dello schermo per selezionare la posizione e proseguire con il processo di ripristino.

Breve descrizione	Dettagli	Soluzione
	Token should be retrieved from (Nessun Emergency Recovery Token fornito. Selezionare la posizione da cui richiamare l'Emergency Recovery Token).	
I PSD multiutente non funzionano in un ambiente a commutazione rapida.	Questo errore si verifica se sono stati creati più utenti ai quali è stato fornito un PSD con la stessa lettera di identificazione. Se si tenta di eseguire una commutazione rapida fra utenti mentre il PSD viene caricato, il secondo utente non potrà utilizzare il PSD.	Il PSD del secondo utente sarà disponibile solo dopo essere stato riconfigurato per utilizzare una lettera diversa oppure se il primo utente si disconnette.
Il PSD viene disabilitato e non può essere eliminato dopo la formattazione del disco rigido in cui è stato generato.	L'icona del PSD rimane visibile, ma se l'utente cerca di accedere al PSD viene visualizzato il messaggio di errore **drive is not accessible** (unità non accessibile). L'utente non può eliminare il PSD e viene visualizzato il seguente messaggio: **your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process** (Il PSD è in uso. Controllare che il PSD non contenga file aperti e che non sia utilizzato da un altro processo). Per eliminare il PSD, l'utente deve riavviare il sistema. Il PSD non verrà ricaricato.	Secondo progettazione: se un cliente cancella volutamente o si scollega dalla posizione in cui sono memorizzati i dati del PSD, l'emulazione dell'unità PSD di Embedded Security continua a funzionare producendo errori dovuti all'assenza di comunicazione con i dati mancanti. Soluzione: al riavvio successivo, le emulazioni non vengono più caricate e l'utente può cancellare la vecchia emulazione PSD e creare un nuovo PSD.
Quando l'utente esegue un ripristino da Automatic Backup Archive viene rilevato un errore interno.	In Embedded Security, se l'utente seleziona l'opzione **Restore under Backup** (Ripristina da backup) per eseguire un ripristino dall'archivio di backup automatico e successivamente seleziona **SPSystemBackup.xml**, il ripristino guidato non viene completato e viene visualizzato il seguente messaggio di errore: **The selected Backup Archive does not match the restore reason. Please select another archive and continue** (L'archivio di backup selezionato non corrisponde alla motivazione del ripristino. Selezionare un altro archivio e continuare).	Se l'utente seleziona **SPSystemBackup.xml** quando viene richiesto SpBackupArchive.xml, il programma guidato di Embedded Security non viene completato e viene visualizzato il seguente messaggio di errore: **An internal Embedded Security error has been detected** (È stato rilevato un errore interno di Embedded Security). Selezionare il corretto file XML che corrisponda alla motivazione richiesta. I processi vengono eseguiti correttamente. Tuttavia, il messaggio di errore interno a Embedded Security non è chiaro e dovrebbe riportare un messaggio più appropriato. HP sta cercando di ovviare a questo problema nei prodotti futuri.
Il sistema di protezione mostra un errore di ripristino con utenti multipli.	Durante il processo di ripristino, l'amministratore seleziona gli utenti da ripristinare. Gli utenti non selezionati non saranno in grado di ripristinare le chiavi nel caso tentino di effettuare il ripristino in un secondo momento. Viene visualizzato il messaggio di errore che segnala che il **processo di decrittazione non stato completato correttamente**.	Per ripristinare gli utenti non selezionati, reimpostare il TPM, eseguire l'operazione di ripristino e selezionare tutti gli utenti prima che venga eseguito il backup quotidiano predefinito. Con l'esecuzione del backup automatico, gli utenti non ripristinati vengono sovrascritti e tutti i dati vengono eliminati. Una volta salvato il nuovo backup di sistema, non sarà possibile ripristinare gli utenti precedentemente non selezionati. Inoltre, l'utente dovrà ripristinare l'intero backup di sistema. Un backup dell'archivio può essere ripristinato singolarmente.
Con la reimpostazione della ROM del sistema ai	Il ripristino dei valori predefiniti della ROM di sistema nasconde il TPM a Windows, impedendo il corretto	Rendere visibile il TPM nel BIOS:

Breve descrizione	Dettagli	Soluzione
valori predefiniti il TPM non viene più visualizzato.	funzionamento del software di sicurezza e rendendo inaccessibili i dati crittografati dal TPM.	Aprire l'utility Impostazione del computer (F10), selezionare **Security** > **Device security** (Sicurezza > Sicurezza periferiche), quindi modificare il campo da **Hidden** (Nascosto) ad **Available** (Disponibile).
Il backup automatico non funziona con l'unità mappata.	Quando un amministratore configura l'opzione Automatic Backup (Backup automatico) in Embedded Security, viene creata una voce in **Windows** > **Operazioni** > **Operazioni pianificate**. Questa operazione pianificata di Windows è configurata per utilizzare NT AUTHORITY\SYSTEM per i diritti di esecuzione del backup. Funziona correttamente con qualunque unità locale. Quando, invece, l'amministratore configura il backup automatico in modo che il salvataggio avvenga su un'unità mappata, il processo non va a buon fine in quanto NT AUTHORITY\SYSTEM non possiede i diritti per utilizzare l'unità mappata. Se il backup automatico è programmato per avviarsi all'accesso, nell'icona Embedded Security dell'area di notifica sulla barra delle applicazioni viene visualizzato il seguente messaggio: **The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again** (Al momento, la posizione dell'archivio di backup non è accessibile. Fare clic qui per effettuare il backup in un archivio temporaneo fino a quando l'archivio di backup non tornerà disponibile). Tuttavia, se il backup automatico è programmato per un orario specifico, tale operazione non verrà eseguita e non verrà visualizzato alcun messaggio informativo.	Per ovviare al problema, cambiare NT AUTHORITY \SYSTEM in (nome computer)\(nome amministratore). Questa è l'impostazione predefinita se l'Operazione pianificata viene creata manualmente. HP sta lavorando affinché le impostazioni predefinite delle release future comprendano il nome computer \nome amministratore.
Non è possibile disattivare temporaneamente Embedded Security nell'interfaccia di Embedded Security.	Il software 4.0 corrente è stato progettato per implementazioni di HP Notebook 1.1B oltre che per supportare implementazioni di HP Desktop 1.2. Questa possibilità di disabilitazione è tuttora supportata nell'interfaccia software per piattaforme TPM 1.1.	HP si occuperà del problema nelle release future.

Device Access Manager for HP ProtectTools

Descrizione sintetica	Dettagli	Soluzione
Agli utenti è stato negato l'accesso alle periferiche in Device Access Manager, ma le periferiche risultano comunque accessibili.	In Device Access Manager sono stati selezionati Configurazione semplice e/o Configurazioni delle classi di periferiche per negare agli utenti l'accesso alle periferiche. Ciononostante, gli utenti possono comunque accedere alle periferiche.	Verificare che il servizio per il blocco delle periferiche HP ProtectTools sia stato attivato. In qualità di utente con diritti di amministratore, selezionare **Pannello di controllo** > **Strumenti di amministrazione** > **Servizi**. Nella finestra **Servizi**, cercare il servizio **HP ProtectTools Device Locking/ Auditing** (Blocco/audit periferiche HP ProtectTools). Assicurarsi che il servizio sia stato avviato e che il tipo di avvio sia **automatico**.
L'utente ha avuto accesso in modo imprevisto a una periferica oppure a un utente è stato negato in modo imprevisto l'accesso a una periferica.	Device Access Manager è stato utilizzato per negare agli utenti l'accesso ad alcune periferiche e consentirne l'accesso ad altre periferiche. Durante l'utilizzo del sistema, gli utenti riescono a utilizzare periferiche il cui accesso dovrebbe essere negato da Device Access Manager e non riescono a utilizzare periferiche che Device Access Manager dovrebbe rendere accessibili.	Utilizzare Configurazione delle classi di periferiche di Device Access Manager per controllare le impostazioni delle periferiche degli utenti. Fare clic su **Security Manager**, quindi su **Device Access Manager** e infine su **Device Class Configuration** (Configurazione delle classi di periferiche). Espandere i livelli nella struttura ad albero Device Class (Classe periferiche) ed esaminare le impostazioni valide per l'utente. Verificare la presenza di autorizzazioni di tipo Deny (Nega) eventualmente impostate per l'utente o di un gruppo di Windows di cui potrebbero essere membri (ad esempio, Utenti o Amministratori).
Tra le autorizzazioni di tipo Consenti e Nega, quale ha la priorità?	In Configurazione delle classi di periferiche, è stata impostata la seguente configurazione: • L'autorizzazione Consenti è stata concessa a un gruppo di Windows (ad esempio, BUILTIN \Administrators), mentre quella Nega è stata concessa a un altro gruppo di Windows (ad esempio, BUILTIN\Users) allo stesso livello nella gerarchia della classe delle periferiche (ad esempio, Unità DVD/CD-ROM). Se un utente appartiene a entrambi i gruppi (ad esempio, un amministratore), quale ha la priorità?	All'utente viene negato l'accesso alla periferica. Nega ha la priorità rispetto a Consenti. L'accesso viene negato a causa dell'elaborazione di Windows dell'effettiva autorizzazione per la periferica. A un gruppo viene negato l'accesso e all'altro gruppo viene concesso, ma l'utente è membro di entrambi i gruppi. All'utente viene negato l'accesso perché Nega ha la priorità rispetto all'autorizzazione Consenti. Per ovviare a questo problema, è possibile negare l'accesso al gruppo User a livello Unità DVD/CD-ROM e di consentirlo al gruppo Administrators a un livello inferiore a quello Unità DVD/CD-ROM. In alternativa, si consiglia di creare specifici gruppi di Windows, uno per consentire l'accesso all'unità DVD/ CD e uno per negare l'accesso a tale unità. Gli utenti specifici possono quindi essere aggiunti al gruppo desiderato.

Varie

Descrizione sintetica dell'impatto sul software	Dettagli	Soluzione
Security Manager - avviso ricevuto: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (Impossibile installare l'applicazione di protezione finché non viene installato HP ProtectTools Security Manager).	Tutte le applicazioni di protezione, quale Embedded Security, Java Card Security e i sistemi biometrici, sono plug-in modulari dell'interfaccia di Security Manager. Per caricare un plug-in di protezione approvato da HP, è necessario avere installato Security Manager.	Per installare un plug-in di protezione, è necessario avere installato il software Security Manager.
Utility di aggiornamento del firmware TPM per modelli contenenti TPM abilitati per Broadcom. Lo strumento fornito tramite il sito Web dell'assistenza HP restituisce il messaggio **ownership required** (Indicare la proprietà).	Si tratta del comportamento previsto dalla utility del firmware TPM per modelli contenenti TPM abilitati per Broadcom. Lo strumento di aggiornamento del firmware consente all'utente di aggiornare il firmware, con o senza la chiave di approvazione (Endorsement Key, EK). In assenza della chiave di approvazione, l'aggiornamento del firmware può essere completato senza alcuna autorizzazione. Se la chiave è presente, è necessario che vi sia un proprietario TPM che autorizzi l'aggiornamento. Al termine dell'aggiornamento, la piattaforma deve essere riavviata perché abbia effetto il nuovo firmware. Se il BIOS TPM è resettato di fabbrica, la proprietà viene rimossa e la funzione di aggiornamento del firmware impedita finché non siano state configurate la piattaforma Embedded Security Software e la procedura guidata di inizializzazione utente. **NOTA:** Dopo avere effettuato l'aggiornamento del software, si consiglia di riavviare il sistema. La versione del firmware non viene identificata correttamente fino alla fine del riavvio.	1. Installare nuovamente il software Embedded Security. 2. Eseguire la procedura guidata di configurazione della piattaforma e dell'utente. 3. Assicurarsi che Microsoft .NET framework 1.1 sia installato nel sistema: a. Fare clic su **Start/Avvio**. b. Fare clic su **Pannello di controllo**. c. Fare clic su **Installazione applicazioni**. d. Assicurarsi che **Microsoft .NET Framework 1.1** sia incluso nell'elenco. 4. Controllare la configurazione hardware e software: a. Fare clic su **Start/Avvio**. b. Fare clic su **Tutti i programmi**. c. Fare clic su **HP ProtectTools Security Manager for Administrators** in Windows Vista o su **HP ProtectTools Security Manager** in Windows XP. d. Selezionare **Embedded Security** dal menu. e. Fare clic su **More Details** (Altri dettagli) Il sistema dovrebbe avere la seguente configurazione: • Versione prodotto = V4.0.1 • Stato sicurezza integrata: Stato chip = Abilitato, Stato proprietario = Inizializzato, Stato utente = Inizializzato • Informazioni sui componenti: Spec. TCG Versione = 1.2 • Casa produttrice = Broadcom Corporation

Descrizione sintetica dell'impatto sul software	Dettagli	Soluzione
		• Versione FW = 2.18 (o superiore) • Libreria driver TPM versione 2.0.0.9 (o superiore) 5. Se la versione del firewall non corrisponde alla 2.18, scaricare e aggiornare il firmware TPM. TPM Firmware SoftPaq è un download di supporto disponibile sul sito Web di HP all'indirizzo http://www.hp.com.
HP ProtectTools Security Manager: Ad intermittenza, viene riportato un errore quando si chiude l'interfaccia Security Manager.	A livello intermittente (1 su 12 casi), si crea un errore con l'uso del pulsante di chiusura, a destra, nella parte superiore della videata, per chiudere Security Manager prima che siano state caricate tutte le applicazioni plug-in.	Ciò è associato ad una dipendenza dal tempo di caricamento dei servizi plug-in quando si chiude e si riavvia Security Manager. Dal momento che PTHOST.exe è l'interfaccia contenente le altre applicazioni (plug-in), completare il tempo di caricamento (servizi) dipende dalla capacità del plug-in. La chiusura dell'interfaccia prima che il plug-in abbia avuto il tempo di completare il caricamento è la causa di fondo. Consentire a Security Manager di completare il messaggio di caricamento dei servizi (visualizzato nella parte superiore della finestra Security Manager) e di tutti i plug-in elencati nella colonna di sinistra. Per evitare errori, attendere qualche minuto per consentire il caricamento dei plug-in.
HP ProtectTools — L'accesso illimitato o i privilegi di amministratore non controllati costituiscono un rischio per la protezione.	L'accesso illimitato al PC client espone la protezione a vari pericoli, fra cui: • Eliminazione della PSD • Modifica a scopi illeciti delle impostazioni degli utenti • Disattivazione dei criteri e delle funzioni di protezione	Si consigliano gli amministratori di adottare le “migliori prassi” limitando i privilegi degli utenti finali e restringendo l'accesso. Agli utenti non autorizzati non dovrebbero essere concessi privilegi amministrativi.
Le password Embedded Security per il BIOS e il sistema operativo sono fuori sincrono.	Se un utente non convalida una nuova password come password Embedded Security per il BIOS, viene ripristinata la password Embedded Security originale tramite il tasto F10 del BIOS.	Questo funzionamento è corretto. Tali password possono essere risincronizzate modificando la password utente base del sistema operativo e autenticandola nella finestra di BIOS Embedded Security in cui viene richiesta la password.
Dopo che nel BIOS è stata abilitata l'autenticazione di preavvio del TPM, solo un utente potrà accedere al sistema.	Il PIN BIOS TPM è associato al primo utente che inizializza l'impostazione utente. Se un computer viene utilizzato da più utenti, il primo risulta essere l'amministratore. Il primo utente dovrà comunicare il proprio PIN utente TPM agli altri utenti per consentirne la connessione.	Questo funzionamento è corretto. HP consiglia che l'ufficio informatico del cliente adotti validi criteri di sicurezza nel definire le proprie soluzioni di protezione e che la password dell'amministratore del BIOS venga configurata dagli amministratori informatici per ottenere una protezione a livello di sistema.
Gli utenti devono modificare il proprio PIN per consentire il corretto funzionamento del preavvio TPM dopo un ripristino TPM.	Per consentire il corretto funzionamento dell'autenticazione BIOS TPM dopo il ripristino, gli utenti devono modificare il proprio PIN o creare un altro utente per inizializzare le proprie impostazioni utente. Non è disponibile alcuna opzione per consentire il corretto funzionamento dell'autenticazione BIOS TPM.	È il funzionamento previsto. Il ripristino cancella la chiave utente di base. Per inizializzare nuovamente la chiave utente di base, l'utente deve modificare il proprio PIN oppure creare un nuovo utente.

Descrizione sintetica dell'impatto sul software	Dettagli	Soluzione
Supporto autenticazione accensione non è stato impostato sui valori predefiniti utilizzando **Reset to Factory Settings** (Ripristina impostazioni iniziali) di Embedded Security.	In Computer Setup, non sono state ripristinate le impostazioni predefinite di **Power-on authentication support** (Supporto autenticazione all'accensione) con l'opzione **Reset to Factory Settings** (Ripristina impostazioni predefinite) di Embedded Security Device. Per impostazione predefinita, **Power-on authentication support** (Supporto autenticazione all'accensione) è impostato su **Disable** (Disabilita).	L'opzione **Reset to Factory Settings** (Ripristina impostazioni iniziali) disattiva la periferica Embedded Security, che nasconde altre opzioni di Embedded Security (fra cui **Supporto autenticazione accensione**). Tuttavia, dopo avere nuovamente abilitato la periferica Embedded Security, **Supporto autenticazione accensione** resta attivato. HP sta lavorando per trovare una soluzione al problema, che verrà inclusa in una futura offerta SoftPaq ROM, distribuita sul Web.
L'autenticazione all'accensione si sovrappone alla password del BIOS durante la sequenza di avvio.	L'autenticazione all'accensione richiede di connettersi al sistema utilizzando la password TPM, ma premendo F10 per accedere al BIOS, l'utente ottiene i diritti di sola lettura.	Per scrivere nel BIOS, l'utente deve digitare la password del BIOS al posto della password TPM nella finestra di autenticazione all'accensione.
Dopo che la password proprietario è stata modificata, il BIOS richiede la password vecchia e la nuova tramite Impostazione del computer.	Dopo che la password proprietario è stata modificata nel software Windows Embedded Security, il BIOS richiede la password vecchia e la nuova tramite Impostazione del computer.	È il funzionamento previsto. Ciò è dovuto all'incapacità del BIOS di comunicare con il TPM una volta che il sistema operativo è in funzione e serve per verificare la frase di accesso del TPM.

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.

archivio di ripristino di emergenza. Area di memorizzazione protetta che consente la nuova crittografia di chiavi utente di base da una chiave del proprietario della piattaforma in un'altra.

attivazione. L'attività che deve essere eseguita per rendere accessibili le funzioni di Drive Encryption. Drive Encryption si attiva utilizzando la configurazione guidata di HP ProtectTools Security Manager for Administrators. Solo un amministratore può attivare Drive Encryption. Il processo di attivazione comprende l'attivazione del software, la crittografia dell'unità, la creazione di un account utente e la creazione della chiave crittografica di backup iniziale su un dispositivo di memorizzazione rimovibile.

autenticazione di accensione. Funzione di protezione che richiede un certo tipo di autenticazione, ad esempio una Java Card, un chip di protezione o una password quando il computer viene acceso.

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.

autorità di certificazione. Servizio che rilascia i certificati necessari per l'esecuzione di un'infrastruttura a chiave pubblica.

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

certificato di Privacy Manager. Un certificato digitale che richiede l'autenticazione ogni volta che viene utilizzato per operazioni di crittografia, ad esempio la firma e la crittografia di messaggi e-mail e di documenti di Microsoft Office.

certificato digitale. Credenziali elettroniche che confermano l'identità di un utente o una società grazie all'associazione dell'identità del proprietario del certificato digitale a una coppia di chiavi elettroniche utilizzate per firmare informazioni digitali.

Chat History Viewer. Un componente di Privacy Manager Chat che consente di cercare e visualizzare le sessioni crittografate di cronologia delle chat.

chip di protezione integrato Trusted Platform Module (TPM). Il termine generico per indicare il chip di HP ProtectTools Embedded Security. Un TPM fornisce l'autenticazione di un computer, e non di un utente, memorizzando informazioni specifiche del sistema host, come ad esempio chiavi di crittografia, certificati digitali e password. Un TPM riduce al minimo il rischio di compromissione dei dati del computer a seguito di furti fisici o di attacchi esterni da parte di hacker.

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.

cifratura. Procedura, come l'utilizzo di un algoritmo, impiegata nella crittografia per convertire testo normale in testo crittografato in modo da impedire la lettura dei dati da parte di destinatari non autorizzati. Sono disponibili diversi tipi di cifratura dei dati che costituiscono la base della protezione della rete. I tipi più comuni includono Data Encryption Standard e la crittografia a chiave pubblica.

contatto attendibile. Una persona che ha accettato l'invito di contatto attendibile.

credenziali. Metodo con cui un utente dimostra l'idoneità all'esecuzione di una specifica attività durante il processo di autenticazione.

crittografia per i contatti attendibili. Un'operazione che aggiunge una firma digitale, crittografa il messaggio e-mail e lo invia dopo che è stata eseguita l'autenticazione attraverso il metodo di accesso di sicurezza selezionato.

crittografia. Procedura utilizzata per cifrare e decifrare i dati in modo che possano essere decodificati solo da specifici utenti.

cronologia chat. Un file crittografato che contiene una registrazione di entrambe le parti di una conversazione in una sessione di chat.

cryptographic service provider (CSP). Provider o libreria di algoritmi di crittografia che è possibile utilizzare in un'interfaccia ben definita per l'esecuzione di specifiche funzioni di crittografia.

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

destinatario di contatto attendibile. Una persona che riceve un invito a diventare un contatto attendibile.

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.

DriveLock Funzione di sicurezza che collega il disco rigido a un utente e richiede all'utente di digitare correttamente la password DriveLock all'avvio del computer.

elenco contatti attendibili. Un elenco dei contatti attendibili.

eliminazione semplice. Eliminazione del riferimento di Windows alla risorsa. Il contenuto della risorsa rimane nell'unità disco rigido fino a che su di esso vengono sovrascritti dati oscuranti mediante la pulizia dello spazio libero.

Encryption File System (EFS). Sistema che consente di crittografare tutti i file e le sottocartelle all'interno della cartella selezionata.

firma digitale. Dati inviati con un file che verificano il mittente del materiale e controllano che il file non sia stato modificato dopo che è stato firmato.

firmatario suggerito. Un utente designato dal proprietario di un documento di Microsoft Word o Microsoft Excel per l'aggiunta di una riga per la firma all'interno del documento.

identità. In HP ProtectTools Credential Manager, gruppo di credenziali e impostazioni gestite come un account o un profilo di uno specifico utente.

Infrastruttura a chiave pubblica (PKI) Standard che definisce le interfacce per la creazione, l'utilizzo e l'amministrazione di certificati e chiavi di crittografia.

invito di contatto attendibile. Un messaggio e-mail inviato a una persona, in cui le si chiede di diventare un contatto attendibile.

Java Card. Una scheda rimovibile che viene inserita nel computer e che contiene le informazioni di identificazione per l'accesso. L'accesso con una Java Card nella schermata di accesso di Drive Encryption richiede l'inserimento della Java Card e l'immissione del nome utente e del PIN della Java Card.

massima sicurezza. Funzione di sicurezza nella configurazione del BIOS che fornisce una protezione potenziata per le password di accensione e dell'amministratore e per altre forme di autenticazione all'avvio.

messaggio attendibile. Una sessione di comunicazione durante la quale i messaggi attendibili vengono inviati da un mittente attendibile a un contatto attendibile.

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

migrazione. Un'operazione che consente la gestione, il ripristino e il trasferimento di certificati e contatti attendibili di Privacy Manager.

mittente attendibile. Un contatto attendibile che invia messaggi e-mail e documenti di Microsoft Office firmati e/o crittografati.

modalità periferica SATA. Modalità di trasferimento dati fra un computer e altri dispositivi di archiviazione di massa, come dischi rigidi e unità ottiche.

modalità sicurezza BIOS. Impostazione in Java Card Security che, quando attivata, richiede l'utilizzo di una Java card e di un PIN valido per l'autenticazione dell'utente.

Password dell'amministratore BIOS. Password di *configurazione* di Impostazione del computer.

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

personal secure drive (PSD). Fornisce un'area di memorizzazione protetta per le informazioni riservate.

Profilo BIOS. Gruppo di impostazioni di configurazione del BIOS che possono essere salvate e applicate ad altri account.

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

pulizia dello spazio libero. La scrittura di dati casuali sullo spazio occupato in precedenza da dati poi eliminati, al fine di occultare il contenuto degli spazi liberi, rendendo più difficoltoso il recupero dei dati precedenti.

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

riavvio. Processo di riavvio del computer.

riga per la firma. Un segnaposto per la visualizzazione di una firma digitale. Quando un documento viene firmato, vengono visualizzati il nome del firmatario e il metodo di verifica. È possibile inserire anche la data della firma e il titolo del firmatario.

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.

rivelazione. Un'operazione che consente all'utente di decrittografare una o più sessioni di chat, visualizzando il nome del contatto in testo normale e rendendo la sessione disponibile per la visualizzazione.

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

Send Security (Sicurezza invio), pulsante. Un pulsante software che viene visualizzato sulla barra degli strumenti dei messaggi e-mail in Microsoft Outlook. Facendo clic sul pulsante è possibile firmare e/o crittografare un messaggio e-mail in Microsoft Outlook.

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

servizio di recupero chiavi di Drive Encryption. Il servizio di recupero SafeBoot memorizza una copia della chiave di crittografia, consentendo l'accesso al computer qualora la password venga dimenticata e non si abbia accesso alla chiave di backup locale. Per impostare l'accesso online alla chiave di backup, è necessario creare un account per il servizio.

sessione di comunicazione IM attendibile. Una sessione di comunicazione durante la quale i messaggi attendibili vengono inviati da un mittente attendibile a un contatto attendibile.

Sign and Encrypt (Firma e crittografa), pulsante. Un pulsante software che viene visualizzato sulla barra degli strumenti delle applicazioni di Microsoft Office. Facendo clic sul pulsante è possibile firmare, crittografare o rimuovere la crittografia in un documento di Microsoft Office.

Single Sign On. Funzione che memorizza le informazioni di autenticazione e consente di utilizzare Credential Manager per accedere a Internet e alle applicazioni Windows che richiedono l'autenticazione della password.

smart card. Piccolo componente hardware simile per dimensioni e forma a una carta di credito che consente di memorizzare informazioni di identificazione sul proprietario. Utilizzato per l'autenticazione del proprietario su un computer.

token USB. Dispositivo di protezione che consente di memorizzare le informazioni di identificazione su un utente. Analogamente alla Java Card o a un lettore biometrico, viene utilizzato per autenticare il proprietario su un computer.

token virtuale. Funzione di sicurezza che funziona in modo molto simile a un lettore di Java Card e di smart card tradizionali. Il token viene salvato sul disco rigido del computer o nel registro di Windows. Quando si effettua l'accesso con un token virtuale, per completare l'autenticazione viene richiesto un PIN utente.

token. Vedere metodo di accesso di sicurezza.

TXT. Trusted Execution Technology. Hardware e firmware che garantiscono la protezione contro gli attacchi portati al software e ai dati di un computer.

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

Indice analitico

D

E

F

G

H