HP ProtectTools

Guida introduttiva

Prima edizione: gennaio 2011

Numero di parte documento: 638391-061

Sommario

1 Introduzione alle modalità di protezione

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

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

La disponibilità dei moduli software può variare a seconda del modello di computer.

I moduli software HP ProtectTools possono essere preinstallati, precaricati o scaricati dal sito Web HP. Per ulteriori informazioni, visitare 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 seguente vengono presentate in dettaglio le principali funzionalità dei moduli HP ProtectTools.

Modulo	Funzioni principali
Console amministrativa di HP ProtectTools Security Manager (per gli amministratori)	• Impostazione e configurazione dei livelli di protezione e dei metodi di accesso di sicurezza mediante l'installazione guidata di Security Manager. • Configurazione delle le opzioni non visibili dagli utenti. • Definizione delle configurazioni di Device Access Manager e dell'accesso dell'utente. • Aggiunta e rimozione degli utenti HP ProtectTools e visualizzazione del relativo stato mediante gli strumenti amministratore.
HP ProtectTools Security Manager (per gli utenti)	• Organizzazione, impostazione e modifica delle password. • Configurazione e modifica delle credenziali dell'utente, ad esempio password di Windows, impronte digitali e smart card. • Configurazione e modifica delle operazioni di distruzione e pulitura tramite File Sanitizer, e di altre impostazioni. • Visualizzazione delle impostazioni di Device Access Manager. • Configurazione di Computrace for HP ProtectTools. • Configurazione delle preferenze delle opzioni di backup e ripristino.
Credential Manager for HP ProtectTools (Gestore password)	• Salvataggio, organizzazione e protezione di nomi utente e password. • Impostazione delle schermate di accesso dei siti Web e programmi per accesso rapido e sicuro. • Salvataggio dei nomi utente e delle password dei siti Web mediante inserimento in Gestore password. Alla successiva visita al sito, Gestore password inserisce e invia automaticamente le informazioni. • Creazione di password più sicure per livelli superiori di protezione dell'account. Gestore password compila le informazioni e le invia in modo automatico.
Drive Encryption for HP ProtectTools (solo in determinati modelli)	• Crittografia completa dell'unità disco rigido. • Forzatura dell'autenticazione di preavvio per la decrittografia dei dati e il loro utilizzo.
File Sanitizer for HP ProtectTools	• Distruzione delle risorse digitali (informazioni riservate tra cui file di applicazioni, contenuti cronologici o correlati al Web o altri dati) presenti sul computer in uso e pulitura periodica delle risorse eliminate nel disco fisso.

Modulo	Funzioni principali
Device Access Manager for HP ProtectTools (solo in determinati modelli)	• Consente ai responsabili IT di controllare l'accesso ai dispositivi in base ai profili utente. • Impedisce agli utenti non autorizzati di rimuovere i dati tramite supporti di archiviazione esterni e di introdurre virus nel sistema da supporti simili. • Consente agli amministratori di disattivare l'accesso ai dispositivi scrivibili da parte di individui o gruppi di utenti specifici.
Privacy Manager for HP ProtectTools (solo in determinati modelli)	• Utilizzato per ottenere i certificati di autorità, che verificano l'origine, l'integrità e la sicurezza delle comunicazioni durante l'utilizzo della posta Microsoft o di documenti Microsoft Office.
Computrace for HP ProtectTools (da acquistare separatamente)	• Offre il monitoraggio sicuro delle risorse. • Esegue il monitoraggio dell'attività dell'utente e delle modifiche apportate all'hardware e al software. • Rimane attivo anche in caso di riformattazione o sostituzione del disco rigido. • L'attivazione richiede l'acquisto a parte di sottoscrizioni per il monitoraggio e il tracciamento.
Embedded Security for HP ProtectTools (solo in determinati modelli)	• Utilizza un chip di protezione incorporato TPM (Trusted Platform Module) per salvaguardare il computer dall'accesso non autorizzato ai dati e alle credenziali degli utenti memorizzati al suo interno. • Consente di creare un'unità protetta personale (PSD, Personal Secure Drive), utile ai fini della protezione dei file dell'utente e delle informazioni relative alle cartelle. • Supporta applicazioni di terze parti, ad esempio Microsoft Outlook e Internet Explorer, per operazioni protette correlate ai certificati digitali.

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

La maggior parte dei prodotti di protezione HP ProtectTools utilizza sia l'autenticazione utente (in genere una password) che il supporto amministrativo per ottenere l'accesso qualora si dimentichino o smarriscano le password, o in tutte le situazioni in cui le operazioni di protezione aziendali richiedono l'accesso.

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

Credential Manager for HP ProtectTools

Credential Manager (componente di Security Manager) è un archivio per nomi utente e password, e può essere utilizzato per:

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

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

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

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

Drive Encryption for HP ProtectTools

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

Esempio 1: un medico desidera avere accesso esclusivo ai dati presenti sull'unità disco rigido del suo computer, pertanto attiva Drive Encryption, che richiede l'autenticazione di preavvio prima dell'accesso a Windows. Terminata la configurazione, l'unità disco rigido non può essere aperta

senza una password persino prima dell'avvio del sistema operativo. Il medico potrebbe aumentare il livello di protezione dell'unità scegliendo di crittografare i dati con l'opzione delle unità che supportano la crittografia automatica.

Embedded Security e Drive Encryption for HP ProtectTools non consentono l'accesso ai dati crittografati anche in caso di rimozione dell'unità, perché sono entrambi associati alla scheda madre originale.

Esempio 2: un amministratore ospedaliero desidera garantire che solo i dottori e il personale autorizzato possano accedere a tutti i dati nei loro computer locali senza condividere le loro password personali. Gli addetti del reparto IT aggiungono l'amministratore, i dottori e tutto il personale autorizzato come utenti di Drive Encryption. A questo punto, solo il personale autorizzato può avviare il computer utilizzando il nome utente e la password personali.

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools viene utilizzato per rimuovere i dati in modo permanente, inclusi l'attività del browser Internet, i file temporanei, i dati eliminati in precedenza o eventuali altre informazioni. File Sanitizer può essere configurato per essere eseguito manualmente o automaticamente in base a una pianificazione definita dall'utente.

Esempio 1: un procuratore ha spesso a che fare con informazioni riservate relative ai clienti e vuole essere certo che i dati presenti nei file eliminati non possano essere ripristinati. Usa quindi File Sanitizer per distruggere i file eliminati affinché risulti quasi impossibile ripristinarli.

In genere, i dati eliminati in Windows non vengono effettivamente cancellati dall'unità disco rigido, ma i settori dell'unità disco rigido vengono contrassegnati come disponibili per uso futuro. Finché i dati non vengono sovrascritti, possono essere facilmente ripristinati tramite strumenti comuni disponibili su Internet. File Sanitizer sovrascrive i settori con dati casuali (più volte se necessario), rendendo i dati eliminati illeggibili e non ripristinabili.

Esempio 2: un ricercatore desidera distruggere i dati eliminati, i file temporanei, l'attività del browser e così via in modo automatico durante la disconnessione. Utilizza quindi File Sanitizer per pianificare la distruzione, in modo da poter selezionare i file comuni o eventuali file personalizzati da rimuovere definitivamente in modo automatico.

Device Access Manager for HP ProtectTools

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

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

Esempio 2: un'agenzia di assicurazioni non vuole che i dipendenti installino o carichino software o dati personali da casa. Alcuni di essi necessitano dell'accesso alla porta USB su tutti i computer. Il

responsabile IT utilizza quindi Device Access Manager per abilitare l'accesso per alcuni dipendenti, bloccando quello esterno ad altri.

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools viene utilizzato quando è necessario che le comunicazioni email via Internet siano protette. L'utente può creare e inviare email che possono essere aperte soltanto da un destinatario autenticato. Con Privacy Manager, le informazioni non possono essere compromesse o intercettate da utenti non autorizzati.

Esempio 1: un agente di cambio vuole essere certo che i suoi messaggi di posta vengano inviati a specifici clienti e che nessuno possa contraffare l'account di posta e intercettarlo. Esegue quindi la sua registrazione e quella dei suoi clienti a Privacy Manager. Privacy Manager rilascia un certificato di autenticazione a ciascun utente. Utilizzando questo strumento, l'agente di cambio e i suoi clienti devono eseguire l'autenticazione prima dello scambio di posta.

Privacy Manager for HP ProtectTools semplifica l'invio e la ricezione della posta da parte di destinatari precedentemente verificati e autenticati. Il servizio di posta può anche essere crittografato. Il processo di crittografia è simile a quello utilizzato quando si effettuano transazioni generiche con carta di credito su Internet.

Esempio 2: un amministratore delegato desidera garantire che soltanto i dirigenti possano visualizzare le informazioni che invia tramite posta elettronica, pertanto utilizza l'opzione per crittografare i messaggi di posta inviati e ricevuti da altri dirigenti. Con Privacy Manager Certificate of Authentication, il CEO e i dirigenti ottengono una copia della chiave di crittografia che consente soltanto a loro di decrittografare la posta riservata.

Computrace for HP ProtectTools (in precedenza LoJack Pro)

Computrace for HP ProtectTools (da acquistare a parte) è un servizio che consente di rintracciare un computer rubato nel momento in cui viene utilizzato per eseguire l'accesso a Internet.

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

Computrace for HP ProtectTools può anche consentire la gestione e l'individuazione remota dei computer, nonché il monitoraggio dell'uso del computer e delle applicazioni.

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

Embedded Security for HP ProtectTools (solo in determinati modelli)

Embedded Security for HP ProtectTools consente di creare un'unità protetta personale. Questa funzionalità consente all'utente di creare una partizione dell'unità virtuale sul PC che risulta completamente nascosta finché non vi si accede. Embedded Security potrebbe essere utilizzato in tutte le situazioni che richiedono la protezione assoluta dei dati mentre il resto delle informazioni non è crittografato.

Esempio 1: il computer di un responsabile di magazzino viene utilizzato periodicamente da più dipendenti nel corso della giornata. Il responsabile desidera crittografare e nascondere i dati di magazzino riservati presenti sul computer. Il suo obiettivo è proteggere i dati in modo che, anche in

caso di furto dell'unità disco rigido, non sia possibile decrittografarli o leggerli. Decide quindi di attivare Embedded Security e trasferisce i dati riservati sull'unità di protezione personale. Il responsabile può immettere una password e accedere ai dati riservati come in una qualsiasi altra unità disco rigido. Una volta eseguita la disconnessione o il riavvio dell'unità di protezione personale, questa non può essere vista o aperta senza l'opportuna password. I dipendenti non vedono mai i dati riservati quando accedono al computer.

Embedded Security protegge le chiavi di crittografia in un chip TPM (Trusted Platform Module) hardware presente sulla scheda madre. È l'unico strumento di crittografia che soddisfa i requisiti minimi necessari per bloccare i tentativi che gli utenti malintenzionati effettuano per indovinare la password di decrittografia. Embedded Security può anche crittografare tutta l'unità e i messaggi di posta elettronica.

Esempio 2: un agente di cambio desidera trasferire dati estremamente riservati su un altro computer utilizzando un'unità portatile. Vuole essere sicuro che l'unità sia accessibile solo da questi due computer, anche in caso di compromissione della password. L'agente usa la migrazione TPM di Embedded Security per consentire l'impiego in un secondo computer delle chiavi di crittografia necessarie per decrittografare i dati. Durante il processo di trasferimento, anche con la password, solo i due computer fisici sono in grado di decrittografare i dati.

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

Protezione da furti mirati

Un esempio di furto mirato è l'asportazione di un computer contenente dati personali e informazioni del cliente in un punto di controllo di sicurezza aeroportuale. Le funzionalità seguenti consentono di proteggere dai furti mirati:

- La funzionalità di autenticazione di preavvio, se abilitata, consente di impedire l'accesso al sistema operativo. Fare riferimento ai seguenti capitoli:
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- La funzione Personal Secure Drive offerta dal modulo Embedded Security for HP ProtectTools consente di crittografare i dati riservati per garantirne l'accesso solo con l'opportuna autenticazione. Fare riferimento al seguente capitolo:
  - Embedded Security for HP ProtectTools
- Computrace consente di individuare la posizione di un computer rubato. Fare riferimento al seguente capitolo:
  - Computrace for HP ProtectTools

Limitazione dell'accesso ai dati sensibili

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

- Device Access Manager for HP ProtectTools consente ai responsabili IT di limitare l'accesso ai dispositivi riscrivibili, in modo da impedire la stampa o la copia di informazioni riservate dall'unità disco rigido in supporti rimovibili.

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

L'accesso non autorizzato a un computer aziendale non protetto rappresenta un rischio reale per le risorse di rete dell'organizzazione, ad esempio le informazioni dei servizi finanziari, di un executive o

di un team di ricerca e sviluppo, nonché informazioni private ad esempio record di pazienti o record finanziari personali. Le seguenti funzionalità consentono di impedire l'accesso non autorizzato:

- La funzionalità di autenticazione di preavvio, se abilitata, consente di impedire l'accesso al sistema operativo. Fare riferimento ai seguenti capitoli:
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Gestore password permette di assicurare che un utente non autorizzato non possa ottenere password o accesso ad applicazioni protette da password.
- Device Access Manager for HP ProtectTools consente ai responsabili IT di limitare l'accesso ai dispositivi riscrivibili, in modo da impedire la stampa o la copia di informazioni riservate dall'unità disco rigido.
- File Sanitizer consente di eliminare in modo sicuro i dati distruggendo i file e le cartelle critici o eseguendo la pulitura delle risorse presenti sull'unità disco rigido (sovrascrittura dei dati eliminati ma ancora ripristinabili).
- Privacy Manager consente di ottenere i certificati di autorità durante l'utilizzo del servizio di posta elettronica Microsoft o dei documenti di Microsoft Office, proteggendo il processo di invio e di salvataggio delle informazioni importanti.

Creazione di criteri password complessi

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

Ulteriori elementi protettivi

Assegnazione dei ruoli per la 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 della protezione: definisce il livello di protezione dell'azienda o della rete, e determina le funzionalità di protezione da distribuire, ad esempio Drive Encryption o Embedded Security.

  NOTA: Molte delle caratteristiche di HP ProtectTools possono essere personalizzate dal responsabile della sicurezza in cooperazione con HP. Per maggiori informazioni, visitare il sito Web di HP all'indirizzo http://www.hp.com.

- Amministratore IT: applica e gestisce le funzionalità di protezione definite dal responsabile della protezione, e può anche abilitare o disabilitare alcune funzionalità. Ad esempio, se il responsabile della protezione ha deciso di implementare l'impiego delle smart card, l'amministratore IT può abilitare sia la modalità password che la modalità smart card.

- Utente: utilizza le funzioni di protezione. Ad esempio, se il responsabile della protezione e l'amministratore IT hanno abilitato le smart card per il sistema, l'utente può impostare il PIN della smart card e utilizzare quest'ultima per l'autenticazione.

ATTENZIONE: Agli amministratori si consiglia di seguire le “pratiche migliori” per limitare i privilegi dell'utente finale e limitarne l'accesso.

Agli utenti non autorizzati non devono essere concessi privilegi amministrativi.

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	Impostato nel modulo seguente	Funzione
Password di accesso di Windows	Pannello di controllo di Windows® o HP ProtectTools Security Manager	Può essere utilizzata per l'accesso manuale e per l'autenticazione di accesso a varie funzionalità di Security Manager.
Password di backup e ripristino di Security Manager	Security Manager, singolo utente	Protegge l'accesso al file di backup e ripristino di Security Manager.

Password di HP ProtectTools	Impostato nel modulo seguente	Funzione
PIN della Smart Card	Credential Manager	Può essere utilizzato come autenticazione a più fattori. Può essere utilizzato come autenticazione Windows. Autentica gli utenti di Drive Encryption se viene selezionato il token della smart card.
Password del token per il ripristino di emergenza	Embedded Security, dall'amministratore IT	Protegge l'accesso al token per il ripristino di emergenza, che è un file di backup per il chip di protezione integrato.
Password proprietario	Embedded Security, dall'amministratore IT	Protegge il sistema e il chip TPM dall'accesso non autorizzato a tutte le funzioni del proprietario di Embedded Security.
Password amministratore BIOS	Computer Setup, dall'amministratore IT	Protegge l'accesso all'utility Computer Setup.

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 come password o qualsiasi altra informazione personale quale data di nascita, nomi di animali domestici o nome da nubile della madre, anche se utilizzati al contrario.
- 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

È possibile utilizzare la funzionalità di backup e ripristino di HP ProtectTools per selezionare ed eseguire il backup di impostazioni e dati credenziali di HP ProtectTools.

2 Operazioni iniziali dell'installazione guidata

L'Installazione guidata di Security Manager assiste l'utente nell'abilitazione delle funzioni di protezione disponibili valide per tutti gli utenti del computer. È anche possibile gestire queste funzioni nella pagina delle opzioni di protezione della Console amministrativa.

Per impostare le funzioni di protezione attraverso l'Installazione guidata di Security Manager, procedere come segue:

1. Aprire HP ProtectTools Security Manager dall'icona del gadget del desktop di HP ProtectTools nella barra laterale di Windows o dall'icona nell'area di notifica situata all'estrema destra della barra delle applicazioni.

Il colore del banner dell'icona del gadget del desktop indica una delle seguenti condizioni:

- Rosso: HP ProtectTools non è stato configurato, oppure si è verificata una condizione di errore in uno dei moduli di ProtectTools.
- Giallo: controllare la pagina Applications Status (Stato applicazion) in Security Manager per apportare le modifiche necessarie alle impostazioni.
- Blu: HP ProtectTools è stato configurato e funziona correttamente.

Viene visualizzato un messaggio nella parte inferiore dell'icona del gadget per indicare una delle seguenti condizioni:

- **Imposta ora**: l'amministratore deve fare clic sull'icona del gadget per avviare la configurazione delle credenziali di autenticazione del computer tramite l'apposita procedura guidata di Security Manager.

  Tale procedura è un'applicazione indipendente.

- **Registra ora**: l'utente deve fare clic sull'icona del gadget per avviare la registrazione delle credenziali di autenticazione tramite la procedura guidata per le operazioni iniziali di Security Manager.

  La procedura guidata per le operazioni iniziali viene visualizzata nel dashboard di Security Manager.

- **Verifica ora**: fare clic sull'icona del gadget per visualizzare ulteriori dettagli nella pagina Stato delle applicazioni di protezione.

NOTA: l'icona del gadget del desktop di HP ProtectTools non è disponibile in Windows XP.

– oppure –

Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**. Nel riquadro di sinistra, fare clic su **Installazione guidata**.

2. Leggere la schermata di benvenuto, quindi fare clic su **Avanti**.

3. Eseguire la verifica dell'identità immettendo la password di Windows, quindi fare clic su **Avanti**.

   Se non è ancora stata creata una password di Windows, viene chiesto di specificarne una. La password di Windows è richiesta per proteggere l'account Windows dall'accesso di utenti non autorizzati e per utilizzare le funzionalità di HP ProtectTools Security Manager.

4. Nella pagina SpareKey, selezionare tre domande di sicurezza, immettere la risposta a ciascuna domanda, quindi fare clic su **Avanti**.

   È possibile selezionare domande diverse oppure cambiare le risposte nella pagina SpareKey in **Credential Manager** nel dashboard di Security Manager

NOTA: questa impostazione SpareKey risulta valida soltanto per l'utente amministrativo.

5. Selezionare le caselle di controllo corrispondenti alle funzioni di protezione desiderate, quindi fare clic su **Avanti**.

   Più funzioni si selezionano, più protetto sarà il computer.

NOTA: queste impostazioni risultano valide per tutti gli utenti. Durante l'Installazione guidata non verrà richiesto di registrare le credenziali di cui si sono deselezionate le caselle di controllo corrispondenti.

- **Protezione di accesso a Windows**: protegge gli account Windows richiedendo l'utilizzo di credenziali specifiche per l'accesso.
- **Drive Encryption**: protegge i dati mediante la crittografia delle unità disco rigido, che rende le informazioni illeggibili agli utenti sprovvisti dell'opportuna autorizzazione.
- **Protezione preavvio**: protegge il computer impedendo l'accesso agli utenti non autorizzati prima dell'avvio di Windows.

NOTA: la funzione Protezione preavvio non è disponibile se il BIOS non la supporta.

6. Durante l'Installazione guidata verrà chiesto di eseguire la registrazione delle credenziali.

   Se non è disponibile un lettore di impronte digitali, una smart card o una webcam, verrà richiesto di immettere la password di Windows. Dopo aver eseguito la registrazione, è possibile utilizzare qualsiasi credenziale registrata per verificare l'identità qualora sia richiesta l'autenticazione.

NOTA: la registrazione di queste credenziali risulta valida soltanto per l'utente amministrativo.

7. Nella pagina finale dell'installazione guidata, fare clic su **Fine**.

   Viene visualizzata la pagina iniziale del dashboard di Security Manager.

3 Console amministrativa HP ProtectTools Security Manager

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

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

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

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

Apertura della Console amministrativa di HP ProtectTools

Per le attività amministrative, quali l'impostazione dei criteri del sistema o la configurazione del software, aprire la console nel modo indicato di seguito:

- Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.

  Oppure

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

Utilizzo della Console amministrativa

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

▲ Per aprire la Console amministrativa di HP ProtectTools, fare clic su **Start**, **Tutti i programmi**, **HP**, quindi su **Console amministrativa di HP ProtectTools**.

– Oppure –

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

La console è composta dai seguenti componenti:

- **Home** consente di configurare le seguenti opzioni di protezione:
  - **Aumenta la protezione del sistema**
  - **Richiedi autenticazione complessa**
  - **Gestione utenti HP ProtectTools**
  - **Informazioni su come gestire HP ProtectTools in modo centralizzato**
- **Sistema**: consente di configurare le seguenti funzioni di protezione e l'autenticazione per utenti e dispositivi:
  - **Protezione**
  - **Utenti**
  - **Credenziali**
- **Applicazioni**: consente di configurare le impostazioni generali di HP ProtectTools Security Manager e delle applicazioni di Security Manager.
- **Dati**: rende disponibile un menu espandibile di collegamenti che rimandano alle applicazioni di Security Manager per la protezione dei dati.
- **Gestione centralizzata**: consente di visualizzare le schede per l'accesso a ulteriori soluzioni, aggiornamenti di prodotto e messaggi.
- **Installazione guidata**: assiste l'utente in tutte le fasi dell'impostazione di HP ProtectTools Security Manager.
- **Informazioni su**: visualizza le informazioni su HP ProtectTools Security Manager, ad esempio il numero di versione e l'informativa sul copyright.
- **Area principale**: visualizza le schermate specifiche dell'applicazione.

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

Configurazione del sistema

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

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

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

Impostazione dell'autenticazione del computer

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

Per impostare l'autenticazione del computer:

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

Criteri di accesso

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

1. Nel riquadro sinistro della Console amministrativa, fare clic su **Protezione**, quindi su **Autenticazione**.
2. Nella scheda **Criterio di accesso**, fare clic sulla freccia rivolta verso il basso, quindi selezionare una categoria di utente:
   - **Per gli amministratori di questo computer**
   - **Per gli utenti non amministratori**
3. Specificare le credenziali di autenticazione richieste per la categoria di utente selezionata.
4. Scegliere se per l'autenticazione di un utente è richiesta UNA credenziale tra quelle specificate o TUTTE le credenziali specificate.
5. Fare clic su **Applica**.

Criterio di sessione

Per definire i criteri che regolano le credenziali richieste per accedere alle applicazioni di HP ProtectTools durante una sessione di Windows:

1. Nel riquadro sinistro della Console amministrativa, fare clic su **Protezione**, quindi su **Autenticazione**.
2. Nella scheda **Criterio di sessione**, fare clic sulla freccia rivolta verso il basso, quindi selezionare una categoria di utente:
   - **Per gli amministratori di questo computer**
   - **Per gli utenti non amministratori**
3. Fare clic sulla freccia rivolta verso il basso, quindi selezionare le credenziali di autenticazione richieste per la categoria di utente selezionata:
   - **Richiedi una delle credenziali specificate**

     NOTA: la deselezione delle caselle di controllo corrispondenti a tutte le credenziali ha lo stesso effetto della selezione dell'opzione **Non richiedere l'autenticazione**.
   - **Richiedi tutte le credenziali specificate**
   - **Non richiedere l'autenticazione**: la selezione di questa opzione comporta l'eliminazione di tutte le credenziali dalla finestra.
4. Fare clic su **Applica**.

Impostazioni

1. Selezionare o deselezionare le caselle di controllo corrispondenti alle seguenti opzioni che si desidera abilitare o disabilitare:

   Consenti accesso One Step Logon: consente agli utenti del computer di ignorare l'accesso di Windows se l'autenticazione è stata eseguita a livello di BIOS o di disco crittografato.
2. Fare clic su **Applica**.

Gestione degli utenti

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

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

Per gestire gli utenti, scegliere tra le seguenti impostazioni:

- Per aggiungere utenti, fare clic su **Aggiungi**.
- Per eliminare un utente, selezionare l'utente desiderato, quindi fare clic su **Elimina**.

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

Credenziali

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

SpareKey

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

1. Selezionare la casella di controllo per abilitare l'utilizzo dell'autenticazione SpareKey per l'accesso a Windows, deselezionarla per disabilitarlo.
2. Selezionare le domande di protezione che verranno visualizzate dagli utenti durante la loro registrazione a SpareKey. È possibile specificare fino a tre domande personalizzate oppure è possibile consentire agli utenti di digitare passphrase personalizzate.
3. Fare clic su **Applica**.

Impronte digitali

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

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

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

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

- **Sensibilità**: spostare il dispositivo di scorrimento per regolare la sensibilità di scansione del lettore di impronte digitali.

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

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

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

Smart card

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

- **Impostazioni**: consente di configurare il computer affinché si blocchi in modo automatico alla rimozione di una smart card.

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

- **Amministrazione** - Selezionare una delle seguenti opzioni:

  - **Initialize the smart card** (Inizializza la smart card): prepara una smart card all'utilizzo con HP ProtectTools. Se una smart card è stata inizializzata in precedenza al di fuori di HP ProtectTools (contiene una coppia di chiavi asimmetrica e un certificato associato), non è necessario eseguire di nuovo questa operazione, a meno che si desideri inizializzarla con un certificato specifico.
  - **Change smart card PIN** (Modifica PIN smart card): consente di modificare il PIN utilizzato con la smart card.

- **Erase HP ProtectTools data only** (Cancella soltanto i dati di HP ProtectTools): consente di cancellare soltanto il certificato di HP ProtectTools creato durante l'inizializzazione della scheda. Nessun altro dato viene cancellato dalla scheda.
- **Erase all data on the smart card** (Cancella tutti i dati dalla smart card): consente di cancellare tutti i dati sulla smart card specificata. La scheda non può più essere utilizzata con HP ProtectTools o qualsiasi altra applicazione.

NOTA: le funzioni che non sono supportate dalla smart card non sono disponibili.

▲ Fare clic su **Applica**.

Viso

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

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
2. Selezionare **Credenziali**, quindi fare clic su **Viso**.
3. Spostare il dispositivo di scorrimento verso sinistra se si desidera maggior praticità, spostarlo verso destra se invece si preferisce una maggiore precisione.
   - **Praticità**: per semplificare l'accesso agli utenti registrati in situazioni marginali, spostare il dispositivo di scorrimento nella posizione **Praticità**.
   - **Bilanciamento**: se si desidera un buon compromesso tra protezione e usabilità oppure se si hanno informazioni riservate o se il computer viene utilizzato in un luogo dove possono verificarsi tentativi di accesso non autorizzati, spostare il dispositivo di scorrimento nella posizione **Bilanciamento**.
   - **Precisione**: per rendere più difficile l'accesso di un utente se le scene registrate o le condizioni di luce correnti sono al di sotto del normale, nonché rendere meno probabile una falsa accettazione, spostare il dispositivo di scorrimento nella posizione **Precisione**.
4. Fare clic su **Avanzate**, quindi configurare la funzione di protezione aggiuntiva. Per ulteriori informazioni, fare riferimento alla sezione Impostazioni utente avanzate a pagina 41.
5. Fare clic su **Applica**.

Configurazione delle applicazioni

È possibile utilizzare Impostazioni per personalizzare il comportamento delle applicazioni di HP ProtectTools Security Manager attualmente installate.

Per modificare le impostazioni delle applicazioni:

1. Nel riquadro sinistro della Console amministrativa, in **Applicazioni**, fare clic su **Impostazioni**.
2. Selezionare o deselezionare le caselle di controllo corrispondenti alle specifiche impostazioni che si desidera abilitare o disabilitare.
3. Fare clic su **Applica**.

Scheda Generale

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

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

Scheda Applicazioni

Le impostazioni visualizzate consentono di modificare il momento in cui vengono aggiunte nuove applicazioni a Security Manager. Le impostazioni minime mostrate per impostazione predefinita sono le seguenti:

- **Stato applicazioni**: consente di visualizzare lo stato per tutte le applicazioni.
- **Password Manager**: consente di attivare Password Manager per tutti gli utenti del computer.
- **Privacy Manager**: consente di attivare Privacy Manager per tutti gli utenti del computer.
- **Enable the Central Management link** (Abilita il collegamento Gestione centralizzata): consente a tutti gli utenti del computer di aggiungere applicazioni a HP ProtectTools Security Manager facendo clic su **Gestione centralizzata**.

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

Gestione centralizzata

È possibile che siano disponibili altre applicazioni per l'aggiunta di nuovi strumenti di protezione in Security Manager. L'amministratore del computer può disattivare questa funzione nella pagina Impostazioni. Nella pagina Gestione centralizzata vengono visualizzate due schede:

- **Soluzioni aziendali**: se è disponibile una connessione Internet, è possibile accedere al sito Web di DigitalPersona all'indirizzo http://www.digitalpersona.com/ per controllare la presenza di nuove applicazioni.
- **Aggiornamenti e messaggi**
  - Per richiedere informazioni su nuovi aggiornamenti e applicazioni, selezionare la casella di controllo **Invia informazioni su nuove applicazioni e aggiornamenti**.
  - Per impostare una pianificazione per gli aggiornamenti automatici, selezionare il numero di giorni.
  - Per controllare la disponibilità di aggiornamenti, fare clic su **Verifica ora**.

4 HP ProtectTools Security Manager

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

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

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

Avvio di Security Manager

Security Manager può essere aperto in uno dei seguenti modi:

- Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **HP ProtectTools Security Manager**.
- Fare doppio clic sull'icona **HP ProtectTools** nell'area di notifica situata a destra della barra delle applicazioni.
- Fare clic con il pulsante destro del mouse sull'icona **HP ProtectTools**, quindi su **Apri HP ProtectTools Security Manager**.
- Fare clic sull'icona del gadget del desktop di **HP ProtectTools**.
- Premere la combinazione di tasti di scelta rapida ctrl + tasto con il logo di Windows +h per aprire il menu **Collegamenti rapidi di Security Manager**.

  Per informazioni su come cambiare la combinazione di tasti di scelta rapida, consultare la sezione Impostazioni a pagina 36.

Utilizzo del dashboard di Security Manager

Il dashboard di Security Manager è la posizione centrale da cui si accede facilmente alle funzioni, alle applicazioni e alle impostazioni di Security Manager.

▲ Per aprire il dashboard di Security Manager, fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **HP ProtectTools Security Manager**.

Nel dashboard si possono visualizzare i seguenti componenti:

- **Scheda ID**: visualizza il nome utente di Windows e un'immagine selezionata che identifica l'account utente che ha eseguito l'accesso.
- **Applicazioni di protezione**: visualizza un menu espandibile di collegamenti per la configurazione delle seguenti categorie di protezione:
  - **Home**: consente di gestire le password, impostare le credenziali di autenticazione e verificare lo stato delle applicazioni di protezione.
  - **Stato**: consente di verificare lo stato delle applicazioni di protezione di HP ProtectTools.

NOTA: se non risultano installate sul computer, le applicazioni non vengono riportate nel seguente elenco.

- **My Logons** (Miei accessi): consente di gestire le credenziali di autenticazione con Password Manager, Credential Manager, Password, SpareKey, Smart Card e i programmi di riconoscimento del viso e delle impronte digitali.
- **My Data** (Miei dati): consente di gestire la protezione dei dati con Drive Encryption e File Sanitizer.
- **My Computer** (Mio computer): consente di gestire la protezione del computer in uso con Device Access Manager.
- **My communications** (Mie comunicazioni): consente di gestire la protezione delle comunicazioni con Privacy Manager.
- **Amministrazione** è riservata agli amministratori per l'accesso alle seguenti opzioni:
  - **Console amministrativa**: consente agli amministratori di gestire utenti e funzioni di protezione.
  - **Gestione centralizzata**: consente agli amministratori di accedere a ulteriori soluzioni, aggiornamenti di prodotto e messaggi.
- **Avanzate**: visualizza i comandi di accesso ad ulteriori funzionalità, tra cui:
  - **Preferenze**: consente di personalizzare le impostazioni di Security Manager.
  - **Backup e ripristino**: consente di eseguire il backup o il ripristino dei dati.
  - **Informazioni su**: visualizza le informazioni su HP ProtectTools Security Manager, ad esempio il numero di versione e l'informativa sul copyright.
- **Area principale**: visualizza le schermate specifiche dell'applicazione.
- **?**: visualizza la Guida in linea di Security Manager. Questa icona si trova nell'angolo superiore destro della finestra, accanto alle icone per la riduzione e l'ingrandimento.

Stato delle applicazioni di protezione

È possibile visualizzare lo stato delle applicazioni di protezione installate in due ubicazioni:

- **Gadget del desktop di HP ProtectTools**

  Il colore del banner visualizzato nella parte superiore dell'icona del gadget di HP ProtectTools cambia a seconda del complessivo stato delle applicazioni di protezione installate.

  - **Rosso**: avvertenza
  - **Giallo**: attenzione: applicazione non configurata
  - **Blu**: OK

  Viene visualizzato un messaggio nella parte inferiore dell'icona del gadget per indicare una delle seguenti condizioni:

  - **Imposta ora**: l'amministratore deve fare clic sull'icona del gadget per avviare la configurazione delle credenziali di autenticazione del computer tramite l'apposita procedura guidata di Security Manager.

    Tale procedura è un'applicazione indipendente.

  - **Registra ora**: l'utente deve fare clic sull'icona del gadget per avviare la registrazione delle credenziali di autenticazione tramite la procedura guidata per le operazioni iniziali di Security Manager.

    La procedura guidata per le operazioni iniziali viene visualizzata nel dashboard di Security Manager.

  - **Verifica ora**: fare clic sull'icona del gadget per visualizzare ulteriori dettagli nella pagina Stato delle applicazioni di protezione.

- **Pagina Stato delle applicazioni di protezione**: fare clic sulla voce **Stato** nel dashboard Security Manager per visualizzare sia lo stato complessivo delle applicazioni di protezione installate che i dettagli sullo stato di protezione di ognuna.

My Logons (Miei accessi)

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

- **Password Manager**: consente di creare e gestire i collegamenti rapidi tramite cui eseguire l'avvio e l'accesso ai siti Web e ai programmi mediante l'autenticazione della password di Windows, l'impronta digitale o una smart card.
- **Credential Manager**: consente di eseguire facilmente le operazioni di modifica della password di Windows, di registrazione delle le impronte digitali o di impostazione di una smart card.

Gli amministratori possono aggiungere ulteriori applicazioni facendo clic su **Amministrazione**, quindi su **Gestione centralizzata** nell'angolo inferiore sinistro del dashboard.

Password Manager

Accedere a Windows, ai siti Web e alle applicazioni è più semplice e sicuro quando si utilizza Password Manager. È possibile utilizzare questo programma per creare password più sicure che non richiedono di essere memorizzate o annotate, quindi accedere facilmente e velocemente con un'impronta digitale, una smart card o la password di Windows.

Password Manager offre le seguenti opzioni:

- Aggiunta, modifica o eliminazione degli accessi dalla scheda **Gestisci**.
- Utilizzo dei collegamenti rapidi per avviare il browser predefinito e accedere a qualsiasi sito Web o programma una volta impostato.
- Trascinamento della selezione per organizzare i collegamenti rapidi in categorie.
- Visualizzazione immediata delle password che rappresentano un rischio alla protezione e generazione automatica di una password sicura da utilizzare per i nuovi siti.

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

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

Per pagine Web o programmi senza accesso disponibile

Nel menu contestuale vengono visualizzate le seguenti opzioni:

- **Aggiungi [qualchedominio.com] a Password Manager**: consente di aggiungere un accesso alla schermata di accesso corrente.
- **Apri Password Manager**: avvia Password Manager.
- **Impostazioni icona**: consente di specificare quali condizioni determinano la visualizzazione dell'icona di **Password Manager**.
- **?**: visualizza la Guida in linea di Security Manager.

Per pagine Web o programmi con accesso disponibile

Nel menu contestuale vengono visualizzate le seguenti opzioni:

- **Immetti dati di accesso**: consente di immettere i dati di accesso negli appositi campi, quindi di inviare la pagina (se l'invio è stato specificato al momento della creazione dell'accesso o della sua ultima modifica).
- **Modifica accesso**: consente di modificare i dati di accesso al sito Web.
- **Aggiungi accesso**: consente di aggiungere l'accesso per un account.
- **Apri Password Manager**: avvia Password Manager.
- **?**: visualizza la Guida in linea di Security Manager.

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

Aggiunta di accessi

È possibile aggiungere facilmente un accesso a un sito Web o programma immettendo i dati di accesso una volta, dopodiché la loro immissione avverrà in modo automatico. Questi accessi possono essere riutilizzati dopo la navigazione al sito Web o al programma, altrimenti si può selezionare la voce desiderata nel menu **Accessi** affinché Password Manager esegua l'accesso automatico al sito Web o al programma.

Per aggiungere un accesso:

1. Aprire la schermata di accesso a un sito Web o programma.
2. Fare clic sulla freccia dell'icona **Password Manager**, quindi fare clic su una delle seguenti opzioni a seconda che la schermata di accesso sia relativa a un sito Web o a un programma:
   - Per un sito Web, fare clic su **Aggiungi [nome dominio] a Password Manager**.
   - Per un programma, fare clic su **Aggiungi schermata accesso a Password Manager**.
3. Immettere i dati di accesso. I campi di accesso nella schermata e i campi corrispondenti nella finestra di dialogo sono identificati con un bordo arancione in grassetto. È inoltre possibile visualizzare questa finestra di dialogo facendo clic su **Aggiungi accesso** dalla scheda Gestisci di **Password Manager**. Alcune opzioni dipendono dalle modalità di protezione associate al computer, ad esempio l'uso della combinazione dei tasti di scelta rapida ctrl + tasto del logo Windows +h, il passaggio dell'impronta digitale o l'inserimento di una smart card.
   a. Per compilare un campo di accesso con una delle opzioni preformattate, fare clic sulle frecce a destra del campo.
   b. Per visualizzare la password di accesso, fare clic su **Mostra password**.
   c. Per compilare i campi di accesso, ma non inviarli, deselezionare la casella di controllo **Invia automaticamente i dati di accesso**.
   d. Per abilitare la funzione di protezione VeriSign VIP, selezionare la casella di controllo **I want VIP security on this site** (Desidero la protezione VIP su questo sito).

      Questa opzione può essere selezionata solo per i siti in cui è disponibile la Protezione di identità VeriSign (VIP). Se supportata dal sito, è anche possibile scegliere la funzione che

consente di immettere automaticamente il codice di protezione VIP, oltre ai dati del normale metodo di autenticazione.

e. Fare clic su **OK**, quindi selezionare il metodo di autenticazione desiderato (impronte digitali, password o riconoscimento del viso), quindi eseguire l'accesso con tale metodo.

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

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

- Selezionare la casella di controllo di ciascun campo obbligatorio per l'accesso oppure deselezionarla per eventuali campi facoltativi.
- Se Password Manager non è in grado di rilevare tutti i campi di accesso, viene visualizzato un messaggio che chiede se si desidera continuare. Fare clic su **Sì**.
- Viene aperta una finestra di dialogo con i campi di accesso compilati. Fare clic sull'icona per ciascun campo e trascinarla nel campo di accesso corrispondente, quindi fare clic sul pulsante per eseguire l'accesso al sito Web.

NOTA: se per immettere i dati di accesso per un sito Web si usa la modalità manuale, si dovrà continuare a utilizzare questa modalità per gli accessi successivi allo stesso sito.

NOTA: la modalità manuale per l'immissione dei dati di accesso è disponibile solo con Internet Explorer 8.

- Fare clic su **Chiudi**.

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

Modifica degli accessi

Per modificare un accesso, procedere come segue:

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

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

   - Per compilare un campo di accesso **Nome utente** con una delle scelte preformattate, fare clic sulla freccia in giù a destra del campo.
   - Per compilare un campo di accesso **Password** con una delle scelte preformattate, fare clic sulla freccia in giù a destra del campo.
   - Per abilitare la funzione di protezione VeriSign VIP, selezionare la casella di controllo **I want VIP security on this site** (Desidero la protezione VIP su questo sito).

Questa opzione può essere selezionata solo per i siti in cui è disponibile la protezione VeriSign VIP. Se supportata dal sito, è anche possibile scegliere la funzione che consente di immettere automaticamente il codice di protezione VIP, oltre ai dati del normale metodo di autenticazione.

- Per aggiungere altri campi dalla schermata all'accesso, fare clic su **Altri campi**.
- Per visualizzare la password di accesso, fare clic su **Mostra password**.
- Per compilare i campi di accesso, ma non inviarli, deselezionare la casella di controllo **Invia automaticamente i dati di accesso**.

4. Fare clic su **OK**.

Utilizzo del menu Accessi

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

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

Per visualizzare il menu **Accessi**:

1. Premere la combinazione di tasti di scelta rapida per **Password Manager** (ctrl + tasto del logo Windows +h è la combinazione predefinita). Per cambiare la combinazione di tasti, nel dashboard di Security Manager fare clic su **Password Manager**, quindi su **Impostazioni**.
2. Passare il dito (sui computer con un lettore di impronte digitali integrato o collegato) oppure immettere la password Windows.

Organizzazione degli accessi in categorie

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

Per aggiungere una categoria:

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

Per aggiungere un accesso a una categoria:

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

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

Gestione degli accessi

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

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

Per gestire gli accessi:

▲ Dal dashboard di Security Manager, fare clic su **Password Manager**, quindi selezionare la scheda **Gestisci**.

- **Aggiungi ad accesso**: fare clic su **Aggiungi accesso** e seguire le istruzioni visualizzate.
- **Accessi personali**: fare clic su un accesso esistente, selezionare una delle seguenti opzioni, quindi seguire le istruzioni visualizzate:
  - **Apri**: apre un sito Web o un programma al quale è già associato un accesso.
  - **Aggiungi**: aggiunge un accesso. Per ulteriori informazioni, fare riferimento alla sezione Aggiunta di accessi a pagina 31.
  - **Modifica**: modifica un accesso. Per ulteriori informazioni, fare riferimento alla sezione Modifica degli accessi a pagina 32.
  - **Elimina**: elimina un sito Web o un programma al quale è già associato un accesso.
- **Aggiungi categoria**: fare clic su **Aggiungi categoria**, quindi seguire le istruzioni visualizzate. Per ulteriori informazioni, fare riferimento alla sezione Organizzazione degli accessi in categorie a pagina 33.

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

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

Verifica della complessità della password

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

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

Impostazioni dell'icona di Gestore password

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

1. Fare clic sulla freccia dell'icona, quindi fare clic su **Impostazioni icona** per personalizzare il modo in cui Password Manager gestisce i possibili siti di accesso.

   - **Richiedi l'aggiunta di accessi per le schermate di accesso**: fare clic su questa opzione se si desidera che Password Manager richieda di aggiungere una voce quando viene visualizzata una schermata per la quale non è stato ancora configurato un accesso.

   - **Escludi questa schermata**: selezionare questa casella di controllo se non si desidera che Password Manager richieda di nuovo di aggiungere un accesso per questa schermata.

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

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

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

       Viene visualizzata la schermata Aggiungi accesso a Password Manager.
     - Seguire le istruzioni visualizzate. Per ulteriori informazioni, fare riferimento alla sezione Aggiunta di accessi a pagina 31.
     - Ogni volta che si apre la schermata di accesso al sito Web o del programma, si visualizza l'icona di **Password Manager**.

2. Per disabilitare la richiesta di aggiunta di accessi per le schermate, selezionare questa casella di opzione.

3. Per accedere alle altre impostazioni di Password Manager, fare clic su **Password Manager**, quindi su **Impostazioni** nel dashboard di Security Manager.

Protezione di identità VeriSign (VIP)

È possibile creare token di accesso da usare con i siti Web per i quali è abilitata la funzione di protezione VeriSign VIP. Si tratta di token utilizzati da Password Manager per creare accessi automatizzati con l'uso incorporato di token trascinati e rilasciati nelle schermate di accesso abilitate alla funzione VIP oppure immessi manualmente nei campi specificati.

Si può abilitare la funzione VeriSign VIP e creare un token dal dashboard di Security Manager oppure in qualsiasi sito Web in cui è abilitata tale funzione. Per utilizzare il token, occorre eseguire la registrazione su ciascun sito Web in cui sarà usato.

Dopo la registrazione e aver usato il token la prima volta, può essere facoltativamente accodato alle normali credenziali di accesso e inviato insieme a tali dati. Per i siti che non consentono

l'accodamento del token, è possibile trascinare e rilasciare i dati del token oppure immetterli manualmente.

Per abilitare la funzione VeriSign VIP e creare un token dal dashboard di Security Manager, procedere come segue:

1. Aprire il dashboard di Security Manager. Per ulteriori informazioni, fare riferimento alla sezione Avvio di Security Manager a pagina 27.
2. Fare clic su **Password Manager**, quindi su clic su **VIP**.
3. Fare clic su **Scarica VIP**.

   Un token VeriSign VIP viene creato e visualizzato nella pagina VeriSign VIP. Il token verrà d'ora in poi visualizzato ad ogni accesso a questa pagina.

Per abilitare la funzione VeriSign VIP e creare un token da un sito Web, procedere come segue:

1. Password Manager invia un avviso ogni volta che si visita un sito Web in cui è abilitata la funzione VeriSign VIP.
2. Creare un accesso per questa schermata. Per ulteriori informazioni, fare riferimento alla sezione Aggiunta di accessi a pagina 31.
3. Nella finestra di dialogo Crea accesso selezionare **I want additional account protection with VIP** (Desidero ulteriore protezione sull'account con VIP).

Per eseguire la registrazione di un token VeriSign VIP per un sito Web, procedere come segue:

1. Eseguire l'accesso manuale oppure tramite Password Manager a un sito Web in cui è abilitata la funzione VeriSign VIP.
2. Fare clic sul fumetto VeriSign VIP visualizzato per creare un accesso per il sito.
3. Nella finestra di dialogo Aggiungi accesso a Password Manager selezionare **I want VIP security on this site** (Desidero la protezione VIP su questo sito).

   Questa opzione può essere selezionata solo per i siti in cui è disponibile la protezione VeriSign VIP. Se supportata dal sito, è anche possibile scegliere la funzione che consente di immettere automaticamente il codice di protezione VIP, oltre ai dati del normale metodo di autenticazione.

Impostazioni

È possibile specificare le impostazioni per la personalizzazione di HP ProtectTools Security Manager:

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

Credential Manager

È possibile utilizzare le credenziali di Security Manager per verificare l'identità dell'utente. L'amministratore del computer in uso può impostare le credenziali da utilizzare per verificare l'identità durante l'accesso all'account Windows, ai siti Web o ai programmi.

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

- password
- SpareKey
- impronte digitali
- smart card
- viso

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

Modifica della password di Windows

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

Per modificare la password di Windows, procedere come segue:

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

Impostazione della SpareKey

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

HP ProtectTools Security Manager richiede di configurare la SpareKey personale durante l'installazione iniziale della procedura guidata per le operazioni iniziali.

Per configurare la SpareKey, procedere come segue:

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

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

Una volta configurata la SpareKey, è possibile accedere al computer utilizzando la SpareKey dalla schermata di accesso Pre-Boot oppure dalla schermata di benvenuto di Windows.

Registrazione delle impronte digitali

Se il computer in uso ha un lettore di impronte digitali integrato o collegato, HP ProtectTools Security Manager richiede di configurare oppure "registrare" le impronte digitali durante l'installazione iniziale della procedura guidata per le operazioni iniziali. È anche possibile registrare le impronte digitali nell'apposita pagina di **Credential Manager** nel dashboard di Security Manager.

1. Viene visualizzata una sagoma con due mani. Le dita che sono state già registrate sono evidenziate in verde. Fare clic su un dito della sagoma.

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

2. Una volta selezionato un dito da registrare, viene richiesto di eseguirne la scansione finché l'impronta digitale corrispondente non risulta registrata correttamente. Un dito registrato viene evidenziato in verde nella sagoma.

3. È necessario registrare almeno due dita, preferibilmente l'indice o il medio. Ripetere i passaggi 1 e 2 per un altro dito.

4. Fare clic su **Avanti**, quindi seguire le istruzioni visualizzate.

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

Configurazione di una smart card

Gli amministratori devono inizializzare e registrare la smart card prima di poterla utilizzare per l'autenticazione.

Inizializzazione della smart card

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

NOTA: il software ActivIdentity deve essere installato.

1. Inserire la scheda nel lettore.

2. Fare clic su **Start**, **Tutti i programmi**, quindi su **ActivClient PIN Initialization Tool** (Strumento di inizializzazione del PIN ActivClient).

3. Immettere e confermare un PIN.

4. Fare clic su **Avanti**.

   Il software della smart card include un codice di sblocco. Dopo il quinto tentativo, la maggior parte delle smart card verrà automaticamente bloccata se si immette il PIN errato. Il codice viene utilizzato per sbloccare la carta.

5. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
6. Fare clic su **Credenziali**, quindi su **Smart Card**.
7. Fare clic sulla scheda **Amministrazione**.
8. Controllare che sia selezionata l'opzione **Configura smart smart**.
9. Immettere il PIN, fare clic su **Applica**, quindi seguire le istruzioni visualizzate.
10. Dopo aver inizializzato la smart card, è necessario eseguirne la registrazione.

Registrazione della smart card

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

1. In **Gestione centralizzata**, fare clic su **Impostazione guidata**.
2. Nella pagina iniziale, fare clic su **Avanti**, quindi immettere la password di Windows.
3. Nella pagina SpareKey, fare clic su **Skip SpareKey Setup** (Ignora impostazione SpareKey), a meno che non si desideri aggiornare le informazioni relative a SpareKey.
4. Nella pagina Attiva funzioni di protezione, fare clic su **Avanti**.
5. Nella pagina di scelta delle credenziali, verificare che sia selezionata l'opzione **Configura smart card**, quindi fare clic su **Avanti**.
6. Nella pagina Smart card, immettere il PIN, quindi fare clic su **Avanti**.
7. Fare clic su **Fine**.

Gli utenti possono anche registrare la smart card in Security Manager. Per ulteriori informazioni, vedere la Guida del software HP ProtectTools Security Manager.

Configurazione della smart card

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

- **Impostazioni**: consente di configurare il computer affinché si blocchi in modo automatico alla rimozione di una smart card.

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

- **Amministrazione** - Selezionare una delle seguenti opzioni:
  - **Initialize the smart card** (Inizializza la smart card): prepara una smart card all'utilizzo con HP ProtectTools. Se una smart card è stata inizializzata in precedenza al di fuori di HP ProtectTools (contiene una coppia di chiavi asimmetrica e un certificato associato), non è necessario eseguire di nuovo questa operazione, a meno che si desideri inizializzarla con un certificato specifico.
  - **Change smart card PIN** (Modifica PIN smart card): consente di modificare il PIN utilizzato con la smart card.

- **Erase HP ProtectTools data only** (Cancella soltanto i dati di HP ProtectTools): consente di cancellare soltanto il certificato di HP ProtectTools creato durante l'inizializzazione della scheda. Nessun altro dato viene cancellato dalla scheda.
- **Erase all data on the smart card** (Cancella tutti i dati dalla smart card): consente di cancellare tutti i dati sulla smart card specificata. La scheda non può più essere utilizzata con HP ProtectTools o qualsiasi altra applicazione.

NOTA: le funzioni che non sono supportate dalla smart card non sono disponibili.

▲ Fare clic su **Applica**.

Registrazione di scene per l'accesso tramite riconoscimento del viso

Se il computer in uso ha una webcam integrata o collegata, HP ProtectTools Security Manager richiede di configurare oppure "registrare" le scene durante l'installazione iniziale della procedura guidata per le operazioni iniziali. È anche possibile registrare le scene nell'apposita pagina per l'accesso tramite il riconoscimento del viso presente in **Credential Manager** nel dashboard di Security Manager.

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

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

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

Per registrare una scena dalla procedura guidata per le operazioni iniziali, procedere come segue:

1. Nella pagina relativa ai dati sul viso della procedura guidata, fare clic su **Avanzate**, quindi configurare la funzione di protezione aggiuntiva. Per ulteriori informazioni, fare riferimento alla sezione Impostazioni utente avanzate a pagina 41.
2. Fare clic su **OK**.
3. Fare clic su **Avvia**, altrimenti se sono già state registrate delle scene, fare clic su **Registra una nuova scena**.
4. Se non è stata selezionata alcuna opzione aggiuntiva per la protezione, viene richiesto di selezionarne una. Seguire le istruzioni visualizzate, quindi fare clic su **Avanti**. Per ulteriori informazioni, fare riferimento alla sezione Impostazioni utente avanzate a pagina 41.
5. Fare clic sull'icona **Camera** (Fotocamera), quindi seguire le istruzioni visualizzate per registrare la scena.

   Seguire le istruzioni visualizzate e non distogliere gli occhi dalla propria immagine durante l'acquisizione delle scene.
6. Fare clic su **Avanti**.
7. Fare clic su **Fine**.

È anche possibile registrare le scene dal dashboard di Security Manager:

1. Aprire il dashboard di Security Manager. Per ulteriori informazioni, fare riferimento alla sezione Avvio di Security Manager a pagina 27.
2. In **My Logons** (Miei accessi) fare clic su **Credential Manager**, quindi su **Face** (Viso).
3. Fare clic su **Avanzate**, quindi configurare la funzione di protezione aggiuntiva. Per ulteriori informazioni, fare riferimento alla sezione Impostazioni utente avanzate a pagina 41.
4. Fare clic su **OK**.
5. Fare clic su **Avvia**, altrimenti se sono già state registrate delle scene, fare clic su **Registra una nuova scena**.
6. Se non è stata selezionata alcuna opzione aggiuntiva per la protezione, viene richiesto di selezionarne una. Seguire le istruzioni visualizzate, quindi fare clic su **Avanti**. Per ulteriori informazioni, fare riferimento alla sezione Impostazioni utente avanzate a pagina 41.
7. Fare clic sull'icona **Camera** (Fotocamera), quindi seguire le istruzioni visualizzate per registrare la scena.

   Seguire le istruzioni visualizzate e non distogliere gli occhi dalla propria immagine durante l'acquisizione delle scene.

Per ulteriori informazioni consultare la guida del software per il riconoscimento del viso, facendo clic sull'icona **?** blu presente nella parte superiore destra della pagina per l'accesso tramite riconoscimento del viso.

Impostazioni utente avanzate

Se non è stata selezionata alcuna opzione di protezione aggiuntiva, queste opzioni vengono visualizzate anche nell'opportuna pagina.

1. Aprire il dashboard di Security Manager. Per ulteriori informazioni, fare riferimento alla sezione Avvio di Security Manager a pagina 27.
2. In **My Logons** (Miei accessi) fare clic su **Credential Manager**, quindi su **Face** (Viso).
3. Fare clic su **Avanzate** per configurare le seguenti opzioni di protezione:

   a. Nella scheda **Protezione** selezionare una delle seguenti opzioni:

   - **No additional security** (Nessuna protezione aggiuntiva): selezionare questa opzione se non si desidera aggiungere ulteriore protezione per l'accesso tramite riconoscimento del viso.
   - **Use PIN for additional security** (Usa PIN per protezione aggiuntiva): selezionare questa opzione per l'immissione obbligatoria di un PIN specificato quando si esegue l'accesso tramite riconoscimento del viso.
     - Fare clic su **Crea PIN**.
     - Immettere la password di Windows.
     - Immettere il nuovo PIN, quindi digitarlo nuovamente per confermarlo.

Una volta creato il PIN, è possibile scegliere tra le seguenti opzioni: **Modifica**, **Reimposta** oppure **Rimuovi PIN**.

- **Use Bluetooth for additional security** (Usa Bluetooth per protezione aggiuntiva): selezionare questa opzione per abbinare il telefono con tecnologia Bluetooth alla funzione di riconoscimento del viso. Durante l'accesso a Windows e successivamente all'avvenuta autenticazione del riconoscimento, questa funzione verifica anche l'eventuale abbinamento di un telefono Bluetooth. Se il telefono risulta presente e la tecnologia Bluetooth abilitata, è consentito l'accesso a Windows.

  - Verificare che Bluetooth sia abilitato sul computer e sul telefono.

    Se non è presente, viene richiesto di abilitare il telefono con tecnologia Bluetooth abbinato e di riavviare la procedura di accesso. Dopo 30 secondi, la finestra per l'accesso tramite riconoscimento del viso viene messa in pausa. Per iniziare la procedura di accesso, fare clic sull'icona **Camera**. Se non è presente un telefono con tecnologia Bluetooth abilitata, è possibile usare la normale password di Windows per completare l'accesso.

  - Fare clic su **Aggiungi**.

  - Quando viene visualizzato il dispositivo Bluetooth, selezionarlo, quindi fare clic su **Avanti**.

Fare clic su **OK**.

b. Nella scheda **Altre impostazioni** selezionare o deselezionare le caselle di controllo corrispondenti alle opzioni che si desidera abilitare o disabilitare. Queste impostazioni risultano valide solo per l'utente corrente.

- **Riproduci un suono in corrispondenza di eventi di riconoscimento del viso**: viene riprodotto un suono quando il riconoscimento del viso viene completato, sia con esito positivo che negativo.

- **Richiedi l'aggiornamento delle scene quando l'accesso non riesce**: se l'accesso tramite il riconoscimento del viso ha esito negativo ma la password viene digitata correttamente, può essere richiesto di salvare una serie di immagini per aumentare le probabilità di accesso tramite riconoscimento del viso la volta successiva.

- **Richiedi la registrazione di una nuova scena quando l'accesso non riesce**: se l'accesso tramite il riconoscimento del viso ha esito negativo ma la password viene digitata correttamente, talvolta si richiede di registrare una nuova scena che possa eventualmente consentire un corretto accesso in futuro.

Fare clic su **OK**.

Scheda ID personale

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

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

Per modificare il nome visualizzato:

1. Aprire il dashboard di Security Manager. Per ulteriori informazioni, fare riferimento alla sezione Avvio di Security Manager a pagina 27.
2. Fare clic sulla scheda ID nell'angolo superiore sinistro del dashboard.
3. Fare clic nella casella che visualizza il nome utente Windows per l'account in uso, digitare il nuovo nome quindi fare clic su **Salva**.

Per modificare l'immagine visualizzata:

1. Aprire il dashboard di Security Manager. Per ulteriori informazioni, fare riferimento alla sezione Avvio di Security Manager a pagina 27.
2. Fare clic sulla scheda ID nell'angolo superiore sinistro del dashboard.
3. Fare clic su **Scegli immagine**, quindi sull'immagine desiderata e infine su **Salva**.

Impostazione delle preferenze

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

Scheda Generale

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

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

Scheda Impronta digitale

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

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

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

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

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

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

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

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

Backup e ripristino dei dati

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

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

NOTA: con questa funzione, viene eseguito il backup soltanto dei dati.

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

Per eseguire il backup dei dati:

1. Aprire il dashboard di Security Manager. Per ulteriori informazioni, fare riferimento alla sezione Avvio di Security Manager a pagina 27.
2. Nel riquadro sinistro del dashboard, fare clic su **Avanzate**, quindi su **Backup e ripristino**.
3. Fare clic su **Backup dei dati**.
4. Selezionare i moduli da includere nel backup. In genere, si selezionano tutti i moduli.
5. Verificare l'identità.
6. Inserire un nome per il file di archiviazione. Per impostazione predefinita, il file viene salvato nella cartella Documenti. Fare clic su **Sfoglia** per specificare un'altra cartella.
7. Immettere una password per proteggere il file.
8. Fare clic su **Fine**.

Per ripristinare i dati:

1. Aprire il dashboard di Security Manager. Per ulteriori informazioni, fare riferimento alla sezione Avvio di Security Manager a pagina 27.
2. Nel riquadro sinistro del dashboard, fare clic su **Avanzate**, quindi su **Backup e ripristino**.
3. Fare clic su **Ripristina dati**.
4. Selezionare il file di archiviazione creato in precedenza. Specificare il percorso nell'apposito campo oppure fare clic su **Sfoglia**.
5. Immettere la password utilizzata per proteggere il file.
6. Selezionare i moduli di cui ripristinare i dati. In genere, si selezionano tutti i moduli riportati in elenco.
7. Verificare la password di Windows.
8. Fare clic su **Fine**.

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

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

L'impostazione guidata di HP ProtectTools Security Manager consente agli amministratori di Windows di attivare Drive Encryption, eseguire il backup della chiave di crittografia, selezionare o deselezionare le unità. Per ulteriori informazioni, vedere la Guida del software HP ProtectTools Security Manager.

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

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

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

- Creazione di chiavi di backup
- Ripristino di una chiave di Drive Encryption
- Abilitazione dell'autenticazione di preavvio di Drive Encryption mediante una password, un'impronta digitale registrata o il PIN di una smart card

Apertura di Drive Encryption

Gli amministratori possono accedere a Drive Encryption dalla Console amministrativa di HP ProtectTools.

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro di sinistra, fare clic su **Drive Encryption**.

Attività generali

Attivazione di Drive Encryption per le unità disco rigido standard

La crittografia delle unità disco rigido standard viene eseguita tramite software. Attenersi ai passaggi riportati di seguito per attivare Drive Encryption:

1. Utilizzare l'installazione guidata di HP ProtectTools Security Manager per attivare Drive Encryption.
2. Seguire le istruzioni visualizzate fino alla pagina **Attiva funzione di protezione**, quindi continuare con il passaggio 4 riportato di seguito.

– Oppure –

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra di **Protezione** per visualizzare le opzioni disponibili.
3. Fare clic su **Caratteristiche**.
4. Selezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.

NOTA: se non si seleziona alcuna unità disco rigido per la crittografia, l'autenticazione di preavvio di Drive Encryption viene attivata, ma le unità non vengono crittografate.

5. In **Unità da crittografare**, selezionare la casella di controllo corrispondente all'unità disco rigido che si desidera crittografare, quindi fare clic su **Avanti**.
6. Per eseguire il backup della chiave di crittografia, inserire il dispositivo di archiviazione nello slot appropriato.

NOTA: per salvare la chiave di crittografia, è necessario utilizzare un dispositivo di archiviazione USB formattato FAT32. Per il backup è possibile utilizzare dischi floppy, unità di archiviazione USB, Secure Digital (SD) Memory Card o MMC.

7. In **Back up Drive Encryption keys** (Backup delle chiavi di Drive Encryption), selezionare la casella di controllo corrispondente al dispositivo di archiviazione in cui salvare la chiave.
8. Fare clic su **Avanti**.

NOTA: il computer verrà riavviato.

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

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

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

Le unità che supportano la crittografia automatica conformi alle specifiche OPAL del Trusted Computing Group relative alla gestione delle unità SED possono essere crittografate tramite

crittografia basata sul software e sull'hardware. Attenersi ai passaggi riportati di seguito per attivare le unità che supportano la crittografia automatica:

1. Utilizzare l'installazione guidata di HP ProtectTools Security Manager per attivare Drive Encryption.
2. Seguire le istruzioni visualizzate fino alla pagina **Attiva funzione di protezione**, quindi continuare con il passaggio 4 riportato nella sezione "Crittografia basata sul software" o "Crittografia basata sull'hardware" riportata di seguito.

NOTA: se il computer non dispone di un'unità che supporta la crittografia automatica conforme alle specifiche OPAL del Trusted Computing Group relative alla gestione delle unità SED, l'opzione della crittografia basata sull'hardware non è disponibile, e la crittografia basata sul software viene utilizzata per impostazione predefinita.

Se il computer include sia unità che supportano la crittografia automatica che unità standard, l'opzione della crittografia basata sull'hardware non è disponibile e la crittografia basata sul software viene utilizzata per impostazione predefinita.

– Oppure –

Crittografia basata sul software

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra di **Protezione** per visualizzare le opzioni disponibili.
3. Fare clic su **Caratteristiche**.
4. Selezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.
5. In **Unità da crittografare**, selezionare la casella di controllo corrispondente all'unità disco rigido che si desidera crittografare, quindi fare clic su **Avanti**.
6. Per eseguire il backup della chiave di crittografia, inserire il dispositivo di archiviazione nello slot appropriato.

   NOTA: per salvare la chiave di crittografia, è necessario utilizzare un dispositivo di archiviazione USB formattato FAT32. Per il backup è possibile utilizzare dischi floppy, unità di archiviazione USB, Secure Digital (SD) Memory Card o MMC.

7. In **Back up Drive Encryption keys** (Backup delle chiavi di Drive Encryption), selezionare la casella di controllo corrispondente al dispositivo di archiviazione in cui salvare la chiave.
8. Fare clic su **Applica**.

   NOTA: il computer verrà riavviato.

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

Crittografia basata sull'hardware

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra di **Protezione** per visualizzare le opzioni disponibili.
3. Fare clic su **Caratteristiche**.
4. Selezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.

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

Se vengono mostrate più unità, le caselle di controllo corrispondenti vengono automaticamente selezionate ma non disattivate.

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

5. Verificare che la casella di controllo **Use hardware drive encryption** (Usa crittografia unità basata sull'hardware) sia selezionata nella parte inferiore della schermata.
6. In **Unità da crittografare**, selezionare la casella di controllo corrispondente all'unità disco rigido che si desidera crittografare, quindi fare clic su **Avanti**.
7. Per eseguire il backup della chiave di crittografia, inserire il dispositivo di archiviazione nello slot appropriato.

NOTA: per salvare la chiave di crittografia, è necessario utilizzare un dispositivo di archiviazione USB formattato FAT32. Per il backup è possibile utilizzare dischi floppy, unità di archiviazione USB, Secure Digital (SD) Memory Card o MMC.

8. In **Back up Drive Encryption keys** (Backup delle chiavi di Drive Encryption), selezionare la casella di controllo corrispondente al dispositivo di archiviazione in cui salvare la chiave.
9. Fare clic su **Applica**.

NOTA: sarà necessario riavviare il computer.

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

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

Disattivazione di Drive Encryption

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

- Seguire le istruzioni visualizzate fino alla pagina **Attiva funzione di protezione**, quindi continuare con il passaggio 4 riportato di seguito.

Oppure

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra di **Protezione** per visualizzare le opzioni disponibili.
3. Fare clic su **Caratteristiche**.
4. Deselezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.

   Viene avviata la disattivazione Drive Encryption.

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

Se viene utilizzata la crittografia basata sull'hardware, viene immediatamente avviata la decrittografia dell'unità e, dopo alcuni minuti, viene disattivato Drive Encryption.

Una volta disattivata l'unità, il computer dovrà essere riavviata.

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: in uno scenario di crittografia basata sull'hardware, assicurarsi che il computer sia spento. Se il computer non viene spento e riavviato, non viene visualizzata la schermata di autenticazione di preavvio di Drive Encryption.

NOTA: durante la disattivazione delle modalità di sospensione o standby, l'autenticazione di preavvio di Drive Encryption non viene visualizzata per la crittografia basata sul software o sull'hardware, tranne se è disabilitata.

Durante la disattivazione della modalità di ibernazione, viene visualizzata l'autenticazione di preavvio di Drive Encryption.

NOTA: se l'amministratore Windows ha abilitato la protezione di preavvio in HP ProtectTools Security Manager, è possibile accedere al computer immediatamente dopo la sua accensione anziché alla visualizzazione della schermata di accesso di Drive Encryption.

1. Fare clic sul proprio nome utente e immettere la password di Windows oppure il PIN della smart card o ancora passare il dito registrato.

NOTA: sono supportate le seguenti smart card:

Smart card

- ActivIdentity 64K V2C Smart Card
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB key V3.0 ZFG-48001-A

Lettori PCMCIA

- Lettore interno Express Card 54 SCR3340
- SCR 201
- SCR 243 (anche con marchio HP)
- ActivCard
- Omnikey 4040
- Cisco

Lettori USB

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- Terminale HP Smart Card

2. Fare clic su **OK**.

NOTA: se si utilizza una chiave di ripristino per accedere alla schermata di accesso di Drive Encryption, viene richiesto di eseguire l'autenticazione con la password, il PIN della smart card o un dito registrato nella schermata di accesso di Windows.

Protezione dei dati tramite la crittografia dell'unità disco rigido

Si consiglia di utilizzare l'installazione guidata di HP ProtectTools Security Manager per proteggere i dati mediante la crittografia dell'unità disco rigido:

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

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

– Oppure –

- ▲ Per le unità crittografate tramite hardware, selezionare le unità desiderate. È necessario selezionare almeno un'unità.

Visualizzazione dello stato di crittografia

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

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

1. Aprire HP ProtectTools Security Manager.
2. In **Dati personali**, fare clic su **Drive Encryption**.

   In uno scenario di crittografia basata sul software, in **Stato unità** viene visualizzata una delle seguenti indicazioni:

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

   In uno scenario di crittografia basata sull'hardware, in **Stato unità** viene visualizzata la seguente indicazione:

   - Crittografata

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

Attività avanzate

Gestione di Drive Encryption (attività dell'amministratore)

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

NOTA: la crittografia basata sull'hardware non può essere modificata nella pagina Impostazioni.

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

Crittografia basata sul software

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

Crittografia basata sull'hardware

- Crittografata

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

Gli amministratori possono utilizzare la pagina Impostazioni per crittografare una o più unità disco rigido presenti nel computer o per decrittografare un'unità che è già stata crittografata.

1. Aprire la Console amministrativa di HP ProtectTools.
2. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra della voce **Drive Encryption** per visualizzare le opzioni disponibili.
3. Fare clic su **Impostazioni**.
4. In **Stato unità**, selezionare o deselezionare la casella di controllo corrispondente a ogni unità disco rigido che si desidera crittografare o decrittografare, quindi fare clic su **Applica**.

NOTA: Durante la crittografia o decrittografia dell'unità disco rigido, una barra di avanzamento visualizza il tempo rimanente alla fine del processo.

Se si spegne il computer o si inizializza la modalità di sospensione/standby o di ibernazione, quindi si riavvia il computer, il tempo rimanente indicato nella barra di avanzamento viene azzerato, ma il processo di crittografia effettivo viene ripreso dal punto in cui era stato interrotto. La barra di avanzamento, che viene mostrato come valore percentuale, e il tempo rimanente cambiano più rapidamente per riflettere l'avanzamento precedente.

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

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

Backup e ripristino (attività dell'amministratore)

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

Backup delle chiavi di crittografia

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

ATTENZIONE: conservare il dispositivo di archiviazione contenente la chiave di backup in un luogo sicuro, perché, se si dimentica la password, se si perde la smart card o se non si è effettuata la registrazione di un dito, questo dispositivo è l'unico modo per poter accedere all'unità disco rigido.

1. Aprire la Console amministrativa di HP ProtectTools.
2. Nel riquadro sinistro, fare clic sull'icona **+** a sinistra della voce **Drive Encryption** per visualizzare le opzioni disponibili.
3. Fare clic su **Encryption Key Backup** (Backup chiave di crittografia).

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

Ripristino delle chiavi di crittografia

Gli amministratori possono ripristinare una chiave di crittografia dal dispositivo di archiviazione rimovibile su cui era stata precedentemente salvata:

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 **Opzioni**.
4. Fare clic su **Ripristino**.
5. Selezionare il file contenente la chiave di backup oppure fare clic su **Sfoglia** per cercarlo, quindi fare clic su **Avanti**.
6. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **OK**.

   Viene avviato il computer.

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

6 Privacy Manager for HP ProtectTools (solo in determinati modelli)

Privacy Manager for HP ProtectTools consente di utilizzare avanzati metodi di accesso protetti (autenticazione) per verificare l'origine, l'integrità e la sicurezza delle comunicazioni durante l'utilizzo della posta elettronica o di documenti Microsoft® Office.

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

- Autenticazione delle impronte digitali
- Password di Windows®
- Smart card
- Face recognition

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

Apertura di Privacy Manager

Per aprire Privacy Manager, procedere come segue:

- Per accedere alle funzioni specifiche di Outlook in Microsoft Outlook, fare clic su **Invia in modo protetto** nel gruppo **Privacy** della scheda **Messaggio**.
- Per accedere alla maggior parte delle funzioni dei documenti Microsoft Office, fare clic su **Firma e crittografa** nel gruppo **Privacy** della scheda **Home**.
- Per accedere a funzionalità aggiuntive, aprire il dashboard di HP ProtectTools Security Manager.
    - Fare clic su **Start**, **Tutti i programmi**, **HP**, **HP ProtectTools Security Manager**, quindi su **Privacy Manager**.

      – Oppure –
    - Fare clic sull'icona del gadget del desktop di **HP ProtectTools**.

      – Oppure –
    - Fare clic con il pulsante destro del mouse sull'icona **HP ProtectTools** nell'area di notifica nella parte destra della barra delle applicazioni, quindi selezionare **Privacy Manager** e **Configurazione**.

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.

Gestione certificati consente di eseguire le seguenti attività:

- Richiesta di un certificato di Privacy Manager a pagina 56
- Acquisizione di un certificato aziendale di Privacy Manager preassegnato a pagina 57
- Impostazione di un certificato di Privacy Manager predefinito a pagina 58
- Importazione di un certificato di terze parti a pagina 57
- Visualizzazione dei dettagli del certificato di Privacy Manager a pagina 58
- Rinnovo di un certificato di Privacy Manager a pagina 58
- Impostazione di un certificato di Privacy Manager predefinito a pagina 58
- Eliminazione di un certificato di Privacy Manager a pagina 59
- Ripristino di un certificato di Privacy Manager a pagina 59
- Revoca del certificato di Privacy Manager a pagina 59

Richiesta di un certificato di Privacy Manager

Prima di poter utilizzare le funzionalità di Privacy Manager, è necessario richiedere e installare un certificato di Privacy Manager dall'interno dell'applicazione utilizzando un indirizzo e-mail valido. L'indirizzo e-mail deve essere impostato come account Microsoft Outlook sullo stesso computer da cui si richiede il certificato.

1. Aprire Privacy Manager, quindi fare clic su **Certificati**.
2. Selezionare **Richiedi un certificato di Privacy Manager**.
3. Leggere la schermata di benvenuto, quindi fare clic su **Avanti**.
4. Leggere il contratto di licenza che viene visualizzato.
5. Verificare che la casella di controllo accanto alla voce **Check here to accept the terms of this license agreement** (Indicare l'accettazione delle condizioni della presente licenza), quindi fare clic su **Avanti**.
6. Nella pagina Dettagli del certificato, immettere le informazioni richieste, quindi fare clic su **Avanti**.
7. Nella pagina Richiesta di certificato accettata, fare clic su **Fine**.

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

Acquisizione di un certificato aziendale di Privacy Manager preassegnato

1. In Outlook, aprire l'e-mail in cui viene comunicata l'avvenuta preassegnazione di un certificato aziendale.
2. Fare clic su **Ottieni**.

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

Per installare il certificato, fare riferimento alla sezione Impostazione di un certificato di Privacy Manager a pagina 57.

Impostazione di un certificato di Privacy Manager

1. Nell'e-mail con il certificato di Privacy Manager allegato, fare clic sul pulsante **Installa**, che in Outlook 2007 e Outlook 2010 si trova in basso a destra del messaggio, mentre in Outlook 2003 si trova in alto a sinistra.
2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
3. Nella pagina Certificato installato, fare clic su **Avanti**.
4. Nella pagina Backup certificato, immettere un nome e un 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 la procedura di invito dei contatti attendibili, seguire le istruzioni visualizzate a partire dal passo 2 dell'argomento Aggiunta di contatti attendibili mediante i contatti di Microsoft Outlook a pagina 61.

   – Oppure –

   Se si fa clic su **Annulla**, fare riferimento alla sezione Gestione dei contatti attendibili a pagina 60 per informazioni sull'aggiunta di un contatto attendibile in un secondo momento.

Importazione di un certificato di terze parti

Un certificato di terze parti può essere importato in Privacy Manager attraverso l'apposita procedura guidata.

Per utilizzare questa funzione, è necessario che l'impostazione **Consenti l'utilizzo di certificati di terze parti** nella Console amministrativa di HP ProtectTools sia stata abilitata nella pagina Impostazioni di **Privacy Manager**.

1. Aprire Privacy Manager, quindi fare clic su **Certificati**.
2. Selezionare la scheda **Gestione certificati**, quindi fare clic su **Import certificates** (Importa certificati).

   Questo pulsante non viene visualizzato se non è consentita l'importazione dei certificati.

3. Scegliere se importare un certificato già installato nel computer o un certificato archiviato come file PFX (Personal Information Exchange/PKCS#12), quindi fare clic su **Avanti**.

   - Per importare un certificato installato nel computer, selezionare il certificato desiderato, quindi fare clic su **Avanti**.
   - Per selezionare un certificato PFX, fare clic su **Sfoglia**, individuare la posizione del file PFX, quindi fare clic su **Avanti**. Digitare la password del file PFX, quindi fare clic su **Avanti**.

4. Al termine della procedura d'importazione, fare clic su **Avanti**.
5. Viene offerta la possibilità di eseguire il backup del certificato importato.

   Si consiglia di eseguire il backup del certificato in una posizione diversa dall'unità disco rigido del computer.

Visualizzazione dei dettagli del certificato di Privacy Manager

1. Aprire Privacy Manager, quindi fare clic su **Certificati**.
2. Fare clic su un certificato di Privacy Manager.
3. Fare clic su **Dettagli certificato**.
4. Al termine della visualizzazione dei dettagli, fare clic su **OK**.

Rinnovo di un certificato di Privacy Manager

Quando il certificato di Privacy Manager è prossimo alla scadenza, ne viene richiesto il rinnovo:

1. Aprire Privacy Manager, quindi fare clic su **Certificati**.
2. Fare clic su **Rinnova certificato**.
3. Seguire le istruzioni visualizzate per ottenere un nuovo certificato di Privacy Manager.

NOTA: con la procedura di rinnovo del certificato di Privacy Manager non si sostituisce il vecchio certificato di Privacy Manager. È necessario ottenere un nuovo certificato di Privacy Manager e installarlo utilizzando le stesse procedure descritte nella sezione Richiesta di un certificato di Privacy Manager a pagina 56.

Per i certificati aziendali rilasciati dalla propria organizzazione utilizzando Microsoft Certificate Authority, l'amministratore dell'autorità di certificazione deve rinnovare il certificato utilizzando la stessa chiave privata dell'originale oppure rilasciarne uno nuovo utilizzando la stessa chiave privata.

Impostazione di un certificato di Privacy Manager predefinito

In Privacy Manager sono visibili soltanto i certificati di Privacy Manager, anche se nel computer sono installati certificati di altre autorità di certificazione.

Se nel computer sono installati più certificati di Privacy Manager all'interno dell'applicazione, è possibile specificarne uno come predefinito:

1. Aprire Privacy Manager, quindi fare clic su **Certificati**.
2. Fare clic sul certificato di Privacy Manager che si desidera utilizzare come predefinito, quindi fare clic su **Imposta predefinito**.
3. Fare clic su **OK**.

NOTA: non è obbligatorio utilizzare il proprio certificato di Privacy Manager predefinito. Dalle diverse funzioni di Privacy Manager, è possibile selezionare qualsiasi certificato di Privacy Manager.

Eliminazione di un certificato di Privacy Manager

Se si elimina un certificato di Privacy Manager, non è possibile aprire i file o visualizzare i dati crittografati con tale certificato. Se si elimina accidentalmente un certificato di Privacy Manager, è possibile ripristinarlo utilizzando il file di backup creato durante l'installazione del certificato. Per ulteriori informazioni, fare riferimento alla sezione Ripristino di un certificato di Privacy Manager a pagina 59.

Per eliminare un certificato di Privacy Manager:

1. Aprire Privacy Manager, quindi fare clic su **Certificati**.
2. Fare clic sul certificato di Privacy Manager da eliminare, quindi 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 su **Applica**.

Ripristino di un certificato di Privacy Manager

Durante l'installazione del certificato di Privacy Manager, viene richiesto di creare una copia di backup del certificato. È anche possibile creare una copia di backup dalla pagina Migrazione. La copia di backup può essere utilizzata durante la migrazione a un altro computer o per ripristinare un certificato sullo stesso computer.

1. Aprire Privacy Manager, quindi fare clic su **Migrazione**.
2. Fare clic su **Ripristina**.
3. Nella pagina File di migrazione, fare clic su **Sfoglia** per cercare il file .dppsm creato durante il processo di backup, quindi fare clic su **Avanti**.
4. Immettere la password utilizzata per la creazione del backup e fare clic su **Avanti**.
5. Fare clic su **Fine**.

Per ulteriori informazioni, fare riferimento alla sezione Impostazione di un certificato di Privacy Manager a pagina 57 o Backup dei certificati di Privacy Manager e dei contatti attendibili a pagina 68.

Revoca del certificato di Privacy Manager

Se si teme che la protezione del certificato di Privacy Manager sia stata compromessa, è possibile revocarlo:

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

1. Aprire Privacy Manager, quindi fare clic su **Certificati**.
2. Fare clic su **Avanzate**.
3. Fare clic sul certificato di Privacy Manager che si desidera revocare, quindi fare clic su **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 dei contatti attendibili

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

Gestione contatti attendibili consente di eseguire le seguenti attività:

- Visualizzare i dettagli dei contatti attendibili
- Eliminare contatti attendibili
- Verificare lo stato della revoca per i contatti attendibili (opzione avanzata)

Aggiunta di contatti attendibili

L'aggiunta di contatti attendibili è un processo in tre fasi:

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 la risposta del contatto attendibile, quindi si fa clic su **Accetto**.

È possibile inviare un messaggio e-mail di invito a singoli destinatari di contatti attendibili o a tutti i contatti inclusi nella rubrica di Microsoft Outlook.

Per aggiungere contatti attendibili, fare riferimento alle seguenti sezioni.

NOTA: per rispondere all'invito a diventare un contatto attendibile, i destinatari devono avere Privacy Manager in esecuzione nei loro computer o il client alternativo installato. Per informazioni sull'installazione del client alternativo, accedere al sito Web di DigitalPersona all'indirizzo http://digitalpersona.com/privacymanager/download.

Aggiunta di un contatto attendibile

1. Avviare Privacy Manager, fare clic su **Gestione contatti attendibili** e quindi scegliere **Invita contatti**.

   Oppure

   In Microsoft Outlook, fare clic sulla freccia giù accanto a **Invia in modalità protetta** sulla barra degli strumenti, quindi fare clic su **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 Invito contatti attendibili, leggere il testo, quindi scegliere **OK**.

   Verrà generato automaticamente un messaggio e-mail.
4. Immettere gli indirizzi e-mail dei destinatari da aggiungere come contatti attendibili.

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

6. Fare clic su **Invio**.

NOTA: se non si dispone di un certificato di Privacy Manager, verrà visualizzato un messaggio per informare l'utente che per inviare la richiesta per un contatto attendibile è necessario un certificato di Privacy Manager. Fare clic su **OK** per avviare la richiesta guidata di un certificato. Per ulteriori informazioni, consultare la sezione Richiesta di un certificato di Privacy Manager a pagina 56.

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

NOTA: quando il contatto attendibile riceve l'e-mail, è necessario che faccia clic su **Accetto** nell'angolo inferiore destro del messaggio e che scelga **OK** nella finestra di dialogo di conferma che viene visualizzata.

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 i contatti di Microsoft Outlook

1. Avviare Privacy Manager, fare clic su **Gestione contatti attendibili** e scegliere **Invita contatti**.

   Oppure

   In Microsoft Outlook, fare clic sulla freccia rivolta verso il basso accanto a **Invia in modo protetto** nella barra degli strumenti, quindi fare clic su **Invita tutti i contatti di Outlook**.

2. Quando viene visualizzata la pagina 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 Invio dell'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 **Invia**.

NOTA: se non si dispone di un certificato di Privacy Manager, verrà visualizzato un messaggio per informare l'utente che per inviare la richiesta per un contatto attendibile è necessario un certificato di Privacy Manager. Fare clic su **OK** per avviare la richiesta guidata di un certificato. Per ulteriori informazioni, consultare la sezione Richiesta di un certificato di Privacy Manager a pagina 56.

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

NOTA: quando il contatto attendibile riceve l'e-mail, è necessario che faccia clic su **Accetto** nell'angolo inferiore destro del messaggio e che scelga **OK** nella finestra di dialogo di conferma che viene visualizzata.

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 **Contatti attendibili**.
2. Fare clic su un contatto attendibile.
3. Fare clic su **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 **Contatti attendibili**.
2. Fare clic sul contatto attendibile che si desidera eliminare.
3. Fare clic su **Elimina contatto**.
4. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

Verifica dello stato della revoca per un contatto attendibile

Per verificare se un contatto attendibile ha revocato il certificato di Privacy Manager:

1. Avviare Privacy Manager e fare clic su **Contatti attendibili**.
2. Fare clic su un contatto attendibile.
3. Fare clic sul pulsante **Avanzate**.

   Viene visualizzata la finestra di dialogo Gestione avanzata contatti attendibili.
4. Fare clic su **Verifica revoca**.
5. Fare clic su **Chiudi**.

Attività generali

È possibile utilizzare Privacy Manager con i seguenti prodotti Microsoft:

- Microsoft Outlook
- Microsoft Office

Uso di Privacy Manager in Microsoft Outlook

Se Privacy Manager è installato, nella barra degli strumenti di Microsoft Outlook viene visualizzato il pulsante Privacy e nella barra degli strumenti di ciascun messaggio Microsoft Outlook viene visualizzato il pulsante Invia in modo protetto. Quando si fa clic sulla freccia rivolta verso il basso accanto a **Privacy** o **Invia in modo protetto**, è possibile scegliere le opzioni riportate di seguito:

- **Firma e invia il messaggio** (solo pulsante Invia in modo protetto): questa opzione consente di aggiungere una firma digitale all'e-mail e di inviarla dopo aver eseguito l'autenticazione utilizzando il metodo di accesso protetto prescelto.
- **Crittografa per i contatti attendibili e invia** (solo pulsante Invia in modo protetto): questa opzione consente di aggiungere una firma digitale all'e-mail, di crittografarla e di inviarla dopo aver eseguito l'autenticazione utilizzando il metodo di accesso protetto prescelto.
- **Invita contatti**: questa opzione consente di inviare un invito a diventare un contatto attendibile. Per ulteriori informazioni, fare riferimento alla sezione Aggiunta di un contatto attendibile a pagina 60.
- **Invita i contatti di Outlook**: questa opzione consente di inviare un invito a diventare un contatto attendibile a tutti i destinatari inclusi nella rubrica di Microsoft Outlook. Per ulteriori informazioni, fare riferimento alla sezione Aggiunta di contatti attendibili mediante i contatti di Microsoft Outlook a pagina 61.
- **Apri software Privacy Manager**: le opzioni Certificati, Contatti attendibili e Impostazioni consentono di aprire il software Privacy Manager per aggiungere, visualizzare o modificare le impostazioni correnti. Per ulteriori informazioni, fare riferimento alla sezione Gestione dei certificati di Privacy Manager a pagina 56, Gestione dei contatti attendibili a pagina 60 o Configurazione di Privacy Manager per Microsoft Outlook a pagina 63.

Configurazione di Privacy Manager per Microsoft Outlook

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

   Oppure

   Nella barra degli strumenti principale di Microsoft Outlook, fare clic sulla freccia rivolta verso il basso accanto a **Invia in modo protetto** (**Privacy** in Outlook 2003), 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 **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

1. In Microsoft Outlook, fare clic su **Nuovo** o **Rispondi**.
2. Digitare il messaggio e-mail.
3. Fare clic sulla freccia giù accanto a **Invia in modo protetto** (**Privacy** in Outlook 2003), quindi fare clic su **Firma e invia**.
4. 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 **Invia in modo protetto** (**Privacy** in Outlook 2003) quindi fare clic su **Crittografa per i 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 un documento di Microsoft Office 2007

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 un pulsante Firma e crittografa. Quando si fa clic sulla freccia giù accanto a **Firma e crittografa**, è possibile scegliere tra le seguenti opzioni:

- **Firma documento**: questa opzione consente di aggiungere la proprio firma digitale al documento.
- **Aggiungi riga firma prima della firma** (solo in Microsoft Word e Microsoft Excel): per impostazione predefinita, viene aggiunta una riga per la firma quando si firma o crittografa un documento Microsoft Word o Microsoft Excel. Per disattivare questa opzione, fare clic su **Aggiungi la riga della firma** per rimuovere il segno di spunta.
- **Crittografa documento**: questa opzione consente di crittografare il documento e di aggiungervi la propria firma digitale.
- **Rimuovi crittografia**: questa opzione consente di rimuovere la crittografia dal documento.
- **Apri software Privacy Manager**: le opzioni Certificati, Contatti attendibili e Impostazioni consentono di aprire il software Privacy Manager per aggiungere, visualizzare o modificare le impostazioni correnti. Per ulteriori informazioni, fare riferimento alla sezione Gestione dei

certificati di Privacy Manager a pagina 56, Gestione dei contatti attendibili a pagina 60 o Configurazione di Privacy Manager per Microsoft Office a pagina 65.

Configurazione di Privacy Manager per Microsoft Office

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 **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 Microsoft Office

1. In Microsoft Word, Microsoft Excel o Microsoft PowerPoint, creare e salvare un documento.
2. Fare clic sulla freccia giù accanto a **Firma e crittografa**, quindi fare clic su **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 **Prepara** quindi su **Contrassegna come finale**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si** e continuare a lavorare.
4. Una volta completata la modifica, firmare di nuovo il documento.

Aggiunta di una riga per la firma in 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. Creare e salvare un documento in Microsoft Word o Microsoft Excel.
2. Fare clic sul menu **Home**.
3. Fare clic sulla freccia giù accanto a **Firma e crittografa**, quindi scegliere **Aggiungi riga prima di firmare**.

   NOTA: viene visualizzato un segno di spunta accanto alla voce 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 **Firma e crittografa**, quindi scegliere **Firma documento**.
5. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

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

È possibile aggiungere più righe per la firma al proprio documento definendo firmatari consigliati. Un firmatario consigliato è un utente che il proprietario di un documento Microsoft Word o Microsoft Excel

incarica ad aggiungere una riga per la firma nel documento. Il proprietario può designare se stesso o un'altra persona come firmatario del documento. Ad esempio, se si prepara un documento che deve essere firmato da tutti i membri di un reparto, è possibile includere le righe corrispondenti alle loro firme nell'ultima pagina del documento, con istruzioni relative alla data entro cui eseguire tale operazione.

Per aggiungere un firmatario consigliato 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 **Inserisci**.
3. Nel gruppo **Testo** sulla barra degli strumenti, fare clic sulla freccia accanto a **Riga per la firma** e scegliere **Provider di firme di Privacy Manager**.

   Viene visualizzata la finestra di dialogo Impostazione firme.
4. Nella casella sotto **Firmatario consigliato**, immettere il nome del firmatario consigliato.
5. Nella casella sotto **Istruzioni per il firmatario**, immettere un messaggio per questo firmatario consigliato.

   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 **Visualizza data della firma sulla riga della firma**.
7. Selezionare la casella di controllo **Visualizza titolo del firmatario sulla riga della firma** per visualizzare il titolo.

   NOTA: Il proprietario del documento assegna firmatari consigliati al suo documento. Le caselle di controllo **Visualizza data della firma sulla riga della firma** e/o **Visualizza il titolo sulla riga della firma** devono essere selezionate per poter consentire al firmatario consigliato di visualizzare la data e/o il titolo nella riga per la firma.
8. Fare clic su **OK**.

Aggiunta di una riga per la firma del firmatario consigliato

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 Microsoft Office

L'utente può crittografare un documento Microsoft Office per sé e per i suoi contatti attendibili. Dopo aver crittografato e chiuso un documento, l'utente e i contatti attendibili da lui selezionati nell'elenco devono autenticarsi prima di poterlo aprire.

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 rivolta verso il basso accanto a **Firma e crittografa**, quindi fare clic su **Crittografa documento**.

   Viene visualizzata la finestra di dialogo 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**.

Se in un secondo momento si decide di modificare il documento, seguire i passaggi delineati nella sezione Rimozione della crittografia da un documento Microsoft Office a pagina 67. Una volta rimossa la crittografia, è possibile modificare il documento. Per crittografare di nuovo il documento, seguire i passaggi riportati in questa sezione.

Rimozione della crittografia da un documento 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 rivolta verso il basso accanto a **Firma e crittografa**, quindi su **Rimuovi crittografia**.

Invio di un documento Microsoft Office crittografato

È possibile allegare un documento Microsoft Office crittografato a un'e-mail senza che questa sia firmata o crittografata. A tal fine, creare e inviare un'e-mail con un documento crittografato o firmato come un normale messaggio con 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 informazioni, fare riferimento alla sezione Crittografia e invio di un messaggio e-mail a pagina 64.

Visualizzazione di un documento Microsoft Office firmato

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

Quando viene aperto un documento Microsoft Office firmato, nella barra di stato nella parte inferiore della finestra del documento viene visualizzata l'icona delle firme digitali.

1. Fare clic sull'icona delle **firme digitali** per attivare o disattivare la visualizzazione della finestra di dialogo Firme, in cui vengono mostrati i nomi di tutti gli utenti che hanno firmato il documento nonché la data di ogni firma.

2. Per visualizzare ulteriori informazioni su ogni firma, fare clic con il pulsante destro del mouse sul nome desiderato nella finestra di dialogo Firme e selezionare **Dettagli firma**.

Visualizzazione di un documento Microsoft Office

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

Se si smarrisce il certificato, per poter visualizzare un documento Microsoft Office crittografato, è necessario ripristinare 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.

Attività avanzate

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

Ai fini della protezione, è possibile eseguire la migrazione protetta dei certificati di Privacy Manager e dei contatti attendibili su un altro computer oppure eseguire una copia di backup dei dati. A tal fine, copiarli in un file protetto da password in un percorso di rete o in un dispositivo di archiviazione rimovibile, quindi ripristinare il file nel nuovo computer.

Backup dei certificati di Privacy Manager e dei contatti attendibili

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

1. Aprire Privacy Manager, quindi fare clic su **Migrazione**.

2. Fare clic su **Backup**.

3. Nella pagina Seleziona dati, selezionare le categorie di dati da includere nel file di migrazione, quindi fare clic su **Avanti**.

4. Nella pagina File di migrazione, immettere un nome per il 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, poiché servirà per ripristinare il file di migrazione.

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

7. Nella pagina File di migrazione salvato, fare clic su **Fine**.

Ripristino dei certificati di Privacy Manager e dei contatti attendibili

Per ripristinare i certificati di Privacy Manager e i contatti attendibili in un computer all'interno del processo di migrazione o nello stesso computer, procedere come segue:

1. Aprire Privacy Manager, quindi fare clic su **Migrazione**.

2. Fare clic su **Ripristina**.

3. Nella pagina File di migrazione, fare clic su **Sfoglia** per cercare il file, quindi fare clic su **Avanti**.

4. Immettere la password utilizzata per la creazione del file di backup e fare clic su **Avanti**.

5. Nella pagina File di migrazione, fare clic su **Fine**.

Amministrazione centralizzata di Privacy Manager

L'installazione di Privacy Manager fa parte di un'installazione centralizzata personalizzata dall'amministratore. È possibile che siano state attivate o disattivate una o più delle seguenti opzioni:

- **Criteri di utilizzo dei certificati**: è possibile che venga autorizzato solo l'uso di certificati di Privacy Manager emessi da Comodo o di certificati digitali emessi da altre autorità di certificazione.

- **Criterio di crittografia**: la crittografia può essere attivata o disattivata in Microsoft Office o Microsoft Outlook.

7 File Sanitizer for HP ProtectTools

File Sanitizer consente di distruggere in modo sicuro risorse quali dati o file personali, dati cronologici o correlati al Web oppure componenti di altri dati presenti sul computer in uso, e di eseguire una pulizia periodica delle risorse eliminate sul disco fisso.

NOTA: la presente versione di File Sanitizer supporta solo il disco fisso del computer.

Distruzione

La distruzione di risorse è un'operazione diversa dall'operazione standard di eliminazione dei dati disponibile in Windows®, che nel contesto di File Sanitizer è nota come eliminazione di tipo semplice. Quando si distrugge una risorsa utilizzando File Sanitizer, i file vengono sovrascritti con dati senza significato, affinché risulti praticamente impossibile recuperare i dati originali. Con l'operazione di Windows che comporta un'eliminazione semplice, il file o la risorsa può rimanere sul disco rigido intatta oppure in uno stato tale da consentirne il recupero da parte di un esperto informatico.

A seconda del profilo scelto per la distruzione (ovvero **Protezione elevata**, **Protezione media** o **Protezione bassa**), si selezionano automaticamente un elenco di risorse e un metodo di cancellazione. È inoltre possibile personalizzare un profilo, specificando il numero di cicli di distruzione, le risorse da distruggere, le risorse che richiedono conferma prima della distruzione e le risorse da escludere. Per ulteriori informazioni, fare riferimento alla sezione Selezione o creazione di un profilo di distruzione a pagina 75.

È possibile pianificare una distruzione automatica oppure attivarla manualmente utilizzando l'icona **HP ProtectTools** nell'area di notifica disponibile a destra nella barra delle applicazioni. Per ulteriori informazioni, fare riferimento alla sezione Impostazione della distruzione pianificata dei dati a pagina 74, Distruzione manuale di una risorsa a pagina 79 o Distruzione manuale di tutti gli elementi selezionati a pagina 80.

NOTA: la distruzione di un file .dll e la rimozione dal sistema vengono eseguite solo se tale file è stato spostato nel Cestino.

Pulizia dello spazio libero

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 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: se si seleziona **Impostazioni eliminazione semplice** in File Sanitizer, è possibile eseguire occasionalmente la pulizia dello spazio lasciato libero dalle risorse spostate nel Cestino di Windows oppure eliminate manualmente. La pulizia dello spazio libero non fornisce ulteriore protezione per le risorse distrutte.

È possibile programmare la pulitura automatica dello spazio libero oppure attivarla manualmente utilizzando l'icona **HP ProtectTools** nell'area di notifica disponibile a destra nella barra delle applicazioni. Per ulteriori informazioni, fare riferimento alla sezione Impostazione della pianificazione per la pulitura dello spazio libero a pagina 74 o Attivazione manuale della pulitura dello spazio libero a pagina 80.

Apertura di File Sanitizer

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **HP ProtectTools Security Manager**.
2. Fare clic su **File Sanitizer**.

– Oppure –

- Fare doppio clic sull'icona **File Sanitizer** disponibile sul desktop.

– Oppure –

- Fare clic con il pulsante destro del mouse sull'icona **HP ProtectTools** nell'area di notifica a destra della barra delle applicazioni, quindi selezionare **File Sanitizer** e infine **Apri File Sanitizer**.

Procedure di configurazione

Impostazione della distruzione pianificata dei dati

È possibile selezionare un profilo predefinito per la distruzione oppure crearne uno personalizzato. Per ulteriori informazioni, fare riferimento alla sezione Selezione o creazione di un profilo di distruzione a pagina 75. Inoltre, è possibile distruggere manualmente le risorse in qualsiasi momento. Per ulteriori informazioni, fare riferimento alla sezione Uso di una sequenza di tasti per avviare la distruzione a pagina 78.

NOTA: un'attività pianificata inizia a un'ora specifica. Se all'ora pianificata il sistema è spento oppure in modalità di sospensione/standby, File Sanitizer non proverà a riavviare l'attività.

1. Aprire File Sanitizer, quindi fare clic su **Distruzione**.
2. Selezionare una o più opzioni di distruzione:
   - **Arresto di Windows**: tutte le risorse selezionate vengono distrutte all'arresto di Windows.

     NOTA: al momento dell'arresto si apre una finestra di dialogo che richiede di confermare se si desidera distruggere le risorse selezionate oppure ignorare tale procedura.

     Fare clic su **Sì** per saltare la procedura oppure su **No** per procedere alla distruzione dei dati.
   - **Si avvia il browser Web**: al momento dell'apertura del browser vengono distrutte tutte le risorse correlate al Web, ad esempio la cronologia degli URL.
   - **Si chiude il browser Web**: al momento della chiusura del browser vengono distrutte tutte le risorse correlate al Web, ad esempio la cronologia degli URL.
   - **Sequenza di tasti**: consente di specificare una sequenza di tasti per avviare l'operazione di distruzione. Per istruzioni dettagliate, fare riferimento alla sezione "Uso di una sequenza di tasti per avviare la distruzione a pagina 78".

   NOTA: la distruzione di un file .dll e la rimozione dal sistema vengono eseguite solo se tale file è stato spostato nel Cestino.
3. Per pianificare un orario futuro per la distruzione delle risorse, selezionare la casella di controllo **Attiva programmazione**, immettere la password di Windows, quindi selezionare data e ora.
4. Fare clic su **Applica**.

Impostazione della pianificazione per la pulitura dello spazio libero

Se si seleziona **Impostazioni eliminazione semplice** in File Sanitizer, è possibile eseguire occasionalmente la pulizia dello spazio lasciato libero dalle risorse spostate nel Cestino di Windows oppure eliminate manualmente. La pulizia dello spazio libero non fornisce ulteriore protezione per le risorse distrutte.

NOTA: un'attività pianificata inizia a un'ora specifica. Se all'ora pianificata il sistema è spento oppure in modalità di sospensione/standby, File Sanitizer non proverà a riavviare l'attività.

1. Aprire File Sanitizer, quindi fare clic su **Pulitura**.
2. Per pianificare un orario futuro per la pulitura delle risorse eliminate sul disco rigido, selezionare la casella di controllo **Attiva programmazione**, immettere la password di Windows, quindi selezionare una data e un orario.
3. Fare clic su **Applica**.

NOTA: la pulitura dello spazio libero può richiedere una notevole quantità di tempo. Sebbene la pulitura dello spazio libero sia un'operazione eseguita in background, le prestazioni del computer possono risultare inferiori a causa di un 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 oppure creandone uno personalizzato.

Selezione di un profilo di distruzione

Quando si sceglie un profilo predefinito, si selezionano automaticamente un metodo di cancellazione e un elenco di risorse predefiniti. Inoltre, è possibile visualizzare l'elenco predefinito di risorse selezionate per la distruzione.

1. Aprire File Sanitizer, quindi fare clic su **Impostazioni**.
2. Fare clic su un profilo di distruzione predefinito:
   - **Protezione elevata**
   - **Protezione media**
   - **Protezione bassa**
3. Per visualizzare le risorse selezionate per la distruzione, fare clic su **Visualizza dettagli**.
   a. **Gli elementi selezionati verranno distrutti e verrà visualizzato un messaggio di conferma. Gli elementi non selezionati verranno eliminati senza messaggio di conferma.** - Selezionare la casella di controllo per visualizzare un messaggio di conferma prima di distruggere l'elemento oppure deselezionarla per eseguire la distruzione senza visualizzarlo.

      NOTA: L'elemento verrà distrutto anche se la sua casella di controllo è deselezionata.

   b. Fare clic su **Applica**.
4. Fare clic su **Applica**.

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. Aprire File Sanitizer, fare clic su **Impostazioni**, quindi su **Impostazioni di protezione avanzate** e infine su **Visualizza dettagli**.
2. Selezionare il numero di cicli di distruzione.

   NOTA: per ciascuna risorsa verrà eseguito il numero di cicli di distruzione selezionato. Ad esempio, se scegli 3 cicli di distruzione, sarà eseguito per tre volte un algoritmo in grado di oscurare i dati. Se si sceglie un maggior numero di cicli di distruzione, tale operazione potrebbe richiedere una notevole quantità di tempo. Tuttavia, con un maggior numero di cicli si riducono le probabilità di recupero dei dati.

3. Per selezionare le risorse da distruggere:

   a. In **Opzioni di distruzione disponibili**, fare clic su una risorsa, quindi scegliere **Aggiungi**.

   b. Per aggiungere una risorsa personalizzata, fare clic su **Aggiungi opzione personalizzata**, quindi cercare o immettere il percorso del file o della cartella.

   c. Fare clic su **Apri**, quindi su **OK**.

   d. In **Opzioni di distruzione disponibili**, fare clic sulla risorsa personalizzata, quindi scegliere **Aggiungi**.

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

4. **Gli elementi selezionati verranno distrutti e verrà visualizzato un messaggio di conferma. Gli elementi non selezionati verranno eliminati senza messaggio di conferma.** - Selezionare la casella di controllo per visualizzare un messaggio di conferma prima di distruggere l'elemento oppure deselezionarla per eseguire la distruzione senza visualizzarlo.

   NOTA: L'elemento verrà distrutto anche se la sua casella di controllo è deselezionata.

   Per rimuovere una risorsa dall'elenco di elementi da distruggere, selezionarla, quindi fare clic su **Rimuovi**.

5. Per proteggere i file o le cartelle dalla distruzione automatica:

   a. In **Non distruggere seguenti**, fare clic su **Aggiungi**, quindi cercare o immettere il percorso del file o della cartella.

   b. Fare clic su **Apri**, quindi su **OK**.

   Per rimuovere una risorsa dall'elenco di esclusione, selezionarla, quindi fare clic su **Elimina**.

6. Fare clic su **Applica**.

Personalizzazione di un profilo di eliminazione semplice

Il profilo di eliminazione semplice consente di eseguire un'operazione standard di eliminazione senza distruzione delle risorse. È possibile personalizzare un profilo di eliminazione semplice specificando

le risorse da includere, le risorse che richiedono conferma prima della distruzione e le risorse da escludere.

NOTA: se si seleziona l'opzione **Impostazioni eliminazione semplice**, è possibile eseguire occasionalmente la pulizia dello spazio lasciato libero dalle risorse eliminate manualmente oppure spostate nel Cestino di Windows.

1. Aprire File Sanitizer, fare clic su **Impostazioni**, quindi su **Impostazioni eliminazione semplice** e infine su **Visualizza dettagli**.
2. Selezionare le risorse che si desidera eliminare:
   a. In **Opzioni di eliminazione disponibili**, fare clic sulla risorsa, quindi scegliere **Aggiungi**.
   b. Per aggiungere una risorsa personalizzata, fare clic su **Aggiungi opzione personalizzata**, quindi cercare o immettere il percorso del file o della cartella e infine fare clic su **OK**.
   c. Fare clic sulla risorsa personalizzata, quindi fare clic su **Aggiungi**.

   Per eliminare una risorsa dalle opzioni di eliminazione disponibili, selezionarla, quindi fare clic su **Elimina**.
3. **Gli elementi selezionati verranno distrutti e verrà visualizzato un messaggio di conferma. Gli elementi non selezionati verranno eliminati senza messaggio di conferma.** - Selezionare la casella di controllo per visualizzare un messaggio di conferma prima di distruggere l'elemento oppure deselezionarla per eseguire la distruzione senza visualizzarlo.

   NOTA: L'elemento verrà distrutto anche se la sua casella di controllo è deselezionata.

   Per rimuovere una risorsa dall'elenco di elementi da eliminare, selezionarla, quindi fare clic su **Rimuovi**.
4. Per proteggere le risorse dall'eliminazione automatica:
   a. In **Non eliminare seguenti**, fare clic su **Aggiungi**, quindi cercare o immettere il percorso del file o della cartella.
   b. Fare clic su **Apri**, quindi su **OK**.

   Per rimuovere una risorsa dall'elenco di esclusione, selezionarla, quindi fare clic su **Elimina**.
5. Fare clic su **Applica**.

Attività generali

È possibile utilizzare File Sanitizer per eseguire le seguenti attività:

- Utilizzare una sequenza di tasti per avviare la distruzione: questa funzione consente di creare una sequenza di tasti (ad esempio, ctrl+alt+s) per attivare la distruzione. Per istruzioni dettagliate, fare riferimento alla sezione Uso di una sequenza di tasti per avviare la distruzione a pagina 78.
- Utilizzare l'icona di File Sanitizer per avviare la distruzione: questa funzione è simile alla funzione di trascinamento della selezione in Windows. Per istruzioni dettagliate, fare riferimento alla sezione Uso dell'icona File Sanitizer a pagina 79.
- Distruggere manualmente una risorsa specifica o tutte le risorse selezionate: queste funzioni consentono di distruggere manualmente degli elementi senza aspettare che venga richiamato il regolare programma di distruzione. Per istruzioni dettagliate, fare riferimento alla sezione Distruzione manuale di una risorsa a pagina 79 o Distruzione manuale di tutti gli elementi selezionati a pagina 80.
- Attivare manualmente la pulizia dello spazio libero: questa funzione consente di attivare manualmente la pulizia dello spazio libero. Per istruzioni dettagliate, fare riferimento alla sezione Attivazione manuale della pulitura dello spazio libero a pagina 80.
- Interrompere l'operazione di distruzione o l'operazione di pulizia dello spazio libero: questa funzione consente di interrompere l'operazione di distruzione o quella di pulizia dello spazio libero. Per istruzioni dettagliate, fare riferimento alla sezione Interruzione di un'operazione di distruzione o di pulitura dello spazio libero a pagina 80.
- Visualizzare i file di registro: questa funzione consente di visualizzare i file di registro di distruzione e di pulizia dello spazio libero, che contengono eventuali errori verificatisi dall'ultima operazione di distruzione o di pulizia dello spazio libero. Per istruzioni dettagliate, fare riferimento alla sezione Visualizzazione dei file di registro a pagina 80.

NOTA: L'operazione di distruzione o di pulizia dello spazio libero potrebbe richiedere molto tempo. Anche se la distruzione e la pulizia dello spazio libero vengono eseguite in background, il computer potrebbe risultare più lento a causa del maggior utilizzo del processore.

Uso di una sequenza di tasti per avviare la distruzione

1. Aprire File Sanitizer, quindi fare clic su **Distruzione**.
2. Selezionare la casella di controllo **Sequenza di tasti**.
3. Immettere un carattere nella casella disponibile.
4. Selezionare la casella **CTRL** o **ALT**, quindi selezionare la casella **MAIUSC**.

   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 premuto maiusc e ctrl o alt (o qualunque combinazione specificata) mentre si premono i tasti scelti.
2. Se viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

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** disponibile sul desktop.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

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 **Distruggi uno**.
2. Quando viene visualizzata la finestra di dialogo Sfoglia, passare alla risorsa che si desidera distruggere, quindi scegliere **OK**.

   NOTA: la risorsa selezionata può corrispondere a un singolo file o cartella.

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

oppure

1. Fare clic con il pulsante destro del mouse sull'icona **File Sanitizer** sul desktop, quindi scegliere **Distruggi uno**.
2. Quando viene visualizzata la finestra di dialogo Sfoglia, passare alla risorsa che si desidera distruggere, quindi scegliere **OK**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

oppure

1. Aprire File Sanitizer, quindi fare clic su **Distruzione**.
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 **Si**.

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 **Distruggi ora**.
2. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

oppure

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

oppure

1. Aprire File Sanitizer, quindi fare clic su **Distruzione**.
2. Fare clic sul pulsante **Distruggi ora**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

Attivazione manuale della pulitura 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 **Pulisci ora**.
2. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

oppure

1. Aprire File Sanitizer, quindi fare clic su **Pulitura spazio libero**.
2. Fare clic su **Pulisci ora**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

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

Quando è in corso un'operazione di distruzione o di pulizia di spazio libero, si visualizza un messaggio sull'icona di HP ProtectTools Security Manager nell'area di notifica situata all'estrema destra della barra delle applicazioni. Il messaggio fornisce dettagli (percentuale di completamento) sulla procedura di distruzione o di pulitura dello spazio libero e consente di scegliere se interrompere l'operazione.

- ▲ Per annullare l'operazione, fare clic sul messaggio, quindi su **Interrompi**.

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.

Una volta creato un file di registro per l'operazione di distruzione, ne viene creato un altro per la pulitura del disco libero. Entrambi i file sono memorizzati sul disco rigido:

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

Per i sistemi a 64 bit, i file di registro sono memorizzati sul disco rigido:

- C:\Programmi (x86)\Hewlett-Packard\File Sanitizer*[nomeutente]*_ShredderLog.txt
- C:\Programmi (x86)\Hewlett-Packard\File Sanitizer*[nomeutente]*_DiskBleachLog.txt

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

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

NOTA: alcune periferiche di input/HID (Human Interface Input), ad esempio mouse, tastiere, touchpad e lettori di impronte digitali, non sono controllate da Device Access Manager. Per ulteriori informazioni, fare riferimento alla sezione Classi di periferiche non gestite a pagina 92.

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

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

Apertura di Device Access Manager

1. Eseguire l'accesso come amministratore.
2. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
3. Nel riquadro di sinistra, fare clic su **Device Access Manager**.

Gli utenti con restrizioni possono visualizzare i criteri di HP ProtectTools Device Access Manager utilizzando HP ProtectTools Security Manager. La console visualizza una schermata di sola lettura.

Procedure di installazione

Configurazione dell'accesso ai dispositivi

HP ProtectTools Device Access Manager presenta quattro schermate:

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

Configurazione semplice

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

- Tutti i supporti rimovibili (dischetti, unità flash USB e così via)
- Tutte le unità DVD/CD-ROM
- Tutte le porte seriali e parallele
- Tutti i dispositivi Bluetooth®
- Tutti i dispositivi modem
- Tutte le periferiche PCMCIA/ExpressCard
- Tutte le periferiche 1394

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

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

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

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

4. Fare clic su **OK**.

Avvio del servizio in background

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

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

Gli amministratori possono inoltre avviare o arrestare questo servizio:

1. In Windows 7, fare clic su **Start**, **Pannello di controllo**, quindi su **Sistema e sicurezza**.

   – Oppure –

   In Windows Vista®, fare clic su **Start**, **Pannello di controllo**, quindi su **Sistema e manutenzione**.

   – Oppure –

   In Windows XP, fare clic su **Start**, **Pannello di controllo**, quindi su **Prestazioni e manutenzione**.

2. Fare clic su **Strumenti di amministrazione**, quindi su **Servizi**.
3. Selezionare il servizio **Controllo/blocco dispositivi HP ProtectTools**.
4. Per avviare il servizio, fare clic su **Avvia**.

   – Oppure –

   Per interrompere il servizio se è in esecuzione, fare clic su **Interrompi**.

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

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

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

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

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

Configurazione delle classi di periferiche

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Negazione dell'accesso a un utente o gruppo

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

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

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

Concessione dell'accesso a un utente o gruppo

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

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

Viene visualizzata la finestra di dialogo Seleziona utenti o gruppi.

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

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

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

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

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

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

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

   Viene visualizzata la finestra di dialogo Seleziona utenti o gruppi.
7. Fare clic su **Avanzate**, quindi su **Trova** per cercare gli utenti o i gruppi da aggiungere.

8. Fare clic su un utente cui consentire l'accesso, quindi su **OK**.
9. Per concedere l'accesso all'utente selezionato, fare clic su **Consenti**.
10. Fare clic su **Applica**.

Rimozione delle impostazioni per un utente o gruppo

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

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

Reimpostazione della configurazione

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

Per ripristinare i valori predefiniti, procedere come segue:

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, quindi su **Configurazione delle classi di periferiche**.
2. Fare clic su **Reimposta**.
3. Fare clic su **Sì** per confermare la richiesta.
4. Fare clic su **Applica**.

Configurazione JITA

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

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

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

autenticazione dell'utente. Con l'immissione delle credenziali, all'utente viene concesso l'accesso all'unità DVD/CD-ROM.

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

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

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

JITA è disponibile per le seguenti classi di periferiche:

- Unità DVD/CD-ROM
- Supporti rimovibili

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

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

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

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

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

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

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

6. Selezionare la casella di controllo **Estendibile**.

7. Fare clic su **Applica**.

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

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

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

1. Nel riquadro di sinistra della Console amministrativa di HP ProtectTools, fare clic su **Device Access Manager**, quindi su **JITA Configuration** (Configurazione JITA).

2. Dal menu a discesa della periferica, selezionare **Supporti rimovibili** o **Unità DVD/CD-ROM**.

3. Selezionare l'utente o un gruppo di cui si desidera disattivare l'autenticazione Just-in-time.

4. Deselezionare la casella di controllo **Abilitata**.

5. Fare clic su **Applica**.

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

Impostazioni avanzate

Le impostazioni avanzate offrono le seguenti funzioni:

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

Il gruppo Amministratori di periferiche viene utilizzato per escludere gli utenti attendibili (attendibili in termini di accesso alle periferiche) dalle restrizioni imposte da un criterio di Device Access Manager. Gli utenti attendibili in genere includono gli amministratori di sistema. Per ulteriori informazioni, fare riferimento alla sezione Gruppo Amministratori di periferiche a pagina 91.

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

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

Per avviare questi servizi, procedere come segue:

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

   – Oppure –

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

   ```
   sc start flcdlock
   ```

   Premere invio.

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

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

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

Gruppo Amministratori di periferiche

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

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

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

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

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

I metodi alternativi per la gestione dell'appartenenza del gruppo includono:

- In Windows 7 Professional o Windows Vista, gli utenti possono essere aggiunti al gruppo utilizzando lo snap-in MMC standard "Utenti e gruppi locali".
- Per le versioni Home di Windows 7, Windows Vista o Windows XP, da un account con privilegi di amministratore, digitare quanto riportato di seguito nella finestra del prompt dei comandi:

  ```
  net localgroup "Device Administrators" username /add
  ```

  In questo comando, "username" è il nome dell'utente che si desidera aggiungere al gruppo.

Supporto eSATA

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

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

Classi di periferiche non gestite

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

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

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

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

9 Ritrovamento di PC rubati

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

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

Per attivare Computrace for HP ProtectTools, procedere come segue:

1. Connettersi a Internet.
2. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **HP ProtectTools Security Manager**.
3. Nel riquadro di sinistra di Security Manager, fare clic su **Ritrovamento in seguito a furto**.
4. Per avviare la procedura guidata di attivazione di Computrace, fare clic sul pulsante **Attiva adesso**.
5. Inserire le proprie informazioni di contatto e i dati della carta di credito, oppure immettere un codice prodotto preacquistato.

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

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

Per accedere al centro assistenza clienti:

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

Nel Centro assistenza clienti è possibile:

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

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

10 Embedded Security for HP ProtectTools (solo in determinati modelli)

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 TPM Embedded Security aumenta il livello di protezione e abilita altre funzionalità di HP ProtectTools Security Manager. Ad esempio, Credential Manager for HP ProtectTools può utilizzare il chip integrato come fattore di autenticazione quando l'utente esegue l'accesso a Windows.

Procedure di installazione

⚠ **ATTENZIONE:** per ridurre i rischi correlati alla protezione, è consigliabile che gli amministratori IT inizializzino immediatamente il chip di protezione integrato. Se non si inizializza il chip, è possibile che un utente non autorizzato, un worm o virus informatico assumano il controllo del computer e delle operazioni del proprietario, ad esempio la gestione degli archivi di ripristino di emergenza e la configurazione delle impostazioni di accesso dell'utente.

Attenersi ai passaggi riportati nelle seguenti sezioni per abilitare e inizializzare il chip di protezione integrato.

Abilitazione del chip di protezione integrato in Computer Setup

Il chip di protezione integrato deve essere abilitato nella procedura guidata di inizializzazione rapida o nell'utility Computer Setup.

Per abilitare il chip di protezione integrato in Computer Setup, procedere come segue:

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 amministratore, utilizzare i tasti freccia per selezionare **Protezione**, **Setup password** (Password di configurazione), quindi 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 dispositivo di Embedded Security), quindi cambiare l'impostazione su **Abilita**.
7. Premere f10 per accettare le modifiche alla configurazione di protezione incorporata.
8. Per salvare le preferenze ed uscire da Computer Setup, utilizzare i tasti freccia per selezionare **File**, **Save Changes and Exit** (Salva le modifiche ed esci), quindi seguire le istruzioni visualizzate.

Inizializzazione del chip di protezione integrato

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** nell'area di notifica a destra della barra delle applicazioni, quindi selezionare **Embedded Security Initialization** (Inizializzazione di Embedded Security).

   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 utente di Embedded Security non è aperta, fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **HP ProtectTools Security Manager**.
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

Utilizzo dell'unità protetta personale

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, procedere come segue:

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **User Settings** (Impostazioni utente).
3. Nel riquadro di destra, in **Basic User password** (Password utente di base), fare clic su **Modifica**.
4. Immettere la vecchia password, quindi impostare e confermare la nuova password.
5. Fare clic su **OK**.

Attività avanzate

Gli amministratori possono eseguire le seguenti operazioni in Embedded Security:

- Backup e ripristino delle credenziali di Embedded Security, delle impostazioni di Embedded Security e delle unità protette personali
- Modifica della password del proprietario
- Reimpostazione di una password utente
- Migrazione sicura delle credenziali di protezione dell'utente da una piattaforma di origine a una piattaforma di destinazione

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**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Backup**.
3. Nel riquadro di destra, fare clic su **Configura**. Viene aperta la procedura guidata di backup di Embedded Security for HP ProtectTools.
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**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Backup**.
3. Nel riquadro di destra, fare clic su **Ripristina tutto**. Viene aperta la procedura guidata di backup di Embedded Security for HP ProtectTools.
4. Seguire le istruzioni visualizzate.

Modifica della password proprietario

Gli amministratori possono modificare le password del proprietario nel seguente modo:

1. Fare clic su **Start**, **Tutti i programmi**, **HP**, infine su **Console amministrativa di HP ProtectTools**.
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.

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.

11 Eccezioni relative alle password localizzate

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

IME (Input Method Editor, Editor del metodo di input) di Windows non supportati a livello di protezione di preavvio o di HP Drive Encryption

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

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

Ad esempio, per alcune installazioni in giapponese di Windows XP, l'editor IME predefinito è denominato Microsoft IME Standard 2002 per il giapponese, che corrisponde effettivamente al layout di tastiera E0010411. Tuttavia, si tratta di un editor IME e non di un layout di tastiera. (Microsoft riserva lo schema di codifica del layout di tastiera agli editor IME, che estendono il concetto di layout di tastiera.) Dal momento che non si tratta di un layout di tastiera rappresentabile nell'ambiente di digitazione per la richiesta di password a livello di HP Drive Encryption o di protezione di preavvio del BIOS, qualsiasi password digitata con questo editor IME viene rifiutata da HP ProtectTools. Microsoft IME Standard 2002 per il giapponese è anche diverso dal "Nome comune" in Microsoft Windows Vista®. Windows associa alcuni editor IME a un layout di tastiera. In alcuni casi, l'editor IME è supportato da HP ProtectTools, perché viene utilizzata la definizione di layout di tastiera sottostante (codice esadecimale).

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

- IME Microsoft per il giapponese
- Layout della tastiera giapponese
- IME per Office 2007 per il giapponese: se Microsoft o una terza parte utilizza il termine IME o Editor del metodo di input, è possibile che il metodo non sia effettivamente un IME. Ciò può causare confusione, ma il software legge la rappresentazione del codice esadecimale. Pertanto, se un IME esegue l'associazione a un layout di tastiera supportato, HP ProtectTools può supportare la configurazione.

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

Modifiche della password con layout di tastiera supportato

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

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

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

Gestione tasti speciali

- Cinese, slovacco, francese canadese e ceco

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

- Coreano

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

- Nella tabella seguente vengono elencati i caratteri non supportati:

Lingua	Windows	BIOS	Drive Encryption
Arabo	I tasti ﻯ ,ﻱ e ﻯ generano due caratteri.	I tasti ﻯ ,ﻱ e ﻯ generano un carattere.	I tasti ﻯ ,ﻱ e ﻯ generano un carattere.
Francese canadese	ç, è, à ed é con blocco maiusc corrispondono a Ç, È, À ed É in Windows.	ç, è, à ed é con blocco maiusc corrispondono a ç, è, à ed é a livello di protezione di preavvio del BIOS.	ç, è, à ed é con blocco maiusc corrispondono a ç, è, à ed é in HP Drive Encryption.
Spagnolo	40a non è supportato, ma funziona comunque perché il software lo converte in c0a. Tuttavia, a causa delle differenze minime tra i layout di tastiera, si consiglia agli utenti di lingua spagnola di passare al layout Windows in 1040a (Spagnolo (varianti)) o 080a (latino americano).	n/a	n/a
USA internazionale	◦ I tasti ¡, ¤, ‘, ’, ¥ e × nella prima fila vengono rifiutati. ◦ I tasti å, ® e Þ nella seconda fila vengono rifiutati. ◦ I tasti á, ð e ø nella terza fila vengono rifiutati. ◦ Il tasto æ nell'ultima fila viene rifiutato.	n/a	n/a

Lingua	Windows	BIOS	Drive Encryption
Ceco	◦ Il tasto ğ viene rifiutato. ◦ Il tasto į viene rifiutato. ◦ Il tasto ų viene rifiutato. ◦ I tasti ė, ı e ż vengono rifiutati. ◦ I tasti ģ, ķ, ļ, ņ e ţ vengono rifiutati.	n/a	n/a
Slovacco	Il tasto ż viene rifiutato.	◦ I tasti š, ś e ş vengono rifiutati al momento della digitazione, ma vengono accettati quando immessi con la tastiera software. ◦ Il tasto ţ senza funzione associata genera due caratteri.	n/a
Ungherese	Il tasto ż viene rifiutato.	Il tasto ţ genera due caratteri.	n/a
Sloveno	Il tasto żŻ viene rifiutato in Windows e il tasto alt genera un tasto senza funzione associata nel BIOS.	I tasti ú, Ú, ů, Ů, ş, Ş, ś, Ś, š e Š vengono rifiutati nel BIOS.	n/a
Giapponese	Solo per Windows XP, il layout di tastiera standard 411 per il giapponese è supportato. Un IME, comunemente rappresentato in Windows XP come Microsoft Standard IME 2002, non è in genere supportato. Tuttavia, test empirici hanno dimostrato che questo editor è quasi un duplicato del layout di tastiera 411 nella digitazione dei caratteri semplici. Il software commuta pertanto questo IME in layout di tastiera 411 durante la protezione del BIOS e di HP Drive Encryption con password giapponesi localizzate. Se disponibile, si consiglia di preferire IME per Microsoft Office 2007. Nonostante il nome IME, si tratta effettivamente di un layout di tastiera 411, che è supportato.	n/a	n/a

Operazioni da eseguire quando una password viene rifiutata

Le password possono essere rifiutate per i seguenti motivi:

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

  1. Fare clic su **Start**, **Pannello di controllo**, quindi su **Opzioni internazionali e della lingua**.
  2. Fare clic sulla scheda **Lingue**.
  3. Fare clic sul pulsante **Dettagli**.
  4. Nella scheda **Impostazioni**, fare clic sul pulsante **Aggiungi** per aggiungere una tastiera supportata (aggiungere le tastiere americane in lingua di input cinese).
  5. Impostare la tastiera supportata per l'input predefinito.
  6. Riavviare HP ProtectTools, quindi immettere di nuovo la password.

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

  1. Modificare la password di Windows utilizzando solo caratteri supportati. I caratteri non supportati sono elencati in Gestione tasti speciali a pagina 108.
  2. Eseguire di nuovo l'installazione guidata di Security Manager, quindi immettere la nuova password di Windows.

Glossario

accesso al sistema
Un oggetto in Security Manager che consiste di nome utente e password (e possibilmente anche altri dati selezionati) utilizzabili per accedere a siti Web o ad altri programmi.

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

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

amministratore
Vedere *Amministratore Windows*.

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

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

ATM
Automatic Technology Manager, consente agli amministratori di rete di gestire in remoto i sistemi a livello di BIOS.

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

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

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

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

backup

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

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

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.

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

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.

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

console
Ubicazione centrale da cui è possibile accedere e gestire le funzionalità e impostazioni nella Console amministrativa di HP ProtectTools.

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

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

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

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

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

crittografia per contatti attendibili
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.

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

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

destinatario di contatto attendibile
Persona che riceve un invito a diventare un contatto attendibile.

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

distruzione automatica
Distruzione programmata che l'utente imposta in File Sanitizer.

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

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

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

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

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 esegue la crittografia di tutti i file e di tutte 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
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.

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

HP SpareKey
Copia di backup della chiave di crittografia dell'unità.

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

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

Invito contatti attendibili
Messaggio e-mail inviato a una persona, in cui le si chiede di diventare un contatto attendibile.

JITA
autenticazione Just-in-time.

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 protezione
Il metodo utilizzato per accedere al computer.

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

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

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

pannello
Ubicazione centrale da cui è possibile accedere e gestire le funzionalità e impostazioni di Security Manager for HP ProtectTools.

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

PIN
Numero identificativo personale.

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

profilo di distruzione
Metodo di cancellazione e un elenco di risorse specifico.

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

PSD
Personal Secure Drive: fornisce un'area di memorizzazione protetta per i dati importanti.

pulizia dello spazio libero
Scrittura sicura di dati casuali sulle risorse eliminate per alterare il contenuto della risorsa eliminata.

pulsante Firma e crittografa
Pulsante software che viene visualizzato nella barra degli strumenti delle applicazioni Microsoft Office. La selezione di questo pulsante consente di firmare, crittografare o rimuovere la crittografia in un documento Microsoft Office.

pulsante Send Security (Sicurezza invio).
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.

riavvio
Processo di riavvio del computer.

riga per la firma
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.

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

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

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

scheda ID
Gadget di Windows che serve a identificare visivamente il desktop con il nome utente e l'immagine selezionata. Fare clic sulla scheda ID per aprire la Console amministrativa di HP ProtectTools.

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

Sequenza di tasti
Combinazione di tasti specifici che, premuti, avviano una distruzione automatica, ad esempio, ctrl+alt+s.

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

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

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

token
Vedere *metodo di accesso di protezione*.

token USB
Dispositivo di protezione in cui sono memorizzate le informazioni di identificazione relative a un utente. Analogamente a una smart card o a un lettore biometrico, viene utilizzato per eseguire l'autenticazione del proprietario su un computer.

token virtuale
Funzionalità di protezione che funziona in modo analogo a una smart card e a un lettore di schede. Il token viene salvato nell'unità disco rigido del computer o nel registro di sistema di Windows. Quando si esegue l'accesso con un token virtuale, viene richiesto di immettere un PIN per completare l'autenticazione.

TXT
Trusted Execution Technology.

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

Indice analitico