ProtectTools
Guida per l'utente

Prima edizione: Luglio 2007

Numero di parte del documento: 451271-061

Sommario

1 Introduzione alle modalità di protezione

HP ProtectTools Security Manager è un software che fornisce funzioni di protezione create per salvaguardare il computer, le reti e i dati critici dall'accesso non autorizzato. I seguenti moduli software forniscono una funzionalità di protezione potenziata:

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Drive Encryption for HP ProtectTools

La disponibilità dei moduli software può variare a seconda del modello di computer. Ad esempio, Embedded Security for HP ProtectTools è disponibile solo per i computer che installano il chip TPM di protezione incorporata.

I moduli software HP ProtectTools possono essere preinstallati, precaricati oppure disponibili per il download dal sito Web HP. Per ulteriori informazioni, visitare il sito http://www.hp.com.

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

Funzioni di HP ProtectTools

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

Modulo	Funzioni principali
Credential Manager for HP ProtectTools	• Credential Manager consente di conservare le proprie password personali. • La funzione Single Sign-on ricorda password multiple per i siti Web, le applicazioni e le risorse di rete protette. • Single Sign-on offre inoltre una protezione ulteriore, in quanto per l'autenticazione degli utenti richiede combinazioni di tecnologie di protezione diverse, quali Java™ Card e sistemi biometrici. • La memorizzazione delle password viene protetta da un sistema di crittografia e può essere reso più rigido con l'utilizzo di un chip di protezione incorporata TPM e/o di un sistema di autenticazione come una Java Card o un sistema biometrico.
Embedded Security for HP ProtectTools	• Embedded Security sfrutta un chip di protezione incorporata TPM (Trusted Platform Module) per accrescere il livello di protezione dagli accessi non autorizzati ai dati sensibili degli utenti o alle credenziali memorizzate a livello locale in un PC. • Embedded Security consente la creazione di una personal secure drive (PSD) per la protezione dei dati utente • Supporta inoltre applicazioni di terzi, quali Microsoft Outlook e Internet Explorer, per le operazioni protette da certificato digitale.
Java Card Security for HP ProtectTools	• Java Card Security configura la Java Card di HP ProtectTools per l'autenticazione degli utenti prima del caricamento del sistema operativo. • Java Card Security configura Java Card separate per amministratore e utente.
BIOS Configuration for HP ProtectTools	• BIOS Configuration consente di accedere alla gestione delle password di accensione per utente e amministratore. • BIOS Configuration fornisce un'alternativa all'utility di configurazione BIOS prima dell'avvio, denominata F10 Setup. • DriveLock contribuisce a proteggere l'unità disco rigido dall'accesso non autorizzato, anche se viene rimossa dal sistema, senza la necessità per l'utente di ricordare password aggiuntive.
Drive Encryption for HP ProtectTools	• Drive Encryption fornisce un sistema completo di crittografia per il disco rigido. • Per eseguire la decodifica e l'accesso ai dati, Drive Encryption impone l'autenticazione di preavvio.

Accesso a HP ProtectTools Security

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

- Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.

NOTA: Dopo aver configurato il modulo Credential Manager, è possibile avviare HP ProtectTools anche accedendo a Credential Manager direttamente dalla schermata di accesso a Windows. Per ulteriori informazioni, consultare la sezione Accesso a Windows con Credential Manager a pagina 17.

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 contro furti mirati

Un esempio di questo tipo di incidente è il furto mirato di dati riservati contenuti in un computer e di informazioni sulla clientela in un ufficio del tipo open space. Le seguenti funzioni contribuiscono a proteggere il computer dai furti mirati:

- Se abilitata, la funzione di autenticazione al preavvio impedisce l'accesso al sistema operativo. Vedere le seguenti procedure:
  - "Attivazione e disattivazione del supporto per l'autenticazione all'accensione delle smart card a pagina 47"
  - "Attivazione e disattivazione del supporto per l'autenticazione di accensione della protezione incorporata a pagina 48"
  - "Assegnazione di un nome a una Java card a pagina 40"
  - "Drive Encryption for HP ProtectTools a pagina 53"
- DriveLock contribuisce a impedire l'accesso ai dati anche nel caso in cui il disco rigido venga fisicamente smontato e reinstallato in un sistema non protetto. Vedere "Abilitare e disabilitare la protezione DriveLock dell'unità disco rigido a pagina 49".
- La funzione Personal Secure Drive, inclusa nel modulo Embedded Security for HP ProtectTools, consente di crittografare i dati sensibili per impedirne l'accesso senza autenticazione. Vedere le seguenti procedure:
  - Embedded Security "Procedure di installazione a pagina 29"
  - "Uso dell'unità personale protetta (PSD) a pagina 32"

Limitazione dell'accesso ai dati sensibili

Si supponga che un revisore dei conti in appalto lavora in loco ed ha accesso ai computer per la revisione dei dati finanziari sensibili: non si desidera che il revisore sia in grado di stampare i file o salvarli su un supporto scrivibile come un CD. La seguente funzione contribuisce a limitare l'accesso ai dati:

- DriveLock contribuisce a impedire l'accesso ai dati anche nel caso in cui il disco rigido venga fisicamente smontato e reinstallato in un sistema non protetto. Vedere "Abilitare e disabilitare la protezione DriveLock dell'unità disco rigido a pagina 49".

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

Se un PC contenente dati riservati e informazioni sui clienti risulta accessibile dall'interno o dall'esterno della sede, degli utenti non autorizzati potrebbero riuscire a introdursi nelle risorse della rete aziendale oppure ai dati dei servizi finanziari, alle informazioni gestionali o dei reparti di Ricerca & Sviluppo o,

ancora, alle informazioni personali, come ad esempio le cartelle cliniche dei pazienti o ai dati finanziari personali. Le funzioni indicate di seguito consentono di bloccare gli accessi non autorizzati:

- Se abilitata, la funzione di autenticazione al preavvio impedisce l'accesso al sistema operativo. Vedere le seguenti procedure:
  - "Attivazione e disattivazione del supporto per l'autenticazione all'accensione delle smart card a pagina 47"
  - "Attivazione e disattivazione del supporto per l'autenticazione di accensione della protezione incorporata a pagina 48"
  - "Assegnazione di un nome a una Java card a pagina 40"
  - "Drive Encryption for HP ProtectTools a pagina 53"
- Embedded Security for HP ProtectTools protegge i dati sensibili le credenziali memorizzate a livello locale in un PC utilizzando le seguenti procedure.
  - Embedded Security "Procedure di installazione a pagina 29"
  - "Uso dell'unità personale protetta (PSD) a pagina 32"
- Credential Manager for HP ProtectTools aiuta a impedire che utenti non autorizzati possano ottenere le password o accedere alle applicazioni protette da password. A tale scopo, utilizza le seguenti procedure:
  - Credential Manager "Procedure di installazione a pagina 12"
  - "Uso di Single Sign-on a pagina 18"
- La funzione Personal Secure Drive utilizza le seguenti procedure per crittografare i dati sensibili in modo da impedirne l'accesso senza autenticazione.
  - Embedded Security "Procedure di installazione a pagina 29"
  - "Uso dell'unità personale protetta (PSD) a pagina 32"

Creazione di criteri per password sicure

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

- Credential Manager "Procedure di installazione a pagina 12"
- "Uso di Single Sign-on a pagina 18"

Per garantire ancora più sicurezza, Embedded Security for HP ProtectTools protegge il deposito dei nomi utente e delle password. In questo modo, gli utenti potranno utilizzare molte password protette senza doverle memorizzare o annotare per iscritto. Vedere Embedded Security "Procedure di installazione a pagina 29."

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 per la protezione: stabilisce il livello di protezione per l'azienda o la rete e decide quali funzioni di protezione utilizzare, come Java™ Card, lettori biometrici o token USB.

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

- Amministratore IT: applica e gestisce le funzioni di protezione decise dal responsabile per la protezione. Può anche attivare e disattivare alcune funzioni. Ad esempio, se il responsabile per la protezione ha deciso di utilizzare le Java Card, l'amministratore IT può attivare la modalità di protezione del BIOS con Java Card.

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

Gestione delle password di HP ProtectTools

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

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

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

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

Creazione di una password di protezione

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

- Scegliere password che contengano più di 6 caratteri, preferibilmente più di 8.
- Scegliere una password che contenga sia maiuscole che minuscole.
- Se possibile, usare una combinazione di caratteri alfanumerici e aggiungere caratteri speciali e segni di punteggiatura.
- Sostituire alcune lettere di una parola chiave con caratteri speciali o numeri. Ad esempio, è possibile sostituire la lettera I o L con il numero 1.
- Usare una combinazione di parole appartenenti a 2 o più lingue diverse.
- Inserire numeri o caratteri speciali all'interno di una parola o frase. Ad esempio, "Maria2-2Gatto45".
- Scegliere una password non elencata nel dizionario.
- Non utilizzare il proprio nome o altre informazioni personali, come la data di nascita, il nome dei propri animali domestici, o il cognome da nubile della propria madre, nemmeno se digitato in senso inverso.
- Modificare le password regolarmente. È possibile modificare solo un paio di caratteri, ad esempio incrementandoli.
- Se si annota la password, non conservarla in un luogo facilmente visibile in prossimità del computer.
- Non salvare la password in un file, come ad esempio un messaggio di posta elettronica, nel computer.
- Non condividere account e non rivelare a nessuno la password.

Backup e ripristino di HP ProtectTools

HP ProtectTools Backup and Restore costituisce un modo rapido e comodo per effettuare il backup e il ripristino delle credenziali di tutti i moduli di HP ProtectTools supportati.

Backup di credenziali e impostazioni

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

- Utilizzare Backup guidato di HP ProtectTools per selezionare i moduli HP ProtectTools ed eseguirne il backup
- Effettuare il backup di moduli HP ProtectTools preselezionati

NOTA: Per utilizzare questo metodo è necessario che le opzioni di backup siano impostate.

- Pianificare i backup

NOTA: Per utilizzare questo metodo è necessario che le opzioni di backup siano impostate.

Utilizzo di Backup guidato di HP ProtectTools per selezionare i moduli HP ProtectTools ed eseguirne il backup

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro a sinistra fare clic su **HP ProtectTools** e quindi su **Backup and Restore** (Backup e ripristino).
3. Nel riquadro a destra fare clic su **Backup Options** (Opzioni backup). Si apre la finestra Backup guidato di HP ProtectTools. Seguire le istruzioni visualizzate per effettuare il backup delle credenziali.

Impostazione delle opzioni di backup

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro a sinistra fare clic su **HP ProtectTools** e quindi su **Backup and Restore** (Backup e ripristino).
3. Nel riquadro a destra fare clic su **Backup Options** (Opzioni backup). Si apre la finestra Backup guidato di HP ProtectTools.
4. Seguire le istruzioni visualizzate.
5. Dopo avere impostato e confermato la **Password del file di memorizzazione**, selezionare **Remember all passwords and authentication values** (Memorizza tutte le password e i valori di autenticazione) che consentirà in futuro di effettuare backup automatici.
6. Fare clic su **Save Settings** (Salva impostazioni), quindi su **Fine**.

Backup di moduli HP ProtectTools preselezionati

NOTA: Per utilizzare questo metodo è necessario che le opzioni di backup siano impostate.

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro a sinistra fare clic su **HP ProtectTools** e quindi su **Backup and Restore** (Backup e ripristino).
3. Nel riquadro di destra, fare clic su **Backup**.

Pianificazione dei backup

NOTA: Per utilizzare questo metodo è necessario che le opzioni di backup siano impostate.

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro a sinistra fare clic su **HP ProtectTools** e quindi su **Backup and Restore** (Backup e ripristino).
3. Nel riquadro a destra fare clic su **Schedule Backups** (Programma backup).
4. Nella scheda **Task** (Attività) selezionare la casella di controllo **Enabled** (Abilitato) per attivare i backup programmati.
5. Fare clic su **Set Password** (Imposta password), quindi digitare e confermare la password nella finestra di dialogo **Set Password** (Imposta password). Fare clic su **OK**.
6. Fare clic su **Applica**. Fare clic sulla scheda **Schedule** (Programma). Fare clic sulla freccia **Schedule Task** (Programma attività) e selezionare la frequenza dei backup automatici.
7. In **Start time** (Ora di avvio) utilizzare le frecce **Start time** (Ora di avvio) per selezionare l'ora precisa in cui dare inizio al backup.

8. Fare clic su **Advanced** (Avanzate) per selezionare la data di inizio, la data di fine e le impostazioni per le attività ripetitive. Fare clic su **Applica**.

9. Fare clic su **Settings**(Impostazioni) e selezionare le impostazioni per **Scheduled Task Completed** (Attività programmata completata), **Idle Time** (Tempo di pausa) e **Risparmio energia**.

10. Per chiudere la finestra di dialogo, fare clic su **Applica** e quindi su **OK**.

Ripristino delle credenziali

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.

2. Nel riquadro a sinistra fare clic su **HP ProtectTools** e quindi su **Backup and Restore** (Backup e ripristino).

3. Nel riquadro di destra, fare clic su **Restore** (Ripristina). Si apre la finestra Ripristino guidato di HP ProtectTools. Seguire le istruzioni visualizzate.

Configurazione delle impostazioni

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.

2. Nel riquadro a sinistra fare clic su **HP ProtectTools** e quindi su **Impostazioni**.

3. Nel riquadro a destra selezionare le impostazioni desiderate e fare clic su **OK**.

2 Credential Manager for HP ProtectTools

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

- Alternative alle password nella procedura di accesso a Windows, come ad esempio l'utilizzo di una Java Card o di un lettore biometrico per accedere a Windows. Per ulteriori informazioni, consultare la sezione Registrazione delle credenziali a pagina 13.
- Funzione Single Sign-on che ricorda automaticamente le credenziali per i siti Web, le applicazioni e le risorse di rete protette.
- Supporto per dispositivi di protezione opzionali, come ad esempio le Java Card e i lettori biometrici.
- Supporto per impostazioni di protezione aggiuntive, come la richiesta di autenticazione mediante un dispositivo di protezione opzionale per sbloccare il computer.

Procedure di installazione

Accesso a Credential Manager

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

- Accesso guidato a Credential Manager (consigliato)
- Icona HP ProtectTools Security Manager nell'area di notifica
- HP ProtectTools Security Manager

NOTA: Se per accedere a Credential Manager viene utilizzata la richiesta di accesso a Credential Manager sulla schermata di accesso a Windows, si effettua contemporaneamente l'accesso a Windows.

La prima volta che si apre Credential Manager, accedere utilizzando la password di accesso a Windows. Un account di Credential Manager viene quindi automaticamente creato con le credenziali di accesso a Windows.

Dopo aver effettuato l'accesso a Credential Manager, è possibile registrare credenziali aggiuntive, come un'impronta digitale o una Java Card. Per ulteriori informazioni, consultare la sezione Registrazione delle credenziali a pagina 13.

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

Uso della procedura di accesso guidato a Credential Manager

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

1. Aprire la procedura di accesso guidato a Credential Manager con uno dei seguenti metodi:
   - Dalla schermata di accesso a Windows
   - Dall'area di notifica, facendo doppio clic sull'icona **HP ProtectTools Security Manager**
   - Dalla pagina "Credential Manager" di ProtectTools Security Manager, facendo clic sul collegamento **Accedi a** nell'angolo superiore destro della finestra
2. Seguire le istruzioni visualizzate per accedere a Credential Manager.

Primo accesso

Prima di iniziare, è necessario accedere a Windows con un account amministratore, ma senza accedere a Credential Manager.

1. Aprire HP ProtectTools Security Manager facendo doppio clic sull'icona HP ProtectTools Security Manager nell'area di notifica. Si apre la finestra HP ProtectTools Security Manager.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi fare doppio clic su **Accedi a** nell'angolo superiore destro del riquadro di destra. Si apre la schermata di accesso guidato a Credential Manager.
3. Immettere la password di Windows nel campo **Password**, quindi fare clic su **Avanti**.

Registrazione delle credenziali

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

Registrazione delle impronte digitali

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

Configurazione del lettore di impronte digitali

1. Dopo aver effettuato l'accesso a Credential Manager, passare il dito sul lettore di impronte digitali. Si apre la procedura guidata per la registrazione di Credential Manager.
2. Seguire le istruzioni visualizzate per completare la registrazione delle impronte digitali e impostare il lettore delle impronte digitali.
3. Per impostare il lettore di impronte digitali per un altro utente Windows, accedere a Windows con quel nome utente e ripetere i passaggi 1 e 2.

Utilizzo dell'impronta digitale registrata per accedere a Windows

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

Registrazione di una Java Card, di un eToken USB o di un token virtuale

NOTA: È necessario disporre di un lettore di schede o una tastiera Smart Card configurato per questa procedura. Se si sceglie di non utilizzare una Smart Card, è possibile registrare un token virtuale come descritto in "Creazione di un token virtuale a pagina 15."

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**.
3. Nel riquadro di destra, fare clic su **Register Smart Card or Token** (Registra smart card o token). Si apre la procedura guidata per la registrazione di Credential Manager.
4. Seguire le istruzioni visualizzate.

Registrazione di un eToken USB

1. Accertarsi che i driver per eToken USB siano installati.

   NOTA: Per ulteriori informazioni, consultare la guida per l'utente di eToken USB.

2. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
3. Nel riquadro di sinistra, fare clic su **Credential Manager**.
4. Nel riquadro di destra, fare clic su **Register Smart Card or Token** (Registra smart card o token). Si apre la procedura guidata per la registrazione di Credential Manager.
5. Seguire le istruzioni visualizzate.

Registrazione di altre credenziali

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**.
3. Nel riquadro di destra fare clic su **Register Credentials** (Registra credenziali). Si apre la procedura guidata per la registrazione di Credential Manager.
4. Seguire le istruzioni visualizzate.

Attività generali

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

- Creazione di un token virtuale
- Modifica della password di accesso a Windows
- Gestione di un PIN del token
- Gestione dell'identità
- Blocco del computer

NOTA: Questa opzione è disponibile solo se la richiesta di accesso classica a Credential Manager è abilitata. Vedere "Esempio 1: uso della pagina "Advanced Settings" (Impostazioni avanzate) per consentire l'accesso a Windows da Credential Manager a pagina 25".

Creazione di un token virtuale

Il token virtuale funziona in modo molto simile a una Java Card o a un eToken USB. Il token viene salvato nell'unità disco rigido del computer oppure nel registro di sistema di Windows. Quando si accede con un token virtuale, viene richiesto un PIN utente per completare l'autenticazione.

Per creare un nuovo token virtuale:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**.
3. Nel riquadro di destra, fare clic su **Virtual Token** (Token virtuale). Si apre la procedura guidata per la registrazione di Credential Manager.

NOTA: Se l'opzione **Virtual Token** (Token virtuale) non è disponibile, utilizzare la procedura per "Registrazione di altre credenziali a pagina 14".

4. Seguire le istruzioni visualizzate.

Modifica della password di accesso a Windows

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**.
3. Nel riquadro di destra fare clic su **Change Windows Password** (Modifica password di Windows).
4. Immettere la vecchia password nel campo **Password vecchia**.
5. Digitare la nuova password nei campi **Nuova password** e **Conferma password**.
6. Fare clic su **Fine**.

Modifica di un PIN del token

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**.
3. Nel riquadro di destra fare clic su **Change Token PIN** (Modifica PIN del token).

4. Selezionare il token del quale si desidera modificare il PIN, quindi fare clic su **Avanti**.
5. Seguire le istruzioni visualizzate per completare la modifica del PIN.

Gestione dell'identità

Cancellazione di un'identità dal sistema

NOTA: Questa operazione non modifica l'account utente Windows.

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**.
3. Nel riquadro di destra fare clic su **Clear Identity for this Account** (Cancella identità per questo account).
4. Fare clic su **Sì** nella finestra di dialogo di conferma. L'identità viene quindi disconnessa e rimossa dal sistema.

Blocco del computer

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

NOTA: Questa opzione è disponibile solo se la richiesta di accesso classica a Credential Manager è abilitata. Vedere "Esempio 1: uso della pagina "Advanced Settings" (Impostazioni avanzate) per consentire l'accesso a Windows da Credential Manager a pagina 25".

A garanzia di maggior protezione, è possibile configurare la funzione Lock Workstation (Blocca workstation) per la richiesta di una Java Card, di un lettore biometrico o di un token per sbloccare il computer. Per ulteriori informazioni, vedere "Configurazione delle impostazioni di Credential Manager a pagina 25."

Per bloccare il computer:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**.
3. Nel riquadro di destra fare clic su **Lock Workstation** (Blocca workstation). Viene visualizzata la schermata di accesso a Windows. Per sbloccare il computer, è necessario utilizzare una password di Windows o la procedura di accesso guidato a Credential Manager.

Utilizzo dell'accesso a Windows

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

Accesso a Windows con Credential Manager

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

1. Se per accedere a Windows sono state registrate le impronte digitali, passare il dito per effettuare l'accesso.
2. Se non sono state registrate impronte digitali, fare clic sull'icona della tastiera nell'angolo superiore sinistro della schermata accanto all'icona delle impronte digitali. Si apre la schermata di accesso guidato a Credential Manager.
3. Fare clic sulla freccia **User name** (Nome utente) e fare clic sul nome dell'utente.
4. Digitare la password nella casella **Password**, quindi fare clic su **Avanti**.
5. Selezionare **More > Wizard Options** (Altro - Opzioni procedura guidata).
   a. Se si desidera che il nome utente venga impostato come default per il successivo accesso al computer, selezionare la casella di controllo **Use last user name on next logon** (Utilizza l'ultimo nome al prossimo accesso).
   b. Se si desidera che questo criterio di accesso venga impostato come default, selezionare la casella di controllo **Use last policy on next logon** (Utilizza l'ultimo criterio al prossimo accesso).
6. Seguire le istruzioni visualizzate. Se le informazioni di autenticazione sono corrette, si effettua l'accesso all'account Windows e a Credential Manager.

Aggiunta di un account

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra fare clic su **Accesso a Windows**, quindi su **Add a Network Account** (Aggiungi account di rete). Viene aperta la procedura guidata per l'aggiunta di un account di rete.
4. Seguire le istruzioni visualizzate.

Rimozione di un account

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra fare clic su **Accesso a Windows**, quindi su **Manage Network Accounts** (Gestisci account di rete). Viene visualizzata la finestra di dialogo **Manage Network Accounts** (Gestisci account di rete).
4. Fare clic sull'account che si desidera rimuovere, quindi fare clic su **Rimuovi**.
5. Fare clic su **Sì** nella finestra di dialogo di conferma.
6. Fare clic su **OK**.

Uso di Single Sign-on

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

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

NOTA: È inoltre possibile configurare Single Sign-On per convalidare le credenziali di autenticazione con una Java Card, un lettore di impronte digitali o un token, prima di effettuare l'accesso a un sito o a un programma protetto. È utile soprattutto quando si accede a programmi o siti Web che contengono informazioni personali, come numeri di conto bancario. Per ulteriori informazioni, consultare la sezione Configurazione delle impostazioni di Credential Manager a pagina 25.

Registrazione di una nuova applicazione

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

Uso della registrazione automatica

1. Aprire un'applicazione che richieda l'accesso.
2. Fare clic sull'icona Credential Manager SSO nella finestra di dialogo della password per il programma o il sito Web.
3. Digitare la password per il programma o il sito Web e fare clic su **OK**. Viene visualizzata la finestra di dialogo **Credential Manager Single Sign On**.

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

Uso della registrazione manuale (trascinamento)

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra fare clic su **Single Sign On** (Single Sign-On), quindi su **Register New Application** (Registra nuova applicazione). Si avvia la procedura guidata per le applicazioni SSO.
4. Seguire le istruzioni visualizzate.

Gestione di applicazioni e credenziali

Modifica delle proprietà dell'applicazione

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra, in **Single Sign On** fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).
4. Fare clic sulla voce dell'applicazione che si desidera modificare, quindi fare clic su **Proprietà**.
5. Fare clic sulla scheda **Generale** per modificare il nome e la descrizione dell'applicazione. Modificare le impostazioni selezionando o deselezionando le caselle di controllo corrispondenti alle impostazioni appropriate.
6. Fare clic sulla scheda **Script** per visualizzare e modificare lo script dell'applicazione SSO.
7. Fare clic su **OK**.

Rimozione di un'applicazione da Single Sign-On

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra, in **Single Sign On** fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).
4. Fare clic sulla voce dell'applicazione che si desidera rimuovere, quindi fare clic su **Rimuovi**.
5. Fare clic su **Sì** nella finestra di dialogo di conferma.
6. Fare clic su **OK**.

Esportazione di un'applicazione

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

Per esportare un'applicazione:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra, in **Single Sign On** fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).
4. Fare clic sulla voce relativa all'applicazione che si desidera esportare. Quindi, fare clic su **More > Applications > Export Script** (Altro – Applicazioni – Esporta script).
5. Seguire le istruzioni visualizzate per completare l'esportazione.
6. Fare clic su **OK**.

Importazione di un'applicazione

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra, in **Single Sign On** fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).
4. Fare clic sulla voce relativa all'applicazione che si desidera importare. Quindi, selezionare **More > Applications > Import Script** (Altro – Applicazioni – Importa script).
5. Seguire le istruzioni visualizzate per completare l'importazione.
6. Fare clic su **OK**.

Modifica delle credenziali

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra, in **Single Sign On** fare clic su **Manage Applications and Credentials** (Gestisci applicazioni e credenziali).
4. Fare clic sulla voce dell'applicazione che si desidera modificare, quindi fare clic su **More** (Altro).
5. Selezionare una delle seguenti opzioni:
   - Applicazioni
     - Add New (Aggiungi nuova)
     - Rimuovi
     - Proprietà

- Import Script (Importa script)
- Export Script (Esporta script)

- Credenziali
  - Create New (Crea nuova)
- View Password (Visualizza password)

NOTA: È necessario autenticare l'identità prima di visualizzare la password.

6. Seguire le istruzioni visualizzate.
7. Fare clic su **OK**.

Utilizzo della protezione applicazioni

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

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

Limitazione dell'accesso a un'applicazione

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra, in **Application Protection** (Protezione delle applicazioni), fare clic su **Manage Protected Applications** (Gestisci applicazioni protette). Viene visualizzata la finestra di dialogo **Application Protection Service** (Servizio di protezione delle applicazioni).
4. Selezionare una categoria di utente per cui si desidera gestire l'accesso.

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

5. Fare clic su **Aggiungi**. Viene aperta la procedura guidata per l'aggiunta di un programma.
6. Seguire le istruzioni visualizzate.

Rimozione della protezione da un'applicazione

Per rimuovere le limitazioni da un'applicazione:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra, in **Application Protection** (Protezione delle applicazioni), fare clic su **Manage Protected Applications** (Gestisci applicazioni protette). Viene visualizzata la finestra di dialogo **Application Protection Service** (Servizio di protezione delle applicazioni).
4. Selezionare una categoria di utente per cui si desidera gestire l'accesso.

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

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

Modifica delle impostazioni di limitazione per un'applicazione protetta

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Credential Manager**, quindi selezionare **Servizi e applicazioni**.
3. Nel riquadro di destra, in **Application Protection** (Protezione delle applicazioni), fare clic su **Manage Protected Applications** (Gestisci applicazioni protette). Viene visualizzata la finestra di dialogo **Application Protection Service** (Servizio di protezione delle applicazioni).
4. Selezionare una categoria di utente per cui si desidera gestire l'accesso.

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

5. Fare clic sull'applicazione da modificare, quindi fare clic su **Proprietà**. Viene visualizzata la finestra di dialogo **Proprietà** relativa all'applicazione selezionata.
6. Fare clic sulla scheda **Generale**. Selezionare una delle seguenti impostazioni:
   - Disabled (Cannot be used) (Disabilitato - Non utilizzabile)
   - Enabled (Can be used without restrictions) (Abilitato - Utilizzabile senza limitazioni))
   - Restricted (Usage depends on settings) (Limitato - L'utilizzo dipende dalle impostazioni)
7. Se si seleziona l'utilizzo limitato, sono disponibili le seguenti impostazioni:
   a. Per limitare l'utilizzo in base all'ora, al giorno o alla data, fare clic sulla scheda **Programma** e configurare le impostazioni.
   b. Per limitare l'accesso in base all'inattività, fare clic sulla scheda **Avanzate** e selezionare il periodo di inattività.
8. Per chiudere la finestra di dialogo **Proprietà** dell'applicazione, fare clic su **OK**.
9. Fare clic su **OK**.

Attività avanzate (riservate all'amministratore)

Le pagine "Authentication and Credentials" (Autenticazione e credenziali) e "Advanced Settings" (Impostazioni avanzate) di Credential Manager sono accessibili esclusivamente agli utenti dotati dei privilegi di amministratore. Da queste pagine è possibile effettuare le seguenti operazioni:

- Definizione della modalità di accesso per utenti e amministratori
- Configurazione di requisiti di autenticazione personalizzati
- Configurazione delle proprietà delle credenziali
- Configurazione delle impostazioni di Credential Manager

Definizione della modalità di accesso per utenti e amministratori

Nella pagina "Authentication and Credentials" (Autenticazione e credenziali), è possibile specificare quale tipo o combinazione di credenziali sono richiesti per utenti o amministratori.

Per definire la modalità di accesso per utenti e amministratori:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**, quindi selezionare **Authentication and Credentials** (Autenticazione e credenziali).
3. Nel riquadro di destra, fare clic sulla scheda **Authentication** (Autenticazione).
4. Fare clic sulla categoria [**Users** (Utenti) o **Administrators** (Amministratori)] nell'elenco delle categorie.
5. Nell'elenco fare clic sul tipo o combinazione di metodi di autenticazione.
6. Fare clic su **Applica**, quindi su **OK**.

Configurazione di requisiti di autenticazione personalizzati

Se la serie di credenziali di autenticazione desiderata non è presente nell'elenco della scheda di autenticazione nella pagina "Authentication and Credentials" (Autenticazione e credenziali), è possibile creare requisiti personalizzati.

Per configurare i requisiti personalizzati:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**, quindi selezionare **Authentication and Credentials** (Autenticazione e credenziali).
3. Nel riquadro di destra, fare clic sulla scheda **Authentication** (Autenticazione).
4. Fare clic sulla categoria [**Users** (Utenti) o **Administrators** (Amministratori)] nell'elenco delle categorie.
5. Fare clic su **Custom** (Personalizzato) nell'elenco dei metodi di autenticazione.
6. Fare clic su **Configura**.
7. Selezionare i metodi di autenticazione che si desidera utilizzare.
8. Scegliere la combinazione di metodi facendo clic su una delle seguenti opzioni:
   - Uso dell'operatore AND per eseguire la combinazione dei metodi di autenticazione

     (Ad ogni accesso, gli utenti dovranno autenticarsi con tutti i metodi selezionati).
   - Utilizzare OR per richiedere uno dei due o più metodi di autenticazione

     (Ad ogni accesso, gli utenti potranno scegliere uno dei metodi selezionati).
9. Fare clic su **OK**.
10. Fare clic su **Applica**, quindi su **OK**.

Configurazione delle proprietà delle credenziali

Nella scheda delle credenziali della pagina "Authentication and Credentials" (Autenticazione e credenziali), è possibile visualizzare l'elenco dei metodi di autenticazione disponibili e modificare le impostazioni.

Per configurare le credenziali:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**, quindi selezionare **Authentication and Credentials** (Autenticazione e credenziali).
3. Nel riquadro di destra, fare clic sulla scheda **Credentials** (Credenziali).

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

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

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

Configurazione delle impostazioni di Credential Manager

Dalla pagina "Impostazioni" è possibile accedere a varie impostazioni e modificarle utilizzando le seguenti schede:

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

Per modificare le impostazioni di Credential Manager:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**, quindi selezionare **Impostazioni**.
3. Nel riquadro di destra, fare clic sulla scheda appropriata per le impostazioni che si desidera modificare.
4. Seguire le istruzioni visualizzate per modificare le impostazioni.
5. Fare clic su **Applica**, quindi su **OK**.

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

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Credential Manager**, quindi selezionare **Impostazioni**.
3. Nel riquadro di destra, fare clic sulla scheda **Generale**.
4. In **Select the way users log on to Windows (requires restart)** (Seleziona il metodo di accesso a Windows – È necessario riavviare), selezionare la casella di controllo **Use Credential Manager with classic logon prompt** (Utilizza Credential Manager con la richiesta di avvio classico).
5. Fare clic su **Applica**, quindi su **OK**.
6. Riavviare il computer.

NOTA: Selezionando la casella di controllo **Use Credential Manager with classic logon prompt** (Utilizza Credential Manager con la richiesta di avvio classico) è possibile bloccare il computer. Vedere "Blocco del computer a pagina 17".

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

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

3 Embedded Security for HP ProtectTools

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

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

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

Il chip di protezione incorporata TPM potenzia e attiva altre funzioni di protezione di HP ProtectTools Security Manager. Ad esempio, Credential Manager for HP ProtectTools è in grado di utilizzare il chip incorporato come fattore di autenticazione quando l'utente effettua l'accesso a Windows. In determinati modelli, il chip di protezione incorporata TPM attiva anche le funzionalità di protezione del BIOS potenziate, alle quali è possibile accedere mediante BIOS Configuration for HP ProtectTools.

Procedure di installazione

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

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

Attivazione del chip di protezione incorporata

È necessario attivare il chip di protezione incorporata nell'utilità Impostazione del computer. Non è possibile eseguire questa procedura in BIOS Configuration for HP ProtectTools.

Per attivare il chip di protezione incorporata:

1. Aprire Computer Setup avviando o riavviando il computer e quindi premendo F10 mentre nell'angolo in basso a sinistra dello schermo è visualizzato il messaggio "F10 = Setup su base ROM".
2. Se non è stata impostata una password di amministratore, utilizzare i tasti freccia per selezionare **Security > Setup password** (Protezione – Imposta password) quindi premere Invio.
3. Immettere la password nelle caselle **New Password** (Nuova password) e **Verify new password** (Verifica nuova password), quindi premere F10.
4. Nel menu **Protezione**, utilizzare i tasti freccia per selezionare **TPM protezione integrata**, quindi premere invio.
5. Se la periferica è nascosta, in **Protezione integrata** selezionare **Available** (Disponibile).
6. Selezionare **Embedded security device state** (Stato della periferica di protezione incorporata) e modificarlo in **Enable** (Attivo).
7. Premere F10 per accettare le modifiche alla configurazione di Embedded Security.
8. Per salvare le preferenze e uscire da Computer Setup, utilizzare i tasti freccia per selezionare **File > Save Changes and Exit** (Salva modifiche ed esci). Quindi, seguire le istruzioni visualizzate.

Inizializzazione del chip di protezione incorporata

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

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

Per inizializzare il chip di protezione incorporata:

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

   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 Embedded Security non è aperta, selezionare **Start > Tutti i programmi > 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 la posta elettronica protetta, è prima necessario configurare il client di posta elettronica per l'uso di un certificato digitale creato con Protezione integrata. Se non si dispone di un certificato digitale, occorre ottenerne uno da un'autorità di certificazione. Per informazioni sulla configurazione della posta elettronica e l'ottenimento di un certificato digitale, consultare la Guida in linea del client di posta elettronica.

Attività generali

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

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

Uso dell'unità personale protetta (PSD)

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

Crittografia di file e cartelle

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

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

Per crittografare file e cartelle:

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

Invio e ricezione di posta elettronica crittografata

Protezione integrata consente di inviare e ricevere posta elettronica crittografata, ma le procedure variano a seconda del programma utilizzato per accedere alla posta elettronica. Per ulteriori informazioni, consultare la Guida in linea per la protezione incorporata e la Guida in linea per la posta elettronica.

Modifica della password chiave utente di base

Per modificare la password chiave utente di base:

1. Selezionare **Start > Tutti i programmi > 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 Key password** (Password chiave utente di base), fare clic su **Change** (Cambia).
4. Immettere la vecchia password, quindi impostare e confermare la nuova password.
5. Fare clic su **OK**.

Attività avanzate

Backup e ripristino

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

Creazione di un file di backup

Per creare un file di backup:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Backup**.
3. Nel riquadro destro, fare clic su **Backup**. Viene avviata la procedura guidata di backup di Embedded Security.
4. Seguire le istruzioni visualizzate.

Ripristino dei dati relativi alla certificazione dal file di backup

Per ripristinare dati dal file di backup:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Backup**.
3. Nel riquadro destro, fare clic su **Restore** (Ripristina). Viene avviata la procedura guidata di backup Embedded Security.
4. Seguire le istruzioni visualizzate.

Modifica della password proprietario

Per modificare la password proprietario:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
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 guidare l'utente nel ripristino di una password. Per ulteriori informazioni, consultare la Guida in linea.

Attivazione e disattivazione di Protezione integrata

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

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

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

Disattivazione definitiva di Protezione integrata

Per disattivare definitivamente Protezione integrata:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Avanzate**.
3. Nel riquadro di destra, in **Protezione integrata**, fare clic su **Disable** (Disattiva).
4. Alla richiesta, immettere la password proprietario, quindi fare clic su **OK**.

Attivazione di Protezione integrata dopo la disattivazione definitiva

Per attivare Protezione integrata dopo la disattivazione definitiva:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Protezione integrata**, quindi su **Avanzate**.
3. Nel riquadro di destra, in **Protezione integrata**, fare clic su **Enable** (Attiva).
4. Alla richiesta, immettere la password proprietario, quindi fare clic su **OK**.

Migrazione delle chiavi con Migrazione guidata

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

Per informazioni sulla migrazione, consultare la Guida in linea di Protezione integrata.

4 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools gestisce l'impostazione e la configurazione delle Java card per i computer dotati di un lettore di Java Card opzionale.

Con Java Card Security sono disponibili le seguenti funzioni:

- Accesso alle funzioni di Java Card Security
- Opera in combinazione con l'utilità Impostazione del computer per attivare l'autenticazione delle Java Card al momento dell'accensione.
- Configura Java Card separate per amministratore e utente. Per consentire il caricamento del sistema, l'utente dovrà quindi inserire la Java card e un PIN.
- Impostare e modificare il PIN utilizzato per autenticare gli utenti della Java card

Attività generali

La pagina "Generale" consente di effettuare le seguenti attività:

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

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

Modifica di un PIN Java card

Per modificare un PIN Java card:

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

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Generale**.
3. Inserire una Java card (con un PIN esistente) nel lettore.
4. Nel riquadro di destra, fare clic su **Change** (Modifica).
5. Nella finestra di dialogo **Modifica PIN**, digitare il PIN corrente nella casella **PIN attuale**.
6. Digitare un nuovo PIN nella casella **Nuovo PIN** e digitarlo nuovamente nella casella **Conferma nuovo PIN**.
7. Fare clic su **OK**.

Selezione del lettore

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

Per selezionare il lettore:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Generale**.
3. Inserire la Java card nel lettore.
4. Nel riquadro di destra, sotto **Selected card reader** (Lettore selezionato), fare clic sul lettore desiderato.

Attività avanzate (solo per amministratori)

La pagina "Avanzate" consente di eseguire le seguenti attività:

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

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

Assegnazione di un PIN Java card

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

Per assegnare un PIN a una Java card:

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

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Avanzate**.
3. Inserire una nuova Java card nel lettore.
4. Quando viene visualizzata la finestra di dialogo **New Card** (Nuova scheda), digitare un nuovo nome nella casella **New display name** (Nuovo nome visualizzato), digitare un nuovo PIN nella casella **Nuovo PIN** e immettere nuovamente il PIN nella casella **Conferma nuovo PIN**.
5. Fare clic su **OK**.

Assegnazione di un nome a una Java card

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

Per assegnare un nome a una Java card:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Avanzate**.
3. Inserire la Java card nel lettore.

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

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

Impostazione di autenticazione di accensione

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

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

1. Abilitare il supporto di autenticazione di accensione della Java card in BIOS Configuration o Impostazione del computer. Per ulteriori informazioni, vedere "Attivazione e disattivazione del supporto per l'autenticazione all'accensione delle smart card a pagina 47."
2. Abilitare la Java card per l'autenticazione di accensione in Java Card Security.
3. Creazione e abilitazione della Java card dell'amministratore.

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

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

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **Java Card Security**, quindi su **Avanzate**.
3. Inserire la Java card nel lettore.

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

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

   oppure

   Se DriveLock è abilitato:

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

      oppure

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

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

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

   c. Digitare il PIN Java card.

   d. Fare clic su **OK**.

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

NOTA: Per ulteriori informazioni, vedere "Backup e ripristino di HP ProtectTools a pagina 8."

Creazione di una Java card utente

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

Per creare una Java card utente:

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

Disabilitazione di una Java card per l'autenticazione di accensione

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

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

5 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools fornisce accesso alle impostazioni di configurazione e di protezione dell'utilità Impostazione del computer. Offre agli utenti l'accesso Windows alle funzioni di protezione del sistema gestite dall'Impostazione del computer.

Con BIOS Configuration è possibile ottenere quanto segue:

- Gestire le password di accensione e dell'amministratore.
- Configurare altre funzioni di autenticazione all'accensione, come l'attivazione del supporto per l'autenticazione della protezione incorporata.
- Attivare e disattivare le funzionalità hardware, come l'avvio da CD-ROM o da altre porte hardware.
- Configurare le opzioni di avvio, tra cui l'attivazione di MultiBoot e la modifica dell'ordine di avvio.

NOTA: Molte delle funzionalità di BIOS Configuration for HP ProtectTools sono disponibili anche in Impostazione del computer.

Attività generali

BIOS Configuration consente di gestire diverse impostazioni del computer che sarebbero altrimenti accessibili solo premendo F10 all'avvio e accedendo all'utility Computer Setup.

Gestione delle opzioni di avvio

È possibile utilizzare BIOS Configuration per gestire varie impostazioni per attività che vengono eseguite all'accensione o al riavvio del computer.

Per gestire le opzioni di avvio:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**.
3. Digitare la password amministratore di Impostazione del computer alla richiesta di immissione della password amministratore del BIOS, quindi fare clic su **OK**.

   NOTA: La richiesta di immissione della password amministratore del BIOS viene visualizzata solo se è stata già impostata la password di Impostazione del computer. Per ulteriori informazioni, sull'impostazione della password di Impostazione del computer, vedere "Configurazione della password di configurazione a pagina 51."

4. Nel riquadro di sinistra, fare clic su **Configurazione di sistema**.
5. Nel riquadro destro, selezionare i ritardi (in secondi) per F9, F10 e F12, quindi per **Express Boot Popup Delay (Sec)** (Ritardo popup avvio espresso (secondi)).
6. Attivare o disattivare **MultiBoot**.
7. Se MultiBoot è attivato, selezionare l'ordine di avvio selezionando un dispositivo di avvio, quindi facendo clic sulla freccia su o giù per impostare l'ordine nell'elenco.
8. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

Attivazione e disattivazione delle opzioni di configurazione del sistema

NOTA: Alcuni degli elementi elencati di seguito potrebbero non essere supportati dal computer in uso.

Per attivare o disattivare le opzioni relative alle periferiche o alla protezione:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**.
3. Digitare la password amministratore di Impostazione del computer alla richiesta di immissione della password amministratore del BIOS, quindi fare clic su **OK**.
4. Nel riquadro di sinistra, fare clic su **Configurazione del sistema**, quindi attivare o disattivare un'opzione di configurazione del sistema, oppure configurare una qualunque delle seguenti opzioni di configurazione del sistema nel riquadro di destra:
   - Opzioni porta
     - Porta seriale
     - Porta a infrarossi
     - Porta parallela
     - Slot SD
     - Porta USB
     - Porta 1394
     - Slot Cardbus
     - Slot ExpressCard
   - Opzioni di avvio
     - Ritardo F9, F10 e F12 Delay (sec.)
     - MultiBoot
     - Ritardo (sec.) avvio veloce
     - Avvio da CD-ROM
     - Avvio da floppy
     - Avvio da adattatore di rete interno
     - Modalità di avvio da adattatore di rete interno (PXE o RPL)
     - Ordine di avvio
   - Configurazioni periferiche
     - Bloc num all'avvio
     - Inversione dei tasti fn/Ctrl
     - Dispositivi di puntamento multipli
     - Supporto USB Legacy
     - Modalità porta parallela (standard, bidirezionale, EPP (Enhanced Parallel Port) o ECP (Enhanced Capabilities Port).

- Protezione dall'esecuzione dei dati
- Modalità SATA nativa
- CPU Dual Core
- Supporto della funzionalità Intel® SpeedStep automatica
- Ventola sempre attiva con alimentazione CA
- Trasferimenti di dati DMA BIOS
- Tecnologia Execution Disable di Intel o AMD PSAE

- Opzioni periferiche integrate
  - Periferica LAN senza fili incorporata
  - Periferica senza fili WAN incorporata
  - Periferica Bluetooth® incorporata
  - Commutazione LAN/WLAN
  - Riattivazione LAN

5. Fare clic su **Applica**, quindi fare clic su **OK** nella finestra di HP ProtectTools per salvare le modifiche e uscire.

Attività avanzate

Gestione delle impostazioni dei moduli aggiuntivi di HP ProtectTools

Alcune funzionalità di HP ProtectTools Security Manager possono essere gestite in BIOS Configuration.

Attivazione e disattivazione del supporto per l'autenticazione all'accensione delle smart card

L'attivazione di questa opzione consente di utilizzare una smart card per l'autenticazione utente all'accensione del computer.

NOTA: Per attivare completamente la funzione di autenticazione all'accensione, occorre anche configurare una smart card utilizzando il modulo Java Card Security for HP ProtectTools.

Per attivare il supporto per l'autenticazione di accensione della smart card:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**.
3. Digitare la password amministratore di Impostazione del computer alla richiesta di immissione della password amministratore del BIOS, quindi fare clic su **OK**.
4. Nel riquadro di sinistra, fare clic su **Protezione**.
5. In **Protezione Smart Card**, fare clic su **Abilita**.

   NOTA: Per disattivare l'autenticazione di accensione delle smart card, fare clic su **Disabilita**.

6. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

Attivazione e disattivazione del supporto per l'autenticazione di accensione della protezione incorporata

L'abilitazione di questa opzione consente al sistema di utilizzare il chip di protezione incorporata TPM (se disponibile) per l'autenticazione utente all'accensione del computer.

NOTA: Per attivare completamente la funzione di autenticazione di accensione, occorre anche configurare il chip di protezione incorporata TPM utilizzando il modulo Embedded Security for HP ProtectTools.

Per attivare il supporto per l'autenticazione di accensione per la protezione incorporata:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**.
3. Digitare la password amministratore di Impostazione del computer alla richiesta di immissione della password amministratore del BIOS, quindi fare clic su **OK**.
4. Nel riquadro di sinistra, fare clic su **Protezione**.
5. In **Protezione incorporata**, fare clic su **Enable Power-on Authentication Support** (Abilita il supporto per l'autenticazione di accensione).

   NOTA: Per attivare l'autenticazione di accensione per la protezione incorporata, fare clic su **Disabilita**.

6. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

Abilitare e disabilitare la protezione DriveLock dell'unità disco rigido

DriveLock è una funzione di sicurezza di standard industriale che impedisce l'accesso non autorizzato ai dati memorizzati su unità disco rigido ATA. DriveLock è stato implementato come estensione di Computer Setup ed è disponibile solo se vengono rilevate unità disco rigido che supportano il set di comandi di protezione ATA. DriveLock è destinato a clienti HP per i quali la sicurezza dei dati è fondamentale. Per tali clienti il costo del disco fisso e la perdita dei dati ivi memorizzati hanno un'importanza secondaria rispetto al danno provocato da un accesso non autorizzato al contenuto. Per bilanciare questo livello di sicurezza con l'esigenza pratica di consentire l'accesso in caso di smarrimento della password, l'implementazione HP di DriveLock utilizza uno schema di sicurezza a doppia password: una deve essere impostata ed utilizzata da un amministratore di sistema, mentre l'altra viene normalmente impostata ed utilizzata dall'utente finale. Non sono previsti accorgimenti per sbloccare l'unità se vengono smarrite entrambe le password. Pertanto, DriveLock risulta maggiormente indicato quando i dati contenuti sul disco fisso vengono replicati su un sistema informatico aziendale o quando ne viene effettuato il backup su base regolare. Se entrambe le password di DriveLock vengono smarrite, il disco fisso viene reso inutilizzabile. Per gli utenti che non presentano questo tipo di esigenza, questo può essere un rischio inaccettabile. Per quelli, invece, che presentano questo tipo di esigenza, il rischio può essere tollerabile, data la natura dei dati memorizzati sul disco.

Uso di DriveLock

Quando vengono rilevate una o più unità disco rigido che supportano il set di comandi di protezione ATA, l'opzione DriveLock compare nel menu Security di Computer Setup. L'utente ha la possibilità di impostare la password principale o di abilitare DriveLock. Per abilitare DriveLock deve essere specificata una password utente. Dal momento che la configurazione iniziale di DriveLock viene normalmente eseguita da un amministratore di sistema, deve essere prima di tutto impostata la password principale. HP invita gli amministratori di sistema ad impostare una password principale sia che prevedano di abilitare DriveLock, sia che prevedano di non abilitarlo. In tal modo gli amministratori avranno la possibilità di modificare le impostazioni di DriveLock se si deciderà di bloccare il disco in un secondo tempo. Una volta impostata la password principale l'amministratore di sistema potrà abilitare o meno DriveLock.

Se è presente un disco fisso bloccato, verrà chiesta la password per sbloccarlo durante il POST. Se viene impostata una password di accensione e quest'ultima coincide con quella dell'utente della periferica, durante il POST non viene richiesto all'utente di reimmettere la password. Diversamente, all'utente viene richiesto di immettere la password per accedere a DriveLock. Dopo un avvio a freddo, è possibile utilizzare la password principale o quella dell'utente. Dopo un avvio a caldo, immettere la stessa password utilizzata per sbloccare l'unità durante il precedente avvio a freddo. Gli utenti hanno a disposizione due tentativi per immettere la password corretta. Se dopo l'avvio a freddo nessun tentativo ha esito positivo, il POST prosegue, ma i dati sull'unità restano inaccessibili. Se dopo l'avvio a freddo o il riavvio da Windows nessun tentativo ha esito positivo, il POST si interromperà e verrà richiesto di spegnere e riaccendere il computer.

Applicazioni di DriveLock

L'utilizzo più pratico della funzione di protezione DriveLock è negli ambienti aziendali. L'amministratore di sistema è responsabile della configurazione dell'unità disco rigido che comporta, tra l'altro, l'impostazione della password principale di DriveLock e una password utente temporanea. Se l'utente dimentica la sua password o la macchina viene ceduta ad un altro impiegato, è possibile utilizzare la password principale per cambiare la password utente e riaccedere al disco.

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

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

Gestione delle password di configurazione del computer

È possibile utilizzare BIOS Configuration per impostare e modificare le password di accensione e di impostazione in Impostazione del computer e per gestire altre impostazioni relative alle password.

△ **ATTENZIONE:** Le password impostate nella pagina "Password" in BIOS Configuration vengono salvate immediatamente dopo aver fatto clic sul pulsante **Applica** o su **OK** nella finestra HP ProtectTools. Assicurarsi di ricordare la password impostata, poiché non sarà possibile annullare un'impostazione della password senza fornire la password precedente.

La password di accensione può impedire l'uso non autorizzato del computer notebook.

NOTA: Una volta impostata una password di accensione, il pulsante Imposta nella pagina "Password" viene sostituito da un pulsante Modifica.

La password di Impostazione del computer protegge le impostazioni di configurazione e le informazioni di identificazione del sistema in Impostazione del computer. Una volta impostata tale password, sarà necessario utilizzarla per accedere a Impostazione del computer. Se è stata già impostata una password di configurazione, quest'ultima verrà richiesta prima di aprire la sezione BIOS Configuration di HP ProtectTools.

NOTA: Una volta impostata una password di configurazione, il pulsante Imposta nella pagina "Password" viene sostituito da un pulsante Modifica.

Configurazione della password di accensione

Per impostare la password di accensione:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**, quindi su **Protezione**.
3. Nel riquadro di destra, accanto a **Password di accensione**, fare clic su **Set** (Imposta).
4. Immettere e confermare la password nelle caselle **Immissione della password** e **Verify Password** (Verifica password).
5. Fare clic su **OK** nella finestra di dialogo **Password**.
6. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

Modifica della password di accensione

Per modificare la password di accensione:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**, quindi su **Protezione**.
3. Nel riquadro di destra, accanto a **Password di accensione**, fare clic su **Change** (Modifica).
4. Immettere la password corrente nella casella **Password vecchia**.
5. Impostare e confermare la nuova password nel campo **Inserire nuova password**.

6. Fare clic su **OK** nella finestra di dialogo **Password**.
7. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

Configurazione della password di configurazione

Per impostare la password di Impostazione del computer:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**, quindi su **Protezione**.
3. Nel riquadro di destra, accanto a **Password di configurazione**, fare clic su **Set** (Imposta).
4. Immettere e confermare la password nelle caselle **Immissione della password** e **Conferma password**.
5. Fare clic su **OK** nella finestra di dialogo **Password**.
6. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

Modifica della password di configurazione

Per modificare la password di Impostazione del computer:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**, quindi su **Protezione**.
3. Nel riquadro di destra, accanto a **Setup Password** (Password di configurazione), fare clic su **Change** (Modifica).
4. Immettere la password corrente nella casella **Password vecchia**.
5. Immettere e confermare la nuova password nelle caselle **Inserire nuova password** e **Verifica la nuova password**.
6. Fare clic su **OK** nella finestra di dialogo **Password**.
7. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

Impostazione delle opzioni password

È possibile utilizzare BIOS Configuration for HP ProtectTools per impostare le opzioni password per ottimizzare la protezione del sistema.

Attivazione e disattivazione della massima sicurezza

△ **ATTENZIONE:** Per evitare che il computer diventi inutilizzabile in modo permanente, annotare la password di configurazione, la password di accensione o il PIN della smart card in un luogo sicuro, lontano dal computer. In mancanza di queste password o del PIN, il computer non può essere sbloccato.

L'abilitazione della massima sicurezza ottimizza la protezione delle password amministratore e di accensione e di altre forme di autenticazione di accensione.

Per attivare o disattivare la massima sicurezza:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**, quindi su **Protezione**.
3. Nel riquadro di destra, in **Opzioni password**, attivare o disattivare **Massima sicurezza**.

NOTA: Se si desidera disattivare la massima sicurezza, deselezionare la casella di controllo **Abilita massima sicurezza**.

4. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

Attivazione e disattivazione dell'autenticazione di accensione al riavvio di Windows

Questa opzione consente di ottimizzare la protezione richiedendo all'utente di digitare una password di accensione, TPM, o smart card al riavvio di Windows.

Per attivare o disattivare l'autenticazione di accensione al riavvio di Windows:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra, fare clic su **BIOS Configuration**, quindi su **Protezione**.
3. Nel riquadro di destra, in **Opzioni password**, abilitare o disabilitare **Richiedi password al riavvio**.
4. Nella finestra di HP ProtectTools fare clic su **Applica** e quindi su **OK**.

6 Drive Encryption for HP ProtectTools

△ **ATTENZIONE:** Prima di disinstallare il modulo Drive Encryption è necessario decrittografare tutte le unità crittografate. In caso contrario, non sarà possibile accedere ai dati presenti nelle unità crittografate, a meno che non siano state registrate con il servizio di recupero Drive Encryption (vedere "Ripristino a pagina 56"). La reinstallazione del modulo Drive Encryption non consentirà di accedere alle unità crittografate.

Encryption management (Gestione crittografia)

Crittografia di un'unità

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Encryption Management** (Gestione crittografia).
3. Nel riquadro di destra, fare clic su **Activate** (Attiva). Viene visualizzata la procedura guidata di Drive Encryption for HP ProtectTools.
4. Seguire le istruzioni visualizzate per attivare la crittografia.

NOTA: Sarà necessario specificare un dischetto, un dispositivo di memorizzazione flash o un altro supporto di memorizzazione USB in cui salvare le informazioni di ripristino.

Change encryption (Modifica crittografia)

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Encryption Management** (Gestione crittografia).
3. Nel riquadro di destra fare clic su **Change encryption** (Modifica crittografia). Nella finestra di dialogo **Change Encryption** (Modifica crittografia) selezionare i dischi da crittografare e fare clic su **OK**.
4. Fare nuovamente clic su **OK** per avviare la crittografia.

Decrittografia di un'unità

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Encryption Management** (Gestione crittografia).
3. Nel riquadro di destra fare clic su **Deactivate** (Disattiva).

Gestione utente

Aggiunta di un utente

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Gestione utente**.
3. Nel riquadro di destra fare clic su **Aggiungi**. Selezionare un nome utente nell'elenco **User name** (Nome utente) oppure digitare il nome dell'utente nella casella **Username** (Nome utente). Fare clic su **Avanti**.
4. Digitare la password di Windows per l'utente selezionato, quindi fare clic su **Avanti**.
5. Selezionare un metodo di autenticazione per il nuovo utente e fare clic su **Fine**.

Rimozione di un utente

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Gestione utente**.
3. Nel riquadro di destra selezionare il nome dell'utente da eliminare nell'elenco **User name** (Nome utente). Fare clic su **Rimuovi**.
4. Fare clic su **Sì** per confermare l'eliminazione.

Change token (Modifica token)

Il metodo di autenticazione viene modificato nel modo seguente:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Gestione utente**.
3. Nel riquadro di destra selezionare un nome utente nell'elenco **User name** (Nome utente) e fare clic su **Change Token** (Modifica token).
4. Digitare la password di Windows per l'utente e fare clic su **Avanti**.
5. Selezionare un nuovo metodo di autenticazione e fare clic su **Fine**.
6. Se come metodo di autenticazione è stata selezionata una Java Card, digitarne la password quando richiesto e fare clic su **OK**.

Set password (Imposta password)

Consente di impostare una password o di modificare il metodo di autenticazione:

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Gestione utente**.
3. Nel riquadro di destra selezionare un utente nell'elenco **User name** (Nome utente) e fare clic su **Set password** (Imposta password).
4. Digitare la password di Windows per l'utente e fare clic su **Avanti**.
5. Selezionare un nuovo metodo di autenticazione e fare clic su **Fine**.
6. Se come metodo di autenticazione è stata selezionata una Java Card, digitarne la password quando richiesto e fare clic su **OK**.

Ripristino

Sono disponibili le due seguenti misure di protezione:

- Se la password viene dimenticata, non sarà possibile accedere alle unità crittografate. Tuttavia, è possibile registrarsi al servizio di recupero Drive Encryption che consentirà di accedere al computer anche nel caso in cui la password venga dimenticata.
- È possibile utilizzare un dischetto, un dispositivo di memorizzazione flash o un altro supporto di memorizzazione USB per eseguire una copia di backup delle chiavi di Drive Encryption.

Registrazione al servizio di recupero Drive Encryption

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Recovery** (Recupero).
3. Nel riquadro di destra fare clic su **Click here to register** (Fare clic qui per registrarsi). Digitare le informazioni richieste per completare la procedura di backup di protezione.

Backup delle chiavi di Drive Encryption

1. Selezionare **Start > Tutti i programmi > HP ProtectTools Security Manager**.
2. Nel riquadro di sinistra fare clic su **Drive Encryption**, quindi selezionare **Recovery** (Recupero).
3. Nel riquadro di destra fare clic su **Click here to backup your keys** (Fare clic qui per il backup delle chiavi).
4. Specificare un dischetto, un dispositivo di memorizzazione flash o un altro supporto di memorizzazione USB in cui salvare le informazioni di ripristino, quindi fare clic su **Avanti**. Viene visualizzata la procedura guidata di Drive Encryption for HP ProtectTools.
5. Seguire le istruzioni visualizzate per effettuare il backup delle chiavi di Drive Encryption.

NOTA: Sarà necessario specificare un dischetto, un dispositivo di memorizzazione flash o un altro supporto di memorizzazione USB in cui salvare le informazioni di ripristino.

7 Risoluzione dei problemi

Credential Manager per ProtectTools

Breve descrizione	Dettagli	Soluzione
Utilizzando l'opzione Network Accounts di Credential Manager, l'utente può selezionare l'account di dominio cui accedere. Quando si utilizza l'autenticazione TPM, questa opzione non è disponibile. Tutti gli altri metodi di autenticazione funzionano correttamente.	Utilizzando l'autenticazione TPM, l'utente accede soltanto al computer locale.	Utilizzando gli strumenti di accesso singolo (Single Sign On) di Credential Manager l'utente ha la possibilità di autenticare altri account.
La credenziale del token USB non è disponibile con l'accesso a Windows XP Service Pack 1	Dopo aver installato il software del token USB, aver registrato le credenziali del token USB e aver impostato Credential Manager come login primario, il token USB non è elencato né disponibile nell'accesso a Credential Manager/gina. Quando si torna a Windows, uscire da Credential Manager, riaccedere a Credential Manager e riselezionare il token come accesso primario. L'operazione di login al token funziona normalmente.	Ciò si verifica soltanto con Windows XP Service Pack 1. Aggiornare la versione di Windows al Service Pack 2 tramite Windows Update per eliminare il problema. Per aggirare il problema se si mantiene Service Pack 1, effettuare nuovamente l'accesso a Windows con un'altra credenziale (password Windows) per uscire e riaccedere in Credential Manager.
Le pagine Web di alcune applicazioni creano errori che impediscono all'utente di eseguire o completare funzioni	Alcune applicazioni di tipo Web smettono di funzionare e riportano errori dovuti alla disabilitazione del tipo di funzionalità di Single Sign On. Ad esempio, in Internet Explorer un **!** in un triangolo giallo appare per segnalare che si è verificato un errore.	Credential Manager Single Sign On non supporta tutte le interfacce software di tipo Web. Disattivare il supporto Single Sign On per quella particolare pagina Web. Vedere la documentazione completa su Single Sign On, disponibile nei file della guida di Credential Manager. Se per una data applicazione non è possibile disabilitare uno specifico supporto Single Sign On, contattare il centro di assistenza HP e richiedere un supporto di terzo livello.
Manca l'opzione **Browse for Virtual Token** (Cerca token virtuale) durante il processo di login.	L'utente non può spostare la posizione di token virtuali registrati in Credential Manager in quanto la possibilità di ricerca è stata rimossa per evitare rischi alla sicurezza.	L'opzione di ricerca è stata rimossa dal prodotto attuale perché consentiva a non utenti di cancellare e rinominare file e di assumere il controllo di Windows.
L'accesso con autenticazione TPM non prevede l'opzione **Network Account** (Account di rete).	Tramite l'opzione **Network Account** (Account di rete), l'utente può selezionare l'account di dominio cui accedere. Quando si utilizza l'autenticazione TPM, questa opzione non è disponibile.	HP sta cercando una soluzione per migliorare il prodotto nel futuro.

Breve descrizione	Dettagli	Soluzione
L'amministratore di dominio non può modificare la password di Windows anche con l'autorizzazione.	Questa situazione si verifica dopo che un amministratore di dominio ha effettuato l'accesso ad un dominio e ne ha registrato l'identità con Credential Manager utilizzando un account con diritti di amministratore su dominio e PC locale. Quando l'amministratore di dominio prova a modificare la password di Windows da Credential Manager, ottiene un errore di accesso non riuscito: **User account restriction** (Restrizione account utente).	Credential Manager non può modificare la password dell'account di un utente di dominio con **Change Windows password** (Modifica password di Windows). Credential Manager può modificare soltanto le password degli account PC locali. L'utente di dominio può modificare la password tramite l'opzione **Windows security** > **Change password** (Sicurezza Windows - Modifica password) ma, dato che non possiede un account fisico sul PC locale, Credential Manager può modificare soltanto la password utilizzata per l'accesso.
Le impostazioni predefinite di Credential Manager Single Sign On dovrebbero essere impostate in modo da essere avvisati ed evitare confusione.	Per impostazione predefinita, Single Sign On viene impostato per consentire l'accesso automatico degli utenti. Tuttavia, quando si crea il secondo documento protetto da password, Credential Manager utilizza l'ultima password registrata (quella del primo documento).	HP sta cercando una soluzione per migliorare il prodotto nel futuro.
Problemi di incompatibilità con la password gina di Corel WordPerfect 12.	Se l'utente entra in Credential Manager, crea un documento in WordPerfect e salva con protezione della password, Credential Manager non è in grado di rilevare o riconoscere – né manualmente né automaticamente – la password gina.	HP sta cercando una soluzione per migliorare il prodotto nel futuro.
Credential Manager non riconosce il pulsante **Connect** (Connetti) sullo schermo.	Se le credenziali Single Sign On per connessione desktop remoto (RDP) sono impostate su **Connect** (Connetti), Single Sign On, al momento del riavvio, immette sempre **Save As** (Salva con nome) anziché **Connect** (Connetti).	HP sta cercando una soluzione per migliorare il prodotto nel futuro.
La procedura guidata di configurazione di ATI Catalyst non è utilizzabile con Credential Manager.	Credential Manager Single Sign On è in conflitto con la procedura guidata di configurazione di ATI Catalyst.	Disabilitare Credential Manager Single Sign On.
Quando si accede utilizzando l'autenticazione TPM, il pulsante **Back** (Indietro) dello schermo salta l'opzione, scegliendo un altro metodo di autenticazione.	Se l'utente che utilizza l'autenticazione d'accesso TPM per Credential Manager immette la password, il pulsante **Back** (Indietro) non funziona correttamente, ma visualizza immediatamente la schermata di accesso di Windows.	HP sta cercando una soluzione per migliorare il prodotto nel futuro.
Credential Manager si apre da standby pur essendo configurato per non farlo.	Se l'opzione **use Credential Manager log on to Windows** (Usa Credential Manager per accedere a Windows) non è selezionata, consentendo al sistema di portarsi in sospensione S3 e riattivandolo si provoca l'apertura del login di Credential Manager su Windows.	Senza password amministratore impostata, l'utente non può accedere a Windows attraverso Credential Manager a causa delle restrizioni account richieste da Credential Manager. • Senza Java Card/token, l'utente può annullare l'accesso di Credential Manager e visualizzare la schermata di accesso di Microsoft Windows. A questo punto l'utente può effettuare l'accesso. • Con Java Card/token, la seguente soluzione permette all'utente di abilitare/disabilitare

Breve descrizione	Dettagli	Soluzione
		l'apertura di Credential Manager all'atto dell'inserimento della Java Card. 1. Fare clic su **Advanced Settings** (Impostazioni avanzate). 2. Fare clic su **Service & Applications** (Assistenza e applicazioni). 3. Fare clic su **Java Cards and Tokens** (Java Card e token). 4. Fare clic quando la Java Card/il token sono stati inseriti. 5. Selezionare la casella di controllo **Advise to log-on** (Avvisa di effettuare l'accesso).
Gli utenti perdono tutte le credenziali di Credential Manager protette dal TPM, nel caso in cui il modulo TPM venga rimosso o sia danneggiato.	Se il modulo TPM viene rimosso o è danneggiato, gli utenti perdono tutte le credenziali protette dal TPM.	Come da progettazione. Il modulo TPM è stato progettato per proteggere le credenziali di Credential Manager. HP consiglia all'utente di effettuare il backup dell'identità da Credential Manager prima di rimuovere il TPM.
Credential Manager non è impostato come accesso primario in Windows 2000.	Durante l'installazione di Windows 2000, la politica di accesso è impostata per il login manuale o automatico da parte dell'amministratore. Se si sceglie l'accesso automatico, le impostazioni di registrazione predefinite di Windows definiscono il valore predefinito per l'accesso automatico da parte dell'amministratore su 1, e Credential Manager non prevale su tale impostazione.	Come da progettazione. Se l'utente desidera modificare le impostazioni di livello del sistema operativo relative ai valori di login automatico dell'amministratore, è necessario che accede al seguente percorso di modifica: `HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/WinLogon`. **ATTENZIONE:** Registry Editor viene utilizzato a proprio rischio! L'utilizzo improprio di Registry Editor (regedit) può comportare gravi problemi che possono richiedere la reinstallazione del sistema operativo. Non vi è garanzia di poter risolvere i problemi derivanti dall'uso improprio di Registry Editor.
Viene visualizzato il messaggio di accesso con impronte digitali indipendentemente dal fatto che sia installato o registrato un lettore di impronte digitali.	Se l'utente seleziona l'accesso di Windows, sulla barra delle applicazioni di Credential Manager appare il seguente allarme desktop: **You can place your finger on the fingerprint reader to log on to Credential Manager.** (Porre il dito sul lettore per accedere a Credential Manager.)	Lo scopo dell'allarme su desktop è quello di segnalare all'utente che è disponibile l'autenticazione con impronte digitali, se configurata.
La finestra di login di Credential Manager per Windows 2000 chiede di **inserire la card** quando non è presente il lettore.	La schermata introduttiva di Windows Credential in Windows chiede all'utente di accedere con un messaggio **insert card** (inserire card) quando non è presente il lettore di Java Card.	Lo scopo dell'allarme è quello di segnalare all'utente che è disponibile l'autenticazione via Java Card, se configurata.
Impossibile accedere a Credential Manager dopo il passaggio dalla condizione di sleep alla sospensione solo su Windows XP Service Pack 1.	Dopo aver consentito al sistema il passaggio nello stato di sospensione e sleep, l'amministratore o l'utente non riescono ad accedere a Credential Manager e la schermata di accesso a Windows resta visualizzata indipendentemente dal tipo di credenziale d'accesso (password, impronte digitale o Java Card) selezionato.	Questo problema sembra essere risolto nel Service Pack 2 da Microsoft. Per maggiori informazioni sulla causa del problema consultare l'articolo 813301 nella Microsoft Knowledge Base all'indirizzo http://www.microsoft.com. Per poter effettuare l'accesso, l'utente deve selezionare Credential Manager ed effettuare l'accesso. Una volta entrato in Credential Manager, all'utente viene richiesto di effettuare l'accesso a Windows (l'utente deve eventualmente selezionare l'opzione di accesso a Windows) per completare il processo.

Breve descrizione	Dettagli	Soluzione
		Se l'utente accede prima a Windows, deve effettuare manualmente l'accesso a Credential Manager.
Il ripristino di Embedded Security impedisce a Credential Manager di andare a buon fine.	Credential Manager non riesce a registrare le credenziali in seguito al ripristino delle impostazioni predefinite della ROM.	HP Credential Manager for ProtectTools non riesce ad accedere al TPM dopo il ripristino delle impostazioni predefinite della ROM successivo all'installazione di Credential Manager. Il chip di protezione integrato nel TPM può essere abilitato nell'utility BIOS Computer Setup, in BIOS Configuration per ProtectTools oppure in HP Client Manager. Per abilitare il chip di protezione integrato nel TPM: 1. Aprire Computer Setup avviando o riavviando il computer e quindi premendo F10 mentre nell'angolo in basso a sinistra dello schermo è visualizzato il messaggio **F10 = Setup su base ROM**. 2. Utilizzare i tasti freccia per selezionare **Security** (Sicurezza)> **Setup Password** (Password di configurazione). Impostare una password. 3. Selezionare **Embedded Security Device** (Dispositivo di sicurezza integrata). 4. Utilizzare i tasti freccia per selezionare **Embedded Security Device–Disable** (Dispositivo di sicurezza integrata - Disabilita). Utilizzare i tasti freccia per modificarlo in **Embedded Security Device–Enable** (Dispositivo di sicurezza integrata - Abilita). 5. Selezionare **Enable** (Abilita) > **Save changes and exit** (Salvare le modifiche e uscire). HP sta valutando alcune soluzioni per le future release.
Il processo di sicurezza **Restore Identity** (Ripristina identità) perde l'associazione con il token virtuale.	Quando l'utente ripristina l'identità, è possibile che Credential Manager perda l'associazione con la posizione del token virtuale nella schermata di accesso. Anche se Credential Manager ha il token virtuale registrato, l'utente deve registrare nuovamente il token per ripristinare l'associazione.	Attualmente secondo progettazione. Quando si disinstalla Credential Manager senza mantenere le identità, la parte server del sistema del token viene distrutta, per cui il token non può più essere usato per l'accesso, anche se la parte client del token viene ripristinata attraverso il ripristino dell'identità. HP sta valutando opzioni a lungo termine per risolvere il problema.

Embedded Security per ProtectTools

Breve descrizione	Dettagli	Soluzione
La crittografia di cartelle, sottocartelle e file su PSD provoca un messaggio d'errore.	Se l'utente copia file e cartella nell'unità PSD e prova a crittografare cartelle/file oppure cartelle/sottocartelle, viene visualizzato il messaggio **Error Applying Attributes** (Errore di applicazione attributi). L'utente può crittografare gli stessi file dell'unità C:\ su un disco fisso aggiuntivo.	Come da progettazione. I file/cartelle spostati nell'unità PSD vengono automaticamente crittografati. Non serve crittografarli due volte. Se si cerca di crittografarli una seconda volta sull'unità PSD utilizzando EFS viene generato questo messaggio d'errore.
Non è possibile assumere la proprietà con un altro SO in piattaforma multi-avvio.	Se un'unità è configurata per l'avvio di più SO, la proprietà può essere assunta solo con la procedura di inizializzazione della piattaforma in un solo sistema operativo.	Come da progettazione, per motivi di sicurezza.
Un amministratore non autorizzato ha la possibilità di visualizzare, cancellare, rinominare e spostare il contenuto delle cartelle crittografate EFS.	La crittografia di una cartella non impedisce ad utenti non autorizzati in possesso di diritti amministrativi di visualizzare, cancellare o spostare il contenuto della cartella.	Come da progettazione. Si tratta di una funzione EFS, e non Embedded Security TPM. Embedded Security utilizza il software Microsoft EFS ed EFS mantiene i diritti di accesso a file/cartelle per tutti gli amministratori.
Le cartelle crittografate con EFS in Windows 2000 non sono evidenziate in verde.	Le cartelle crittografate con EFS sono evidenziate in verde in Windows XP, ma non in Windows 2000.	Come da progettazione. Il fatto di non evidenziare le cartelle crittografate in Windows 2000, ma di evidenziarle in Windows XP è una caratteristica di EFS. Ciò succede indipendentemente dal fatto che sia installato o meno un Embedded Security TPM.
EFS non richiede la password per visualizzare file crittografati in Windows 2000.	Se l'utente configura Embedded Security, effettua l'accesso come amministratore, quindi esce e rientra come amministratore, potrà visualizzare i file/le cartelle in Windows 2000 senza la password. Ciò avviene solo nel primo account amministratore in Windows 2000. Se viene effettuato l'accesso a un secondo account amministratore, questo problema non si verifica.	Come da progettazione. Si tratta di una caratteristica di EFS in Windows 2000. Invece, in Windows XP, EFS non consente, di default, agli utenti di aprire file/cartelle senza la password.
Il software non deve essere installato in seguito a ripristino con partizione FAT32.	Se l'utente cerca di ripristinare il disco fisso mediante FAT32, non vi saranno opzioni di crittografia per i file/le cartelle che utilizzano EFS.	Come da progettazione. Microsoft EFS è supportato soltanto su NTFS e non funziona su FAT32. Si tratta di una caratteristica di Microsoft EFS, non correlata al software HP ProtectTools.
Gli utenti di Windows 2000 possono condividere in rete qualsiasi PSD con condivisione nascosta ($).	Gli utenti di Windows 2000 possono condividere in rete qualsiasi PSD con condivisione nascosta ($). La condivisione nascosta è accessibile in rete mediante ($).	Normalmente, la funzione PSD non viene condivisa in rete, ma può esserlo utilizzando la condivisione nascosta ($) soltanto in Windows 2000. HP consiglia sempre di proteggere con password l'account amministratore integrato.
L'utente ha la possibilità di crittografare o cancellare il file XML nell'archivio di recupero.	In base alla progettazione, gli ACL per questa cartella non sono impostati per cui un utente potrebbe inavvertitamente o volutamente crittografare o eliminare il file, rendendolo inaccessibile. Così facendo, nessuno potrebbe utilizzare il software TPM.	Come da progettazione. Gli utenti hanno diritto di accesso ad un archivio d'emergenza per poter salvare/aggiornare la propria copia di backup della chiave per l'utente di base. I clienti sono invitati ad adottare un approccio di sicurezza secondo la 'miglior prassi' e a richiedere agli utenti di non crittografare né eliminare mai i file dell'archivio di recupero.
L'interazione di HP ProtectTools Embedded	I file crittografati interferiscono con la scansione antivirus di Symantec	Per accorciare i tempi richiesti per la scansione di file HP ProtectTools Embedded Security EFS, l'utente può

Breve descrizione	Dettagli	Soluzione
Security EFS con Symantec Antivirus o Norton Antivirus comporta tempi di scansione e crittografia/decrittazione più lunghi.	Antivirus o Norton Antivirus 2005. Durante il processo di scansione, all'utente viene richiesto di inserire la password per la chiave utente base all'incirca ogni 10 file. Se l'utente non immette la password, la richiesta scade, consentendo a NAV2005 di continuare la scansione. La crittografia dei file con HP ProtectTools Embedded Security EFS richiede più tempo quando Symantec Antivirus o Norton Antivirus è in esecuzione.	sia immettere la password di crittografia prima della scansione sia effettuare la decrittazione prima della scansione. Per accorciare i tempi richiesti per crittografare/decifrare dati con HP ProtectTools Embedded Security EFS, l'utente deve disabilitare Auto-Protect su Symantec Antivirus o Norton Antivirus.
Impossibile salvare l'archivio di recupero di emergenza su supporti rimovibili.	Se l'utente inserisce una scheda MMC o SD durante la creazione del percorso dell'archivio di recupero d'emergenza mentre è in corso l'inizializzazione a sicurezza integrata, viene visualizzato un messaggio d'errore.	Come da progettazione. La memorizzazione dell'archivio di recupero su supporti rimovibili non è supportata. L'archivio di recupero può essere memorizzato su un disco di rete o altro disco locale diverso dal disco C.
Impossibile crittografare dati in ambiente Windows 2000 francese (Francia).	Quando si fa clic con il pulsante destro del mouse sull'icona del file non è disponibile l'opzione **Encrypt** (Crittografa).	Si tratta di un limite del sistema operativo Microsoft. Se si cambia l'impostazione locale (per esempio, francese (Canada)), viene visualizzata l'opzione **Encrypt** (Crittografa). Per evitare il problema, crittografare il file come segue: fare clic con il pulsante destro sull'icona del file e selezionare **Properties** (Proprietà) > **Advanced** (Avanzate) > **Encrypt Contents** (Crittografa contenuto).
Si verificano errori nell'assunzione della proprietà durante l'inizializzazione a sicurezza integrata in seguito ad interruzione dell'alimentazione.	In caso di mancanza di alimentazione durante l'inizializzazione del chip Embedded Security, si verificano i seguenti problemi: • Quando si cerca di lanciare la procedura guidata di inizializzazione Embedded Security, viene visualizzato il seguente errore: **The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.** (Impossibile inizializzare la sicurezza integrata in quanto il chip Embedded Security ha già un utente Embedded Security.) • Quando si cerca di lanciare la procedura guidata di inizializzazione utente, viene visualizzato il seguente errore: **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.** (Embedded Security non è inizializzato. Per utilizzare la procedura guidata, si deve inizializzare preventivamente l'Embedded Security.)	Per il ripristino successivamente ad una perdita di alimentazione, eseguire la procedura seguente: **NOTA:** Utilizzare i tasti freccia per selezionare i vari menu e le voci di menu e per modificare i valori (salvo diversa indicazione). 1. Avviare o riavviare il computer. 2. Premere F10 quando sullo schermo appare il messaggio **F10=Setup** (oppure non appena il LED del monitor diventa verde). 3. Selezionare l'opzione della lingua. 4. Premere Invio. 5. Selezionare **Security** (Sicurezza) > **Embedded Security**. 6. Impostare l'opzione **Embedded Security Device** (Dispositivo di sicurezza integrata) su **Enable** (Abilita). 7. Premere F10 per accettare la modifica. 8. Selezionare **File** > **Save Changes and Exit** (Salva modifiche ed esci). 9. Premere INVIO. 10. Premere F10 per salvare le modifiche ed uscire dalla utility F10 Setup.
Dopo avere abilitato il modulo TPM è possibile eliminare la password per	Per abilitare il modulo TPM è richiesta una password per la utility Computer Setup (F10). Dopo aver abilitato il modulo, l'utente può rimuovere la	Come da progettazione. La password della utility Computer Setup (F10) può essere rimossa soltanto da un utente che la conosca.

Breve descrizione	Dettagli	Soluzione
la utility Computer Setup (F10).	password. In questo modo, chiunque abbia l'accesso diretto al sistema avrà la possibilità di ripristinare il modulo TPM e di provocare una possibile perdita di dati.	Tuttavia, HP consiglia vivamente di mantenere sempre protetta da password la utility Computer Setup (F10).
Il campo della password PSD non viene più visualizzato quando il sistema si attiva dopo la modalità standby	Quando l'utente accede al sistema dopo aver creato un PSD, il TPM chiede la password per l'utente base. Se l'utente non inserisce la password e il sistema si porta in modalità standby, la finestra di dialogo della password non è più disponibile quanto l'utente riavvia il sistema.	Secondo progettazione. L'utente deve uscire dal sistema e riaccedere per visualizzare di nuovo la finestra della password PSD.
Non è richiesta la password per modificare le Security Platform Policies (Politiche piattaforma di sicurezza).	L'accesso alle Security Platform Policies (Politiche piattaforma di sicurezza) (per macchina e utente) non richiede una password TPM per gli utenti in possesso di diritti amministrativi sul sistema.	Secondo progettazione. Qualunque amministratore può modificare le politiche della piattaforma di sicurezza con o senza inizializzazione utente TPM.
Microsoft EFS non è completamente compatibile con Windows 2000.	Un amministratore può accedere ad informazioni crittografate sul sistema anche senza conoscere la password. Se l'amministratore immette una password non corretta o elimina la finestra di dialogo relativa alla password, il file crittografato si apre come se fosse stata immessa la password giusta. Ciò succede indipendentemente dalle impostazioni di sicurezza utilizzate per crittografare i dati. Ciò avviene solo nel primo account amministratore in Windows 2000.	La politica di recupero dati viene configurata automaticamente per designare un amministratore come addetto al recupero. Quando non è possibile richiamare una chiave utente, come nel caso in cui si immetta la password errata o si elimini la finestra di dialogo Enter password (Immetti password), il file viene automaticamente decifrato con una chiave di recupero. Ciò dipende da Microsoft EFS. Per maggiori informazioni vedere l'articolo Q257705 nella Microsoft Knowledge Base all'indirizzo http://www.microsoft.com. I documenti possono essere aperti solo dagli amministratori
Un certificato viene visualizzato come non affidabile.	Dopo aver configurato HP ProtectTools e lanciato la procedura guidata di inizializzazione utente, l'utente ha la possibilità di visualizzare il certificato emesso che, però, viene visualizzato come non affidabile. Benché sia possibile installare il certificato facendo clic sul pulsante Install (Installa), l'installazione non lo rende affidabile.	I certificati autofirmati non vengono considerati affidabili. In un ambiente aziendale configurato correttamente, i certificati EFS vengono rilasciati da autorità di certificazione online e vengono considerati affidabili.
Si verifica un errore intermittente di crittografia e decrittazione: **Il processo non riesce ad accedere al file in quanto utilizzato da altro processo.**	L'errore intermittente durante la crittografia o la decrittazione del file è dovuto al fatto che il file viene utilizzato da un altro processo, anche se tale file o cartella non viene elaborato dal sistema operativo o da altre applicazioni.	Per correggere l'errore: 1. Riavviare il sistema. 2. Disconnettersi. 3. Eseguire nuovamente il login.
Si verifica una perdita di dati nei dispositivi di memorizzazione rimovibili nel caso siano rimossi prima della creazione o del trasferimento di nuovi dati.	Quando si rimuovono supporti di memorizzazione, ad esempio, un disco fisso MultiBay, continua a essere indicata la disponibilità PSD e non vengono generati errori quando si aggiungono/modificano dati al PSD. Dopo il riavvio del sistema, il PSD non rispecchia le modifiche del file effettuate nel periodo di indisponibilità del supporto rimovibile.	Questo problema si verifica soltanto se l'utente accede al PSD, quindi rimuove il disco fisso prima di completare la creazione o il trasferimento di nuovi dati. Se si cerca di accedere al PSD quando non è presente il disco fisso, viene visualizzato un messaggio d'errore che segnala che **il dispositivo non è pronto**.
Durante la disinstallazione, se l'utente non ha inizializzato l'utente base	L'utente può procedere in due modi: disinstallare senza disabilitare il TPM oppure disabilitare il TPM con lo strumento Administration	Lo strumento Admin (Amministrazione) serve per disabilitare il chip TPM, ma tale opzione non è disponibile se non è stata inizializzata preventivamente la Basic User Key (Chiave utente base). In caso

Breve descrizione	Dettagli	Soluzione
e apre lo strumento Administration (Amministrazione), l'opzione **Disable** (Disabilita) non è disponibile e la disinstallazione non procede finché non viene chiuso lo strumento Administration (Administration).	(Amministrazione), quindi procedere alla disinstallazione. L'accesso allo strumento Administration (Amministrazione) richiede l'inizializzazione della Basic User Key (Chiave utente base). Se non è stata eseguita l'inizializzazione di base, tutte le opzioni restano inaccessibili all'utente. Dal momento che l'utente ha scelto esplicitamente di aprire lo strumento Admin (Amministrazione) facendo clic su **Yes** (Sì) nella finestra di dialogo in cui è visualizzato il messaggio **Click Yes to open Embedded Security Administration tool** (Fare clic su Sì per aprire lo strumento Embedded Security Administration), la disinstallazione non procede finché non si chiude lo strumento Admin. Se l'utente fa clic su **No** nella finestra di dialogo, lo strumento Admin (Amministrazione) non si apre e la disinstallazione procede.	negativo, selezionare **OK** oppure **Cancel** (Annulla) per continuare il processo di disinstallazione.
Si verificano blocchi intermittenti del sistema dopo aver creato PSD su 2 account utente e aver utilizzato la commutazione rapida utente in configurazioni di sistema a 128 MB.	Il sistema potrebbe bloccarsi con schermata nera e tastiera e mouse inattivi anziché mostrare la schermata introduttiva (login) quando si utilizza la commutazione rapida con una quantità minima di RAM.	La probabile causa remota è un problema legato ai tempi nelle configurazioni con poca memoria. La grafica integrata utilizza architettura UMA che richiede 8 MB di memoria, lasciandone disponibili all'utente soltanto 120, che vengono condivisi fra i due utenti che hanno effettuato l'accesso e che sono a commutazione rapida di utente quando viene generato l'errore. Per risolvere il problema, riavviare il sistema. Inoltre, si consiglia di incrementare la configurazione della memoria (HP non rilascia configurazioni a 128 MB di default con moduli di sicurezza).
L'autenticazione utente EFS (è richiesta la password) scade con **accesso negato**.	La password per l'autenticazione utente EFS si riapre dopo aver fatto clic su **OK** oppure tornando allo stato di standby dopo il timeout.	Come da progettazione. Per evitare problemi con Microsoft EFS, è stato creato un timer watchdog di 30 secondi per generare il messaggio d'errore.
Durante la configurazione del giapponese si osservano dei troncamenti, anche se minimi, a livello di descrizione funzionale	Durante la configurazione personalizzata della procedura di installazione guidata le descrizioni funzionali vengono tagliate.	HP si occuperà del problema in una release futura.
La crittografia EFS funziona senza immissione di password nel prompt.	Anche se il prompt per la password utente scade, la crittografia resta attiva su file o cartelle.	La capacità di crittografare non richiede l'autentica della password dato che si tratta di una funzione di Microsoft EFS. La decrittazione richiede la password utente.
La posta elettronica sicura è supportata, anche se non selezionata nella procedura guidata di inizializzazione utente o se la configurazione di posta elettronica sicura è disabilitata nelle politiche utente.	Il software a sicurezza integrata e la procedura guidata non gestiscono le impostazioni dei client di posta elettronica (Outlook, Outlook Express o Netscape)	Comportamento secondo progettazione. La configurazione delle impostazioni di posta elettronica del TPM non impediscono la modifica delle impostazioni di crittografia direttamente dal client di posta elettronica. L'utilizzo della posta elettronica sicura viene impostato e controllato da applicazioni di terze parti. La procedura guidata HP consente il collegamento alle tre applicazioni di riferimento per una personalizzazione immediata.
Eseguendo una seconda volta Large Scale Deployment sullo stesso	L'esecuzione Large Scale Deployment su un qualsiasi sistema HP ProtectTools Embedded Security inizializzato in	HP sta lavorando per risolvere il problema della sovrascrittura dei file xml e fornirà una soluzione in un SoftPaq futuro.

Breve descrizione	Dettagli	Soluzione
PC o su un PC inizializzato in precedenza vengono sovrascritti i file Emergency Recovery e Emergency Token. I nuovi file non possono essere utilizzati per il recupero.	precedenza sovrascrive i file xml di Recovery Archive e Recovery Token, rendendoli inutilizzabili.	
Gli script di login automatizzato non funzionano durante il ripristino utente in Embedded Security.	L'errore si verifica dopo che l'utente • inizializza proprietario e utente in Embedded Security (utilizzando le posizioni predefinite: **Documenti**). • Ripristina le impostazioni predefinite del chip nel BIOS. • Riavvia il computer. • Inizia a ripristinare Embedded Security. Durante il processo di ripristino, Credential Manager chiede all'utente se il sistema può automatizzare l'accesso all'autenticazione utente TPM Infineon. Se l'utente sceglie **Yes** (Sì), la posizione di SPEmRecToken appare automaticamente nella casella di testo. Anche se questa posizione è corretta, viene visualizzato il seguente messaggio d'errore: **No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from** (Nessun Emergency Recovery Token fornito. Selezionare la posizione da cui richiamare l'Emergency Recovery Token).	Fare clic sul pulsante **Browse** (Sfoglia) dello schermo per selezionare la posizione e proseguire con il processo di ripristino.
I PSD per più utenti non funzionano in ambienti a commutazione rapida utente.	Questo errore si verifica quando vengono creati più utenti ai quali viene assegnato un PSD con la stessa lettera di unità. Se si cerca di effettuare la commutazione rapida tra utenti quando il PSD è caricato, il PSD del secondo utente non sarà disponibile.	Il PSD del secondo utente sarà disponibile soltanto se configurato per utilizzare un'altra lettera di unità o se il primo utente si è disconnesso.
Il PSD è disattivato e non può essere cancellato dopo avere formattato il disco fisso su cui era stato generato.	Il PSD è disattivato e non può essere cancellato dopo aver formattato il disco fisso secondario su cui era stato generato. L'icona del PSD è tuttora visibile ma, quando si cerca di accedervi, viene visualizzato il messaggio d'errore **drive is not accessible** (unità non accessibile). L'utente non è in grado di cancellare il PSD e viene visualizzato il seguente messaggio: **Your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process** (Il PSD dell'utente è ancora in uso. Verificare che non contenga file aperti e non sia utilizzato da un altro processo). L'utente deve riavviare il sistema per poter cancellare il	Secondo progettazione: Se un cliente cancella volutamente o si scollega dalla posizione in cui sono memorizzati i dati del PSD, l'emulazione dell'unità PSD di Embedded Security continua a funzionare producendo errori dovuti all'assenza di comunicazione con i dati mancanti. Soluzione: Al riavvio successivo, le emulazioni non vengono più caricate e l'utente può cancellare la vecchia emulazione PSD e creare un nuovo PSD.

Breve descrizione	Dettagli	Soluzione
	PSD e fare in modo che non venga caricato dopo il riavvio.	
È stato rilevato un errore interno durante il ripristino dall'archivio di backup automatico.	Se l'utente • fa clic sull'opzione **Restore under Backup** (Ripristina da backup) di Embedded Security in HPPTSM per effettuare il ripristino dall'archivio di backup automatico • seleziona **SPSystemBackup .xml** la procedura guidata di ripristino non viene completata e viene visualizzato il seguente messaggio d'errore: **The selected Backup Archive does not match the restore reason. Please select another archive and continue** (L'archivio di backup selezionato non corrisponde al motivo del ripristino. Selezionare un altro archivio e continuare).	Se l'utente seleziona **SpSystemBackup.xml** quando è richiesto SpBackupArchive.xml, la procedura guida di Embedded Security non viene completata e viene visualizzato il seguente messaggio di errore: **An internal Embedded Security error has been detected.** (È stato rilevato un errore interno a Embedded Security.) L'utente deve selezionare il file .xml corretto e corrispondente al motivo richiesto. I processi vengono eseguiti correttamente. Tuttavia, il messaggio di errore interno a Embedded Security non è chiaro e dovrebbe riportare un messaggio più appropriato. HP sta cercando di ovviare a questo problema nei prodotti futuri.
Errore di ripristino di Security System con più utenti.	Durante il processo di ripristino, l'amministratore seleziona gli utenti da ripristinare. Gli utenti non selezionati non saranno in grado di ripristinare le chiavi nel caso tentino di effettuare il ripristino in un secondo momento. Viene visualizzato il messaggio di errore che segnala che il **processo di decrittazione non stato completato correttamente**.	Gli utenti non selezionati possono essere ripristinati con il reset del TPM, eseguendo il processo di ripristino e selezionando tutti gli utenti prima che venga eseguito il successivo backup giornaliero predefinito. Se eseguito, il backup automatizzato sovrascrive gli utenti non ripristinati con perdita dei rispettivi dati. Se viene archiviato un nuovo backup di sistema, non sarà possibile ripristinare gli utenti che in precedenza non erano stati selezionati. Inoltre, l'utente deve ripristinare tutto il backup di sistema. Un backup di archivio può essere ripristinato individualmente.
Il ripristino dei valori predefiniti della ROM di sistema nasconde il TPM.	Il ripristino dei valori predefiniti della ROM di sistema nasconde il TPM a Windows, impedendo il corretto funzionamento del software di sicurezza e rendendo inaccessibili i dati crittografati dal TPM.	Rendere visibile il TPM nel BIOS: Aprire la utility Computer Setup (F10), portarsi su **Security** (Sicurezza) > **Device Security** (Sicurezza dispositivi) e modificare il campo da **Hidden** (Nascosto) a **Available** (Disponibile).
Il backup automatico non funziona con le unità mappate.	Quando l'amministratore configura il backup automatico in Embedded Security, viene creata una voce in **Windows** > **Operazioni** > **Operazione pianificata**. Questa Operazione pianificata di Windows è impostata per utilizzare NT AUTHORITY\ SYSTEM per i diritti di esecuzione del backup e funziona regolarmente su qualsiasi unità locale. Quando, invece, l'amministratore configura il backup automatico in modo che il salvataggio avvenga su un'unità mappata, il processo non va a buon fine in quanto NT AUTHORITY\SYSTEM non possiede i diritti per utilizzare l'unità mappata. Se il backup automatico è programmato perché avvenga al momento dell'accesso, l'icona Embedded Security TNA visualizza il seguente messaggio: **The Backup Archive location is**	Per ovviare al problema, cambiare NT AUTHORITY \SYSTEM in (nome computer)\(nome amministratore). Questa è l'impostazione predefinita se l'Operazione pianificata viene creata manualmente. HP sta lavorando affinché le impostazioni predefinite delle release future comprendano il nome computer \nome amministratore.

Breve descrizione	Dettagli	Soluzione
	currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again. (La posizione dell'archivio di backup non è al momento accessibile. Fare clic qui per effettuare il backup su un archivio temporaneo finché non sia nuovamente disponibile l'archivio di backup.) Tuttavia, se il backup automatico è programmato per attivarsi a una data ora, l'operazione di backup non verrà completata e non verrà visualizzato alcun messaggio.	
Impossibile disabilitare temporaneamente Embedded Security State nell'interfaccia grafica utente di Embedded Security	Il software 4.0 corrente è stato progettato per implementazioni di HP Notebook 1.1B oltre che per supportare implementazioni di HP Desktop 1.2. Questa possibilità di disabilitazione è tuttora supportata nell'interfaccia software per piattaforme TPM 1.1.	HP si occuperà del problema nelle release future.

Varie

Descrizione sintetica dell'impatto sul software	Dettagli	Soluzione
HP ProtectTools Security Manager: Avvertenza ricevuta: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (L'applicazione di sicurezza non può essere installata finché non è stato installato HP Protect Tools Security Manager).	Tutte le applicazioni di sicurezza, quali Embedded Security, Java Card e lettori biometrici, sono plug-in estensibili per l'interfaccia HP Security Manager. Per caricare un plug-in di sicurezza approvato da HP, occorre avere preventivamente installato Security Manager.	Il software HP ProtectTools Security Manager deve essere installato prima di qualsiasi plug-in di sicurezza.
HP ProtectTools TPM Firmware Update Utility per dc7600 modelli contenenti TPM con abilitazione Broadcom: Lo strumento fornito tramite il sito Web di supporto HP indica che è **richiesta la proprietà**	Questo rappresenta il comportamento previsto dell'utility software TPM per dc7600 e modelli contenenti TPM con abilitazione Broadcom Lo strumento di aggiornamento del firmware consente all'utente di aggiornare il firmware, con o senza la chiave di approvazione (Endorsement Key, EK). In assenza della chiave di approvazione, l'aggiornamento del firmware può essere completato senza alcuna autorizzazione. Se la chiave è presente, è necessario che vi sia un proprietario TPM che autorizzi l'aggiornamento. Al termine dell'aggiornamento, la piattaforma deve essere riavviata perché abbia effetto il nuovo firmware. Se il BIOS TPM è resettato di fabbrica, la proprietà viene rimossa e la funzione di aggiornamento del firmware impedita finché non siano state configurate la piattaforma Embedded Security Software e la procedura guidata di inizializzazione utente. *Dopo aver eseguito l'aggiornamento del firmware si raccomanda sempre di effettuare il riavvio. La versione del firmware non viene identificata correttamente finché non avviene il riavvio.	1. Reinstallare il software HP ProtectTools Embedded Security 2. Eseguire la procedura di configurazione guidata della piattaforma e dell'utente. 3. Accertarsi che il sistema contenga l'installazione di Microsoft .NET framework 1.1: a. Fare clic su **Start**. b. Fare clic su **Pannello di controllo**. c. Fare clic su **Installazione applicazioni**. d. Verificare che **Microsoft .NET Framework 1.1** sia nell'elenco. 4. Controllare la configurazione hardware e software: a. Fare clic su **Start**. b. Fare clic su **Tutti i programmi**. c. Fare clic su **HP ProtectTools Security Manager**. d. Selezionare **Embedded Security** dal menu ad albero. e. Fare clic su **More Details** (Altri dettagli) Il sistema dovrebbe avere la seguente configurazione: • Versione prodotto = V4.0.1 • Stato sicurezza integrata: Stato chip = Abilitato, Stato proprietario = Inizializzato, Stato utente = Inizializzato • Informazioni sui componenti: Spec. TCG Versione = 1.2 • Casa produttrice = Broadcom Corporation

Descrizione sintetica dell'impatto sul software	Dettagli	Soluzione
		• Versione FW = 2.18 (o superiore) • Libreria driver TPM versione 2.0.0.9 (o superiore) 5. Se la versione FW non corrisponde a 2.18, scaricare e aggiornare il firmware TPM. Il firmware TPM SoftPaq è un download di supporto disponibile al sito Web http://www.hp.com.
HP ProtectTools Security Manager: Ad intermittenza, viene riportato un errore quando si chiude l'interfaccia Security Manager.	A livello intermittente (1 su 12 casi), si crea un errore con l'uso del pulsante di chiusura, a destra, nella parte superiore della videata, per chiudere Security Manager prima che siano state caricate tutte le applicazioni plug-in.	Ciò è associato ad una dipendenza dal tempo di caricamento dei servizi plug-in quando si chiude e si riavvia Security Manager. Dal momento che PTHOST.exe è l'interfaccia contenente le altre applicazioni (plug-in), completare il tempo di caricamento (servizi) dipende dalla capacità del plug-in. La chiusura dell'interfaccia prima che il plug-in abbia avuto il tempo di completare il caricamento è la causa di fondo. Lasciare che Security Manager completi il messaggio di caricamento dei servizi (visualizzato in alto nella finestra di Security Manager) e che tutti i plug-in vengano elencati nella colonna di sinistra. Prevedere un tempo ragionevole per consentire il caricamento di questi plug-in.
HP ProtectTools * General: L'accesso illimitato o i privilegi amministratore non controllati comportano il rischio della sicurezza.	Sono possibili numerosi rischi legati all'accesso illimitato al PC client: • cancellazione di PSD • modifica intenzionale di impostazioni utente • disabilitazione di funzioni e politiche di sicurezza	Si consigliano gli amministratori di adottare le "migliori prassi" limitando i privilegi degli utenti finali e restringendo l'accesso. Agli utenti non autorizzati non dovrebbero essere concessi privilegi amministrativi.
Le password del BIOS e di Embedded Security sono fuori sincrono.	Se l'utente non convalida una nuova password come password di BIOS Embedded Security, verrà utilizzata la password di sicurezza integrata originale tramite BIOS F10.	Questo funzionamento è corretto. Tali password possono essere risincronizzate modificando la password utente base del sistema operativo e autenticandola nella finestra di BIOS Embedded Security in cui viene richiesta la password.
Dopo che nel BIOS è stata abilitata l'autenticazione di preavvio del TPM, solo un utente potrà accedere al sistema.	IL PIN BIOS TPM è associato al primo utente che inizializza le impostazioni utente. Se un computer ha più utenti, il primo utente diventa, in pratica, l'amministratore. Il primo utente dovrà fornire il proprio PIN utente TPM agli altri utenti del computer.	Questo funzionamento è corretto. HP consiglia che l'ufficio informatico del cliente adotti validi criteri di sicurezza nel definire le proprie soluzioni di protezione e che la password dell'amministratore del BIOS venga configurata dagli amministratori informatici per ottenere una protezione a livello di sistema.
L'utente deve modificare il PIN affinché il preavvio del TPM funzioni dopo un ripristino.	Affinché il BIOS del TPM funzioni correttamente dopo un ripristino, l'utente deve modificare il PIN o creare un nuovo utente per inizializzare le proprie impostazioni utente. Non sono disponibili altre opzioni che consentano il funzionamento dell'autenticazione del BIOS del TPM.	Come da progettazione. Il ripristino elimina la Basic User Key (Chiave utente base). L'utente dovrà modificare il proprio PIN utente o creare un nuovo utente per inizializzare la Basic User Key (Chiave utente base).
Non sono state ripristinate le impostazioni predefinite di **Power-on authentication support** (Supporto autenticazione all'accensione) con l'opzione **Reset to**	In Computer Setup, non sono state ripristinate le impostazioni predefinite di **Power-on authentication support** (Supporto autenticazione all'accensione) con l'opzione **Reset to Factory Settings** (Ripristina impostazioni predefinite) di Embedded	L'opzione **Reset to Factory Settings** (Ripristina impostazioni predefinite) disabilita Embedded Security Device, che nasconde le altre opzioni di Embedded Security, fra cui **Power-on authentication support** (Supporto autenticazione all'accensione). Tuttavia, dopo avere nuovamente abilitato Embedded Security

Descrizione sintetica dell'impatto sul software	Dettagli	Soluzione
Factory Settings (Ripristina impostazioni predefinite) di Embedded Security	Security Device. Per impostazione predefinita, **Power-on authentication support** (Supporto autenticazione all'accensione) è impostato su **Disable** (Disabilita).	Device, **Power-on authentication support** (Supporto autenticazione all'accensione) resta abilitato. HP sta lavorando per trovare una soluzione al problema, che verrà inclusa in una futura offerta SoftPaq ROM, distribuita sul Web.
Security Power-On Authentication (Autenticazione di sicurezza all'accensione) si sovrappone alla password del BIOS durante la sequenza di avvio.	L'autenticazione all'accensione chiede all'utente di accedere al sistema utilizzando la password TPM, ma se l'utente preme F10 per accedere al BIOS, vengono concessi solo i diritti di lettura.	Per scrivere nel BIOS, l'utente deve immettere la password del BIOS e non quella del TPM nella finestra di autenticazione all'accensione.
Dopo che la password Proprietario è stata modificata nel software Windows Embedded Security, il BIOS richiede la password vecchia e quella nuova tramite Computer Setup.	Dopo che la password Proprietario è stata modificata nel software Windows Embedded Security, il BIOS richiede la password vecchia e quella nuova tramite Computer Setup.	Come da progettazione. Ciò è dovuto all'incapacità del BIOS di comunicare con il TPM, una volta che il sistema operativo è in funzione, e di verificare la frase di accesso al TPM rispetto alla chiave TPM.

Glossario

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

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

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

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

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

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

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

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 incorporata TPM (Trusted Platform Module) (solo in determinati modelli) Chip di protezione integrata in grado di proteggere le informazioni riservate degli utenti da attacchi dannosi. Rappresenta l'entità attendibile principale in una specifica piattaforma. TPM fornisce operazioni e algoritmi di crittografia conformi alle specifiche TCG (Trusted Computing Group).

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

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

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

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

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

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

DriveLock Funzione di protezione che consente di collegare l'unità disco rigido a un utente e richiede all'utente di digitare in modo corretto la password DriveLock all'avvio del computer.

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.

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

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

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

Massima sicurezza Funzione di protezione in BIOS Configuration che consente di ottimizzare la protezione delle password amministratore e di accensione e di altre forme di autenticazione di accensione.

Migrazione Attività che consente la gestione, il ripristino e il trasferimento di chiavi e certificati.

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

Partizione FAT File Allocation Table (Tabella di allocazione file), metodo per l'indicizzazione dei supporti di memorizzazione.

Partizione NTFS File system NT, metodo per l'indicizzazione dei supporti di memorizzazione. Questo metodo è standard con Windows Vista e Windows XP.

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

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

Riavvio Processo che consente di riavviare il computer.

Single Sign-on Funzione che consente di memorizzare le informazioni di autenticazione e di utilizzare Credential Manager per accedere ad applicazioni Internet e Windows che richiedono l'autenticazione della password.

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

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

Token virtuale Funzione di protezione che opera in modo molto simile a una Java Card o a un lettore. Il token viene salvato nell'unità disco rigido del computer oppure nel registro di sistema di Windows. Quando si accede con un token virtuale, viene richiesto un PIN utente per completare l'autenticazione.

Unità personale protetta (PSD) Fornisce un'area di memorizzazione protetta per le informazioni riservate.

Indice analitico