HP Client Security

Guida introduttiva

Prima edizione: Agosto 2013

Numero di parte del documento: 735339-061

Sommario

1 Introduzione all'HP Client Security Manager

HP Client Security consente di proteggere i dati, i dispositivi e l'identità, aumentando così la protezione del computer.

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

I moduli software HP Client Security possono essere preinstallati, precaricati o scaricati dal sito Web HP. Per ulteriori informazioni, consultare http://www.hp.com.

NOTA: Le istruzioni presenti in questa guida presuppongono che sia già stata effettuata l'installazione dei moduli software HP Client Security applicabili.

Funzioni di HP Client Security

Nella tabella seguente vengono presentate in dettaglio le principali funzioni dei moduli HP Client Security.

Modulo	Funzioni principali
HP Client Security Manager	Gli amministratori possono eseguire le seguenti attività: • Proteggere il computer in uso prima dell'avvio di Windows® • Proteggere l'account di Windows utilizzando un'autenticazione complessa • Gestire l'accesso e le password per siti web e applicazioni • Modificare facilmente la password del sistema operativo Windows • Utilizzo delle impronte digitali per maggior protezione e praticità • Configurazione di una smart card, di una scheda senza contatti o di una scheda di prossimità per l'autenticazione • Utilizzare il telefono cellulare Bluetooth come metodo di identificazione • Impostare un PIN per ampliare le scelte di autenticazione • Configurare dei criteri di accesso e di sessione • Backup e ripristino dei dati di programma • Aggiungere altre applicazioni, ad esempio HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager e HP Computrace Gli utenti generici possono eseguire le funzioni che seguono: • Visualizzare le impostazioni di Stato crittografia e Device Access Manager. • Attivare Computrace. • Configurare Preferenze e opzioni di Backup e ripristino.

Modulo	Funzioni principali
Password Manager	Gli utenti di base possono eseguire le seguenti attività: • Organizzazione e impostazione delle password e dei nomi utente. • Creare password più sicure per una migliore protezione degli account, per gli account di posta elettronica e Web. Gestore password compila le informazioni e le invia in modo automatico. • Semplificazione della procedura di accesso con la funzione Single Sign On, che consente di salvare e applicare automaticamente le credenziali dell'utente. • Contrassegnare un account come compromesso in modo da essere avvisati per altri account(s) con credenziali simili. • Importare i dati di accesso da un browser supportato.
HP Drive Encryption (solo in determinati modelli)	• Crittografia completa dell'unità disco rigido. • Forzatura dell'autenticazione di preavvio per la decrittografia dei dati e il loro utilizzo. • Possibilità di attivazione delle unità che supportano la crittografia automatica (solo in determinati modelli).
HP Device Access Manager	• Consente ai responsabili IT di controllare l'accesso ai dispositivi in base ai profili utente. • Impedisce agli utenti non autorizzati di rimuovere i dati tramite supporti di archiviazione esterni e di introdurre virus nel sistema da supporti simili. • Consente agli amministratori di impedire a utenti o gruppi di utenti specifici di accedere ai dispositivi di comunicazione.
HP Trust Circles	• Garantisce protezione per file e documenti. • Crittografa i file collocati in cartelle specificate dall'utente e li protegge all'interno di un trust circle. • Consente l'utilizzo e la condivisione dei file solo da parte dei membri del trust circle.
Ritrovamento di PC rubati (Computrace, da acquistare separatamente)	• L'attivazione richiede l'acquisto a parte di sottoscrizioni per il monitoraggio e il tracciamento. • Offre il monitoraggio sicuro delle risorse. • Esegue il monitoraggio dell'attività dell'utente e delle modifiche apportate all'hardware e al software. • Rimane attivo anche in caso di riformattazione o sostituzione del disco rigido.

Descrizione del prodotto HP Client Security e esempi di utilizzo comune.

La maggior parte dei prodotti HP Client Security, presentano un'autenticazione utente (solitamente una password) e un backup amministrativo per effettuare l'accesso in caso di password perse, non disponibili o dimenticate e qualora sia necessario un accesso ai fini della sicurezza aziendale.

NOTA: Alcuni prodotti HP Client Security sono studiati in modo da limitare l'accesso ai dati. I dati devono essere crittografati nel caso in cui l'utente preferisca perdere tali informazioni piuttosto che comprometterle. Si consiglia di eseguire il backup di tutti i dati in una posizione sicura.

Password Manager

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

- Salvare i nomi e le password di accesso a Internet o alla posta elettronica.
- Eseguire automaticamente l'accesso dell'utente a un sito Web o alla posta.
- Gestire e organizzare le autenticazioni.
- Selezionare una risorsa Web o di rete ed accedere direttamente al link.
- Visualizzare nomi e password se necessario.
- Contrassegnare un account come compromesso in modo da essere avvisati per altri account(s) con credenziali simili.
- Importare i dati di accesso da un browser supportato.

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

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

Esempio 2: Un dipendente dinamico è stato promosso e ora dovrà gestire l'intero ufficio contabile. Il team deve accedere a molti account Web client, ciascuno con credenziali diverse. Questi dati di accesso devono essere condivisi con altri utenti, pertanto la riservatezza è un aspetto critico. Il dipendente decide quindi di organizzare tutti i link Web, i nomi utente e le password aziendali in Password Manager. Una volta completato il processo, il dipendente distribuisce Password Manager ai dipendenti affinché possano lavorare negli account Web senza mai conoscere le credenziali di accesso in uso.

HP Drive Encryption (solo in determinati modelli)

HP Drive Encryption è utilizzato per limitare l'accesso ai dati sull'intera unità disco rigido del computer o su un'unità secondaria. Drive Encryption è anche in grado di gestire unità con auto-crittografia.

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

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

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

HP Device Access Manager (solo in determinati modelli)

HP Device Access Manager consente a un amministratore di limitare e gestire l'accesso all'hardware. Device Access Manager può essere utilizzato per bloccare l'accesso non autorizzato alle unità flash USB in cui potrebbero essere copiati i dati. È inoltre possibile limitare l'accesso alle unità CD/DVD, il controllo dei dispositivi USB, le connessioni di rete e così via. Un esempio potrebbe essere una situazione in cui dei fornitori esterni necessitano l'accesso ai computer aziendali ma non sono in grado di copiare i dati in un'unità USB.

Esempio 1: il responsabile di un'azienda di forniture mediche lavora spesso con la documentazione medica personale e con le informazioni aziendali. I dipendenti devono accedere a tali dati ma è estremamente importante che i dati non vengano rimossi dal computer tramite unità USB o altro supporto di memorizzazione esterno. La rete è protetta ma i computer sono dotati di masterizzatori e porte USB che potrebbero consentire la copia o il furto dei dati. Il responsabile utilizza Device Access Manager per disattivare le porte USB e i masterizzatori in modo da impedirne l'utilizzo. Anche se le porte USB sono bloccate, il mouse e le tastiere continueranno a funzionare.

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

Computrace (da acquistare separatamente)

Computrace (da acquistare separatamente) è un servizio in grado di rintracciare la posizione di un computer rubato se l'utente effettua l'accesso a Internet. Computrace consente anche di gestire e localizzare in remoto i computer e di monitorare l'utilizzo dei computer e le applicazioni.

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

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

Conseguimento degli obiettivi principali in materia di protezione

I moduli HP Client Security sono in grado di lavorare insieme per offrire soluzioni per un'ampia gamma di problemi di protezione, tra cui i seguenti obiettivi di protezione chiave:

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

Protezione da furto mirato

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

- La funzionalità di autenticazione di preavvio, se abilitata, consente di impedire l'accesso al sistema operativo.
  - HP Client Security: vedere HP Client Security a pagina 13.
  - HP Drive Encryption: vedere HP Drive Encryption (solo in determinati modelli) a pagina 30.
- La crittografia consente di impedire l'accesso ai dati anche in caso di rimozione dell'unità disco rigido e installazione in un sistema non protetto.
- Computrace consente di individuare la posizione di un computer rubato.
  - Computrace: vedere Ritrovamento in seguito a furto (solo in determinati modelli) a pagina 54.

Restrizione dell'accesso ai dati riservati

Supponiamo che un revisore dei conti esterno lavori in sede e disponga dell'accesso al computer per esaminare dati finanziari sensibili; Non si desidera il revisore abbia la possibilità di stampare i file o di salvarli su un dispositivo scrivibile, come un CD. La funzionalità seguente consente di limitare l'accesso ai dati:

- HP Device Access Manager consente ai responsabili IT di limitare l'accesso ai dispositivi di comunicazione in modo che le informazioni sensibili non possano essere copiate dal disco rigido. Vedere Schermata sistema a pagina 44.

Blocco dell'accesso non autorizzato da posizioni esterne o interne

L'accesso non autorizzato a un computer aziendale non protetto rappresenta un rischio reale per le risorse della rete aziendale, come ad esempio le informazioni dei servizi finanziari, di un executive o di un team di ricerca e sviluppo e per le informazioni private ad esempio i dati dei pazienti o la documentazione finanziaria personale. Le seguenti funzionalità consentono di impedire l'accesso non autorizzato:

- La funzionalità di autenticazione di preavvio, se abilitata, consente di impedire l'accesso al sistema operativo. (Vedere HP Drive Encryption (solo in determinati modelli) a pagina 30.)
- HP Client Security consente di impedire che un utente non autorizzato possa ottenere le password o l'accesso ad applicazioni protette tramite password. Vedere HP Client Security a pagina 13.
- Device Access Manager per HP Client Security consente ai responsabili IT di limitare l'accesso ai dispositivi scrivibili in modo che le informazioni sensibili non possano essere copiate dal disco rigido. Vedere HP Device Access Manager (solo in determinati modelli) a pagina 43.

Creazione di criteri per password complesse

Se i criteri aziendali richiedono l'utilizzo di criteri della password per dozzine di database e applicazioni basate sul Web, Password Manager offre un archivio protetto per le password e la funzione Single Sign On. Vedere Password Manager a pagina 19.

Elementi per protezione aggiuntiva

Assegnazione di ruoli di protezione

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

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

Per HP Client Security, gli obblighi e i privilegi di sicurezza possono essere divisi secondo i ruoli seguenti:

- Addetto alla protezione: definisce il livello di protezione per l'azienda o la rete e determina le funzioni di protezione da distribuire, ad es. Drive Encryption.

  NOTA: Molte funzioni di HP Client Security possono essere personalizzate dall'addetto alla protezione in collaborazione con HP. Per ulteriori informazioni, consultare 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 distribuire le smart card, l'amministratore IT può attivare la modalità password e smart card.
- Utenti: utilizzano le funzioni di protezione. Ad esempio, se il responsabile per la protezione e l'amministratore IT hanno attivato le smart card per il sistema, l'utente può impostare il PIN smart card e utilizzare la card per l'autenticazione.

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

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

Gestione delle password di HP Client Security

Molte funzioni di protezione HP Client Security utilizzano le password. Nelle seguenti tabelle vengono elencate le più comuni password utilizzate, i moduli software in cui è impostata la password e la funzione della password.

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

Password di HP Client Security	Modulo di impostazione	Funzione
Password di accesso Windows	Pannello di controllo di Windows o HP Client Security	Può essere utilizzata per l'accesso manuale e per l'autenticazione di accesso a varie funzionalità di HP Client Security.
Password di backup e ripristino di HP Client Security	HP Client Security, dal singolo utente	Protegge l'accesso al file di backup e ripristino di HP Client Security.
PIN della Smart Card	Credential Manager	Può essere utilizzato come autenticazione a più fattori. Può essere utilizzato come autenticazione Windows. Se è selezionata la smart card, autentica gli utenti di Drive Encryption.

Creazione di una password sicura

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

- Utilizzare password con più di 6 caratteri, preferibilmente più di 8.
- Utilizzare sia lettere maiuscole che minuscole.
- Quando possibile, utilizzare caratteri alfanumerici e includere caratteri speciali e segni di punteggiatura.
- Sostituire i caratteri speciali o i numeri con le lettere, ad esempio utilizzare il numero 1 per le lettere I o L.
- Combinare parole di 2 o più lingue.
- Suddividere una parola o frase con numeri o caratteri speciali al centro, ad esempio, “Maria2-2Cat45.”
- Non utilizzare come password una parola che potrebbe essere presente in un dizionario.
- Non utilizzare il proprio nome come password o qualsiasi altra informazione personale quale data di nascita, nomi di animali domestici o nome da nubile della madre, anche se utilizzati al contrario.
- Cambiare le password periodicamente. È possibile cambiare anche soltanto un paio di caratteri per aumentarne la sicurezza.
- Se si trascrive la password, non tenerla vicino al computer.
- Non salvare la password in un file, ad esempio in un'e-mail sul computer.
- Non condividere gli account o comunicare la password a terzi.

Backup delle credenziali e delle impostazioni

È possibile utilizzare lo strumento di Backup e ripristino in HP Client Security come posizione centrale da cui poter eseguire il backup e ripristinare le credenziali di protezione da alcuni dei moduli HP Client Security.

2 Informazioni introduttive

Per configurare HP Client Security per l'utilizzo con le proprie credenziali, avviare HP Client Security con una delle seguenti modalità. Una volta che la procedura guidata è stata completata da un utente, essa non può essere avviata nuovamente da tale utente.

1. Dalla schermata Start o Apps, fare clic su o toccare l'app **HP Client Security** (Windows 8).

   oppure

   Dal Desktop di Windows, fare clic su o toccare **HP Client Security Gadget** (Windows 7).

   oppure

   Dal desktop di Windows, fare doppio clic su o toccare con due colpetti leggeri l'icona **HP Client Security** nell'area di notifica situata a destra della barra delle applicazioni.

   oppure

   Dal desktop di Windows, fare clic su o toccare con due colpetti leggeri l'icona **HP Client Security** nell'area di notifica, quindi selezionare **Open HP Client Security** (Apri HP Client Security).

2. L'impostazione guidata di HP Client Security viene avviata con la visualizzazione della Pagina di benvenuto.

3. Leggere la schermata di benvenuto, eseguire la verifica dell'identità immettendo la password di Windows, quindi fare clic su o toccare **Avanti**.

   Se non si dispone ancora di una password di Windows, verrà richiesto di crearne una. La password di Windows è necessaria per poter proteggere l'account di Windows dall'accesso non autorizzato e poter utilizzare le funzioni di HP Client Security features.

4. Nella pagina HP SpareKey, selezionare tre domande per la protezione dei dati. Immettere la risposta a ciascuna domanda, quindi fare clic su **Avanti**. Sono consentite domande personalizzate. Per ulteriori informazioni, vedere HP SpareKey - Recupero della password a pagina 15.

5. Nella pagina Impronte digitali, registrare almeno il numero minimo di impronte digitali necessarie, quindi fare clic su o toccare **Avanti**. Per ulteriori informazioni, vedere Impronte digitali a pagina 13.

6. Nella pagina Drive Encryption, attivare la crittografia, eseguire il backup della chiave di crittografia, quindi fare clic su o toccare **Avanti**. Per ulteriori informazioni, vedere la Guida del software di HP Drive Encryption.

NOTA: Questo è valido per uno scenario in cui l'utente è un amministratore, e l'impostazione guidata di HP Client Security non è stata configurata da un amministratore in precedenza.

7. Nella pagina finale della procedura guidata, fare clic su o toccare **Fine**.

   Questa pagina fornisce lo stato di funzioni e credenziali.

8. L'impostazione guidata di HP Client Security garantisce l'attivazione delle funzioni di Just In Time Authentication e di File Sanitizer. Per ulteriori informazioni, consultare la Guida del software di HP Device Access Manager e la Guida del software di HP File Sanitizer.

NOTA: Questo è valido per uno scenario in cui l'utente è un amministratore, e l'impostazione guidata di HP Client Security non è stata configurata da un amministratore in precedenza.

Aprire HP Client Security

È possibile aprire l'applicazione HP Client Security in uno dei seguenti modi:

NOTA: L'impostazione guidata di HP Client Security deve essere completata prima che l'applicazione HP Client Security possa essere avviata.

- Dalla schermata Start o Apps, fare clic su o toccare l'app **HP Client Security**.

  – oppure –

  Dal desktop di Windows, fare clic su o toccare **HP Client Security Gadget** (Windows 7).

  – oppure –

  Dal desktop di Windows, fare doppio clic su o toccare con due colpetti leggeri l'icona **HP Client Security** nell'area di notifica situata a destra della barra delle applicazioni.

  – oppure –

  Dal desktop di Windows, fare clic su o toccare con due colpetti leggeri l'icona **HP Client Security** nell'area di notifica, quindi selezionare **Open HP Client Security** (Apri HP Client Security).

3 Guida rapida all'installazione per piccole aziende

Questo capitolo intende dimostrare i passaggi basilari per l'attivazione delle opzioni più comuni e maggiormente utili all'interno di HP Client Security per le piccole aziende. Numerosi strumenti e opzioni di questo software consentono all'utente di ottimizzare le proprie preferenze e impostare il controllo di accesso. Lo scopo di questa Guida di installazione rapida è di consentire il funzionamento di ciascun modulo in tempi brevi e con il minimo sforzo. Per ulteriori informazioni, selezionare il modulo interessato, quindi fare clic su **?** o sul pulsante Guida nell'angolo in alto a destra. Questo pulsante visualizza automaticamente le informazioni di aiuto relative alla finestra visualizzata.

Guida introduttiva

1. Dal desktop di Windows, aprire HP Client Security facendo doppio clic sull'icona **HP Client Security** nell'area di notifica collocata all'estrema destra della barra delle applicazioni.
2. Immettere la password di Windows o crearne una.
3. Completare l'esecuzione di HP Client Security Setup.

Per fare in modo che HP Client Security richieda l'autenticazione una sola volta quando si accede a Windows, vedere Funzionalità di protezione a pagina 27.

Password Manager

Chiunque dispone di un certo numero di password, in particolare se si accede regolarmente a siti Web o si utilizzano applicazioni che richiedono l'accesso. L'utente normale utilizza la stessa password per ciascuna applicazione o sito Web o sceglie delle password creative e dimentica immediatamente la password relativa a ciascuna applicazione.

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

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

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

1. Ad esempio, provate ad accedere a un sito o un'applicazione ad accesso ristretto, poi fate clic sull'icona di Password Manager nell'angolo in alto a sinistra della pagina Web.
2. Assegnare un nome al collegamento (facoltativo) e immettere un nome utente e una password in Password Manager.
3. Al termine, fare clic sul pulsante **OK**.
4. Password Manager può anche salvare il nome utente e le password per le condivisioni di rete o per le unità di rete mappate.

Visualizzazione e gestione delle autenticazioni salvate in Password Manager

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

Per aprire Password Manager, utilizzare la combinazione di tasti Ctrl+tasto logo di Windows+h per aprire Password Manager, quindi fare clic su **Accedi** per lanciare e autenticare il collegamento.

L'opzione **Modifica** di Password Manager consente all'utente di modificare il nome, il nome di accesso e persino di conoscere le password.

HP Client Security per le piccole aziende consente di effettuare il backup di tutte le credenziali e le impostazioni e/o di copiarle su un altro computer.

HP Device Access Manager

Device Access Manager può essere usato per limitare l'utilizzo di diversi dispositivo di archiviazione esterni e interni in modo da consentire la protezione dei dati sull'unità disco rigido e facendo in modo che non escano dall'azienda. Un esempio potrebbe essere consentire a un utente di accedere ai propri dati impedendogli la copia degli stessi su un CD, un lettore musicale personale o un dispositivo di memoria USB.

1. Aprire **Device Access Manager** (vedere Apertura di Device Access Manager a pagina 43).

   Viene visualizzato l'accesso per l'utente corrente.

2. Per modificare l'accesso per utenti, gruppi o periferiche, toccare o fare clic su **Modifica**. Per ulteriori informazioni, vedere Schermata sistema a pagina 44.

HP Drive Encryption

HP Drive Encryption è usato per proteggere i dati dell'utente mediante la crittografia dell'intera unità disco rigido. I dati sull'unità disco rigido rimarranno protetti in caso di furto del PC e/o in caso di rimozione dell'unità disco rigido dal computer originale per posizionarla in un computer differente.

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

Per facilitare l'utente, i moduli software multipli sincronizzano automaticamente le password, inclusi gli account utente di Windows, i domini di autenticazione, HP Drive Encryption, Password Manager e HP Client Security.

Per impostare l'HP Drive Encryption durante la configurazione con l'impostazione guidata HP Client Security, vedere Informazioni introduttive a pagina 8.

4 HP Client Security

La Pagina iniziale di HP Client Security è la posizione centrale da cui si accede facilmente alle funzioni, alle applicazioni e alle impostazioni di HP Client Security. La Pagina iniziale è divisa in tre sezioni:

- **DATI**: consente l'accesso alle applicazioni utilizzate per la gestione della protezione dei dati.
- **DISPOSITIVO**: consente l'accesso alle applicazioni utilizzate per la gestione della protezione dei dispositivi.
- **IDENTITÀ**: fornisce l'iscrizione e la gestione delle credenziali di autenticazione.

Spostare il cursore sul riquadro di un'applicazione per visualizzare una descrizione dell'applicazione.

HP Client Security può fornire collegamenti agli utenti e impostazioni amministrative in fondo a una pagina. HP Client Security consente di accedere alle Impostazioni e funzioni avanzate toccando o facendo clic sull'icona (impostazioni) **Gear** (Dispositivo).

Caratteristiche di identità, applicazioni e impostazioni

Le caratteristiche di identità, le applicazioni e le impostazioni fornite da HP Client Security assistono l'utente nella gestione di vari aspetti dell'identità digitale. Fare clic su o toccare uno dei seguenti riquadri sulla Pagina iniziale di HP Client Security, quindi immettere la password di Windows:

- **Impronte digitali**: iscrive e gestisce le credenziali delle impronte digitali.
- **SpareKey**: configura e gestisce le credenziali HP SpareKey, che possono essere utilizzate per accedere al computer se altre credenziali sono state perse o smarrite. Permette inoltre di reimpostare la password dimenticata.
- **Password di Windows**: consente un facile accesso per modificare la password di Windows.
- **Bluetooth Devices** (Dispositivi Bluetooth): permette di registrare e gestire i dispositivi Bluetooth.
- **Cards** (Schede): permette di registrare e gestire le smart card, le schede senza contatto e le schede di prossimità.
- **PIN**: permette di registrare e gestire le credenziali PIN.
- **RSA SecurID**: permette di registrare e gestire le credenziali RSA SecurID (se l'impostazione appropriata è attivata).
- **Password Manager**: consente di gestire le password per gli account e le applicazioni online.

Impronte digitali

L'impostazione guidata di HP Client Security guida l'utente attraverso il processo di impostazione, o "iscrizione", delle impronte digitali.

È inoltre possibile registrare o cancellare le impronte digitali nella pagina Impronte digitali, a cui è possibile accedere facendo clic su o toccando l'icona **Impronte digitali** nella Pagina iniziale di HP Client Security.

1. Nella pagina Impronte digitali, passare un dito fino a quando esso venga registrato correttamente.

   Il numero di dita che devono essere registrate è indicato nella pagina. Sono preferibili l'indice o il dito medio.

2. Per eliminare le impronte digitali precedentemente registrate, fare clic su o toccare **Elimina**.

3. Per registrare dita aggiuntive, fare clic su o toccare **Enroll an additional fingerprint** (Registra impronta digitale aggiuntiva).

4. Fare clic su o toccare **Salva** prima di uscire dalla pagina.

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

- ▲ Per accedere alle Impostazioni di amministrazione delle Impronte digitali, in cui gli amministratori possono specificare l'iscrizione, la precisione e altre impostazioni, fare clic su o toccare **Administrative Settings** (Impostazioni di amministrazione) (richiede privilegi di amministratore).
- ▲ Per accedere alle Impostazioni utente delle Impronte digitali, in cui è possibile specificare le impostazioni che regolano l'aspetto e il comportamento del riconoscimento mediante impronte digitali, fare clic su o toccare **User Settings** (Impostazioni utente).

Impostazioni di amministrazione delle Impronte digitali

Gli amministratori possono specificare l'iscrizione, la precisione e altre impostazioni per un lettore di impronte digitali. Sono necessari i privilegi di amministratore.

- ▲ Per accedere alle Impostazioni di amministrazione per le credenziali delle impronte digitali, fare clic su o toccare **Administrative Settings** (Impostazioni di amministrazione) nella pagina Impronte digitali.

- **Registrazione utente**: scegliere il numero minimo e massimo di impronte digitali che un utente può registrare.
- **Recognition** (Riconoscimento): spostare il dispositivo di scorrimento per regolare la sensibilità di scansione del lettore di impronte digitali al passaggio del dito.

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

Impostazioni utente delle Impronte digitali

Nella pagina Impostazioni utente impronte digitali, è possibile specificare le impostazioni che regolano l'aspetto e il comportamento del riconoscimento delle impronte digitali.

▲ Per accedere alle Impostazioni utente per le credenziali delle impronte digitali, fare clic su o toccare **User Settings** (Impostazioni utente) nella pagina Impronte digitali.

- **Attiva feedback acustico**: quando è stata eseguita la scansione di un'impronta digitale, in HP Client Security viene riprodotto un feedback acustico con suoni diversi in corrispondenza di eventi di programma specifici. È possibile assegnare nuovi suoni a questi eventi tramite la scheda Suoni nel Pannello di controllo di Windows oppure disabilitare il feedback audio deselezionando la casella di controllo.
- **Mostra feedback qualità scansione**: selezionare la casella di controllo per visualizzare tutte le scansioni, a prescindere dalla qualità. Deselezionare la casella di controllo per visualizzare solo le scansioni di buona qualità.

HP SpareKey - Recupero della password

HP SpareKey consente di accedere al computer in uso (su piattaforme supportate) fornendo la risposta a tre domande per la protezione.

HP Client Security richiede di configurare la HP SpareKey personale durante l'impostazione guidata iniziale di HP Client Security.

Per configurare HP SpareKey, procedere come segue:

1. Nella pagina HP SpareKey della procedura guidata selezionare le tre domande di protezione, quindi immettere la risposta per ciascuna risposta.

   È possibile selezionare una domanda da un elenco predefinito o scrivere una domanda.

2. Fare clic su o toccare **Registra**.

Per eliminare HP SpareKey, procedere come segue:

▲ Fare clic su o toccare **Elimina SpareKey**.

Una volta configurata la SpareKey, è possibile utilizzarla per accedere al computer da una schermata di accesso di Autenticazione all'accensione oppure dalla schermata di benvenuto di Windows.

È possibile selezionare diverse domande o modificare le risposte nella pagina SpareKey, alla quale si accede dal riquadro del Recupero password nella Pagina iniziale di HP Client Security.

Per accedere alle Impostazioni di HP SpareKey, dove un amministratore può specificare le impostazioni relative alle credenziali di HP SpareKey, fare clic su **Impostazioni** (richiede privilegi di amministratore).

Impostazioni SpareKey di HP

Nella pagina delle Impostazioni di HP SpareKey, è possibile specificare le impostazioni che regolano il comportamento e l'utilizzo delle credenziali di HP SpareKey.

▲ Per aprire la pagina delle Impostazioni di HP SpareKey, fare clic su o toccare **Impostazioni** sulla pagina HP SpareKey (richiede privilegi di amministratore).

Gli amministratori possono selezionare le seguenti impostazioni:

- Specificare le domande che vengono presentate a ciascun utente durante l'impostazione di HP SpareKey.
- Aggiungere fino a tre domande sulla protezione personalizzate da aggiungere all'elenco presentato agli utenti.
- Scegliere se consentire o meno agli utenti di scrivere le proprie domande sulla protezione.
- Specificare quali ambienti di autenticazione (Windows o Autenticazione all'accensione) consentono 'utilizzo di HP SpareKey per il recupero della password.

Password di Windows

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

Per modificare la password di Windows, procedere come segue:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare **Password di Windows**.
2. Immettere la password corrente nella casella di testo **Password di Windows corrente**.
3. Digitare la nuova password nella casella di testo **Nuova password di Windows**, quindi immetterla di nuovo nella casella di testo **Conferma nuova password**.
4. Fare clic su o toccare **Modifica** per sostituire immediatamente la password corrente con quella nuova appena immessa.

Dispositivi Bluetooth

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

NOTA: Sono supportati soltanto i telefoni Bluetooth.

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

Per accedere alla pagina Impostazioni dei Dispositivi Bluetooth a pagina 16 dove un amministratore può specificare le impostazioni per i dispositivi Bluetooth, fare clic su **Impostazioni** (richiede privilegi di amministratore).

Impostazioni dei Dispositivi Bluetooth

Gli amministratori possono specificare le seguenti impostazioni che regolano il comportamento e l'utilizzo delle credenziali dei dispositivi Bluetooth:

Autenticazione silenziosa

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Utilizza automaticamente il dispositivo Bluetooth connesso e registrato durante la verifica dell'identità): selezionare la casella di di controllo per consentire agli utenti di utilizzare le

credenziali di Bluetooth per l'autenticazione senza bisogno di un'azione da parte dell'utente, o deselezionare la casella di controllo per disabilitare questa opzione.

Prossimità Bluetooth

- **Blocca il computer quando il dispositivo Bluetooth registrato si muove fuori dall'intervallo del computer**: selezionare la casella di controllo per bloccare il computer quando un Dispositivo Bluetooth, che è stato collegato durante l'accesso, si muove fuori dall'intervallo o deselezionare la casella di controllo per disabilitare questa opzione.

NOTA: Per sfruttare questa funzione, il modulo Bluetooth del computer deve supportare questa funzionalità.

Schede

HP Client Security è in grado di supportare una serie di diversi tipi di schede di identificazione, che sono piccole schede di plastica che contengono un chip di computer. Esse includono smart card, schede senza contatto e schede di prossimità. È possibile utilizzare una scheda come credenziale di autenticazione se una di queste schede, e il lettore di schede appropriato, è collegato al computer, se l'amministratore ha installato il driver associato del relativo produttore e se ha abilitato la scheda come credenziale di autenticazione.

Il produttore delle smart card in genere fornisce gli strumenti necessari per l'installazione di un certificato di protezione e per la gestione del PIN che HP Client Security utilizzerà nei suoi algoritmi di protezione. Il numero e il tipo di caratteri usati come PIN possono variare. Per poter essere utilizzata, la smart card deve essere prima inizializzata dagli amministratori.

HP Client Security supporta i seguenti formati di smart card:

- CSP
- PKCS11

In HP Client Security, sono supportati i seguenti tipi di schede senza contatti:

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

HP Client Security supporta le seguenti schede di prossimità:

- Scheda di prossimità HID

Per registrare una smart card, procedere come segue:

1. Inserire la scheda in un lettore di smart card collegato.
2. Quando la scheda viene riconosciuta, immettere il PIN della scheda, quindi fare clic su o toccare **Registra**.

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

1. Inserire la scheda in un lettore di smart card collegato.
2. Quando la scheda viene riconosciuta, immettere il PIN della scheda, quindi fare clic su o toccare **Autentica**.
3. Fare clic su o toccare **Modifica PIN**, quindi immettere il nuovo PIN.

Per registrare una scheda senza contatto o di prossimità, procedere come segue:

1. Posizionare la scheda su o molto vicino al lettore appropriato.
2. Quando la scheda viene riconosciuta, fare clic su o toccare **Registra**.

Per eliminare una scheda registrata, procedere come segue:

1. Presentare la scheda al lettore.
2. Solo per le smart card, immettere il PIN assegnato della scheda, quindi fare clic su o toccare **Autentica**.
3. Fare clic su o toccare **Elimina**.

Una volta che la scheda è stata registrata, i dettagli della scheda vengono visualizzati in **Enrolled Cards** (Schede registrate). Quando una scheda viene eliminata, è rimossa dall'elenco.

Per accedere alle Impostazioni delle schede di prossimità, senza contatto, e smart card, in cui gli amministratori possono specificare le impostazioni relative alle credenziali delle schede, fare clic su o toccare **Impostazioni** (richiede privilegi di amministratore).

Impostazioni delle schede di prossimità, senza contatto, e smart card

Per accedere alle impostazioni di una scheda, fare clic su o toccare la scheda nell'elenco, quindi fare clic su o toccare la freccia che viene visualizzata.

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

1. Presentare la scheda al lettore
2. Immettere il PIN assegnato della scheda, quindi fare clic su o toccare **Continua**.
3. Immettere e confermare il nuovo PIN, quindi fare clic su o toccare **Continua**.

Per inizializzare il PIN smart card, procedere come segue:

1. Presentare la scheda al lettore
2. Immettere il PIN assegnato della scheda, quindi fare clic su o toccare **Continua**.
3. Immettere e confermare il nuovo PIN, quindi fare clic su o toccare **Continua**.
4. Fare clic su o toccare **Sì** per confermare l'inizializzazione.

Per cancellare i dati della scheda:

1. Presentare la scheda al lettore
2. Immettere il PIN assegnato della scheda (solo per smart card), quindi fare clic su o toccare **Continua**.
3. Fare clic su o toccare **Sì** per confermare l'eliminazione.

PIN

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

Per impostare un nuovo PIN:

- Immettere il PIN, immetterlo nuovamente per confermarlo, quindi fare clic su o toccare **Applica**.

Per eliminare un PIN, procedere come segue:

▲ Fare clic su o toccare **Elimina**, quindi fare clic su o toccare **Sì** per confermare.

Per accedere alle Impostazioni del PIN, in cui gli amministratori possono specificare le impostazioni relative alle credenziali PIN, fare clic su o toccare **Impostazioni** (richiede privilegi di amministratore).

Impostazioni PIN

Nella pagina Impostazioni PIN, è possibile specificare le lunghezze minime e massime accettabili per le credenziali PIN.

RSA SecurID

Se l'amministratore ha abilitato RSA come credenziale di autenticazione, e le seguenti condizioni sono vere, è possibile registrare o eliminare una credenziale RSA SecurID.

NOTA: È richiesta la configurazione appropriata.

- L'utente deve essere stato creato su un server RSA.
- Il token RSA SecurID assegnato all'utente e il computer devono essere stati aggiunti al dominio del Server RSA.
- Il software SecurID è installato sul computer.
- Una connessione è disponibile per il server RSA che è stato configurato correttamente.

Per registrare una credenziale RSA SecurID, procedere come segue:

▲ Inserire il nome utente e la password RSA SecurID (codice token RSA SecurID o PIN più codice token, a seconda dell'ambiente), quindi fare clic su o toccare **Applica**.

A registrazione riuscita, viene visualizzato il messaggio seguente: "Your RSA SecurID credential has been successfully enrolled" (La tua credenziale RSA SecurID è stata registrata con successo), e il pulsante Elimina è abilitato.

Per eliminare una credenziale RSA SecurID:

▲ Fare clic su **Elimina**, quindi selezionare **Sì** nella finestra di popup che chiede "Are you sure you want to delete your RSA SecurID credential?" (Eliminare la tua credenziale RSA SecurID?)

Password Manager

Accedere ai siti Web e alle applicazioni è più semplice e sicuro quando si utilizza Password Manager. È possibile creare password più sicure che non richiedono di essere memorizzate o annotate, quindi accedere facilmente e velocemente con un'impronta digitale, una smart card, una scheda di prossimità, una scheda senza contatto, un telefono Bluetooth, il PIN, le credenziali RSA, o la password di Windows.

NOTA: A causa della struttura mutevole delle schermate di accesso Web, Password Manager può non essere in grado di supportare sempre tutti i siti Web.

Password Manager offre le seguenti opzioni:

Pagina Password Manager

- Fare clic u so toccare un account per avviare automaticamente una pagina Web o un applicazione e accedere.
- Utilizzare le categorie per organizzare gli account.

Complessità della Password

- Visualizzazione rapida delle eventuali password che presentano un rischio per la protezione.
- Quando si aggiungono dati di accesso, controllare la complessità delle singole password utilizzate per i siti Web e per le applicazioni.
- La complessità della password è illustrata da indicatori di stato di color rosso, giallo o verde.

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

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

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

Per pagine Web o programmi senza accesso disponibile

Nel menu contestuale vengono visualizzate le seguenti opzioni:

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

Per pagine Web o programmi con accesso disponibile

Nel menu contestuale vengono visualizzate le seguenti opzioni:

- **Immetti i dati di accesso**: visualizza la pagina **Verifica la tua identità**. Se l'autenticazione viene eseguita correttamente, i dati di accesso vengono immessi negli appositi campi e la pagina viene inviata (se l'invio è stato specificato al momento della creazione dell'accesso o della sua ultima modifica).
- **Modifica accesso**: consente di modificare i dati di accesso al sito Web.
- **Aggiungi accesso**: consente di aggiungere un account a Password Manager.
- **Apri Password Manager**: avvia Password Manager.
- **?**: visualizza la Guida in linea di Security Manager.

NOTA: L'amministratore di questo computer potrebbe avere configurato HP Client Security affinché richieda più di una credenziale durante la verifica dell'identità.

Aggiunta di accessi

È possibile aggiungere facilmente un accesso a un sito Web o programma immettendo i dati di accesso una volta, dopodiché la loro immissione avverrà in modo automatico. È possibile utilizzare questi accessi dopo la navigazione nel sito o programma.

Per aggiungere un accesso:

1. Aprire la schermata di accesso a un sito Web o programma.
2. Fare clic su o toccare l'icona **Password Manager**, quindi fare clic su o toccare una delle seguenti opzioni a seconda che la schermata di accesso sia relativa a un sito Web o a un programma:
   - Per un sito Web, fare clic su o toccare **Aggiungi [nome dominio] a Password Manager**.
   - Per un programma, fare clic su o toccare **Aggiungi schermata accesso a Password Manager**.
3. Immettere i dati di accesso. I campi di accesso nella schermata e i campi corrispondenti nella finestra di dialogo sono identificati con un bordo arancione in grassetto.
   a. Per compilare un campo di accesso con una delle opzioni preformattate, fare clic su o toccare le frecce a destra del campo.
   b. Per visualizzare la password di accesso, fare clic su o toccare **Mostra password**.
   c. Per compilare i campi di accesso, ma non inviarli, deselezionare la casella di controllo **Invia automaticamente i dati di accesso**.
   d. Fare clic su o toccare **OK** per selezionare il metodo di autenticazione desiderato (impronte digitali, smart card, scheda di prossimità o senza contatti, telefono Bluetooth, PIN o password), quindi eseguire l'accesso con tale metodo.

      Il segno "+" viene rimosso dall'icona di **Password Manager** per indicare che l'accesso è stato creato.
   e. Se Password Manager non rileva i campi di accesso, fare clic su o toccare **Altri campi**.
      - Selezionare la casella di controllo di ciascun campo richiesto per l'accesso, oppure deselezionare la casella di controllo dei campi non richiesti per l'accesso.
      - Fare clic su o toccare **Chiudi**.

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

Modifica degli accessi

Per modificare un accesso:

1. Aprire la schermata di accesso a un sito Web o programma.
2. Per visualizzare una finestra di dialogo in cui è possibile modificare i dati di accesso, fare clic su o toccare l'icona **Password Manager**, quindi fare clic su o toccare **Modifica accesso**.

   I campi di accesso nella schermata e i campi corrispondenti nella finestra di dialogo sono identificati con un bordo arancione in grassetto.

   È inoltre possibile modificare le informazioni di account all'interno della pagina Password Manager facendo clic su o toccando l'accesso per visualizzare le opzioni di modifica, quindi selezionando **Modifica**.
3. Modificare le informazioni di accesso.
   - Per modificare il **Nome account**, immettere un nuovo nome nel campo.
   - Per aggiungere o modificare il nome di una **Categoria**, immettere o modificare il nome nel campo **Categoria**.

- Per selezionare un campo di accesso **Nome utente** con una delle scelte preformattate, fare clic su o toccare la freccia giù a destra del campo.

  Le scelte preformattate sono disponibili solo quando si modifica l'accesso dal comando Modifica nel menu contestuale dell'icona Password Manager.

- Per selezionare un campo di accesso **Password** con una delle scelte preformattate, fare clic su o toccare la freccia giù a destra del campo.

  Le scelte preformattate sono disponibili solo quando si modifica l'accesso dal comando Modifica nel menu contestuale dell'icona Password Manager.

- Per aggiungere altri campi dalla schermata all'accesso, fare clic su o toccare **Altri campi**.
- Per visualizzare la password per l'accesso, fare clic su o toccare l'icona **Mostra password**.
- Per compilare i campi di accesso, ma non inviarli, deselezionare la casella di controllo **Invia automaticamente i dati di accesso**.
- Per contrassegnare la password di questo accesso come compromessa, selezionare la casella di controllo **This password is compromised** (Questa password è compromessa).

  Dopo che le modifiche vengono salvate, tutti gli altri accessi che condividono la stessa password saranno contrassegnati come compromessi. È quindi possibile visitare ogni account interessato e modificare le password, se necessario.

4. Fare clic su o toccare **OK**.

Utilizzo del menu Collegamenti rapidi Password Manager

Password Manager offre un modo semplice e veloce per avviare i siti Web e i programmi per i quali sono stati creati gli accessi. Fare doppio clic o toccare con due colpetti leggeri l'accesso a un programma o a un sito Web dal menu **Collegamenti rapidi Password Manager** oppure dalla pagina Password Manager all'interno di HP Client Security per aprire la schermata in cui immettere i dati di accesso.

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

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

▲ Premere la combinazione di tasti di scelta rapida **Password Manager** (Ctrl+tasto del logo Windows+h è l'impostazione predefinita). Per cambiare la combinazione di tasti di scelta rapida, nella pagina iniziale di HP Client Security fare clic su **Password Manager**, quindi fare clic su o toccare **Impostazioni**.

Organizzazione degli accessi in categorie

Creare una o più categorie per mantenere in ordine gli accessi.

Per assegnare un accesso a una categoria:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare **Password Manager**.
2. Fare clic su o toccare la voce dell'account, quindi fare clic su o toccare **Modifica**.
3. Nel campo **Categoria**, immettere un nome di categoria.
4. Fare clic su o toccare **Salva**.

Per rimuovere un account da una categoria:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare **Password Manager**.
2. Fare clic su o toccare la voce dell'account, quindi fare clic su o toccare **Modifica**.
3. Nel campo **Categoria**, cancellare un nome di categoria.
4. Fare clic su o toccare **Salva**.

Per rinominare una categoria:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare **Password Manager**.
2. Fare clic su o toccare la voce dell'account, quindi fare clic su o toccare **Modifica**.
3. Nel campo **Categoria**, modificare il nome di categoria.
4. Fare clic su o toccare **Salva**.

Gestione degli accessi

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

Gli accessi vengono elencati nella pagina Password Manager.

Per gestire gli accessi:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare **Password Manager**.
2. Fare clic su o toccare un accesso esistente, selezionare una delle seguenti opzioni, quindi seguire le istruzioni visualizzate:
   - **Modifica**: modifica un accesso. Per ulteriori informazioni, vedere Modifica degli accessi a pagina 21.
   - **Accedi**: esegue l'accesso all'account selezionato.
   - **Elimina**: eliminare l'accesso all'account selezionato.

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

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

Verifica della complessità della password

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

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

Quando si immette una password durante la creazione di un accesso Password Manager a un account, una barra colorata viene visualizzata sotto la password per indicare la complessità della password. I colori indicano i seguenti valori:

- **Rosso**: bassa
- **Giallo**: discreta
- **Verde**: alta

Impostazioni dell'icona di Gestore password

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

1. Fare clic su o toccare l'icona, quindi fare clic su o toccare **Impostazioni icone** per personalizzare il modo in cui Password Manager gestisce i possibili siti di accesso.
   - **Richiedi l'aggiunta di accessi per le schermate di accesso**: fare clic su o toccare questa opzione se si desidera che Password Manager richieda di aggiungere una voce quando viene visualizzata una schermata per la quale non è stato ancora configurato un accesso.
   - **Escludi questa schermata**: selezionare questa casella di controllo se non si desidera che Password Manager richieda di nuovo di aggiungere un accesso per questa schermata.
   - **Non richiedere l'aggiunta di accessi per la schermata di accesso**: selezionare il pulsante di opzione.
2. Per aggiungere un accesso per una schermata esclusa in precedenza, procedere come segue:
   a. Accedere al sito Web precedentemente escluso.
   b. Affinché Password Manager memorizzi la password per questo sito, fare clic su o toccare **Ricorda** nella finestra di popup per salvare la password e creare un accesso per lo schermo.
3. Per accedere a ulteriori impostazioni di Password Manager, fare clic su o toccare l'icona Password Manager, fare clic su o toccare **Apri Password Manager**, quindi fare clic su o toccare **Impostazioni** nella pagina Password Manager.

Importare ed esportare accessi

Nella pagina Importa ed esporta di HP Password Manager, è possibile importare gli accessi salvati dal browser Web sul computer. È inoltre possibile importare i dati da un file di backup di HP Client Security ed esportare i dati a un file di backup di HP Client Security.

▲ Per avviare la pagina Importa ed esporta, fare clic su o toccare **Importa ed esporta** sulla pagina Password Manager.

Per importare le password da un browser:

1. Fare clic su o toccare il browser da cui si desidera importare le password (vengono visualizzati solo i browser installati).
2. Deselezionare la casella di controllo degli account per i quali non si desidera importare le password.
3. Fare clic su o toccare **Importa**.

L'importazione o l'esportazione di dati da e verso un file di backup di HP Client Security può essere realizzata attraverso i link associati (in **Altre Opzioni** (Altre Opzioni)) nella pagina Importa ed esporta.

NOTA: Questa funzione importa ed esporta soli dati Password Manager. Per informazioni sul backup e ripristino dei dati aggiuntivi di HP Client Security, vedere Backup e ripristino dei dati a pagina 29.

Per importare dati da un file di backup di HP Client Security:

1. Dalla pagina di Import ed export di HP Password Manager, fare clic su o toccare **Import data from an HP Client Security backup file** (Importa dati da un file di backup di HP Client Security).
2. Verificare l'identità.
3. Selezionare il file di backup creato in precedenza oppure immettere il percorso nel campo fornito, quindi fare clic su o toccare **Sfoglia**.
4. Immettere la password utilizzata per proteggere il file, quindi fare clic su o toccare **Avanti**.
5. Fare clic o toccare **Ripristina**.

Per esportare dati da un file di backup di HP Client Security:

1. Dalla pagina di Import ed export di HP Password Manager, fare clic su o toccare **Export data from an HP Client Security backup file** (Esporta dati da un file di backup di HP Client Security).
2. Verificare l'identità, e quindi fare clic su o toccare **Avanti**.
3. Immettere un nome per il file di backup. Per impostazione predefinita, il file viene salvato nella cartella Documenti. Per specificare una posizione diversa, fare clic su o toccare **Sfoglia**.
4. Immettere e confermare la password per proteggere il file, quindi fare clic su o toccare **Salva**.

Impostazioni

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

- **Richiedi di aggiungere gli accessi per le schermate di accesso**: l'icona di **Password Manager** con il segno "+" viene visualizzata ogni volta che viene rilevata una schermata di accesso di un sito Web o di un programma. Ciò indica che è possibile aggiungere un accesso per tale schermata nel menu **Accessi**.

  Per disabilitare questa funzione, deselezionare la casella di controllo accanto a **Richiedi di aggiungere gli accessi per le schermate di accesso**.

- **Apri Password Manager con Ctrl+Win+h**: la combinazione predefinita di tasti di scelta rapida che apre il menu **Collegamenti rapidi Password Manager** è Ctrl+tasto logo di Windows+h.

  Per modificarla, fare clic su o toccare questa opzione e immettere una nuova combinazione di tasti. Le combinazioni possono includere uno o più tasti seguenti: ctrl, alt o maiusc e qualsiasi tasto alfabetico o numerico.

  Combinazioni riservate alle applicazioni Windows o a Windows non possono essere utilizzate.

- Per ripristinare i valori delle impostazioni predefinite, fare clic su o toccare **Ripristina impostazioni predefinite**.

Impostazioni avanzate

Gli amministratori possono accedere alle seguenti opzioni selezionando l'icona (impostazioni) **Gear** (Dispositivo) nella Pagina iniziale di HP Client Security.

- **Administrator Policies** (Criteri dell'amministratore): consente di configurare i criteri di accesso e di sessione per gli amministratori.
- **Standard User Policies** (Criteri degli utenti standard): consente di configurare i criteri di accesso e di sessione per gli utenti standard.
- **Funzioni di protezione**: permette di aumentare la protezione del computer proteggendo l'account di Windows con un'autenticazione complessa e/o abilitando l'autenticazione prima dell'avvio di Windows.
- **Utenti**: consente di gestire gli utenti e le relative credenziali.
- **My Policies** (Criteri): permette di rivedere i criteri di autenticazione e lo stato di registrazione.
- **Backup e ripristino**: consente di eseguire il backup o il ripristino dei dati di HP Client Security.
- **Informazioni su HP Client Security**: consente di visualizzare le informazioni sulla versione di HP Client Security.

Criteri di amministratore

È possibile configurare i criteri di accesso e di sessione per gli amministratori di questo computer. I criteri di accesso impostati qui regolano le credenziali richieste a un amministratore locale per accedere a Windows. I criteri di sessione impostati qui regolano le credenziali richieste a un amministratore locale per verificare l'identità all'interno di una sessione di Windows.

Per impostazione predefinita, tutti i criteri nuovi o modificati vengono applicati immediatamente dopo aver toccato o fatto clic su **Applica**.

Per aggiungere un nuovo criterio:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare l'icona **Gear** (Dispositivo).
2. Nella pagina Impostazioni avanzate, fare clic su o toccare **Administrator Policies** (Criteri dell'amministratore).
3. Fare clic su o toccare **Add new policy** (Aggiungi nuovo criterio).
4. Fare clic sulla freccia giù per selezionare le credenziali primarie e secondarie (opzionale) per il nuovo criterio, quindi fare clic su o toccare **Aggiungi**.
5. Fare clic su **Applica**.

Per ritardare l'attuazione di un criterio nuovo o modificato:

1. Fare clic su o toccare **Enforce this policy immediately** (Imponi questo criterio immediatamente).
2. Selezionare **Enforce this policy on the specific date** (Imponi questo criterio in una data specifica).
3. Immettere una data o utilizzare il calendario popup per selezionare la data in cui si desidera imporre tale criterio.
4. Se si desidera, selezionare la data in cui ricordare agli utenti l'imposizione del nuovo criterio.
5. Fare clic su **Applica**.

Criteri degli utenti standard

È possibile configurare i criteri di accesso e di sessione per gli utenti standard di questo computer. I criteri di accesso impostati qui regolano le credenziali richieste a un utente standard per accedere a Windows. I criteri di sessione impostati qui regolano le credenziali richieste a un utente standard per verificare l'identità all'interno di una sessione di Windows.

Per impostazione predefinita, tutti i criteri nuovi o modificati vengono applicati immediatamente dopo aver toccato o fatto clic su **Applica**.

Per aggiungere un nuovo criterio:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare l'icona **Gear** (Dispositivo).
2. Nella pagina Impostazioni avanzate, fare clic su o toccare **Standard User Policies** (Criteri degli utenti standard).
3. Fare clic su o toccare **Add new policy** (Aggiungi nuovo criterio).
4. Fare clic sulla freccia giù per selezionare le credenziali primarie e secondarie (opzionale) per il nuovo criterio, quindi fare clic su o toccare **Aggiungi**.
5. Fare clic su **Applica**.

Per ritardare l'attuazione di un criterio nuovo o modificato:

1. Fare clic su o toccare **Enforce this policy immediately** (Imponi questo criterio immediatamente).
2. Selezionare **Enforce this policy on the specific date** (Imponi questo criterio in una data specifica).
3. Immettere una data o utilizzare il calendario popup per selezionare la data in cui si desidera imporre tale criterio.
4. Se si desidera, selezionare la data in cui ricordare agli utenti l'imposizione del nuovo criterio.
5. Fare clic su **Applica**.

Funzionalità di protezione

È possibile abilitare le funzionalità di HP Client Security per contribuire a proteggere dall'accesso non autorizzato al computer.

Per configurare le funzionalità di protezione, procedere come segue:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare l'icona **Gear** (Dispositivo).
2. Nella pagina Impostazioni avanzate, fare clic su o toccare **Funzioni di protezione**.

3. Selezionare le caselle di controllo corrispondenti alle funzionalità di protezione desiderate, quindi fare clic su **Applica**. Più funzioni si selezionano, più protetto sarà il computer.

   queste impostazioni risultano valide per tutti gli utenti.

   - **Protezione di accesso a Windows**: protegge gli account Windows richiedendo l'utilizzo di credenziali HP Client Security per l'accesso.
   - **Pre-Boot Security (Power-on authentication)** (Protezione di preavvio (Autenticazione all'accensione)): protegge il computer prima dell'avvio di Windows. la funzione Protezione preavvio non è disponibile se il BIOS non la supporta.
   - **Consenti accesso One Step logon**: questa impostazione consente di saltare l'accesso a Windows se l'autenticazione è stata precedentemente eseguita a livello di Autenticazione all'accensione o di Drive Encryption.

4. Toccare o fare clic su **Utenti**, quindi toccare o fare clic sul riquadro dell'utente.

Utenti

È possibile monitorare e gestire gli utenti di HP Client Security di questo computer.

Per aggiungere un altro utente di Windows a HP Client Security, procedere come segue:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare l'icona **Gear** (Dispositivo).
2. Nella pagina Impostazioni avanzate, fare clic su o toccare **Utenti**.
3. Fare clic su o toccare **Add another Windows user to HP Client Security** (Aggiungi un altro utente di Windows a HP Client Security).
4. Immettere il nome dell'utente che si desidera aggiungere, quindi fare clic su o toccare **OK**.
5. Immettere la password dell'utente di Windows selezionato.

   Nella Pagina utente viene visualizzato un riquadro per l'utente aggiunto.

Per eliminare un utente di Windows da HP Client Security, procedere come segue:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare l'icona **Gear** (Dispositivo).
2. Nella pagina Impostazioni avanzate, fare clic su o toccare **Utenti**.
3. Fare clic su o toccare il nome dell'utente che si desidera eliminare.
4. Toccare o fare clic su **Elimina utente**, quindi toccare o fare clic su **Sì** per confermare.

Per visualizzare una sintesi dei criteri di accesso e di sessione applicate a un utente, procedere come segue:

▲ Toccare o fare clic su **Utenti**, quindi toccare o fare clic sul riquadro dell'utente.

Criteri

È possibile visualizzare i criteri di autenticazione e lo stato di registrazione. La pagina Criteri fornisce anche i collegamenti alle pagine dei criteri degli amministratori e dei criteri degli utenti standard.

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare l'icona **Gear** (Dispositivo).
2. Nella pagina Impostazioni avanzate, fare clic su o toccare **My Policies** (Criteri).

   Vengono visualizzati i criteri di accesso e di sessione applicati all'utente attualmente connesso.

La pagina Criteri fornisce inoltre i link a Criteri di amministratore a pagina 26 e Criteri degli utenti standard a pagina 27.

Backup e ripristino dei dati

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

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

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

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

Per eseguire il backup dei dati:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare l'icona **Gear** (Dispositivo).
2. Nella pagina Impostazioni avanzate, fare clic su o toccare **Administrator Policies** (Criteri dell'amministratore).
3. Fare clic su o toccare **Backup e ripristino**.
4. Fare clic su o toccare **Backup**, quindi verificare l'identità.
5. Selezionare il modulo che si desidera includere nel backup, quindi fare clic su o toccare **Avanti**.
6. Inserire un nome per il file di archiviazione. Per impostazione predefinita, il file viene salvato nella cartella Documenti. Per specificare una posizione diversa, fare clic su o toccare **Sfoglia**.
7. Immettere e confermare una password per proteggere il file.
8. Fare clic su o toccare **Salva**.

Per ripristinare i dati:

1. Dalla Pagina iniziale di HP Client Security, fare clic su o toccare l'icona **Gear** (Dispositivo).
2. Nella pagina Impostazioni avanzate, fare clic su o toccare **Administrator Policies** (Criteri dell'amministratore).
3. Fare clic su o toccare **Backup e ripristino**.
4. Selezionare **Ripristina**, quindi verificare l'identità.
5. Selezionare il file di archiviazione creato in precedenza. Specificare il percorso nell'apposito campo. Per specificare una posizione diversa, fare clic su o toccare **Sfoglia**.
6. Immettere la password utilizzata per proteggere il file, quindi fare clic su o toccare **Avanti**.
7. Selezionare i moduli di cui ripristinare i dati.
8. Fare clic o toccare **Ripristina**.

5 HP Drive Encryption (solo in determinati modelli)

HP Drive Encryption garantisce la protezione completa dei dati del computer tramite crittografia. Una volta attivato Drive Encryption, sarà necessario accedere tramite la schermata di accesso di Drive Encryption visualizzata prima dell'avvio del sistema operativo Windows®.

La Schermata iniziale HP Client Security consente agli amministratori di Windows di attivare Drive Encryption, eseguire il backup della chiave di crittografia, selezionare o deselezionare le unità o le partizioni per la crittografia. Per ulteriori informazioni, vedere la Guida del software di HP Client Security.

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

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

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

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

Apertura di Drive Encryption

Gli amministratori possono accedere a Drive Encryption aprendo HP Client Security:

1. Dalla schermata Start, fare clic o toccare l'app **HP Client Security** (Windows 8).

   – oppure –

   Dal desktop di Windows, fare doppio clic su o toccare con due colpetti leggeri l'icona **HP Client Security** nell'area di notifica situata a destra della barra delle applicazioni.

2. Fare clic su o toccare l'icona **Drive Encryption**.

Attività generali

Attivazione di Drive Encryption per le unità disco rigido standard

La crittografia delle unità disco rigido standard viene eseguita tramite software. Seguire la procedura riportata di seguito per crittografare un'unità o una partizione del disco:

1. Avviare **Drive Encryption**. Per ulteriori informazioni, vedere Apertura di Drive Encryption a pagina 30.
2. Selezionare la casella di controllo per l'unità o la partizione che si desidera crittografare, quindi fare clic su o toccare **Backup Key** (Esegui backup chiave).

NOTA: Per maggiore protezione, selezionare la casella di controllo **Disable sleep mode for increased security** (Disabilita modalità sospensione per maggiore protezione). Quando si disabilita la modalità di sospensione, non vi sono rischi che le credenziali utilizzate per sbloccare l'unità vengano archiviate in memoria.

3. Selezionare una o più delle opzioni di backup, quindi fare clic su o toccare **Backup**. Per ulteriori informazioni, vedere Backup delle chiavi di crittografia a pagina 34.
4. È possibile continuare a lavorare mentre si esegue il backup della chiave di crittografia. Non riavviare il computer.

NOTA: Viene richiesto di riavviare il computer. Dopo il riavvio, viene visualizzata la schermata di preavvio di Drive Encryption che richiede di eseguire l'autenticazione prima del nuovo avvio di Windows.

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

Per ulteriori informazioni, vedere la Guida del software di HP Client Security.

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

Le unità che supportano la crittografia automatica conformi alle specifiche OPAL del Trusted Computing Group relative alla gestione delle unità SED possono essere crittografate tramite crittografia basata sul software e sull'hardware. La crittografia dell'hardware è molto più rapida rispetto alla crittografia basata sul software. Tuttavia non è possibile scegliere quali partizioni del disco crittografare. L'intero disco, comprese le partizioni del disco, è crittografato.

Per crittografare partizioni specifiche, utilizzare la crittografia basata sul software. Assicurarsi di deselezionare la casella di controllo **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Consentire crittografia hardware solo per unità con crittografia automatica (SED)).

Attenersi ai passaggi riportati di seguito per attivare le unità che supportano la crittografia automatica:

1. Avviare **Drive Encryption**. Per ulteriori informazioni, vedere Apertura di Drive Encryption a pagina 30.
2. Selezionare la casella di controllo per l'unità che si desidera crittografare, quindi toccare o fare clic su **Chiave di backup**.

NOTA: Per maggiore protezione, selezionare la casella di controllo **Disabilita modalità sospensione per maggiore protezione**. Quando si disabilita la modalità di sospensione, non vi sono rischi che le credenziali utilizzate per sbloccare l'unità vengano archiviate in memoria.

3. Selezionare una o più delle opzioni di backup, quindi fare clic su o toccare **Backup**. Per ulteriori informazioni, vedere Backup delle chiavi di crittografia a pagina 34.

4. È possibile continuare a lavorare mentre si esegue il backup della chiave di crittografia. Non riavviare il computer.

NOTA: Per le unità con crittografia automatica, viene richiesto di spegnere il computer.

Per ulteriori informazioni, vedere la Guida del software di HP Client Security.

Disattivazione di Drive Encryption

1. Avviare **Drive Encryption**. Per ulteriori informazioni, vedere Apertura di Drive Encryption a pagina 30.

2. Deselezionare la casella di controllo per tutte le unità crittografate, quindi fare clic su o toccare **Apply** (Applica).

   Ha inizio la disattivazione di Drive Encryption.

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

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

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

Accesso dopo l'attivazione di Drive Encryption

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

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

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

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

Accesso utente singolo:

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

Accesso multi-utente:

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

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

Smart card supportate

- Gemalto Cyberflex Access 64k V2c

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

Crittografia di Unità disco rigido aggiuntive

Si consiglia vivamente di utilizzare HP Drive Encryption per proteggere i dati crittografando il disco rigido. Dopo l'attivazione, è possibile crittografare qualsiasi unità disco rigido aggiunta attenendosi alla seguente procedura:

1. Avviare **Drive Encryption**. Per ulteriori informazioni, vedere Apertura di Drive Encryption a pagina 30.
2. Per le unità crittografate tramite software, selezionare le partizioni da crittografare.

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

– Oppure –

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

Attività avanzate

Gestione di Drive Encryption (attività dell'amministratore)

Gli amministratori possono utilizzare Drive Encryption per visualizzare e modificare lo stato di crittografia (non crittografate o crittografate) di tutte le unità disco rigido del computer.

- Se lo stato è abilitato, Drive Encryption è stato attivato e configurato. L'unità si trova in uno dei seguenti stati:

Crittografia basata sul software

- Nessuna crittografia
- Crittografata
- Crittografia in corso
- Decrittografia in corso

Crittografia basata sull'hardware

- Crittografata
- Non crittografate (per unità aggiuntive)

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

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

1. Avviare **Drive Encryption**. Per ulteriori informazioni, vedere Apertura di Drive Encryption a pagina 30.
2. In **Stato unità**, selezionare o deselezionare la casella di controllo corrispondente a ogni partizione dell'unità disco rigido che si desidera crittografare o decrittografare, quindi toccare o fare clic su **Applica**.

NOTA: Durante le operazioni di crittografia o decrittografia di una partizione, una barra di avanzamento visualizza la percentuale di partizione crittografata.

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

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

Gestione disco

- **Nickname** (Nome alternativo): è possibile assegnare nomi alle unità o alle partizioni per una più facile identificazione.
- **Disconnected drives** (Unità disconnessa): Drive Encryption è in grado di identificare i dischi che vengono rimossi dal computer. Un disco che viene rimosso dal computer viene automaticamente spostato nell'Elenco disconnessi. Se il disco viene restituito al sistema, verrà nuovamente visualizzato nell'Elenco connessi.
- Se non si ha più bisogno di identificare o gestire l'unità disconnessa, è possibile rimuovere l'unità scollegata dall'Elenco disconnessi.
- Drive Encryption rimane attiva fino a quando le caselle di controllo per tutte le unità connesse vengono deselezionate, e l'Elenco disconnessi è vuoto.

Backup e ripristino (attività amministratore)

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

Backup delle chiavi di crittografia

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

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

1. Avviare **Drive Encryption**. Per ulteriori informazioni, vedere Apertura di Drive Encryption a pagina 30.
2. Selezionare la casella di controllo per un'unità, quindi toccare o fare clic su **Chiave di backup**.
3. In **Create HP Drive Encryption recovery key** (Crea chiave di ripristino HP Drive Encryption), selezionare una o più delle seguenti opzioni:
   - **Removable Storage** (Dispositivo di archiviazione rimovibile): selezionare la casella di controllo, quindi selezionare il dispositivo di archiviazione in cui salvare la chiave di crittografia.
   - **SkyDrive**: selezionare la casella di controllo. È necessario essere collegati ad Internet. Accedere a Microsoft SkyDrive, quindi fare clic su o toccare **Sì**.

     NOTA: Per utilizzare la chiave di backup HP Drive Encryption memorizzata su SkyDrive, è necessario scaricarla da SkyDrive su un dispositivo di archiviazione rimovibile, quindi inserire il dispositivo di archiviazione nel computer.
   - **TPM** (solo su determinati modelli): consente di recuperare i dati utilizzando la password TPM.

     ATTENZIONE: Se il TPM viene cancellato o il computer è danneggiato, si perderà l'accesso al backup. Se questo metodo è stato selezionato, è consigliabile selezionare un altro metodo di backup.
4. Fare clic su o toccare **Backup** (Backup).

   La chiave di crittografia viene salvata nel dispositivo di archiviazione selezionato.

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

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

1. Inserire il dispositivo di archiviazione rimovibile in cui è memorizzata la chiave di backup.
2. Accendere il computer.
3. Quando viene visualizzata la finestra di dialogo di accesso di HP Drive Encryption, fare clic su o toccare **Ripristino**.
4. Immettere il nome o il percorso del file contenente la chiave di backup, quindi fare clic su **Ripristino**.
5. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su o toccare **OK**.

   La finestra di accesso di Windows è visualizzata.

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

Esecuzione di un ripristino con HP SpareKey

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

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

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

   NOTA: Se la SpareKey non è stata inizializzata in HP Client Security, il pulsante **SpareKey** non è disponibile.

4. Digitare le risposte corrette alle domande visualizzate, quindi fare clic su **Accesso**.

   La finestra di accesso di Windows è visualizzata.

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

6 File Sanitizer HP (solo in determinati modelli)

File Sanitizer consente di distruggere in modo sicuro risorse quali dati o file personali, dati cronologici o correlati al Web oppure componenti di altri dati presenti sull'unità disco rigido interna del computer in uso, e di eseguire un'operazione di pulitura periodica dell'unità.

HP File Sanitizer non può essere utilizzato con i seguenti tipi di unità:

- Unità a stato solido, inclusi i volumi RAID di un dispositivo SSD
- Unità esterne collegate tramite interfaccia eSATA, USB o firewire

Se si tenta di distruggere o pulire i dati di un'unità a stato solido, viene visualizzato un messaggio di avviso e l'operazione non viene eseguita.

Distruzione

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

È possibile pianificare un orario di distruzione futuro, oppure è possibile attivare manualmente la distruzione selezionando l'icona **File Sanitizer** nella schermata iniziale HP Client Security o utilizzando l'icona **File Sanitizer** sul desktop di Windows. Per ulteriori informazioni, fare riferimento alla sezione Impostazione della distruzione pianificata dei dati a pagina 39, Distruzione facendo clic con il pulsante destro del mouse a pagina 41 o Avvio manuale di un'operazione di distruzione a pagina 41.

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

Pulizia dello spazio libero

Con l'eliminazione di una risorsa in Windows, non vengono rimossi completamente i contenuti dall'unità disco rigido, ma solo il riferimento a tale risorsa o alla sua posizione sull'unità disco rigido. I contenuti della risorsa rimangono nell'unità disco rigido finché l'area da essi occupata non viene sovrascritta con nuovi dati di un'altra risorsa.

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

NOTA: La pulizia dello spazio libero non fornisce ulteriore protezione per le risorse distrutte.

È possibile impostare un orario futuro di pulitura dello spazio libero, oppure è possibile attivare manualmente la pulitura dello spazio libero di risorse precedentemente distrutte selezionando l'icona **File Sanitizer** nella schermata iniziale HP Client Security o utilizzando l'icona **File Sanitizer** sul desktop di Windows. Per ulteriori informazioni, fare riferimento alla sezione Impostazione della

pianificazione per la pulitura dello spazio libero a pagina 40, Avvio manuale della pulitura dello spazio libero a pagina 42 o Uso dell'icona File Sanitizer a pagina 41.

Apertura di File Sanitizer

1. Dalla schermata Start, fare clic o toccare l'app **HP Client Security** (Windows 8).

   – oppure –

   Dal desktop di Windows, fare doppio clic su o toccare con due colpetti leggeri l'icona **HP Client Security** nell'area di notifica situata a destra della barra delle applicazioni.

2. In **Dati**, fare clic su o toccare **File Sanitizer**.

– Oppure –

▲ Fare doppio clic su o toccare con due colpetti leggeri l'icona **File Sanitizer** disponibile sul desktop di Windows.

oppure

▲ Fare clic con il pulsante destro del mouse su o toccare e tenere premuta l'icona **File Sanitizer** sul desktop di Windows, quindi selezionare **Apri File Sanitizer**.

Procedure di installazione

Distruzione: File Sanitizer elimina o distrugge in modo protetto selezionate categorie di risorse.

1. In **Distruzione**, selezionare la casella di controllo per ogni tipo di file da distruggere, o deselezionare la casella di controllo per non distruggere tali file.
   - **Cestino**: distrugge tutte i file all'interno del Cestino.
   - **File di sistema temporanei**: distrugge tutti i file trovati nella cartella temporanea del sistema. La ricerca delle variabili di ambiente viene eseguita nel seguente ordine e il primo percorso individuato viene considerato come la cartella di sistema:
     - TMP
     - TEMP
   - **File Internet temporanei**: distrugge copie di pagine Web, immagini, e file multimediali salvati dai browser Web per una visualizzazione più rapida.
   - **Cookies**: distrugge tutti i file memorizzati dai siti Web su un computer per salvare preferenze come i dati di login.
2. Per iniziare la distruzione, fare clic su o toccare **Distruggi**.

Pulitura: scrive dati senza significato per liberare spazio e impedisce il recupero di file eliminati.

▲ Per iniziare la pulitura, fare clic su o toccare **Pulisci**.

File Sanitizer Options (Opzioni File Sanitizer): selezionare o deselezionare le caselle di controllo corrispondenti alle seguenti opzioni che si desidera abilitare o disabilitare:

- **Enable Desktop icon** (Abilita Icona Desktop): visualizza l'icona File Sanitizer sul desktop di Windows.
- **Enable right-click** (Abilita pulsante destro del mouse): consente di fare clic con il pulsante destro del mouse su o toccare e tenere premuta una risorsa, quindi selezionare **HP File Sanitizer – Distruggi**.

- **Ask for Windows password before manual shredding** (Chiedi la password di Windows prima della distruzione manuale): richiede l'autenticazione con la password di Windows prima della distruzione manuale di un file.
- **Shred Cookies and Temporary Internet Files on browser close** (Distruggi cookie e file Internet temporanei alla chiusura del browser): al momento della chiusura del browser Web vengono distrutte tutte le risorse correlate al Web, ad esempio la cronologia degli URL.

Impostazione della distruzione pianificata dei dati

È possibile programmare un orario per eseguire automaticamente la distruzione, oppure è anche possibile distruggere le risorse manualmente in qualsiasi momento. Per ulteriori informazioni, consultare Procedure di installazione a pagina 38.

1. Aprire File Sanitizer, quindi fare clic su o toccare **Impostazioni**.
2. Per programmare un tempo futuro per la distruzione delle risorse selezionate, in **Shred Schedule** (Pianificazione della distruzione), selezionare **Never** (Mai), **Once** (Una volta), **Daily** (Ogni giorno), **Weekly** (Ogni settimana) oppure **Monthly** (Ogni mese), quindi selezionare un giorno e l'ora:
   a. Fare clic su o toccare l'ora, il minuto, o il campo AM/PM.
   b. Scorrere fino a quando il valore desiderato è stato visualizzato sullo stesso livello degli altri campi.
   c. Fare clic su o toccare lo spazio bianco che circonda i campi di impostazione dell'orario.
   d. Ripetere l'operazione per ogni campo fino a quando è stata selezionata la corretta pianificazione.
3. Sono elencati i seguenti quattro tipi di risorse:
   - **Cestino**: distrugge tutte i file all'interno del Cestino.
   - **File di sistema temporanei**: distrugge tutti i file trovati nella cartella temporanea del sistema. La ricerca delle variabili di ambiente viene eseguita nel seguente ordine e il primo percorso individuato viene considerato come la cartella di sistema:
     - TMP
     - TEMP
   - **File Internet temporanei**: distrugge copie di pagine Web, immagini, e file multimediali salvati dai browser Web per una visualizzazione più rapida.
   - **Cookies**: distrugge tutti i file memorizzati dai siti Web su un computer per salvare preferenze come i dati di login.

   Se selezionate, tali risorse verranno distrutte all'orario pianificato.
4. Per selezionare risorse personalizzate aggiuntive da distruggere:
   a. In **Scheduled Shred List** (Elenco di distruzione pianificata), fare clic su o toccare **Aggiungi cartella**, quindi spostarsi sul file o sulla cartella.
   b. Fare clic su o toccare **Apri**, quindi fare clic su o toccare **OK**.

   Per rimuovere una risorsa dall'Elenco di distruzione pianificata, deselezionare la casella di controllo della risorsa.

Impostazione della pianificazione per la pulitura dello spazio libero

La pulizia dello spazio libero non fornisce ulteriore protezione per le risorse distrutte.

1. Aprire File Sanitizer, quindi fare clic su o toccare **Impostazioni**.
2. Per programmare un tempo futuro per la pulitura dell'unità disco rigido, in **Bleach Schedule** (Pianificazione della pulitura), selezionare **Mai**, **Una volta**, **Ogni giorno**, **Ogni settimana** o **Ogni mese**, quindi selezionare un giorno e l'ora.
   a. Fare clic su o toccare l'ora, il minuto, o il campo AM/PM.
   b. Scorrere fino a quando il valore desiderato è stato visualizzato allo stesso livello degli altri campi.
   c. Fare clic su o toccare lo spazio bianco che circonda i campi di impostazione dell'orario.
   d. Ripetere l'operazione fino a quando è stata selezionata la corretta pianificazione.

NOTA: la pulitura dello spazio libero può richiedere una notevole quantità di tempo. Assicurarsi che il computer sia collegato all'alimentazione CA. Sebbene la pulitura dello spazio libero sia un'operazione eseguita in background, le prestazioni del computer possono risultare inferiori a causa di un maggior utilizzo del processore. La pulizia dello spazio libero può essere eseguita in orari non lavorativi o quando il computer non è in uso.

Protezione dei file dalla distruzione

Per proteggere i file o le cartelle dalla distruzione:

1. Aprire File Sanitizer, quindi fare clic su o toccare **Impostazioni**.
2. In **Never Shred List** (Elenco degli elementi da non distruggere mai), fare clic su o toccare **Aggiungi cartella**, quindi spostarsi sul file o sulla cartella.
3. Fare clic su o toccare **Apri**, quindi fare clic su o toccare **OK**.

NOTA: I file sono protetti finché rimangono nell'elenco.

Per rimuovere una risorsa dall'elenco di esclusione, deselezionare la casella di controllo della risorsa.

Attività generali

File Sanitizer consente di effettuare le seguenti attività:

- **Utilizzare l'icona File Sanitizer per avviare la distruzione**: trascinare i file sull'icona **File Sanitizer** disponibile sul desktop. Per istruzioni dettagliate, fare riferimento alla sezione "Uso dell'icona File Sanitizer a pagina 41".
- **Distruzione manuale di una risorsa specifica o di tutte le risorse selezionate**: distruggere manualmente gli elementi prima che venga eseguita la regolare operazione pianificata. Per informazioni dettagliate, fare riferimento alla sezione Distruzione facendo clic con il pulsante destro del mouse a pagina 41 o Avvio manuale di un'operazione di distruzione a pagina 41.
- **Attivazione manuale della pulitura dello spazio libero**: attivare in qualsiasi momento la pulitura dello spazio libero. Per istruzioni dettagliate, fare riferimento alla sezione "Avvio manuale della pulitura dello spazio libero a pagina 42".
- **Visualizzazione dei file registro**: visualizzare i file di registro relativi alle operazioni di distruzione e di pulitura dello spazio libero che riportano eventuali errori rilevati durante l'ultima

operazione di distruzione o di pulitura dello spazio libero. Per istruzioni dettagliate, fare riferimento alla sezione "Visualizzazione dei file di registro a pagina 42".

NOTA: L'operazione di distruzione o di pulizia dello spazio libero potrebbe richiedere molto tempo. Benché le operazioni di distruzione e di pulizia dello spazio libero vengano eseguite in background, l'aumento di utilizzo del processore potrebbe influire sulle prestazioni del computer

Uso dell'icona File Sanitizer

ATTENZIONE: I file distrutti non potranno essere recuperati. Considerare attentamente quali elementi si desidera selezionare per la distruzione manuale.

Quando si avvia manualmente un'operazione di distruzione, l'elenco di distruzione standard sulla schermata File Sanitizer viene distrutto (vedi Procedure di installazione a pagina 38).

È possibile avviare un'operazione di distruzione manuale in uno dei modi seguenti:

1. Aprire File Sanitizer (vedere Apertura di File Sanitizer a pagina 38), quindi fare clic su o toccare **Distruggi**.
2. Quando si apre la finestra di dialogo di conferma, assicurarsi che le risorse che si desidera distruggere siano selezionate, quindi fare clic su o toccare **OK**.

oppure

1. Fare clic con il pulsante destro del mouse su o toccare e tenere premuta l'icona **File Sanitizer** sul desktop di Windows, quindi fare clic su o toccare **Distruggi ora**.
2. Quando si apre la finestra di dialogo di conferma, assicurarsi che le risorse che si desidera distruggere siano selezionate, quindi fare clic su o toccare **Distruggi**.

Distruzione facendo clic con il pulsante destro del mouse

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

Se **Enable right-click shredding** (Abilita la distruzione facendo clic con il pulsante destro del mouse) è stata selezionata nella schermata File Sanitizer, è possibile distruggere una risorsa nel modo seguente:

1. Spostarsi sul documento o sulla cartella che si desidera distruggere.
2. Fare clic con il pulsante destro del mouse su o toccare e tenere premuto il file o la cartella, quindi selezionare **HP File Sanitizer – Distruggi**.

Avvio manuale di un'operazione di distruzione

ATTENZIONE: I file distrutti non potranno essere recuperati. Considerare attentamente quali elementi si desidera selezionare per la distruzione manuale.

Quando si avvia manualmente un'operazione di distruzione, l'elenco di distruzione standard sulla schermata File Sanitizer viene distrutto (vedi Procedure di installazione a pagina 38).

È possibile avviare un'operazione di distruzione manuale in uno dei modi seguenti:

1. Aprire File Sanitizer (vedere Apertura di File Sanitizer a pagina 38), quindi fare clic su o toccare **Distruggi**.
2. Quando si apre la finestra di dialogo di conferma, assicurarsi che le risorse che si desidera distruggere siano selezionate, quindi fare clic su o toccare **OK**.

oppure

1. Fare clic con il pulsante destro del mouse su o toccare e tenere premuta l'icona **File Sanitizer** sul desktop di Windows, quindi fare clic su o toccare **Distruggi ora**.
2. Quando si apre la finestra di dialogo di conferma, assicurarsi che le risorse che si desidera distruggere siano selezionate, quindi fare clic su o toccare **Distruggi**.

Avvio manuale della pulitura dello spazio libero

Quando si avvia manualmente un'operazione di pulitura, l'elenco di pulitura standard sulla schermata File Sanitizer viene pulito (vedi Procedure di installazione a pagina 38).

È possibile avviare un'operazione di pulitura manuale in uno dei modi seguenti:

1. Aprire File Sanitizer (see Apertura di File Sanitizer a pagina 38), quindi fare clic su o toccare **Pulisci**.
2. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su o toccare **OK**.

– oppure –

1. Fare clic con il pulsante destro del mouse su o toccare e tenere premuta l'icona **File Sanitizer** sul desktop di Windows, quindi fare clic su o toccare **Pulisci ora**.
2. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su o toccare **Pulisci**.

Visualizzazione dei file di registro

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

NOTA: I file correttamente distrutti o eliminati tramite pulitura non vengono visualizzati nel file di registro.

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

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

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

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

7 HP Device Access Manager (solo in determinati modelli)

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

NOTA: Alcune periferiche di input/HID (Human Interface Input), ad esempio mouse, tastiere, touchpad e lettori di impronte digitali, non sono controllate da Device Access Manager. Per ulteriori informazioni, vedere Classi di dispositivi non gestite a pagina 46.

Gli amministratori del sistema operativo Windows® utilizzano HP Device Access Manager per controllare l'accesso alle periferiche in un sistema e proteggerle dall'accesso non autorizzato:

- I profili periferica vengono creati per ciascun utente per definire i dispositivi per cui dispongono o meno del permesso di accesso.
- L'autenticazione Just-In-Time (JITA) consente agli utenti predefiniti di autenticarsi per poter accedere a periferiche altrimenti non accessibili.
- Gli amministratori e gli utenti attendibili possono essere esclusi dalle limitazioni di accesso al dispositivo imposte da Device Access Manager aggiungendoli al gruppo Amministratori di periferiche. L'appartenenza a questo gruppo viene gestita tramite le Impostazioni avanzate.
- L'accesso alle periferiche può essere concesso o negato in base all'appartenenza al gruppo o per utenti singoli.
- Per classi di periferiche quali unità CD-ROM e DVD, l'accesso in lettura e scrittura può essere concesso o negato separatamente.

HP Device Access Manager è configurato automaticamente con le seguenti impostazioni durante il completamento dell'impostazione guidata di HP Client Security:

- Il supporto rimovibile Just In Time Authentication (JITA) è abilitato per Amministratori e Utenti.
- Il criterio del dispositivo consente l'accesso completo ad altri dispositivi.

Apertura di Device Access Manager

1. Dalla schermata Start, fare clic o toccare l'app **HP Client Security** (Windows 8).

   – Oppure –

   Dal desktop di Windows, fare doppio clic su o toccare con due colpetti leggeri l'icona **HP Client Security** nell'area di notifica situata a destra della barra delle applicazioni.

2. In **Device** (Dispositivo), fare clic su o toccare **Device Permissions** (Autorizzazioni del dispositivo).

   - Gli utenti standard possono visualizzare il loro accesso al dispositivo corrente (vedere Schermata utente a pagina 44).
   - Gli amministratori possono visualizzare e modificare l'accesso al dispositivo che è attualmente configurato per il computer facendo clic o toccando **Modifica**, quindi immettendo la password di Amministratore (consultare Schermata sistema a pagina 44).

Schermata utente

Quando si seleziona **Device Permissions** (Autorizzazione del dispositivo), viene mostrata la visualizzazione Utente. A seconda del criterio, gli utenti e gli amministratori standard possono visualizzare il loro accesso alle classi di dispositivi o ai singoli dispositivi sul computer.

- **Current user** (Utente corrente): è visualizzato il nome dell'utente che è attualmente connesso.
- **Classe periferica**: sono visualizzati i tipi di dispositivi.
- **Accesso**: è visualizzato l'accesso attualmente configurato a tipi di dispositivi o dispositivi specifici.
- **Durata**: è visualizzato il limite di tempo dell'accesso alle unità CD/DVD-ROM o alle unità disco rimovibili.
- **Impostazioni**: gli Amministratori possono modificare le unità che hanno l'accesso controllato da Device Access Manager.

Schermata sistema

Nella schermata sistema, gli amministratori possono concedere o negare l'accesso ai dispositivi su questo computer al Gruppo utenti o al Gruppo amministratori.

▲ Gli Amministratori possono accedere alla schermata sistema facendo clic o toccando **Modifica**, immettendo la password dell'amministratore, quindi selezionando una delle seguenti opzioni:

- **Device Access Manager**: per attivare o disattivare HP Device Access Manager con Just In Time Authentication, cliccare o toccare **On** (Attivato) oppure **Off** (Disattivato).
- **Users and groups on this PC** (Utenti e gruppi su questo PC): consente di visualizzare il Gruppo utenti o il Gruppo amministratori al quale è concesso o negato l'accesso alle classi di dispositivi selezionate.
- **Classe periferica**: consente di visualizzare tutte le classi di dispositivi e tutti i dispositivi installati nel sistema o quelli che sono stati installati nel sistema in precedenza. Per espandere l'elenco, fare clic sull'icona **+**. Tutti i dispositivi connessi al computer vengono visualizzati, e il Gruppo amministratori e utenti viene espanso per mostrare la loro appartenenza. Per aggiornare l'elenco dei dispositivi, fare clic sull'icona della freccia rotonda (aggiorna).
  - La protezione viene in genere applicata a una classe di dispositivi. Se l'accesso è impostato su **Consenti**, l'utente o il gruppo selezionato saranno in grado di accedere a qualsiasi dispositivo in tale classe di dispositivo.
  - La protezione può essere anche applicata a dispositiv specifici.
  - Configurare Just In Time authentication (JITA) consente agli utenti selezionati l'accesso alle unità DVD/CD-ROM o alle unità disco rimovibili mediante l'autenticazione. Per ulteriori informazioni, vedere Configurazione JITA (Just-in-time authentication) a pagina 45.
  - Consentire o negare l'accesso ad altre classi di dispositivi, come ad esempio i supporti rimovibili (ad esempio unità flash USB), porte seriali e parallele, dispositivi Bluetooth®, dispositivi modem, dispositivi PCMCIA/ExpressCard, dispositivi 1394, lettore impronte digitali e lettore di smart card. Se l'accesso al lettore impronte digitali e al lettore di smart card è negato, essi possono essere utilizzati come credenziali di autenticazione, ma non possono essere utilizzati a livello di criterio della Sessione.

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

- Quando si seleziona un'impostazione a livello di Gruppo o di Classe di dispositivo, verrà chiesto se applicare l'impostazione agli oggetti figlio:

  Sì: l'impostazione si propagherà.

  No: l'impostazione non si propagherà.

- Alcune classi di dispositivi, ad esempio, DVD e CD-ROM, possono essere controllate ulteriormente consentendo o negando l'accesso separatamente per le operazioni di lettura e scrittura.

NOTA: Il gruppo Amministratori non può essere aggiunto all'elenco utenti.

- **Accesso**: fare clic su o toccare la freccia giù, quindi selezionare uno dei seguenti tipi di accesso per consentire o negare l'accesso:
  - **Consenti – Accesso completo**
  - **Consenti – Sola lettura**
  - **Allow – JITA Required** (Consenti – JITA necessaria): per ulteriori informazioni, vedere Configurazione JITA (Just-in-time authentication) a pagina 45.

    Se si seleziona questo tipo di accesso, in **Durata**, fare clic su o toccare la freccia giù per selezionare un limite di tempo.
  - **Nega**
- **Durata**: fare clic su o toccare la freccia giù per selezionare un limite di tempo per l'accesso alle unità CD/DVD-ROM o alle unità disco rimovibili (vedi Configurazione JITA (Just-in-time authentication) a pagina 45).

Configurazione JITA (Just-in-time authentication)

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

Gli utenti abilitati all'autenticazione JITA saranno in grado di accedere ad alcuni dispositivi i cui criteri creati nella schermata **Configurazione delle classi di periferiche** sono stati limitati.

È possibile autorizzare la durata della sessione JITA in base a un numero di minuti definito o senza limiti di tempo. Gli utenti con accesso illimitato avranno accesso al dispositivo dal momento in cui si autenticano fino a quando si disconnettono dal sistema.

Se all'utente viene assegnata una durata limitata della sessione JITA, un minuto prima della scadenza della sessione JITA verrà chiesto all'utente se estendere l'accesso. Non appena l'utente si disconnette dal sistema o un altro utente si connette, il periodo della sessione JITA scade. Al successivo accesso, quando l'utente tenta di accedere a una periferica abilitata all'autenticazione JITA, viene visualizzato un messaggio che richiede di immettere le credenziali.

JITA è disponibile per le seguenti classi di dispositivi:

- Unità DVD/CD-ROM
- Unità disco rimovibili

Creazione di un criterio JITA per un utente o gruppo

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

1. Avviare **Device Access Manager**, quindi fare clic su o toccare **Modifica**.
2. Selezionare l'utente o il gruppo, quindi in **Accesso** sia per **Unità disco rimovibili** sia per **Tutte le unità DVD/CD-ROM** cliccare o toccare la freccia giù, quindi selezionare **Allow – JITA Required** (Consenti - JITA necessaria).
3. In **Durata**, fare clic su o toccare la freccia giù per selezionare un periodo di tempo per l'accesso JITA.

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

Disabilitazione di un criterio JITA per un utente o gruppo

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

1. Avviare **Device Access Manager**, quindi fare clic su o toccare **Modifica**.
2. Selezionare l'utente o il gruppo, quindi in **Accesso** sia per **Unità disco rimovibili** sia per **Tutte le unità DVD/CD-ROM** cliccare o toccare la freccia giù, quindi selezionare **Nega**.

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

Impostazioni

La schermata **Impostazioni** consente agli amministratori di visualizzare e modificare le unità che hanno l'accesso controllato da Device Access Manager.

NOTA: Device Access Manager deve essere abilitato quando l'elenco delle lettere del dispositivo è configurato (vedere Schermata sistema a pagina 44).

Classi di dispositivi non gestite

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

- Dispositivi di input/output
  - CD-ROM
  - Unità disco
  - Controller floppy disk (FDC, Floppy Disk Controller)
  - Controller unità disco rigido (HDC, Hard Disk Controller)
  - Classe Human Interface Device (HID)
  - Human Interface Device (HID) a infrarossi
  - Mouse
  - Dispositivi seriali multi-porta
  - Tastiera
  - Stampanti Plug and play (PnP)

- Stampante
- Aggiornamento stampante

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

8 HP Trust Circles

HP Trust Circles è un'applicazione di protezione per file e documenti che combina la crittografia dei file delle cartelle con la comoda funzionalità dei trust circle e di condivisione dei documenti. L'applicazione crittografa i file collocati in cartelle specificate dall'utente, proteggendoli all'interno di un trust circle. Una volta protetti, i file possono essere utilizzati e condivisi solo dai membri del trust circle. Se un file protetto viene ricevuto da un non membro, il file rimane crittografato, e il non membro non può accedere al contenuto.

Apertura di Trust Circles

1. Sul menu Avvio, fare clic su o toccare l'app **HP Client Security**.

   oppure

   Dal desktop di Windows, fare doppio clic sull'icona **HP Client Security** nell'area di notifica, all'estrema destra della barra delle applicazioni.

2. In **Data** (Dati), fare clic su o toccare **Trust Circles**.

Guida introduttiva

Ci sono due modi per inviare inviti e-mail e rispondere ad essi:

- **Utilizzando Microsoft® Outlook**: l'utilizzo di Trust Circles con Microsoft Outlook consente di automatizzare l'elaborazione di qualsiasi invito Trust Circles e delle risposte di altri utenti di Trust Circles.
- **Utilizzando Gmail, Yahoo, Outlook.com o altri servizi di posta elettronica (SMTP)**: quando si inserisce il nome, l'indirizzo e-mail e la password, Trust Circles utilizza il servizio e-mail dell'utente per inviare inviti e-mail ai membri selezionati per entrare nel trust circle dell'utente.

Per impostare il profilo di base:

1. Inserire il nome e l'indirizzo e-mail, quindi fare clic su o toccare **Next** (Avanti).

   Il nome è visibile a tutti i membri che sono invitati a entrare nel trust circle dell'utente. L'indirizzo e-mail viene utilizzato per inviare, ricevere o rispondere agli inviti.

2. Immettere la password per l'account e-mail, quindi toccare o fare clic su **Avanti**.

   Una e-mail di prova viene inviata per assicurare che le impostazioni di posta elettronica siano accurate.

   NOTA: il computer deve essere collegato in rete.

3. Nel campo **Trust Circle Name** (Nome trust circle), immettere un nome per il trust circle, quindi toccare o fare clic su **Avanti**.

4. Aggiungere i membri e le cartelle, quindi toccare o fare clic su **Avanti**. Il trust circle viene creato con tutte le cartelle che sono state selezionate e invia inviti e-mail a tutti i membri che sono stati selezionati. Se, per qualsiasi motivo, un invito non può essere inviato, viene visualizzata una notifica. I membri possono essere invitati nuovamente in qualsiasi momento dalla schermata Trust Circle facendo clic su **Your Trust Circles** (Trust Circles), quindi facendo doppio clic su o

toccando con due colpetti leggeri il trust circle. Per ulteriori informazioni, vedere Trust Circles a pagina 49.

Trust Circles

È possibile creare un trust circle durante la configurazione iniziale dopo aver inserito l'indirizzo e-mail, o nella schermata Trust Circle:

▲ Dalla schermata Trust Circle, fare clic su o toccare **Create Trust Circle** (Crea trust circle), quindi immettere un nome per il trust circle.

- Per aggiungere membri al trust circle, fare clic su o toccare l'icona **M+** icona accanto a **Members** (Membri), quindi seguire le istruzioni visualizzate.
- Per aggiungere cartelle al trust circle, fare clic su o toccare l'icona **+** icona accanto a **Folders** (Cartelle), quindi seguire le istruzioni visualizzate.

Aggiungere cartelle a un trust circle

Aggiungere cartelle a un nuovo trust circle:

- Durante la creazione di un trust circle, è possibile aggiungere cartelle facendo clic o toccando l'icona **+** accanto a **Folders** (Cartelle), quindi seguire le istruzioni visualizzate.

  oppure

- In Esplora risorse, fare clic con il pulsante destro del mouse su o toccare e tenere premuta una cartella che non fa attualmente parte di un trust circle, selezionare **Trust Circle**, quindi selezionare **Create Trust Circle from Folder** (Crea trust circle da cartella).

SUGGERIMENTO: È possibile selezionare una o più cartelle.

Aggiungere cartelle a un trust circle esistente:

- Dalla schermata Trust Circle, fare clic su **Your Trust Circles** (Trust Circles), fare doppio clic su o toccare con due colpetti leggeri il trust circle esistente per visualizzare le cartelle correnti, fare clic su o toccare l'icona **+** accanto a **Folders** (Cartelle), quindi seguire le istruzioni visualizzate.

  – oppure –

- In Esplora risorse, fare clic con il pulsante destro del mouse su o toccare e tenere premuta una cartella che non fa attualmente parte di un trust circle, selezionare **Trust Circle**, quindi selezionare **Add to existing Trust Circle from Folder** (Aggiungi a trust circle esistente da cartella).

SUGGERIMENTO: È possibile selezionare una o più cartelle.

Una volta che una cartella è stata aggiunta a un trust circle, Trust Circles crittografa automaticamente la cartella e il suo contenuto. Una volta che tutti i file sono crittografati, viene visualizzata una notifica. Inoltre, un simbolo di blocco verde viene visualizzato su tutte le icone delle cartelle crittografate e le icone dei file all'interno delle cartelle per indicare che essi sono completamente protetti.

Aggiungere membri a un trust circle

Sono necessari tre passaggi per aggiungere membri a un trust circle:

1. **Invitare**: in primo luogo, il proprietario del trust circle invita i membri. La e-mail di invito può essere inviata a più utenti o elenchi/gruppi di distribuzione.
2. **Accettare**: l'invitato riceve l'invito e sceglie se accettare o rifiutare. Se l'invitato accetta l'invito, una risposta e-mail viene inviata all'autore dell'invito. Se l'invito è stato inviato a un gruppo, ogni membro riceve un invito e sceglie se accettare o rifiutare.
3. **Registrare**: l'autore dell'invito ha una ultima opportunità di decidere se aggiungere il membro al trust circle. Se l'autore dell'invito decide di registrare il membro, una e-mail viene inviata all'invitato confermando la risposta. L'autore dell'invito e l'invitato possono eventualmente verificare la protezione della procedura di invito. L'invitato visualizza un codice di verifica che deve essere letto al telefono all'autore dell'invito. Una volta che il codice è stato verificato, l'autore dell'invito può inviare l'e-mail di registrazione finale.

Aggiungere membri a un nuovo trust circle:

▲ Durante la creazione di un trust circle, è possibile aggiungere membri facendo clic o toccando l'icona **M+** accanto a **Members** (Membri), quindi seguire le istruzioni visualizzate.

- Se si utilizza Outlook, selezionare i contatti dalla rubrica di Outlook, quindi fare clic su **OK** (OK)
- Se si utilizza un altro servizio e-mail, è possibile aggiungere i nuovi indirizzi e-mail a Trust Circle manualmente, oppure è possibile farli recuperare dall'indirizzo e-mail registrato su Trust Circle.

Aggiungere membri a un trust circle esistente:

▲ Dalla schermata Trust Circle, fare clic su **Your Trust Circles** (Trust Circles), fare doppio clic su o toccare con due colpetti leggeri il trust circle esistente per visualizzare i membri correnti, fare clic su o toccare l'icona **M+** accanto a **Members** (Membri), quindi seguire le istruzioni visualizzate.

- Se si utilizza Outlook, selezionare i contatti dalla rubrica di Outlook, quindi fare clic su **OK** (OK).
- Se si utilizza un altro servizio e-mail, è possibile aggiungere i nuovi indirizzi e-mail a Trust Circle manualmente, oppure è possibile farli recuperare dall'indirizzo e-mail registrato su Trust Circle.

Aggiungere file a un trust circle

È possibile aggiungere file a un trust circle in uno dei seguenti modi:

- Copiare o spostare il file in una cartella esistente del trust circle.

  – oppure –

- In Esplora risorse, fare clic con il pulsante destro del mouse o toccare e tenere premuto un file che non è attualmente crittografato, selezionare **Trust Circle**, quindi selezionare **Encrypt** (Crittografa). Verrà richiesto di selezionare il trust circle a cui deve essere aggiunto il file.

SUGGERIMENTO: È possibile selezionare uno o più file.

Cartelle crittografate

Ogni membro di un trust circle è in grado di visualizzare e modificare i file che appartengono a tale trust circle.

NOTA: Trust Circle Manager/Reader non sincronizza i file tra i membri.

I file devono essere condivisi con i mezzi esistenti, come ad esempio e-mail, FTP o provider di archiviazione cloud. I file copiati, spostati o creati all'interno di una cartella del trust circle sono protetti immediatamente.

Rimuovere cartelle da un trust circle

Rimuovere una cartella da un trust circle decrittografa la cartella e tutto il suo contenuto e rimuove la sua protezione.

- Dalla schermata Trust Circle, fare clic su o toccare **Your Trust Circles** (Trust Circles), fare doppio clic su o toccare con due colpetti leggeri il trust circle esistente per visualizzare le cartelle correnti, quindi fare clic su o toccare l'icona **trash can** (cestino) accanto a tale cartella.

  oppure

- In Esplora risorse, fare clic con il pulsante destro del mouse su o toccare e tenere premuta una cartella che fa attualmente parte di un trust circle, selezionare **Trust Circle**, quindi selezionare **Remove from trust circle** (Rimuovi dal trust circle).

SUGGERIMENTO: È possibile selezionare una o più cartelle.

Rimuovere un file da un trust circle

Per rimuovere un file da un trust circle, in Esplora risorse, fare clic con il pulsante destro del mouse o toccare e tenere premuto un file che non è attualmente crittografato, selezionare **Trust Circle**, selezionare **Decrypt File** (Decrittografa file).

Rimuovere membri da un trust circle

Un membro che è stato pienamente registrato non può essere rimosso da un trust circle. In alternativa, si potrebbe creare un nuovo trust circle con tutti gli altri membri, spostare tutti i file e le cartelle nel nuovo trust circle, quindi eliminare il trust circle precedente. Questo consentirà che tutti i nuovi file che il membro riceve non siano accessibili, ma tutto ciò che è stato condiviso in precedenza rimanga accessibile al membro del trust circle precedente.

Se un membro non è completamente registrato (sia che il membro sia stato invitato ad unirsi al trust circle sia che non abbia accettato l'invito al trust circle), è possibile rimuovere il membro dal trust circle in uno dei seguenti modi:

- Dalla schermata di Trust Circle, toccare o fare clic su **Your Trust Circles** (Trust Circles), quindi toccare con due colpetti leggeri o fare doppio clic sul trust circle per mostrare l'elenco corrente dei membri. Fare clic su o toccare l'icona **trash can** (cestino) accanto al nome del membro che si desidera rimuovere.
- Dalla schermata di Trust Circle, fare clic su o toccare **Members** (Membri), quindi fare doppio clic su o toccare con due colpetti leggeri il membro per mostrare i trust circle di cui è membro. Fare clic su o toccare l'icona **trash can** (cestino) accanto a un trust circle per rimuovere il membro da tale trust circle.

Eliminare un trust circle

Per eliminare un trust circle, è necessario averne la proprietà.

▲ Dalla schermata di Trust Circle, toccare o fare clic su **Your Trust Circles** (Trust Circles), toccare o fare clic sull'icona **trash can** (cestino) accanto al trust circle che si desidera cancellare.

Questo rimuove il trust circle dalla pagina e invia e-mail a tutti i membri del trust circle per informarli che il trust circle è stato eliminato. Tutti i file o le cartelle che erano stati inclusi in quel trust circle vengono decrittografati.

Impostazione delle preferenze

Dalla schermata di Trust Circle, fare clic su o toccare **Preferences** (Preferenze). Vengono visualizzate tre schede

- **Impostazioni e-mail**

Opzione	Descrizione
Nome utente	Viene visualizzato il nome utente attualmente in uso. Per modificarlo, immettere un nuovo nome utente nella casella di testo. Le modifiche vengono salvate automaticamente.
Indirizzo E-mail	Viene visualizzato l'account e-mail attualmente in uso. Per modificarlo, fare clic su o toccare **Change Email Settings** (Modifica Impostazioni E-mail), quindi seguire le istruzioni visualizzate.
Conferma nuovo membro	Selezionare una delle seguenti opzioni: ◦ **Conferma automaticamente**: dopo aver ricevuto l'accettazione da parte degli invitati, essi sono confermati nel trust circle senza alcun input manuale, e una e-mail di conferma viene inviata agli invitati. ◦ **Conferma manualmente**: dopo aver ricevuto l'accettazione da parte degli invitati, l'input manuale è necessario per registrare i nuovi membri nel trust circle, successivamente una e-mail di conferma viene inviata agli invitati. ◦ **Richiedi verifica**: dopo aver ricevuto l'accettazione da parte degli invitati, è necessario un codice di verifica per registrare completamente gli invitati. Il proprietario del trust circle deve contattare gli invitati e acquisire da loro il codice di verifica. Dopo aver immesso il codice corretto, le e-mail di conferma vengono inviate.
Autenticazione periodica	L'autenticazione periodica richiede all'utente di immettere la password di Windows dopo il timeout specificato (registrato in minuti) e anche durante l'esecuzione di operazioni sensibili. Questa impostazione consente agli utenti di attivare o disattivare l'autenticazione.
Timeout autenticazione	Selezionare il periodo di timeout specificato (registrato in minuti) prima che venga richiesta l'autenticazione.
Non visualizzare messaggio di conferma	Selezionare la casella di controllo per disabilitare la visualizzazione di messaggi di conferma, o deselezionare la casella di controllo per visualizzare i messaggi di conferma.
Vorrei contribuire a migliorare HP Trust Circle attraverso il monitoraggio dell'utilizzo in modo anonimo.	Selezionare la casella di controllo per partecipare al programma o deselezionare la casella di controllo se non si desidera partecipare.

- **Backup/Ripristino**

Opzione	Descrizione
Backup	Consente di copiare i dati delle applicazioni Trust Circle Manager/Reader (impostazioni e trust circle) in un file di backup. In caso di arresto anomalo o errore del sistema, è possibile utilizzare questo file per ripristinare la nuova installazione di Trust Circles allo stato salvato nel file. **NOTA:** Solo i dati delle applicazioni di Trust Circle vengono salvati (trust circle, impostazioni e membri). Non viene eseguito il backup dei file effettivi nelle cartelle dei trust circle. È consigliabile eseguire il backup di tali file separatamente. Per eseguire il backup delle impostazioni e dei dati utente di Trust Circle: **1.** Fare clic su o toccare **Backup** (Backup). **2.** Scegliere un nome di file e una directory per il file di backup, quindi fare clic su o toccare **Save** (Salva). **3.** Immettere una password, confermarla, quindi fare clic su o toccare **OK** (OK). Questa password sarà necessaria per ripristinare questo file.
Ripristino	Ripristina le impostazioni e i trust circle da un file di backup, in genere dopo un arresto anomalo del sistema o la migrazione a un altro computer. Per ripristinare le impostazioni e i dati utente di Trust Circle Manager: **1.** Fare clic su o toccare **Restore** (Ripristina). **2.** Spostarsi sulla directory e sul nome di file del file di backup, quindi fare clic su o toccare **Open** (Apri). **3.** Immettere la password che è stata impostata durante l'esecuzione del backup.

- **About** (Ulteriori informazioni): viene visualizzata la versione del software Trust Circle Manager/Reader. I collegamenti sono visualizzati per consentire di aggiornare Trust Circle Manager/Reader alla versione Pro o di visualizzare l'informativa sulla privacy di HP.

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

Computrace (da acquistare separatamente) consente all'utente di monitorare, gestire e tener traccia in remoto del proprio computer.

Una volta attivato, Computrace viene configurato dal Centro Clienti del software Absolute. Dal Centro Clienti, l'amministratore può configurare Computrace per il monitoraggio o la gestione del computer. Se il sistema viene smarrito o rubato, il Centro Clienti può aiutare le autorità locali a individuare e recuperare il computer. Se configurato, Computrace continua a funzionare anche se viene cancellata o sostituita l'unità disco rigido.

Per attivare Computrace, procedere come segue:

1. Connettersi a Internet.
2. Aprire HP Client Security. Per ulteriori informazioni, vedere Aprire HP Client Security a pagina 9.
3. Fare clic su **Ritrovamento di PC rubati**.
4. Per avviare l'attivazione guidata di Computrace, fare clic sul pulsante **Inizio**.
5. Inserire le proprie informazioni di contatto e i dati della carta di credito, oppure immettere un codice prodotto preacquistato.

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

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

Per accedere al centro assistenza clienti:

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

Nel Centro assistenza clienti è possibile:

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

▲ Fare clic su **Ulteriori informazioni** per ulteriori informazioni su Computrace.

10 Eccezioni relative alle password localizzate

Al livello dell'Autenticazione all'accensione e di HP Drive Encryption, il supporto alla localizzazione della password è limitato. Per ulteriori informazioni, vedere IME di Windows non supportati a livello di autenticazione all'accensione o di HP Drive Encryption a pagina 55.

Operazioni da eseguire quando una password viene rifiutata

Le password possono essere rifiutate per i seguenti motivi:

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

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

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

  1. Modificare la password di Windows utilizzando solo caratteri supportati. Per ulteriori informazioni sui caratteri non supportati, vedere Gestione tasti speciali a pagina 56.
  2. Avviare HP Client Security, quindi immettere la password di Windows.

IME di Windows non supportati a livello di autenticazione all'accensione o di HP Drive Encryption

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

Gli editor IME (Input Method Editor, Editor del metodo di input) non sono supportati a livello di autenticazione all'accensione o di Drive Encryption. Non è possibile immettere una password di Windows con un editor IME nella schermata di accesso all'autenticazione all'accensione o a HP Drive Encryption, in quanto ciò potrebbe causare una situazione di blocco. In alcuni casi, Microsoft® Windows non visualizza l'editor IME quando l'utente immette la password.

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

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

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

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

Modifiche della password con layout di tastiera supportato

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

NOTA: Gli amministratori possono risolvere questo problema utilizzando la pagina Utenti di HP Client Security (accessibile dall'icona **Gear** (Dispositivo) nella pagina iniziale) per rimuovere l'utente da HP Client Security, selezionando il layout della tastiera desiderato nel sistema operativo, quindi eseguendo nuovamente l'impostazione guidata di HP Client Security per lo stesso utente. Nel BIOS è memorizzato il layout di tastiera desiderato e le password che possono essere digitate con questo layout verranno correttamente impostate nel BIOS.

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

Gestione tasti speciali

- Cinese, slovacco, francese canadese e ceco

  Quando un utente seleziona uno dei precedenti layout della tastiera ed immette una password (ad esempio, abcdef), è necessario immettere la stessa password premendo il tasto maiusc per il carattere minuscolo e il tasto maiusc e bloc maiusc per il carattere maiuscolo a livello di autenticazione all'accensione e HP Drive Encryption. Le password numeriche devono essere immesse utilizzando il tastierino numerico.

- Coreano

  Quando un utente seleziona un layout di tastiera coreano supportato ed immette una password, è necessario immettere la stessa password premendo il tasto destro alt per il carattere minuscolo e il tasto destro alt e bloc maiusc per il carattere maiuscolo a livello di autenticazione all'accensione e HP Drive Encryption.

- Nella tabella seguente vengono elencati i caratteri non supportati:

Language (Lingua)	Windows	BIOS	Drive Encryption
Arabo	I tasti ﻻ ,ﻷ, e ﻹ generano due caratteri.	I tasti ﻻ ,ﻷ, e ﻹ generano un carattere.	I tasti ﻻ ,ﻷ, e ﻹ generano un carattere.

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

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

Glossario

accesso al sistema
Un oggetto di HP Client sicurezza che comprende un nome utente e una password (e possibilmente altre informazioni selezionata) utilizzabili per eseguire l'accesso ai siti web o ad altri programmi.

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

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

amministratore
Vedere *Amministratore Windows*.

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

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

attivazione
Operazione che deve essere completata prima che qualsiasi funzionalità di Drive Encryption sia accessibile. Gli amministratori possono attivare Drive Encryption con l'impostazione guidata di HP Client Security o con HP Client Security. La procedura di attivazione consiste nell'attivazione del software, la crittografia dell'unità e la creazione della chiave di crittografia di backup iniziale su un dispositivo di archiviazione rimovibile.

autenticazione
La procedura di verifica dell'identità di un individuo avviene attraverso l'utilizzo di credenziali, tra cui la password di Windows, l'impronta digitale, una smart card, una scheda senza contatti o di prossimità.

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

Autenticazione di preavvio Drive Encryption
schermata di accesso che viene visualizzata prima dell'avvio di Windows. Gli utenti devono immettere il loro nome utente e la loro password di Windows oppure il PIN della smart card, o ancora passare un dito registrato. Se è selezionato l'accesso One Step logon, l'immissione delle informazioni corrette nella finestra di accesso di Drive Encryption consente l'accesso diretto a Windows, senza dover ripetere la procedura nella schermata di accesso di quest'ultimo.

Autenticazione Just-In-Time
Vedere la Guida del software di HP Device Access Manager.

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

Bluetooth
tecnologia che utilizza la trasmissione radio per abilitare entro un raggio limitato le comunicazioni wireless con computer, stampanti, mouse, telefoni cellulari e altri dispositivi sui quali è abilitata tale funzionalità.

Cartella Trust Circle

Qualsiasi cartella protetta da un trust circle.

chip di protezione integrato TPM (Trusted Platform Module)
La funzione TPM consente di autenticare un computer, anziché un utente, memorizzando informazioni specifiche relative al sistema host, quali chiavi di crittografia, certificati digitali e password. Il TPM riduce il rischio di compromissione delle informazioni presenti sul computer in caso di furto fisico o di attacco da parte di hacker esterno.

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

credenziali
dati specifici o dispositivo hardware utilizzato per autenticare un singolo utente.

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

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

Crittografia basata sul software
uso del software per crittografare l'unità disco rigido settore per settore Questo processo è più lento rispetto alla crittografia basata sull'hardware

Crittografia basata sull'hardware
uso delle unità che supportano la crittografia automatica e che soddisfano le specifiche OPAL del Trusted Computing Group in materia di gestione delle stesse per il completamento della crittografia immediata. La crittografia basata sull'hardware è immediata e potrebbe richiedere soltanto alcuni minuti, mentre quella basata sul software potrebbe richiedere diverse ore.

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

dispositivo collegato
un dispositivo hardware collegato a una porta del computer.

distruzione
esecuzione di un algoritmo che sovrascrive i dati di una risorsa con dati senza significato.

distruzione automatica
operazione pianificata in File Sanitizer.

distruzione manuale
Distruzione immediata di una risorsa o di risorse selezionate, che elude una distruzione pianificata.

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

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

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

Encryption File System (EFS)

Sistema che esegue la crittografia di tutti i file e di tutte le sottocartelle all'interno della cartella selezionata.

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

Home page
Posizione centrale da cui è possibile accedere e gestire le funzioni e impostazioni di HP Client Security.

identità
In HP Client Security, un gruppo di credenziali e impostazioni gestite come un account o un profilo di un particolare utente.

impronta digitale
estrazione digitale dell'immagine dell'impronta digitale. L'immagine dell'impronta digitale effettiva non viene mai memorizzata da HP Client Security.

Manager/Lettore Trust Circle
Il Trust Circle Reader può solo accettare inviti inviati da utenti di Trust Circle Manager. Tuttavia, Trust Circle Manager consente la creazione di trust circle. Le funzioni includono invitare qualcuno via e-mail a un trust circle e accettare inviti ai trust circle da parte di altri. Una volta che un trust circle è stabilito tra pari, i file protetti da tale trust circle possono essere condivisi in modo sicuro.

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

PIN
numero di identificazione personale per un utente registrato da utilizzare per l'autenticazione.

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

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

pulizia dello spazio libero
Sovrascrittura delle risorse eliminate con dati casuali e spazio non utilizzato. Questa procedura rende ancora più difficile il ripristino della risorsa originale.

riavvio
Processo di riavvio del computer.

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

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

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

Scheda di prossimità
una scheda di plastica contenente un chip di computer che può essere utilizzata per l'autenticazione insieme ad altre credenziali per ulteriore protezione.

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

Scheda senza contatti
una scheda di plastica contenente un chip di computer che può essere utilizzata per l'autenticazione.

schermata di accesso di Drive Encryption
vedere autenticazione di preavvio di Drive Encryption.

Single Sign-on
Una funzione che memorizza le informazioni di autenticazione e consente di utilizzare HP Client Security per accedere a Internet e alle applicazioni Windows che richiedono l'autenticazione tramite password.

smart card
dispositivo hardware che può essere utilizzato con un PIN per l'autenticazione.

Trust Circle
Fornisce contenimento dati associando i dati a un gruppo definito di utenti attendibili. Questo impedisce che i dati finiscano nelle mani sbagliate, accidentalmente o intenzionalmente. Protetti con la tecnologia di gestione delle chiavi di CryptoMill’s Zero Overhead, i dati vengono associati in modo crittografato a un trust circle. Questo impedisce la decrittografazione di documenti o altre informazioni riservate all'esterno del trust circle

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

Indice analitico