

# HP ProtectTools

## Guida per l'utente

© Copyright 2009 Hewlett-Packard  
Development Company, L.P.

Bluetooth è un marchio del rispettivo proprietario usato da Hewlett-Packard Company su licenza. Java è un marchio statunitense di Sun Microsystems, Inc. Microsoft e Windows sono marchi registrati negli USA di Microsoft Corporation. Il logo SD è un marchio del rispettivo proprietario.

Le informazioni contenute in questo documento sono soggette a modifiche senza preavviso. Le sole garanzie per i prodotti e i servizi HP sono definite nelle norme esplicite di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento va interpretato come costituente una garanzia aggiuntiva. HP non risponde di eventuali errori tecnici ed editoriali o di omissioni presenti in questo documento.

Prima edizione: Ottobre 2009

Numero di parte documento: 572661-061

---

# Sommario

## 1 Introduzione alle modalità di protezione

Funzioni di HP ProtectTools .....	2
Raggiungimento degli obiettivi chiave relativi alla protezione .....	3
Protezione da furti mirati .....	3
Limitazione dell'accesso ai dati sensibili .....	3
Blocco degli accessi non autorizzati dall'interno o dall'esterno della sede .....	3
Creazione di criteri password complessi .....	4
Ulteriori elementi protettivi .....	5
Assegnazione dei ruoli per la protezione .....	5
Gestione delle password di HP ProtectTools .....	5
Creazione di una password di protezione .....	7
Backup e ripristino delle credenziali di HP ProtectTools .....	7

## 2 Guida introduttiva

Apertura della console amministrativa di HP ProtectTools .....	9
Attivazione delle funzioni di protezione .....	10
Registrazione delle impronte digitali .....	11
Configurazione di una smart card .....	12
Uso della console amministrativa .....	13

## 3 Configurazione del sistema

Impostazione dell'autenticazione del computer .....	15
Criterio di accesso .....	15
Criterio di sessione .....	15
Impostazioni .....	16
Gestione degli utenti .....	17
Specificazione delle impostazioni dei dispositivi .....	18
Impronte digitali .....	18
Smart card .....	18

## 4 Configurazione delle applicazioni

Scheda Generale .....	20
Scheda Applications (Applicazioni) .....	21

## 5 Aggiunta di strumenti di gestione

### 6 HP ProtectTools Security Manager

Procedure di installazione .....	24
Guida introduttiva .....	24
Registrazione delle credenziali .....	24
Registrazione delle impronte digitali .....	24
Modifica della password di Windows .....	25
Configurazione di una smart card .....	25
Utilizzo del dashboard di Security Manager .....	25
Apertura di HP ProtectTools Security Manager .....	26
Attività generali .....	27
Gestore password .....	27
Per le pagine Web o i programmi per i quali non è stato ancora creato un accesso .....	27
Per le pagine Web o i programmi per i quali è stato già creato un accesso .....	28
Aggiunta di accessi .....	28
Modifica degli accessi .....	29
Utilizzo del menu degli accessi .....	29
Organizzazione degli accessi in categorie .....	29
Gestione degli accessi .....	30
Valutazione della complessità della password .....	30
Impostazioni dell'icona di Gestore password .....	30
Impostazioni .....	31
Credenziali .....	31
Scheda ID personale .....	32
Impostazione delle preferenze .....	32
Backup e ripristino dei dati .....	33
Aggiunta di applicazioni .....	34
Stato delle applicazioni di protezione .....	34

### 7 Drive Encryption per HP ProtectTools (solo in determinati modelli)

Procedure di configurazione .....	36
Apertura di Drive Encryption .....	36
Attività generali .....	37
Attivazione di Drive Encryption .....	37
Disattivazione di Drive Encryption .....	37
Accesso dopo l'attivazione di Drive Encryption .....	37
Protezione dei dati tramite crittografia del disco rigido .....	38
Visualizzazione dello stato di crittografia .....	38
Attività avanzate .....	39
Gestione di Drive Encryption (attività dell'amministratore) .....	39
Crittografia o decrittografia di singole unità disco .....	39

Backup e ripristino (attività dell'amministratore) .....	39
Creazione delle chiavi di backup .....	39
Esecuzione di un ripristino .....	40

## 8 Privacy Manager per HP ProtectTools (solo in determinati modelli)

Procedure di configurazione .....	42
Apertura di Privacy Manager .....	42
Gestione dei certificati di Privacy Manager .....	42
Richiesta e installazione di un certificato di Privacy Manager .....	42
Richiesta di un certificato di Privacy Manager .....	43
Come ottenere un certificato aziendale preassegnato di Privacy Manager .....	43
Installazione di un certificato di Privacy Manager .....	43
Visualizzazione dei dettagli del certificato di Privacy Manager .....	44
Rinnovo di un certificato di Privacy Manager .....	44
Impostazione di un certificato predefinito di Privacy Manager .....	44
Eliminazione di un certificato di Privacy Manager .....	44
Ripristino di un certificato di Privacy Manager .....	45
Revoca di un certificato di Privacy Manager .....	45
Gestione di contatti attendibili .....	46
Aggiunta di contatti attendibili .....	46
Aggiunta di un contatto attendibile .....	46
Aggiunta di contatti attendibili mediante i contatti di Microsoft Outlook .....	47
Visualizzazione dei dettagli dei contatti attendibili .....	48
Eliminazione di un contatto attendibile .....	48
Verifica dello stato della revoca per un contatto attendibile .....	48
Attività generali .....	49
Uso di Privacy Manager in Microsoft Outlook .....	49
Configurazione di Privacy Manager per Microsoft Outlook .....	49
Firma e invio di un messaggio e-mail .....	50
Crittografia e invio di un messaggio e-mail .....	50
Visualizzazione di un messaggio e-mail crittografato .....	50
Uso di Privacy Manager in un documento di Microsoft Office 2007 .....	50
Configurazione di Privacy Manager per Microsoft Office .....	51
Firma di un documento di Microsoft Office .....	51
Aggiunta di una riga per la firma di un documento Microsoft Word o Microsoft Excel .....	51
Aggiunta di firmatari suggeriti a un documento Microsoft Word o Microsoft Excel .....	52
Aggiunta di una riga per la firma dei firmatari suggeriti .....	52
Crittografia di un documento di Microsoft Office .....	53
Rimozione della crittografia da un documento di Microsoft Office .....	53
Invio di un documento crittografato di Microsoft Office .....	53
Visualizzazione di un documento firmato di Microsoft Office .....	54

Visualizzazione di un documento crittografato di Microsoft Office .....	54
Utilizzo di Privacy Manager in Windows Live Messenger .....	54
Avvio di una sessione di Privacy Manager Chat .....	55
Configurazione di Privacy Manager per Windows Live Messenger .....	56
Chat nella finestra di Privacy Manager Chat .....	56
Visualizzazione della cronologia chat .....	57
Rivelazione di tutte le sessioni .....	57
Rivelazione delle sessioni di un account specifico .....	57
Visualizzazione di un ID sessione .....	58
Visualizzazione di una sessione .....	58
Ricerca di testo specifico nelle sessioni .....	58
Eliminazione di una sessione .....	58
Aggiunta o rimozione di colonne .....	59
Filtro delle sessioni visualizzate .....	59
Attività avanzate .....	60
Migrazione dei certificati di Privacy Manager e dei contatti attendibili su un altro computer .....	60
Backup dei certificati di Privacy Manager e dei contatti attendibili .....	60
Ripristino dei certificati di Privacy Manager e dei contatti attendibili .....	60
Amministrazione centralizzata di Privacy Manager .....	61

## 9 File Sanitizer per HP ProtectTools

Distruzione .....	63
Pulizia dello spazio libero .....	64
Procedure di configurazione .....	65
Avvio di File Sanitizer .....	65
Impostazione di un programma di distruzione .....	65
Impostazione di un programma di pulizia dello spazio libero .....	66
Selezione o creazione di un profilo di distruzione .....	66
Selezione di un profilo di distruzione predefinito .....	66
Personalizzazione di un profilo di distruzione .....	67
Personalizzazione di un profilo di eliminazione semplice .....	67
Attività generali .....	69
Uso di una sequenza di tasti per avviare la distruzione .....	69
Uso dell'icona File Sanitizer .....	70
Distruzione manuale di una risorsa .....	70
Distruzione manuale di tutti gli elementi selezionati .....	71
Attivazione manuale della pulizia dello spazio libero .....	71
Interruzione di un'operazione di distruzione o di pulizia dello spazio libero .....	71
Visualizzazione dei file di registro .....	71

## 10 Device Access Manager per HP ProtectTools (solo in determinati modelli)

Procedure di installazione .....	74
----------------------------------	----

Apertura di Device Access Manager .....	74
Configurazione dell'accesso alle periferiche .....	74
Gruppo amministratori periferica .....	74
Configurazione semplice .....	74
Avvio del servizio in background .....	75
Configurazione delle classi di periferiche .....	76
Negazione dell'accesso a un utente o gruppo .....	77
Concessione dell'accesso per un utente o gruppo .....	78
Rimozione dell'accesso per un utente o gruppo .....	78
Concessione dell'accesso a una classe di periferiche per un utente di un gruppo .....	79
Concessione dell'accesso a una periferica specifica per un utente di un gruppo .....	79
Ripristino della configurazione .....	80
Attività avanzate .....	81
Controllo dell'accesso alle impostazioni di configurazione .....	81
Concessione dell'accesso a un utente o gruppo esistente .....	81
Negazione dell'accesso a un utente o gruppo esistente .....	82
Aggiunta di un nuovo gruppo o utente .....	82
Rimozione dell'accesso a un gruppo o utente .....	82
Documentazione correlata .....	82

## 11 LoJack Pro for HP ProtectTools

## 12 Risoluzione dei problemi

HP ProtectTools Security Manager .....	85
Device Access Manager per HP ProtectTools .....	87
Varie .....	89

<b>Glossario .....</b>	<b>90</b>
------------------------	-----------

<b>Indice analitico .....</b>	<b>95</b>
-------------------------------	-----------





---

# 1 Introduzione alle modalità di protezione

HP ProtectTools Security Manager è un software che fornisce funzioni di protezione create per salvaguardare il computer, le reti e i dati critici dall'accesso non autorizzato. L'amministrazione di HP ProtectTools Security Manager viene fornita tramite la funzione Console amministrativa.


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

- Abilitare o disabilitare le funzioni di protezione
- Registrare le impronte digitali degli utenti del computer
- Configurare una smart card
- Specificare le credenziali di autenticazione obbligatorie
- Gestire gli utenti del computer
- Modificare i parametri specifici del dispositivo
- Configurare le applicazioni di Security Manager installate
- Aggiungere altre applicazioni di Security Manager

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

I moduli software HP ProtectTools possono essere preinstallati, precaricati o scaricati dal sito Web HP. Per ulteriori informazioni, visitare <http://www.hp.com>.

---

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

---

# Funzioni di HP ProtectTools

Nella tabella seguente vengono presentate in dettaglio le principali funzionalità dei moduli HP ProtectTools.

Modulo	Funzioni principali
Credential Manager per HP ProtectTools	<ul style="list-style-type: none"><li>• Password Manager è un contenitore di password personale, che semplifica il processo di accesso con la funzione Single Sign On, che ricorda automaticamente e applica le credenziali utente.</li><li>• Questa funzione offre inoltre un livello di protezione aggiuntivo, poiché per l'autenticazione utente richiede combinazioni di tecnologie di sicurezza diverse, quali le Java™ Card e la biometrica.</li><li>• La memorizzazione della password viene protetta dalla crittografia software e può essere ottimizzata mediante l'impiego dell'autenticazione del dispositivo di protezione, come Java Card o biometria.</li></ul> <p><b>NOTA:</b> La funzionalità di Credential Manager è disponibile nell'opzione Password Manager di HP ProtectTools Security Manager</p>
Drive Encryption per HP ProtectTools (solo in determinati modelli)	<ul style="list-style-type: none"><li>• Drive Encryption fornisce una crittografia completa e integrale dei dischi rigidi.</li><li>• Impone che venga effettuata un'autenticazione pre-avvio per poter decrittografare i dati e accedere a essi.</li></ul>
Privacy Manager per HP ProtectTools (solo in determinati modelli)	<ul style="list-style-type: none"><li>• Privacy Manager utilizza tecniche di accesso avanzate per verificare l'origine, l'integrità e la sicurezza delle comunicazioni quando si utilizza e-mail, documenti di Microsoft® Office o messaggi istantanei (IM).</li></ul>
File Sanitizer per HP ProtectTools	<ul style="list-style-type: none"><li>• File Sanitizer consente di distruggere in modo sicuro le risorse di dati (informazioni sensibili compresi file di applicazioni, dati cronologici o relativi al Web o altri componenti di dati) presenti sul computer ed eseguire la pulizia periodica del disco rigido.</li></ul>
Device Access Manager per HP ProtectTools (solo in determinati modelli)	<ul style="list-style-type: none"><li>• Device Access Manager consente ai gestori informatici di controllare l'accesso alle periferiche sulla base dei profili degli utenti.</li><li>• Device Access Manager impedisce agli utenti non autorizzati di usare supporti di memorizzazione esterna per rimuovere dati introdurre virus nel sistema.</li><li>• L'amministratore può disattivare l'accesso ai dispositivi scrivibili a singoli utenti o a gruppi.</li></ul>

# Raggiungimento degli obiettivi chiave relativi alla protezione

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

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

## Protezione da furti mirati

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

- Se abilitata, la funzione di autenticazione al preavvio impedisce l'accesso al sistema operativo. Vedere le seguenti procedure:
  - Security Manager
  - Drive Encryption

## Limitazione dell'accesso ai dati sensibili

Si supponga che un collaboratore esterno lavori in sede e disponga di accesso al computer per esaminare dati finanziari sensibili; non si desidera che tale persona abbia la possibilità di stampare i file o di salvarli su un dispositivo di scrittura, come un CD. La funzionalità seguente consente di limitare l'accesso ai dati:

- Device Access Manager per HP ProtectTools consente ai manager IT di limitare l'accesso ai dispositivi di scrittura in modo che le informazioni sensibili non possano essere stampate o copiate dal disco rigido su supporti rimovibili.

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

L'accesso non autorizzato a un PC di lavoro non protetto presenta un rischio molto tangibile per le risorse presenti nella rete aziendale, quali le informazioni provenienti da servizi finanziari, da un dirigente o da un team R&S, e per informazioni private come i record personali dei pazienti o finanziari. Le funzioni seguenti aiutano a impedire gli accessi non autorizzati:

- Se abilitata, la funzione di autenticazione al preavvio impedisce l'accesso al sistema operativo. Vedere le seguenti procedure:
  - Password Manager
  - Drive Encryption
- Password Manager permette di assicurare che un utente non autorizzato non possa ottenere password o accesso ad applicazioni protette da password.

- Device Access Manager per HP ProtectTools consente ai manager IT di limitare l'accesso ai dispositivi di scrittura in modo che le informazioni sensibili non possano essere copiate dal disco rigido.
- DriveLock consente di impedire l'accesso ai dati anche se il disco rigido viene rimosso e installato in un sistema non protetto.


## Creazione di criteri password complessi

Se viene richiesto l'impiego di criteri complessi per password per decine di database e applicazioni basate su Web, Security Manager costituisce un archivio protetto per password e fornisce la comodità della funzionalità Single Sign On.

# Ulteriori elementi protettivi


## Assegnazione dei ruoli per la protezione

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

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

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

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

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

- Amministratore IT: applica e gestisce le funzioni di protezione decise dal responsabile per la protezione. Può anche attivare e disattivare alcune funzioni. Ad esempio, se il responsabile per la protezione ha deciso di utilizzare le Java Card, l'amministratore IT può attivare la modalità di protezione del BIOS con Java Card.
- Utente: utilizza le funzioni di protezione. Ad esempio, se il responsabile per la protezione e l'amministratore IT hanno attivato le Java Card per il sistema, l'utente può impostare il PIN della Java Card e utilizzare quest'ultima per l'autenticazione.

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

Agli utenti non autorizzati non devono essere concessi privilegi amministrativi.

## Gestione delle password di HP ProtectTools

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

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

Password di HP ProtectTools	Modulo di HP ProtectTools in cui è impostata	Funzione
Password di accesso a Security Manager	Security Manager	Questa password è disponibile per 2 opzioni: <ul style="list-style-type: none"><li>● Può essere utilizzata per accedere a Security Manager dopo aver effettuato l'accesso a Windows.</li><li>● Può essere utilizzata per consentire l'accesso contemporaneo a Windows e a Security Manager.</li></ul>

<b>Password di HP ProtectTools</b>	<b>Modulo di HP ProtectTools in cui è impostata</b>	<b>Funzione</b>
Password del file di ripristino di Security Manager	Security Manager, da amministratore IT	Protegge l'accesso al file di ripristino di Security Manager.
PIN Java™ Card	Java Card Security	<p>Protegge l'accesso al contenuto della Java Card e permette l'autenticazione degli utenti della Java Card. Quando utilizzato per l'autenticazione dell'accensione, il PIN Java Card protegge anche l'accesso all'utilità Impostazione del computer e al contenuto del computer.</p> <p>Permette l'autenticazione degli utenti di Drive Encryption se il token della Java Card è stato selezionato.</p>
Password di accesso a Windows	Pannello di controllo di Windows®	Può essere utilizzata per l'accesso manuale o salvata nella Java Card.

## Creazione di una password di protezione

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


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

## Backup e ripristino delle credenziali di HP ProtectTools

È possibile utilizzare Drive Encryption per HP ProtectTools per selezionare ed eseguire il backup delle credenziali di HP ProtectTools.

---

## 2 Guida introduttiva

 **NOTA:** Per poter amministrare HP ProtectTools è necessario disporre dei privilegi di amministratore.

L'installazione guidata di HP ProtectTools accompagna l'utente nella procedura di installazione delle funzionalità più utilizzate di Security Manager. Tuttavia, sono disponibili numerose altre funzionalità aggiuntive disponibili dalla console amministrativa di HP ProtectTools. Le stesse impostazioni presenti nell'installazione guidata, oltre alle funzionalità di protezione aggiuntive, possono essere configurate tramite la console, a cui è possibile accedere dal menu Start di Windows®. Queste impostazioni si applicano al computer e agli utenti che condividono il computer.

1. Nella pagina iniziale, è possibile disabilitare la visualizzazione della procedura guidata selezionando una delle opzioni disponibili.
2. Una settimana dopo aver configurato il computer o quando un utente con diritti amministrativi passa un dito sul lettore di impronte digitali per la prima volta, l'installazione guidata di HP ProtectTools si avvia automaticamente per accompagnare l'utente attraverso i passaggi basilari di configurazione del programma. Viene avviata automaticamente una esercitazione video sulla configurazione del computer.
3. Seguire le istruzioni visualizzate fino al completamento dell'installazione.

Se non si completa la procedura guidata, questa viene avviata automaticamente ancora due volte. Successivamente, è possibile accedervi dal messaggio che viene visualizzato accanto all'area di notifica della barra delle applicazioni (tranne nel caso in cui sia stato disabilitato, come descritto al passaggio 2) fino a quando non viene completata la procedura.

Per utilizzare le applicazioni di HP ProtectTools Security Manager, avviare il programma dal menu Start oppure fare clic con il pulsante destro del mouse sull'icona di Security Manager nell'area di notifica situata all'estrema destra della barra delle applicazioni. La Console amministrativa di HP ProtectTools e le sue applicazioni sono disponibili a tutti gli utenti che condividono il computer.



# Apertura della console amministrativa di HP ProtectTools

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

- ▲ Fare clic su **Start, Tutti i programmi**, su **HP** e infine su **HP ProtectTools Administrative Console**.

Oppure

Nel riquadro di sinistra di Security Manager, fare clic su **Amministrazione**.

Per le attività dell'utente, come registrazione di impronte digitali o uso di Security Manager, aprire la console come indicato:

- ▲ Fare clic su **Start, Tutti i programmi, HP**, infine su **HP ProtectTools Security Manager**.

Oppure

Fare doppio clic sull'icona **HP ProtectTools Security Manager** nell'area di notifica situata a destra della barra delle applicazioni.

# Attivazione delle funzioni di protezione

Durante l'esecuzione dell'installazione guidata viene richiesta la verifica dell'identità.

1. Leggere le informazioni nella schermata iniziale, quindi fare clic su **Avanti**.
2. Eseguire la verifica dell'identità immettendo la password di Windows, se non si sono ancora registrate le impronte digitali, oppure eseguendo la scansione dell'impronta digitale con il relativo lettore. Fare clic su **Avanti**.


Se la password di Windows è vuota, verrà richiesto di crearne una. È necessaria una password di Windows per proteggere l'account di Windows dall'accesso non autorizzato e poter utilizzare le funzioni di HP ProtectTools Security Manager.

L'installazione guidata accompagna l'utente attraverso il processo di attivazione delle funzionalità di protezione valide per tutti gli utenti del computer:

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

Per abilitare una funzione di protezione, selezionare la casella di controllo corrispondente. Più funzioni si selezionano, più protetto sarà il computer.

---

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


---

# Registrazione delle impronte digitali

Se si è selezionato "Impronta digitale" e il computer in uso ha un lettore di impronte digitali integrato o collegato, si verrà guidati attraverso il seguente processo di impostazione o "registrazione" delle impronte digitali:

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


---

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

---

2. Una volta selezionato un dito da registrare, viene richiesto di eseguire la scansione dell'impronta digitale finché non viene completata la registrazione. Un dito registrato viene evidenziato in verde nel profilo.
3. È necessario registrare almeno due dita, preferibilmente l'indice o il medio. Ripetere i passaggi da 1 a 3 per un altro dito.
4. Fare clic su **Avanti**.

---

 **NOTA:** Quando si registrano le impronte digitali tramite il processo descritto nella sezione Informazioni preliminari, le informazioni sulle impronte digitali non vengono salvate fino a quando non si fa clic su **Avanti**. Se si lascia il computer inattivo per un po' o si chiude il dashboard, le modifiche apportate **non** verranno salvate.

---

## Configurazione di una smart card

Se è stato selezionato "Smart card" e un lettore di smart card è integrato o collegato al computer, l'installazione guidata di HP ProtectTools chiede di configurare un PIN (personal identification number) per la smart card.

Per configurare il PIN di una smart card:

1. Nella pagina di impostazione della smart card, immettere un PIN e confermarlo.

È anche possibile modificare il PIN. A tal fine, immettere il PIN precedente, quindi sceglierne uno nuovo.

2. Per continuare, fare clic su **Avanti**.

# Uso della console amministrativa

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

La console è composta dai seguenti componenti:

- **Strumenti:** visualizza le seguenti categorie per la configurazione della protezione sul computer:
  - **Home:** consente di selezionare le attività di protezione da eseguire.
  - **Sistema:** consente di configurare le funzioni di protezione e l'autenticazione per utenti e dispositivi.
  - **Applicazioni:** visualizza le impostazioni generali di HP ProtectTools Security Manager e delle applicazioni di Security Manager.
  - **Dati:** rende disponibile un menu espandibile di collegamenti che rimandano alle applicazioni di Security Manager per la protezione dei dati.
- **Strumenti di gestione:** offre informazioni su strumenti aggiuntivi e visualizza le seguenti opzioni:
  - **Installazione guidata HP ProtectTools:** accompagna l'utente durante la configurazione di HP ProtectTools Security Manager.
  - **Help (Guida):** visualizza il file della guida, che fornisce informazioni su Security Manager e le applicazioni preinstallate. La guida delle applicazioni che è possibile aggiungere è fornita in tali applicazioni.
  - **Informazioni su:** visualizza le informazioni su HP ProtectTools Security Manager, ad esempio il numero di versione e l'informativa sul copyright.
- **Area principale:** visualizza le schermate specifiche dell'applicazione.

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

---

## 3 Configurazione del sistema

Il gruppo Sistema è accessibile dal riquadro del menu Strumenti sul lato sinistro della schermata della Console amministrativa di HP ProtectTools. È possibile utilizzare le applicazioni in questo gruppo per gestire i criteri e le impostazioni del computer, i suoi utenti e le sue periferiche.

Le applicazioni riportate di seguito sono incluse nel gruppo Sistema:

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

# Impostazione dell'autenticazione del computer

All'interno dell'applicazione Autenticazione, è possibile selezionare le funzioni di protezione da implementare nel computer in uso, impostare i criteri che regolano l'accesso al computer, nonché configurare ulteriori impostazioni avanzate. È possibile specificare le credenziali richieste per eseguire l'autenticazione di ogni classe di utente quando esegue l'accesso a Windows o ai siti Web e ai programmi durante una sessione utente.

Per impostare l'autenticazione del computer:

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

## Criterio di accesso

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

1. Nel menu Strumenti, fare clic su **Protezione**, quindi su **Autenticazione**.
2. Nella scheda **Criterio di accesso**, fare clic su una categoria di utente.
3. Specificare le credenziali di autenticazione richieste per la categoria di utente selezionata. Specificare almeno una credenziale.
4. Scegliere se è richiesta UNA (solo una) delle credenziali specificate, o se TUTTE le credenziali specificate sono richieste per autenticare un utente. È inoltre possibile impedire a qualsiasi utente di accedere al computer.
5. Fare clic su **Applica**.

## Criterio di sessione

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

1. Nel menu Strumenti, fare clic su **Protezione**, quindi su **Autenticazione**.
2. Nella scheda **Criterio di sessione**, fare clic su una categoria di utente.
3. Specificare le credenziali di autenticazione richieste per la categoria di utente selezionata.
4. Scegliere se è richiesta UNA (solo una) delle credenziali specificate, o se TUTTE le credenziali specificate sono richieste per autenticare un utente. È inoltre possibile richiedere nessuna autenticazione per accedere al software HP ProtectTools.
5. Fare clic su **Applica**.

# Impostazioni

È possibile consentire una o più impostazioni di protezione riportate di seguito:

- **Consenti accesso HP One-Step Logon:** consente agli utenti del computer di ignorare l'accesso di Windows se l'autenticazione è stata eseguita a livello di BIOS o di disco crittografato.
- **Consenti autenticazione HP SpareKey per l'accesso a Windows:** consente agli utenti del computer di utilizzare la funzione HP SpareKey per eseguire l'accesso a Windows a prescindere da eventuali altri criteri di autenticazione richiesti da Security Manager.

Per modificare le impostazioni:

1. Fare clic per abilitare o disabilitare un'impostazione specifica.
2. Fare clic su **Applica** per salvare le modifiche apportate.



## Gestione degli utenti

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

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

Per aggiungere utenti, fare clic su **Aggiungi**.

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

Per registrare le impronte digitali o impostare credenziali aggiuntive per l'utente, selezionare l'utente desiderato, quindi fare clic su **Registra**.

Per visualizzare i criteri per un utente specifico, selezionare l'utente desiderato, quindi fare clic su **Visualizza criteri**.

# Specificazione delle impostazioni dei dispositivi

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

## Impronte digitali

Nella pagina Impronte digitali sono disponibili tre schede: Registrazione, Sensibilità e Avanzate.

### Registrazione

È possibile scegliere il numero minimo e massimo di impronte digitali che un utente può registrare.

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

**⚠ AVVERTENZA!** Tutti i dati relativi alle impronte digitali di tutti gli utenti, inclusi gli amministratori, verranno cancellate. Se il criterio di accesso richiede soltanto le impronte digitali, è possibile che l'accesso al computer sia impedito a tutti gli utenti.

### Sensibilità

Per modificare la sensibilità utilizzata dal lettore di impronte digitali durante la scansione, spostare il dispositivo di scorrimento.

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

### Avanzate

È possibile configurare il lettore di impronte digitali in modo da risparmiare energia quando il computer funziona a batteria.

## Smart card

È possibile configurare il computer affinché si blocchi in modo automatico alla rimozione di una smart card. Tuttavia, il computer si bloccherà solo se la smart card è stata utilizzata come credenziale di autenticazione durante l'accesso a Windows. La rimozione di una smart card non utilizzata per eseguire l'accesso a Windows non determinerà il blocco del computer.

▲ Selezionare la casella di controllo per abilitare o disabilitare il blocco del computer alla rimozione della smart card.

---

## 4 Configurazione delle applicazioni

Il gruppo Applicazioni è accessibile dal riquadro del menu Applicazioni di protezione sul lato sinistro della Console amministrativa di HP ProtectTools. È possibile utilizzare Impostazioni per personalizzare il comportamento delle applicazioni di HP ProtectTools Security Manager attualmente installate.

Per modificare le impostazioni delle applicazioni:

1. Nel menu Strumenti, dal gruppo **Applicazioni**, fare clic su **Impostazioni**.
2. Fare clic per abilitare o disabilitare un'impostazione specifica.
3. Fare clic su **Applica** per salvare le modifiche apportate.

## Scheda Generale

Nella scheda Generale, sono disponibili le seguenti impostazioni:

- ▲ **Do not automatically launch the Setup Wizard for administrators** (Non avviare automaticamente l'installazione guidata per amministratori): selezionare questa opzione per impedire l'avvio automatico dell'installazione guidata all'accesso.
- ▲ **Non avviare automaticamente l'introduzione guidata per gli utenti**: selezionare questa opzione per impedire l'apertura automatica della configurazione utente al momento dell'accesso.

## Scheda Applications (Applicazioni)

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

- **Security Manager:** attiva Security Manager per tutti gli utenti del computer.
- **Abilita il pulsante Altre applicazioni:** consente a tutti gli utenti del computer di aggiungere applicazioni a HP ProtectTools Security Manager facendo clic sul pulsante **[+] Altre applicazioni**.

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

---

## 5 Aggiunta di strumenti di gestione

È possibile che siano disponibili altre applicazioni per l'aggiunta di nuovi strumenti di protezione in Security Manager. L'amministratore del computer può disattivare questa funzione tramite l'applicazione Impostazioni.

Per aggiungere strumenti di gestione, fare clic su **[+] Strumenti di gestione**.

È possibile accedere al sito Web di DigitalPersona per controllare la disponibilità di nuove applicazioni oppure è possibile impostare una pianificazione per gli aggiornamenti automatici.

---

## 6 HP ProtectTools Security Manager

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

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


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

# Procedure di installazione

## Guida introduttiva

L'installazione guidata di HP ProtectTools viene visualizzata automaticamente come pagina predefinita in HP ProtectTools Security Manager finché non viene completata la configurazione.

Per impostare Security Manager, procedere come segue:

 **NOTA:** Se non è disponibile un lettore di impronte digitali né una smart card, eseguire soltanto i passaggi 1, 5 e 6.

---

1. Fare clic sulla pagina iniziale, quindi su **Avanti**.
  2. Nella pagina seguente sono elencati i metodi di autenticazione disponibili nel computer. Per continuare, fare clic su **Avanti**.
  3. Nella pagina "Verifica dell'identità", immettere la password di Windows, quindi fare clic su **Avanti**.
  4. Fare riferimento a uno o più dei seguenti argomenti a seconda della configurazione del computer in uso.
    - Se è disponibile un lettore di impronte digitali, consultare [Registrazione delle impronte digitali a pagina 24](#).
    - Se è disponibile una smart card, consultare [Configurazione di una smart card a pagina 25](#).
  5. Se non è disponibile un lettore di impronte digitali né una smart card, verrà richiesto di immettere la password di Windows. Sarà necessario utilizzare questa password ogni volta che verrà richiesta l'autenticazione.
  6. Nella pagina finale della procedura guidata, fare clic su **Fine**.
- Viene visualizzato il dashboard di Security Manager.

## Registrazione delle credenziali

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

## Registrazione delle impronte digitali


Se il computer dispone di un lettore di impronte digitali integrato o collegato, l'installazione guidata di HP ProtectTools accompagna l'utente nel processo di impostazione o "registrazione" delle impronte digitali.

1. Leggere le informazioni nella schermata iniziale, quindi fare clic su **Avanti**.
2. Eseguire la verifica dell'identità immettendo la password di Windows, se non si sono ancora registrate le impronte digitali, oppure eseguendo la scansione dell'impronta digitale con il relativo lettore. Fare clic su **Avanti**.


Se la password di Windows è vuota, verrà richiesto di crearne una. È necessaria una password di Windows per poter proteggere l'account di Windows dall'accesso non autorizzato e poter utilizzare le funzioni di HP ProtectTools Security Manager.



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

 **NOTA:** Per eliminare un'impronta digitale registrata in precedenza, fare clic sull'impronta desiderata.

- Una volta selezionato un dito da registrare, viene richiesto di eseguire la scansione dell'impronta digitale finché non viene completata la registrazione. Un dito registrato viene evidenziato in verde nel profilo.
- È necessario registrare almeno due dita, preferibilmente l'indice o il medio. Ripetere i passaggi 3 e 4 per un altro dito.
- Fare clic su **Avanti**.

 **NOTA:** Quando si registrano le impronte digitali tramite il processo descritto nella sezione Informazioni preliminari, le informazioni sulle impronte digitali non vengono salvate fino a quando non si fa clic su **Avanti**. Se si lascia il computer inattivo per qualche tempo o si chiude il dashboard, le modifiche apportate **non** verranno salvate.

## Modifica della password di Windows

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

Per modificare la password di Windows, procedere come segue:

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

## Configurazione di una smart card

Se un lettore di smart card è integrato o collegato al computer, Security Manager richiederà di impostare un PIN (Personal Identification Number, Numero di identificazione personale) per la smart card.

- Per impostare un PIN per la smart card: accedere alla pagina di impostazione della smart card, immettere un PIN e confermarlo.
- Per modificare il PIN: immettere il PIN precedente, quindi sceglierne uno nuovo.

## Utilizzo del dashboard di Security Manager

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

Il dashboard è composto dai seguenti componenti:

- **Scheda ID:** visualizza il nome utente di Windows e un'immagine selezionata che identifica l'account utente che ha eseguito l'accesso.
- **Applicazioni di protezione:** visualizza un menu espandibile di collegamenti per la configurazione delle seguenti categorie di protezione:
  - **Identità personale**
  - **Dati personali**
  - **Risorse del computer**
- **Altre applicazioni:** consente di aprire una pagina in cui sono disponibili ulteriori applicazioni rivolte ad aumentare la protezione dell'identità, dei dati e delle comunicazioni personali.
- **Area principale:** visualizza le schermate specifiche dell'applicazione.
- **Amministrazione:** apre la console amministrativa di HP ProtectTools.
- **Pulsante Guida:** consente di visualizzare le informazioni sulla schermata corrente.
- **Avanzate:** consente di accedere alle seguenti opzioni:
  - **Preferenze:** consente di personalizzare le impostazioni di Security Manager.
  - **Backup e ripristino:** consente di eseguire il backup o il ripristino dei dati.
  - **Informazioni su:** consente di visualizzare le informazioni sulla versione di Security Manager.

Per aprire il pannello di Security Manager, fare clic su **Start, Tutti i programmi, HP**, quindi su **HP ProtectTools Security Manager**.

## Apertura di HP ProtectTools Security Manager

È possibile aprire HP ProtectTools Security Manager in uno dei modi seguenti:

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

## Attività generali

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

- **Security Manager:** crea e gestisce Quick Links, che consente di avviare e accedere a siti Web e programmi autenticandosi con la password di Windows, le impronte digitali o una smart card.
- **Credenziali:** consente di modificare facilmente la password di Windows, registrare le impronte digitali o impostare una smart card.

Per aggiungere altre applicazioni, fare clic sul pulsante [+] **Altre applicazioni** nell'angolo inferiore sinistro del dashboard. Il pulsante può essere disabilitato dall'amministratore.

## Gestore password

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

Password Manager offre le seguenti opzioni:

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

Molte funzioni di Password Manager sono anche disponibili dall'icona Password Manager che viene visualizzata quando è attiva una schermata di accesso a una pagina Web o ai programmi. Fare clic sull'icona per visualizzare un menu contestuale da cui è possibile scegliere le opzioni riportate di seguito.

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


Nel menu contestuale vengono visualizzate le seguenti opzioni:

- **Aggiungi [undominio.com] a Password Manager:** consente di aggiungere un accesso alla schermata di accesso corrente.
- **Apri Password Manager:** avvia Password Manager.
- **Impostazioni icona:** consente di specificare le condizioni in base a cui visualizzare l'icona di Password Manager.
- **Guida:** visualizza la Guida di Password Manager.

## Per le pagine Web o i programmi per i quali è stato già creato un accesso

Nel menu contestuale vengono visualizzate le seguenti opzioni:

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

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

## Aggiunta di accessi

È possibile aggiungere facilmente un accesso a un sito Web o programma immettendo i dati di accesso una volta, dopodiché la loro immissione avverrà in modo automatico. È possibile utilizzare questi accessi dopo la navigazione al sito Web o al programma oppure fare clic su un accesso dal menu **Accessi** per aprire il sito Web o il programma ed accedervi automaticamente.

Per aggiungere un accesso:

1. Aprire la schermata di accesso a un sito Web o programma.
2. Fare clic sulla freccia dell'icona **Password Manager**, quindi fare clic su una delle seguenti opzioni a seconda che la schermata di accesso sia relativa a un sito Web o a un programma:
  - Per un sito Web, fare clic su **Aggiungi [nome dominio] a Password Manager**.
  - Per un programma, fare clic su **Aggiungi schermata accesso a Password Manager**.
3. Immettere i dati di accesso. I campi di accesso nella schermata e i campi corrispondenti nella finestra di dialogo sono identificati con un bordo arancione in grassetto. È inoltre possibile visualizzare questa finestra di dialogo facendo clic su **Aggiungi accesso** dalla scheda **Gestisci Password Manager**. Alcune opzioni dipendono dai dispositivi di protezione associati al computer, ad esempio l'utilizzo del tasto di scelta rapida **ctrl+alt+H**, la scansione dell'impronta digitale o l'inserimento di una smart card.
  - Per compilare un campo di accesso con una delle opzioni preformattate, fare clic sulle frecce a destra del campo.
  - Per aggiungere altri campi dalla schermata all'accesso, fare clic su **Scegli altri campi**.
  - Per compilare i campi di accesso, ma non inviarli, deselezionare la casella di controllo **Invia dati di accesso**.
  - Per visualizzare la password di accesso, fare clic su **Mostra password**.
4. Fare clic su **OK**.

Il segno "+" viene rimosso dall'icona di Password Manager per notificare la creazione dell'accesso.

Ogni volta che si accede a tale sito Web o si apre tale programma, viene visualizzata l'icona di Password Manager per indicare che è possibile utilizzare le credenziali registrate per eseguire l'accesso.

## Modifica degli accessi

Per modificare un accesso, procedere come segue:

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

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

3. Modificare le informazioni di accesso.
  - Per compilare un campo di accesso con una delle opzioni preformattate, fare clic sulle frecce a destra del campo.
  - Per aggiungere altri campi dalla schermata all'accesso, fare clic su **Scegli altri campi**.
  - Per compilare i campi di accesso, ma non inviarli, deselezionare la casella di controllo **Invia dati di accesso**.
  - Per visualizzare la password di accesso, fare clic su **Mostra password**.
4. Fare clic su **OK**.

## Utilizzo del menu degli accessi

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

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

Per visualizzare il menu Accessi:

1. Premere la combinazione di tasti di scelta rapida di **Password Manager**. **ctrl+alt+h** è l'impostazione predefinita. Per modificare la combinazione di tasti di scelta rapida, fare clic su **Password Manager**, quindi su **Impostazioni**.
2. Eseguire la scansione dell'impronta digitale (sui computer con un lettore di impronte digitali integrato o collegato).

## Organizzazione degli accessi in categorie

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

Per aggiungere una categoria:

1. Dal dashboard di Security Manager, fare clic su **Password Manager**.
2. Fare clic sulla scheda **Gestisci**, quindi su **Aggiungi categoria**.

3. Inserire un nome per la categoria.
4. Fare clic su **OK**.

Per aggiungere un accesso a una categoria:

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

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

## Gestione degli accessi

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

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

Per gestire gli accessi:

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

- **Aggiungi ad accesso:** fare clic su **Aggiungi accesso** e seguire le istruzioni visualizzate.
- **Modifica accesso:** fare clic su un accesso, quindi su **Modifica**, infine modificare i dati di accesso.
- **Elimina un accesso:** fare clic su un accesso, quindi su **Elimina**.

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 sull'icona **Password Manager** per visualizzare il menu dei tasti di scelta rapida.
3. Fare clic su **Aggiungi accesso**, quindi seguire le istruzioni visualizzate.

## Valutazione della complessità della password

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

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

## Impostazioni dell'icona di Gestore password

Password Manager esegue l'identificazione delle schermate di accesso ai siti Web e programmi. Quando rileva una schermata di accesso per la quale non è stato creato un accesso, Password Manager richiede di aggiungere un accesso per tale schermata visualizzando la propria icona con il segno "+".

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

- **Richiedi l'aggiunta di accessi per le schermate di accesso:** fare clic su questa opzione per fare in modo che Password Manager richieda di aggiungere un accesso quando viene visualizzata una schermata di accesso per la quale non è stato ancora configurato un accesso.
- **Escludi questa schermata:** fare clic sulla casella di controllo per fare in modo che Password Manager non chieda di nuovo di aggiungere un accesso per questa schermata.

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

## Impostazioni

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

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

## Credenziali

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

Le credenziali disponibili possono variare in base ai dispositivi di protezione integrati o collegati al computer in uso. Per ogni credenziale supportata sarà presente una voce nel gruppo **Identità personale, Credenziali**.

Le credenziali disponibili, i requisiti e lo stato corrente vengono elencati ed è possibile che sia incluso quanto riportato di seguito:

- Impronte digitali
- Password
- Smart card

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

## Scheda ID personale

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

Uno dei numerosi modi per accedere a Security Manager consiste nel fare clic sulla scheda ID nella barra laterale di Windows.

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

Per modificare il nome di visualizzazione:

1. Dal dashboard di Security Manager, fare clic su **Scheda ID** nell'angolo superiore sinistro.
2. Fare clic sulla casella con il nome immesso per l'account in Windows. Verrà visualizzato il nome utente di Windows per questo account.
3. Per modificare il nome, digitarne uno nuovo, quindi fare clic sul pulsante **Salva**.

Per modificare l'immagine visualizzata:

1. Dal dashboard di Security Manager, fare clic su **Identità personale**, quindi su **Scheda ID** nell'angolo superiore sinistro.
2. Fare clic sul pulsante **Scegli immagine**, quindi selezionare un'immagine e fare clic sul pulsante **Salva**.

## Impostazione delle preferenze

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

### Generale

Nella scheda Generale, sono disponibili le seguenti impostazioni:

#### Visualizza: mostra l'icona nella barra delle applicazioni

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

Per disabilitare la visualizzazione dell'icona nella barra delle applicazioni, deselegionare la casella di controllo.

### Impronta digitale

Nella scheda Impronte digitali, sono disponibili le seguenti impostazioni:

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

Per assegnare un'Azione rapida a uno dei tasti elencati:

- Fare clic sull'opzione **(Tasto)+Impronta digitale**, quindi su una delle seguenti attività disponibili nel menu.



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


- **Abilita suoni feedback:** quando è stata eseguita la scansione di un'impronta digitale, in Security Manager viene riprodotto un feedback audio con suoni diversi in corrispondenza di eventi di programma specifici. È possibile assegnare nuovi suoni a questi eventi tramite la scheda Suoni nel Pannello di controllo di Windows oppure disabilitare il feedback audio deselegzionando questa opzione.
- **Mostra feedback qualità scansione:** per impostazione predefinita, Security Manager mostra l'immagine di un'impronta digitale con un punto interrogativo ogni volta che la qualità di scansione di un'impronta digitale non è sufficiente ad eseguire l'autenticazione. È possibile disabilitare la visualizzazione dell'immagine deselegzionando questa opzione.

## Backup e ripristino dei dati

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

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

---

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

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

---

Per eseguire il backup dei dati:

1. Nel riquadro di sinistra, fare clic su **Avanzate**, quindi su **Backup e ripristino**.
2. Fare clic sul pulsante **Backup dei dati**.
3. Selezionare i moduli da includere nel backup. In genere, si selezionano tutti i moduli.
4. Inserire un nome per il file di archiviazione. Per impostazione predefinita, il file verrà salvato nella cartella Documenti. Fare clic su **Sfogli** per specificare una posizione diversa.
5. Immettere una password per proteggere il file.
6. Verificare l'identità.
7. Fare clic sul pulsante **Fine**.

Per ripristinare i dati:

1. Nel riquadro di sinistra, fare clic su **Avanzate**, quindi su **Backup e ripristino**.
2. Fare clic sul pulsante **Ripristina dati**.
3. Selezionare il file di archiviazione creato in precedenza. È possibile immettere il percorso nell'apposito campo oppure fare clic su **Modifica**.
4. Immettere la password utilizzata per proteggere il file.


5. Selezionare i moduli di cui ripristinare i dati. In genere, si selezionano tutti i moduli elencati.
6. Fare clic sul pulsante **Fine**.

## Aggiunta di applicazioni

Sono disponibili ulteriori applicazioni che consentono di utilizzare nuove funzioni del programma.

Dal dashboard di Security Manager, fare clic su **[+] Altre applicazioni**, quindi cercare le applicazioni aggiuntive.

---

 **NOTA:** Se non è disponibile alcun collegamento **[+] Altre applicazioni** nella parte inferiore sinistra del dashboard, significa che l'amministratore ha disabilitato questa funzione sul computer.

---

## Stato delle applicazioni di protezione

La pagina Stato delle applicazioni di Security Manager visualizza lo stato completo delle applicazioni di protezione installate. Mostra le applicazioni impostate e lo stato della configurazione di ciascuna di essa. Il riepilogo viene visualizzato automaticamente quando si apre il dashboard di Security Manager o si fa clic su **Applicazioni di protezione**.

---

# 7 Drive Encryption per HP ProtectTools (solo in determinati modelli)


△ **ATTENZIONE:** Se si decide di disinstallare il modulo Drive Encryption, prima è necessario decrittografare tutte le unità crittografate. In caso contrario, non sarà possibile accedere ai dati presenti sulle unità crittografate a meno di essere registrati al servizio di recupero di Drive Encryption. La reinstallazione del modulo Drive Encryption non consente di accedere alle unità crittografate.

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

L'installazione guidata di HP ProtectTools consente agli amministratori di Windows di attivare Drive Encryption, eseguire il backup della chiave di crittografia, aggiungere e rimuovere utenti e disattivare Drive Encryption. Per ulteriori informazioni, vedere la Guida del software HP ProtectTools Security Manager.

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

- Gestione crittografia
  - Crittografia o decrittografia di singole unità disco

 **NOTA:** Solo le unità disco rigido interne possono essere crittografate.

- Ripristino
  - Creazione delle chiavi di backup
  - Esecuzione di un ripristino

# Procedure di configurazione


## Apertura di Drive Encryption

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

# Attività generali


## Attivazione di Drive Encryption

Per attivare Drive Encryption utilizzare l'installazione guidata di HP ProtectTools.

 **NOTA:** L'impostazione guidata consente inoltre di aggiungere e rimuovere utenti.

Oppure

1. Fare clic su **Start, Tutti i programmi**, su **HP** e infine su **HP ProtectTools Administrative Console**.
2. Nel riquadro di sinistra, fare clic su **Protezione**, quindi su **Funzioni**.
3. Selezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Avanti**.
4. In **Unità da crittografare**, selezionare la casella di controllo corrispondente all'unità disco rigido che si desidera crittografare.
5. Inserire il dispositivo di archiviazione nello slot appropriato.

 **NOTA:** Per salvare la chiave di crittografia, è necessario utilizzare un dispositivo di archiviazione USB formattato FAT32.

6. In **Dispositivo di archiviazione esterno su cui salvare la chiave di crittografia**, selezionare la casella di controllo corrispondente al dispositivo di archiviazione desiderato.
7. Fare clic su **Applica**.

Viene avviata la crittografia dell'unità.

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

## Disattivazione di Drive Encryption

Per disattivare Drive Encryption utilizzare l'installazione guidata di HP ProtectTools. Per ulteriori informazioni, vedere la Guida del software HP ProtectTools Security Manager.


Oppure

1. Fare clic su **Start, Tutti i programmi**, su **HP** e infine su **HP ProtectTools Administrative Console**.
2. Nel riquadro di sinistra, fare clic su **Protezione**, quindi su **Funzioni**.
3. Deselezionare la casella di controllo **Drive Encryption**, quindi fare clic su **Applica**.


Viene avviata la decrittografia dell'unità.

## Accesso dopo l'attivazione di Drive Encryption

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

 **NOTA:** Se l'amministratore di Windows ha attivato la Protezione preavvio in HP ProtectTools Security Manager, l'accesso al computer verrà eseguito immediatamente dopo l'accensione, piuttosto che nella schermata di accesso di Drive Encryption.


1. Fare clic sul proprio nome utente e immettere la password di Windows oppure il PIN Java™ Card, o ancora passare il dito registrato.
2. Fare clic su **OK**.

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

## Protezione dei dati tramite crittografia del disco rigido


Utilizzare l'installazione guidata di HP ProtectTools per proteggere i dati crittografando il disco rigido:

1. In Security Manager, fare clic su **Guida introduttiva**, quindi fare clic sull'icona **Impostazione di Security Manager**. Verrà avviata la dimostrazione delle funzioni di Security Manager. È anche possibile avviare Security Manager dalla pagina relativa alla crittografia dell'unità.
2. Nel riquadro di sinistra, fare clic su **Drive Encryption**, quindi su **Gestione crittografia**.
3. Fare clic su **Cambia crittografia**.
4. Selezionare le unità da crittografare.

 **NOTA:** Si consiglia di crittografare l'unità disco rigido.

## Visualizzazione dello stato di crittografia

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

 **NOTA:** Per cambiare lo stato della crittografia dell'unità è necessario utilizzare la Console amministrativa di HP ProtectTools.

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

Se Drive Encryption è attivato, viene visualizzato uno dei seguenti codici di stato:

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

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

# Attività avanzate

## Gestione di Drive Encryption (attività dell'amministratore)


Nella pagina “Gestione crittografia”, gli amministratori possono visualizzare e modificare lo stato di Drive Encryption (attivo o inattivo), nonché visualizzare lo stato di crittografia di tutte le unità disco rigido del computer.

- Se lo stato è inattivo, Drive Encryption non è ancora stato attivato in HP ProtectTools Security Manager dall'amministratore di Windows e il disco rigido non è ancora protetto dal software. Per attivare Drive Encryption utilizzare l'installazione guidata di HP ProtectTools Security Manager.
- Se lo stato è attivo, Drive Encryption è stato attivato e configurato. L'unità si trova in uno dei seguenti stati:
  - Non crittografata
  - Crittografata
  - Crittografia in corso
  - Decrittografia in corso

## Crittografia o decrittografia di singole unità disco

Per crittografare una o più unità disco rigido presenti nel computer o per decrittografare un'unità che è già stata crittografata, utilizzare la funzione Cambia crittografia.

1. Aprire **Console amministrativa di HP ProtectTools**, fare clic su **Drive Encryption**, quindi su **Gestione crittografia**.
2. Fare clic su **Cambia crittografia**.
3. Nella finestra di dialogo Cambia crittografia, selezionare o deselezionare la casella di controllo accanto a ciascuna unità disco da crittografare o decrittografare, quindi fare clic su **OK**.

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

## Backup e ripristino (attività dell'amministratore)

La pagina “Ripristino” consente agli amministratori di eseguire le operazioni di backup e ripristino delle chiavi di crittografia.

**Backup delle chiavi di Drive Encryption locale:** consente di eseguire il backup delle chiavi di crittografia su supporti rimovibili durante l'attivazione di Drive Encryption.

## Creazione delle chiavi di backup

È possibile eseguire il backup di una chiave di crittografia di un'unità disco su un dispositivo di archiviazione rimovibile:

△ **ATTENZIONE:** Conservare il dispositivo di archiviazione contenente la chiave di backup in un luogo sicuro: se si dimentica la password o si perde la Java Card, la chiave di backup rappresenta l'unica possibilità di accedere al disco rigido.

---

1. Aprire **Console amministrativa di HP ProtectTools**, fare clic su **Drive Encryption**, quindi su **Ripristino**.
2. Fare clic su **Esegui backup chiavi**.
3. Nella pagina "Selezionare il disco di backup", selezionare la casella di controllo corrispondente al dispositivo sul quale si desidera eseguire il backup della chiave di crittografia, quindi fare clic su **Avanti**.
4. Leggere le informazioni visualizzate sulla pagina successiva, quindi fare clic su **Avanti**. La chiave di crittografia viene salvata sul dispositivo di archiviazione selezionato.
5. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Fine**.


## Esecuzione di un ripristino

Per eseguire un ripristino quando si è dimenticata la password, procedere come segue:

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

Viene avviato il computer.

---

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

---



---

## 8 Privacy Manager per HP ProtectTools (solo in determinati modelli)

Privacy Manager for HP ProtectTools consente di utilizzare metodi di accesso di sicurezza avanzati (autenticazione) per verificare l'origine, l'integrità e la sicurezza delle comunicazioni quando si utilizzano messaggi e-mail, documenti di Microsoft® Office o la messaggistica immediata (IM).

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


- Autenticazione delle impronte digitali
- Password di Windows®
- HP ProtectTools Java™ Card

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

Privacy Manager richiede i seguenti elementi:

- HP ProtectTools Security Manager 5.00 o successivo
- Sistema operativo Windows® 7, Windows Vista® o Windows XP
- Microsoft Outlook 2007 o Microsoft Outlook 2003
- Account e-mail valido

---

 **NOTA:** È necessario richiedere e installare un certificato di Privacy Manager (un certificato digitale) da Privacy Manager prima che sia possibile accedere alle funzioni di protezione. Per informazioni su come richiedere un certificato di Privacy Manager, fare riferimento alla sezione [Richiesta e installazione di un certificato di Privacy Manager a pagina 42](#).

---

# Procedure di configurazione

## Apertura di Privacy Manager

Per aprire Privacy Manager:

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

oppure

Fare clic con il pulsante destro del mouse sull'icona **HP ProtectTools** nell'area di notifica all'estrema destra della barra delle applicazioni, fare clic su **Privacy Manager**, quindi su **Configurazione**.

oppure

Sulla barra degli strumenti di un messaggio e-mail di Microsoft Outlook, fare clic sulla freccia giù accanto a **Invia in modo protetto** e fare clic su **Certificati** o su **Contatti attendibili**.

oppure

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

## Gestione dei certificati di Privacy Manager

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

È possibile eseguire le seguenti attività:

- Richiedere e installare un certificato di Privacy Manager
- Visualizzare i dettagli del certificato di Privacy Manager
- Rinnovare i certificati di Privacy Manager
- Quando sono disponibili più certificati, impostare un certificato di Privacy Manager predefinito che verrà utilizzato da Privacy Manager
- Eliminare e revocare un certificato di Privacy Manager (opzione avanzata)

## Richiesta e installazione di un certificato di Privacy Manager

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

## Richiesta di un certificato di Privacy Manager

1. Avviare Privacy Manager e fare clic su **Certificati**.
2. Selezionare **Richiedi un certificato di Privacy Manager**.
3. Leggere il testo presente nella pagina "Benvenuti" e fare clic su **Avanti**.
4. Leggere il contratto di licenza presente nella pagina "Contratto di licenza".
5. Assicurarsi che la casella di controllo accanto a **Selezionare per accettare i termini del contratto di licenza** sia selezionata e fare clic su **Avanti**.
6. Immettere le informazioni richieste nella pagina "Dettagli certificato", quindi fare clic su **Avanti**.
7. Nella pagina "Richiesta di certificato accettata", fare clic su **Fine**.
8. Fare clic su **OK** per chiudere il certificato.

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

## Come ottenere un certificato aziendale preassegnato di Privacy Manager

1. In Outlook, aprire il messaggio e-mail ricevuto in cui viene comunicata l'assegnazione di un certificato aziendale preassegnato.
2. Fare clic su **Ottieni**.
3. Si riceverà un messaggio e-mail in Microsoft Outlook con allegato il certificato di Privacy Manager.
4. Per installare il certificato, consultare [Installazione di un certificato di Privacy Manager a pagina 43](#)

## Installazione di un certificato di Privacy Manager

1. Quando si riceve il messaggio e-mail con il certificato di Privacy Manager allegato, aprire l'e-mail e fare clic sul pulsante **Installa**, nell'angolo inferiore destro del messaggio in Outlook 2007 oppure nell'angolo superiore sinistro in Outlook 2003.
  2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
  3. Nella pagina "Certificato installato" fare clic su **Avanti**.
  4. Nella pagina "Backup certificato" immettere il nome e il percorso per il file di backup oppure fare clic su **Sfoggia** per cercare un percorso.
- 
- △ **ATTENZIONE:** Assicurarsi di salvare il file in un percorso diverso dall'unità disco rigido e conservarlo in un posto sicuro. Il file dovrà essere riservato all'uso personale e sarà richiesto nel caso in cui risulti necessario ripristinare il certificato di Privacy Manager e le chiavi associate.
5. Immettere e confermare una password, quindi fare clic su **Avanti**.
  6. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
  7. Se si decide di iniziare il processo di invito dei contatti attendibili, seguire le istruzioni visualizzate iniziando dal passo 2 dell'argomento [Aggiunta di contatti attendibili mediante i contatti di Microsoft Outlook a pagina 47](#).

Oppure

Se si sceglie **Annulla**, per informazioni sull'aggiunta di contatti attendibili in un secondo momento, fare riferimento alla sezione [Aggiunta di un contatto attendibile a pagina 46](#).


## Visualizzazione dei dettagli del certificato di Privacy Manager

1. Avviare Privacy Manager e fare clic su **Certificati**.
2. Fare clic su un certificato di Privacy Manager.
3. Selezionare **Dettagli certificato**.
4. Dopo aver terminato la visualizzazione dei dettagli, fare clic su **OK**.

## Rinnovo di un certificato di Privacy Manager

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

1. Avviare Privacy Manager e fare clic su **Certificati**.
2. Selezionare **Rinnova certificato**.
3. Seguire le istruzioni visualizzate per acquistare un nuovo certificato di Privacy Manager.


 **NOTA:** Il processo di rinnovo del certificato di Privacy Manager non sostituisce il precedente certificato di Privacy Manager. Sarà necessario acquistare un nuovo certificato di Privacy Manager e installarlo mediante le stesse procedure illustrate in [Richiesta e installazione di un certificato di Privacy Manager a pagina 42](#).

## Impostazione di un certificato predefinito di Privacy Manager

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

Se dall'interno di Privacy Manager è stato installato nel computer più di un certificato di Privacy Manager, è possibile specificarne uno come certificato predefinito:

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

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

## Eliminazione di un certificato di Privacy Manager

Se si elimina un certificato di Privacy Manager, non sarà possibile aprire i file o visualizzare i dati crittografati con quel certificato. Se si è eliminato per errore un certificato di Privacy Manager, sarà possibile ripristinarlo utilizzando il file di backup creato quando si è installato il certificato. Per ulteriori informazioni, consultare la sezione [Ripristino di un certificato di Privacy Manager a pagina 45](#).

Per eliminare un certificato di Privacy Manager:

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

## Ripristino di un certificato di Privacy Manager


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

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

Per ulteriori informazioni, consultare la sezione [Installazione di un certificato di Privacy Manager a pagina 43](#) o [Backup dei certificati di Privacy Manager e dei contatti attendibili a pagina 60](#).

## Revoca di un certificato di Privacy Manager

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

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

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

## Gestione di contatti attendibili

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

Gestione contatti attendibili consente di eseguire le seguenti attività:

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


## Aggiunta di contatti attendibili

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

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

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

Per aggiungere contatti attendibili, fare riferimento alle seguenti sezioni.

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

## Aggiunta di un contatto attendibile

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

Oppure

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

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

Verrà generato automaticamente un messaggio e-mail.


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

---

 **NOTA:** Se non si è ottenuto un certificato di Privacy Manager, un messaggio informerà che è necessario disporre di un certificato di Privacy Manager per inviare una richiesta di contatto attendibile. Fare clic su **OK** per avviare la Richiesta guidata di un certificato. Per ulteriori informazioni, consultare la sezione [Richiesta e installazione di un certificato di Privacy Manager a pagina 42](#).

---

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

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

---

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

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

9. Fare clic su **OK**.

### Aggiunta di contatti attendibili mediante i contatti di Microsoft Outlook

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

Oppure

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

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


3. Quando viene visualizzata la pagina "Invio dell'invito", fare clic su **Fine**.

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

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


5. Fare clic su **Invia**.

---

 **NOTA:** Se non si è ottenuto un certificato di Privacy Manager, un messaggio informerà che è necessario disporre di un certificato di Privacy Manager per inviare una richiesta di contatto attendibile. Fare clic su **OK** per avviare la Richiesta guidata di un certificato. Per ulteriori informazioni, consultare la sezione [Richiesta e installazione di un certificato di Privacy Manager a pagina 42](#).

---

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

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

---

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

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

8. Fare clic su **OK**.

### Visualizzazione dei dettagli dei contatti attendibili

1. Avviare Privacy Manager e fare clic su **Gestione contatti attendibili**.
2. Fare clic su un contatto attendibile.
3. Fare clic su **Dettagli contatto**.
4. Dopo aver terminato la visualizzazione dei dettagli, fare clic su **OK**.

### Eliminazione di un contatto attendibile

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

### Verifica dello stato della revoca per un contatto attendibile

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

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

Viene visualizzata la finestra di dialogo Gestione avanzata contatti attendibili.

4. Fare clic su **Verifica revoca**.
5. Fare clic su **Chiudi**.



## Attività generali

È possibile utilizzare Privacy Manager con i seguenti prodotti Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

## Uso di Privacy Manager in Microsoft Outlook

Quando si installa Privacy Manager, viene visualizzato un pulsante Privacy sulla barra degli strumenti di Microsoft Outlook e un pulsante Invia in modo protetto viene visualizzato sulla barra degli strumenti di ciascun messaggio e-mail di Microsoft Outlook. Quando si fa clic sulla freccia giù accanto a **Privacy** o a **Invia in modo protetto**, è possibile scegliere tra le seguenti opzioni:

- Firma e invia, solo per il pulsante Invia in modalità protetta: questa opzione consente di aggiungere una firma digitale all'e-mail e di inviarla dopo che è stata eseguita l'autenticazione attraverso il metodo di accesso di sicurezza selezionato.
- Crittografa per i contatti attendibili e invia, solo per il pulsante Invia in modo protetto: questa opzione aggiunge una firma digitale, crittografa l'e-mail e la invia dopo che è stata eseguita l'autenticazione attraverso il metodo di accesso di sicurezza selezionato.
- Invita contatti: questa opzione consente di inviare un messaggio di invito di contatto attendibile. Per ulteriori informazioni, consultare la sezione [Aggiunta di un contatto attendibile a pagina 46](#).
- Invita i contatti di Outlook: questa opzione consente di inviare messaggi di invito di contatto attendibile a tutti i contatti della rubrica di Microsoft Outlook. Per ulteriori informazioni, consultare la sezione [Aggiunta di contatti attendibili mediante i contatti di Microsoft Outlook a pagina 47](#).
- Open the Privacy Manager software (Avvia il software Privacy Manager): le opzioni Certificati, Contatti attendibili e Impostazioni consentono di avviare il software Privacy Manager per aggiungere, visualizzare o modificare le impostazioni correnti. Per ulteriori informazioni, consultare la sezione [Configurazione di Privacy Manager per Microsoft Outlook a pagina 49](#).

## Configurazione di Privacy Manager per Microsoft Outlook

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

oppure

Sulla barra degli strumenti principale di Microsoft Outlook, fare clic sulla freccia giù accanto a **Invia in modo protetto (Privacy in Outlook 2003)**, quindi fare clic su **Impostazioni**.

oppure

Sulla barra degli strumenti di un messaggio e-mail di Microsoft Outlook, fare clic sulla freccia giù accanto a **Invia in modo protetto**, quindi fare clic su **Impostazioni**.

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

## Firma e invio di un messaggio e-mail

1. In Microsoft Outlook, fare clic su **Nuovo** o **Rispondi**.
2. Digitare il messaggio e-mail.
3. Fare clic sulla freccia giù accanto a **Invia in modo protetto (Privacy in Outlook 2003)**, quindi fare clic su **Firma e invia**.
4. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

## Crittografia e invio di un messaggio e-mail

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

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


1. In Microsoft Outlook, fare clic su **Nuovo** o **Rispondi**.
2. Digitare il messaggio e-mail.
3. Fare clic sulla freccia giù accanto a **Invia in modo protetto (Privacy in Outlook 2003)**, quindi fare clic su **Crittografa per i contatti attendibili e invia**.
4. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

## Visualizzazione di un messaggio e-mail crittografato

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

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

## Uso di Privacy Manager in un documento di Microsoft Office 2007

 **NOTA:** Privacy Manager può essere utilizzato solo con documenti di Microsoft Office 2007.

Dopo aver installato il certificato di Privacy Manager, sul lato destro della barra degli strumenti di tutti i documenti di Microsoft Word, Microsoft Excel e Microsoft PowerPoint viene visualizzato un pulsante Firma e crittografa. Quando si fa clic sulla freccia giù accanto a **Firma e crittografa**, è possibile scegliere tra le seguenti opzioni:

- Firma documento: questa opzione consente di aggiungere la firma digitale al documento.
- Aggiungi riga firma prima della firma (solo per Microsoft Word e Microsoft Excel): per impostazione predefinita, quando si firma o crittografa un documento di Microsoft Word o Microsoft Excel viene aggiunta una riga della firma. Per disattivare questa opzione, fare clic su **Aggiungi riga firma** per rimuovere il segno di spunta.
- Crittografa documento: questa opzione consente di aggiungere la firma digitale e crittografare il documento.
- Rimuovi crittografia: questa opzione consente di rimuovere la crittografia dal documento.
- Open the Privacy Manager software (Avvia il software Privacy Manager): le opzioni Certificati, Contatti attendibili e Impostazioni consentono di avviare il software Privacy Manager per

aggiungere, visualizzare o modificare le impostazioni correnti. Per ulteriori informazioni, fare riferimento alle sezioni [Gestione dei certificati di Privacy Manager a pagina 42](#), [Gestione di contatti attendibili a pagina 46](#) o [Configurazione di Privacy Manager per Microsoft Office a pagina 51](#).

## Configurazione di Privacy Manager per Microsoft Office

1. Avviare Privacy Manager, fare clic su **Impostazioni**, quindi selezionare la scheda **Documenti**.  
oppure  
Sulla barra degli strumenti di un documento di Microsoft Office, fare clic sulla freccia giù accanto a **Firma e crittografia**, quindi fare clic su **Impostazioni**.
2. Selezionare le azioni che si desidera configurare, quindi fare clic su **OK**.

## Firma di un documento di Microsoft Office

1. In Microsoft Word, Microsoft Excel o Microsoft PowerPoint, creare e salvare un documento.
2. Fare clic sulla freccia giù accanto a **Firma e crittografia**, quindi scegliere **Firma documento**.
3. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
4. Quando viene visualizzata la finestra di dialogo di conferma, leggere il testo, quindi scegliere **OK**.

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


1. Fare clic sul pulsante **Office** nell'angolo superiore sinistro della schermata.
2. Fare clic su **Prepara** quindi su **Contrassegna come finale**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Sì** e continuare a lavorare.
4. Una volta completata la modifica, firmare di nuovo il documento.

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

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

1. In Microsoft Word o Microsoft Excel creare e salvare un documento.
2. Fare clic sul menu **Home**.
3. Fare clic sulla freccia giù accanto a **Firma e crittografia** quindi scegliere **Aggiungi riga firma prima della firma**.

---

 **NOTA:** Viene visualizzato un segno di spunta accanto alla voce **Aggiungi riga firma prima della firma** quando questa opzione è selezionata. Per impostazione predefinita, questa opzione è attivata.

---

4. Fare clic sulla freccia giù accanto a **Firma e crittografia**, quindi scegliere **Firma documento**.
5. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

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

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


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

1. In Microsoft Word o Microsoft Excel, creare e salvare un documento.
2. Fare clic sul menu **Inserisci**.
3. Nel gruppo **Testo** sulla barra degli strumenti, fare clic sulla freccia accanto a **Signature Line** (Riga per la firma) e scegliere **Privacy Manager Signature Provider** (Provider di firme di Privacy Manager).

Viene visualizzata la finestra di dialogo Impostazione firma.

4. Nella casella sotto **Firmatario suggerito**, immettere il nome del firmatario suggerito.
5. Nella casella sotto **Istruzioni per il firmatario**, immettere un messaggio per questo firmatario suggerito.


---

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

---

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

---

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

---

8. Fare clic su **OK**.

## Aggiunta di una riga per la firma dei firmatari suggeriti

Quando i firmatari suggeriti aprono il documento, verrà visualizzato il loro nome tra parentesi, per indicare che è richiesta la firma.

Per firmare il documento:

1. Fare doppio clic sulla riga per la firma appropriata.
2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.

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

## Crittografia di un documento di Microsoft Office

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


Per crittografare un documento di Microsoft Office:

1. In Microsoft Word, Microsoft Excel o Microsoft PowerPoint, creare e salvare un documento.
2. Fare clic sul menu **Home**.
3. Fare clic sulla freccia giù accanto a **Firma e crittografia**, quindi fare clic su **Crittografia documento**.

Viene visualizzata la finestra di dialogo Seleziona contatti attendibili.

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

---

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

---

5. Fare clic su **OK**.

Se in seguito si desidera modificare il documento, seguire i passaggi riportati in [Rimozione della crittografia da un documento di Microsoft Office a pagina 53](#). Quando la crittografia viene rimossa, è possibile modificare il documento. Seguire i passaggi riportati in questa sezione per crittografare di nuovo il documento.

## Rimozione della crittografia da un documento di Microsoft Office

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

Per rimuovere la crittografia da un documento di Microsoft Office:

1. Aprire un documento crittografato di Microsoft Word, Microsoft Excel o Microsoft PowerPoint.
2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.
3. Fare clic sul menu **Home**.
4. Fare clic sulla freccia giù accanto a **Firma e crittografia** quindi fare clic su **Rimuovi crittografia**.

## Invio di un documento crittografato di Microsoft Office


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

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

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

1. In Microsoft Outlook, fare clic su **Nuovo** o **Rispondi**.
2. Digitare il messaggio e-mail.
3. Allegare il documento di Microsoft Office.
4. Per istruzioni dettagliate, fare riferimento alla sezione [Crittografia e invio di un messaggio e-mail a pagina 50](#).

## Visualizzazione di un documento firmato di Microsoft Office

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

Quando si apre un documento firmato di Microsoft Office, viene visualizzata un'icona di firma digitale nella barra di stato al fondo della finestra documento.

1. Fare clic sull'icona **firme digitali** per attivare/disattivare la visualizzazione della finestra di dialogo Firme, che mostra il nome di tutti gli utenti che hanno firmato il documento e la data di ogni firma.
2. Per visualizzare ulteriori informazioni su ogni firma, fare clic con il pulsante destro del mouse nella finestra di dialogo Firme e selezionare Signature Details (Dettagli firma).

## Visualizzazione di un documento crittografato di Microsoft Office

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

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


## Utilizzo di Privacy Manager in Windows Live Messenger

Privacy Manager aggiunge le seguenti funzionalità di comunicazione protetta a Windows Live Messenger:

- **Chat protetta:** i messaggi vengono trasmessi mediante SSL/TLS (Secure Sockets Layer/Transport Layer Security) sul protocollo XML, la stessa tecnologia che garantisce protezione alle transazioni di e-commerce.
- **Identificazione destinatario:** è possibile verificare la presenza e l'identità di una persona prima di inviare un messaggio.
- **Messaggi firmati:** è possibile firmare elettronicamente i messaggi. Quindi, se il messaggio viene alterato, verrà contrassegnato come non valido quando il destinatario lo riceve.
- **Funzione mostra/nascondi:** è possibile nascondere uno o tutti i messaggi nella finestra Privacy Manager Chat. È possibile anche inviare un messaggio il cui contenuto è nascosto. Per visualizzare il messaggio sarà richiesta l'autenticazione.

- **Cronologia chat protetta:** i registri delle sessioni di chat vengono crittografati prima di essere salvati e la relativa visualizzazione è necessaria l'autenticazione.
- **Blocco/sblocco automatico:** è possibile bloccare e sbloccare la finestra di Privacy Manager Chat o impostarla per il blocco automatico dopo un determinato periodo di inattività.

## Avvio di una sessione di Privacy Manager Chat

 **NOTA:** Per poter utilizzare Privacy Manager Chat, entrambe le parti devono disporre di Privacy Manager e di un certificato di Privacy Manager installati nel computer. Per maggiori informazioni sull'installazione di un certificato di Privacy Manager, fare riferimento alla sezione [Richiesta e installazione di un certificato di Privacy Manager a pagina 42](#).


1. Per avviare Privacy Manager Chat in Windows Live Messenger, eseguire una delle seguenti procedure:
  - a. Fare clic con il pulsante destro del mouse su un contatto online in Live Messenger, quindi scegliere **Start an Activity** (Avvia un'attività).
  - b. Fare clic su **Avvia chat**.

oppure

  - a. Fare doppio clic su un contatto online in Live Messenger, quindi fare clic sul menu **See a list of activities** (Vedi elenco di attività).
  - b. Fare clic su **Azione**, quindi su **Avvia chat**.

oppure

  - a. Fare clic con il pulsante destro del mouse sull'icona di ProtectTools nell'area di notifica, fare clic su **Privacy Manager per HP ProtectTools**, quindi selezionare **Avvia chat**.
  - b. In Live Messenger, fare clic su **Azioni: Start an Activity** (Avvia un'attività), quindi selezionare **Privacy Manager Chat**.

 **NOTA:** Ogni utente deve essere online in Live Messenger e gli utenti devono essere visualizzati nella finestra online di Live Messenger degli altri utenti. Fare clic per selezionare un utente online.

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

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

## Configurazione di Privacy Manager per Windows Live Messenger

1. In Privacy Manager Chat, fare clic sul pulsante **Impostazioni**.  
oppure  
In Privacy Manager, fare clic su **Impostazioni**, quindi selezionare la scheda **Chat**.  
oppure  
Nel Visualizzatore cronologia di Privacy Manager, fare clic sul pulsante **Impostazioni**.
2. Per specificare il tempo di attesa di Privacy Manager Chat prima del blocco della sessione, selezionare un numero dalla casella **Blocca sessione dopo \_ minuti di inattività**.
3. Per indicare una cartella per la cronologia delle sessioni di chat, fare clic su **Sfoggia** per cercarla, quindi fare clic su **OK**.
4. Per crittografare e salvare automaticamente le sessioni quando le si chiudono, selezionare la casella di controllo **Salva automaticamente cronologia chat protetta**.
5. Fare clic su **OK**.

## Chat nella finestra di Privacy Manager Chat

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

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



## Visualizzazione della cronologia chat

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

Con il visualizzatore è possibile svolgere le seguenti attività:

- [Rivelazione di tutte le sessioni a pagina 57](#)
- [Rivelazione delle sessioni di un account specifico a pagina 57](#)
- [Visualizzazione di un ID sessione a pagina 58](#)
- [Visualizzazione di una sessione a pagina 58](#)
- [Ricerca di testo specifico nelle sessioni a pagina 58](#)
- [Eliminazione di una sessione a pagina 58](#)
- [Aggiunta o rimozione di colonne a pagina 59](#)
- [Filtro delle sessioni visualizzate a pagina 59](#)

Per avviare il Visualizzatore cronologia di Live Messenger:

- ▲ Nell'area di notifica nella parte destra della barra delle applicazioni, fare clic con il pulsante destro del mouse sull'icona **HP ProtectTools**, quindi selezionare **Privacy Manager: per HP ProtectTools**, quindi fare clic su **Visualizzatore cronologia di Live Messenger**.

oppure

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

### Rivelazione di tutte le sessioni

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

Per rivelare tutte le sessioni di cronologia delle chat salvate:


1. Nel Visualizzatore cronologia di Live Messenger, fare clic con il pulsante del mouse su una sessione qualsiasi e selezionare **Rivela tutte le sessioni**.
2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.  
I nomi dei contatti vengono decrittografati.
3. Fare doppio clic su una sessione per visualizzarne il contenuto.

### Rivelazione delle sessioni di un account specifico

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

Per rivelare una sessione specifica della cronologia chat:

1. Nel Visualizzatore cronologia di Live Messenger, fare clic con il pulsante del mouse su una sessione qualsiasi e selezionare **Rivela sessione**.
2. Autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.  
Il nome del contatto viene decrittografato.
3. Fare doppio clic sulla sessione rivelata per visualizzarne il contenuto.

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

### Visualizzazione di un ID sessione

Per visualizzare un ID sessione:

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

### Visualizzazione di una sessione

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

Per visualizzare una sessione di cronologia di Live Messenger:

1. Nel Visualizzatore cronologia di Live Messenger, fare clic con il pulsante del mouse su una sessione e scegliere **Visualizza**.
2. Se richiesto, autenticarsi utilizzando il metodo di accesso di sicurezza prescelto.  
Il contenuto della sessione viene decrittografato.

### Ricerca di testo specifico nelle sessioni

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

Per cercare un testo nelle sessioni di cronologia chat:

1. Nel Visualizzatore cronologia di Live Messenger, fare clic sul pulsante **Cerca**.
2. Immettere il testo da cercare, configurare eventuali parametri di ricerca desiderati, infine scegliere **OK**.

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

### Eliminazione di una sessione

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

## Aggiunta o rimozione di colonne

Per impostazione predefinita, nel Visualizzatore cronologia di Live Messenger vengono visualizzate le 3 colonne più utilizzate. È possibile aggiungere o rimuovere colonne dalla visualizzazione.

Per aggiungere colonne alla visualizzazione:

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

Per rimuovere colonne dalla visualizzazione:

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

## Filtro delle sessioni visualizzate

Nel Visualizzatore cronologia di Live Messenger viene riportato un elenco delle sessioni di tutti gli account. È possibile filtrare le sessioni visualizzate in base a:

- Account specifici. Per istruzioni dettagliate, fare riferimento alla sezione [Visualizzazione delle sessioni di un account specifico a pagina 59](#).
- Intervallo di date. Per istruzioni dettagliate, fare riferimento alla sezione [Visualizzazione delle sessioni per un intervallo di date a pagina 59](#).
- Cartelle diverse. Per istruzioni dettagliate, fare riferimento alla sezione [Visualizzazione delle sessioni salvate in una cartella diversa da quella predefinita a pagina 59](#).

## Visualizzazione delle sessioni di un account specifico

- ▲ Nel Visualizzatore cronologia di Live Messenger, selezionare un account dal menu **Visualizza cronologia per:**.

## Visualizzazione delle sessioni per un intervallo di date

1. Nel Visualizzatore cronologia di Live Messenger, fare clic sull'icona **Filtro avanzato**.  
Viene visualizzata la finestra di dialogo Filtro avanzato.
2. Selezionare la casella di controllo **Visualizza solo sessioni entro un intervallo data specificato**.
3. Nelle caselle **Data inizio:** e **Data fine:**, immettere giorno, mese e/o anno oppure fare clic sulla freccia accanto al calendario per selezionare le date.
4. Fare clic su **OK**.

## Visualizzazione delle sessioni salvate in una cartella diversa da quella predefinita

1. Nel Visualizzatore cronologia di Live Messenger, fare clic sull'icona **Filtro avanzato**.
2. Selezionare la casella di controllo **Utilizzare una cartella diversa per i file della cronologia**.

3. Immettere il percorso della cartella o scegliere **Sfoglia** per cercare una cartella.
4. Fare clic su **OK**.

## Attività avanzate


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

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

#### Backup dei certificati di Privacy Manager e dei contatti attendibili

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

1. Avviare Privacy Manager e fare clic su **Migrazione**.
2. Fare clic su **Backup**.
3. Nella pagina "Selezione dati", selezionare le categorie di dati da inserire nel file di migrazione, quindi fare clic su **Avanti**.
4. Nella pagina "File di migrazione", immettere un nome file o fare clic su **Sfoglia** per cercare un percorso, quindi fare clic su **Avanti**.
5. Immettere e confermare una password, quindi fare clic su **Avanti**.

 **NOTA:** Memorizzare questa password in un posto sicuro, poiché servirà per ripristinare il file di migrazione.

---

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

#### Ripristino dei certificati di Privacy Manager e dei contatti attendibili

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

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

## Amministrazione centralizzata di Privacy Manager

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


- **Criteri di utilizzo dei certificati** - È possibile che venga autorizzato solo l'uso di certificati di Privacy Manager emessi da Comodo o di certificati digitali emessi da diverse autorità di certificazione.
- **Criterio di crittografia** - La crittografia può essere attivata o disattivata in Microsoft Office o Outlook e in Windows Live Messenger.

---

## 9 File Sanitizer per HP ProtectTools

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

---

 **NOTA:** Questa versione di File Sanitizer supporta solo l'unità disco rigido di sistema.

---


# Distruzione

La distruzione è diversa dall'eliminazione standard di Windows®, nota anche come eliminazione semplice in File Sanitizer, poiché quando una risorsa viene distrutta utilizzando File Sanitizer, viene richiamato un algoritmo che nasconde i dati, rendendo impossibile recuperare la risorsa originale. L'eliminazione semplice di Windows potrebbe lasciare intatto il file o la risorsa nell'unità disco rigido oppure lasciare il file o la risorsa in uno stato recuperabile con metodi forensi.

Quando si sceglie un profilo di distruzione, ovvero protezione alta, media o bassa, vengono selezionati automaticamente un elenco predefinito di risorse e un metodo di cancellazione per la distruzione. È inoltre possibile personalizzare un profilo di distruzione, consentendo all'utente di specificare il numero di cicli di distruzione, quali risorse includere nella distruzione, quali risorse confermare prima della distruzione e quali risorse escludere dalla distruzione. Per ulteriori informazioni, fare riferimento alla sezione [Selezione o creazione di un profilo di distruzione a pagina 66](#).

È possibile programmare la distruzione automatica oppure distruggere manualmente le risorse quando desiderato. Per ulteriori informazioni, fare riferimento alla sezione [Impostazione di un programma di distruzione a pagina 65](#), [Distruzione manuale di una risorsa a pagina 70](#) o [Distruzione manuale di tutti gli elementi selezionati a pagina 71](#).

---

 **NOTA:** Un file con estensione dll può essere considerato distrutto e rimosso dal sistema solo se è stato spostato nel cestino.


---

## Pulizia dello spazio libero

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

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

---

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

---

È possibile programmare la pulitura automatica dello spazio libero oppure attivarla manualmente utilizzando l'icona **HP ProtectTools** nell'area di notifica all'estrema destra della barra delle applicazioni. Per ulteriori informazioni, fare riferimento alla sezione [Impostazione di un programma di pulizia dello spazio libero a pagina 66](#) o [Attivazione manuale della pulizia dello spazio libero a pagina 71](#).



# Procedure di configurazione

## Avvio di File Sanitizer

Per avviare File Sanitizer:

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


oppure

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


oppure


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

## Impostazione di un programma di distruzione

 **NOTA:** Per informazioni sulla selezione di un profilo di distruzione predefinito o la creazione di un profilo di distruzione, fare riferimento alla sezione [Selezione o creazione di un profilo di distruzione a pagina 66](#).


**NOTA:** Per informazioni sulla distruzione manuale delle risorse, fare riferimento alla sezione [Distruzione manuale di una risorsa a pagina 70](#).

1. Avviare File Sanitizer e fare clic su **Distuggi**.
2. Selezionare un'opzione di distruzione:
  - **Arresto di Windows** - Scegliere questa opzione per distruggere tutte le risorse selezionate all'arresto di Windows.
  -  **NOTA:** Quando è selezionata questa opzione, viene visualizzata una finestra di dialogo al momento dell'arresto in cui viene chiesto se si desidera continuare con la distruzione delle risorse selezionate o se invece si desidera ignorare la procedura. Fare clic su **Si** per ignorare la procedura di distruzione oppure su **No** per continuare l'operazione di distruzione.
  - **Apertura browser** - Scegliere questa opzione per distruggere tutte le risorse correlate al Web, ad esempio la cronologia degli URL, al momento dell'apertura del browser.
  - **Chiusura browser** - Scegliere questa opzione per distruggere tutte le risorse correlate al Web, ad esempio la cronologia degli URL, al momento della chiusura del browser.
  - **Sequenza di tasti** - Scegliere questa opzione per avviare la distruzione mediante una sequenza di tasti.
  - **Programmazione** - Selezionare la casella di controllo **Attiva programmazione**, immettere la password di Windows, quindi immettere un giorno e un'ora per la distruzione delle risorse selezionate.

 **NOTA:** Un file con estensione dll può essere considerato distrutto e rimosso dal sistema solo se è stato spostato nel cestino.

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


## Impostazione di un programma di pulizia dello spazio libero

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

---

Per impostare un programma di pulizia dello spazio libero.

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

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

---

## Selezione o creazione di un profilo di distruzione

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

### Selezione di un profilo di distruzione predefinito

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

Per selezionare un profilo di distruzione predefinito:


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

## Personalizzazione di un profilo di distruzione

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

1. Avviare File Sanitizer e scegliere **Impostazioni**, fare clic su **Impostazioni di sicurezza avanzate**, quindi scegliere **Visualizza dettagli**.
2. Specificare il numero di cicli di distruzione.


---

 **NOTA:** Per ogni risorsa verrà eseguito il numero di cicli di distruzione selezionato. Ad esempio, se si scelgono 3 cicli di distruzione, l'algoritmo che nasconde i dati verrà eseguito 3 volte. Se si sceglie di eseguire il numero più elevato di cicli di distruzione di protezione, le operazioni di distruzione potrebbero richiedere parecchio tempo. Tuttavia, maggiore è il numero di cicli di distruzione specificato, minori sono le probabilità che i dati possano venire recuperati.

---

3. Selezionare le risorse che si desidera distruggere:
  - a. In **Opzioni di distruzione disponibili**, fare clic su una risorsa, quindi scegliere **Aggiungi**.
  - b. Per aggiungere una risorsa personalizzata, fare clic su **Aggiungi opzione personalizzata**, quindi cercare o immettere il percorso del file o della cartella. Fare clic su **Apri**, quindi su **OK**. In **Opzioni di distruzione disponibili**, fare clic sulla risorsa personalizzata, quindi scegliere **Aggiungi**.


---

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

---

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


---

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

---

5. Per proteggere i file o le cartelle dalla distruzione automatica, fare clic su **Aggiungi in Non distruggere seguenti**, quindi cercare o immettere il percorso del file o della cartella. Fare clic su **Apri**, quindi su **OK**.

---

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


---

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

## Personalizzazione di un profilo di eliminazione semplice




L'utilizzo del profilo di eliminazione semplice determina l'eliminazione standard di una risorsa ma non la sua distruzione. Quando si personalizza un profilo di eliminazione semplice, è possibile specificare quali risorse includere nell'eliminazione semplice, quali risorse confermare prima dell'esecuzione di un'operazione di eliminazione semplice e quali risorse escludere dall'eliminazione semplice.

---

 **NOTA:** Se si utilizza l'opzione di eliminazione semplice, è possibile eseguire occasionalmente la pulizia dello spazio libero delle risorse che sono state eliminate manualmente o utilizzando il Cestino di Windows.

---

Per personalizzare un profilo di eliminazione semplice:


1. Avviare File Sanitizer, fare clic su **Impostazioni**, scegliere **Impostazioni di eliminazione semplice**, quindi fare clic su **Visualizza dettagli**.
  2. Selezionare le risorse che si desidera eliminare:
    - a. In **Opzioni di eliminazione disponibili**, fare clic sulla risorsa, quindi scegliere **Aggiungi**.
    - b. Per aggiungere una risorsa personalizzata, fare clic su **Aggiungi opzione personalizzata**, immettere il nome del file o della cartella, quindi scegliere **OK**. Fare clic sulla risorsa personalizzata, quindi scegliere **Aggiungi**.
- 
-  **NOTA:** Per eliminare una risorsa dalle opzioni di eliminazione disponibili, fare clic sulla risorsa, quindi scegliere **Elimina**.
- 
3. In **Elimina seguenti**, selezionare la casella di controllo accanto a ciascuna risorsa che si desidera confermare prima dell'eliminazione.
- 
-  **NOTA:** Per rimuovere una risorsa dall'elenco di eliminazione, fare clic sulla risorsa, quindi scegliere **Rimuovi**.
- 
4. In **Non eliminare seguenti**, fare clic su **Aggiungi** per selezionare le risorse specifiche che si desidera escludere dalla distruzione.
- 
-  **NOTA:** Per rimuovere una risorsa dall'elenco delle esclusioni, fare clic sulla risorsa, quindi scegliere **Elimina**.
- 
5. Al termine della configurazione del profilo di eliminazione semplice, fare clic su **Applica**, quindi scegliere **OK**.

## Attività generali

È possibile utilizzare File Sanitizer per eseguire le seguenti attività:

- Utilizzare una sequenza di tasti per avviare la distruzione: questa funzione consente di creare una sequenza di tasti (ad esempio, [ctrl+alt+s](#)) per attivare la distruzione. Per istruzioni dettagliate, fare riferimento alla sezione [Uso di una sequenza di tasti per avviare la distruzione a pagina 69](#).
- Utilizzare l'icona di File Sanitizer per avviare la distruzione: questa funzione è simile alla funzione di trascinamento della selezione in Windows. Per istruzioni dettagliate, fare riferimento alla sezione [Uso dell'icona File Sanitizer a pagina 70](#).
- Distruggere manualmente una risorsa specifica o tutte le risorse selezionate: queste funzioni consentono di distruggere manualmente degli elementi senza aspettare che venga richiamato il regolare programma di distruzione. Per istruzioni dettagliate, fare riferimento alla sezione [Distruzione manuale di una risorsa a pagina 70](#) o [Distruzione manuale di tutti gli elementi selezionati a pagina 71](#).
- Attivare manualmente la pulizia dello spazio libero: questa funzione consente di attivare manualmente la pulizia dello spazio libero. Per istruzioni dettagliate, fare riferimento alla sezione [Attivazione manuale della pulizia dello spazio libero a pagina 71](#).
- Interrompere l'operazione di distruzione o l'operazione di pulizia dello spazio libero: questa funzione consente di interrompere l'operazione di distruzione o quella di pulizia dello spazio libero. Per istruzioni dettagliate, fare riferimento alla sezione [Interruzione di un'operazione di distruzione o di pulizia dello spazio libero a pagina 71](#).
- Visualizzare i file di registro: questa funzione consente di visualizzare i file di registro di distruzione e di pulizia dello spazio libero, che contengono eventuali errori verificatisi dall'ultima operazione di distruzione o di pulizia dello spazio libero. Per istruzioni dettagliate, fare riferimento alla sezione [Visualizzazione dei file di registro a pagina 71](#).

---

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

---


## Uso di una sequenza di tasti per avviare la distruzione

Per specificare una sequenza di tasti, procedere come segue:

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

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

---

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

---

Per avviare la distruzione mediante una sequenza di tasti:

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

## Uso dell'icona File Sanitizer


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

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

## Distruzione manuale di una risorsa

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

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

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

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

oppure

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

oppure

1. Avviare File Sanitizer e fare clic su **Distruggi**.
2. Fare clic sul pulsante **Sfoglia**.
3. Quando viene visualizzata la finestra di dialogo Sfoglia, spostarsi sulla risorsa che si desidera distruggere, quindi scegliere **OK**.
4. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

## Distruzione manuale di tutti gli elementi selezionati

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

oppure

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

oppure

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

## Attivazione manuale della pulizia dello spazio libero

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

oppure

1. Avviare File Sanitizer e fare clic su **Pulizia dello spazio libero**.
2. Fare clic su **Pulisci ora**.
3. Quando viene visualizzata la finestra di dialogo di conferma, fare clic su **Si**.

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

Durante un'operazione di distruzione o di pulizia dello spazio libero, viene visualizzato un messaggio sull'icona di HP ProtectTools Security Manager nell'area di notifica. Il messaggio fornisce informazioni sul processo di distruzione o di pulizia dello spazio libero (percentuale completata) e consente di interrompere l'operazione.


Per interrompere l'operazione:

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

## Visualizzazione dei file di registro

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

---

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

Viene creato un file registro per le operazioni di distruzione e un altro file registro per le operazioni di pulizia dello spazio libero. Entrambi i file registro si trovano nell'unità disco rigido nel percorso:

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



---

## 10 Device Access Manager per HP ProtectTools (solo in determinati modelli)

Gli amministratori del sistema operativo Windows® utilizzano Device Access Manager per HP ProtectTools 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.
- Gli utenti vengono inoltre organizzati in gruppi, ad esempio gli amministratori predefiniti oppure gruppi possono essere definiti mediante l'opzione Gestione Computer della sezione Strumenti di amministrazione del Pannello di controllo.
- L'accesso alle periferiche può essere concesso o negato in base all'appartenenza al gruppo.
- Per classi di periferiche quali unità CD-ROM e DVD, l'accesso in lettura e scrittura può essere concesso o negato separatamente.

Un numero limitato di utenti può inoltre ottenere l'autorizzazione a leggere e modificare i criteri che controllano l'accesso alle periferiche.

# Procedure di installazione

## Apertura di Device Access Manager

Per aprire a Device Access Manager, procedere come segue:

1. Fare clic su **Start, Tutti i programmi**, su **HP** e infine su **HP ProtectTools Administrative Console**.
2. Nel riquadro a sinistra, fare clic su **Device Access Manager**.

## Configurazione dell'accesso alle periferiche


Device Access Manager per HP ProtectTools offre tre viste:

- La vista Configurazione semplice consente di concedere o negare l'accesso alle classi di periferiche per i membri del gruppo Amministratori dispositivi.
- La vista Configurazione delle classi di periferiche consente di concedere o negare l'accesso ai tipi di periferiche o a periferiche specifiche per gruppi o utenti specifici.
- La vista Impostazioni di accesso utente consente di specificare quali utenti possono visualizzare o modificare le informazioni in Configurazione semplice e Configurazione delle classi di periferiche.

## Gruppo amministratori periferica

Quando è installato Device Access Manager, viene creato un gruppo Amministratori periferica.

L'amministratore del sistema può implementare un semplice criterio di controllo di accesso alla periferica negando l'accesso a un set di classi di periferiche a meno che l'utente non sia classificato come attendibile (relativamente all'accesso alla periferica). Il modo consigliato per distinguere tra utenti "attendibili per le periferiche" e "non attendibili per le periferiche" è rendere tutti gli utenti "attendibili per le periferiche" membri del gruppo amministratori periferica. La concessione ai membri del gruppo amministratori periferica dell'accesso alle periferiche mediante le viste Configurazione semplice o Configurazione classe di periferica assicura che gli utenti "affidabili per le periferiche" avranno accesso completo al set specificato di classi di periferiche.

 **NOTA:** L'aggiunta di un utente al gruppo amministratori periferica non consente l'accesso automatico alle periferiche. È tuttavia possibile utilizzare la vista Configurazione semplice per concedere l'accesso al set richiesto di classi di periferiche per gli utenti "attendibili".

Per aggiungere utenti al gruppo amministratori periferica, seguire la procedura indicata:


- Per Windows 7, Vista o XP Professional, utilizzare lo snap-in MMC standard "Utenti e gruppi locali" MMC.
- Per le versioni home di Windows 7, Vista® o XP, da un account privilegiato, digitare il comando seguente nel prompt della riga di comando:

```
c:\> net localgroup "Amministratori periferica" nomeutente /ADD
```

## Configurazione semplice

Amministratori e utenti autorizzati possono utilizzare la vista Configurazione semplice per modificare l'accesso alle seguenti classi di periferiche per tutti i non amministratori periferica:

---

 **NOTA:** Per utilizzare questa vista per la lettura delle informazioni di accesso alla periferica, è necessario concedere a un utente o a un gruppo accesso in "lettura" nella vista **Impostazioni di accesso utente**. Per utilizzare questa vista per la modifica delle informazioni di accesso alla periferica, è necessario concedere a un utente o a un gruppo accesso in "modifica" nella vista **Impostazioni di accesso utente**.

---

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


Per negare l'accesso a una classe di periferiche per tutti i non amministratori periferiche:

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

Se questa casella è disattivata, i valori associati allo scenario di accesso sono stati modificati dalla vista Configurazione delle classi di periferiche. Per ripristinare i valori alle impostazioni semplici, fare clic sulla casella di controllo per attivarla o disattivarla, quindi fare clic su **Sì** per confermare.

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

---

 **NOTA:** Se il servizio in background non è in esecuzione, si apre una finestra di dialogo che ne chiede l'avvio. Fare clic su **Sì**.


---

4. Fare clic su **OK**.

### Avvio del servizio in background

Prima di poter applicare i profili, HP ProtectTools Security Manager apre una finestra di dialogo che chiede se si desidera avviare il servizio in background HP ProtectTools Device Locking/Auditing. Fare clic su **Sì**. Il servizio in background si avvia e si avvierà automaticamente a ogni avvio del sistema.

---

 **NOTA:** Prima della visualizzazione del prompt del servizio in background, è necessario definire un profilo della periferica.

---

Anche gli amministratori possono avviare o arrestare questo servizio:

1. Facendo clic su **Start**, quindi su **Pannello di controllo**.
2. Fare clic su **Strumenti di amministrazione**, quindi su **Servizi**.
3. Cercare il servizio **HP ProtectTools Device Locking/Auditing**.

L'arresto del servizio di audit/blocco dispositivi non determina il blocco della periferica. Due componenti determinano il blocco della periferica:

- Servizio audit/blocco periferica
- Driver DAMDrv.sys

Avviando il servizio si avvia il driver della periferica, ma l'arresto del servizio non arresta il driver.


Per stabilire se il servizio in background è in esecuzione, aprire la riga del prompt di comandi e digitare `sc query f1cdlock`.

Per stabilire se il driver della periferica è in esecuzione, aprire la riga del prompt di comandi e digitare `sc query damdrv`.

## Configurazione delle classi di periferiche

Gli amministratori e gli utenti autorizzati possono visualizzare e modificare elenchi di utenti e gruppi a cui è consentito o negato accedere a classi di periferiche o a periferiche specifiche.

---

 **NOTA:** Per utilizzare questa vista per la lettura delle informazioni di accesso alla periferica, è necessario concedere a un utente o a un gruppo accesso in "lettura" nella vista **Impostazioni di accesso utente**. Per utilizzare questa vista per la modifica delle informazioni di accesso alla periferica, è necessario concedere a un utente o a un gruppo accesso in "modifica" nella vista **Impostazioni di accesso utente**.


---

Nella vista Configurazione delle classi di periferiche sono presenti le sezioni seguenti:

- **Elenco periferiche:** mostra tutte le classi di periferiche e le periferiche installate nel sistema o che possono essere state installate in precedenza.
  - La protezione viene in genere applicata per una classe di periferiche. Un utente o gruppo selezionato sarà in grado di accedere a qualsiasi periferica nella classe.
  - La protezione può anche essere applicata a periferiche specifiche.
- **Elenco utenti:** mostra tutti gli utenti e i gruppi a cui è consentito o negato accedere alla classe di periferica selezionata o alla periferica specifica.
  - La voce in Elenco utenti può essere associata a un utente specifico o a un gruppo a cui questo utente appartiene.
  - Quando una voce di gruppo o utente presente in Elenco utenti non è disponibile, la sua impostazione è stata ereditata dalla classe del dispositivo in Elenco periferiche o dalla stessa cartella Classe.
  - Alcune classi di periferiche, come DVD e CD-ROM, possono essere ulteriormente controllate concedendo o negando l'accesso separatamente per le operazioni di lettura e scrittura.

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

---

 **NOTA:** Se la casella di selezione Lettura è vuota, la voce di controllo di accesso non ha effetto sull'accesso in lettura alla periferica. Non concede né nega neppure l'accesso in lettura alla periferica.

---

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

Allo stesso utente, gruppo o membro dello stesso gruppo può essere concesso l'accesso in scrittura o in lettura e scrittura a una periferica di livello inferiore nella gerarchia delle periferiche.

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

Allo stesso utente, gruppo o membro dello stesso gruppo può essere negato l'accesso in scrittura o in lettura e scrittura solo per la stessa periferica o la periferica di livello inferiore nella gerarchia delle periferiche.

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

Allo stesso utente, gruppo o membro dello stesso gruppo può essere negato l'accesso in lettura o in lettura e scrittura solo per la stessa periferica o la periferica di livello inferiore nella gerarchia delle periferiche.

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

Allo stesso utente, gruppo o membro dello stesso gruppo può essere concesso accesso in lettura o in lettura e scrittura a una periferica di livello inferiore nella gerarchia delle periferiche.

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

Allo stesso utente, gruppo o membro dello stesso gruppo può essere negato l'accesso in scrittura o in lettura e scrittura solo per la stessa periferica o la periferica di livello inferiore nella gerarchia delle periferiche.

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


Allo stesso utente, gruppo o membro dello stesso gruppo può essere concesso accesso in lettura o in lettura e scrittura a una periferica di livello inferiore nella gerarchia delle periferiche.

## Negazione dell'accesso a un utente o gruppo

Per impedire a un utente o gruppo di accedere a una periferica o una classe di periferiche, seguire queste indicazioni:

1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Configurazione delle classi di periferiche**.
2. Nell'elenco di periferiche, fare clic sulla classe da configurare.
  - Classe periferica
  - Tutte le periferiche
  - Singola periferica
3. In **Utente/Gruppi**, fare clic sull'utente o gruppo per cui negare l'accesso.
4. Fare clic su **Nega** vicino a un utente o gruppo.
5. Fare clic sull'icona **Salva**.

---

 **NOTA:** Dopo aver configurato le impostazioni di negazione e concessione per lo stesso livello di periferica per un utente, la negazione dell'accesso è prioritaria sulla concessione.

---

### Concessione dell'accesso per un utente o gruppo

Per concedere a un utente o gruppo l'autorizzazione ad accedere a una periferica o una classe di periferiche, seguire queste indicazioni:

1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Configurazione delle classi di periferiche**.
2. Nell'elenco periferiche, fare clic su una delle opzioni seguenti:
  - Classe periferica
  - Tutte le periferiche
  - Singola periferica
3. Fare clic su **Aggiungi**.  
Viene visualizzata la finestra di dialogo **Select Users or Groups** (Seleziona utenti o gruppi).
4. Fare clic su **Avanzate**, quindi su **Find Now (Trova ora)** per cercare utenti o gruppi da aggiungere.
5. Fare clic su un utente o gruppo da aggiungere all'elenco di utenti e gruppi disponibili, quindi su **OK**.
6. Fare di nuovo clic su **OK**.
7. Fare clic su **Consenti** per concedere l'accesso a questo utente o gruppo.
8. Fare clic sull'icona **Salva**.

### Rimozione dell'accesso per un utente o gruppo

Per rimuovere da un utente o gruppo l'autorizzazione ad accedere a una periferica o una classe di periferiche, seguire queste indicazioni:

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

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

Per consentire a un utente di accedere a una classe di periferiche, negando contemporaneamente l'accesso a tutti gli altri membri del suo gruppo, seguire la procedura indicata:

1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Configurazione delle classi di periferiche**.
2. Nell'elenco di periferiche, fare clic sulla classe da configurare.
  - Classe periferica
  - Tutte le periferiche
  - Singola periferica
3. In **Utente/Gruppi**, selezionare il gruppo a cui negare l'accesso, quindi fare clic su **Nega**.
4. Selezionare la cartella di livello inferiore rispetto a quella della classe richiesta, e aggiungere l'utente specifico.
5. Fare clic su **Consenti** per concedere l'accesso a questo utente.
6. Fare clic sull'icona **Salva**.

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

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

1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Configurazione delle classi di periferiche**.
2. Nell'elenco periferiche, fare clic sulla classe da configurare, quindi selezionare la cartella di livello inferiore.
3. Fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo **Select Users or Groups** (Seleziona utenti o gruppi).
4. Fare clic su **Avanzate**, quindi su **Find Now** (Trova ora) per cercare il gruppo dell'utente a cui verrà negato l'accesso a tutte le periferiche nella classe.
5. Fare clic sul gruppo, quindi su **OK**.
6. Selezionare la periferica specifica nella classe a cui l'accesso deve essere consentito all'utente.
7. Fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo **Select Users or Groups** (Seleziona utenti o gruppi).
8. Fare clic su **Avanzate**, quindi su **Find Now (Trova ora)** per cercare utenti o gruppi da aggiungere.
9. Fare clic sull'utente a cui concedere l'accesso, quindi su **OK**.
10. Fare clic su **Consenti** per concedere l'accesso a questo utente.
11. Fare clic sull'icona **Salva**.

## Ripristino della configurazione

△ **ATTENZIONE:** Con il ripristino della configurazione si eliminano tutte le modifiche apportate e ripristinano i valori predefiniti.

---

Per ripristinare le impostazioni predefinite della configurazione, seguire la procedura indicata:


1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Configurazione delle classi di periferiche**.
2. Selezionare il pulsante **Reset**.
3. Fare clic su **Sì** per confermare.
4. Fare clic sull'icona **Salva**.




# Attività avanzate

## Controllo dell'accesso alle impostazioni di configurazione

Nella vista **Impostazioni di accesso utente**, gli amministratori specificano i gruppi o gli utenti a cui è consentito utilizzare le pagine Configurazione semplice e Configurazione delle classi di periferiche.

 **NOTA:** Per modificare le impostazioni nella vista Impostazioni di accesso utente, è necessario concedere a un utente o a un gruppo "diritti di amministratore completi".

- Per visualizzare le informazioni relative a Configurazione semplice e Configurazione delle classi di periferiche, è necessario concedere a un utente o a un gruppo accesso "Visualizza (sola lettura) impostazioni di configurazione" nella vista Impostazioni di accesso utente.
- Per modificare le informazioni relative a Configurazione semplice e Configurazione delle classi di periferiche, è necessario concedere a un utente o a un gruppo accesso "Cambia impostazioni di configurazione" nella vista Impostazioni di accesso utente.


 **NOTA:** Tuttavia, anche ai membri del gruppo Amministratori deve essere concesso accesso in "lettura" per visualizzare le viste Configurazione semplice e Configurazione delle classi di periferiche e accesso in "modifica" per modificare i dati tramite le viste Configurazione semplice e Configurazione delle classi di periferiche.

**NOTA:** Dopo aver valutato i livelli di accesso per tutti gli utenti e gruppi, se per utente non è selezionato Consenti o Nega per un particolare livello di accesso, all'utente viene negato l'accesso a tale livello.

## Concessione dell'accesso a un utente o gruppo esistente

Per concedere l'autorizzazione a un utente o gruppo esistente a visualizzare o modificare le impostazioni di configurazione, seguire la procedura indicata:

1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Impostazioni di accesso utente**.
2. Fare clic su un utente o gruppo a cui concedere l'accesso.
3. In **Autorizzazioni**, fare clic su **Consenti** per ogni tipo di autorizzazione da concedere all'utente o gruppo selezionato:

 **NOTA:** Le autorizzazioni concesse sono cumulative. Ad esempio, a un utente a cui è concessa l'autorizzazione "Cambia impostazioni di configurazione", viene automaticamente concessa anche "Visualizza (sola lettura) impostazioni di configurazione". A un utente a cui è concessa l'autorizzazione "Diritti amministratore utente completi" vengono concesse "Cambia impostazioni di configurazione" e "Visualizza (sola lettura) impostazioni di configurazione".

- Diritti amministratore utente completi
  - Cambia impostazioni di configurazione
  - Visualizza (sola lettura) impostazioni di configurazione
4. Fare clic sull'icona **Salva**.

## Negazione dell'accesso a un utente o gruppo esistente

Per negare l'autorizzazione a un utente o gruppo esistente a visualizzare o modificare le impostazioni di configurazione, seguire la procedura indicata:

1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Impostazioni di accesso utente**.
2. Fare clic su un utente o gruppo a cui negare l'accesso.
3. In **Autorizzazioni**, fare clic su **Nega** per ogni tipo di autorizzazione da negare all'utente o gruppo selezionato:
  - Diritti amministratore utente completi
  - Cambia impostazioni di configurazione
  - Visualizza (sola lettura) impostazioni di configurazione
4. Fare clic sull'icona **Salva**.

## Aggiunta di un nuovo gruppo o utente

Per concedere l'autorizzazione a un nuovo utente o gruppo a visualizzare o modificare le impostazioni di configurazione, seguire la procedura indicata:

1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Impostazioni di accesso utente**.
2. Fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo **Select Users or Groups** (Seleziona utenti o gruppi).
3. Fare clic su **Avanzate**, quindi su **Find Now (Trova ora)** per cercare utenti o gruppi da aggiungere.
4. Fare clic su un gruppo o un utente, su **OK**, quindi di nuovo su **OK**.
5. Fare clic su **Consenti** per concedere l'accesso a questo utente.
6. Fare clic sull'icona **Salva**.

## Rimozione dell'accesso a un gruppo o utente

Per rimuovere l'autorizzazione a un utente o gruppo a visualizzare o modificare le impostazioni di configurazione, seguire la procedura indicata:

1. Nel riquadro di sinistra di **HP ProtectTools Administrative Console**, fare clic su **Device Access Manager**, quindi su **Impostazioni di accesso utente**.
2. Selezionare un gruppo o utente, quindi fare clic su **Rimuovi**.
3. Fare clic sull'icona **Salva**.

## Documentazione correlata

Device Access Manager per HP ProtectTools è compatibile con il prodotto aziendale HP ProtectTools Enterprise Device Access Manager. Quando si lavora con il prodotto aziendale, Device Access Manager per HP ProtectTools consente solo accesso in lettura alle proprie funzionalità.

Ulteriori informazioni su Device Access Manager per HP ProtectTools sono disponibili sul Web all'indirizzo <http://www.hp.com/hps/security/products>.

---


# 11 LoJack Pro for HP ProtectTools

Computrace LoJack Pro, di Absolute Software (da acquistare separatamente), risolve il problema crescente dei computer persi o rubati.

Attivando questo software si abilita l'agente Computrace, che rimane attivo nel computer anche se il disco rigido viene riformattato o sostituito.

LoJack Pro consente controllo, gestione e tracciatura remoti del computer. Se il computer corre il rischio di furto o perdita, il team Recovery di Absolute aiuterà nel ripristino.\*

---

 **NOTA:** \*Questa funzionalità dipende dalla posizione geografica. Per ulteriori informazioni, consultare l'accordo di sottoscrizione di Absolute Software.

---

# 12 Risoluzione dei problemi

## HP ProtectTools Security Manager

Breve descrizione	Dettagli	Soluzione
Smart card e token USB non sono disponibili in Security Manager se installati dopo l'installazione di Security Manager.	<p>Per utilizzare smart card o token USB in Security Manager, il software di supporto (driver, provider PKCS#1, e così via) deve essere installato prima di installare Security Manager.</p> <p>Se Security Manager è già installato, seguire questa procedura dopo l'installazione del software di supporto di smart card o token:</p>	<p>Accedere a Password Manager.</p> <p>In HP ProtectTools Security Manager, fare clic su <b>Password Manager, Credenziali</b>, quindi su <b>Smart Card</b></p> <p>Riavviare il computer, se richiesto.</p>
Le pagine Web di alcune applicazioni creano errori che impediscono agli utenti di eseguire o completare le attività.	Alcune applicazioni Web cessano di funzionare e producono errori a causa dello schema di disabilitazione di Single Sign On. Ad esempio, in Internet Explorer verrà visualizzato un ! racchiuso in un triangolo giallo a indicare la presenza di un errore.	<p>Security Manager Single Sign On non supporta tutte le interfacce Web software. Disattivare il supporto Single Sign On per la pagina Web specifica disattivando il supporto Single Sign On. Consultare la documentazione completa di Single Sign On, disponibile nei file della guida di Security Manager.</p> <p>Se non fosse possibile disabilitare uno specifico Single Sign per una determinata applicazione, chiamare il servizio di assistenza tecnica di HP e richiedere, tramite il proprio contatto, un intervento di assistenza di terzo livello.</p>
L'opzione <b>Browse for Virtual Token</b> (Cerca token virtuale) non viene visualizzata durante il processo di connessione.	L'utente non può spostare la posizione di un token virtuale registrato in Password Manager in quanto l'opzione per la selezione è stata rimossa per ridurre i rischi di protezione.	Tale opzione consentiva ai non utenti di eliminare e rinominare i file e di assumere il controllo di Windows.
L'amministratore di dominio non può modificare la password di Windows anche con l'autorizzazione.	Questa situazione si verifica dopo l'accesso di un amministratore di dominio a un dominio e la successiva registrazione dell'identità di dominio con Password Manager tramite un account con diritti di amministratore sul dominio e il computer locale. Quando l'amministratore di dominio cerca di modificare la password di Windows da Password Manager, l'amministratore ottiene un errore di accesso: <b>Limitazione account utente.</b>	Password Manager non è in grado di modificare una password di account utente di dominio tramite <b>Change Windows password</b> (Cambia password di Windows). Security Manager è solo in grado di modificare le password account del computer. L'utente di dominio può modificare la propria password tramite l'opzione <b>Cambia password di Protezione di Windows</b> , ma poiché l'utente di dominio non dispone di account fisico sul computer locale, Password Manager può solo modificare la password utilizzata per l'accesso.
Password Manager ha problemi di incompatibilità con Corel WordPerfect 12 password GINA.	Se l'utente accede a Password Manager, crea un documento WordPerfect e salva con protezione tramite password, Password Manager non è in grado di	HP sta cercando una soluzione per migliorare il prodotto nel futuro.

Breve descrizione	Dettagli	Soluzione
	rilevare o riconoscere, manualmente o automaticamente, la password GINA.	
Password Manager non riconosce il pulsante <b>Connect</b> (Connetti) sullo schermo.	Se le credenziali Single Sign On per Remote Desktop Connection (RDP) sono impostate su <b>Connect</b> (Connetti), quando Single Sign On viene riavviato, immette sempre <b>Save As</b> (Salva con nome) al posto di <b>Connect</b> (Connetti).	HP sta cercando una soluzione per migliorare il prodotto nel futuro.
L'utente non è in grado di accedere a Password Manager dopo il passaggio dal modo di standby alla sospensione solo in Windows XP Service Pack 1.	Dopo aver consentito al sistema di passare nel modo sospensione e standby, l'amministratore o l'utente non può accedere a Password Manager e la schermata di accesso a Windows resta visualizzata indipendentemente dalla credenziale di accesso (password, impronte digitali o Java Card) selezionata.	<p>Effettuare l'aggiornamento al Service Pack 2 di Windows mediante Windows Update. Per maggiori informazioni sulla causa del problema, fare riferimento all'articolo 813301 della knowledge base Microsoft all'indirizzo <a href="http://www.microsoft.com">http://www.microsoft.com</a>.</p> <p>Per poter accedere, l'utente deve selezionare Password Manager e accedere. Dopo l'accesso a Password Manager, all'utente viene chiesto di accedere a Windows (l'utente potrebbe dover selezionare l'opzione di accesso a Windows) per completare il procedimento di accesso.</p> <p>L'utente, se accede prima a Windows, deve accedere manualmente a Password Manager.</p>
Il processo di protezione <b>Restore Identity</b> (Ripristina identità) perde l'associazione con il token virtuale.	Quando l'utente ripristina l'identità, Password Manager può perdere l'associazione con l'ubicazione del token virtuale nella schermata di accesso. Anche se in Password Manager è registrato il token virtuale, l'utente deve registrare il token per ripristinare l'associazione.	<p>Attualmente secondo progettazione.</p> <p>Quando si disinstalla Security Manager senza conservare le identità, la parte di sistema (server) del token viene distrutta e non è più possibile utilizzare il token per l'accesso, anche se la parte client del token viene ripristinata tramite il ripristino dell'identità.</p> <p>HP sta valutando opzioni a lungo termine per risolvere il problema.</p>

# Device Access Manager per HP ProtectTools

**Agli utenti è stato negato l'accesso alle periferiche da Device Access Manager, ma le periferiche sono ancora accessibili.**

- **Spiegazione:** per negare agli utenti l'accesso alle periferiche, sono state usate le schermate Configurazione semplice e/o Configurazione delle classi di periferiche all'interno di Device Access Manager. Benché l'accesso sia negato, gli utenti possono ancora accedere alle periferiche.
- **Risoluzione:**
  - Verificare che il servizio Controllo/blocco dispositivi HP ProtectTools sia avviato.
  - L'utente amministrativo deve fare clic su **Pannello di controllo**, quindi su **Sistema manutenzione**. Nella finestra **Strumenti di amministrazione**, fare clic su Servizi e cercare il servizio **Controllo/blocco dispositivi HP ProtectTools**. Verificare che il servizio sia avviato e che il tipo di avvio sia **Automatico**.

**A un utente è concesso l'accesso non previsto a una periferica oppure a un utente viene inaspettatamente negato l'accesso a una periferica.**

- **Spiegazione:** Device Access Manager è stato utilizzato per negare l'accesso degli utenti ad alcune periferiche e per consentirlo ad altre. Quando l'utente utilizza il sistema, può accedere alle periferiche a cui ritiene di non avere accesso e non può accedere a quelle a cui ritiene di disporre dell'autorizzazione.
- **Risoluzione:**
  - Utilizzare Configurazione delle classi di periferiche all'interno di Device Access Manager per analizzare le impostazioni delle periferiche per l'utente.
  - Fare clic su **Security Manager**, su **Device Access Manager**, quindi su **Configurazione delle classi di periferiche**. Espandere i livelli nella struttura della classe di periferiche e rivedere le impostazioni applicabili all'utente. Controllare eventuali autorizzazioni "Nega" impostate per l'utente o eventuali gruppi di Windows a cui può appartenere, ad esempio Utenti o Amministratori.

### **Consenti o Nega: quale ha la precedenza?**

- **Spiegazione:** nella schermata Configurazione delle classi di periferiche è stata impostata la seguente configurazione:
  - L'autorizzazione Consenti è stata concessa a un gruppo di Windows (ad esempio, BUILTIN\Administratori) e l'autorizzazione Nega è stata concessa a un altro gruppo di Windows (ad esempio BUILTIN\Utenti) allo stesso livello della gerarchia di classe di periferiche (ad esempio, unità DVD/CD-ROM).
  - Se un utente è membro di entrambi i gruppi (ad esempio Amministratore), quale avrà la precedenza?
- **Risoluzione:**
  - All'utente è negato l'accesso alla periferica. L'autorizzazione Nega ha la precedenza su Consenti.
  - L'accesso viene negato a causa del modo in cui Windows elabora l'autorizzazione effettiva della periferica. A un gruppo viene negato l'accesso e a un gruppo viene consentito, ma l'utente è membro di entrambi i gruppi. All'utente viene negato l'accesso perché l'autorizzazione Nega ha la precedenza su Consenti.
  - Una soluzione alternativa consiste nel negare l'accesso al gruppo Utenti al livello delle unità DVD/CD-ROM e consentire l'accesso al gruppo Amministratori al livello al di sotto delle unità DVD/CD-ROM.
  - Una soluzione alternativa consiste nel creare gruppi di Windows specifici, uno per consentire l'accesso a DVD/CD e uno per negarlo. In questo modo, utenti specifici vengono aggiunti al gruppo appropriato.

**La schermata Configurazione semplice è stata utilizzata per definire un criterio di controllo dell'accesso alle periferiche, ma gli utenti amministrativi non possono accedere alle periferiche.**

- **Spiegazione:** nella schermata Configurazione semplice viene negato l'accesso a Utenti e Ospiti, mentre viene consentito ad Amministratori di periferiche.
- **Risoluzione:** aggiungere l'utente Amministratore al gruppo Amministratori di periferiche.



## Varie

Descrizione sintetica dell'impatto sul software	Dettagli	Soluzione
Security Manager - avviso ricevuto: <b>The security application can not be installed until the HP Protect Tools Security Manager is installed</b> (Impossibile installare l'applicazione di protezione finché non viene installato HP ProtectTools Security Manager).	Tutte le applicazioni di protezione come Java Card Security e biometria sono plug-in estensibili per l'interfaccia Security Manager. Security Manager deve essere installato prima di poter caricare un plug-in di protezione approvato da HP.	Per installare un plug-in di protezione, è necessario avere installato il software Security Manager.
HP ProtectTools Security Manager: Ad intermittenza, viene riportato un errore quando si chiude l'interfaccia Security Manager.	A livello intermittente (1 su 12 casi), si crea un errore con l'uso del pulsante di chiusura, a destra, nella parte superiore della videata, per chiudere Security Manager prima che siano state caricate tutte le applicazioni plug-in.	<p>Ciò è associato ad una dipendenza dal tempo di caricamento dei servizi plug-in quando si chiude e si riavvia Security Manager. Dal momento che PTHOST.exe è l'interfaccia contenente le altre applicazioni (plug-in), completare il tempo di caricamento (servizi) dipende dalla capacità del plug-in. La chiusura dell'interfaccia prima che il plug-in abbia avuto il tempo di completare il caricamento è la causa di fondo.</p> <p>Consentire a Security Manager di completare il messaggio di caricamento dei servizi (visualizzato nella parte superiore della finestra Security Manager) e di tutti i plug-in elencati nella colonna di sinistra. Per evitare errori, attendere qualche minuto per consentire il caricamento dei plug-in.</p>
HP ProtectTools — L'accesso illimitato o i privilegi di amministratore non controllati costituiscono un rischio per la protezione.	<p>L'accesso illimitato al PC client espone la protezione a vari pericoli, fra cui:</p> <ul style="list-style-type: none"> <li>• Eliminazione della PSD</li> <li>• Modifica a scopi illeciti delle impostazioni degli utenti</li> <li>• Disattivazione dei criteri e delle funzioni di protezione</li> </ul>	<p>Agli amministratori si consiglia di seguire le "pratiche migliori" per limitare i privilegi dell'utente finale e limitarne l'accesso.</p> <p>Agli utenti non autorizzati non devono essere concessi privilegi amministrativi.</p>

---

# Glossario

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

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

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

**amministratore** *Vedere* amministratore di 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 la nuova crittografia di chiavi utente di base da una chiave del proprietario della piattaforma in un'altra.

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

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

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

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

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

**background, servizio** Per applicare i criteri di accesso dispositivo, il servizio in background HP ProtectTools Device Locking/Auditing deve essere in esecuzione. Questo servizio può essere visualizzato dall'applicazione Servizi sotto l'opzione Strumenti di amministrazione nel Pannello di controllo. Se il servizio non è attivo, HP Protect Tools Security Manager tenterà di avviarlo durante l'applicazione dei criteri di controllo dispositivo.

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

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

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

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

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

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

**console** Un'ubicazione centralizzata a cui è possibile accedere e in cui gestire impostazioni e funzionalità del programma.

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

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

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

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

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

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

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

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

**Destinatario di contatto attendibile** Persona che riceve un invito a diventare un contatto attendibile.

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

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

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

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

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

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

**Elenco contatti attendibili** Un elenco dei contatti attendibili.

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

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

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

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

**gruppo** Un gruppo di utenti con lo stesso livello di accesso o negazione di accesso a una classe di periferiche o a una periferica specifica.

**HP SpareKey** Copia di backup della chiave di Drive Encryption.

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

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

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

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

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

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

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

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

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

**pannello** Un'ubicazione centralizzata a cui è possibile accedere e in cui gestire impostazioni e funzionalità del programma.

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

**PKI** Public Key Infrastructure (infrastruttura a chiave pubblica): standard che definisce le interfacce per creare, utilizzare e amministrare certificati e chiavi di crittografia.

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

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

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

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

**pulsante Firma e crittografia** Pulsante software che viene visualizzato sulla barra degli strumenti delle applicazioni di Microsoft Office. Facendo clic sul pulsante è possibile firmare, crittografare o rimuovere la crittografia in un documento di Microsoft Office.

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

**riavvio** Processo di riavvio del computer.

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

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

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

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

**scheda ID** Una barra laterale di Windows che consente di identificare visivamente il desktop con nome utente e immagine selezionata. Fare clic sulla scheda ID per avviare HP ProtectTools Administrative Console.

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

**sequenza di tasti** Combinazione di tasti specifici che, premuti, avviano una distruzione automatica, ad esempio, [ctrl+alt+s](#).

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

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

**Single Sign-on** Funzione che archivia i dati di autenticazione e permette di utilizzare Security Manager per accedere a Internet e alle applicazioni Windows che richiedono un'autenticazione tramite password.

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

**token** Vedere metodo di accesso di sicurezza.

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

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

**TXT** Trusted Execution Technology.

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

**utente autorizzato** Un utente a cui è stata concessa l'autorizzazione nella vista Impostazioni di accesso utente per visualizzare o modificare le impostazioni di configurazione nelle viste Configurazione semplice o Configurazione delle classi di periferiche.

**Visualizzatore cronologia di Live Messenger** Un componente di Privacy Manager Chat che consente di cercare e visualizzare le sessioni crittografate di cronologia delle chat.

# Indice analitico

## A

accessi  
aggiunta 28  
categorie 29  
gestione 30  
menu 29  
modifica 29  
accessi non autorizzati, blocco 3  
accesso  
blocco degli accessi non autorizzati 3  
concessione 78  
concessione a utenti o gruppi esistenti 81  
controllo 73  
negazione 77  
negazione a utenti o gruppi esistenti 82  
accesso al computer 37  
aggiunta  
firmatari suggeriti 52  
gruppo 82  
riga per la firma 51  
riga per la firma firmatario suggerito 52  
utente 82  
amministrazione centralizzata 61  
apertura  
console amministrativa HP ProtectTools 9  
Device Access Manager per HP ProtectTools 74  
Drive Encryption per HP ProtectTools 36  
File Sanitizer for HP ProtectTools 65

HP ProtectTools Security Manager 26  
Privacy Manager per HP ProtectTools 42  
applicazioni, configurazione 19  
applicazioni, impostazioni scheda 21  
Applicazioni, scheda, impostazioni 34  
attivazione  
Drive Encryption 37  
pulizia dello spazio libero 71  
autenticazione 15  
avvio sessione di Privacy Manager Chat 55

## B

background, servizio 75  
backup  
certificati di Privacy Manager 60  
contatti attendibili 60  
credenziali HP ProtectTools 7  
dati 33

## C

certificato di Privacy Manager  
eliminazione 44  
impostazione di predefinito 44  
revoca 45  
richiesta 43  
rinnovo 44  
ripristino 45  
visualizzazione dettagli 44  
certificato digitale  
eliminazione 44  
impostazione di predefinito 44  
installazione 43  
revoca 45  
ricezione 43

richiesta 43  
rinnovo 44  
ripristino 45  
visualizzazione dettagli 44  
certificato preassegnato 43  
chat nella finestra Comunicazioni 56  
chiavi di backup, creazione 39  
ciclo di distruzione 67  
concessione accesso 78  
configurazione  
accesso periferiche 74  
applicazioni 19  
classe periferica 76  
console amministrativa HP ProtectTools 14  
controllo accesso 81  
impostazioni 81  
Privacy Manager per Microsoft Outlook 49  
Privacy Manager per un documento di Microsoft Office 51  
Privacy Manager per Windows Live Messenger 56  
ripristino 80  
semplice 74  
configurazione semplice 74  
contatti attendibili  
aggiunta 46  
eliminazione 48  
verifica dello stato della revoca 48  
visualizzazione dettagli 48  
controllo dell'accesso alle periferiche 73  
creazione  
chiavi di backup 39  
profilo di distruzione 66

- creazione guidata
    - installazione HP ProtectTools 8
  - credenziali 31, 32
  - credenziali, registrazione 24
  - crittografia
    - documento di Microsoft Office 53
    - unità 35, 38, 39
  - crittografia, visualizzazione stato 38
  - cronologia chat, visualizzazione 57
- D**
- Dashboard, impostazioni 25
  - dati
    - backup 33
    - limitazione accesso a 3 ripristino 33
  - decrittografia unità 35, 39
  - definizione
    - quali risorse da confermare prima dell'eliminazione 68
    - quali risorse da confermare prima della distruzione 67
  - determinazione impostazioni di protezione 16
  - Device Access Manager per HP ProtectTools
    - apertura 74
    - risoluzione dei problemi 87
  - disattivazione di Drive Encryption 37
  - distruzione manuale
    - tutti gli elementi selezionati 71
    - una risorsa 70
  - Drive Encryption per HP ProtectTools
    - accesso dopo l'attivazione di Drive Encryption 37
    - apertura 36
    - attivazione 37
    - backup e ripristino 39
    - crittografia singole unità 39
    - decrittografia singole unità 39
    - disattivazione 37
    - gestione di Drive Encryption 39
- E**
- e-mail, messaggio
    - crittografia per i contatti attendibili 50
    - firma 50
    - visualizzazione di un messaggio crittografato 50
  - eliminazione semplice 67
  - esclusione di risorse dall'eliminazione automatica 68
  - Excel, aggiunta di una riga per la firma 51
- F**
- File Sanitizer for HP ProtectTools
    - apertura 65
    - icona 70
    - procedure di configurazione 65
  - firma
    - documento di Microsoft Office 51
    - messaggio e-mail 50
  - firmatario suggerito
    - aggiunta 52
    - aggiunta di una riga per la firma 52
  - funzioni di HP ProtectTools 2
  - funzioni di protezione, attivazione 10
  - furto, protezione 3, 84
- G**
- Generale, scheda, impostazioni 20
  - gestione
    - credenziali 31
    - password 21, 27, 28
    - utenti 17
  - gestore password 27, 28
  - gruppo
    - concessione accesso 78
    - negazione accesso 77
    - rimozione 78
- H**
- HP ProtectTools Security Manager
    - apertura 26
    - installazione guidata 8
    - password del file di ripristino 6
  - procedure di
    - configurazione 24
    - risoluzione dei problemi 85
  - HP ProtectTools, console amministrativa
    - apertura 9
    - configurazione 14
    - uso 13
  - HP ProtectTools, funzioni 2
- I**
- impostazione
    - pianificazione distruzione 65
    - pianificazione pulizia dello spazio libero 66
  - impostazioni
    - aggiunta 21, 25, 34
    - applicazioni 21, 25, 34
    - icona 30
    - scheda Generale 20
  - impostazioni dispositivo
    - impronta digitale 18
    - Smart Card 18
    - specificazione 18
  - impronte digitali
    - impostazioni 18
    - registrazione 11, 24
  - installazione guidata 8, 24
  - interruzione di un'operazione di distruzione o di pulizia 71
  - invio tramite e-mail di un documento crittografato di Microsoft Office 53
- J**
- Java Card Security for HP ProtectTools, PIN 6
- L**
- limitazione
    - accesso ai dati sensibili 3
  - LoJack Pro for HP ProtectTools 84
- M**
- Microsoft Excel, aggiunta di una riga per la firma 51
  - Microsoft Office
    - crittografia di un documento 53
    - firma di un documento 51



invio tramite e-mail di un documento crittografato 53  
rimozione crittografia 53  
visualizzazione di un documento crittografato 54  
visualizzazione di un documento firmato 54  
Microsoft Word, aggiunta di una riga per la firma 51

**N**  
negazione accesso 77

**O**  
obiettivi chiave, protezione 3

**P**  
password  
    complessità 30  
    criteri 4  
    gestione 5  
    HP ProtectTools 5  
    istruzioni 7  
    modifica 25  
    protezione 7  
periferica, classe  
    concessione accesso per un utente 79  
    configurazione 76  
periferica, concessione accesso per un utente 79  
personalizzazione  
    profilo di distruzione 67  
    profilo di eliminazione semplice 67  
Preferenze, impostazioni 32  
Privacy Manager  
    uso con Microsoft Outlook 49  
    uso con un documento di Microsoft Office 2007 50  
    utilizzo in Windows Live Messenger 54  
Privacy Manager per HP ProtectTools  
    apertura 42  
    certificato di Privacy Manager 42  
    gestione dei certificati di Privacy Manager 42  
    gestione di contatti attendibili 46

metodi di accesso di sicurezza 41  
metodi di autenticazione 41  
migrazione dei certificati di Privacy Manager e dei contatti attendibili su un altro computer 60  
procedure di  
    configurazione 42  
    requisiti del sistema 41  
Privacy Manager, certificato  
    installazione 43  
    ricezione 43  
profilo di distruzione predefinito 66  
protezione  
    obiettivi chiave 3  
    riepilogo 34  
    ruoli 5  
protezione delle risorse dalla distruzione automatica 67  
protezione, obiettivi 3  
pulizia dello spazio libero 66

**R**  
registrazione delle credenziali 24  
requisiti del sistema 41  
restrizione  
    dell'accesso alle periferiche 73  
richiesta di un certificato digitale 43  
rimozione  
    accesso gruppo 82  
    accesso utente 82  
    crittografia da un documento di Microsoft Office 53  
ripristino  
    certificati di Privacy Manager e dei contatti attendibili 60  
    credenziali HP ProtectTools 7  
    dati 33  
ripristino, esecuzione 40  
risoluzione dei problemi  
    Device Access Manager 87  
    Security Manager 85  
    varie 89  
ruoli per la protezione 5

**S**  
scheda ID 32  
Security Manager  
    installazione guidata 24  
    password di accesso 5  
selezione  
    profilo di distruzione 66  
    risorse per distruzione 66  
sequenza di tasti 69  
Smart Card  
    configurazione 12  
    impostazioni 18  
stato applicazioni di protezione 34  
strumenti di gestione, aggiunta 22  
strumenti, aggiunta 22

**U**  
utente  
    concessione accesso 78  
    negazione accesso 77  
    rimozione 78

**V**  
visualizzazione  
    cronologia chat 57  
    documento di Microsoft Office crittografato 54  
    documento di Microsoft Office firmato 54  
    file di registro 71  
    messaggio e-mail crittografato 50

**W**  
Windows Live Messenger, chat 56  
Windows, password di accesso 6  
Word, aggiunta di una riga per la firma 51

