HP ProtectTools
Benutzerhandbuch

Erste Ausgabe: Oktober 2009

Teilenummer des Dokuments: 572661-041

Inhaltsverzeichnis

1 Einführung in die Sicherheitsfunktionen

Die HP ProtectTools Security Manager Software enthält Sicherheitsfunktionen, die vor unberechtigtem Zugriff auf den Computer, Netzwerke und kritische Daten schützen. HP ProtectTools Security Manager können Sie mit dem Merkmal Administrator-Konsole verwalten.

Mittels dieser Konsole kann der lokale Administrator die folgenden Aufgaben ausführen:

- Aktivieren oder Deaktivieren von Sicherheitsfunktionen
- Registrieren von Fingerabdrücken für Benutzer dieses Computers
- Einrichten einer Smart Card
- Festlegen der erforderlichen Anmeldedaten für die Authentifizierung
- Verwalten der Benutzer des Computers
- Anpassen gerätespezifischer Parameter
- Konfigurieren installierter Security ManagerAnwendungen
- Hinzufügen weiterer Security ManagerAnwendungen

Welche Softwaremodule für Ihren Computer verfügbar sind, ist vom Modell abhängig.

Die HP ProtectTools Softwaremodule sind möglicherweise vorinstalliert oder bereits geladen, oder sie sind auf der HP Website zum Download verfügbar. Weitere Informationen finden Sie unter http://www.hp.com.

HINWEIS: Bei den Anleitungen in diesem Handbuch wird davon ausgegangen, dass die HP ProtectTools Softwaremodule bereits installiert sind.

HP ProtectTools Funktionen

In der folgenden Tabelle finden Sie nähere Informationen zu den HP ProtectTools Modulen.

Modul	Funktionen
Credential Manager for HP ProtectTools	• Password Manager fungiert als persönlicher Kennwortspeicher und beschleunigt den Anmeldeprozess mithilfe der Single Sign On-Funktion, die automatisch Benutzerzugangsdaten speichert und anwendet. • Single Sign On bietet außerdem zusätzliche Sicherheit, weil es Kombinationen aus verschiedenen Sicherheitstechnologien erfordert, beispielsweise eine Java™ Card und biometrische Benutzerauthentifizierung. • Die Kennwortspeicherung wird durch eine Softwareverschlüsselung geschützt und kann durch eine Authentifizierung über ein Sicherheitsgerät wie eine Java Card oder ein biometrisches Lesegerät noch sicherer gemacht werden. **HINWEIS:** Auf die Credential Manager Funktionen können Sie über die HP ProtectTools Security Manager Option Password Manager zugreifen.
Drive Encryption for HP ProtectTools (bestimmte Modelle)	• Drive Encryption bietet eine vollständige Festplattenverschlüsselung für das gesamte Volume. • Drive Encryption erfordert für die Entschlüsselung und den Zugriff auf die Daten eine Authentifizierung vor dem Systemstart.
Privacy Manager for HP ProtectTools (bestimmte Modelle)	• Privacy Manager nutzt erweiterte Anmeldetechniken zur Überprüfung der Quelle, Integrität und Sicherheit der Kommunikation über E-Mail, Microsoft® Office Dokumente oder Instant Messaging (IM).
File Sanitizer for HP ProtectTools	• Mit File Sanitizer können Sie Datenbestände (sensible Informationen wie Anwendungsdateien, Verlaufsdaten oder Web-Inhalte sowie andere vertrauliche Daten) auf Ihrem Computer sicher vernichten und regelmäßig den freien Speicherplatz auf Ihrer Festplatte überschreiben.
Device Access Manager for HP ProtectTools (bestimmte Modelle)	• Device Access Manager ermöglicht IT-Experten die Kontrolle des Gerätezugriffs auf Basis von Benutzerprofilen. • Device Access Manager verhindert, dass unbefugte Benutzer unter Verwendung externer Speichermedien Daten kopieren oder Viren über externe Medien in das System einschleppen. • Der Administrator kann Einzelpersonen oder Benutzergruppen den Zugriff auf beschreibbare Geräte verweigern.

Lösungen für grundlegende Sicherheitsaufgaben

Die HP ProtectTools Module bieten zusammengenommen Lösungen für eine Vielzahl von Sicherheitsproblemen. Hierzu zählen auch die folgenden grundlegenden Sicherheitsmaßnahmen:

- Schutz gegen Diebstahl
- Einschränken des Zugriffs auf sensible Daten
- Verhindern des unbefugten Zugriffs von internen oder externen Standorten
- Erstellen von Richtlinien für den starken Kennwortschutz
- Einhalten behördlicher Sicherheitsvorschriften

Schutz vor gezieltem Diebstahl

Ein Beispiel für gezielten Diebstahl ist der Diebstahl eines Computers mit vertraulichen Daten und Kundeninformationen an einer Sicherheitskontrolle eines Flughafens. Die folgenden Merkmale helfen Ihnen, Ihren Computer vor gezieltem Diebstahl zu schützen:

- Wenn die Funktion für eine Authentifizierung vor dem Systemstart aktiviert ist, kann ein unbefugter Benutzer nicht auf das Betriebssystem zugreifen. Siehe auch die Vorgehensweisen für folgende Merkmale:
  - Security Manager
  - Drive Encryption

Einschränken des Zugriffes auf sensible Daten

Angenommen, ein Wirtschaftsprüfer wird vor Ort eingesetzt. Ihm wird der Zugriff auf die Computer gewährt, um sensible Finanzdaten zu prüfen. Sie möchten allerdings nicht, dass er die Daten drucken oder auf einem beschreibbaren Medium wie einer CD speichern kann. Mit dem folgenden Merkmal können Sie den Zugriff auf Daten einschränken:

- Device Access Manager for HP ProtectTools ermöglicht IT-Leitern, den Zugriff auf beschreibbare Medien einzuschränken, damit keine sensiblen Daten gedruckt oder von der Festplatte auf tragbare Speichermedien kopiert werden können.

Verhindern des unbefugten Zugriffs von internen oder externen Standorten

Der unbefugte Zugriff auf einen ungesicherten PC in einem Unternehmen stellt ein erhebliches Risiko für die Netzwerkressourcen des Unternehmens dar, beispielsweise Informationen von

Finanzdienstleistern, Führungskräften oder dem F&E-Team oder persönliche Daten wie z. B. Patientenakten oder Bankdaten. Die folgenden Funktionen bieten Schutz gegen unbefugten Zugriff:

- Wenn die Funktion für eine Authentifizierung vor dem Systemstart aktiviert ist, kann ein unbefugter Benutzer nicht auf das Betriebssystem zugreifen. Siehe auch die Vorgehensweisen für folgende Merkmale:
  - Password Manager
  - Drive Encryption
- Mit Password Manager können Sie sicherstellen, dass unberechtigte Benutzer keine Kennwörter bzw. keinen Zugriff auf kennwortgeschützte Anwendungen erhalten.
- Device Access Manager for HP ProtectTools ermöglicht IT-Leitern, den Zugriff auf beschreibbare Medien einzuschränken, damit keine sensiblen Daten von der Festplatte kopiert werden können.
- Mit DriveLock ist gewährleistet, dass auch dann nicht auf die Daten zugegriffen werden kann, wenn die Festplatte ausgebaut und in ein nicht gesichertes System wieder eingebaut wird.

Realisieren von strengen Kennwortrichtlinien

Für den Fall, dass die Verwendung sicherer Kennwörter für Dutzende von webbasierten Anwendungen und Datenbanken erforderlich ist, bietet Security Manager ein geschütztes Repository für Kennwörter und eine bequeme Single Sign On Funktion.

Weitere Sicherheitselemente

Zuweisen von Sicherheitsrollen

Bei der Verwaltung der Computersicherheit (besonders für große Unternehmen) besteht ein wichtiger Faktor darin, die Zuständigkeiten und Berechtigungen auf verschiedene Typen von Administratoren und Benutzern zu verteilen.

HINWEIS: In kleineren Unternehmen oder im heimischen Büro können diese Rollen selbstverständlich auch alle von einer Person wahrgenommen werden.

Bei HP ProtectTools können die Pflichten und Berechtigungen in folgende Rollen unterteilt werden:

- Sicherheitsmitarbeiter – Definiert die Sicherheitsstandards für das Unternehmen oder das Netzwerk und legt die anwendbaren Sicherheitsfunktionen fest, wie z. B. Java™ Cards, biometrische Lesegeräte oder USB-Tokens.

  HINWEIS: Viele Funktionen in HP ProtectTools können vom Sicherheitsbeauftragten in Zusammenarbeit mit HP noch weiter angepasst werden. Weitere Informationen finden Sie auf der HP Website unter http://www.hp.com.

- IT-Administrator – Wendet die vom Sicherheitsmitarbeiter definierten Sicherheitsfunktionen an und verwaltet diese. Der IT-Administrator kann manche Funktionen auch aktivieren und deaktivieren. Wenn sich der Sicherheitsmitarbeiter z. B. für den Einsatz von Java Cards entscheidet, kann der IT-Administrator den Java Card BIOS-Sicherheitsmodus aktivieren.

- Benutzer – Verwendet die Sicherheitsfunktionen. Wenn der Sicherheitsmitarbeiter und der IT-Administrator z. B. Java Cards für das System aktiviert haben, kann der Benutzer die PIN für die Java Card festlegen und die Karte zur Authentifizierung verwenden.

ACHTUNG: Administratoren wird geraten, gemäß den „Best Practices“ die Rechte für Endbenutzer und den Benutzerzugriff einzuschränken.

Unberechtigte Benutzer sollten nicht über Administratorrechte verfügen.

Verwalten der Kennwörter für HP ProtectTools

Die meisten HP ProtectTools Security Manager Funktionen sind durch Kennwörter geschützt. Die folgende Tabelle enthält die gängigsten Kennwörter, die Softwaremodule, für welche die Kennwörter eingerichtet wurden, sowie die Kennwortfunktion.

Die Kennwörter, die nur vom IT-Administrator eingerichtet und verwendet werden können, werden ebenfalls in dieser Tabelle angegeben. Alle anderen Kennwörter können von normalen Benutzern oder Administratoren eingerichtet werden.

HP ProtectTools Kennwort	In diesem HP ProtectTools Modul einzurichten	Funktion
Anmeldekennwort für Security Manager	Security Manager	Dieses Kennwort bietet 2 Optionen: • Es kann nach dem Anmelden bei Windows in einem Security Manager Anmeldevorgang für den Zugriff auf Security Manager verwendet werden. • Es kann für den Zugriff auf Windows und Security Manager gleichzeitig verwendet werden.

HP ProtectTools Kennwort	In diesem HP ProtectTools Modul einzurichten	Funktion
Kennwort für Wiederherstellungsdatei von Security Manager	Security Manager, durch IT-Administrator	Schützt den Zugriff auf die Security Manager Wiederherstellungsdatei.
Java™ Card PIN	Java Card Security	Schützt den Zugriff auf die Daten der Java Card und authentifiziert Benutzer der Java Card. Schützt bei der Verwendung für die Authentifizierung beim Systemstart den Zugriff auf Daten auf dem Computer, wenn der Computer eingeschaltet oder neu gestartet wird bzw. wenn der Ruhezustand beendet wird. Authentifiziert Benutzer von Drive Encryption, wenn das Java Card-Token ausgewählt wird.
Windows Anmeldekennwort	Windows® Systemsteuerung	Kann für die manuelle Anmeldung verwendet oder auf der Java Card gespeichert werden.

Erstellen eines sicheren Kennworts

Das Einrichten von Kennwörtern ist nur möglich, wenn Sie die vom Programm festgelegten Anforderungen erfüllen. Beachten Sie im Allgemeinen folgende Richtlinien für das Einrichten von sicheren Kennwörtern, um die Risiken in Bezug auf Kennwörter zu verringern:

- Verwenden Sie Kennwörter mit mehr als 6 Zeichen, vorzugsweise mehr als 8 Zeichen.
- Mischen Sie im gesamten Kennwort Klein- und Großbuchstaben.
- Verwenden Sie nach Möglichkeit sowohl alphanumerische als auch Sonderzeichen und Interpunktionszeichen.
- Ersetzen Sie Buchstaben in einem Kennwort durch Sonderzeichen oder Zahlen. Sie können z. B. die Zahl 1 für den Buchstaben I oder L verwenden.
- Mischen Sie im Kennwort zwei oder mehrere Sprachen.
- Trennen Sie ein Wort oder einen Begriff durch Zahlen oder Sonderzeichen in der Mitte, z. B. „Mary2-2Cat45“.
- Verwenden Sie kein Kennwort, das in einem Wörterbuch vorkommt.
- Verwenden Sie nicht Ihren Namen oder andere persönliche Informationen, wie Geburtstage, Namen von Haustieren oder den Mädchennamen der Mutter, selbst dann nicht, wenn Sie diese rückwärts buchstabieren.
- Ändern Sie das Kennwort regelmäßig. Es genügt, wenn Sie nur einige Zeichen ändern.
- Wenn Sie Ihr Kennwort aufschreiben, bewahren Sie es auf keinen Fall sichtbar in der Nähe des Computers auf.
- Speichern Sie das Kennwort nicht in einer Datei, wie z. B. einer E-Mail, auf dem Computer.
- Nutzen Sie das Konto nicht gemeinsam mit anderen Benutzern, und geben Sie Ihr Kennwort nicht weiter.

Sichern und Wiederherstellen von Zugangsdaten in HP ProtectTools

Sie können die Zugangsdaten von HP ProtectTools über Drive Encryption for HP ProtectTools auswählen und diese sichern.

2 Einführung

HINWEIS: Für die Verwaltung von HP ProtectTools sind Administratorrechte erforderlich.

Der Installations-Assistent für HP ProtectTools hilft Ihnen beim Einrichten der am häufigsten verwendeten Merkmale von Security Manager. Es stehen zudem noch zahlreiche weitere Funktionen über die HP ProtectTools Administrator-Konsole zur Verfügung. Die Einstellungen, die mit dem Assistenten vorgenommen werden können, und weitere Sicherheitsmerkmale können in der Administrator-Konsole konfiguriert werden, auf die Sie über das Windows® Startmenü zugreifen können. Diese Einstellungen sind für den Computer wirksam und für alle Benutzer, die den Computer verwenden.

1. Sie können auf dem Anfangsbildschirm festlegen, dass der Assistent zukünftig nicht mehr angezeigt wird, indem Sie eine der Optionen auswählen.
2. Eine Woche nach der Einrichtung der Computers bzw. wenn ein Benutzer mit Administratorrechten zum ersten Mal mit einem Finger über das Fingerabdruck-Lesegerät streicht, wird der Installations-Assistent für HP ProtectTools automatisch gestartet. Dieser führt Sie durch die grundlegenden Schritte der Programmkonfiguration. Ein Lernvideo über das Einrichten Ihres Computers wird automatisch gestartet.
3. Folgen Sie den Anleitungen auf dem Bildschirm, bis das Setup abgeschlossen ist.

Wenn Sie den Assistenten nicht abschließen, wird er noch zweimal automatisch gestartet. Danach können Sie über die Benachrichtigungssprechblase, die nahe des Infobereichs der Taskleiste angezeigt wird, auf den Assistenten zugreifen (sofern Sie ihn nicht wie in Schritt 2 oben beschrieben deaktiviert haben), um das Setup zu beenden.

Wenn Sie die Anwendungen von HP ProtectTools Security Manager nutzen möchten, starten Sie HP ProtectTools Security Manager über das Startmenü, oder klicken Sie mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste (rechts außen). Die HP ProtectTools Administrator-Konsole und die zugehörigen Anwendungen stehen allen Benutzern des Computers zur Verfügung.

Öffnen der HP ProtectTools Administrator-Konsole

Für Administrationsaufgaben wie z. B. das Einrichten von Systemrichtlinien oder die Konfiguration von Software öffnen Sie die Konsole folgendermaßen:

- Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.

  – ODER –

  Klicken Sie auf der linken Seite von Security Manager auf **Verwaltung**.

Für Benutzeraufgaben wie z. B. das Registrieren von Fingerabdrücken oder Verwenden von Security Manager öffnen Sie die Konsole folgendermaßen:

- Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.

  – ODER –

  Doppelklicken Sie auf das Symbol **HP ProtectTools Security Manager** im Infobereich ganz rechts in der Taskleiste.

Aktivieren der Sicherheitsfunktionen

Sie werden vom Installations-Assistenten aufgefordert, Ihre Identität zu bestätigen.

1. Lesen Sie den Anfangsbildschirm, und klicken Sie dann auf **Weiter**.
2. Bestätigen Sie Ihre Identität entweder durch Eingabe Ihres Windows Kennworts, wenn Sie noch keine Fingerabdrücke registriert haben, oder durch das Einlesen Ihrer Fingerabdrücke mit dem Fingerabdruck-Lesegerät. Klicken Sie auf **Weiter**.

   Wenn kein Windows Kennwort eingerichtet ist, werden Sie dazu aufgefordert, ein Kennwort zu erstellen. Ein Windows Kennwort ist erforderlich, um Ihr Windows Konto vor dem Zugriff unbefugter Personen zu schützen und die HP ProtectTools Security Manager Funktionen nutzen zu können.

Der Installations-Assistent führt Sie durch die Schritte zum Aktivieren von Sicherheitsfunktionen, die für alle Benutzer des Computers wirksam sind:

- Windows Anmeldesicherheit schützt Ihr(e) Windows Konto/Konten, indem es dafür sorgt, dass der Zugriff nur mit bestimmten Anmeldedaten möglich ist.
- Drive Encryption schützt Ihre Daten durch die Verschlüsselung Ihrer Festplatte(n), so dass Informationen für Personen ohne die entsprechende Berechtigung nicht lesbar sind.
- Pre-Boot Security schützt Ihren Computer, indem es den Zugriff unbefugter Personen verhindert, bevor Windows gestartet wird.

Aktivieren Sie das zugehörige Kontrollkästchen, um eine Sicherheitsfunktion auszuwählen. Je mehr Funktionen Sie auswählen, desto sicherer ist Ihr Computer.

HINWEIS: Pre-Boot Security steht nur dann zur Verfügung, wenn diese Funktion vom BIOS des Computers unterstützt wird.

Registrieren Ihrer Fingerabdrücke

Wenn Sie „Fingerabdruck“ ausgewählt haben und Ihr Computer über ein integriertes oder angeschlossenes Fingerabdruck-Lesegerät verfügt, werden Sie durch die Konfiguration bzw. „Registrierung” Ihrer Fingerabdrücke geleitet:

1. Es wird eine Abbildung von zwei Händen angezeigt. Finger, die bereits registriert wurden, werden grün dargestellt. Klicken Sie auf einen Finger in der Darstellung.

   HINWEIS: Wenn Sie einen bereits registrierten Fingerabdruck löschen möchten, klicken Sie auf den entsprechenden Finger.

2. Wenn Sie einen Finger für die Registrierung ausgewählt haben, werden Sie aufgefordert, diesen Fingerabdruck zu scannen, bis er erfolgreich registriert wird. Ein registrierter Finger wird in der Abbildung grün hervorgehoben.

3. Sie müssen mindestens zwei Finger registrieren, wobei Zeige- und Mittelfinger vorzuziehen sind. Wiederholen Sie die Schritte 1 bis 3 für einen weiteren Finger.

4. Klicken Sie auf **Weiter**.

HINWEIS: Wenn die Fingerabdrücke in der Einführungsphase registriert werden, werden die Fingerabdruck-Informationen erst mit einem Klick auf **Weiter** gespeichert. Wenn der Computer eine Zeit lang inaktiv ist oder Sie die Anwendung schließen, werden die Änderungen, die Sie vornehmen, **nicht** gespeichert.

Smart Card einrichten

Wenn Sie „Smart Card“ ausgewählt haben und ein Smart Card Reader im Computer installiert oder am Computer angeschlossen ist, werden Sie vom Installations-Assistenten für HP ProtectTools aufgefordert, eine Smart Card PIN einzurichten.

So richten Sie eine Smart CardPIN ein:

1. Auf der Seite „Smart Card einrichten” geben Sie eine PIN ein und bestätigen diese.

   Sie können Ihre PIN auch ändern. Geben Sie Ihre alte PIN ein, und wählen Sie dann eine neue.

2. Klicken Sie auf **Weiter**, um fortzufahren.

Verwenden der Administrator-Konsole

Die HP ProtectTools Administrator-Konsole ist die zentrale Stelle für die Verwaltung der Funktionen und Anwendungen von HP ProtectTools Security Manager.

Die Konsole setzt sich aus den folgenden Komponenten zusammen:

- **Tools** – Zeigt die folgenden Kategorien für die Konfiguration der Sicherheit auf dem Computer an:
  - **Startseite** – Hier können Sie die Sicherheitsaufgaben auswählen, die ausgeführt werden sollen.
  - **System** – Ermöglicht die Konfiguration von Sicherheitsfunktionen und die Authentifizierung für Benutzer und Geräte.
  - **Anwendungen** – Zeigt die allgemeinen Einstellungen für HP ProtectTools Security Manager und für Security ManagerAnwendungen an.
  - **Daten** – Enthält ein erweitertes Menü mit Links zu den Security ManagerAnwendungen, die Ihre Daten schützen.
- **Management-Tools** – Bietet Informationen zu weiteren Tools. Im Fenster unten werden die folgenden Auswahlmöglichkeiten angezeigt:
  - **Installations-Assistent für HP ProtectTools** – Führt Sie durch die Einrichtung von HP ProtectTools Security Manager.
  - **Hilfe** – Zeigt die Hilfedatei an, in der Sie Informationen über Security Manager und seine vorinstallierten Anwendungen finden. Hilfe für Anwendungen, die Sie möglicherweise hinzufügen, finden Sie in den entsprechenden Anwendungen.
  - **Info** – Zeigt Informationen zu HP ProtectTools Security Manager, wie etwa Versionsnummer und Copyright-Hinweis, an.
- **Hauptbereich** – Zeigt anwendungsspezifische Bildschirme an.

Um die HP ProtectTools Administrator-Konsole zu öffnen, klicken Sie auf **Start**, auf **Alle Programme**, auf **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.

3 Konfigurieren Ihres Systems

Der Zugriff auf die System-Gruppe erfolgt über das Menü „Tools” auf der linken Seite der HP ProtectTools Administrator-Konsole. Mit den Anwendungen aus dieser Gruppe können Sie die Richtlinien und Einstellungen für den Computer sowie die Benutzer und angeschlossenen Geräte verwalten.

Die folgenden Anwendungen sind in der System-Gruppe enthalten.

- **Sicherheit** – Verwalten von Funktionen, der Authentifizierung und von Einstellungen, die steuern, wie die Benutzer mit diesem Computer interagieren.
- **Benutzer** – Einrichten, Verwalten und Registrieren von Benutzern dieses Computers.
- **Geräte** – Verwalten von Einstellungen für integrierte bzw. an den Computer angeschlossene Sicherheitsgeräte.

Einrichten der Authentifizierung für Ihren Computer

In der Authentifizierungsanwendung können Sie auswählen, welche Sicherheitsfunktionen auf diesem Computer implementiert werden sollen. Sie können den Zugriff auf den Computer verwalten und zusätzliche erweiterte Einstellungen konfigurieren. Sie können Anmeldeinformationen festlegen, die für die Authentifizierung jeder Benutzerklasse für die Anmeldung bei Windows oder auf Websites und Programmen während einer Benutzersitzung benötigt werden.

So richten Sie eine Authentifizierung auf Ihrem Computer ein:

1. Klicken Sie im Menü „Sicherheit” auf **Authentifizierung**.
2. Zur Konfiguration der Anmeldeauthentifizierung klicken Sie auf die Registerkarte **Anmelderichtlinie**, nehmen die Änderungen vor und klicken dann auf **Übernehmen**.
3. Zur Konfiguration der Sitzungsauthentifizierung klicken Sie auf die Registerkarte **Sitzungsrichtlinie**, nehmen die Änderungen vor und klicken dann auf **Übernehmen**.

Anmelderichtlinie

So definieren Sie Richtlinien für die Verwaltung der Anmeldedaten, die für die Authentifizierung eines Benutzers bei der Windows Anmeldung erforderlich sind:

1. Klicken Sie im Menü „Tools” auf **Sicherheit**, und klicken Sie dann auf **Authentifizierung**.
2. Klicken Sie auf der Registerkarte **Anmelderichtlinie** auf eine Benutzerkategorie.
3. Geben Sie die für die ausgewählte Benutzerkategorie benötigen Anmeldeinformationen zur Authentifizierung an. Es muss mindestens eine Anmeldeinformation angegeben werden.
4. Wählen Sie, ob BELIEBIGE (nur eine) der angegebenen Methoden oder ALLE der angegebenen Methoden für die Authentifizierung eines Benutzers verwendet werden sollen. Sie können auch festlegen, dass kein Benutzer Zugriff auf den Computer erhält.
5. Klicken Sie auf **Übernehmen**.

Sitzungsrichtlinie

So bestimmen Sie Richtlinien, die regulieren, welche Anmeldedaten für den Zugriff auf HP ProtectTools Anwendungen in einer Windows Sitzung erforderlich sind:

1. Klicken Sie im Menü „Tools” auf **Sicherheit**, und klicken Sie dann auf **Authentifizierung**.
2. Klicken Sie auf der Registerkarte **Sitzungsrichtlinie** auf eine Benutzerkategorie.
3. Geben Sie die für die ausgewählte Benutzerkategorie benötigten Anmeldeinformationen zur Authentifizierung an.
4. Wählen Sie, ob BELIEBIGE (nur eine) der angegebenen Methoden oder ALLE der angegebenen Methoden für die Authentifizierung eines Benutzers verwendet werden sollen. Sie können auch festlegen, dass keine Authentifizierung für den Zugriff auf die HP ProtectTools Software erforderlich ist.
5. Klicken Sie auf **Übernehmen**.

Einstellungen

Sie können eine oder mehrere der folgenden Sicherheitseinstellungen zulassen:

- **One-Step Logon zulassen** – Ermöglicht es den Benutzern dieses Computers, die Windows Anmeldung zu überspringen, wenn die Authentifizierung im BIOS oder über eine verschlüsselte Festplatte erfolgt ist.
- **HP SpareKey Authentifizierung für Windows Anmeldung zulassen** – Ermöglicht es den Benutzern dieses Computers, die Funktion HP SpareKey für die Anmeldung bei Windows zu verwenden, obwohl von Security Manager andere Authentifizierungsrichtlinien verlangt werden.

So bearbeiten Sie die Einstellungen:

1. Klicken Sie auf eine bestimmte Einstellung, um sie zu aktivieren oder zu deaktivieren.
2. Klicken Sie auf **Übernehmen**, um die Änderungen, die Sie vorgenommen haben, zu speichern.

Verwalten von Benutzern

In der Anwendung „Benutzer” können Sie die HP ProtectTools Benutzer dieses Computers überprüfen und verwalten.

Alle HP ProtectTools Benutzer werden aufgeführt, und es wird geprüft, ob Sie die Richtlinien von Security Manager erfüllen und ob sie die richtigen Anmeldedaten registriert haben, die es ihnen ermöglichen, diese Richtlinien einzuhalten.

Um weitere Benutzer hinzuzufügen, klicken Sie auf **Hinzufügen**.

Um einen Benutzer zu löschen, klicken Sie auf den Benutzer und danach auf **Löschen**.

Um Fingerabdrücke zu registrieren oder zusätzliche Anmeldeinformationen für den Benutzer einzurichten, klicken Sie auf **Registrieren**.

Um sich die Richtlinien für einen bestimmten Benutzer anzusehen, wählen Sie den Benutzer aus, und klicken Sie dann auf **Richtlinien anzeigen**.

Geräteeinstellungen

In der Anwendung „Geräte” können Sie Einstellungen für integrierte oder angeschlossene Sicherheitsgeräte, die von HP ProtectTools Security Manager erkannt werden, festlegen.

Fingerabdrücke

Die Seite „Fingerabdrücke” hat drei Registerkarten: Registrierung, Empfindlichkeit und Erweitert.

Registrierung

Sie können die Mindest- und die Höchstanzahl an Fingerabdrücken wählen, die ein Benutzer registrieren kann.

Sie können ebenfalls alle Daten vom Fingerabdruck-Lesegerät löschen.

⚠ **VORSICHT!** Alle Fingerabdruckdaten für alle Benutzer, einschließlich Administratoren, werden dann gelöscht. Falls die Anmelderichtlinie nur die Authentifizierung per Fingerabdruck vorsieht, kann dies dazu führen, dass sich alle Benutzer nicht mehr an diesem Computer anmelden können.

Empfindlichkeit

Zum Anpassen der Empfindlichkeit, mit der das Fingerabdruck-Lesegerät Ihre Fingerabdrücke scannt, bewegen Sie den Schieberegler.

Wenn Ihr Fingerabdruck nicht konsistent erkannt wird, ist es möglicherweise erforderlich, die Empfindlichkeit zu vermindern. Eine höhere Einstellung erhöht die Empfindlichkeit für Abweichungen bei den Fingerabdruckscans und verringert dadurch die Möglichkeit eines fälschlicherweise zugelassenen Zugriffs. Eine mittlere Einstellung bietet ein ausgewogenes Verhältnis aus Sicherheit und Komfort.

Erweitert

Sie können das Fingerabdruck-Lesegerät so konfigurieren, dass es weniger Strom verbraucht, wenn der Computer über den Akku betrieben wird.

Smart Card

Sie können den Computer so einstellen, dass er automatisch gesperrt wird, wenn eine Smart Card entfernt wird. Der Computer wird jedoch nur dann gesperrt, wenn die Smart Card als Anmeldemöglichkeit zur Authentifizierung bei der Windows Anmeldung genutzt wurde. Wenn eine Smart Card entfernt wird, die nicht für die Windows Anmeldung verwendet wurde, wird der Computer nicht gesperrt.

▲ Aktivieren Sie das Kontrollkästchen, um das Sperren des Computers beim Entfernen der Smart Card zu aktivieren oder zu deaktivieren.

4 Konfigurieren Ihrer Anwendungen

Der Zugriff auf die Anwendungsgruppe erfolgt über das Menü „Sicherheitsanwendungen” auf der linken Seite der HP ProtectTools Administrator-Konsole. Sie können die Einstellungen nutzen, um das Verhalten der installierten HP ProtectTools Security ManagerAnwendungen anzupassen.

So bearbeiten Sie die Anwendungseinstellungen:

1. Klicken Sie im Menü „Tools” aus der Gruppe **Anwendungen** auf **Einstellungen**.
2. Klicken Sie auf eine bestimmte Einstellung, um sie zu aktivieren oder zu deaktivieren.
3. Klicken Sie auf **Übernehmen**, um die Änderungen, die Sie vorgenommen haben, zu speichern.

Registerkarte „Allgemein”

Die folgenden Einstellungen stehen auf dieser Registerkarte zur Verfügung:

- **Installations-Assistent für Administratoren nicht automatisch starten** – Wählen Sie diese Option, um zu verhindern, dass beim Start automatisch der Assistent ausgeführt wird.
- **Einführungsassistent für Benutzer nicht automatisch starten** – Wählen Sie diese Option, um zu verhindern, dass die Benutzerinstallation automatisch bei der Anmeldung geöffnet wird.

Registerkarte Anwendungen

Die hier dargestellten Einstellungen können sich ändern, wenn neue Anwendungen zu Security Manager hinzugefügt werden. Standardmäßig werden jedoch mindestens die folgenden Einstellungen angezeigt:

- **Security Manager** – Aktiviert die Anwendung Security Manager für alle Benutzer des Computers.
- **Schaltfläche „Weitere Anwendungen“ aktivieren** – Ermöglicht es allen Benutzern dieses Computers, Anwendungen zu HP ProtectTools Security Manager hinzuzufügen, indem sie auf die Schaltfläche **[+] Weitere Anwendungen** klicken.

Um alle Anwendungen auf die Werkseinstellung zurückzusetzen, klicken Sie auf die Schaltfläche **Standardeinstellungen wiederherstellen**.

5 Management-Tools hinzufügen

Es können zusätzliche Anwendungen zur Verfügung stehen, um neue Management-Tools in Security Manager aufzunehmen. Der Administrator dieses Computers kann diese Funktion über die Anwendung „Einstellungen“ deaktivieren.

Zum Hinzufügen zusätzlicher Management-Tools klicken Sie auf **[+] Management-Tools**.

Auf der Website von DigitalPersona finden Sie neue Anwendungen, oder Sie können einen Zeitplan für automatische Updates einrichten.

6 HP ProtectTools Security Manager

HP ProtectTools Security Manager ermöglicht Ihnen, die Sicherheit Ihres Computers beträchtlich zu erhöhen.

Sie können vorinstallierte Security ManagerAnwendungen sowie zusätzliche Anwendungen nutzen, die zum sofortigen Download aus dem Internet zur Verfügung stehen:

- Benutzernamen und Kennwörter verwalten
- Kennwort für das Windows® Betriebssystem schnell und einfach ändern
- Programmeinstellungen festlegen
- Fingerabdrücke für zusätzliche Sicherheit und gesteigerten Komfort verwenden
- Eine Smart Card zur Authentifizierung einrichten
- Programmdaten sichern und wiederherstellen
- Weitere Anwendungen hinzufügen

Setup-Verfahren

Einführung

Der Installations-Assistent für HP ProtectTools wird automatisch als Standardseite in HP ProtectTools Security Manager angezeigt, bis die Einrichtung abgeschlossen wurde.

Gehen Sie wie folgt vor, um Security Manager einzurichten:

HINWEIS: Wenn weder ein Fingerabdruck-Lesegerät noch eine Smart Card zur Verfügung steht, führen Sie nur die Schritte 1, 5 und 6 durch.

1. Klicken Sie auf dem Anfangsbildschirm auf **Weiter**.
2. Auf der folgenden Seite sind die Authentifizierungsmethoden aufgeführt, die für diesen Computer zur Verfügung stehen. Klicken Sie auf **Weiter**, um fortzufahren.
3. Geben Sie auf der Seite „Identität bestätigen“ Ihr Windows Kennwort ein, und klicken Sie dann auf **Weiter**.
4. Je nach Konfiguration Ihres Computers finden Sie weitere Informationen unter folgenden Themen:
   - Wenn ein Fingerabdruck-Lesegerät verfügbar ist, siehe „Registrieren Ihrer Fingerabdrücke“ auf Seite 24.
   - Wenn eine Smart Card verfügbar ist, siehe „Smart Card einrichten“ auf Seite 25.
5. Wenn weder ein Fingerabdruck-Lesegerät noch eine Smart Card zur Verfügung steht, werden Sie aufgefordert, Ihr Windows Kennwort einzugeben. Sie müssen dieses Kennwort künftig immer verwenden, wenn eine Authentifizierung erforderlich ist.
6. Klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

   Das Security Menü-Übersicht wird angezeigt.

Registrieren von Anmeldeinformationen

Auf der Seite „Meine Identität“ können Sie Ihre verschiedenen Authentifizierungsmethoden oder Anmeldeinformationen registrieren. Nachdem diese registriert wurden, können Sie sich damit bei Security Manager anmelden.

Registrieren Ihrer Fingerabdrücke

Wenn ein Fingerabdruck-Lesegerät in Ihrem Computer installiert oder an Ihrem Computer angeschlossen ist, führt Sie der Installations-Assistent für HP ProtectTools durch die Einrichtung bzw. Registrierung Ihrer Fingerabdrücke.

1. Lesen Sie den Anfangsbildschirm, und klicken Sie dann auf **Weiter**.
2. Bestätigen Sie Ihre Identität entweder durch Eingabe Ihres Windows Kennworts, wenn Sie noch keine Fingerabdrücke registriert haben, oder durch das Einlesen Ihrer Fingerabdrücke mit dem Fingerabdruck-Lesegerät. Klicken Sie auf **Weiter**.

   Wenn kein Windows Kennwort eingerichtet ist, werden Sie dazu aufgefordert, ein Kennwort zu erstellen. Ein Windows Kennwort ist erforderlich, um Ihr Windows Konto vor dem Zugriff unbefugter Personen zu schützen und um die HP ProtectTools Security Manager Funktionen nutzen zu können.

3. Es wird eine Abbildung von zwei Händen angezeigt. Finger, die bereits registriert wurden, werden grün dargestellt. Klicken Sie auf einen Finger in der Darstellung.

   HINWEIS: Wenn Sie einen bereits registrierten Fingerabdruck löschen möchten, klicken Sie auf den entsprechenden Fingerabdruck.

4. Wenn Sie einen Finger für die Registrierung ausgewählt haben, werden Sie aufgefordert, diesen Fingerabdruck zu scannen, bis er erfolgreich registriert wird. Ein registrierter Finger wird in der Abbildung grün hervorgehoben.

5. Sie müssen mindestens zwei Finger registrieren, wobei Zeige- und Mittelfinger vorzuziehen sind. Wiederholen Sie die Schritte 3 und 4 für einen weiteren Finger.

6. Klicken Sie auf **Weiter**.

HINWEIS: Wenn die Fingerabdrücke in der Einführungsphase registriert werden, werden die Fingerabdruck-Informationen erst mit einem Klick auf **Weiter** gespeichert. Wenn der Computer eine Zeit lang inaktiv ist oder Sie das Programm schließen, werden die Änderungen, die Sie vornehmen, **nicht** gespeichert.

Ändern Ihres Windows Kennworts

Mit Security Manager lässt sich Ihr Windows Kennwort schneller und einfacher ändern als über die Systemsteuerung.

Gehen Sie folgendermaßen vor, um Ihr Windows Kennwort zu ändern:

1. Klicken Sie im Security Manager-Dashboard auf **Meine Identität**, **Anmeldedaten** und anschließend auf **Kennwort**.

2. Geben Sie in das Textfeld **Aktuelles Windows Kennwort** Ihr aktuelles Kennwort ein.

3. Geben Sie in das Textfeld **Neues Windows Kennwort** ein neues Kennwort ein, und wiederholen Sie dieses im Textfeld **Neues Kennwort bestätigen**.

4. Klicken Sie auf **Ändern**, um Ihr aktuelles Kennwort sofort durch das soeben eingegebene Kennwort zu ersetzen.

Smart Card einrichten

Wenn ein Lesegerät für Smart Cards in den Computer integriert bzw. daran angeschlossen ist, fordert Sie Security Manager auf, eine Smart Card PIN einzurichten (persönliche Identifikationsnummer).

- Zum Einrichten einer Smart Card PIN geben Sie auf der Seite „Smart Card einrichten” eine PIN ein, und bestätigen Sie diese.
- Zum Ändern Ihrer PIN geben Sie zuerst die alte PIN ein, und wählen Sie dann eine neue.

Verwenden des Security der Menü-Übersicht von

Das Security Die Menü-Übersicht von ist die zentrale Zugriffsstelle auf die Funktionen, Anwendungen und Einstellungen von Security Manager.

Die Menü-Übersicht setzt sich aus den folgenden Komponenten zusammen:

- **ID-Card** – Zeigt den Windows Benutzernamen und ein ausgewähltes Bild zur Ermittlung des angemeldeten Benutzerkontos an.
- **Sicherheitsanwendungen** – Zeigt ein erweitertes Menü mit Links an, über die folgende Sicherheitskategorien konfiguriert werden können:
  - **Meine Identität**
  - **Meine Daten**
  - **Arbeitsplatz**
- **Weitere Anwendungen** – Öffnet eine Seite, auf der Sie zusätzliche Anwendungen zur Verbesserung der Sicherheit Ihrer Identität, Ihrer Daten und Ihrer Kommunikationen finden.
- **Hauptbereich** – Zeigt anwendungsspezifische Bildschirme an.
- **Verwaltung** – Öffnet die HP ProtectTools Administrator-Konsole.
- Schaltfläche **Hilfe** – Zeigt Informationen zum aktuellen Bildschirm an.
- **Erweitert** – Ermöglicht den Zugriff auf folgende Optionen:
  - **Voreinstellungen** – Ermöglicht die Personalisierung der Security Manager Einstellungen.
  - **Sichern und Wiederherstellen** – Ermöglicht die Sicherung und Wiederherstellung von Daten.
  - **Info** – Zeigt Versionsinformationen zu Security Manager an.

Um die Menü-Übersicht von Security Manager zu öffnen, klicken Sie auf **Start**, auf **Alle Programme**, auf **HP** und anschließend auf **HP ProtectTools Security Manager**.

Öffnen von HP ProtectTools Security Manager

Es stehen folgende Möglichkeiten zur Verfügung, um HP ProtectTools Security Manager zu öffnen:

- Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
- Doppelklicken Sie auf das Symbol **HP ProtectTools** im Infobereich außen rechts in der Taskleiste.
- Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** und anschließend auf **HP ProtectTools Security Manager öffnen**.
- Klicken Sie auf die Minianwendung **Security Manager ID-Card** in der Windows Randleiste.
- Drücken Sie die Tastenkombination strg+alt+h, um das Verknüpfungsmenü für Security Manager anzuzeigen.

Allgemeine Aufgaben

Die in dieser Gruppe enthaltenen Anwendungen unterstützen Sie bei der Verwaltung verschiedener Aspekte Ihrer digitalen Identität.

- **Security Manager** – Erstellt und verwaltet Verknüpfungen, die Ihnen ermöglichen, Websites und Programme zu öffnen und sich bei diesen mithilfe einer Authentifizierung mit Ihrem Windows Kennwort, Ihrem Fingerabdruck oder einer Smart Card anzumelden.
- **Anmeldedaten** – Hier können Sie ganz einfach Ihr Windows Kennwort ändern, Ihre Fingerabdrücke registrieren oder eine Smart Card einrichten.

Zum Hinzufügen weiterer Anwendungen klicken Sie unten links in der Menü-Übersicht auf die Schaltfläche [+] **Weitere Anwendungen**. Diese Schaltfläche kann vom Administrator deaktiviert werden.

Password Manager

Mit Password Manager wird das Anmelden bei Windows, Websites und Anwendungen einfacher und sicherer. Sie können dieses Tool verwenden, um Kennwörter mit höherer Sicherheit zu erstellen, die Sie nicht aufschreiben oder im Kopf behalten müssen. Sie können sich dann schnell und einfach per Fingerabdruck, Smart Card oder mit Ihrem Windows Kennwort anmelden.

Password Manager bietet folgende Optionen:

- Hinzufügen, Bearbeiten oder Löschen von Anmeldedaten über die Registerkarte „Verwalten“
- Verwenden von Verknüfungen zum Starten Ihres Standardbrowsers und Anmelden bei beliebigen Websites oder Programmen (nach entsprechender Einrichtung)
- Verschieben von Verknüpfungen per Ziehen und Ablegen, um diese nach Belieben in Kategorien einzuordnen
- Auf einen Blick erkennen, ob eines Ihrer Kennwörter ein Sicherheitsrisiko birgt, und automatisch komplexe Kennwörter mit hoher Sicherheit für neue Websites generieren

Viele Funktionen von Password Manager sind auch über das Password Manager Symbol verfügbar, das angezeigt wird, wenn der Anmeldebildschirm einer Website oder eines Programms aktiv ist. Klicken Sie auf das Symbol, um ein Kontextmenü anzuzeigen, in dem Sie aus folgenden Optionen wählen können:

Für Websites oder Programme, für die noch keine Anmeldedaten festgelegt wurden

Folgende Optionen werden im Kontextmenü angezeigt:

- **[Domänenname] zu Password Manager hinzufügen** – Ermöglicht das Hinzufügen von Anmeldedaten für den aktuellen Anmeldebildschirm.
- **Password Manager öffnen** – Startet Password Manager.
- **Symboleinstellungen** – Hier können Sie Bedingungen festlegen, unter denen das Password Manager Symbol angezeigt werden soll.
- **Hilfe** – Zeigt die Softwarehilfe zu Password Manager an.

Für Websites oder Programme, für die bereits Anmeldedaten festgelegt wurden

Folgende Optionen werden im Kontextmenü angezeigt:

- **Anmeldedaten eingeben** – Fügt Ihre Anmeldedaten in die Anmeldefelder ein und sendet sie an die Seite (wenn das Senden beim Erstellen oder bei der letzten Änderung der Anmeldedaten festgelegt wurde).
- **Anmeldedaten bearbeiten** – Hier können Sie Ihre Anmeldedaten für diese Website bearbeiten.
- **Neues Konto hinzufügen** – Hier können Sie bestimmten Anmeldedaten ein Konto hinzufügen.
- **Password Manager öffnen** – Startet Password Manager.
- **Hilfe** – Zeigt die Softwarehilfe zu Password Manager an.

HINWEIS: Möglicherweise hat der Administrator dieses Computers Security Manager so eingerichtet, dass mehr als eine Authentifizierung zur Verifizierung Ihrer Identität erforderlich ist.

Hinzufügen von Anmeldedaten

Sie können ganz einfach Anmeldedaten für eine Website oder ein Programm hinzufügen, indem Sie diese einmal eingeben. Ab diesem Zeitpunkt gibt Password Manager diese Daten automatisch für Sie ein. Sie können diese Anmeldedaten verwenden, nachdem Sie zur entsprechenden Website oder zum Programm navigiert sind, oder indem Sie im Menü **Anmeldedaten** auf bestimmte Anmeldedaten klicken, woraufhin Password Manager die Website oder das Programm für Sie öffnet und die Anmeldung vornimmt.

So fügen Sie Anmeldedaten hinzu:

1. Öffnen Sie den Anmeldebildschirm für eine Website oder ein Programm.
2. Klicken Sie auf den Pfeil am **Password Manager**-Symbol, und klicken Sie dann auf eine der folgenden Optionen, je nachdem, ob es sich um den Anmeldebildschirm einer Website oder eines Programms handelt.
   - Klicken Sie im Falle einer Website auf **[Domänenname] zu Password Manager hinzufügen**.
   - Klicken Sie im Falle eines Programms auf **Diesen Anmeldebildschirm zu Password Manager hinzufügen**.
3. Geben Sie Ihre Anmeldedaten ein. Anmeldefelder auf dem Bildschirm und ihre entsprechenden Felder im Dialogfeld sind mit einer fett formatierten orangen Umrandung gekennzeichnet. Sie können dieses Dialogfeld auch anzeigen, indem Sie auf der Registerkarte **Verwalten** im **Password Manager** auf **Anmeldedaten hinzufügen** klicken. Einige Optionen sind abhängig von den an den Computer angeschlossenen Sicherheitsgeräten, z. B. davon, ob Sie strg+alt+h drücken, Ihren Fingerabdruck scannen oder eine Smart Card einsetzen.
   - Zum Füllen eines Anmeldefelds mit einer der vorformatierten Auswahlmöglichkeiten klicken Sie auf die Pfeile rechts vom Feld.
   - Um weitere Felder vom Bildschirm zu Ihren Anmeldedaten hinzuzufügen, klicken Sie auf **Andere Felder wählen**.

- Um die Anmeldefelder ausfüllen zu lassen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldedaten senden**.
- Um das Kennwort für diese Anmeldedaten anzuzeigen, klicken Sie auf **Kennwort einblenden**.

4. Klicken Sie auf **OK**.

   Das Pluszeichen wird vom Password Manager Symbol entfernt, was anzeigt, dass die Anmeldedaten erstellt wurden.

Jedes Mal, wenn Sie diese Website oder dieses Program aufrufen, wird das Password Manager Symbol angezeigt. Dies bedeutet, dass Sie für die Anmeldung Ihre registrierten Anmeldedaten verwenden können.

Bearbeiten von Anmeldedaten

Gehen Sie folgendermaßen vor, um Anmeldedaten zu bearbeiten:

1. Öffnen Sie den Anmeldebildschirm für eine Website oder ein Programm.
2. Um ein Dialogfeld anzuzeigen, in dem Sie Ihre Anmeldedaten bearbeiten können, klicken Sie auf den Pfeil auf dem **Password Manager**-Symbol und anschließend auf **Anmeldedaten bearbeiten**. Anmeldefelder auf dem Bildschirm und ihre entsprechenden Felder im Dialogfeld sind mit einer fett formatierten orangen Umrandung gekennzeichnet.

   Sie können dieses Dialogfeld auch anzeigen, indem Sie auf der Registerkarte **Verwalten** im **Password Manager** auf **Für gewünschte Anmeldedaten bearbeiten** klicken.
3. Bearbeiten Sie Ihre Anmeldedaten.
   - Um ein Anmeldefeld mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken Sie auf die Pfeile rechts vom Feld.
   - Um weitere Felder vom Bildschirm zu Ihren Anmeldedaten hinzuzufügen, klicken Sie auf **Andere Felder wählen**.
   - Um die Anmeldefelder ausfüllen zu lassen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldedaten senden**.
   - Um das Kennwort für diese Anmeldedaten anzuzeigen, klicken Sie auf **Kennwort einblenden**.
4. Klicken Sie auf **OK**.

Verwenden des Anmeldemenüs

Password Manager ermöglicht es Ihnen, auf schnelle und einfache Art Websites und Programme zu starten, für die Sie Anmeldedaten festgelegt haben. Doppelklicken Sie im Menü **Anmeldedaten** oder auf der Registerkarte **Verwalten** im **Password Manager** auf die Anmeldedaten für ein Programm oder eine Website, um den Anmeldebildschirm zu öffnen, und geben Sie dann Ihre Anmeldedaten ein.

Wenn Sie Anmeldedaten festlegen, werden diese automatisch in das Anmeldemenü von Password Manager übernommen.

So zeigen Sie das Anmeldemenü an:

1. Drücken Sie die Tastenkombination für **Password Manager**. strg+alt+h ist die Werkseinstellung. Zum Ändern der Tastenkombination klicken Sie auf **Password Manager** und anschließend auf **Einstellungen**.
2. Scannen Sie Ihren Fingerabdruck (bei Computern mit integriertem oder angeschlossenem Fingerabdruck-Lesegerät).

Organisieren von Anmeldedaten in Kategorien

Erstellen Sie zum Ordnen Ihrer Anmeldedaten verschiedene Kategorien. Verschieben Sie dann die Anmeldedaten per Drag and Drop in die gewünschten Kategorien.

So fügen Sie eine Kategorie hinzu:

1. Klicken Sie im Security in der Menü-Übersicht von Security Manager auf **Password Manager**.
2. Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Kategorie hinzufügen**.
3. Geben Sie einen Namen für die Kategorie ein.
4. Klicken Sie auf **OK**.

So fügen Sie Anmeldedaten einer Kategorie hinzu:

1. Platzieren Sie den Mauszeiger über den gewünschten Anmeldedaten.
2. Halten Sie die linke Maustaste gedrückt.
3. Ziehen Sie die Anmeldedaten auf die Liste der Kategorien. Die Kategorien werden hervorgehoben, wenn Sie die Maus darüberziehen.
4. Lassen Sie die Maustaste los, wenn die gewünschte Kategorie hervorgehoben wird.

Ihre Anmeldedaten werden nicht in die ausgewählte Kategorie verschoben, sondern lediglich dorthin kopiert. Sie können dieselben Anmeldedaten zu mehreren Kategorien hinzufügen und alle Ihre Anmeldedaten anzeigen, indem Sie auf **Alle** klicken.

Verwalten Ihrer Anmeldedaten

Mit Password Manager können Sie ganz einfach Ihre Anmeldedaten für Benutzernamen, Kennwörter und mehrere Anmeldekonten von einer zentralen Stelle aus verwalten.

Ihre Anmeldedaten werden auf der Registerkarte „Verwalten“ aufgeführt. Wenn mehrere Anmeldedaten für dieselbe Website erstellt wurden, werden die einzelnen Anmeldedaten unter dem Website-Namen aufgelistet und in der Anmeldeliste eingerückt.

So verwalten Sie Ihre Anmeldedaten:

Klicken Sie im Security in der Menü-Übersicht von Security Manager auf **Password Manager** und anschließend auf die Registerkarte **Verwalten**.

- **Anmeldedaten hinzufügen** – Klicken Sie auf **Anmeldedaten hinzufügen**, und folgen Sie den Anleitungen auf dem Bildschirm.
- **Anmeldedaten bearbeiten** – Klicken Sie auf die gewünschten Anmeldedaten, klicken Sie auf **Bearbeiten**, und ändern Sie dann die Anmeldedaten.
- **Anmeldedaten löschen** – Klicken Sie auf die gewünschten Anmeldedaten und anschließend auf **Löschen**.

So fügen Sie zusätzliche Anmeldedaten für eine Website oder ein Programm hinzu:

1. Öffnen Sie den Anmeldebildschirm für die Website oder das Programm.
2. Klicken Sie auf das **Password Manager**-Symbol, um das Kontextmenü anzuzeigen.
3. Klicken Sie auf **Zusätzliche Anmeldedaten hinzufügen**, und folgen Sie den Anleitungen auf dem Bildschirm.

Festlegen der Kennwortsicherheit

Das Verwenden von Kennwörtern mit hoher Sicherheit für die Anmeldung bei Ihren Programmen und Websites stellt einen wichtigen Aspekt beim Schutz Ihrer Identität dar.

Password Manager analysiert sofort und automatisch die Sicherheit der Kennwörter, die Sie zum Anmelden bei Websites und Programmen verwenden, und ermöglicht auf diese Weise eine einfache Überwachung und Verbesserung Ihrer Sicherheit.

Einstellungen für das Password Manager Symbol

Password Manager versucht, Anmeldebildschirme für Websites und Programe zu ermitteln. Wenn ein Anmeldebildschirm erkannt wird, für den Sie noch keine Anmeldedaten erstellt haben, fordert Sie Password Manager auf, Anmeldedaten für diesen Bildschirm zu erstellen, indem das Password Manager Symbol mit einem Pluszeichen angezeigt wird.

Klicken Sie auf das Pfeilsymbol und anschließend auf **Symboleinstellungen**, um festzulegen, wie **Password Manager** mögliche Anmelde-Sites behandelt.

- **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern** – Klicken Sie auf diese Option, wenn Sie möchten, dass Password Manager Sie zum Erstellen von Benutzerdaten auffordert, wenn ein Anmeldebildschirm angezeigt wird, für den noch keine Anmeldedaten eingerichtet sind.
- **Diesen Bildschirm ausschließen** – Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht erneut von Password Manager aufgefordert werden möchten, Anmeldedaten für diesen Anmeldebildschirm zu erstellen.

Für den Zugriff auf weitere Password Manager Einstellungen klicken Sie auf **Password Manager** und anschließend in der Menü-Übersicht von Security Manager auf **Einstellungen**.

Einstellungen

Sie können Einstellungen zur Personalisierung von HP ProtectTools Security Manager vornehmen:

1. **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern** – Das Password Manager Symbol wird immer dann mit einem Pluszeichen angezeigt, wenn der Anmeldebildschirm einer Website oder eines Programms erkannt wird. Dies zeigt an, dass Sie Anmeldedaten für diesen Bildschirm im Kennwortspeicher hinterlegen können. Um diese Funktion zu deaktivieren, deaktivieren Sie im Dialogfeld **Symboleinstellungen** das Kontrollkästchen neben der Option **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern**.

2. **Password Manager mit strg+alt+h öffnen** – Die Standardtastenkombination zum Öffnen des Password Manager Verknüpfungsmenüs lautet strg+alt+h. Zum Ändern der Tastenkombination klicken Sie auf diese Option, und geben Sie eine neue Tastenkombination ein. Die Kombinationen können sich aus folgenden Elementen zusammensetzen: strg, alt oder umschalttaste plus eine beliebige Buchstaben- oder Zifferntaste.

3. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Anmeldedaten

Mit den Security Manager Anmeldedaten weisen Sie Ihre Identität nach. Der lokale Administrator dieses Computers kann einstellen, mit welchen Anmeldedaten Sie Ihre Identität beim Anmelden bei Ihrem Windows Konto, bei Websites oder Programmen nachweisen können.

Die verfügbaren Anmeldedaten können je nach integrierten oder an den Computer angeschlossenen Sicherheitsgeräten variieren. Für alle unterstützten Anmeldedaten wird ein Eintrag in der Gruppe **Meine Identität, Anmeldedaten** erstellt.

Es werden die verfügbaren Anmeldedaten, die Anforderungen und der aktuelle Status aufgeführt:

- Fingerabdrücke
- Kennwort
- Smart Card

Um Anmeldedaten festzulegen oder zu ändern, klicken Sie auf den Link, und folgen Sie den Anleitungen auf dem Bildschirm.

Ihre persönliche ID-Card

Ihre ID-Card identifiziert Sie eindeutig als den Eigentümer dieses Windows Kontos und zeigt Ihren Namen und ein Bild Ihrer Wahl an. Sie wird oben links auf den Security Manager Seiten und als Windows Randleisten-Minianwendung angezeigt.

Das Anklicken Ihrer ID-Card in der Windows Randleiste ist nur eine von vielen Möglichkeiten zum schnellen Aufrufen von Security Manager.

Sie können das Bild und die Art der Anzeige Ihres Namens ändern. Standardmäßig werden Ihr vollständiger Windows Benutzername und das Bild angezeigt, das Sie bei der Windows Einrichtung ausgewählt haben.

So ändern Sie den angezeigten Namen:

1. Klicken Sie im in der Menü-Übersicht von Security Manager oben links auf **ID-Card**.
2. Klicken Sie auf das Feld mit dem Namen, den Sie für Ihr Konto in Windows eingegeben haben. Das System zeigt Ihren Windows Benutzernamen für dieses Konto an.
3. Zum Ändern dieses Namens geben Sie den neuen Namen ein, und klicken Sie anschließend auf die Schaltfläche **Speichern**.

So ändern Sie das angezeigte Bild:

1. Klicken Sie in der Menü-Übersicht von Security Manager auf **Meine Identität** und anschließend oben links auf **ID-Card**.
2. Klicken Sie auf die Schaltfläche **Bild wählen**, klicken Sie auf ein Bild, und klicken Sie anschließend auf die Schaltfläche **Speichern**.

Festlegen der Einstellungen

Sie können die Einstellungen für HP ProtectTools Security Manager personalisieren. Klicken Sie in der Menü-Übersicht von Security Manager auf **Erweitert** und anschließend auf **Voreinstellungen**. Die verfügbaren Einstellungen werden auf zwei Registerkarten angezeigt: „Allgemein“ und „Fingerabdruck“.

Allgemein

Die folgenden Einstellungen stehen auf der Registerkarte „Allgemein“ zur Verfügung:

Darstellung – Symbol in der Taskleiste anzeigen

Um die Funktion zum Anzeigen des Symbols in der Taskleiste zu aktivieren, aktivieren Sie dieses Kontrollkästchen.

Um die Funktion zum Anzeigen des Symbols in der Taskleiste zu deaktivieren, deaktivieren Sie dieses Kontrollkästchen.

Fingerabdruck

Die folgenden Einstellungen stehen auf der Registerkarte „Fingerabdruck“ zur Verfügung:

Schnellaktionen – Hiermit können Sie die Security Manager Aufgaben auswählen, die ausgeführt werden sollen, wenn Sie beim Scannen Ihres Fingerabdrucks eine bestimmte Taste gedrückt halten.

So weisen Sie einer der aufgeführten Tasten eine Schnellaktion zu:

- Klicken Sie auf eine **(Taste)+Fingerabdruck**-Option und anschließend auf eine der verfügbaren Aufgaben aus dem Menü.

Fingerabdruckscan-Feedback – Wird nur angezeigt, wenn ein Fingerabdruck-Lesegerät verfügbar ist. Verwenden Sie diese Einstellung, um die Rückmeldung anzupassen, die erfolgt, wenn Sie Ihren Fingerabdruck scannen.

- **Sound-Feedback aktivieren** – Security Manager gibt akustische Signale aus, wenn ein Fingerabdruck gescannt wurde, wobei für spezifische Programmereignisse verschiedene Signale verwendet werden. Sie können diesen Ereignissen über die Registerkarte „Sounds“ in der Windows Systemsteuerung neue Signale zuweisen oder die akustischen Signale ausschalten, indem Sie diese Option deaktivieren.
- **Feedback zur Scanqualität anzeigen** – Security Manager zeigt standardmäßig ein Bild eines Fingerabdrucks mit einem Fragezeichen an, wenn die Qualität eines Fingerabdrucks nicht zur Authentifizierung ausreicht. Sie können die Anzeige dieses Bildes deaktivieren, indem Sie diese Option deaktivieren.

Sichern und Wiederherstellen Ihrer Daten

Es wird empfohlen, regelmäßig eine Sicherungskopie der Security Manager Daten zu erstellen. Wie oft dies erforderlich ist, hängt davon ab, wie häufig sich die Daten ändern. Wenn Sie beispielsweise täglich neue Anmeldedaten hinzufügen, sollten Sie Ihre Daten auch täglich sichern.

Sicherungskopien können auch für die Migration von einem Computer auf einen anderen verwendet werden (importieren und exportieren).

HINWEIS: Mit dieser Funktion werden nur die Daten gesichert.

HP ProtectTools Security Manager muss auf jedem Computer installiert werden, auf dem gesicherte Daten gespeichert werden sollen, andernfalls können die Daten aus der Sicherungskopie nicht wiederhergestellt werden.

So sichern Sie Ihre Daten:

1. Klicken Sie auf der linken Seite auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
2. Klicken Sie auf **Daten sichern**.
3. Wählen Sie die Module aus, die gesichert werden sollen. In den meisten Fällen empfiehlt es sich, alle Module auszuwählen.
4. Geben Sie einen Namen für die Speicherdatei ein. Die Datei wird standardmäßig im Ordner „Eigene Dateien“ gespeichert. Klicken Sie auf **Durchsuchen**, um einen anderen Speicherort anzugeben.
5. Geben Sie ein Kennwort ein, um die Datei zu schützen.
6. Bestätigen Sie Ihre Identität.
7. Klicken Sie auf **Fertig stellen**.

So stellen Sie Ihre Daten wieder her:

1. Klicken Sie auf der linken Seite auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
2. Klicken Sie auf **Daten wiederherstellen**.
3. Wählen Sie die zuvor erstellte Speicherdatei aus. Sie können den Pfad in das entsprechende Feld eingeben oder auf **Bearbeiten** klicken.
4. Geben Sie das zuvor verwendete Kennwort zum Schützen der Datei ein.
5. Wählen Sie die Module aus, deren Daten wiederhergestellt werden sollen. In den meisten Fällen empfiehlt es sich, alle aufgelisteten Module auszuwählen.
6. Klicken Sie auf **Fertig stellen**.

Hinzufügen von Anwendungen

Es stehen möglicherweise zusätzliche Anwendungen zur Verfügung, die neue Funktionen für dieses Programm bereitstellen.

Klicken Sie in der Menü-Übersicht von Security Manager auf **[+] Weitere Anwendungen**, um nach zusätzlichen Anwendungen zu suchen.

HINWEIS: Wenn unten links in der Menü-Übersicht der Link **[+] Weitere Anwendungen** nicht angezeigt wird, dann wurde er vom Administrator dieses Computers deaktiviert.

Status der Sicherheitsanwendungen

Auf der Seite mit dem Status der Security Manager Anwendungen wird der Gesamtstatus Ihrer installierten Sicherheitsanwendungen angezeigt. Es werden die eingerichteten Anwendungen und deren jeweiliger Status angezeigt. Die Übersicht wird automatisch angezeigt, wenn Sie die Menü-Übersicht von Security Manager oder auf **Sicherheitsanwendungen** klicken.

7 Drive Encryption for HP ProtectTools (bestimmte Modelle)

△ **ACHTUNG:** Wenn Sie das Drive Encryption Modul deinstallieren möchten, müssen Sie zuerst alle verschlüsselten Laufwerke entschlüsseln. Anderenfalls können Sie auf die Daten auf den verschlüsselten Laufwerken erst dann wieder zugreifen, wenn Sie sich beim Dienst zur Schlüsselwiederherstellung von Drive Encryption registrieren. Eine erneute Installation des Drive Encryption Moduls allein ermöglicht Ihnen keinen Zugriff auf die verschlüsselten Laufwerke.

Drive Encryption for HP ProtectTools bietet eine umfassende Datenschutzlösung durch Verschlüsselung der Festplatte Ihres Computers. Wenn Drive Encryption aktiviert ist, müssen Sie sich auf dem Drive Encryption Anmeldebildschirm anmelden, der vor dem Starten des Windows® Betriebssystems angezeigt wird.

Mit dem Installations-Assistenten für HP ProtectTools können Windows Administratoren Drive Encryption aktivieren, den Chiffrierschlüssel sichern, Benutzer hinzufügen und entfernen sowie Drive Encryption deaktivieren. Weitere Informationen finden Sie in der Hilfe zur HP ProtectTools Security Manager Software.

Die folgenden Aufgaben können mit Drive Encryption durchgeführt werden:

- Verschlüsselungsverwaltung
  - Verschlüsseln oder Entschlüsseln einzelner Laufwerke

    HINWEIS: Nur interne Festplatten können verschlüsselt werden.
- Wiederherstellung
  - Erstellen von Sicherungsschlüsseln
  - Durchführen einer Wiederherstellung

Setup-Verfahren

Aufrufen von Drive Encryption

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Drive Encryption**.

Allgemeine Aufgaben

Aktivieren von Drive Encryption

Verwenden Sie den Installations-Assistenten für HP ProtectTools, um Drive Encryption zu aktivieren.

HINWEIS: Verwenden Sie ebenfalls diesen Assistenten, um Benutzer hinzuzufügen und zu entfernen.

– ODER –

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Sicherheit**, und klicken Sie anschließend auf **Funktionen**.
3. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.
4. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die Festplatte, die verschlüsselt werden soll.
5. Schließen Sie das Speichergerät an den richtigen Steckplatz an.

   HINWEIS: Um den Verschlüsselungsschlüssel zu speichern, müssen Sie ein USB-Speichergerät im FAT32-Format verwenden.

6. Aktivieren Sie unter **Externes Speichergerät zum Sichern des Verschlüsselungsschlüssels** das Kontrollkästchen für das Speichergerät, auf dem der Verschlüsselungsschlüssel gespeichert werden soll.
7. Klicken Sie auf **Übernehmen**.

   Die Verschlüsselung wird gestartet.

Weitere Informationen finden Sie in der Hilfe zur HP ProtectTools Security Manager Software.

Deaktivieren von Drive Encryption

Verwenden Sie den Installations-Assistenten für HP ProtectTools, um Drive Encryption zu deaktivieren. Weitere Informationen finden Sie in der Hilfe zur HP ProtectTools Security Manager Software.

– ODER –

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Sicherheit** und anschließend auf **Funktionen**.
3. Deaktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Übernehmen**.

   Die Entschlüsselung wird gestartet.

Anmelden, nachdem Drive Encryption aktiviert wurde

Wenn Sie den Computer einschalten, nachdem Drive Encryption aktiviert und Ihr Benutzerkonto registriert wurde, müssen Sie sich beim Drive Encryption Anmeldebildschirm anmelden:

HINWEIS: Wenn der Windows Administrator Pre-Boot Security in HP ProtectTools Security Manager aktiviert hat, melden Sie sich direkt nach dem Einschalten des Computers an und nicht erst auf dem Drive Encryption Anmeldebildschirm.

1. Klicken Sie auf Ihren Benutzernamen, und geben Sie anschließend Ihr Windows Kennwort oder Ihre Java™ Card PIN ein, oder streichen Sie mit einem registrierten Finger über den Sensor.
2. Klicken Sie auf **OK**.

HINWEIS: Wenn Sie einen Wiederherstellungsschlüssel verwenden, um sich beim Drive Encryption Anmeldebildschirm anzumelden, werden Sie zusätzlich aufgefordert, auf dem Windows Anmeldebildschirm Ihren Windows Benutzernamen und das Windows Kennwort einzugeben.

Schützen Ihrer Daten durch Verschlüsselung Ihrer Festplatte

Verwenden Sie den Installations-Assistenten für HP ProtectTools, um Ihre Daten durch Verschlüsselung Ihrer Festplatte zu schützen:

1. Klicken Sie in Security Manager auf **Einführung** und anschließend auf das Symbol **Security Manager Setup**. Eine Demonstration der Security Manager Funktionen beginnt. (Sie können Security Manager auch über die Seite „Drive Encryption“ starten.)
2. Klicken Sie im linken Fensterausschnitt auf **Drive Encryption**, und klicken Sie dann auf **Verschlüsselungsverwaltung**.
3. Klicken Sie auf **Verschlüsselung ändern**.
4. Wählen Sie das Laufwerk oder die Laufwerke für die Verschlüsselung aus.

HINWEIS: Es wird dringend empfohlen, die Festplatte zu verschlüsseln.

Anzeigen der Verschlüsselungsstatus

Benutzer können den Verschlüsselungsstatus von HP ProtectTools Security Manager aus anzeigen.

HINWEIS: Änderungen am Verschlüsselungsstatus des Laufwerks müssen mithilfe von HP ProtectTools Administrator Konsole durchgeführt werden.

1. Öffnen Sie **HP ProtectTools Security Manager**.
2. Klicken Sie unter **Meine Daten** auf **Verschlüsselungsstatus**.

   Wenn Drive Encryption aktiv ist, wird für den Laufwerkstatus einer der folgenden Statuscodes angezeigt:

   - Aktiv
   - Inaktiv
   - Nicht verschlüsselt
   - Verschlüsselt
   - Wird gerade verschlüsselt
   - Wird gerade entschlüsselt

Wenn die Festplatte gerade verschlüsselt oder entschlüsselt wird, wird eine Fortschrittsanzeige mit Angabe des Fortschritts in Prozent und der noch verbleibenden Zeit bis zum Abschluss der Verschlüsselung oder Entschlüsselung angezeigt.

Erweiterte Aufgaben

Verwalten von Drive Encryption (Administrator Aufgabe)

Auf der Seite „Verschlüsselungsverwaltung“ können Administratoren den Status von Drive Encryption (Aktiv oder Inaktiv) anzeigen und ändern und den Verschlüsselungsstatus aller Festplatten auf dem Computer anzeigen.

- Wenn der Status „Inaktiv“ ist, wurde Drive Encryption noch nicht vom Windows Administrator in HP ProtectTools Security Manager aktiviert und die Festplatte wird nicht geschützt. Verwenden Sie den Installations Assistenten von HP ProtectTools Security Manager, um Drive Encryption zu aktivieren.
- Wenn der Status „Aktiv“ ist, wurde Drive Encryption aktiviert und konfiguriert. Der Status des Laufwerks ist entweder:
  - nicht verschlüsselt
  - verschlüsselt
  - wird gerade verschlüsselt
  - wird gerade entschlüsselt

Verschlüsseln oder Entschlüsseln einzelner Laufwerke

Wenn Sie eine oder mehrere Festplatten auf dem Computer verschlüsseln oder ein bereits verschlüsseltes Laufwerk entschlüsseln möchten, verwenden Sie die Funktion „Verschlüsselung ändern“.

1. Öffnen Sie die **HP ProtectTools Administrator Konsole**, klicken Sie auf **Drive Encryption** und anschließend auf **Verschlüsselungsverwaltung**.
2. Klicken Sie auf **Verschlüsselung ändern**.
3. Aktivieren oder deaktivieren Sie im Dialogfeld „Verschlüsselung ändern“ das Kontrollkästchen neben den einzelnen Festplatten, die Sie verschlüsseln oder entschlüsseln möchten, und klicken Sie dann auf **OK**.

HINWEIS: Wenn das Laufwerk verschlüsselt oder entschlüsselt wird, zeigt die Fortschrittsanzeige die Zeit an, die in der aktuellen Sitzung bis zum Abschließen des Vorgangs verbleibt. Wenn der Computer während des Verschlüsselungsvorgangs heruntergefahren wird oder in den Energiesparmodus oder Ruhezustand wechselt und dann neu gestartet wird, wird die Anzeige der verbleibenden Zeit zwar zurückgesetzt, die eigentliche Verschlüsselung jedoch dort fortgesetzt, wo sie unterbrochen wurde. Die Anzeige der verbleibenden Zeit und des Fortschritts ändert sich schneller, um den bisherigen Fortschritt wiederzugeben.

Sicherung und Wiederherstellung (Administrator Aufgabe)

Auf der Seite „Wiederherstellung“ können Administratoren Verschlüsselungsschlüssel sichern und wiederherstellen.

Lokales Backup des Drive Encryption Schlüssels – Ermöglicht es Ihnen, während der Aktivierung von Drive Encryption Verschlüsselungsschlüssel auf Wechselmedien zu sichern.

Erstellen von Sicherungsschlüsseln

Sie können den Verschlüsselungsschlüssel für ein verschlüsseltes Laufwerk auf einem Wechselmediengerät speichern:

△ **ACHTUNG:** Bewahren Sie das Speichergerät, auf dem sich der Sicherungsschlüssel befindet, an einem sicheren Ort auf, da dieses Gerät den einzigen Zugang zu Ihrer Festplatte ermöglicht, wenn Sie Ihr Kennwort vergessen oder Ihre Java Card verloren haben.

1. Öffnen Sie die **HP ProtectTools Administrator Konsole**, klicken Sie auf **Drive Encryption** und anschließend auf **Wiederherstellung**.
2. Klicken Sie auf **Schlüssel sichern**.
3. Aktivieren Sie auf der Seite „Backup Datenträger auswählen“ das Kontrollkästchen für das Gerät, auf dem Sie Ihren Verschlüsselungsschlüssel sichern möchten, und klicken Sie dann auf **Weiter**.
4. Lesen Sie die Informationen auf der daraufhin angezeigten Seite, und klicken Sie auf **Weiter**. Der Verschlüsselungsschlüssel wird auf dem ausgewählten Speichergerät gesichert.
5. Klicken Sie im Bestätigungsdialogfeld auf **Fertig stellen**.

Wiederherstellen des Systems

Gehen Sie folgendermaßen vor, um Ihr System wiederherzustellen, wenn Sie Ihr Kennwort vergessen haben:

1. Schalten Sie den Computer ein.
2. Schließen Sie das Wechselmediengerät an, das Ihren Sicherungsschlüssel enthält.
3. Klicken Sie im Anmeldedialogfeld für Drive Encryption for HP ProtectTools auf **Abbrechen**.
4. Klicken Sie in der unteren rechten Bildschirmecke auf **Optionen** und danach auf **Wiederherstellung**.
5. Wählen Sie die Datei aus, die Ihren Sicherungsschlüssel enthält, oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen, und klicken Sie danach auf **Weiter**.
6. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Ihr Computer wird gestartet.

HINWEIS: Nach der Wiederherstellung sollten Sie Ihr Kennwort unbedingt zurücksetzen.

8 Privacy Manager for HP ProtectTools (bestimmte Modelle)

Mit Privacy Manager for HP ProtectTools können Sie Anmeldemethoden (Authentifizierung) für erhöhte Sicherheit verwenden, um die Quelle, Integrität und Sicherheit für E-Mails, Microsoft® Office Dokumente oder Instant Messages (IM) zu überprüfen.

Privacy Manager ergänzt die Sicherheitsinfrastruktur von HP ProtectTools Security Manager, die die folgenden Sicherheits Anmeldemethoden umfasst:

- Fingerabdruck Authentifizierung
- Windows® Kennwort
- HP ProtectTools Java™ Card

Sie können jede der vorstehend genannten Sicherheits Anmeldemethoden in Privacy Manager verwenden.

Privacy Manager setzt voraus:

- HP ProtectTools Security Manager 5.00 oder höher
- Windows® 7, Windows Vista® oder Windows XP als Betriebssystem
- Microsoft Outlook 2007 oder Microsoft Outlook 2003
- Ein gültiges E Mail Konto

HINWEIS: Für den Zugriff auf die Sicherheitsfunktionen muss in Privacy Manager ein Privacy Manager Zertifikat (ein digitales Zertifikat) angefordert und installiert werden. Informationen zum Anfordern eines Privacy Manager Zertifikats finden Sie unter „Anfordern und Installieren eines Privacy Manager Zertifikats“ auf Seite 43.

Setup Verfahren

Aufrufen von Privacy Manager

So öffnen Sie Privacy Manager:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie auf **Privacy Manager**:

– ODER –

Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **Privacy Manager** und dann auf **Konfiguration**

– ODER –

Klicken Sie in Microsoft Outlook in der Symbolleiste einer E Mail Nachricht neben **Sicher senden** auf den Pfeil nach unten und anschließend auf **Zertifikate** oder **Vertrauenswürdige Kontaktpersonen**.

– ODER –

Klicken Sie in der Symbolleiste eines Microsoft Office Dokuments neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Zertifikate** oder **Vertrauenswürdige Kontaktpersonen**.

Verwalten von Privacy Manager Zertifikaten

Privacy Manager Zertifikate schützen Daten und Nachrichten mithilfe der Verschlüsselungstechnik PKI (Public Key Infrastructure). Für diese Verschlüsselungstechnik benötigen die Benutzer Verschlüsselungsschlüssel und ein Privacy Manager Zertifikat, das von einer Zertifizierungsstelle (CA) ausgestellt wird. Im Gegensatz zu den meisten Datenverschlüsselungs und Authentifizierungsprogrammen, die lediglich eine regelmäßige Authentifizierung verlangen, erfordert Privacy Manager für jede Signierung einer E-Mail Nachricht oder eines Microsoft Office Dokuments eine Authentifizierung mit einem Verschlüsselungsschlüssel. Privacy Manager garantiert das sichere Speichern und Senden wichtiger Informationen.

Sie können folgende Aufgaben ausführen:

- Anfordern und Installieren eines Privacy Manager Zertifikats
- Anzeigen von Details eines Privacy Manager Zertifikats
- Erneuern von Privacy Manager Zertifikaten
- Legen Sie bei Verfügbarkeit mehrerer Zertifikate ein Privacy Manager Standardzertifikat fest, das Privacy Manager verwenden soll
- Löschen und Widerrufen eines Privacy Manager Zertifikats (erweitert)

Anfordern und Installieren eines Privacy Manager Zertifikats

Bevor Sie die Funktionen von Privacy Manager nutzen können, müssen Sie (in Privacy Manager) unter Angabe einer gültigen E-Mail-Adresse ein Privacy Manager Zertifikat anfordern und installieren. Die E-Mail-Adresse muss als Konto in Microsoft Outlook auf demselben Computer eingerichtet sein, auf dem Sie das Privacy Manager Zertifikat anfordern.

Anfordern eines Privacy Manager Zertifikats

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Zertifikate**.
2. Klicken Sie auf **Privacy Manager Zertifikat anfordern**.
3. Lesen Sie den Text auf der Willkommensseite, und klicken Sie dann auf **Weiter**.
4. Lesen Sie den Lizenzvertrag auf der Seite „License Agreement“ (Lizenzvertrag).
5. Markieren Sie das Kontrollkästchen neben **Bedingungen dieses Lizenzvertrags akzeptieren**, und klicken Sie anschließend auf **Weiter**.
6. Geben Sie auf der Seite „Ihre Zertifikatdetails“ die verlangten Informationen ein, und klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite „Zertifikatanforderung akzeptiert“ auf **Beenden**.
8. Klicken Sie auf **OK**, um das Zertifikat zu schließen.

Sie erhalten eine E-Mail in Microsoft Outlook, in deren Anhang Sie Ihr Privacy Manager Zertifikat finden.

Erhalten eines vorab zugewiesenen Privacy Manager Unternehmenszertifikats

1. Öffnen Sie in Outlook die E-Mail, in der Sie darüber informiert wurden, dass Ihnen ein Unternehmenszertifikat vorab zugewiesen wurde.
2. Klicken Sie auf **Abrufen**.
3. Sie erhalten eine E-Mail in Microsoft Outlook, in deren Anhang Sie Ihr Privacy Manager Zertifikat finden.
4. Um das Zertifikat zu installieren, lesen Sie den Abschnitt „Installieren eines Privacy Manager Zertifikats“ auf Seite 44.

Installieren eines Privacy Manager Zertifikats

1. Wenn Sie die E-Mail mit Ihrem Privacy Manager Zertifikat erhalten haben, öffnen Sie sie, und klicken Sie auf die Schaltfläche **Setup**. Diese befindet sich in Outlook 2007 unten rechts und in Outlook 2003 oben links in der Nachricht.
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
3. Klicken Sie auf der Seite „Zertifikat installiert“ auf **Weiter**.
4. Geben Sie auf der Seite „Zertifikatsicherung“ einen Speicherort und einen Namen für die Sicherungsdatei ein, oder klicken Sie auf **Durchsuchen**, um nach einem Speicherort zu suchen.

   △ **ACHTUNG:** Speichern Sie die Datei nicht auf der Festplatte, und bewahren Sie das Speichermedium an einem sicheren Platz auf. Diese Datei ist ausschließlich zu Ihrer Verwendung bestimmt und wird benötigt, wenn Sie Ihr Privacy Manager Zertifikat und die zugehörigen Schlüssel wiederherstellen müssen.

5. Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.
6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
7. Wenn Sie den Einladungsprozess für eine vertrauenswürdige Kontaktperson starten möchten, befolgen Sie die Anleitungen auf dem Bildschirm, die mit Schritt 2 des Abschnitts „Hinzufügen von

vertrauenswürdigen Kontaktpersonen unter Verwendung der Microsoft Outlook Kontakte“ auf Seite 48 beginnen.

– ODER –

Wenn Sie auf **Abbrechen** klicken, lesen Sie unter „Hinzufügen einer vertrauenswürdigen Kontaktperson“ auf Seite 47 nach, wie Sie zu einem späteren Zeitpunkt eine vertrauenswürdige Kontaktperson hinzufügen können.

Anzeigen von Details eines Privacy Manager Zertifikats

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Zertifikate**.
2. Klicken Sie auf ein Privacy Manager Zertifikat.
3. Klicken Sie auf **Zertifikatdetails**.
4. Klicken Sie auf **OK**, um die Anzeige der Details zu schließen.

Erneuern eines Privacy Manager Zertifikats

Wenn das Ablaufdatum für Ihr Privacy Manager Zertifikat kurz bevorsteht, werden Sie darüber informiert, dass Sie es erneuern müssen:

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Zertifikate**.
2. Klicken Sie auf **Zertifikat erneuern**.
3. Befolgen Sie die Anleitungen auf dem Bildschirm, um ein neues Privacy Manager Zertifikat zu erwerben.

HINWEIS: Der Erneuerungsprozess für das Privacy Manager Zertifikat ersetzt nicht Ihr altes Privacy Manager Zertifikat. Sie müssen ein neues Privacy Manager Zertifikat erwerben und wie unter „Anfordern und Installieren eines Privacy Manager Zertifikats“ auf Seite 43 beschrieben installieren.

Festlegen eines Privacy Manager Standardzertifikats

In Privacy Manager sind nur Privacy Manager Zertifikate sichtbar, auch wenn weitere Zertifikate anderer Zertifizierungsstellen auf dem Computer installiert sind.

Wenn auf Ihrem Computer mehrere Privacy Manager Zertifikate vorhanden sind, die in Privacy Manager installiert wurden, können Sie eines dieser Zertifikate als Standardzertifikat festlegen:

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Zertifikate**.
2. Klicken Sie auf das Privacy Manager Zertifikat, das als Standardzertifikat verwendet werden soll, und klicken Sie anschließend auf **Als Standard festlegen**.
3. Klicken Sie auf **OK**.

HINWEIS: Sie sind nicht verpflichtet, das Privacy Manager Standardzertifikat zu verwenden. Innerhalb der verschiedenen Funktionen von Privacy Manager können Sie aus Ihren Privacy Manager Zertifikaten ein beliebiges Zertifikat zur Verwendung auswählen.

Löschen eines Privacy Manager Zertifikats

Wenn Sie ein Privacy Manager Zertifikat löschen, können Sie die Dateien nicht mehr öffnen oder die Daten nicht mehr anzeigen, die Sie mit diesem Zertifikat verschlüsselt haben. Wenn Sie versehentlich

ein Privacy Manager Zertifikat gelöscht haben, können Sie es mithilfe der Backup-Datei wiederherstellen, die Sie während der Installation des Zertifikats erstellt haben. Weitere Informationen finden Sie unter „Wiederherstellen eines Privacy Manager Zertifikats“ auf Seite 46.

So löschen Sie ein Privacy Manager Zertifikat:

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Zertifikate**.
2. Klicken Sie auf das Privacy Manager Zertifikat, das gelöscht werden soll, und anschließend auf **Erweitert**.
3. Klicken Sie auf **Löschen**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.
5. Klicken Sie auf **Schließen** und dann auf **Übernehmen**.

Wiederherstellen eines Privacy Manager Zertifikats

Bei der Installation des Privacy Manager Zertifikats müssen Sie eine Sicherungskopie des Zertifikats erstellen. Sie können auch von der Migrationsseite aus eine Sicherungskopie erstellen. Diese Sicherungskopie kann verwendet werden, wenn Sie die Anwendung auf einen anderen Computer migrieren oder ein Zertifikat auf demselben Computer wiederherstellen.

1. Öffnen Sie **Privacy Manager**, und klicken Sie auf **Migration**.
2. Klicken Sie auf **Wiederherstellen**.
3. Klicken Sie auf der Seite „Migrationsdatei“ auf **Durchsuchen**, um nach der Datei mit der Erweiterung DPPSM zu suchen, die Sie während des Sicherungsprozesses erstellt haben, und klicken Sie auf **Weiter**.
4. Geben Sie das Kennwort ein, das Sie beim Erstellen der Sicherungsdatei verwendet haben, und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Fertig stellen**.
6. Klicken Sie auf **OK**.

Weitere Informationen finden Sie unter „Installieren eines Privacy Manager Zertifikats“ auf Seite 44 oder „Sichern von Privacy Manager Zertifikaten und vertrauenswürdigen Kontaktpersonen“ auf Seite 62.

Widerrufen Ihres Privacy Manager Zertifikats

Wenn Sie das Gefühl haben, dass die Sicherheit Ihres Privacy Manager Zertifikats nicht mehr gewährleistet ist, können Sie Ihr eigenes Zertifikat widerrufen:

HINWEIS: Ein widerrufenes Privacy Manager Zertifikat ist nicht gelöscht. Das Zertifikat kann immer noch verwendet werden, um verschlüsselte Dateien anzuzeigen.

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Zertifikate**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf das Privacy Manager Zertifikat, das widerrufen werden soll, und anschließend auf **Widerrufen**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

5. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

6. Folgen Sie den Anleitungen auf dem Bildschirm.

Verwalten von vertrauenswürdigen Kontaktpersonen

Vertrauenswürdige Kontaktpersonen sind Benutzer, mit denen Sie Privacy Manager Zertifikate ausgetauscht haben, sodass Sie sicher mit ihnen kommunizieren können.

Mit dem vertrauenswürdigen Kontaktpersonen Manager können Sie folgende Aufgaben ausführen:

- Anzeigen von Details zu Vertrauenswürdige Kontaktpersonen
- Löschen von vertrauenswürdigen Kontaktpersonen
- Prüfen des Widerruf-Status für vertrauenswürdigen Kontaktpersonen (erweitert)

Hinzufügen von Vertrauenswürdige Kontaktpersonen

Das Hinzufügen von vertrauenswürdigen Kontaktpersonen erfolgt in drei Schritten:

1. Sie senden per E-Mail eine Einladung an einen Trusted Contact-Empfänger.
2. Der Trusted Contact-Empfänger antwortet auf die E-Mail.
3. Sie erhalten eine E-Mail-Antwort von dem Trusted Contact-Empfänger und klicken auf **Akzeptieren**.

Sie können per E-Mail Trusted Contact-Einladungen an einzelne Empfänger oder an alle Kontakte in Ihrem Microsoft Outlook-Adressbuch senden.

Nachstehend erfahren Sie, wie Sie vertrauenswürdigen Kontaktpersonen hinzufügen.

HINWEIS: Um auf Ihre Einladung antworten zu können und Empfänger der Einladung zu werden, muss auf den Computern der Empfänger der Einladung Privacy Manager oder der alternative Client installiert sein. Informationen zur Installation des alternativen Clients finden Sie auf der Website von DigitalPersona unter http://DigitalPersona.com/PrivacyManager.

Hinzufügen einer vertrauenswürdigen Kontaktperson

1. Öffnen Sie **Privacy Manager**, klicken Sie auf **vertrauenswürdigen Kontaktpersonen Manager** und anschließend auf **Kontakte einladen**.

   – ODER –

   Klicken Sie in Microsoft Outlook neben **Sicher senden** in der Symbolleiste auf den Pfeil nach unten und anschließend auf **Kontakte einladen**.

2. Nach dem Öffnen des Dialogfelds **Zertifikat auswählen** klicken Sie auf das Privacy Manager Zertifikat, das Sie verwenden möchten. Klicken Sie abschließend auf **OK**.

3. Lesen Sie den Text im Dialogfeld **Einladung an vertrauenswürdige Kontaktperson(en)**, und klicken Sie dann auf **OK**.

   Es wird automatisch eine E-Mail erzeugt.

4. Geben Sie die E-Mail-Adressen der Empfänger ein, die Sie als vertrauenswürdigen Kontaktpersonen hinzufügen möchten.

5. Bearbeiten Sie den Text, und unterschreiben Sie mit Ihrem Namen (optional).

6. Klicken Sie auf **Senden**.

HINWEIS: Wenn Sie kein Privacy Manager Zertifikat erhalten haben, informiert Sie eine Meldung darüber, dass Sie im Besitz eines Privacy Manager Zertifikats sein müssen, um eine Anforderung vertrauenswürdiger Kontaktperson(en) senden zu können. Klicken Sie auf **OK**, um den Assistenten zum Anfordern eines Zertifikats aufzurufen. Weitere Informationen finden Sie unter „Anfordern und Installieren eines Privacy Manager Zertifikats“ auf Seite 43.

7. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

HINWEIS: Nach Erhalt muss der Empfänger der Einladung die E-Mail öffnen und unten rechts in der E-Mail auf **Akzeptieren** und anschließend, wenn das Bestätigungsdialogfeld erscheint, auf **OK** klicken.

8. Wenn Sie eine E-Mail-Antwort von einem Empfänger erhalten, der die Einladung, eine vertrauenswürdige Kontaktperson zu werden, annimmt, klicken Sie unten rechts in der E-Mail auf **Akzeptieren**.

   Ein Dialogfeld wird geöffnet, das bestätigt, dass der Empfänger erfolgreich zu Ihrer Liste der vertrauenswürdigen Kontaktpersonen hinzugefügt wurde.

9. Klicken Sie auf **OK**.

Hinzufügen von vertrauenswürdigen Kontaktpersonen unter Verwendung der Microsoft Outlook Kontakte

1. Öffnen Sie Privacy Manager, klicken Sie auf **vertrauenswürdigen Kontaktpersonen Manager** und anschließend auf **Kontakte einladen**.

   – ODER –

   Klicken Sie in Microsoft Outlook neben **Sicher senden** in der Symbolleiste auf den Pfeil nach unten und anschließend auf **Meine Outlook-Kontakte einladen**.

2. Wählen Sie nach dem Öffnen der Seite „Einladung an vertrauenswürdige Kontaktperson(en)“ die E-Mail-Adressen der Empfänger aus, die Sie als vertrauenswürdige Kontaktpersonen hinzufügen möchten, und klicken Sie anschließend auf **Weiter**.

3. Wenn die Seite „Einladung wird gesendet“ geöffnet wird, klicken Sie auf **Beenden**.

   Es wird automatisch eine E-Mail mit den ausgewählten Microsoft Outlook-E-Mail-Adressen erzeugt.

4. Bearbeiten Sie den Text, und unterschreiben Sie mit Ihrem Namen (optional).

5. Klicken Sie auf **Senden**.

HINWEIS: Wenn Sie kein Privacy Manager Zertifikat erhalten haben, informiert Sie eine Meldung darüber, dass Sie im Besitz eines Privacy Manager Zertifikats sein müssen, um eine Anforderung vertrauenswürdiger Kontaktperson(en) senden zu können. Klicken Sie auf **OK**, um den Assistenten zum Anfordern eines Zertifikats aufzurufen. Weitere Informationen finden Sie unter „Anfordern und Installieren eines Privacy Manager Zertifikats“ auf Seite 43.

6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

HINWEIS: Nach Erhalt muss der der Empfänger der Einladung die E-Mail öffnen und unten rechts in der E-Mail auf **Akzeptieren** und in dem daraufhin angezeigten Bestätigungsdialogfeld auf **OK** klicken.

7. Wenn Sie eine E-Mail-Antwort von einem Empfänger erhalten, der die Einladung, ein vertrauenswürdiger Kontakt zu werden, annimmt, klicken Sie unten rechts in der E-Mail auf **Akzeptieren**.

   Ein Dialogfeld wird geöffnet, das bestätigt, dass der Empfänger erfolgreich zu Ihrer Liste der vertrauenswürdigen Kontaktpersonen hinzugefügt wurde.

8. Klicken Sie auf **OK**.

Anzeigen von Details zu Vertrauenswürdige Kontaktpersonen

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Trusted Contact**.
2. Klicken Sie auf einen Trusted Contact.
3. Klicken Sie auf **Kontaktdetails**.
4. Klicken Sie auf **OK**, um die Anzeige der Details zu schließen.

Löschen eines Trusted Contact

1. Öffnen Sie Privacy Manager, und klicken Sie auf **eine vertrauenswürdige Kontaktperson**.
2. Klicken Sie auf eine vertrauenswürdige Kontaktperson, der gelöscht werden soll.
3. Klicken Sie auf **Kontakt löschen**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Prüfen des Widerruf-Status für eine vertrauenswürdige Kontaktperson

So stellen Sie fest, ob ein Trusted Contact sein Privacy Manager Zertifikat widerrufen hat:

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Trusted Contact**.
2. Klicken Sie auf eine vertrauenswürdige Kontaktperson.
3. Klicken Sie auf die Schaltfläche **Erweitert**.

   Das Dialogfeld **Erweiterte Trusted Contact-Verwaltung** wird geöffnet.

4. Klicken Sie auf **Auf Widerruf prüfen**.
5. Klicken Sie auf **Schließen**.

Allgemeine Aufgaben

Sie können Privacy Manager mit den folgenden Microsoft Produkten verwenden:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Verwenden von Privacy Manager in Microsoft Outlook

Wenn Privacy Manager installiert ist, wird in der Symbolleiste von Microsoft Outlook eine Privacy-Schaltfläche angezeigt. Außerdem steht in der Symbolleiste jeder Microsoft Outlook E-Mail-Nachricht die Schaltfläche „Sicher Senden“ zur Verfügung. Wenn Sie neben **Datenschutz** oder **Sicher senden** auf den Pfeil nach unten klicken, können Sie eine der folgenden Optionen auswählen:

- Signieren und senden (nur Schaltfläche „Sicher senden“) – Diese Option fügt der E-Mail eine digitale Signatur hinzu und sendet die E-Mail, nachdem Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode authentifiziert haben.
- Für vertrauenswürdige Kontaktpersonen versiegeln und senden (nur Schaltfläche „Sicher senden“) – Diese Option fügt der E-Mail eine digitale Signatur hinzu, verschlüsselt die E-Mail und sendet sie, nachdem Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode authentifiziert haben.
- Kontakte einladen – Mit dieser Option können Sie eine Einladung an vertrauenswürdige Kontaktpersonen senden. Weitere Informationen finden Sie unter „Hinzufügen einer vertrauenswürdigen Kontaktperson“ auf Seite 47.
- Meine Outlook-Kontakte einladen – Mit dieser Option können Sie eine Einladung für vertrauenswürdige Kontaktpersonen an alle Kontakte in Ihrem Microsoft Outlook Adressbuch senden. Weitere Informationen finden Sie unter „Hinzufügen von vertrauenswürdigen Kontaktpersonen unter Verwendung der Microsoft Outlook Kontakte“ auf Seite 48.
- Privacy Manager öffnen – Über die Optionen „Zertifikate“, „Vertrauenswürdige Kontaktpersonen“ und „Einstellungen“ können Sie die Software „Privacy Manager“ öffnen, um Einstellungen hinzuzufügen oder die aktuellen Einstellungen anzuzeigen oder zu ändern. Weitere Informationen finden Sie unter „Konfigurieren von Privacy Manager für Microsoft Outlook“ auf Seite 50.

Konfigurieren von Privacy Manager für Microsoft Outlook

1. Öffnen Sie **Privacy Manager**, klicken Sie auf **Einstellungen** und anschließend auf die Registerkarte **E-Mail**.

   – ODER –

   Klicken Sie in der Symbolleiste von Microsoft Outlook neben **Sicher Senden** (in Outlook 2003 **Datenschutz**) auf den Pfeil nach unten und anschließend auf **Einstellungen**.

   – ODER –

   Klicken Sie in der Symbolleiste einer Microsoft Outlook E-Mail-Nachricht neben **Sicher senden** auf den Pfeil nach unten und anschließend auf **Einstellungen**.

2. Wählen Sie die Aktionen aus, die ausgeführt werden sollen, wenn Sie eine sichere E-Mail senden, und klicken Sie anschließend auf **OK**.

Signieren und Senden einer E-Mail-Nachricht

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Schreiben Sie Ihre E-Mail-Nachricht.
3. Klicken Sie neben **Sicher senden** (in Outlook 2003 **Datenschutz**) auf den Pfeil nach unten und anschließend auf **Signieren und senden**.
4. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Versiegeln und Senden einer E-Mail-Nachricht

Versiegelte E-Mail-Nachrichten, die digital signiert und versiegelt (verschlüsselt) sind, können nur von den Personen angezeigt werden, die Sie aus Ihrer Liste der vertrauenswürdigen Kontaktpersonen ausgewählt haben.

So versiegeln und senden Sie eine E-Mail-Nachricht an eine vertrauenswürdige Kontaktperson:

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Schreiben Sie Ihre E-Mail-Nachricht.
3. Klicken Sie neben **Sicher senden** auf den Pfeil nach unten (in Outlook 2003 auf **Datenschutz**) und anschließend auf **Für vertrauenswürdige Kontaktpersonen versiegeln und senden**.
4. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Anzeigen einer versiegelten E-Mail-Nachricht

Wenn Sie eine versiegelte E-Mail-Nachricht öffnen, wird das Sicherheits-Label in der Kopfzeile der E-Mail angezeigt. Das Sicherheits-Label enthält die folgenden Informationen:

- die Anmeldeinformationen, die zur Überprüfung der Identität der Person verwendet wurden, die die E-Mail signiert hat
- das Produkt, das zur Überprüfung der Anmeldeinformationen der Person verwendet wurde, die die E-Mail signiert hat

Verwenden von Privacy Manager in einem Microsoft Office 2007 Dokument

HINWEIS: Privacy Manager kann nur mit Microsoft Office 2007 Dokumenten verwendet werden.

Nach der Installation Ihres Privacy Manager Zertifikats wird die Schaltfläche „Signieren und verschlüsseln“ rechts in der Symbolleiste aller Microsoft Word, Microsoft Excel und Microsoft PowerPoint Dokumente angezeigt. Wenn Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten klicken, können Sie eine der folgenden Optionen auswählen:

- Dokument signieren – Diese Option fügt dem Dokument Ihre digitale Signatur hinzu.
- Signaturzeile vor Signieren hinzufügen (nur Microsoft Word und Microsoft Excel) – Standardmäßig wird eine Signaturzeile hinzugefügt, wenn ein Microsoft Word oder Microsoft Excel Dokument signiert oder verschlüsselt wird. Zum Deaktivieren dieser Option klicken Sie auf **Signaturzeile vor Signieren hinzufügen**, um die Markierung aus dem Kontrollkästchen zu entfernen.
- Dokument verschlüsseln – Diese Option fügt dem Dokument Ihre digitale Signatur hinzu und verschlüsselt das Dokument.

- Verschlüsselung entfernen – Diese Option entfernt die Verschlüsselung für das Dokument.
- Privacy Manager öffnen – Über die Optionen „Zertifikate“, „Vertrauenswürdige Kontaktpersonen“ und „Einstellungen“ können Sie die Software „Privacy Manager“ öffnen, um Einstellungen hinzuzufügen oder die aktuellen Einstellungen anzuzeigen oder zu ändern. Weitere Informationen finden Sie unter „Verwalten von Privacy Manager Zertifikaten“ auf Seite 43, „Verwalten von vertrauenswürdigen Kontaktpersonen“ auf Seite 47 oder „Konfigurieren von Privacy Manager für Microsoft Office“ auf Seite 52.

Konfigurieren von Privacy Manager für Microsoft Office

1. Öffnen Sie Privacy Manager, klicken Sie auf **Einstellungen** und anschließend auf die Registerkarte **Dokumente**.

   – ODER –

   Klicken Sie in der Symbolleiste eines Microsoft Office Dokuments neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Einstellungen**.

2. Wählen Sie die Aktionen aus, die Sie konfigurieren möchten, und klicken Sie anschließend auf **OK**.

Signieren eines Microsoft Office Dokuments

1. Erstellen Sie in Microsoft Word, Microsoft Excel oder Microsoft PowerPoint ein Dokument, und speichern Sie es.
2. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Dokument signieren**.
3. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
4. Lesen Sie den Text im Bestätigungsdialogfeld, und klicken Sie dann auf **OK**.

Wenn Sie das Dokument später bearbeiten möchten, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Office** links oben auf dem Bildschirm.
2. Klicken Sie auf **Vorbereiten** und dann auf **Als abgeschlossen kennzeichnen**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**, und fahren Sie mit Ihrer Arbeit fort.
4. Wenn Sie die Bearbeitung abgeschlossen haben, signieren Sie das Dokument erneut.

Hinzufügen einer Signaturzeile beim Signieren eines Microsoft Word oder Microsoft Excel Dokuments

Mit Privacy Manager können Sie eine Signaturzeile hinzufügen, wenn Sie ein Microsoft Word oder Microsoft Excel Dokument signieren:

1. Erstellen Sie in Microsoft Word oder Microsoft Excel ein Dokument, und speichern Sie es.
2. Klicken Sie auf das Menü **Start**.
3. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Signaturzeile vor Signieren hinzufügen**.

HINWEIS: Bei aktivierter Option ist das Kontrollkästchen neben „Signaturzeile vor Signieren hinzufügen“ aktiviert. Diese Option ist standardmäßig aktiviert.

4. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Dokument signieren**.

5. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Hinzufügen empfohlener Signierer zu einem Microsoft Word oder Microsoft Excel Dokument

Sie können mehrere Signaturzeilen zu Ihrem Dokument hinzufügen, indem Sie empfohlene Signierer benennen. Ein empfohlener Signierer ist ein Benutzer, den der Eigentümer eines Microsoft Word oder Microsoft Excel Dokuments für das Hinzufügen einer Signaturzeile zu dem Dokument benennt. Bei empfohlenen Signierern kann es sich um Sie selbst oder eine andere Person handeln, die Ihr Dokument signieren soll. Wenn Sie beispielsweise ein Dokument erstellen, das von allen Mitgliedern Ihrer Abteilung signiert werden muss, können Sie für diese Benutzer am Ende der letzten Seite des Dokuments Signaturzeilen hinzufügen mit der Anleitung, das Dokument bis zu einem bestimmten Datum zu signieren.

So fügen Sie einen empfohlenen Signierer zu einem Microsoft Word oder Microsoft Excel Dokument hinzu:

1. Erstellen Sie in Microsoft Word oder Microsoft Excel ein Dokument, und speichern Sie es.

2. Klicken Sie auf das Menü **Einfügen**.

3. Klicken Sie in der Gruppe **Text** in der Symbolleiste neben **Signaturzeile** auf den Pfeil nach unten und anschließend auf **Privacy Manager Signature Provider**.

   Das Dialogfeld „Einrichten der Signatur“ wird geöffnet.

4. Geben Sie in das Feld unter **Empfohlener Signierer** den Namen des empfohlenen Signierers ein.

5. Geben Sie in das Feld unter **Anleitungen für Signierer** eine Mitteilung für diesen empfohlenen Signierer ein.

HINWEIS: Diese Mitteilung wird anstelle eines Titels angezeigt und nach dem Signieren entweder gelöscht oder durch den Titel des Benutzers ersetzt.

6. Aktivieren Sie das Kontrollkästchen **Signierungsdatum in Signaturzeile anzeigen**, um das Datum anzuzeigen.

7. Aktivieren Sie das Kontrollkästchen **Titel des Signierers in Signaturzeile anzeigen**, um den Titel anzuzeigen.

HINWEIS: Wenn die Kontrollkästchen **Signierungsdatum in Signaturzeile anzeigen** und/oder **Titel des Signierers in Signaturzeile anzeigen** nicht aktiviert sind, sind die vom Dokumenteigentümer zugewiesenen, empfohlenen Signierer nicht in der Lage, das Datum und/oder den Titel in der Signaturzeile anzuzeigen, auch wenn die Dokumenteinstellungen des betreffenden empfohlenen Signierers entsprechend konfiguriert sind.

8. Klicken Sie auf **OK**.

Hinzufügen der Signaturzeile eines empfohlenen Signierers

Wenn empfohlene Signierer das Dokument öffnen, sehen sie ihren Namen in Klammern; das bedeutet, dass ihre Signatur erforderlich ist.

So signieren Sie das Dokument:

1. Doppelklicken Sie auf die entsprechende Signaturzeile.
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

   Die Signaturzeile wird gemäß den Einstellungen angezeigt, die der Eigentümer des Dokuments festgelegt hat.

Verschlüsseln eines Microsoft Office Dokuments

Sie können ein Microsoft Office Dokument für sich und für Ihre vertrauenswürdigen Kontaktpersonen verschlüsseln. Wenn Sie ein Dokument verschlüsseln und schließen, kann das Dokument erst geöffnet werden, nachdem Sie oder die vertrauenswürdigen Kontaktpersonen, die Sie aus der Liste ausgewählt haben, sich authentifiziert haben.

So verschlüsseln Sie ein Microsoft Office Dokument:

1. Erstellen Sie in Microsoft Word, Microsoft Excel oder Microsoft PowerPoint ein Dokument, und speichern Sie es.
2. Klicken Sie auf das Menü **Start**.
3. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Dokument verschlüsseln**.

   Das Dialogfeld „Vertrauenswürdige Kontaktpersonen auswählen“ wird geöffnet.
4. Klicken Sie auf den Namen einer vertrauenswürdigen Kontaktperson, die berechtigt sein soll, das Dokument zu öffnen und seinen Inhalt anzuzeigen.

HINWEIS: Halten Sie zur Auswahl mehrerer vertrauenswürdigen Kontaktpersonen die Taste strg gedrückt, und klicken Sie auf die einzelnen Namen.

5. Klicken Sie auf **OK**.

Wenn Sie das Dokument später bearbeiten möchten, gehen Sie wie unter „Entfernen der Verschlüsselung für ein Microsoft Office Dokument“ auf Seite 54 beschrieben vor. Nach dem Entfernen der Verschlüsselung lässt sich das Dokument bearbeiten. Führen Sie die Schritte in diesem Abschnitt durch, um das Dokument erneut zu verschlüsseln.

Entfernen der Verschlüsselung für ein Microsoft Office Dokument

Wenn Sie die Verschlüsselung für ein Microsoft Office Dokument entfernen, ist weder für Sie noch für Ihre vertrauenswürdigen Kontaktpersonen eine Authentifizierung erforderlich, um das Dokument zu öffnen und seinen Inhalt anzuzeigen.

So entfernen Sie die Verschlüsselung für ein Microsoft Office Dokument:

1. Öffnen Sie ein verschlüsseltes Microsoft Word, Microsoft Excel oder Microsoft PowerPoint Dokument.
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
3. Klicken Sie auf das Menü **Start**.
4. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Verschlüsselung entfernen**.

Senden eines verschlüsselten Microsoft Office Dokuments

Sie können ein verschlüsseltes Microsoft Office Dokument an eine E-Mail-Nachricht anhängen, ohne die E-Mail selbst zu signieren oder zu verschlüsseln. Erstellen Sie dazu eine E-Mail mit einem signierten oder verschlüsselten Dokument, und versenden Sie sie – genauso, wie Sie normalerweise eine gewöhnliche E-Mail mit Anhang versenden.

Für optimale Sicherheit empfiehlt es sich jedoch, die E-Mail zu verschlüsseln, wenn ein signiertes oder verschlüsseltes Microsoft Office Dokument angehängt wird.

Gehen Sie folgendermaßen vor, um eine versiegelte E-Mail zu versenden, an die ein signiertes und/oder verschlüsseltes Microsoft Office Dokument angehängt ist:

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Schreiben Sie Ihre E-Mail-Nachricht.
3. Hängen Sie das Microsoft Office Dokument an.
4. Weitere Anleitungen finden Sie unter „Versiegeln und Senden einer E-Mail-Nachricht“ auf Seite 51.

Anzeigen eines signierten Microsoft Office Dokuments

HINWEIS: Sie müssen kein Privacy Manager Zertifikat besitzen, um ein signiertes Microsoft Office Dokument anzuzeigen.

Wenn ein signiertes Microsoft Office Dokument geöffnet ist, wird ein Symbol „Digitale Signatur“ in der Statusleiste unten im Dokumentfenster angezeigt.

1. Klicken Sie auf das Symbol **Digitale Signaturen**, um das Dialogfeld „Signaturen“ mit den Namen aller Benutzer, die das Dokument signiert haben, und dem Datum, an dem jeder Benutzer das Dokument signiert hat, anzuzeigen bzw. auszublenden.
2. Um weitere Details über jede Signatur anzuzeigen, klicken Sie mit der rechten Maustaste auf einen Namen im Dialogfeld „Signaturen“, und wählen Sie „Details“.

Anzeigen eines verschlüsselten Microsoft Office Dokuments

Zum Anzeigen eines verschlüsselten Microsoft Office Dokuments auf einem anderen Computer muss Privacy Manager auf diesem Computer installiert sein. Darüber hinaus müssen Sie das Privacy Manager Zertifikat wiederherstellen, das für die Verschlüsselung der Datei verwendet wurde.

Eine vertrauenswürdige Kontaktperson, die ein verschlüsseltes Microsoft Office Dokument anzeigen möchte, muss über ein installiertes Privacy Manager Zertifikat sowie über Privacy Manager auf ihrem Computer verfügen. Außerdem muss die vertrauenswürdige Kontaktperson vom Eigentümer des verschlüsselten Microsoft Office Dokuments ausgewählt worden sein.

Verwenden von Privacy Manager in Windows Live Messenger

Privacy Manager fügt Windows Live Messenger die folgenden Funktionen für sichere Kommunikation hinzu:

- **Secure chat** (Sicherer Chat) – Die Nachrichten werden mit SSL/TLS (Secure Sockets Layer/ Transport Layer Security) über das XML-Protokoll übertragen; das ist dieselbe Technologie, die die Sicherheit von E-Commerce-Transaktionen gewährleistet.
- **Recipient identification** (Empfängeridentifikation) – Sie können die Anwesenheit und Identität einer Person überprüfen, bevor Sie eine Nachricht senden.
- **Signierte Nachrichten** – Sie haben die Möglichkeit, Ihre Nachrichten elektronisch zu signieren. Wird dann versucht, die Nachricht zu manipulieren, wird sie als ungültig gekennzeichnet, wenn sie der Empfänger erhält.
- **Hide/show feature** (Ausblenden/Einblenden) – Sie können einige oder alle Nachrichten im Fenster „Privacy Manager Chat“ ausblenden. Es ist auch möglich, eine Nachricht zu senden, deren Inhalt ausgeblendet ist. Vor dem Anzeigen der Nachricht muss eine Authentifizierung durchgeführt werden.
- **Secure chat history** (Protokoll für sicheren Chat) – Die Protokolle Ihrer Chat-Sitzungen werden verschlüsselt, bevor sie gespeichert werden. Vor dem Anzeigen muss eine Authentifizierung durchgeführt werden.
- **Automatic locking/unlocking** (Automatisches Sperren/Entsperren) – Sie können das Fenster „Privacy Manager Chat“ sperren und entsperren oder festlegen, dass es nach einer bestimmten Dauer ohne Aktivität automatisch gesperrt wird.

Starten einer Privacy Manager Chat-Sitzung

HINWEIS: Um Privacy Manager Chat einsetzen zu können, müssen beide Parteien sowohl Privacy Manager als auch ein Privacy Manager Zertifikat installiert haben. Informationen zum Installieren eines Privacy Manager Zertifikats finden Sie unter „Anfordern und Installieren eines Privacy Manager Zertifikats“ auf Seite 43.

1. Verwenden Sie zum Starten von Privacy Manager Chat in Windows Live Messenger eines der folgenden Verfahren:

   a. Klicken Sie mit der rechten Maustaste auf einen Online-Kontakt in Live Messenger, und wählen Sie **Programm starten**.

   b. Klicken Sie auf **Chat starten**.

   – ODER –

   a. Doppelklicken Sie auf einen Online-Kontakt in Live Messenger. Klicken Sie dann auf das Menü **Liste der Programme anzeigen**.

   b. Klicken Sie auf **Action** (Aktion) und anschließend auf **Chat starten**.

   – ODER –

   a. Klicken Sie mit der rechten Maustaste im Infobereich auf das Symbol ProtectTools, klicken Sie auf **Privacy Manager for HP ProtectTools**, und wählen Sie dann **Chat starten**.

   b. Klicken Sie in Live Messenger auf **Aktionen: Programm starten**, und wählen Sie dann **Privacy Manager Chat**.

HINWEIS: Jeder der Benutzer muss in Live Messenger online sein, und die Benutzer müssen in den Live Messenger Online-Fenster der anderen Benutzer angezeigt werden. Klicken Sie auf einen Online-Benutzer, um ihn auszuwählen.

Privacy Manager sendet eine Einladung an den Kontakt, um Privacy Manager Chat zu starten. Wenn der eingeladene Kontakt die Einladung annimmt, wird das Fenster „Privacy Manager Chat“ geöffnet. Wenn der eingeladene Kontakt nicht über Privacy Manager verfügt, wird er aufgefordert, die Software herunterzuladen.

2. Klicken Sie auf **Start**, um einen sicheren Chat zu beginnen.

Konfigurieren von Privacy Manager für Windows Live Messenger

1. Klicken Sie in Privacy Manager Chat auf die Schaltfläche **Einstellungen**.

   – ODER –

   Klicken Sie in Privacy Manager auf **Einstellungen** und anschließend auf die Registerkarte **Chat**.

   – ODER –

   Klicken Sie im **Privacy Manager Protokollanzeigeprogramm** auf die Schaltfläche **Einstellungen**.

2. Um anzugeben, wie lange Privacy Manager Chat bis zum Sperren Ihrer Sitzung warten soll, wählen Sie im Feld **Sitzung sperren nach _ Minuten ohne Aktivität** einen Zahlenwert aus.

3. Zum Festlegen eines Protokollordners für Ihre Chat-Sitzungen klicken Sie auf **Durchsuchen**, um nach einem Ordner zu suchen. Klicken Sie anschließend auf **OK**.

4. Damit Ihre Sitzungen automatisch verschlüsselt und gespeichert werden, wenn Sie sie schließen, aktivieren Sie das Kontrollkästchen **Protokoll für sicheren Chat automatisch speichern**.

5. Klicken Sie auf **OK**.

Chatten im Fenster „Privacy Manager Chat“

Nach dem Start von Privacy Manager Chat wird das Fenster „Privacy Manager Chat“ in Windows Live Messenger geöffnet. Die Verwendung von Privacy Manager Chat ist ähnlich der von Windows Live Messenger, wobei die folgenden Funktionen zusätzlich im Fenster „Privacy Manager Chat“ verfügbar sind:

- **Speichern** – Klicken Sie auf diese Schaltfläche, um Ihre Chat-Sitzung in dem Ordner zu speichern, den Sie in den Konfigurationseinstellungen angegeben haben. Sie können Privacy Manager Chat auch so konfigurieren, dass automatisch jede Sitzung gespeichert wird, wenn Sie sie schließen.
- **Alles ausblenden** und **Alles anzeigen** – Klicken Sie auf die entsprechende Schaltfläche, um die Nachrichten, die im Fenster „Sichere Kommunikation“ angezeigt werden, ein- oder auszublenden. Sie können auch einzelne Nachrichten ausblenden oder anzeigen, indem Sie auf die Kopfzeile der Nachricht klicken.
- **Sind Sie da?** – Klicken Sie auf diese Schaltfläche, um Ihren Kontakt zur Authentifizierung aufzufordern.
- **Sperren** – Klicken Sie auf diese Schaltfläche, um das Fenster „Privacy Manager Chat“ zu schließen und zum für die Chat-Eingabe zurückzukehren. Zum erneuten Anzeigen des Fensters „Sichere Kommunikation“ klicken Sie auf **Sitzung fortsetzen**. Authentifizieren Sie sich anschließend mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

- **Senden** – Klicken Sie auf diese Schaltfläche, um eine verschlüsselte Nachricht an Ihren Kontakt zu senden.
- **Signiert senden** – Aktivieren Sie dieses Kontrollkästchen, um Ihre Nachrichten elektronisch zu signieren und zu verschlüsseln. Wird dann versucht, die Nachricht zu manipulieren, wird sie als ungültig gekennzeichnet, wenn sie der Empfänger erhält. Sie müssen sich jedes Mal authentifizieren, wenn Sie eine signierte Nachricht senden möchten.
- **Ausgeblendet senden** – Aktivieren Sie diese Option, um eine Nachricht zu verschlüsseln und zu senden, für die nur die Kopfzeile angezeigt wird. Ihr Kontakt muss sich authentifizieren, um den Inhalt der Nachricht lesen zu können.

Anzeigen des Chat-Protokolls

Privacy Manager Chat: Live Messenger History Viewer zeigt verschlüsselte Dateien von Privacy Manager Chat-Sitzungen an. Sie können die Sitzungen speichern, indem Sie im Fenster „Privacy Manager Chat“ auf **Speichern** klicken oder auf der Registerkarte „Chat“ in Privacy Manager die Funktion für automatisches Speichern konfigurieren. Im Protokollanzeigeprogramm von Privacy Manager Chat werden für jede Sitzung der (verschlüsselte) Anzeigename des Kontakts sowie Datum und Uhrzeit von Beginn und Ende der Sitzung angezeigt. Standardmäßig werden die Sitzungen für alle E-Mail-Konten angezeigt, die Sie eingerichtet haben. Über das Menü **Protokoll anzeigen für** können Sie bestimmte Konten zum Anzeigen auswählen.

Mit dem Protokollanzeigeprogramm von Privacy Manager Chat können Sie folgende Aufgaben ausführen:

- „Sichtbarmachen aller Sitzungen“ auf Seite 58
- „Sichtbarmachen der Sitzungen für ein bestimmtes Konto“ auf Seite 59
- „Anzeigen einer Sitzungs-ID“ auf Seite 59
- „Anzeigen einer Sitzung“ auf Seite 59
- „Durchsuchen von Sitzungen nach bestimmtem Text“ auf Seite 60
- „Löschen einer Sitzung“ auf Seite 60
- „Hinzufügen oder Entfernen von Spalten“ auf Seite 60
- „Filtern der angezeigten Sitzungen“ auf Seite 60

So starten Sie Live Messenger History Viewer:

▲ Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **Privacy Manager for HP ProtectTools** und dann auf **Live Messenger History Viewer**.

– ODER –

▲ Klicken Sie in einer Chat-Sitzung auf **Protokollanzeigeprogramm** oder **History** (Protokoll).

Sichtbarmachen aller Sitzungen

Beim Sichtbarmachen aller Sitzungen werden der entschlüsselte Anzeigename des Kontakts für die aktuell ausgewählten Sitzungen sowie alle Sitzungen im selben Konto angezeigt.

So machen Sie alle Ihre gespeicherten Chat-Protokollsitzungen sichtbar:

1. Klicken Sie in Live Messenger History Viewer mit der rechten Maustaste auf eine Sitzung, und wählen Sie dann die Option **Alle Sitzungen sichtbar machen**.
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

   Die Anzeigenamen der Kontakte sind entschlüsselt.
3. Doppelklicken Sie auf eine Sitzung, um ihren Inhalt anzuzeigen.

Sichtbarmachen der Sitzungen für ein bestimmtes Konto

Beim Sichtbarmachen einer Sitzung wird der entschlüsselte Anzeigename des Kontakts für die aktuell ausgewählte Sitzung angezeigt.

So machen Sie eine bestimmte Chat-Protokollsitzung sichtbar:

1. Klicken Sie in Live Messenger History Viewer mit der rechten Maustaste auf eine Sitzung, und wählen Sie dann die Option **Sitzung sichtbar machen**.
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

   Der Anzeigename des Kontakts ist entschlüsselt.
3. Doppelklicken Sie auf die sichtbare Sitzung, um ihren Inhalt anzuzeigen.

HINWEIS: Weitere Sitzungen, die mit demselben Zertifikat verschlüsselt wurden, sind mit einem Entsperrt-Symbol versehen. Das bedeutet, dass Sie sie mit einem Doppelklick auf diese Sitzungen ohne zusätzliche Authentifizierung anzeigen können. Sitzungen, die mit einem anderen Zertifikat verschlüsselt wurden, sind mit einem Gesperrt-Symbol versehen. Das bedeutet, dass eine weitere Authentifizierung für diese Sitzungen erforderlich ist, bevor die Anzeigenamen der Kontakte oder der Inhalt angezeigt werden können.

Anzeigen einer Sitzungs-ID

So zeigen Sie eine Sitzungs-ID an:

- Klicken Sie in Live Messenger History Viewer mit der rechten Maustaste auf eine sichtbare Sitzung, und wählen Sie die Option **Sitzungs-ID anzeigen**.

Anzeigen einer Sitzung

Beim Anzeigen einer Sitzung wird die Datei für die Anzeige geöffnet. Wenn die Sitzung nicht vorher sichtbar gemacht wurde (und der entschlüsselte Anzeigename des Kontakts angezeigt wird), wird sie gleichzeitig sichtbar gemacht.

So zeigen Sie ein Protokoll für eine Live Messenger Sitzung an:

1. Klicken Sie in Live Messenger History Viewer mit der rechten Maustaste auf eine Sitzung, und wählen Sie dann die Option **Anzeigen**.
2. Authentifizieren Sie sich nach entsprechender Aufforderung mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

   Der Sitzungsinhalt ist entschlüsselt.

Durchsuchen von Sitzungen nach bestimmtem Text

Sie können nur sichtbar gemachte (entschlüsselte) Sitzungen nach Text durchsuchen, die im Fenster des Anzeigeprogramms angezeigt werden. Bei diesen Sitzungen erscheint der Anzeigename des Kontakts als normaler Text.

So durchsuchen Sie Chat-Protokollsitzungen nach einem bestimmten Text:

1. Klicken Sie in Live Messenger History Viewer auf die Schaltfläche **Suchen**.
2. Geben Sie den Suchtext ein, konfigurieren Sie die gewünschten Suchparameter, und klicken Sie dann auf **OK**.

   Sitzungen, die den gesuchten Text enthalten, werden im Fenster des Anzeigeprogramms hervorgehoben.

Löschen einer Sitzung

1. Wählen Sie eine Chat-Protokollsitzung aus.
2. Klicken Sie auf **Löschen**.

Hinzufügen oder Entfernen von Spalten

Standardmäßig werden die drei am häufigsten verwendeten Spalten in Live Messenger History Viewer angezeigt. Sie können der Ansicht jedoch weitere Spalten hinzufügen oder Spalten aus der Ansicht entfernen.

So fügen Sie der Ansicht Spalten hinzu:

1. Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, und wählen Sie dann die Option **Spalten hinzufügen/entfernen**.
2. Markieren Sie in der linken Fensterhälfte eine Spaltenüberschrift, und klicken Sie anschließend auf **Hinzufügen**, um sie in die rechte Fensterhälfte zu verschieben.

So entfernen Sie Spalten aus der Ansicht:

1. Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, und wählen Sie dann die Option **Spalten hinzufügen/entfernen**.
2. Markieren Sie in der rechten Fensterhälfte eine Spaltenüberschrift, und klicken Sie anschließend auf **Entfernen**, um sie in die linke Fensterhälfte zu verschieben.

Filtern der angezeigten Sitzungen

In Live Messenger History Viewer wird eine Liste der Sitzungen für alle Ihre Konten angezeigt. Sie können aber auch die angezeigten Sitzungen nach den folgenden Kriterien filtern:

- Bestimmte Konten. Nähere Informationen zu diesem Thema finden Sie unter „Anzeigen der Sitzungen für ein bestimmtes Konto“ auf Seite 61.
- Datumsbereich. Nähere Informationen zu diesem Thema finden Sie unter „Anzeigen der Sitzungen für einen bestimmten Datumsbereich“ auf Seite 61.
- Verschiedene Ordner. Nähere Informationen zu diesem Thema finden Sie unter „Anzeigen der Sitzungen, die nicht im Standardordner gespeichert sind“ auf Seite 61.

Anzeigen der Sitzungen für ein bestimmtes Konto

- Wählen Sie in Live Messenger History Viewer ein Konto aus dem Menü **Protokoll anzeigen für** aus.

Anzeigen der Sitzungen für einen bestimmten Datumsbereich

1. Klicken Sie in Live Messenger History Viewer auf das Symbol **Erweiterter Filter**.

   Das Dialogfeld „Erweiterter Filter“ wird geöffnet.

2. Aktivieren Sie das Kontrollkästchen **Nur Sitzungen innerhalb des festgelegten Datumsbereichs anzeigen**.

3. Geben Sie in die Felder **Vom** und **Bis** Tag, Monat und/oder Jahr ein, oder klicken Sie auf den Pfeil neben dem Kalender, um die Datumswerte auszuwählen.

4. Klicken Sie auf **OK**.

Anzeigen der Sitzungen, die nicht im Standardordner gespeichert sind

1. Klicken Sie in Live Messenger History Viewer auf das Symbol **Erweiterter Filter**.

2. Aktivieren Sie das Kontrollkästchen **Anderen Ordner für Protokolldateien verwenden**.

3. Geben Sie den Pfad für den Ordner ein, oder klicken Sie auf **Durchsuchen**, um nach einem Ordner zu suchen.

4. Klicken Sie auf **OK**.

Erweiterte Aufgaben

Migrieren von Privacy Manager Zertifikaten und vertrauenswürdigen Kontaktpersonen auf einen anderen Computer

Sie können Ihre Privacy Manager Zertifikate und vertrauenswürdigen Kontaktpersonen sicher auf einen anderen Computer migrieren oder Sicherungskopien Ihrer Daten anlegen. Sichern Sie dazu die Privacy Manager Zertifikate und Vertrauenswürdige Kontaktpersonen als kennwortgeschützte Datei in einen Netzwerkordner oder auf einen Wechseldatenträger, und stellen Sie anschließend die Datei auf dem neuen Computer wieder her.

Sichern von Privacy Manager Zertifikaten und vertrauenswürdigen Kontaktpersonen

Gehen Sie folgendermaßen vor, um Ihre Privacy Manager Zertifikate und Vertrauenswürdige Kontaktpersonen in einer kennwortgeschützten Datei zu sichern:

1. Öffnen Sie **Privacy Manager**, und klicken Sie auf **Migration**.
2. Klicken Sie auf **Sicherung**.
3. Wählen Sie auf der Seite „Daten auswählen“ die Datenkategorien aus, die in die Migrationsdatei einbezogen werden sollen, und klicken Sie anschließend auf **Weiter**.
4. Geben Sie auf der Seite „Migrationsdatei“ einen Dateinamen ein, oder klicken Sie auf **Durchsuchen**, um nach einem Speicherort zu suchen, und klicken Sie dann auf **Weiter**.
5. Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.

HINWEIS: Bewahren Sie dieses Kennwort an einem sicheren Ort auf, da Sie zum Wiederherstellen der Migrationsdatei benötigen.

6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
7. Klicken Sie auf der Seite „Migrationsdatei gespeichert“ auf **Beenden**.

Wiederherstellen von Privacy Manager Zertifikaten und vertrauenswürdigen Kontaktpersonen

Gehen Sie folgendermaßen vor, um Ihre Privacy Manager Zertifikate und Vertrauenswürdige Kontaktpersonen als Teil des Migrationsprozesses auf einem anderen Computer oder auf demselben Computer wiederherzustellen:

1. Öffnen Sie **Privacy Manager**, und klicken Sie auf **Migration**.
2. Klicken Sie auf **Wiederherstellen**.
3. Klicken Sie auf der Seite „Migrationsdatei“ auf **Durchsuchen**, um nach der Datei zu suchen, und klicken Sie dann auf **Weiter**.
4. Geben Sie das Kennwort ein, das Sie beim Erstellen der Sicherungsdatei verwendet haben, und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite „Migrationsdatei gespeichert“ auf **Beenden**.

Zentrale Verwaltung von Privacy Manager

Bei Ihrer Installation von Privacy Manager kann es sich um einen Teil einer zentralen Installation handeln, die von Ihrem Administrator benutzerdefiniert angepasst wurde. Eine oder mehrere der folgenden Funktionen können entweder aktiviert oder deaktiviert sein:

- **Richtlinien zur Zertifikatsverwendung** – Es kann eine Beschränkung auf die Verwendung von Privacy Manager Zertifikaten vorliegen, die von Comodo ausgegeben wurden, oder Sie können zur Nutzung digitaler Zertifikate anderer Zertifizierungsstellen berechtigt sein.
- **Verschlüsselungsrichtlinien** – Verschlüsselungsfunktionen können in Microsoft Office oder Outlook und in Windows Live Messenger individuell aktiviert oder deaktiviert werden.

9 File Sanitizer for HP ProtectTools

File Sanitizer ist ein Tool, mit dem Sie Datenbestände (persönliche Daten oder Dateien, historische oder Internet-bezogene Daten sowie andere Datenkomponenten) auf Ihrem Computer sicher shreddern und regelmäßig freien Speicherplatz auf Ihrer Festplatte überschreiben können.

HINWEIS: Diese Version von File Sanitizer kann nur für die Systemfestplatte eingesetzt werden.

Shreddern

Shreddern unterscheidet sich von einem normalen Löschvorgang unter Windows® (in File Sanitizer auch als einfaches Löschen bezeichnet). Beim Shreddern eines Datenbestandes mit File Sanitizer wird ein Algorithmus aufgerufen, der die Daten unleserlich macht. Damit ist es nahezu unmöglich, den Originalbestand abzurufen. Bei einem einfachen Löschvorgang unter Windows bleibt die Datei (oder der Datenbestand) auf der Festplatte möglicherweise intakt oder so erhalten, dass sie mit forensischen Methoden wiederhergestellt werden kann.

Wenn Sie ein Shred Profil auswählen (Hohe, mittlere oder geringe Sicherheit), wird für das Shreddern automatisch eine voreingestellte Liste von Datenbeständen sowie eine Löschmethode ausgewählt. Sie können ein Shred Profil auch individuell anpassen. Dabei können Sie die Anzahl der Shred-Zyklen festlegen und angeben, welche Datenbestände geshreddert werden sollen und welche Datenbestände nur nach vorheriger Bestätigung oder überhaupt nicht geshreddert werden sollen. Weitere Informationen finden Sie unter „Auswählen oder Erstellen eines Shred Profils“ auf Seite 68.

Sie können einen Shred-Zeitplan erstellen. Datenbestände können aber auch jederzeit manuell geshreddert werden. Weitere Informationen finden Sie unter „Erstellen eines Shred-Zeitplans“ auf Seite 67, „Manuelles Shreddern eines Datenbestands“ auf Seite 72 oder „Manuelles Shreddern aller ausgewählten Datenbestände“ auf Seite 73.

HINWEIS: Eine .dll-Datei wird nur dann geshreddert und vom System entfernt, wenn sie zuvor in den Papierkorb verschoben wurde.

Überschreiben von freiem Speicherplatz

Das Löschen eines Datenbestands in Windows entfernt den Inhalt des betreffenden Datenbestands nicht vollständig von der Festplatte. Windows löscht lediglich den Verweis zu dem Datenbestand. Der Inhalt ist auch weiterhin auf der Festplatte vorhanden, bis ein anderer Datenbestand denselben Bereich auf der Festplatte mit neuen Informationen überschreibt.

Beim Überschreiben von freiem Speicherplatz werden gelöschte Datenbestände sicher mit willkürlichen Daten überschrieben, sodass die Originalinhalte nicht mehr angezeigt werden können.

HINWEIS: Durch das Überschreiben von freiem Speicherplatz können Sie die Datenbestände von der Festplatte entfernen, die Sie über den Windows Papierkorb oder manuell gelöscht haben. Das Überschreiben bietet jedoch keine zusätzliche Sicherheit für geshredderte Datenbestände.

Sie können einen Zeitplan für das automatische Überschreiben von freiem Speicherplatz erstellen oder das Überschreiben manuell mithilfe des Symbols **HP ProtectTools** aktivieren, das sich im Infobereich ganz am rechten Rand der Taskleiste befindet. Weitere Informationen finden Sie unter „Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz“ auf Seite 68 oder „Manuelles Aktivieren des Überschreibens von freiem Speicherplatz“ auf Seite 73.

Setup-Verfahren

Öffnen von File Sanitizer

So öffnen Sie File Sanitizer:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie auf **File Sanitizer**.

– ODER –

▲ Doppelklicken Sie auf das Symbol **File Sanitizer** auf dem Desktop.

– ODER –

▲ Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **File Sanitizer öffnen**.

Erstellen eines Shred-Zeitplans

HINWEIS: Informationen zum Auswählen eines voreingestellten Shred Profils oder zur Erstellung eines Shred Profils finden Sie unter „Auswählen oder Erstellen eines Shred Profils“ auf Seite 68.

HINWEIS: Informationen zum manuellen Shreddern von Datenbeständen finden Sie unter „Manuelles Shreddern eines Datenbestands“ auf Seite 72.

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shreddern**.
2. Wählen Sie eine Shred-Option:
   - **Beim Herunterfahren von Windows** – Wählen Sie diese Option, um alle ausgewählten Datenbestände beim Herunterfahren von Windows zu shreddern.

     HINWEIS: Wenn diese Option aktiviert ist, wird beim Herunterfahren ein Dialogfeld angezeigt, in dem Sie angeben können, ob Sie mit dem Shreddern der ausgewählten Datenbestände fortfahren oder den Vorgang überspringen möchten. Klicken Sie auf **Ja**, wenn Sie den Shred-Vorgang überspringen möchten, oder klicken Sie auf **Nein**, wenn Sie den Shred-Vorgang fortsetzen möchten.
   - **Beim Öffnen eines Webbrowsers** – Wählen Sie diese Option, um beim Öffnen eines Webbrowsers alle Internet-bezogenen Datenbestände, wie beispielsweise das URL-Protokoll des Browsers, zu shreddern.
   - **Beim Schließen eines Webbrowsers** – Wählen Sie diese Option, um beim Schließen eines Webbrowsers alle Internet-bezogenen Datenbestände, wie beispielsweise das URL-Protokoll des Browsers, zu shreddern.
   - **Tastenfolge** – Wählen Sie diese Option, um den Shred-Vorgang mit einer Tastenfolge einzuleiten.
   - **Planer** – Markieren Sie das Kontrollkästchen **Planer aktivieren**, geben Sie Ihr Windows Kennwort ein, und tragen Sie anschließend Tag und Uhrzeit für das Shreddern bestimmter Datenbestände ein.

HINWEIS: Eine .dll-Datei wird nur dann geshreddert und vom System entfernt, wenn sie zuvor in den Papierkorb verschoben wurde.

3. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz

HINWEIS: Das Überschreiben von freiem Speicherplatz bietet sich für Datenbestände an, die Sie über den Windows Papierkorb oder manuell gelöscht haben. Das Überschreiben bietet jedoch keine zusätzliche Sicherheit für geshredderte Datenbestände.

So erstellen Sie einen Zeitplan für das Überschreiben von freiem Speicherplatz:

1. Öffnen Sie **File Sanitizer**, und klicken Sie auf **Überschreiben von freiem Speicherplatz**.
2. Markieren Sie das Kontrollkästchen **Planer aktivieren**, geben Sie Ihr Windows Kennwort ein, und tragen Sie anschließend Tag und Uhrzeit für das Überschreiben von freiem Speicherplatz ein.
3. Klicken Sie auf **Übernehmen** und dann auf **OK**.

HINWEIS: Das Überschreiben von freiem Speicherplatz kann längere Zeit in Anspruch nehmen. Auch wenn das Überschreiben im Hintergrund stattfindet, wird die Verarbeitungsleistung Ihres Computers unter Umständen durch die erhöhte Prozessorbeanspruchung beeinträchtigt.

Auswählen oder Erstellen eines Shred Profils

Sie können eine Löschmethode festlegen und die zu shreddernden Datenbestände auswählen, indem Sie ein vordefiniertes Profil aufrufen oder ein eigenes Profil erstellen.

Auswählen eines vordefinierten Shred Profils

Wenn Sie ein vordefiniertes Shred Profil (Hohe Sicherheit, Mittlere Sicherheit oder Geringe Sicherheit) auswählen, werden automatisch eine vordefinierte Löschmethode und eine Liste der Datenbestände aufgerufen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um die vordefinierte Liste der Datenbestände, die für den Shred-Vorgang ausgewählt wurden, aufzurufen.

So wählen Sie ein vordefiniertes Shred Profil aus:

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Einstellungen**.
2. Klicken Sie auf ein vordefiniertes Shred Profil.
3. Klicken Sie auf **Details anzeigen**, um die Liste der Datenbestände, die für den Shred-Vorgang ausgewählt wurden, anzuzeigen.
4. Aktivieren Sie unter **Folgende Elemente shreddern** das Kontrollkästchen neben jedem Datenbestand, für den Sie das Shreddern bestätigen möchten.
5. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Anpassen eines Shred Profils

Beim Erstellen eines Shred Profils können Sie die folgenden Informationen angeben: Anzahl der Shred-Zyklen, welche Datenbestände in den Shred-Vorgang einbezogen werden sollen, für welche

Datenbestände das Shreddern vor dem Ausführen des Befehls bestätigt werden soll und welche Datenbestände vom Shred Prozess ausgeschlossen werden sollen.

1. Öffnen Sie **File Sanitizer**, und klicken Sie nacheinander auf **Einstellungen**, **Einstellungen für erhöhte Sicherheit**. Klicken Sie anschließend auf **Details anzeigen**.

2. Geben Sie die Anzahl der Shred-Zyklen an.

HINWEIS: Für jeden Datenbestand wird die ausgewählte Anzahl von Shred-Zyklen ausgeführt. Wenn Sie beispielsweise drei Shred-Zyklen auswählen, wird ein Algorithmus, der die Daten unleserlich macht, drei Mal separat ausgeführt. Wenn Sie für die Shred-Zyklen die höhere Sicherheitsstufe wählen, kann der Shred-Vorgang erhebliche Zeit in Anspruch nehmen. Je mehr Shred-Zyklen Sie jedoch festlegen, desto unwahrscheinlicher wird es, dass die Daten wiederhergestellt werden können.

3. Wählen Sie die Datenbestände aus, die geshreddert werden sollen:

   a. Klicken Sie unter **Verfügbare Shred-Optionen** auf einen Datenbestand und anschließend auf **Hinzufügen**.

   b. Zum Hinzufügen eines benutzerdefinierten Datenbestands klicken Sie auf **Benutzerdefinierte Option hinzufügen**. Suchen Sie dann den Pfad zum Dateinamen oder Ordner, oder tippen Sie ihn ein. Klicken Sie auf **Öffnen** und dann auf **OK**. Klicken Sie unter **Verfügbare Shred-Optionen** auf einen Datenbestand und anschließend auf **Hinzufügen**.

HINWEIS: Zum Löschen eines Datenbestands aus den verfügbaren Shred-Optionen klicken Sie auf den betreffenden Datenbestand und anschließend auf **Löschen**.

4. Aktivieren Sie unter **Folgende Elemente shreddern** das Kontrollkästchen neben jedem Datenbestand, für den Sie das Shreddern bestätigen möchten.

HINWEIS: Zum Entfernen eines Datenbestands aus der Shred-Liste klicken Sie auf den betreffenden Datenbestand und anschließend auf **Entfernen**.

5. Wenn bestimmte Dateien oder Ordner nicht automatisch geshreddert werden sollen, klicken Sie unter **Folgende Elemente nicht shreddern** auf **Hinzufügen**. Suchen Sie dann den Pfad zum Dateinamen oder Ordner, oder tippen Sie ihn ein. Klicken Sie auf **Öffnen** und dann auf **OK**.

HINWEIS: Zum Entfernen eines Datenbestands aus der Ausschlussliste klicken Sie auf den betreffenden Datenbestand und anschließend auf **Löschen**.

6. Klicken Sie nach Beendigung der Konfiguration des Shred Profils auf **Übernehmen** und anschließend auf **OK**.

Anpassen eines Profils für einfaches Löschen

Mit dem Profil für einfaches Löschen werden Datenbestände nur gelöscht, nicht jedoch geshreddert. Wenn Sie ein Profil für einfaches Löschen anpassen, legen Sie fest, welche Bestände gelöscht werden sollen und welche Bestände nur nach vorheriger Bestätigung oder überhaupt nicht gelöscht werden sollen.

HINWEIS: Wenn Daten einfach nur gelöscht werden, kann das Überschreiben von freiem Speicherplatz auf der Festplatte gelegentlich für Datenbestände ausgeführt werden, die Sie über den Windows Papierkorb oder manuell gelöscht haben.

So erstellen Sie ein Profil für einfaches Löschen:

1. Öffnen Sie **File Sanitizer**, und klicken Sie nacheinander auf **Einstellungen**, **Einstellungen für einfaches Löschen** und **Details anzeigen**.
2. Wählen Sie die zu löschenden Datenbestände aus:
   a. Klicken Sie unter **Verfügbare Löschoptionen** auf einen Datenbestand und anschließend auf **Hinzufügen**.
   b. Zum Hinzufügen eines benutzerdefinierten Datenbestands klicken Sie auf **Benutzerdefinierte Option hinzufügen**. Geben Sie anschließend einen Datei- oder Ordnernamen ein, und klicken Sie auf **OK**. Klicken Sie auf den benutzerdefinierten Datenbestand und dann auf **Hinzufügen**.

HINWEIS: Zum Löschen eines Datenbestands aus den verfügbaren Löschoptionen klicken Sie auf den betreffenden Datenbestand und anschließend auf **Löschen**.

3. Aktivieren Sie unter **Folgende Elemente löschen** das Kontrollkästchen neben jedem Datenbestand, für den Sie das Löschen bestätigen möchten.

HINWEIS: Zum Entfernen eines Datenbestands aus der Löschliste klicken Sie auf den betreffenden Datenbestand und anschließend auf **Entfernen**.

4. Klicken Sie unter **Folgende Elemente nicht löschen** auf **Hinzufügen**, um die Datenbestände auszuwählen, die vom Löschen ausgeschlossen werden sollen.

HINWEIS: Zum Entfernen eines Datenbestands aus der Ausschlussliste klicken Sie auf den betreffenden Datenbestand und anschließend auf **Löschen**.

5. Klicken Sie nach der Konfiguration des Profils für einfaches Löschen auf **Übernehmen** und anschließend auf **OK**.

Allgemeine Aufgaben

Sie können mit File Sanitizer die folgenden Aufgaben ausführen:

- Einleiten des Shred-Vorgangs über eine Tastenfolge – Mit dieser Funktion können Sie eine Tastenfolge (z. B. strg+alt+s) zum Einleiten des Shred-Vorgangs festlegen. Nähere Informationen zu diesem Thema finden Sie unter „Verwenden von Tastenfolgen zum Einleiten des Shred-Vorgangs“ auf Seite 71.
- Einleiten des Shred-Vorgangs über das Symbol „File Sanitizer“ – Diese Funktion ist vergleichbar mit der Funktion Ziehen und Ablegen unter Windows. Nähere Informationen zu diesem Thema finden Sie unter „Verwenden des Symbols „File Sanitizer““ auf Seite 72.
- Manuelles Shreddern eines bestimmten Datenbestands oder aller ausgewählten Datenbestände – Diese Funktionen ermöglichen das manuelle Shreddern außerhalb des Shred-Zeitplans. Nähere Informationen zu diesem Thema finden Sie unter „Manuelles Shreddern eines Datenbestands“ auf Seite 72 oder „Manuelles Shreddern aller ausgewählten Datenbestände“ auf Seite 73.
- Manuelles Aktivieren des Überschreibens von freiem Speicherplatz – Mithilfe dieser Funktion können Sie das Überschreiben von freiem Speicherplatz auf der Festplatte manuell aktivieren. Nähere Informationen zu diesem Thema finden Sie unter „Manuelles Aktivieren des Überschreibens von freiem Speicherplatz“ auf Seite 73.
- Abbrechen eines Shred-Vorgangs oder einer Überschreibung von freiem Speicherplatz – Über diese Funktion haben Sie die Möglichkeit, den aktuellen Shred-Vorgang oder das Überschreiben von freiem Speicherplatz auf der Festplatte abzubrechen. Nähere Informationen zu diesem Thema finden Sie unter „Abbrechen eines Shred-Vorgangs oder des Überschreibens von freiem Speicherplatz“ auf Seite 73.
- Anzeigen der Protokolldateien – Zeigen Sie mit dieser Funktion die Protokolldateien für Shred-Vorgänge und Überschreibungsvorgänge von freiem Speicherplatz an, die sämtliche Fehler für den letzten Shred-Vorgang bzw. die letzte Überschreibung von freiem Speicherplatz enthalten. Nähere Informationen zu diesem Thema finden Sie unter „Anzeigen der Protokolldateien“ auf Seite 73.

HINWEIS: Der Shred-Vorgang oder die Überschreibung von freiem Speicherplatz kann viel Zeit in Anspruch nehmen. Auch wenn das Shreddern und das Überschreiben im Hintergrund stattfinden, wird die Verarbeitungsleistung Ihres Computers unter Umständen durch die erhöhte Prozessorbeanspruchung beeinträchtigt.

Verwenden von Tastenfolgen zum Einleiten des Shred-Vorgangs

Gehen Sie folgendermaßen vor, um eine Tastenfolge festzulegen:

1. Öffnen Sie **File Sanitizer**, und klicken Sie auf **Shreddern**.
2. Aktivieren Sie das Kontrollkästchen **Tastenfolge**.
3. Geben Sie ein Zeichen in das entsprechende Feld ein.
4. Markieren Sie das Kontrollkästchen **STRG** oder **ALT**, und markieren Sie dann die Option **UMSCHALTTASTE**.

   Um zum Beispiel das automatische Shreddern mit der Tastenfolge s und strg+Umschalttaste auszulösen, geben Sie in das dafür vorgesehene Feld den Buchstaben s ein und markieren die Kontrollkästchen **STRG** und **UMSCHALTTASTE**.

HINWEIS: Achten Sie darauf, keine bereits für andere Zwecke konfigurierte Tastenfolge zu verwenden.

So leiten Sie den Shred-Vorgang mit einer Tastenfolge ein:

1. Halten Sie die umschalttaste und entweder die Taste strg oder alt (oder eine andere festgelegte Kombination) gedrückt, während Sie die Taste für das ausgewählte Zeichen drücken.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Verwenden des Symbols „File Sanitizer“

△ **ACHTUNG:** Geshredderte Datenbestände können nicht wiederhergestellt werden. Gehen Sie daher bei der Auswahl von Datenbeständen für manuelles Shreddern mit Bedacht vor.

1. Navigieren Sie zu dem Dokument oder Ordner, das bzw. der geshreddert werden soll.
2. Ziehen Sie den Datenbestand auf das Symbol **File Sanitizer** auf dem Desktop.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Shreddern eines Datenbestands

△ **ACHTUNG:** Geshredderte Datenbestände können nicht wiederhergestellt werden. Gehen Sie daher bei der Auswahl von Datenbeständen für manuelles Shreddern mit Bedacht vor.

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **Ein Element shreddern**.
2. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.

   HINWEIS: Bei dem von Ihnen ausgewählten Datenbestand kann es sich um eine einzelne Datei oder einen einzelnen Ordner handeln.

3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Desktop, und klicken Sie dann auf **Ein Element shreddern**.
2. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Öffnen Sie **File Sanitizer**, und klicken Sie auf **Shreddern**.
2. Klicken Sie auf die Schaltfläche **Durchsuchen**.
3. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Shreddern aller ausgewählten Datenbestände

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **Jetzt shreddern**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Desktop, und klicken Sie dann auf **Jetzt shreddern**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Öffnen Sie **File Sanitizer**, und klicken Sie auf **Shreddern**.
2. Klicken Sie auf die Schaltfläche **Jetzt shreddern**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Aktivieren des Überschreibens von freiem Speicherplatz

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **Jetzt überschreiben**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Öffnen Sie **File Sanitizer**, und klicken Sie auf **Überschreiben von freiem Speicherplatz**.
2. Klicken Sie auf **Jetzt überschreiben**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Abbrechen eines Shred-Vorgangs oder des Überschreibens von freiem Speicherplatz

Wenn gerade ein Shred-Vorgang oder das Überschreiben von freiem Speicherplatz durchgeführt wird, wird über dem Symbol „HP ProtectTools Security Manager“ im Infobereich eine entsprechende Meldung angezeigt. Diese Meldung enthält Informationen über den jeweiligen Shred-Vorgang bzw. das Überschreiben von freiem Speicherplatz (Fortschrittsanzeige) sowie die Option zum Abbrechen des Vorgangs.

So brechen Sie den Vorgang ab:

- Klicken Sie auf die Meldung und anschließend auf **Stop**, um den Vorgang abzubrechen.

Anzeigen der Protokolldateien

Für jeden Shred-Vorgang und jedes Überschreiben von freiem Speicherplatz werden Protokolldateien erzeugt, die eventuell während der Ausführung aufgetretene Fehler aufzeichnen. Die Protokolldateien werden immer wieder aktualisiert, sodass sich ihr Inhalt jeweils auf den letzten Shred-Vorgang bzw. die letzte Überschreibung bezieht.

HINWEIS: Dateien, die erfolgreich geshreddert wurden, oder erfolgreiche Überschreibevorgänge werden in den Protokolldateien nicht aufgeführt.

Es werden ein Protokoll für Shred-Vorgänge und ein Protokoll für das Überschreiben von freiem Speicherplatz erstellt. Beide Protokolle befinden sich auf der Festplatte unter:

- C:\Programme\Hewlett-Packard\File Sanitizer*[Benutzername]*_ShredderLog.txt
- C:\Programme\Hewlett-Packard\File Sanitizer*[Benutzername]*_DiskBleachLog.txt

10 Device Access Manager for HP ProtectTools (bestimmte Modelle)

Administratoren des Windows® Betriebssystems verwenden Device Access Manager for HP ProtectTools, um den Zugriff auf die Geräte in einem System zu kontrollieren und unbefugte Zugriffe zu verhindern:

- Geräteprofile werden für jeden Benutzer erstellt, um festzulegen, auf welche Geräte die jeweiligen Benutzer zugreifen können.
- Die Benutzer sind außerdem in Gruppen aufgeteilt, wie zum Beispiel die voreingestellte Gruppe „Geräte-Administrator“. Sie können in der Systemsteuerung unter Verwaltung mithilfe der Option Computerverwaltung auch Gruppen selbst definieren.
- Der Gerätezugriff kann in Abhängigkeit von der Gruppe gewährt oder verweigert werden.
- Für Geräteklassen wie CD-ROM- und DVD-Laufwerke können Lesezugriff und Schreibzugriff separat gewährt oder verweigert werden.

Bestimmte Benutzer können außerdem berechtigt werden, die Richtlinie für die Gerätezugriffssteuerung abzurufen und zu ändern.

Setup-Verfahren

Aufrufen von Device Access Manager

So öffnen Sie Device Access Manager:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie auf der linken Seite auf **Device Access Manager**.

Konfigurieren von Zugriffrechten auf Geräte

Es gibt drei Ansichten in Device Access Manager for HP ProtectTools:

- Die Ansicht Einfache Konfiguration wird verwendet, um Mitgliedern der Gruppe Geräte-Administratoren den Zugriff auf Geräteklassen zu gewähren oder verweigern.
- Die Ansicht Geräteklassen-Konfiguration wird verwendet, um bestimmten Benutzern oder Gruppen den Zugriff auf Gerätetypen oder auf bestimmte Geräte zu gewähren oder verweigern.
- Die Ansicht Benutzerzugriffseinstellungen wird verwendet, um festzulegen, welche Benutzer die Informationen der Ansicht Einfache Konfiguration und der Ansicht Geräteklassen-Konfiguration anzeigen oder ändern können.

Gruppe „Geräte-Administratoren“

Wenn Device Access Manager installiert wird, wird eine Gruppe „Geräte-Administratoren“ erstellt.

Der Systemadministrator kann eine einfache Gerätezugriffsrichtlinie implementieren, indem er den Zugriff auf verschiedene Geräteklassen grundsätzlich verweigert, es sei denn, ein Benutzer ist als vertrauenswürdig (in Bezug auf den Gerätezugriff) eingestuft. Es wird empfohlen, Benutzer als „vertrauenswürdig“ oder „nicht vertrauenswürdig“ einzustufen, indem Sie alle vertrauenswürdigen Benutzer der Gruppe Geräte-Administratoren hinzufügen. Wenn Sie den Mitgliedern der Gruppe Geräte-Administratoren über die Ansicht Einfache Konfiguration oder Geräteklassen-Konfiguration den Zugriff auf Geräte gewähren, so ist sichergestellt, dass die „vertrauenswürdigen Benutzer“ uneingeschränkten Zugriff auf die ausgewählten Geräteklassen haben.

HINWEIS: Wenn Sie einen Benutzer zur Gruppe Geräte-Administratoren hinzufügen, wird diesem Benutzer nicht automatisch der Zugriff auf Geräte gewährt. Um „vertrauenswürdigen Benutzern“ den Zugriff auf bestimmte Geräteklassen zu gewähren, verwenden Sie die Ansicht Einfache Konfiguration.

So fügen Sie Benutzer zur Gruppe Geräte-Administratoren hinzu:

- Verwenden Sie unter Windows 7, Vista oder XP Professional Snap-In „Lokale Benutzer und Gruppen“ der MMC.
- Geben Sie unter den Home Editionen von Windows 7, Vista® oder XP auf einem Konto mit Administratorrechten den folgenden Befehl über eine Eingabeaufforderung ein:

```
c:\> net localgroup “Geräte-Administratoren” Benutzername /ADD
```

Einfache Konfiguration

Administratoren und befugte Benutzer können die Ansicht Einfache Konfiguration verwenden, um den Zugriff auf die folgenden Geräteklassen für alle Benutzer, die nicht Mitglieder der Gruppe Geräte-Administratoren sind, anzuzeigen und zu ändern:

HINWEIS: Damit ein Benutzer in dieser Ansicht Informationen über den Gerätezugriff anzeigen kann, muss dem Benutzer oder der Gruppe über der Ansicht **Benutzerzugriffseinstellungen** Lesezugriff gewährt werden. Damit ein Benutzer in dieser Ansicht Informationen über den Gerätezugriff ändern kann, muss dem Benutzer oder der Gruppe über der Ansicht **Benutzerzugriffseinstellungen** das Zugriffsrecht „Ändern“ gewährt werden.

- Alle tragbaren Medien (Disketten, USB-Flash-Laufwerke usw.)
- Alle DVD-/CD-ROM-Laufwerke
- Alle Seriell- und Parallelanschlüsse
- Alle Bluetooth®-Geräte
- Alle Infrarotgeräte
- Alle Modemgeräte
- Alle PCMCIA-Geräte
- Alle 1394-Geräte

So gewähren oder verweigern Sie allen Benutzern, die nicht Mitglied der Gruppe Geräte-Administratoren sind, den Zugriff auf eine Geräteklasse:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Einfache Konfiguration**.
2. Um den Zugriff zu verweigern, aktivieren Sie auf der rechten Seite das Kontrollkästchen für eine Geräteklasse oder ein bestimmtes Gerät. Um den Zugriff auf diese Geräteklasse oder dieses bestimmte Gerät zu gewähren, deaktivieren Sie das Kontrollkästchen.

   Wenn ein Kontrollkästchen grau ist, wurden die Werte, die sich auf diese Konfiguration auswirken, in der Ansicht Geräteklassen-Konfiguration geändert. Um die Werte der einfachen Konfiguration zu übernehmen, aktivieren oder deaktivieren Sie das Kontrollkästchen, und klicken Sie dann zur Bestätigung auf **Ja**.
3. Klicken Sie auf das Symbol **Speichern**.

   HINWEIS: Wenn der Hintergrunddienst nicht ausgeführt wird, wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie den Dienst starten möchten. Klicken Sie auf **Ja**.
4. Klicken Sie auf **OK**.

Starten des Hintergrunddiensts

Bevor Geräteprofile angewendet werden können, wird ein HP ProtectTools Security Manager Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie den Hintergrunddienst HP ProtectTools Gerätesperre/Überwachung starten möchten. Klicken Sie auf **Ja**. Der Hintergrunddienst wird gestartet und wird jedes Mal, wenn das System gebootet wird, automatisch gestartet.

HINWEIS: Bevor dieses Hintergrunddienst-Dialogfeld geöffnet wird, muss ein Geräteprofil definiert werden.

Administratoren können diesen Dienst starten und stoppen:

1. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
2. Klicken Sie auf **Verwaltung** und dann auf **Dienste**.
3. Suchen Sie den Dienst **HP ProtectTools Gerätesperre/Überwachung**.

Wenn der Dienst Gerätesperre/Überwachung gestoppt wird, wird nicht die Gerätesperre gestoppt. Durch diese zwei Komponenten wird die Gerätesperre aktiviert:

- Der Dienst Gerätesperre/Überwachung
- Der Treiber DAMDrv.sys

Wenn Sie den Dienst gestartet haben, wird der Gerätetreiber gestartet, doch wenn der Dienst gestoppt wird, wird nicht der Gerätetreiber gestoppt.

Um festzustellen, ob der Hintergrunddienst aktiv ist, öffnen Sie ein Fenster zur Eingabeaufforderung, und geben Sie den Befehl sc query flcdlock ein.

Um festzustellen, ob der Gerätetreiber aktiv ist, öffnen Sie ein Fenster zur Eingabeaufforderung, und geben Sie den Befehl sc query damdrv ein.

Geräteklassen-Konfiguration

Administratoren und berechtigte Benutzer können Listen der Benutzer und Gruppen anzeigen und ändern, denen der Zugriff auf Geräteklassen oder bestimmte Geräte gewährt oder verweigert wird.

HINWEIS: Damit ein Benutzer in dieser Ansicht Informationen über den Gerätezugriff anzeigen kann, muss dem Benutzer oder der Gruppe über der Ansicht **Benutzerzugriffseinstellungen** Lesezugriff gewährt werden. Damit ein Benutzer in dieser Ansicht Informationen über den Gerätezugriff ändern kann, muss dem Benutzer oder der Gruppe über der Ansicht **Benutzerzugriffseinstellungen** Schreibzugriff gewährt werden.

Die Ansicht Geräteklassen-Konfiguration enthält die folgenden Bereiche:

- **Geräteliste** – Hier werden die Geräteklassen und Geräte angezeigt, die im System installiert sind bzw. waren.
  - Der Schutz wird in der Regel für eine ganze Geräteklasse aktiviert. Ein Benutzer oder eine Gruppe kann dann auf jedes Gerät der Geräteklasse zugreifen.
  - Der Schutz kann auch auf der Ebene des entsprechenden Geräts aktiviert werden.
- **Benutzerliste** – Hier werden alle Benutzer und Gruppen angezeigt, denen der Zugriff auf die ausgewählte Geräteklasse oder das ausgewählte Gerät gewährt oder verweigert wird.
  - Der Eintrag in der Benutzerliste kann sich auf den einzelnen Benutzer beziehen oder auf eine Gruppe, zu der dieser Benutzer gehört.
  - Wenn ein Benutzer- oder Gruppeneintrag in der Benutzerliste nicht verfügbar ist, wurden die Einstellungen übernommen, die für die Geräteklasse in der Geräteliste oder im Ordner Klassen festgelegt wurden.
  - Für einige Geräteklassen wie DVD- und CD-ROM-Laufwerke können weitere Zugriffseinstellungen vorgenommen werden, indem zwischen Lese- und Schreibzugriff unterschieden wird.

Wie bei anderen Geräten und Klassen, können auch die Einstellungen für Lese- und Schreibzugriff übernommen werden. Beispielsweise kann der Lesezugriff von einer höheren Klasse übernommen werden, aber der Schreibzugriff kann speziell für einen Benutzer oder eine Gruppe verweigert werden.

HINWEIS: Wenn das Kontrollkästchen für den Lesezugriff deaktiviert ist, hat der Eintrag für den Zugriff keine Auswirkungen auf den Lesezugriff auf das Gerät. Der Lesezugriff auf das Gerät wird weder gewährt noch verweigert.

Beispiel 1 – Wenn einem Benutzer oder einer Gruppe der Schreibzugriff auf ein Gerät oder eine Geräteklasse verweigert wird:

Der Schreibzugriff oder Lese-/Schreibzugriff kann demselben Benutzer, derselben Gruppe oder einem Mitglied derselben Gruppe nur für ein Gerät gewährt werden, das sich in der Gerätehierarchie unter diesem Gerät befindet.

Beispiel 2 – Wenn einem Benutzer oder einer Gruppe der Schreibzugriff auf ein Gerät oder eine Geräteklasse gewährt wird:

Der Schreibzugriff oder Lese-/Schreibzugriff kann demselben Benutzer, derselben Gruppe oder einem Mitglied derselben Gruppe nur für dieses Gerät verweigert werden oder für ein Gerät, das sich in der Gerätehierarchie unter diesem Gerät befindet.

Beispiel 3 – Wenn einem Benutzer oder einer Gruppe der Lesezugriff auf ein Gerät oder eine Geräteklasse gewährt wird:

Der Lesezugriff oder Lese-/Schreibzugriff kann demselben Benutzer, derselben Gruppe oder einem Mitglied derselben Gruppe nur für dieses Gerät verweigert werden oder für ein Gerät, das sich in der Gerätehierarchie unter diesem Gerät befindet.

Beispiel 4 – Wenn einem Benutzer oder einer Gruppe der Lesezugriff auf ein Gerät oder eine Geräteklasse verweigert wird:

Der Lesezugriff oder Lese-/Schreibzugriff kann demselben Benutzer, derselben Gruppe oder einem Mitglied derselben Gruppe nur für ein Gerät gewährt werden, das sich in der Gerätehierarchie unter diesem Gerät befindet.

Beispiel 5 – Wenn einem Benutzer oder einer Gruppe der Lese-/Schreibzugriff auf ein Gerät oder eine Geräteklasse gewährt wird:

Der Schreibzugriff oder Lese-/Schreibzugriff kann demselben Benutzer, derselben Gruppe oder einem Mitglied derselben Gruppe nur für dieses Gerät verweigert werden oder für ein Gerät, das sich in der Gerätehierarchie unter diesem Gerät befindet.

Beispiel 6 – Wenn einem Benutzer oder einer Gruppe der Lese-/Schreibzugriff auf ein Gerät oder eine Geräteklasse verweigert wird:

Der Lesezugriff oder Lese-/Schreibzugriff kann demselben Benutzer, derselben Gruppe oder einem Mitglied derselben Gruppe nur für ein Gerät gewährt werden, das sich in der Gerätehierarchie unter diesem Gerät befindet.

Verweigern des Zugriffs für einen Benutzer oder einer Gruppe

So verweigern Sie einem Benutzer oder einer Gruppe den Zugriff auf ein Gerät oder eine Geräteklasse:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.
   - Geräteklasse
   - Alle Geräte
   - Bestimmtes Gerät
3. Klicken Sie unter **Benutzer/Gruppen** auf den Benutzer oder die Gruppe, dem/der Sie den Zugriff verweigern möchten.
4. Klicken Sie neben einem Benutzer oder einer Gruppe auf **Verweigern**.
5. Klicken Sie auf das Symbol **Speichern**.

HINWEIS: Wenn die Einstellungen „Verweigern“ und „Zulassen“ auf derselben Ebene für einen Benutzer aktiviert sind, hat die Zugriffsverweigerung Vorrang vor der Zugriffsberechtigung.

Gewähren des Zugriffs für einen Benutzer oder eine Gruppe

So gewähren Sie einem Benutzer oder einer Gruppe den Zugriff auf ein Gerät oder eine Geräteklasse:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Geräteklassen-Konfiguration**.
2. Wählen Sie in der Geräteliste die gewünschten Elemente:
   - Geräteklasse
   - Alle Geräte
   - Bestimmtes Gerät
3. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld zum Auswählen von Benutzern oder Gruppen wird angezeigt.
4. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um die hinzuzufügenden Benutzer oder Gruppen zu suchen.
5. Klicken Sie in der Liste mit den verfügbaren Benutzern und Gruppen auf einen Benutzer oder eine Gruppe, und klicken Sie dann auf **OK**.
6. Klicken Sie erneut auf **OK**.
7. Klicken Sie auf **Zulassen**, um diesem Benutzer bzw. dieser Gruppe den Zugriff zu gewähren.
8. Klicken Sie auf das Symbol **Speichern**.

Aufheben des Zugriffsrechts für einen Benutzer oder eine Gruppe

So heben Sie den Zugriff auf ein Gerät oder eine Geräteklasse für einen Benutzer oder eine Gruppe auf:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.
   - Geräteklasse
   - Alle Geräte
   - Bestimmtes Gerät
3. Klicken Sie unter **Benutzer/Gruppe** auf den Benutzer oder die Gruppe, die Sie entfernen möchten, und klicken Sie dann auf **Entfernen**.
4. Klicken Sie auf das Symbol **Speichern**.

Gewähren des Zugriffs auf eine Geräteklasse für einen Benutzer einer Gruppe

So gewähren Sie einem Benutzer den Zugriff auf eine Geräteklasse, während allen anderen Mitgliedern der Gruppe dieses Benutzers der Zugriff verweigert wird:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.
   - Geräteklasse
   - Alle Geräte
   - Bestimmtes Gerät
3. Wählen Sie unter **Benutzer/Gruppen** die Gruppe, der Sie den Zugriff verweigern möchten, und klicken Sie dann auf **Verweigern**.
4. Navigieren Sie zum untergeordneten Ordner der entsprechenden Geräteklasse, und fügen Sie den bestimmten Benutzer hinzu.
5. Klicken Sie auf **Zulassen**, um diesem Benutzer den Zugriff zu gewähren.
6. Klicken Sie auf das Symbol **Speichern**.

Gewähren des Zugriffs auf ein bestimmtes Gerät für einen Benutzer einer Gruppe

Administratoren können einem Benutzer den Zugriff auf ein bestimmtes Gerät gewähren, während allen anderen Mitgliedern der Gruppe dieses Benutzers der Zugriff auf alle Geräte in der Klasse verweigert wird:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten, und navigieren Sie dann zu dem untergeordneten Ordner.

3. Klicken Sie auf **Hinzufügen**. Das Dialogfeld zum Auswählen von Benutzern oder Gruppen wird angezeigt.
4. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um nach der Gruppe des Benutzers zu suchen, der Sie den Zugriff auf alle Geräte der Klasse verweigern möchten.
5. Klicken Sie auf die Gruppe und anschließend auf **OK**.
6. Navigieren Sie innerhalb der Geräteklasse zu dem Gerät, auf das der Benutzer Zugriff erhalten soll.
7. Klicken Sie auf **Hinzufügen**. Das Dialogfeld zum Auswählen von Benutzern oder Gruppen wird angezeigt.
8. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um die hinzuzufügenden Benutzer oder Gruppen zu suchen.
9. Klicken Sie auf den Benutzer, dem Sie den Zugriff gewähren möchten, und klicken Sie dann auf **OK**.
10. Klicken Sie auf **Zulassen**, um diesem Benutzer den Zugriff zu gewähren.
11. Klicken Sie auf das Symbol **Speichern**.

Zurücksetzen der Konfiguration

△ **ACHTUNG:** Nach dem Zurücksetzen der Konfiguration werden alle vorgenommenen Änderungen an der Gerätekonfiguration verworfen und alle werksseitigen Einstellungen wiederhergestellt.

So setzen Sie die Konfigurationseinstellungen auf den Auslieferungszustand zurück:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Geräteklassen-Konfiguration**.
2. Wählen Sie die Schaltfläche **Zurücksetzen**.
3. Klicken Sie zur Bestätigung auf **Ja**.
4. Klicken Sie auf das Symbol **Speichern**.

Erweiterte Aufgaben

Steuern des Zugriff auf die Konfigurationseinstellungen

In der Ansicht **Benutzerzugriffseinstellungen** legen Administratoren die Gruppen oder Benutzer fest, welche die Ansichten **Einfache Konfiguration** und **Geräteklassen-Konfiguration** verwenden dürfen.

HINWEIS: Ein Benutzer oder eine Gruppe muss über „Alle Administrator-Benutzerrechte“ verfügen, um die Einstellungen in der Ansicht **Benutzerzugriffseinstellungen** ändern zu können.

- Um die Informationen in den Ansichten Einfache Konfiguration und Geräteklassen-Konfiguration anzeigen zu können, muss der Benutzer oder die Gruppe über das Zugriffsrecht „Konfigurationseinstellungen anzeigen (nur Lesezugriff)“ in der Ansicht Benutzerzugriffseinstellungen verfügen.
- Um die Informationen in den Ansichten Einfache Konfiguration und Geräteklassen-Konfiguration ändern zu können, muss der Benutzer oder die Gruppe über das Zugriffsrecht „Konfigurationseinstellungen ändern“ in der Ansicht Benutzerzugriffseinstellungen verfügen.

HINWEIS: Trotzdem muss Mitgliedern der Gruppe Administrator das Zugriffsrecht „Lesen“ gewährt werden, um die Ansichten **Einfache Konfiguration** und **Geräteklassen-Konfiguration** anzeigen zu können und das Zugriffsrecht „Ändern“ gewährt werden, um Einstellungen in den Ansichten **Einfache Konfiguration** und **Geräteklassen-Konfiguration** ändern zu können.

HINWEIS: Benutzer nach Berücksichtigung aller Benutzer, Gruppen und Zugriffsebenen weder das Kontrollkästchen „Zulassen“ noch das Kontrollkästchen „Verweigern“ für eine Zugriffsebene aktiviert ist, hat dieser Benutzer kein Zugriffsrecht auf dieser Ebene.

Gewähren des Zugriffs für eine vorhandene Gruppe oder einen vorhandenen Benutzer

So erteilen Sie einer vorhandenen Gruppe oder einem vorhandenen Benutzer das Recht, die Konfigurationseinstellungen zu ändern:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Benutzerzugriffseinstellungen**.
2. Klicken Sie auf eine Gruppe oder einen Benutzer, der/dem Sie den Zugriff gewähren möchten.
3. Klicken Sie unter **Berechtigungen** für jeden Zugriffstyp, den Sie der gewählten Gruppe oder dem gewählten Benutzer gewähren möchten, auf **Zulassen**:

   HINWEIS: Die gewährten Rechte sind kumulativ. Beispiel: Wenn ein Benutzer über das Zugriffsrecht „Konfigurationseinstellungen ändern“ verfügt, dann wird ihm automatisch auch das Zugriffrecht „Konfigurationseinstellungen anzeigen (nur Lesezugriff)“ gewährt. Wenn ein Benutzer über das Zugriffsrecht „Alle Administrator-Benutzerrechte“ verfügt, werden ihm auch die Zugriffsrechte „Konfigurationseinstellungen ändern“ und „Konfigurationseinstellungen anzeigen (nur Lesezugriff)“ gewährt.

   - Alle Administrator-Benutzerrechte
   - Konfigurationseinstellungen ändern
   - Konfigurationseinstellungen anzeigen (nur Lesezugriff)
4. Klicken Sie auf das Symbol **Speichern**.

Verweigern des Zugriffs für eine vorhandene Gruppe oder einen vorhandenen Benutzer

So verweigern Sie einer vorhandenen Gruppe oder einem vorhandenen Benutzer das Recht, die Konfigurationseinstellungen zu ändern:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Benutzerzugriffseinstellungen**.
2. Klicken Sie auf eine Gruppe oder einen Benutzer, der/dem Sie den Zugriff verweigern möchten.
3. Klicken Sie unter **Berechtigungen** für jeden Zugriffstyp, den Sie der gewählten Gruppe oder dem gewählten Benutzer gewähren möchten, auf **Verweigern**:
   - Alle Administrator-Benutzerrechte
   - Konfigurationseinstellungen ändern
   - Konfigurationseinstellungen anzeigen (nur Lesezugriff)
4. Klicken Sie auf das Symbol **Speichern**.

Hinzufügen einer neuen Gruppe oder eines neuen Benutzers

So erteilen Sie einer neuen Gruppe oder einem neuen Benutzer das Recht, die Konfigurationseinstellungen zu ändern:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Benutzerzugriffseinstellungen**.
2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld zum Auswählen von Benutzern oder Gruppen wird angezeigt.
3. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um die hinzuzufügenden Benutzer oder Gruppen zu suchen.
4. Klicken Sie auf eine Gruppe oder einen Benutzer, klicken Sie auf **OK** und anschließend noch einmal auf **OK**.
5. Klicken Sie auf **Zulassen**, um diesem Benutzer den Zugriff zu gewähren.
6. Klicken Sie auf das Symbol **Speichern**.

Aufheben eines Zugriffrechts für eine Gruppe oder einen Benutzer

So heben Sie für eine Gruppe oder einen Benutzer das Recht auf, die Konfigurationseinstellungen zu ändern:

1. Klicken Sie auf der linken Seite der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und dann auf **Benutzerzugriffseinstellungen**.
2. Klicken Sie auf eine Gruppe oder einen Benutzer und dann auf **Entfernen**.
3. Klicken Sie auf das Symbol **Speichern**.

Zugehörige Dokumentation

Device Access Manager for HP ProtectTools ist kompatibel mit HP ProtectTools Enterprise Device Access Manager. Wenn Sie mit der Enterprise Version arbeiten, können in HP Device Access Manager for ProtectTools die programmeigenen Einstellungen nur gelesen werden.

Weitere Informationen über Device Access Manager for HP ProtectTools finden Sie im Internet unter http://www.hp.com/hps/security/products.

11 LoJack Pro for HP ProtectTools

Computrace LoJack Pro von Absolute Software (separat zu erwerben), ist eine Lösung zur Wiederbeschaffung von verloren gegangenen oder gestohlenen Computern an.

Wenn diese Software aktiviert wird, wird der Computrace Agent aktiviert, der in Ihrem Computer sogar dann aktiv bleibt, wenn die Festplatte formatiert oder ausgetauscht wird.

LoJack Pro ermöglicht die Fernüberwachung, -verwaltung und -nachverfolgung Ihres Computers. Sollte Ihr Computer verloren gegangen oder gestohlen sein, ist Ihnen das Team von Absolute beim Wiederauffinden Ihres Computers behilflich.*

HINWEIS: *Dieses Merkmal ist von der geografischen Lage abhängig. Weitere Details finden Sie in der Abonnementvereinbarung von Absolute Software.

12 Fehlerbeseitigung

HP ProtectTools Security Manager

Kurzbeschreibung	Einzelheiten	Lösung
Smart Cards und USB-Token sind in Security Manager nicht verfügbar, wenn sie erst nach der Installation von Security Manager installiert wurden.	Um Smart Cards oder USB-Token in Security Manager verwenden zu können, muss die unterstützende Software (Treiber, PKCS#11-Anbieter usw.) vor der Installation von Security Manager installiert werden. Wenn Sie Security Manager bereits installiert haben, gehen Sie nach der Installation der Unterstützungssoftware für Smart Cards oder USB-Token folgendermaßen vor:	Melden Sie sich bei Password Manager an. Klicken Sie in HP ProtectTools Security Manager auf **Password Manager**, dann auf **Anmeldeinformationen** und anschließend auf **Smart Card**. Starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.
Bestimmte Webseiten von Anwendungen erzeugen Fehler, infolge derer der Benutzer die gewünschten Aufgaben nicht durchführen oder abschließen kann.	Aufgrund der Single Sign On-Funktion wird die Ausführung bestimmter webbasierter Anwendungen beendet, und es werden Fehlermeldungen angezeigt. So weist im Internet Explorer ein **!** in einem gelben Dreieck z. B. darauf hin, dass ein Fehler aufgetreten ist.	Security Manager Single Sign-On unterstützt nicht alle Web-Schnittstellen der Software. Deaktivieren Sie die Single Sign-On-Unterstützung für die jeweilige Web-Seite. Siehe dazu die vollständige Dokumentation über Single Sign-On in den Software-Hilfedateien von Security Manager. Wenn sich Single Sign On für eine konkrete Anwendung nicht deaktivieren lässt, wenden Sie sich an den technischen Support von HP und bitten um Third-Level-Support über Ihren HP Service-Ansprechpartner.
Bei der Anmeldung wird die Option **Browse for Virtual Token** (Nach virtuellem Token suchen) nicht angezeigt.	Der Benutzer kann den Ort eines registrierten virtuellen Token in Password Manager nicht verschieben, da die Option zum Durchsuchen entfernt wurde, um das Sicherheitsrisiko zu senken.	Durch die Entfernung der Option zum Durchsuchen soll verhindert werden, dass unbefugte Benutzer Dateien löschen oder umbenennen bzw. Windows nutzen können.
Domänenadministratoren können das Windows Kennwort selbst mit Autorisierung nicht ändern.	Dieser Fall tritt auf, nachdem sich ein Domänenadministrator bei einer Domäne anmeldet und die Domänenidentität mithilfe von Password Manager mit Administratorrechten auf der Domäne und dem lokalen PC registriert. Wenn der Domänenadministrator versucht, das Windows Kennwort von Password Manager aus zu ändern, wird eine Anmeldefehlermeldung angezeigt: **User account restriction** (Benutzerkontoeinschränkung).	Password Manager kann das Kontokennwort eines Domänenbenutzers nicht über die Funktion **Windows Anmeldekennwort ändern** ändern. Security Manager kann nur die Kennwörter der lokalen PC-Konten ändern. Der Domänenbenutzer kann sein Kennwort mithilfe der Option **Kennwort ändern** in **Windows-Sicherheit** ändern, da er aber kein physikalisches Konto auf dem lokalen PC hat, kann Password Manager nur das zum Anmelden verwendete Kennwort ändern.

Kurzbeschreibung	Einzelheiten	Lösung
Es treten In Kompatibilitätsprobleme mit Password Manager und dem Corel WordPerfect 12 Kennwort GINA auf.	Wenn sich der Benutzer bei Password Manager anmeldet, ein Dokument in WordPerfect erstellt und dieses mit Kennwortschutz speichert, kann Password Manager das Kennwort GINA nicht erkennen, weder manuell noch automatisch.	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.
Password Manager erkennt die Schaltfläche **Verbinden** nicht.	Wenn für die SSO-Zugangsdaten für Remote Desktop Connection (RDP) beim erneuten Starten von Single Sign On **Connect** (Verbinden) festgelegt wurde, wird jedes Mal **Save As** (Speichern unter) anstelle von **Connect** (Verbinden) angezeigt.	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.
Der Benutzer kann sich unter Windows XP Service Pack 1 nach dem Übergang vom Energiesparmodus in den Ruhezustand nicht mehr bei Password Manager anmelden.	Nachdem das System den Ruhezustand und den Energiesparmodus eingeleitet hat, kann sich der Administrator oder Benutzer nicht bei Password Manager anmelden, und der Windows Anmeldebildschirm wird angezeigt, auch wenn andere Anmeldemöglichkeiten (Kennwort, Fingerabdruck oder Java Card) ausgewählt werden.	Aktualisieren Sie Windows mithilfe der Windows Update-Funktion auf Service Pack 2. Zur Ursache des Problems siehe auch den Artikel Nummer 813301 in der Microsoft Knowledge Base unter http://www.microsoft.com. Um sich anmelden zu können, muss der Benutzer Password Manager wählen und sich anmelden. Nach der Anmeldung bei Password Manager wird der Benutzer aufgefordert, sich bei Windows anzumelden (möglicherweise muss der Benutzer die Windows Anmeldeoption wählen), um den Anmeldevorgang fertig zu stellen. Wenn sich der Benutzer zuerst bei Windows anmeldet, muss sich der Benutzer manuell bei Password Manager anmelden.
Beim Sicherheitsprozess **Restore Identity** (Identität wiederherstellen) geht die Verknüpfung mit dem virtuellen Token verloren.	Wenn der Benutzer die Identität wiederherstellt, verliert Password Manager möglicherweise die Zuordnung zum Speicherort des virtuellen Token beim Anmeldebildschirm. Obwohl das virtuelle Token bei Password Manager registriert ist, muss der Benutzer das Token erneut registrieren, um die Zuordnung wiederherzustellen.	Dies ist zurzeit das beabsichtigte Standardverhalten der Anwendung. Wenn Security Manager deinstalliert wird, ohne Identitäten beizubehalten, wird der System-(Server-) Teil des Token zerstört. Das Token kann dann nicht mehr für die Anmeldung verwendet werden, auch wenn der Client-Teil des Token durch eine Identitätswiederherstellung wiederhergestellt wird. HP untersucht langfristige Optionen zur Behebung des Problems.

Device Access Manager for HP ProtectTools

Benutzern wurde der Zugriff auf Geräte innerhalb von Device Access Manager verweigert, es kann aber immer noch auf die Geräte zugegriffen werden.

- **Erklärung** – Die Ansicht „Einfache Konfiguration“ und/oder „Geräteklassen-Konfiguration“ wurde innerhalb von Device Access Manager verwendet, um Benutzern den Zugriff auf Geräte zu verweigern. Obwohl der Zugriff verweigert wurde, können die Benutzer auf die Geräte zugreifen.
- **Lösung:**
  - Prüfen Sie, ob der Dienst „HP ProtectTools Gerätesperre“ gestartet wurde.
  - Klicken Sie als Administrator auf **Systemsteuerung** und dann auf **System und Wartung**. Klicken Sie im Fenster „Verwaltung“ auf **Dienste**, und suchen Sie den Dienst **HP ProtectTools Gerätesperre/Überwachung**. Prüfen Sie, ob der Dienst gestartet wird und ob der Starttyp **Automatisch** lautet.

Ein Benutzer hat unerwartet Zugriff auf ein Gerät, oder einem Benutzer wird der Zugriff auf ein Gerät unerwartet verweigert.

- **Erklärung** – Device Access Manager wurde verwendet, um Benutzern den Zugriff auf einige Geräte zu verweigern und den Zugriff auf andere Geräte zu erteilen. Wenn der Benutzer das System verwendet, kann er auf Geräte zugreifen, auf die er eigentlich keinen Zugriff haben dürfte, und er hat keinen Zugriff auf Geräte, auf die er eigentlich zugreifen dürfte.
- **Lösung:**
  - Prüfen Sie die Geräteeinstellungen des Benutzers mithilfe der Geräteklassen-Konfiguration in Device Access Manager.
  - Klicken Sie auf **Security Manager**, dann auf **Device Access Manager** und schließlich auf **Geräteklassen-Konfiguration**. Erweitern Sie die Ebenen im Geräteklassen-Verzeichnis, und prüfen Sie die Einstellungen für diesen Benutzer. Suchen Sie nach Einträgen mit der Berechtigung „Verweigern“, die für den Benutzer oder eine Windows Gruppe festgelegt wurde, zu der der Benutzer gehört (z. B. Benutzer, Administratoren).

Zulassen oder verweigern — was hat Vorrang?

- **Erklärung** – In der Ansicht „Geräteklassen-Konfiguration“ wurde die folgende Konfiguration eingerichtet:
  - Die Berechtigung „Zulassen“ wurde einer Windows Gruppe (z. B. BUILTIN\Administratoren) und die Berechtigung „Verweigern“ wurde einer anderen Windows Gruppe (z. B. BUILTIN \Benutzer) auf der gleichen Ebene in der Geräteklassen-Hierarchie (z. B. DVD\CD-ROM-Laufwerke) erteilt.
  - Welche Berechtigung hat Vorrang, wenn ein Benutzer zu beiden Gruppen gehört (z. B. Administratoren)?
- **Lösung:**
  - Der Benutzer erhält keinen Zugriff auf das Gerät. Die Berechtigung „Verweigern“ hat Vorrang vor „Zulassen“.
  - Der Zugriff wird aufgrund der Art und Weise verweigert, in der Windows die tatsächliche Berechtigung für das Gerät ermittelt. Einer Gruppe wird der Zugriff verweigert und einer Gruppe wird er erteilt. Der Benutzer gehört aber zu beiden Gruppen. Dem Benutzer wird der Zugriff verweigert, weil die Zugriffsverweigerung Vorrang hat vor der Zugriffserteilung.
  - Dieses Problem lässt sich z. B. umgehen, indem der Gruppe „Benutzer“ auf DVD/CD-ROM-Laufwerksebene der Zugriff verweigert und der Gruppe „Administratoren“ auf der Ebene unterhalb der DVD/CD-ROM-Laufwerksebene der Zugriff erteilt wird.
  - Alternativ dazu können spezielle Windows Gruppen erstellt werden, eine mit Zugriff auf DVD/CD-Laufwerke und eine ohne Zugriff auf DVD/CD-Laufwerke. Der entsprechenden Gruppe würden dann bestimmte Benutzer hinzugefügt.

Die Ansicht „Einfache Konfiguration“ wurde verwendet, um eine Richtlinie für die Gerätezugriffssteuerung zu definieren, die Administratoren können jedoch nicht auf die Geräte zugreifen.

- **Erklärung** – Die einfache Konfiguration verweigert Benutzern und Gästen den Zugriff, während Geräte-Administratoren Zugriff erteilt wird.
- **Lösung:** Fügen Sie den Administrator zur Gruppe „Geräte-Administratoren“ hinzu.

Sonstiges

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
Security Manager — Warnmeldung: **Diese Sicherheitsanwendung kann erst installiert werden, wenn HP ProtectTools Security Manager installiert ist.**	Alle Sicherheitsanwendungen wie Java Card Security und biometrische Anmeldemöglichkeiten sind erweiterbare Plug-ins für die Security Manager Schnittstelle. Security Manager muss bereits installiert sein, bevor ein von HP zugelassenes Sicherheits-Plug-In geladen werden kann.	Die Security Manager Software muss installiert sein, bevor ein Sicherheits-Plug-In installiert werden kann.
HP ProtectTools Security Manager – Beim Schließen der Security Manager Schnittstelle wird zeitweilig ein Fehler zurückgegeben.	Wenn der Benutzer Security Manager über die Schließen-Schaltfläche in der oberen rechten Ecke des Bildschirms schließt, bevor alle Plug-In-Anwendungen vollständig geladen wurden, tritt zeitweilig (in einem von 12 Fällen) ein Fehler auf.	Dies ist auf eine Zeitsteuerungsabhängigkeit von Ladezeiten für Plug-In-Dienste beim Schließen und Neustarten von Security Manager zurückzuführen. Da die Datei **PTHOST.exe** die Shell für die anderen Anwendungen (Plug-Ins) bildet, ist sie davon abhängig, dass Plug-Ins ihre Ladezeiten (Dienste) regulär abschließen. Das Problem tritt dann auf, wenn die Shell geschlossen wird, bevor ein Plug-In erfolgreich geladen werden konnte. Warten Sie, bis Security Manager die Meldung über das Laden der Dienste (oben im Security Manager Fenster) abgeschlossen hat und alle in der linken Spalte aufgeführten Plug-Ins geladen sind. Um einen Fehler zu vermeiden, warten Sie einige Sekunden, bis sämtliche Plug-Ins geladen wurden.
HP ProtectTools – Durch unbeschränkten Zugriff oder unkontrollierte Administratorrechte kommt es zu einem Sicherheitsrisiko.	Ein unbeschränkter Zugriff auf den Client-PC kann eine Vielzahl von Sicherheitsrisiken mit sich bringen, z. B.: • Löschen eines PSD • Unbefugte Änderungen von Benutzereinstellungen • Deaktivieren von Sicherheitsrichtlinien und -funktionen	Administratoren wird geraten, gemäß den „Best Practices“ die Rechte für Endbenutzer und den Benutzerzugriff einzuschränken. Unberechtigte Benutzer sollten nicht über Administratorrechte verfügen.

Glossar

Administrator *Siehe* Windows Administrator.

Aktivierung Die Aufgabe, die durchgeführt werden muss, bevor auf die anderen Funktionen von Drive Encryption zugegriffen werden kann. Verwenden Sie den Installations-Assistenten von HP ProtectTools, um Drive Encryption zu aktivieren. Drive Encryption kann nur von einem Administrator aktiviert werden. Der Aktivierungsvorgang besteht aus dem Aktivieren der Software, dem Verschlüsseln des Laufwerks, dem Erstellen eines Benutzerkontos sowie dem Erstellen des ursprünglichen Sicherungs-Chiffrierschlüssels auf einem Wechselmediengerät.

Anmeldedaten Methode, mit der ein Benutzer seine Berechtigung für ein bestimmtes Vorhaben im Authentifizierungsvorgang beweist.

Anmeldung Ein Element innerhalb von Security Manager, das aus einem Benutzernamen und einem Kennwort besteht (und eventuell anderen ausgewählten Informationen), die zur Anmeldung bei Websites oder anderen Programmen verwendet werden können.

ATM Automatic Technology Manager. Bietet Netzwerkadministratoren die Möglichkeit, Systeme remote auf BIOS-Ebene zu verwalten.

Authentifizierung In diesem Vorgang wird überprüft, ob ein Benutzer autorisiert ist, ein bestimmtes Vorhaben durchzuführen, z. B. auf einen Computer zuzugreifen, Einstellungen für ein bestimmtes Programm zu ändern oder sichere Daten einzusehen.

Authentifizierung beim Systemstart Sicherheitsfunktion, die beim Starten eine Form der Authentifizierung, wie z. B. eine Java Card, einen Sicherheits-Chip oder ein Kennwort, erfordert.

Automatisches Shreddern Geplante Shred-Vorgänge, die der Benutzer in File Sanitizer festlegt.

Autorisierter Benutzer Ein Benutzer, dem in der Ansicht Benutzerzugriffseinstellungen das Recht gewährt wurde, Konfigurationseinstellungen in der Ansicht Einfache Konfiguration oder Geräteklassen-Konfiguration anzuzeigen oder zu ändern.

Benutzer Jede bei Drive Encryption registrierte Person. Nicht-Administratoren verfügen nur über eingeschränkte Rechte in Drive Encryption. Benutzer können sich nur (mit Genehmigung des Administrators) registrieren und anmelden.

Biometrisch Kategorie der Authentifizierungsinformationen, die eine physische Komponente, wie z. B. einen Fingerabdruck, beinhalten, um den Benutzer zu identifizieren.

Chat-Protokollsitzung Eine verschlüsselte Datei, die einen Datensatz für beide Seiten einer Unterhaltung in einer Chat-Sitzung enthält.

Datenbestand Eine Datenkomponente, die aus persönlichen Informationen oder Dateien, Verlaufsdaten und Internet-bezogenen Daten usw. besteht und sich auf der Festplatte befindet.

Digitale Signatur Mit einer Datei gesendete Daten, die den Absender des Materials verifizieren und überprüfen, ob die Datei nach der Unterschrift geändert wurde.

Digitales Zertifikat Elektronische Anmeldeinformationen, die die Identität einer Person oder eines Unternehmens durch Verknüpfung der Identität des Besitzers des digitalen Zertifikats mit zwei elektronischen Kennwörtern, die zum Unterschreiben digitaler Informationen verwendet werden, bestätigen.

Domäne Gruppe von Computern, die Teil eines Netzwerks sind und auf eine gemeinsame Verzeichnisdatenbank zugreifen. Domänen tragen eindeutige Namen, wobei jede über einen Satz gemeinsamer Regeln und Vorgänge verfügt.

Drive Encryption Schützt Ihre Daten, indem Ihre Festplatte(n) verschlüsselt wird/werden und somit die Informationen für Benutzer ohne entsprechende Berechtigung unlesbar werden.

Drive Encryption Anmeldebildschirm Ein Anmeldebildschirm, der angezeigt wird, bevor Windows startet. Benutzer müssen Ihren Windows Benutzernamen und das Kennwort oder die Java Card PIN eingeben. In den meisten Fällen ermöglicht die Eingabe der korrekten Informationen auf dem Drive Encryption Anmeldebildschirm den direkten Zugriff auf Windows ohne die erneute Anmeldung auf dem Windows Anmeldebildschirm.

DriveLock Sicherheitsmerkmal, durch das die Festplatte mit einem Benutzer verknüpft wird, der beim Start des Computers das korrekte DriveLock Kennwort eingeben muss.

Einfaches Löschen Das Löschen des Windows Verweises zu einem Datenbestand. Der Inhalt des Datenbestands verbleibt auf der Festplatte, bis die Daten beim Überschreiben von freiem Speicherplatz überschrieben werden.

Einladung an vertrauenswürdige Kontaktperson(en) Eine E-Mail-Nachricht, die an eine Person gesendet wird, um sie zu bitten, eine vertrauenswürdige Kontaktperson zu werden.

Empfänger einer Einladung an vertrauenswürdige Kontaktperson(en) Eine Person, die die Einladung erhält, eine vertrauenswürdige Kontaktperson zu werden.

Empfohlener Signierer Ein Benutzer, den der Eigentümer eines Microsoft Word oder Microsoft Excel Dokuments für das Hinzufügen einer Signaturzeile zu dem Dokument benennt.

Encryption File System (EFS) System zur Verschlüsselung aller Dateien und Unterordner innerhalb des ausgewählten Ordners.

Entschlüsselung In der Kryptografie verwendeter Vorgang zur Konvertierung verschlüsselter Daten in reinen Text.

Fingerabdruck Eine digitale Extraktion Ihres Fingerabdruck-Abbilds. Das Fingerabdruck-Abbild selbst wird nie von Security Manager gespeichert.

Geräteklasse Alle Geräte eines bestimmten Typs, beispielsweise Laufwerke.

Gerätezugriffsrichtlinie Die Liste mit den Geräten, für die ein Benutzer ein Zugriffsrecht oder kein Zugriffsrecht besitzt.

Gruppe Eine Benutzergruppe, der dasselbe Zugriffrecht für eine Geräteklasse oder ein bestimmtes Gerät gewährt oder verweigert wird.

Hintergrunddienst Der Hintergrunddienst HP ProtectTools Gerätesperre/Überwachung, der ausgeführt werden muss, damit die Gerätezugriffsrichtlinien zur Anwendung kommen. Sie können den Dienst in der Systemsteuerung über die Option Verwaltung in der Anwendung Dienste anzeigen. Wenn der Dienst nicht ausgeführt wird, versucht HP ProtectTools Security Manager, ihn zu starten, wenn Gerätezugriffsrichtlinien angewendet werden.

HP SpareKey Sicherungskopie des Drive Encryption Schlüssels.

ID-Card Ein Tool in der Windows Sidebar, das Ihren Desktop mit Ihrem Benutzernamen und einem ausgewählten Bild personalisiert. Klicken Sie auf die IC-Card, um die HP ProtectTools Administrator-Konsole zu öffnen.

Identität Eine Gruppe von Anmeldeinformationen und Einstellungen in ProtectTools Security Manager, die wie ein Konto oder Profil eines bestimmten Benutzers behandelt werden.

Java Card Eine entnehmbare Karte, die in den Computer eingesteckt wird. Sie enthält Identifikationsdaten für die Anmeldung. Wenn Sie sich mit der Java Card beim Drive Encryption Anmeldebildschirm anmelden, müssen Sie die Java Card einsetzen und Ihren Benutzernamen und die Java Card PIN eingeben.

Konsole Eine zentrale Schnittstelle, über die Sie auf die Merkmale und Einstellungen des Programms zugreifen und sie verwalten können.

Kryptographie Verschlüsseln und Entschlüsseln von Daten mit dem Ergebnis, dass sie nur von bestimmten Personen decodiert werden können.

Kryptographiediensteanbieter (Cryptographic Service Provider = CSP) Provider oder Bibliothek kryptografischer Algorithmen, die auf einer klar definierten Oberfläche verwendet werden können, um bestimmte kryptografische Funktionen auszuführen.

Liste der vertrauenswürdigen Kontaktpersonen Eine Liste der vertrauenswürdigen Kontaktpersonen.

Live Messenger History Viewer Eine Komponente von Privacy Manager Chat, mit der Sie nach verschlüsselten Chat-Protokollsitzungen suchen und sie anzeigen können.

Manuelles Shreddern Das sofortige Shreddern eines Datenbestands oder ausgewählter Datenbestände unter Umgehung des Zeitplans für automatisches Shreddern.

Menü-Übersicht Eine zentrale Schnittstelle, über die Sie auf die Merkmale und Einstellungen des Programms zugreifen und sie verwalten können.

Migration Eine Aufgabe, die das Verwalten, Wiederherstellen und Übertragen von Privacy Manager Zertifikaten und vertrauenswürdigen Kontaktpersonen ermöglicht.

Netzwerkkonto Windows Benutzer- oder Administratorkonto auf einem lokalen Computer, in einer Arbeitsgruppe oder auf einer Domäne.

Neustart Vorgang, bei dem ein bereits laufender Computer erneut gestartet wird.

Notfallwiederherstellungsarchiv Geschützter Speicherbereich, der die erneute Verschlüsselung der allgemeinen Benutzerschlüssel aus dem Schlüssel eines Plattformeigentümers für eine andere ermöglicht.

PKI Public Key Infrastructure. Standard, der die Schnittstellen zur Erstellung, Verwendung und Verwaltung von Zertifikaten und Kryptographie-Schlüsseln definiert.

Privacy Manager Zertifikat Ein digitales Zertifikat, das jedes Mal eine Authentifizierung erforderlich macht, wenn es zur Verschlüsselung verwendet wird, z. B. um E-Mail-Nachrichten und Microsoft Office Dokumente zu signieren und zu verschlüsseln.

PSD PSD-Laufwerk (Personal Secure Drive). Bietet einen geschützten Speicherbereich für sensible Daten.

SATA-Gerätemodus Datenübertragungsmodus zwischen einem Computer und Massenspeichergeräten, z. B. Festplatten und optischen Laufwerken.

Schaltfläche „Sicher Senden“ Eine Softwareschaltfläche in der Symbolleiste von Microsoft Outlook-E-Mail-Nachrichten. Klicken Sie auf diese Schaltfläche, um eine Microsoft Outlook-E-Mail-Nachricht zu signieren und/oder zu verschlüsseln.

Schaltfläche „Signieren und verschlüsseln“ Eine Softwareschaltfläche in der Symbolleiste von Microsoft Office-Anwendungen. Klicken Sie auf diese Schaltfläche, um ein Microsoft Office Dokument zu signieren oder zu verschlüsseln oder die Verschlüsselung für ein Microsoft Office Dokument zu entfernen.

Shreddern Die Ausführung eines Algorithmus, der die Daten in einem Datenbestand überschreibt.

Shred Profil Eine spezielle Löschmethode mit einer Liste von Datenbeständen.

Shred-Zyklus Die Häufigkeit, mit der der Shred-Algorithmus für jeden Datenbestand ausgeführt wird. Je mehr Shred-Zyklen ausgeführt werden, desto sicherer ist der Computer.

Sicherheits-Anmeldemethode Die Methode, mit der Benutzer sich auf dem Computer anmelden.

Sichern Die Verwendung des Sicherungsmerkmals, um eine Kopie von wichtigen Programminformationen außerhalb des Programms zu speichern. Die Kopie kann zu einem späteren Zeitpunkt verwendet werden, um die Informationen auf demselben oder einem anderen Computer wiederherzustellen.

Sichtbar machen Eine Aufgabe, die es dem Benutzer ermöglicht, eine oder mehrere Chat-Protokollsitzungen zu entschlüsseln. Die Contact Screen Names erscheinen daraufhin in normalem Text, und die Sitzung kann angezeigt werden.

Signaturzeile Ein Platzhalter zur optischen Markierung einer digitalen Signatur. Wenn ein Dokument signiert ist, werden der Name des Signierers und die Überprüfungsmethode angezeigt. Das Signierungsdatum und der Titel des Signierers können ebenfalls einbezogen werden.

Smart Card Kleines Hardware-Gerät, das in etwa die Größe und Form einer Kreditkarte aufweist und auf dem Identifizierungsinformationen über den Besitzer gespeichert werden. Wird zur Authentifizierung des Besitzers an einem Computer verwendet.

SSO (Single Sign On) Funktion, die Authentifizierungsdaten speichert und den Zugriff auf Internet- und Windows Anwendungen mit Kennwortauthentifizierung über den Security Manager ermöglicht.

Tastenfolge Eine Kombination aus bestimmten Tasten, die gedrückt wird, um einen automatischen Shred-Vorgang auszulösen, z. B. strg+alt+s.

Token Siehe Sicherheits-Anmeldemethode.

Trusted Contact Eine Person, die eine Einladung an vertrauenswürdige Kontaktperson(en) angenommen hat.

TXT Trusted Execution Technology.

Überschreiben von freiem Speicherplatz Das sichere Überschreiben gelöschter Datenbestände mit willkürlichen Daten, um den Inhalt der gelöschten Datenbestände unwiderruflich zu vernichten.

USB-Token Sicherheitsgerät, das Identifizierungsinformationen eines Benutzers speichert. Genau wie eine Java Card oder ein biometrisches Lesegerät wird es zur Authentifizierung eines Benutzers auf einem Computer verwendet.

Verschlüsselung Vorgang, wie z. B. die Verwendung eines Algorithmus, der in der Kryptografie zur Konvertierung reinen Texts in Zifferntext verwendet wird, um zu vermeiden, dass unberechtigte Empfänger diese Daten lesen. Es gibt viele Arten der Datenverschlüsselung. Sie bilden die Basis der Netzwerksicherheit. Zu den bekannten Arten gehören der Verschlüsselungsalgorithmus DES (Data Encryption Standard) und die Verschlüsselung mit öffentlichen Schlüsseln.

Versiegeln für Vertrauenswürdige Kontaktpersonen Eine Aufgabe, die eine digitale Signatur hinzufügt, die E-Mail verschlüsselt und sie versendet, nachdem Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode authentifiziert haben.

Vertrauenswürdige IM-Kommunikation Eine Kommunikationssitzung, während der vertrauenswürdige Nachrichten von einem vertrauenswürdigen Absender an eine vertrauenswürdige Kontaktperson gesendet werden.

Vertrauenswürdige Nachricht Eine Kommunikationssitzung, während der vertrauenswürdige Nachrichten von einem vertrauenswürdigen Absender an eine vertrauenswürdige Kontaktperson gesendet werden.

Vertrauenswürdiger Absender Eine vertrauenswürdige Kontaktperson, die signierte und/oder verschlüsselte E-Mails und Microsoft Office Dokumente versendet.

Virtuelles Token Sicherheitsmerkmal, das ähnlich wie eine Java Card in einem Lesegerät funktioniert. Das Token wird auf der Festplatte des Computers oder in der Windows Registrierung gespeichert. Wenn Sie sich mit einem virtuellen Token anmelden, wird zur Vervollständigung der Authentifizierung eine Benutzer-PIN angefordert.

Widerruf-Kennwort Ein Kennwort, das erstellt wird, wenn ein Benutzer ein digitales Zertifikat anfordert. Der Benutzer benötigt das Kennwort, um sein digitales Zertifikat zu widerrufen. Dadurch wird sichergestellt, dass nur der Benutzer in der Lage ist, das Zertifikat zu widerrufen.

Wiederherstellen Ein Vorgang, bei dem Programminformationen von einer zuvor erstellten Sicherungsdatei in das entsprechende Programm kopiert werden.

Windows Administrator Ein Benutzer mit umfassenden Rechten zum Ändern von Berechtigungen und Verwalten anderer Benutzer.

Windows Anmeldesicherheit Schützt Ihr(e) Windows Konto/Konten, indem die Verwendung von bestimmten Anmeldedaten für den Zugriff erfordert wird.

Windows Benutzerkonto Profil für eine Person mit der Berechtigung, sich in einem Netzwerk oder an einem bestimmten Computer anzumelden.

Zertifizierungsstelle Dienst, der die erforderlichen Zertifikate zur Ausführung einer Infrastruktur mit öffentlichen Schlüsseln ausstellt.

Index

Z