HP ProtectTools for Small Business Sicherheitssoftware, Version 5.10

Benutzerhandbuch

HP ProtectTools for Small Business Sicherheitssoftware, Version 5.10, Benutzerhandbuch

HP Business PC

Zweite Ausgabe: Mai 2010

Teilenummer des Dokuments: 610663-042

Allgemeines

Dieses Handbuch enthält Informationen zur HP ProtectTools for Small Business Sicherheitssoftware.

⚠ **VORSICHT!** In dieser Form gekennzeichneter Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anleitungen hin.

△ **ACHTUNG:** In dieser Form gekennzeichneter Text weist auf die Gefahr von Hardware-Schäden oder Datenverlust bei Nichtbefolgen der Anleitungen hin.

HINWEIS: In dieser Form gekennzeichneter Text weist auf wichtige Zusatzinformationen hin.

Inhaltsverzeichnis

1 Einführung in die Sicherheitsfunktionen

HP weiß, dass Ihre Zeit sehr wertvoll ist. Sie müssen sich darauf konzentrieren, Ihre Geschäfte zu führen und auszuweiten und möchten sich keine Gedanken über die geeignete Sicherheitssoftware machen, mit der Sie PC, Daten und Unternehmen schützen.

Es ist wichtig, dass Sie sich proaktiv mit Sicherheitslösungen befassen, die benutzerfreundlich sind und dennoch einen starken Schutz für Ihre Unternehmensressourcen bieten. Sicherheit ist kein „Luxus“, sondern ein „Muss“!

HP bietet leicht zu implementierenden und benutzerfreundlichen Schutz mit HP ProtectTools for Small Business.

Die Sicherheitssoftware HP ProtectTools for Small Business bietet Funktionen, die den unbefugten Zugriff auf den Computer sowie auf Netzwerke und kritische Daten verhindern. Die verschiedenen HP ProtectTools Softwaremodule bieten erweiterte Sicherheitsfunktionen.

HP ProtectTools for Small Business gibt es in zwei Versionen: HP ProtectTools Security Manager Administrator-Konsole und HP ProtectTools Security Manager (für Standardbenutzer ohne Administratorrechte). Beide Versionen sind im Menü **Start** > **Alle Programme** aufgelistet.

Funktion	Merkmale
HP ProtectTools Security Manager Administrator-Konsole	• Erfordert Microsoft Windows Administratorrechte. • Ermöglicht den Zugriff auf Module, die von einem Administrator konfiguriert werden müssen und Benutzern ohne Administratorrechte nicht zur Verfügung stehen. • Ermöglicht das anfängliche Sicherheitssetup und dient zur Konfiguration von Optionen bzw. Anforderungen für alle Benutzer.
HP ProtectTools Security Manager (für Standardbenutzer)	• Ermöglicht Benutzern die Konfiguration der vom Administrator bereitgestellten Optionen. • Ermöglicht Zugriffsbeschränkungen sowie die Beschränkung von Einstellmöglichkeiten für bestimmte Benutzer bei einer Reihe von HP ProtectTools Modulen.

Die Module der HP ProtectTools Software sind entweder vorinstalliert, auf der Festplatte vorhanden oder als konfigurierbare Option bzw. After-Market-Option erhältlich. Weitere Informationen hierzu finden Sie unter http://www.hp.com.

HP ProtectTools Funktionen

Die folgende Tabelle enthält Einzelheiten zu den wichtigsten Modulfunktionen von HP ProtectTools for Small Business:

Modul	Funktionen
HP ProtectTools Security Manager Administrator-Konsole	• Der Security Manager Installationsassistent wird von Administratoren verwendet, um Sicherheitsstufen und Sicherheits-Anmeldemethoden einzurichten und zu konfigurieren. • Ermöglicht die Konfiguration von Optionen, die Standardbenutzern nicht angezeigt werden. • Ermöglicht die Konfiguration von Device Access Manager und des Benutzerzugriffs. • Mit den Administrator-Tools können HP ProtectTools Benutzer hinzugefügt oder entfernt und der Benutzerstatus angezeigt werden.
HP ProtectTools Security Manager (für Standardbenutzer)	• Ermöglicht die Verwaltung, Einrichtung und Änderung von Benutzernamen und -kennwörtern. • Ermöglicht die Konfiguration und Änderung von Anmeldeinformationen wie beispielsweise Windows und Smart Card-Kennwort. • Ermöglicht die Konfiguration und Änderung von File Sanitizer Funktionen für das Shreddern und Bereinigen sowie von File Sanitizer Einstellungen. • Ermöglicht das Anzeigen von Einstellungen für Device Access Manager. • Ermöglicht die Konfiguration von Einstellungen sowie von Sicherungs- und Wiederherstellungsoptionen.
Credential Manager for HP ProtectTools (Password Manager)	• Ermöglicht die Speicherung, die Verwaltung und den Schutz Ihrer Benutzernamen und -kennwörter. • Ermöglicht die Einrichtung von Anmeldebildschirmen für Websites und Programme, sodass Sie sich besonders schnell und sicher dort anmelden können. • Wenn Sie auf verschiedene Websites zugreifen und Ihren Benutzernamen und Ihr Kennwort speichern möchten, geben Sie Benutzername und Kennwort in Password Manager ein, um sich die Daten nicht merken zu müssen. Wenn Sie diese Site beim nächsten Mal aufrufen, trägt Password Manager die betreffenden Daten automatisch ein und übergibt sie dem System. • Ermöglicht das Festlegen effizienterer Kennwörter, ohne sich diese notieren oder merken zu müssen, und schützt Ihre Konten zuverlässiger.

Modul	Funktionen
Drive Encryption for HP ProtectTools	• Ermöglicht die vollständige Datenträgerverschlüsselung für eine Festplatte. • Erfordert die Authentifizierung vor dem Systemstart, um die Festplatte zu entschlüsseln und den Datenzugriff zu gewähren. • Unterstützt Sie bei der Einhaltung von rechtlichen Bestimmungen oder Branchenanforderungen beim Schutz von wichtigen und vertraulichen Daten. • Schützt Ihre Daten vor unberechtigtem Zugriff durch Verschlüsseln der gesamten Festplatte. Für den Fall, dass der Computer gestohlen und das Laufwerk aus dem ursprünglichen System entfernt und in ein anderes System eingebaut wird, sind die Daten nicht gefährdet.
File Sanitizer for HP ProtectTools	• Beim Löschen von Daten in Windows wird der Inhalt nicht vollständig von der Festplatte entfernt. Windows löscht lediglich den Verweis auf die Daten. Die Daten bleiben so lange auf der Festplatte, bis eine andere Datei diesen Bereich auf der Festplatte mit neuen Daten überschreibt. Mit File Sanitizer können Sie Dokumente, den Verlauf des Webbrowsers, temporäre Dateien usw. jedoch vollständig und automatisch löschen. • Ermöglicht das sichere Löschen (oder Shreddern) kritischer Dateien und Ordner (persönliche Daten oder Dateien, Verlaufs- oder webbezogene Daten sowie andere Datenkomponenten) auf Ihrem Computer und die regelmäßige Bereinigung (Überschreiben zuvor gelöschter Daten) Ihrer Festplatte.
Device Access Manager for HP ProtectTools	• Kann zum Steuern des Zugriffs auf Medienlaufwerke, USB- und andere Hardwaregeräte auf der Basis von Benutzerprofilen verwendet werden. • Erlaubt Ihnen, die Möglichkeiten eines Benutzers zum Speichern kritischer Daten einzuschränken. • Verhindert, dass Benutzer über externe Speichergeräte (z. B. persönliche Music Player) Daten von einem PC oder vom Netzwerk kopieren können. • Verhindert, dass Benutzer Viren von externen Medien in das System einschleusen. • Ermöglicht die selektive Deaktivierung einer Gruppe von Geräten (z. B. USB-Sticks, beschreibbare Geräte, persönliche Musik Player usw.) nach dem Benutzer oder nach der Benutzergruppe. Die Person mit einem Administratorkennwort kann sich anmelden und Daten vom PC kopieren; andere Benutzer können dies nicht.

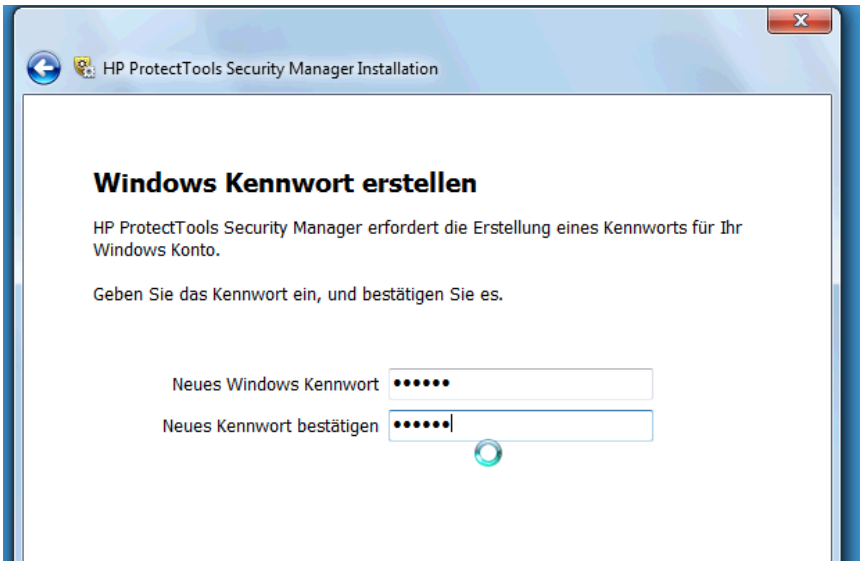
2 Kurzanleitung zur Einrichtung für die nützlichsten Optionen

Diese Kurzanleitung zur Einrichtung erläutert die grundlegenden Schritte zur Aktivierung der am häufigsten verwendeten und nützlichsten Optionen in HP ProtectTools for Small Business. Diese Software verfügt über zahlreiche Tools und Optionen, mit denen Sie Ihre Einstellungen optimieren und eine Zugriffssteuerung einrichten können. Die Kurzanleitung zur Einrichtung erläutert, wie sich jedes Modul mit möglichst wenig Einrichtungs- und Zeitaufwand verwenden lässt. Wenn Sie zusätzliche Informationen benötigen, wählen Sie einfach das gewünschte Modul aus und klicken auf das Fragezeichen (?) oder die Schaltfläche „Hilfe“ in der oberen rechten Ecke. Diese Schaltfläche stellt automatisch Informationen bereit, die Sie bei der Arbeit mit dem angezeigten Fenster unterstützen.

Einführung

1. Öffnen Sie HP ProtectTools Security Manager über das Programmsymbol oder das Taskleistensymbol (goldenes Schild), oder klicken Sie auf **Start** > **Alle Programme** > **HP**.

2. Geben Sie Ihr Windows Kennwort ein, oder erstellen Sie ein Windows Kennwort.

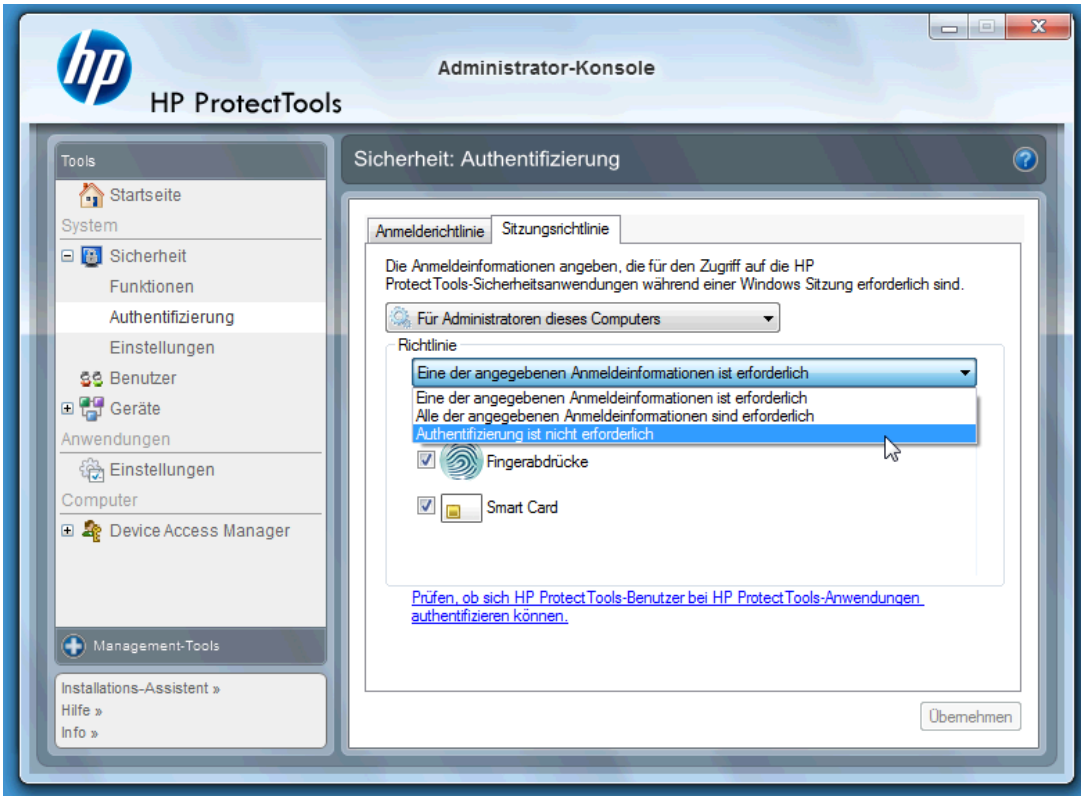


3. Führen Sie den Installationsassistenten aus.

HINWEIS: HP ProtectTools Security Manager ist standardmäßig auf eine starke Authentifizierung eingestellt.

Diese Einstellung soll einen nicht autorisierten Zugriff verhindern, während der Benutzer bei Windows angemeldet ist. Sie sollte verwendet werden, wenn eine hohe Sicherheit erforderlich ist oder wenn ein Benutzer häufig nicht am Platz ist. Wenn Sie diese Einstellung ändern möchten, klicken Sie auf die Registerkarte „Sitzungsrichtlinie“ und wählen die gewünschten Optionen aus.

Ändern Sie die folgende Konfiguration, um HP ProtectTools Security Manager so zu konfigurieren, dass die Windows Anmeldung für die gesamte Sitzung verwendet wird.



So führt HP ProtectTools Security Manager die Authentifizierung nur einmal während der Windows Anmeldung aus:

1. Klicken Sie auf **Start** > **Alle Programme** > **HP** > **HP ProtectTools Administrator-Konsole**.
2. Wählen Sie im linken Fenster **Tools** die Option **Authentifizierung** aus der Gruppe **Sicherheit**.
3. Klicken Sie auf die Registerkarte **Sitzungsrichtlinie**, und wählen Sie **Authentifizierung ist nicht erforderlich** aus dem Dropdown-Menü unter **Richtlinie**.
4. Klicken Sie auf **Übernehmen**, wenn Sie fertig sind.

Credential Manager for HP ProtectTools (Password Manager)

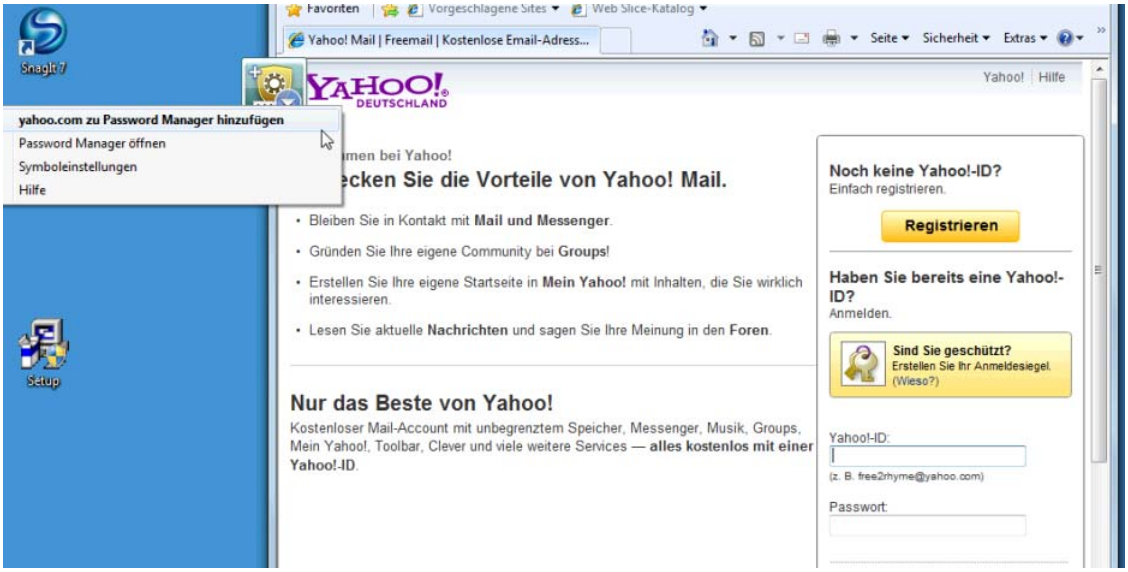
Kennwörter! Davon haben Sie sicher auch jede Menge, vor allem dann, wenn Sie regelmäßig auf Websites zugreifen oder Anwendungen nutzen, die eine Anmeldung erfordern. Der Standardbenutzer verwendet entweder dasselbe Kennwort für alle Anwendungen und Websites oder wird kreativ und vergisst prompt, welches Kennwort zu welcher Anwendung gehört.

Wäre es nicht besser, wenn eine Software die Kennwörter für nicht kritische Sites automatisch speichern würde oder Sie auswählen könnten, welche Sites gespeichert werden sollen und welche nicht? Mit Credential Manager for HP ProtectTools ist dies möglich. Credential Manager ist ein Password Manager mit den entsprechenden Fähigkeiten. Sobald Sie sich am PC anmelden, stellt Credential Manager Ihre Kennwörter oder Anmeldeinformationen nach Bedarf bereit.

Beim Öffnen einer Anwendung oder einer Website, für die eine Anmeldung erforderlich ist, erkennt Credential Manager die Site automatisch und fragt, ob die Software die Informationen speichern soll. Wenn Sie dem zustimmen, müssen Sie sich dieses Kennwort nie wieder merken. Sie können es auch ablehnen, Daten zu speichern, wenn Sie bestimmte Sites ausschließen möchten.

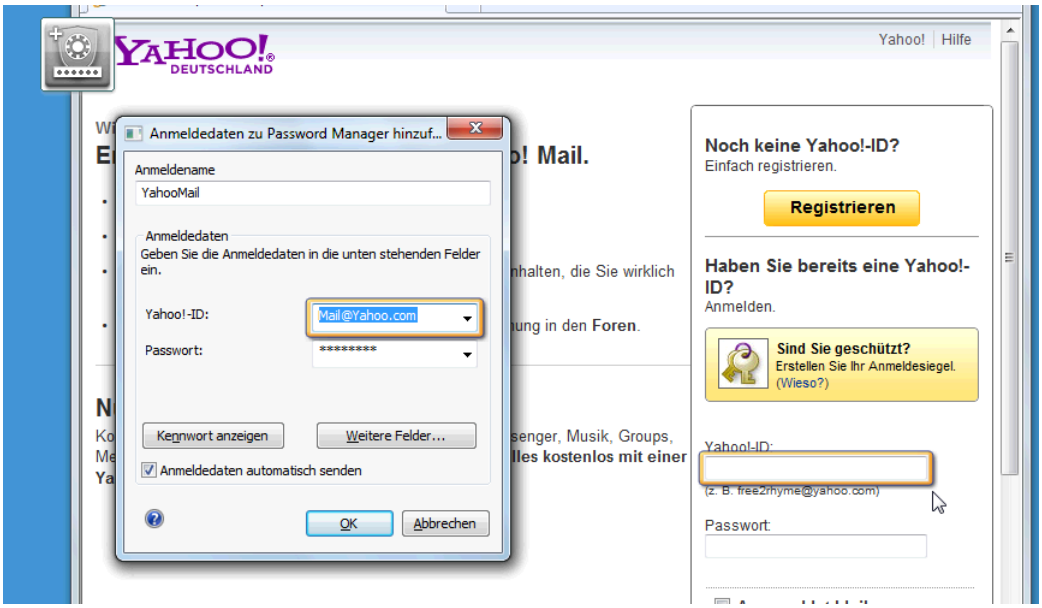
So beginnen Sie mit dem Speichern von Websites, Benutzernamen und Kennwörtern:

1. Öffnen Sie beispielsweise Ihr Web-Mail-Konto, und fügen Sie die Webauthentifizierung mithilfe von Credential Manager (indem Sie auf das Symbol klicken) hinzu.



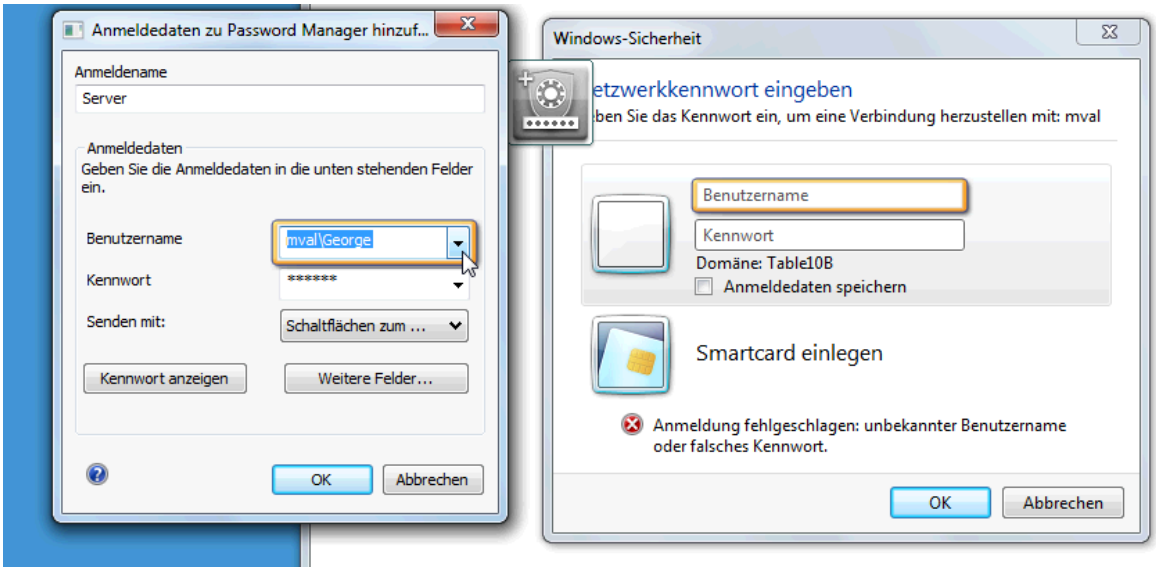
2. Vergeben Sie einen Namen für den Link (optional), und geben Sie einen Benutzernamen und ein Kennwort in Credential Manager ein.

HINWEIS: Auf der Website werden die Bereiche hervorgehoben, die von Credential Manager jetzt und für spätere Aufrufe verwendet werden.



3. Wenn Sie fertig sind, klicken Sie auf die Schaltfläche **OK**.

4. Credential Manager kann Ihren Benutzernamen und Ihre Kennwörter auch für Netzwerkfreigaben oder die Zuordnung von Netzwerklaufwerken speichern.



Anzeigen und Verwalten der gespeicherten Authentifizierungsinformationen in Credential Manager

Credential Manager bietet den Vorteil, dass Sie Ihre Authentifizierungsinformationen zentral anzeigen, verwalten, sichern und aufrufen können. Credential Manager unterstützt darüber hinaus das Aufrufen gespeicherter Sites von Windows.

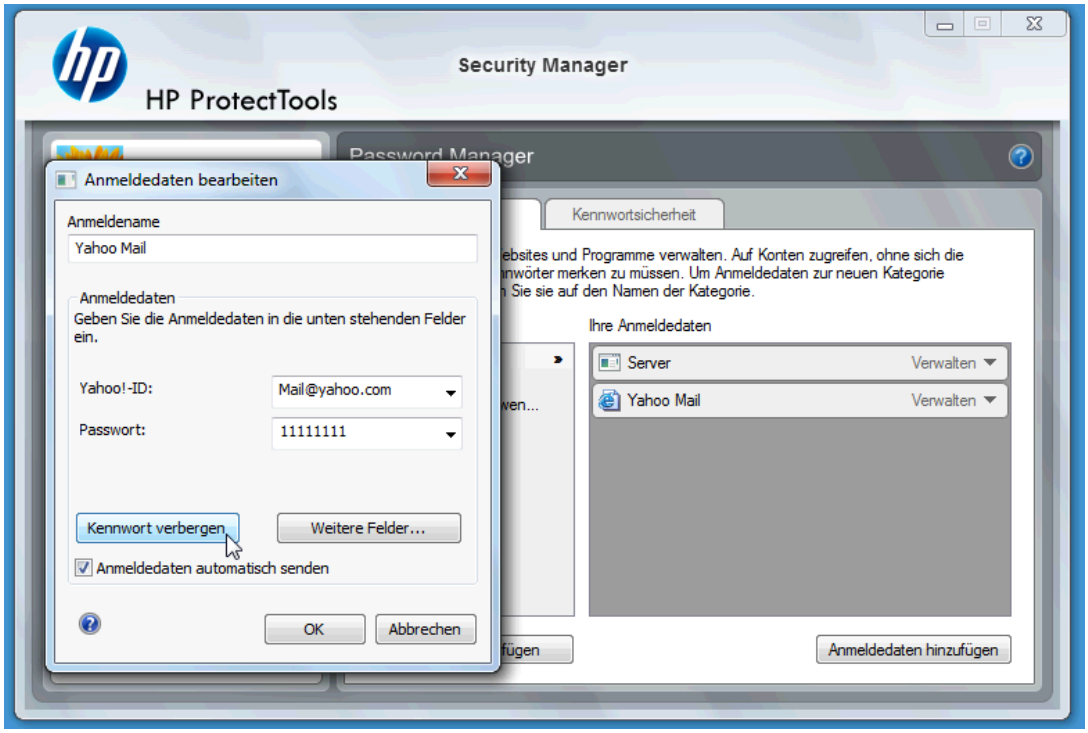
Verwenden Sie eine der beiden folgenden Vorgehensweisen, um Password Manager zu öffnen:

- Verwenden Sie die Tastenkombination Strg + Windows + H, um Password Manager zu öffnen. Durch Auswahl von **Öffnen** wird die gespeicherte Verknüpfung schnell aufgerufen und authentifiziert.

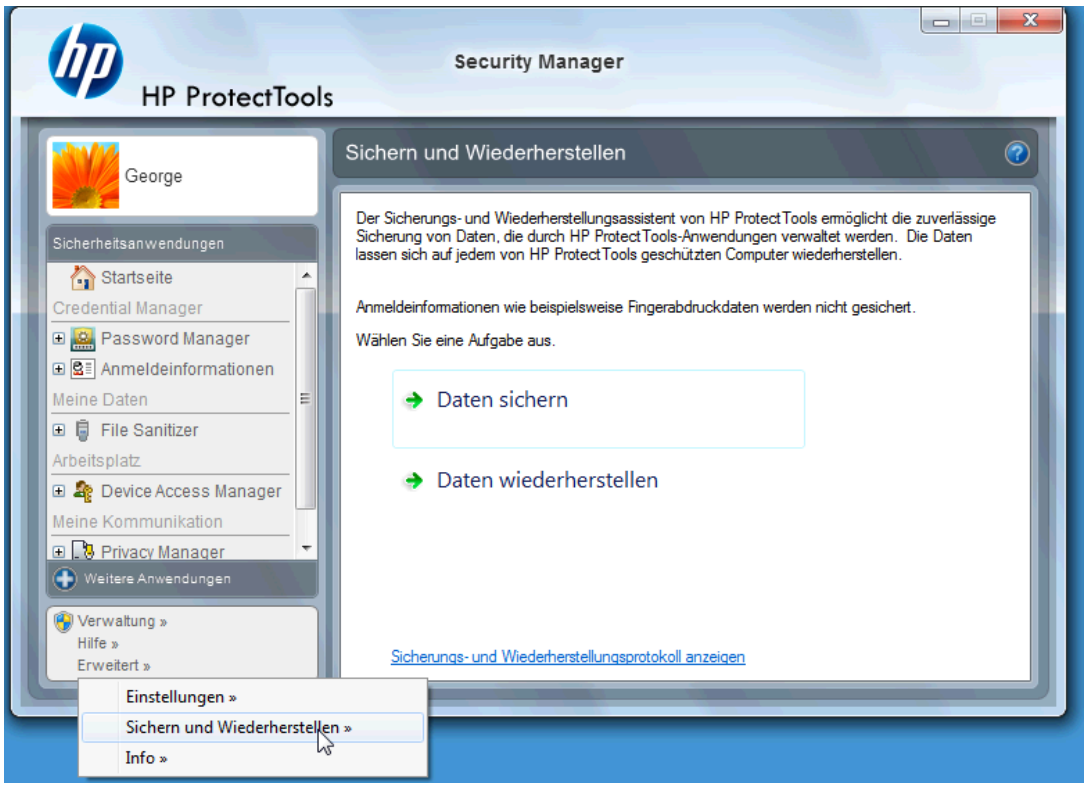
ODER

- Wählen Sie die Registerkarte **Verwalten** in Password Manager aus, und öffnen Sie HP ProtectTools Security Manager, wo Sie die Anmeldeinformationen bearbeiten können.

Die Option **Bearbeiten** von Credential Manager bietet Ihnen die Möglichkeit, Namen und Anmeldenamen anzuzeigen und zu ändern und sogar die Kennwörter offenzulegen.



Mit HP ProtectTools for Small Business können alle Anmeldeinformationen und Einstellungen gesichert und/oder auf einen anderen PC kopiert werden.



File Sanitizer for HP ProtectTools

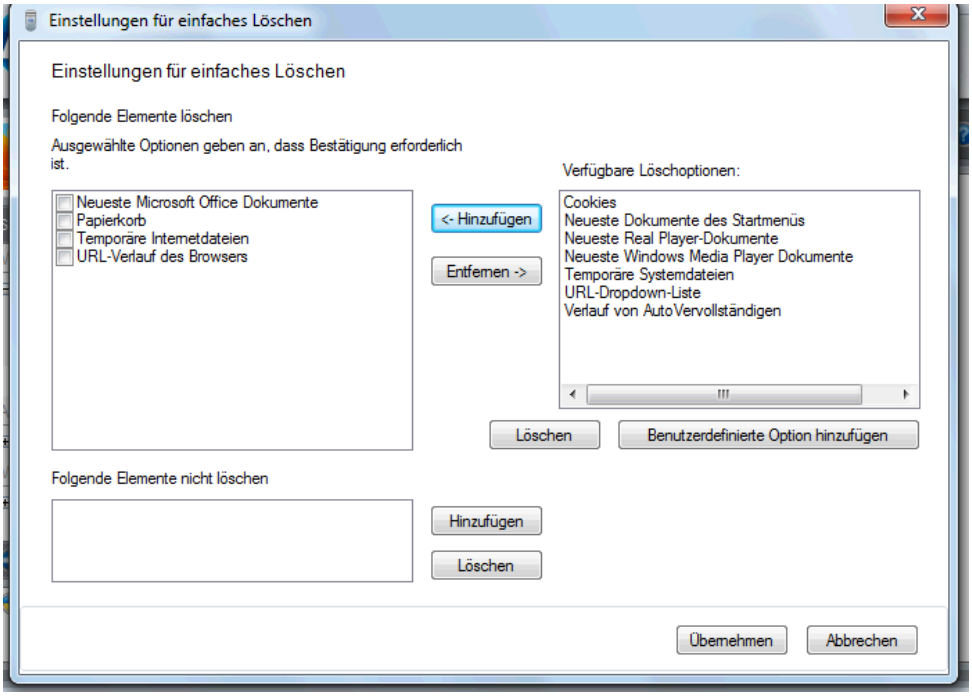
File Sanitizer ist so konzipiert, dass es für nicht autorisierte Personen sehr schwierig ist, gelöschte Daten wiederherzustellen. Ihnen stehen mehrere Optionen zur Verfügung, mit denen Sie ausgewählte Dateien und Ordner, einschließlich des Browser-Verlaufs, manuell löschen oder einen Zeitplan dafür erstellen können.

Nachfolgend sind ein paar einfache Konfigurationseinstellungen aufgeführt.

Um die gelöschten Daten permanent zu entfernen, wählen Sie die nicht mehr benötigten Dateien oder Ordner aus.

1. Gehen Sie zu **Security Manager** > **File Sanitizer** > **Einstellungen**. Wählen Sie **Einstellungen für einfaches Löschen** aus, und klicken Sie auf die Schaltfläche **Details anzeigen**.

2. Wählen Sie anhand der Optionen auf der rechten Seite des Fensters „Einstellungen für einfaches Löschen“ aus, welche Elemente Sie regelmäßig löschen möchten, und klicken Sie auf die Schaltfläche **<-Hinzufügen**, um die ausgewählten Elemente auf die Seite der zu löschenden Elemente zu verschieben.



3. Beginnen Sie mit dem Papierkorb, und fügen Sie andere Elemente hinzu, die Sie durch Shreddern entfernen möchten.

4. Klicken Sie auf die Schaltfläche **Übernehmen**, wenn Sie alle Elemente ausgewählt haben, die Sie permanent löschen möchten.

5. Klicken Sie auf die Option **Shreddern**, und konfigurieren Sie den Zeitpunkt der Aktion. Mit der Schaltfläche **Jetzt shreddern** werden die im Fenster „Einstellungen für einfaches Löschen“ ausgewählten Elemente, die Sie gerade konfiguriert haben, sofort gelöscht.

6. In der Taskleiste wird jedes Mal eine Meldung angezeigt, wenn die Shredder-Funktion startet und stoppt.

Device Access Manager for HP ProtectTools

Mit Device Access Manager können Sie die Verwendung verschiedener interner und externer Speichergeräte einschränken, sodass die Daten sicher auf der Festplatte und in Ihrem Büro bleiben. Sie können einem Benutzer zum Beispiel Zugriff auf Ihre Daten gewähren, das Kopieren der Daten auf eine CD, einen persönlichen Music Player oder ein USB-Speichergerät jedoch blockieren. Im Folgenden ist eine einfache Vorgehensweise beschrieben.

1. Klicken Sie auf **Start** > **Alle Programme** > **HP** > **Administrator-Konsole** > **Device Access Manager** > **Einfache Konfiguration**.

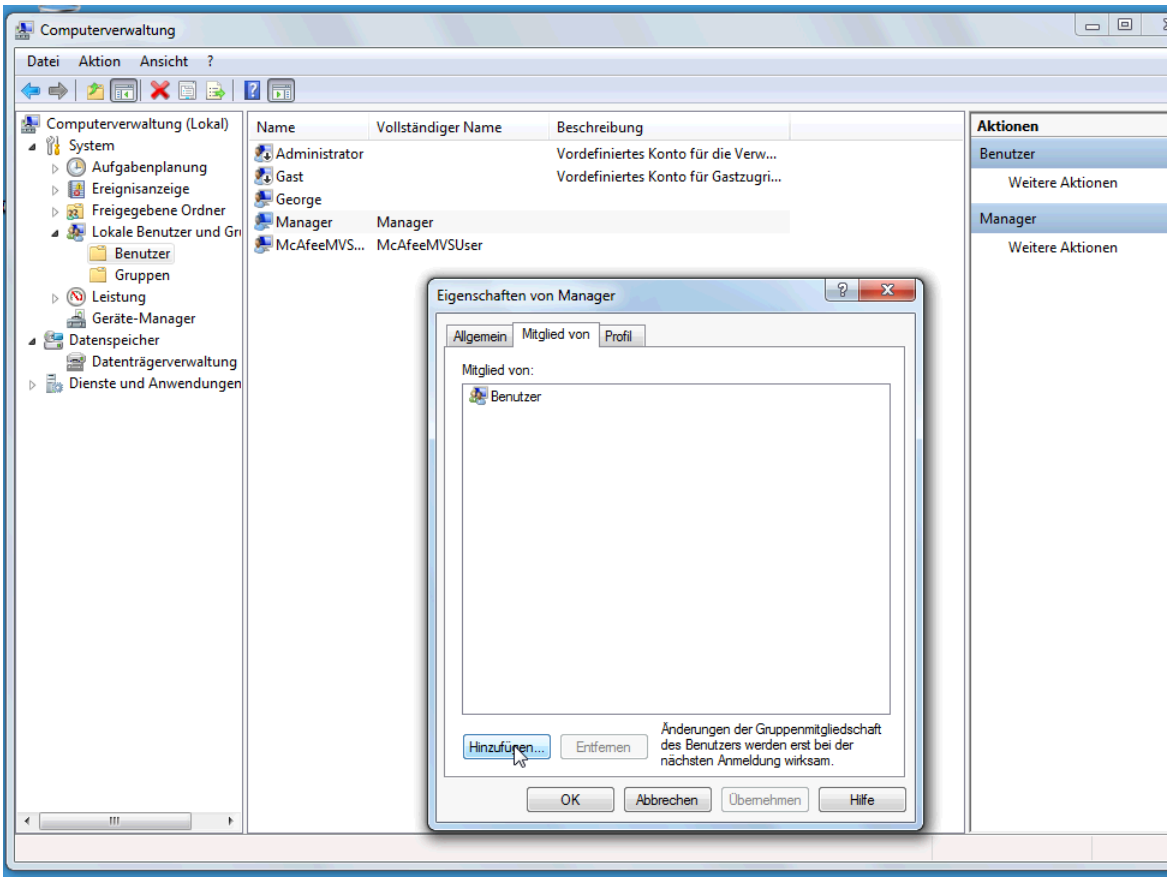
2. Wählen Sie die Hardwaregeräte aus, für die Sie eine Einschränkung festlegen möchten, und klicken Sie auf die Schaltfläche **Übernehmen**, um den Vorgang abzuschließen.

3. Danach müssen Sie auswählen, wer weiterhin Zugriff erhalten soll. Alle anderen Benutzer werden dann gesperrt werden.

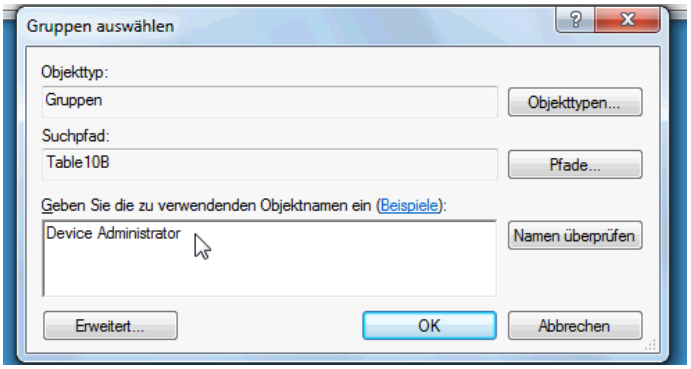
4. Gehen Sie zu **Computer**, und wählen Sie den Eintrag aus. Klicken Sie mit der rechten Maustaste, und wählen Sie **Verwalten** > **Computerverwaltung** > **Systemprogramme** > **Lokale Benutzer und Gruppen** > **Benutzer**.

5. Doppelklicken Sie auf den Benutzer (in diesem Beispiel „Manager“), der weiterhin Zugriff auf die blockierte Hardware haben soll.

6. Klicken Sie auf der Registerkarte **Mitglied von** auf die Schaltfläche **Hinzufügen**.



7. Im Fenster **Gruppen auswählen** können Sie entweder auf die Schaltfläche **Erweitert** klicken oder „Device Administrator“ eingeben. Klicken Sie auf die Schaltfläche **OK**, und schließen Sie die Fenster durch Klicken auf die Schaltflächen **OK**. Sie müssen sich ab- und wieder anmelden, um die Berechtigungen zu erhalten.



Alle internen und externen Speichergeräte (einschließlich CD-Laufwerke, USB-Laufwerke, persönliche Music Player usw.) funktionieren nun nur noch bei den Personen, die in der Gruppe „Device Administrator“ enthalten sind.

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools ist ein Programm, das Ihre Daten durch Verschlüsseln der gesamten Festplatte schützt. Die Daten auf Ihrer Festplatte sind auch dann geschützt, wenn Ihr Computer gestohlen wird und/oder die Festplatte aus dem ursprünglichen System aus- und in ein anderes System eingebaut wird.

Ein weiteres Sicherheitsmerkmal besteht darin, dass Drive Encryption eine Authentifizierung mit Benutzernamen und Kennwort erfordert, bevor das System gestartet wird. Dieser Prozess wird als Authentifizierung beim Systemstart bezeichnet.

Zur Vereinfachung der Kennwortsynchronisation arbeiten die Windows Benutzeranmeldung, Domänen, Credential Manager for HP ProtectTools und HP ProtectTools Security Manager mit Drive Encryption zusammen.

Anhand der folgenden einfachen Schritte können Sie Drive Encryption for HP ProtectTools aktivieren.

1. Klicken Sie auf **Start** > **Alle Programme** > **HP** > **HP ProtectTools Administrator-Konsole** > **Management-Tools** > **Installations-Assistent**. Der folgende Bildschirm wird angezeigt:

2. Wählen Sie im Begrüßungsbildschirm **Weiter**.
3. Zum Starten des Aktivierungsassistenten ist ein Windows Kennwort erforderlich > **Weiter**.
4. Markieren Sie das Kontrollkästchen **Drive Encryption**, und wählen Sie **Weiter**.

5. Das unten abgebildete Drive Encryption-Fenster zeigt die für die Verschlüsselung zur Verfügung stehenden Laufwerke an. Außerdem muss ein USB-Speichergerät zum Sichern des Chiffrierschlüssels angegeben werden. Bewahren Sie diesen Chiffrierschlüssel an einem sicheren Ort auf. Sie benötigen ihn, um Daten wiederherzustellen oder auf das Laufwerk zuzugreifen, falls das Kennwort für den Systemstart verloren geht oder nicht mehr gültig ist.

6. Wählen Sie **Weiter**, um den Vorgang abzuschließen, und wählen Sie anschließend **Fertig stellen**. Entfernen Sie das USB-Speichergerät, wenn Sie dazu aufgefordert werden, und starten Sie anschließend das System neu.

7. Wenn das System von der Festplatte startet, werden Sie von Drive Encryption zur Eingabe Ihres Windows Kennworts aufgefordert. Geben Sie das Kennwort ein, und klicken Sie auf **OK**.

HINWEIS: Der Computer läuft möglicherweise langsamer, während das Laufwerk verschlüsselt wird. Sobald der Verschlüsselungsvorgang abgeschlossen ist, arbeitet das System wieder mit normaler Geschwindigkeit. Beim Zugriff auf Daten, die sich auf dem Laufwerk befinden, werden diese, je nach Bedarf, ver- und entschlüsselt.

Die Drive Encryption-Authentifizierung gilt gleichzeitig als Credential Manager Windows-Anmeldung, so dass direkt der Desktop angezeigt wird, ohne dass Sie Ihr Kennwort noch einmal eingeben müssen.

3 Vorteile von HP ProtectTools for Small Business

Zugriff auf die HP ProtectTools for Small Business Sicherheitssoftware

So greifen Sie im Windows Startmenü auf HP ProtectTools Security Manager zu:

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

So greifen Sie im Windows Startmenü auf die HP ProtectTools Security Manager Administrator-Konsole zu:

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

Lösungen für grundlegende Sicherheitsaufgaben

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

- Einschränken des Zugriffs auf sensible Daten
- Verhindern des unbefugten Zugriffs von internen oder externen Standorten
- Erstellen von Richtlinien für den starken Kennwortschutz

Einschränken des Zugriffs auf sensible Daten

Falls beispielsweise ein externer Prüfer im Unternehmen tätig ist und Zugriff auf sensible Finanzdaten erhalten hat, soll diese Person dennoch nicht in der Lage sein, die betreffenden Dateien zu drucken oder auf einem beschreibbaren Datenträger wie z. B. einer CD zu speichern. Mit der folgenden Funktion lässt sich der Datenzugriff beschränken:

Mit Device Access Manager for HP ProtectTools können Administratoren den Zugriff auf beschreibbare Geräte einschränken, um das Drucken oder Kopieren von sensiblen Informationen von der Festplatte auf Wechselmedien zu verhindern. Siehe „Geräteklassen-Konfiguration (erweitert)“ auf Seite 52.

Verhindern des unbefugten Zugriffs von internen oder externen Standorten

Der unberechtigte Zugriff auf ungeschützte Geschäfts-PCs ist eine ernsthafte Gefährdungsquelle für kritische Daten, wie beispielsweise Informationen der Finanzbuchhaltung, der Geschäftsführung oder der F&E-Abteilung. Auch persönliche Informationen wie Patientenakten oder persönliche Finanzinformationen sind gefährdet. Die folgenden Funktionen verhindern den unberechtigten Datenzugriff:

- Wenn die Authentifizierung vor dem Systemstart aktiviert ist, verhindert sie den Zugriff auf das Betriebssystem. Siehe auch folgende Kapitel:
  - „Credential Manager for HP ProtectTools (Password Manager)“ auf Seite 37
  - „Drive Encryption for HP ProtectTools“ auf Seite 34
- Credential Manager for HP ProtectTools stellt sicher, dass unberechtigte Benutzer nicht in den Besitz von Kennwörtern gelangen oder auf kennwortgeschützte Anwendungen zugreifen können. Siehe auch folgendes Kapitel:
  - „Credential Manager for HP ProtectTools (Password Manager)“ auf Seite 37
- Mit Device Access Manager for HP ProtectTools können Administratoren den Zugriff auf beschreibbare Geräte einschränken, um das Kopieren von sensiblen Informationen zu verhindern, die sich auf der Festplatte befinden. Siehe auch folgendes Kapitel:
  - „Device Access Manager for HP ProtectTools“ auf Seite 51
- File Sanitizer ermöglicht das sichere Löschen von Daten, indem kritische Dateien und Ordner geshreddert werden oder die Festplatte bereinigt wird (Überschreiben von Daten, die vorher gelöscht wurden, aber noch auf der Festplatte vorhanden sind, um die Wiederherstellung dieser Daten zu erschweren). Siehe auch folgendes Kapitel:
  - „File Sanitizer for HP ProtectTools“ auf Seite 42

Erstellen von Richtlinien für den starken Kennwortschutz

Wenn Sie einen starken Kennwortschutz (d. h. komplexe, schwer zu hackende Kennwörter) für eine Reihe von webbasierten Anwendungen und Datenbanken benötigen, bietet Credential Manager for HP ProtectTools ein geschütztes Repository für Kennwörter und Single Sign On-Anmeldung zur Verfügung. Siehe auch folgendes Kapitel:

- „Credential Manager for HP ProtectTools (Password Manager)“ auf Seite 37

Weitere Sicherheitselemente

Zuweisen von Sicherheitsrollen

Beim ordnungsgemäßen Schutz der Daten werden Zuständigkeiten und Berechtigungen häufig auf verschiedene Arten von Administratoren und Benutzern verteilt.

HINWEIS: In einem kleinen Unternehmen oder für die individuelle Benutzung können diese Rollen von derselben Person verwaltet werden.

Bei HP ProtectTools for Small Business können die Sicherheitspflichten und -rechte auf die folgenden Rollen verteilt werden:

- Administrator – wendet Sicherheitsfunktionen an und verwaltet sie. Kann manche Funktionen auch aktivieren und deaktivieren.
- Benutzer – verwendet die Sicherheitsfunktionen.

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.

Diese Tabelle enthält auch die Kennwörter, die ausschließlich von Administratoren festgelegt und verwendet werden können. Alle anderen Kennwörter können von Standardbenutzern festgelegt werden.

HP ProtectTools Kennwort	In diesem HP ProtectTools Modul eingerichtet	Funktion
Password Manager Anmeldekennwort	Password Manager	Dieses Kennwort bietet 2 Optionen: • Es kann für einen separaten Anmeldevorgang verwendet werden, um nach der Anmeldung bei Windows auf Password Manager zugreifen zu können. • Es kann anstelle der Windows Anmeldung verwendet werden, um sich gleichzeitig bei Windows und Password Manager anmelden zu können.

HP ProtectTools Kennwort	In diesem HP ProtectTools Modul eingerichtet	Funktion
Kennwort für Computer Setup **HINWEIS:** Auch bekannt als BIOS-Administrator-, F10-Setup- oder Sicherheits-Setup-Kennwort	BIOS (durch Administrator)	Schützt den Zugriff auf Computer Setup Utility.
Systemstart-Kennwort	BIOS	Schützt den Zugriff auf die Daten auf dem Computer, wenn der Computer eingeschaltet oder neu gestartet wird bzw. wenn der Ruhezustand beendet wird.
Windows Anmeldekennwort	Windows Systemsteuerung	Kann für die manuelle Anmeldung verwendet werden.

Einrichten 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.
- Verwenden Sie Groß- und Kleinschreibung innerhalb des Kennworts.
- Verwenden Sie nach Möglichkeit 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 von Zugangsdaten und Einstellungen

Verwenden Sie das Tool „Backup and Recovery“ in HP ProtectTools Security Manager als zentralen Ort zum Sichern und Wiederherstellen von Sicherheitsinformationen aus installierten HP ProtectTools Modulen.

4 HP ProtectTools Security Manager Administrator-Konsole

Informationen zur HP ProtectTools Administrator-Konsole

Die Verwaltung von HP ProtectTools Security Manager erfolgt über die zugehörige Administrator-Konsole.

Sie bietet dem lokalen Administrator folgende Möglichkeiten:

- Aktivieren und Deaktivieren von Sicherheitsfunktionen
- Verwalten von Computerbenutzern
- Festlegen von gerätespezifischen Parametern
- Konfigurieren von Security Manager Anwendungen
- Hinzufügen weiterer Security Manager Anwendungen

Verwenden der Administrator-Konsole

Die Security Manager Administrator-Konsole dient zur zentralen Verwaltung von HP ProtectTools Security Manager.

So öffnen Sie die Konsole:

- Wählen Sie **Start** > **Alle Programme** > **HP ProtectTools Administrator-Konsole** oder
- Klicken Sie auf den Link **Verwaltung** links unten in der Security Manager Konsole.

Die Administrator-Konsole besteht aus zwei Fenstern: Das linke Fenster enthält die Verwaltungstools. Das rechte Fenster enthält den Arbeitsbereich für die Konfiguration dieser Tools.

Das linke Fenster der Administrator-Konsole enthält folgende Elemente:

- **Startseite** - Ermöglicht den einfachen Zugriff auf gängige Aufgaben wie die Aktivierung von Sicherheitsfunktionen, die Festlegung von Sicherheitsinformationen und die Verwaltung von Benutzern.
- **System** - Hier kann die Konfiguration von systemweiten Sicherheitsfunktionen, Benutzern und Authentifizierungsgeräten wie Smart Card-Lesegeräten verwaltet werden.

- **Anwendungen** - Beinhaltet Tools, mit denen sich das Verhalten von Security Manager und den zugehörigen Anwendungen konfigurieren lässt.
- **Daten** - Hier finden Sie Tools für das Sichern und Wiederherstellen von Codierungsschlüsseln.
- **Computer** - Stellt erweiterte Sicherheitsoptionen bereit, mit denen verschiedenen Arten von Geräten, die eine Gefahr für die PC-Sicherheit darstellen könnten, selektiv der Zugriff untersagt werden kann. Außerdem können hier Berechtigungen für diverse Benutzer und Gruppen festgelegt werden.
- **Management-Tools** - Öffnet mithilfe des Standardbrowsers eine Website, auf der Sie weitere Verwaltungsanwendungen und –tools finden, die das Funktionsspektrum von Security Manager ergänzen. Außerdem finden Sie auf dieser Website Informationen zu neuen Anwendungen und Updates.
- **Links** - Bietet die folgenden Optionen:
  - **Installationsassistent** - Startet den Installationsassistenten, der Sie durch die Erstkonfiguration von Security Manager führt.
  - **Hilfe** - Öffnet die Online-Hilfe mit nützlichen Informationen zu Security Manager und den zugehörigen Anwendungen.
  - **Info** - Zeigt wichtige Informationen zu Security Manager einschließlich der Versionsnummer und dem Copyright-Vermerk an.

Einführung in den Installationsassistenten

Die Verwaltung von HP ProtectTools Security Manager erfordert Administratorrechte.

Der HP ProtectTools Security Manager Installationsassistent führt Sie durch die Einrichtung der Sicherheitsfunktionen. Darüber hinaus bietet die HP ProtectTools Security Manager Konsole eine Fülle zusätzlicher Funktionen. Die mit dem Assistenten vorgenommenen Einstellungen und eine Reihe weiterer Sicherheitsfunktionen können auch über die Konsole definiert werden. Alternativ können Sie über das Windows Startmenü oder über einen Link in der Administrator-Konsole darauf zugreifen. Diese Einstellungen gelten für den betreffenden Computer und alle Benutzer, die damit arbeiten.

Bei der ersten Anmeldung in Windows werden Sie zur Einrichtung von HP ProtectTools Security Manager aufgefordert. Klicken Sie auf **OK**, um den Security Manager Installationsassistenten zu starten, der Sie durch die grundlegenden Schritte für die Konfiguration des Programms führt.

HINWEIS: Alternativ können Sie den Installationsassistenten auch aufrufen, indem Sie am unteren Rand des linken Fensters der Administrator-Konsole auf **Security-Assistent** klicken.

Folgen Sie den Anleitungen des Installationsassistenten bis zum erfolgreichen Abschluss des Setups.

Wenn Sie den Assistenten vorzeitig abbrechen, wird er so lange automatisch gestartet, bis Sie auf **Diesen Assistenten nicht mehr anzeigen** klicken.

Zum Verwenden der HP ProtectTools Security Manager Anwendungen starten Sie HP ProtectTools Security Manager im **Startmenü** oder klicken im Infobereich der Taskleiste mit der rechten Maustaste auf das Symbol **Security Manager**. Die Security Manager Konsole und die zugehörigen Anwendungen stehen allen Benutzern des Computers zur Verfügung.

Systemkonfiguration

Die Anwendungsgruppe **System** kann über das Menü **Extras** in der linken Hälfte der Administrator-Konsole aufgerufen werden.

Mit den Anwendungen dieser Gruppe können Sie die Richtlinien und Einstellungen für den Computer, seine Benutzer und die zugehörigen Geräte konfigurieren und verwalten.

Die System-Gruppe umfasst die folgenden Anwendungen:

- **Sicherheit** - Verwaltet Sicherheitsfunktionen, Authentifizierungsrichtlinien und andere Einstellungen, die festlegen, wie Benutzer bei der Anmeldung an dem Computer oder an HP ProtectTools Anwendungen auf ihre Identität überprüft werden.
- **Benutzer** - Dient zum Einrichten, Verwalten und Registrieren der Computerbenutzer.
- **Geräte** - Verwaltet die Einstellungen von Sicherheitsgeräten, die in den Computer integriert oder mit ihm verbunden sind.

Aktivieren von Sicherheitsfunktionen

Die hier aktivierten Sicherheitsfunktionen gelten für alle Benutzer des betreffenden Computers.

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Sicherheit**, und klicken Sie dann auf **Merkmale**.
2. Zur Aktivierung einer Sicherheitsfunktion klicken Sie auf das zugehörige Kontrollkästchen neben **Windows Anmeldesicherheit** und/oder **Drive Encryption**.
   - **Windows Anmeldesicherheit** - Schützt Windows Konten, indem für den Kontozugriff spezifische Anmeldeinformationen eingegeben werden müssen.
   - **Drive Encryption** - Schützt die Daten, indem die Festplatte(n) verschlüsselt wird bzw. werden. Auf diese Weise können nur berechtigte Benutzer die betreffenden Informationen aufrufen.
3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Übernehmen**.

Festlegen der Security Manager Authentifizierungsrichtlinien

Die Security Manager Authentifizierungsrichtlinien für diesen Computer werden mithilfe zweier Registerkarten („Anmelden“ und „Sitzung“) festgelegt. Sie geben an, mit welchen Anmeldeinformationen sich die einzelnen Benutzerklassen ausweisen müssen, wenn sie während einer Sitzung auf den Computer und auf HP ProtectTools zugreifen.

Registerkarte „Anmelden“

So legen Sie die Anmeldeinformationen fest, die für die Anmeldung am Computer bzw. bei Windows erforderlich sind:

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Sicherheit**, und klicken Sie dann auf **Authentifizierung**.
2. Wählen Sie in der Registerkarte **Anmelden** eine Benutzerkategorie aus der Dropdown-Liste aus.

3. Legen Sie unter **Richtlinie** die Anmeldeinformationen für die ausgewählte Benutzerkategorie fest, indem Sie das/die Kontrollkästchen neben den betreffenden Anmeldeinformationen aktivieren. Es muss mindestens eine Anmeldeinformation festgelegt werden.

4. Wählen Sie in der Dropdown-Liste unter **Richtlinie** aus, ob „EINE BELIEBIGE“ (d. h. nur eine) der festgelegten Anmeldeinformationen oder aber ALLE festgelegten Anmeldeinformationen für eine Authentifizierung benötigt werden.

5. Klicken Sie auf **Übernehmen**.

Registerkarte „Sitzung“

So definieren Sie Richtlinien zu den Anmeldeinformationen, die ein Benutzer eingeben muss, um sich während einer Windows Sitzung erfolgreich bei HP ProtectTools Anwendungen anzumelden:

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Sicherheit**, und klicken Sie dann auf **Authentifizierung**.

2. Wählen Sie auf der Registerkarte **Sitzung** eine Benutzerkategorie aus.

3. Legen Sie unter **Richtlinie** die Anmeldeinformationen für die ausgewählte Benutzerkategorie fest, indem Sie das/die Kontrollkästchen neben den betreffenden Anmeldeinformationen aktivieren. Es muss mindestens eine Anmeldeinformation festgelegt werden.

4. Wählen Sie in der Dropdown-Liste unter **Richtlinie** aus, ob „EINE BELIEBIGE“ (d. h. nur eine) der festgelegten Anmeldeinformationen oder aber ALLE festgelegten Anmeldeinformationen für eine Authentifizierung benötigt werden.

5. Klicken Sie auf **Übernehmen**.

Definieren von Einstellungen

Sie können angeben, welche erweiterten Sicherheitsfunktionen zulässig sein sollen. So bearbeiten Sie die Einstellungen:

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Sicherheit**, und klicken Sie dann auf **Einstellungen**.

2. Klicken Sie auf das betreffende Kontrollkästchen, um eine Einstellung zu aktivieren bzw. zu deaktivieren.

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

HINWEIS: Mit der Einstellung **One-Step Logon zulassen** können Benutzer dieses Computers die Windows Anmeldung übergehen, falls sie sich bereits auf Ebene des BIOS authentifiziert haben.

Verwalten von Benutzern

Mit der Anwendung „Benutzer“ kann der Windows Administrator die Benutzer des betreffenden Computers und die für sie geltenden Richtlinien festlegen. Zum Öffnen der Anwendung „Benutzer“ in der Administrator-Konsole klicken Sie auf **Benutzer**.

Die HP ProtectTools Benutzer werden in einer Liste erfasst, und es wird überprüft, ob sie die Security Manager Authentifizierungsrichtlinien einhalten und die vorgeschriebenen Anmeldeinformationen eingeben.

Zur Anzeige der Richtliniein für einen bestimmten Benutzer wählen Sie den Benutzer aus der Liste aus und klicken dann auf **Richtlinien anzeigen**.

Um einen Benutzer bei der Registrierung von Anmeldeinformationen zu überwachen, wählen Sie den Benutzer aus der Liste aus und klicken dann auf **Registrieren**.

Hinzufügen eines Benutzers

Mit diesem Vorgang können Sie Benutzer zur Anmeldeliste hinzufügen. Um einen Benutzer hinzufügen zu können, muss er bereits ein Windows Konto auf dem Computer besitzen und während des folgenden Vorgangs anwesend sein, um das Kennwort bereitzustellen.

So fügen Sie der Benutzerliste einen Benutzer hinzu:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fenster der Administrator-Konsole auf **Benutzer**.
3. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Benutzer auswählen** wird geöffnet.
4. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um nach Benutzern zu suchen, die hinzugefügt werden sollen.
5. Klicken Sie auf Benutzer, die in die Liste aufgenommen werden sollen, und anschließend auf **OK**.
6. Klicken Sie im Dialogfeld **Benutzer auswählen** auf **OK**.
7. Geben Sie das Windows Kennwort für das ausgewählte Konto ein, und klicken Sie auf **Fertig stellen**.

HINWEIS: Sie müssen ein vorhandenes Windows Konto verwenden und dessen Namen genau eingeben. In diesem Dialogfeld können Sie Windows Benutzerkonten weder ändern noch hinzufügen.

Entfernen eines Benutzers

HINWEIS: Bei dieser Vorgehensweise wird das Windows Benutzerkonto nicht gelöscht. Das Konto wird lediglich aus Security Manager entfernt. Um den Benutzer vollständig zu entfernen, müssen Sie den Benutzer sowohl aus Security Manager als auch aus Windows entfernen.

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fenster der Administrator-Konsole auf **Benutzer**.
3. Klicken Sie auf den Benutzernamen für das Konto, das Sie entfernen möchten, und anschließend auf **Löschen**.
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Überprüfen des Benutzerstatus

Der Benutzerbereich der Administrator-Konsole zeigt den aktuellen Status der einzelnen Benutzer an:

- **Grünes Häkchen** - Gibt an, dass der Benutzer die erforderliche(n) Sicherheits-Anmeldemethode(n) konfiguriert hat.
- **Rotes X** - Gibt an, dass der Benutzer keine der erforderlichen Sicherheits-Anmeldemethoden konfiguriert hat und vom Computer gesperrt wird, wenn er versucht, sich anzumelden. Der Benutzer muss den Installationsassistenten ausführen, um die erforderlichen Anmeldemethoden zu konfigurieren.
- **Leer** - Gibt an, dass keine Sicherheits-Anmeldemethode erforderlich ist.

Konfigurieren von Anwendungseinstellungen

Das Fenster „Einstellungen“ beinhaltet Tools, mit denen sich das Verhalten von Security Manager und den zugehörigen Anwendungen konfigurieren lässt. So ändern Sie die Einstellungen:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fenster der Administrator-Konsole auf **Einstellungen**.
3. Wählen Sie auf der Registerkarte **Allgemein** die allgemeinen Einstellungen für HP ProtectTools Security Manager aus, und klicken Sie dann auf **Übernehmen**.
4. Wählen Sie auf der Registerkarte **Anwendungen** die Anwendungen aus, die Sie aktivieren bzw. deaktivieren möchten, und klicken Sie dann auf **Übernehmen**.

HINWEIS: Die Aktivierung/Deaktivierung einer Anwendung wird erst nach dem Neustart des Computers wirksam.

Verschlüsseln von Laufwerken

Drive Encryption for HP ProtectTools ermöglicht die Verschlüsselung der Festplatten und legt damit unbefugten Personen, die auf diese Daten zugreifen wollen, das Handwerk. Dies gilt auch dann, wenn die Festplatte ausgebaut bzw. an eine Wiederherstellungsfirma übergeben wird.

Zur Aktivierung/Deaktivierung von Drive Encryption klicken Sie in der Administrator-Konsole auf den Installationsassistenten.

△ **ACHTUNG:** Es ist wichtig, dass Sie Chiffrierschlüssel auf einem USB-Speichergerät speichern und an einem sicheren Ort aufbewahren. Wenn Sie das Kennwort vergessen, können Sie nur mithilfe des Speichergeräts auf Ihre Festplatte zugreifen.

Weitere Informationen zur Verwendung von Drive Encryption for HP ProtectTools finden Sie unter „Drive Encryption for HP ProtectTools“ auf Seite 34.

Verwalten des Gerätezugriffs

Device Access Manager for HP ProtectTools stellt erweiterte Sicherheitsfunktionen bereit, mit denen verschiedenen Arten von Geräten, die eine Gefahr für die PC-Sicherheit darstellen könnten, selektiv der Zugriff verweigert werden kann. Weitere Informationen zur Verwendung von Device Access

Manager for HP ProtectTools finden Sie unter „Device Access Manager for HP ProtectTools“ auf Seite 51.

5 HP ProtectTools Security Manager

Mit HP ProtectTools Security Manager lässt sich die Sicherheit des Computers signifikant verbessern. Dabei bieten die Security Manager Anwendungen folgende Möglichkeiten:

- Verwalten von Anmeldedaten und Kennwörtern
- Einfaches Ändern des Windows Kennworts
- Einrichten von Authentifizierungsinformationen einschließlich einer Smart Card
- Shreddern von Datenbeständen und Bereinigen der Festplatte
- Anzeige des Verschlüsselungsstatus eines Laufwerks
- Anzeige der Einstellungen für den Gerätezugriff
- Sichern und Wiederherstellen von Security Manager Daten

Verwalten von Kennwörtern

Credential Manager for HP ProtectTools (Password Manager) ermöglicht die Erstellung und Verwaltung von Anmeldedaten, mit denen Sie Websites und Programme aufrufen und sich dort anmelden können, indem Sie Ihre registrierten Anmeldeinformationen eingeben.

Weitere Informationen zur Kennwortverwaltung finden Sie unter „Credential Manager for HP ProtectTools (Password Manager)“ auf Seite 37.

Festlegen von Anmeldeinformationen

Anhand der Security Manager Anmeldeinformationen weisen Sie Ihre Identität nach. Der Administrator des Computers kann festlegen, welche Anmeldeinformationen für die Anmeldung bei Ihrem Windows Konto, bei Websites oder Programmen zulässig sind.

Welche Anmeldeinformationen zur Verfügung stehen, kann von der Art des integrierten bzw. mit dem Computer verbundenen Sicherheitsgeräts abhängig sein. Für jede unterstützte Anmeldeinformation wird in der Gruppe „Anmeldeinformationen“ ein Eintrag angelegt.

Ändern des Windows Kennworts

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

So ändern Sie Ihr Windows Kennwort:

1. Klicken Sie im linken Fenster von HP ProtectTools Security Manager auf **Anmeldeinformationen**.
2. Klicken Sie auf **Windows Kennwort**.
3. Geben Sie Ihr aktuelles Kennwort im Feld **Aktuelles Windows Kennwort** ein.
4. Geben Sie das neue Kennwort in **Neues Windows Kennwort** und **Neues Kennwort bestätigen** ein.
5. Klicken Sie auf **Ändern**.

Shreddern und Bereinigen von Dateien

File Sanitizer for HP ProtectTools löscht Dateien, indem diese durch bedeutungslose Daten überschrieben werden. Dieser auch als Shreddern bezeichnete Vorgang sorgt für eine sehr viel höhere Datensicherheit, da sich die gelöschten Dateien kaum noch wiederherstellen lassen. File Sanitizer erhöht die Datensicherheit außerdem, indem bereits beschriebene Sektoren der Festplatte mit einem als „Bereinigung“ bezeichneten Vorgang überschrieben werden. Mit File Sanitizer gelöschte Dateien können weder vom Betriebssystem noch von handelsüblichen Wiederherstellungsprogrammen wiederhergestellt werden.

Weitere Informationen zur Verwendung von File Sanitizer for HP ProtectTools finden Sie unter „File Sanitizer for HP ProtectTools“ auf Seite 42.

Anzeigen des Verschlüsselungsstatus eines Laufwerks

Die Konfiguration von Drive Encryption erfolgt durch den Windows Administrator in der Administrator-Konsole. Die Benutzer können den Verschlüsselungsstatus in Security Manager anzeigen lassen.

So lassen Sie den Verschlüsselungsstatus eines Laufwerks anzeigen:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fenster von Security Manager auf **Verschlüsselungsstatus**. Die Seite „Verschlüsselungsstatus“ zeigt an, ob Drive Encryption aktiviert ist und welche Laufwerke verschlüsselt bzw. nicht verschlüsselt sind.

Anzeigen des Gerätezugriffs

Die Konfiguration von Device Access Manager erfolgt durch den Windows Administrator in der Administrator-Konsole. Die Benutzer können die Einstellungen für den Gerätezugriff in Security Manager anzeigen lassen.

So lassen Sie die Einstellungen für den Gerätezugriff anzeigen:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager**.
2. Erweitern Sie im linken Fenster von Security Manager die Option **Device Access Manager**.
3. Um anzeigen zu lassen, welchen Geräten der Zugriff verweigert ist, klicken Sie auf **Einfache Konfiguration**. Geräte mit verweigertem Zugriff sind durch ein Häkchen gekennzeichnet.

4. Um anzeigen zu lassen, welchen Benutzern oder Gruppen der Zugriff verweigert ist, klicken Sie auf **Geräteklassen-Konfiguration**.

5. Durch Klicken auf ein Gerät können Sie anzeigen lassen, welchen Benutzern oder Gruppen der Zugriff auf ein Gerät verwehrt bzw. gestattet ist.

Hinzufügen von Anwendungen

Mit zusätzlichen Anwendungen, die unter Umständen verfügbar sind, kann die Funktionalität dieses Programms erweitert werden.

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

2. Klicken Sie im linken Fenster von Security Manager auf **Weitere Anwendungen**.

HINWEIS: Wenn kein Link **Weitere Anwendungen** zur Auswahl steht, wurde er vom zuständigen Administrator deaktiviert.

3. Suchen Sie auf der Registerkarte **Anwendungen hinzufügen** nach weiteren Anwendungen.

4. Auf der Registerkarte **Updates und Nachrichten** können Sie sich über neue Anwendungen und Updates informieren, indem Sie auf das Kontrollkästchen **Über neue Anwendungen und Updates informieren** klicken und festlegen, wann nach Updates gesucht werden soll. Alternativ klicken Sie auf **Jetzt suchen**, um sofort nach Updates zu suchen.

Festlegen von Einstellungen

Auf der Seite „Einstellungen“ können Sie das Kontrollkästchen **Symbol in der Taskleiste anzeigen** aktivieren, um das Security Manager Symbol im Infobereich der Taskleiste anzeigen zu lassen.

So rufen Sie die Seite „Einstellungen“ auf:

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

2. Klicken Sie im linken Fenster von Security Manager auf **Erweitert** und anschließend auf **Einstellungen**.

3. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Symbol in der Taskleiste anzeigen**, und klicken Sie dann auf **Übernehmen**.

Sichern und Wiederherstellen

Sie sollten es sich angewöhnen, Ihre Security Manager Daten regelmäßig zu sichern. Wie oft Sie eine Sicherung vornehmen, ist davon abhängig, wie häufig sich die Daten ändern. Wenn Sie z. B. täglich neue Anmeldedaten hinzufügen, sollten Sie Ihre Security Manager Daten täglich sichern.

Mithilfe von Sicherungen können Sie Daten auch auf einen anderen Computer migrieren. Dieser Vorgang wird auch als Importieren und Exportieren von Daten bezeichnet. Denken Sie jedoch daran, dass mit dieser Funktion nur Daten gesichert werden.

Wenn Sie die Sicherungsdatei auf einem anderen Computer oder aber auf dem ursprünglichen Computer nach der Neuinstallation des Betriebssystems wiederherstellen, muss vor der

Wiederherstellung der Daten aus der Sicherungsdatei HP ProtectTools Security Manager installiert worden sein.

Sichern von Daten

Beim Sichern Ihrer Daten speichern Sie Anmeldedaten in einer verschlüsselten Datei, die durch ein von Ihnen eingegebenes Kennwort geschützt ist.

So sichern Sie Ihre Daten:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fenster von Security Manager auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Daten sichern**.
4. Wählen Sie aus, welche Module gesichert werden sollen. In den meisten Fällen empfiehlt es sich, alle Module zu sichern. Klicken Sie auf **Weiter**.
5. Bestätigen Sie Ihre Identität mit Ihrem Kennwort, und klicken Sie dann auf die Pfeiltaste.
6. Geben Sie einen Pfad und einen Namen für die Sicherungsdatei ein. Die Datei wird standardmäßig im Ordner „Eigene Dateien“ abgelegt. Klicken Sie auf **Durchsuchen**, um einen anderen Speicherort anzugeben. Klicken Sie dann auf **Weiter**.
7. Geben Sie ein Kennwort ein, und bestätigen Sie Ihre Eingabe, um die Datei zu schützen.
8. Klicken Sie auf **Fertig stellen**.

Wiederherstellen von Daten

Die Wiederherstellung der Daten erfolgt aus einer kennwortgeschützten, verschlüsselten Datei, die mit der Sicherungs- und Wiederherstellungsfunktion von Security Manager erstellt wurde.

So stellen Sie Ihre Daten wieder her:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fenster von Security Manager auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Daten wiederherstellen**.
4. Geben Sie den Pfad und den Namen der Sicherungsdatei ein; alternativ klicken Sie auf **Durchsuchen** und wählen die betreffende Datei aus.
5. Geben Sie das Kennwort für die Datei ein, und klicken Sie dann auf **Weiter**.
6. Wählen Sie die Module aus, die wiederhergestellt werden sollen. Meist sollen alle aufgeführten Module wiederhergestellt werden. Klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.

Ändern von Windows Benutzername und Bild

Ihr Windows Benutzername und das zugehörige Bild werden oben links in Security Manager angezeigt.

So ändern Sie Ihren Windows Benutzernamen und/oder Ihr Bild:

1. Klicken Sie auf den Bereich in Security Manager, in dem Ihr Benutzername und Ihr Bild angezeigt werden.
2. Um den Benutzernamen zu ändern, geben Sie im Feld **Windows Benutzername** einen Namen ein.
3. Um das Bild zu ändern, klicken Sie auf **Bild wählen** und wählen dann ein Bild aus.
4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

6 Drive Encryption for HP ProtectTools

HINWEIS: Drive Encryption for HP ProtectTools wird nur bei bestimmten Modellen unterstützt.

In der heutigen Wirtschaftswelt müssen Sie jederzeit damit rechnen, dass ein Computer, der Ihnen oder einem Ihrer Mitarbeiter gehört, gestohlen wird und die darauf enthaltenen Unternehmensinformationen missbräuchlich verwendet werden. Durch die Verschlüsselung sämtlicher Daten auf der Festplatte legen Sie unbefugten Personen, die auf diese Daten zugreifen wollen, das Handwerk. Dies gilt auch dann, wenn die Festplatte ausgebaut bzw. an eine Wiederherstellungsfirma übergeben wird.

Drive Encryption for HP ProtectTools bietet einen umfassenden Datenschutz durch die Verschlüsselung der Festplatte. Wenn Drive Encryption aktiviert ist, müssen Sie sich am Drive Encryption Anmeldebildschirm anmelden. Dieser Bildschirm wird vor dem Starten von Windows angezeigt.

Drive Encryption verhindert nicht den unberechtigten Zugriff, wenn Sie bereits unter Windows angemeldet sind. Wenn der Computer gestartet ist und Sie Ihren Benutzernamen und das Kennwort eingegeben haben, sind die Daten auf der Festplatte zwar verschlüsselt, das System ist aber für andere Benutzer zugänglich. Schützen Sie deshalb Ihre Windows Sitzung mithilfe eines Kennworts, wenn Sie sich vom Computer entfernen.

HINWEIS: Drive Encryption for HP ProtectTools kann nur über den Installationsassistenten in der HP ProtectTools Administrator-Konsole aktiviert werden.

HINWEIS: Drive Encryption wird von 64-Bit-Betriebssystemen, die auf Systemen mit RAID-Konfiguration und AMD-Prozessor installiert sind, nicht unterstützt.

HINWEIS: Drive Encryption kann einen Wörterbuchangriff nicht verhindern.

Drive Encryption:

- Ermöglicht die Verschlüsselung sämtlicher Daten auf den internen Festplatten des betreffenden Computers.
- Ermöglicht den einfachen Kennwortzugriff und die Authentifizierung vor dem Systemstart.
- Unterstützt Microsoft Windows XP, Windows Vista und Windows 7.

Mit Drive Encryption for HP ProtectTools können Sie verschiedene Aufgaben durchführen:

- Verwalten von Drive Encryption
  - Verschlüsseln bzw. Entschlüsseln einzelner Laufwerke
- Sichern und Wiederherstellen
  - Erstellen von Sicherungsschlüsseln
  - Durchführen einer Wiederherstellung

△ **ACHTUNG:** Es ist wichtig, dass Sie Chiffrierschlüssel auf einem USB-Speichergerät speichern und an einem sicheren Ort aufbewahren. Wenn Sie Ihr Kennwort vergessen, können Sie nur mithilfe des Speichergeräts auf Ihre Festplatte zugreifen.

ACHTUNG: Wenn Sie das Modul „Drive Encryption“ deinstallieren oder eine Sicherungs- und Wiederherstellungslösung verwenden, müssen Sie zunächst alle verschlüsselten Laufwerke entschlüsseln. Andernfalls können Sie nicht mehr auf die Daten auf verschlüsselten Laufwerken zugreifen. Auch wenn Sie das Modul „Drive Encryption“ erneut installieren, haben Sie keinen Zugriff auf die verschlüsselten Daten.

Setup-Verfahren

Aufrufen von Drive Encryption

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

Allgemeine Aufgaben

Aktivieren von Drive Encryption

Verwenden Sie den Installationsassistenten für die HP ProtectTools Administrator-Konsole, um Drive Encryption zu aktivieren.

Deaktivieren von Drive Encryption

Verwenden Sie den Installationsassistenten für die HP ProtectTools Administrator-Konsole, um Drive Encryption zu deaktivieren.

Anmelden, nachdem Drive Encryption aktiviert wurde

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

HINWEIS: Falls der Windows Administrator die Funktion „Pre-boot Security“ (Sicherheit vor dem Systemstart) in der HP ProtectTools Administrator-Konsole aktiviert hat, können Sie sich nach dem Einschalten des Computers direkt beim Computer anmelden, ohne dies im Drive Encryption Anmeldebildschirm tun zu müssen.

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

Fortgeschrittene Vorgehensweisen

Verwalten von Drive Encryption (Administrator-Aufgabe)

Im Fenster „Drive Encryption“ können Windows Administratoren den Status von Drive Encryption anzeigen und ändern (aktiv/inaktiv). Darüber hinaus können Sie hier den Verschlüsselungsstatus aller Festplatten des Computers anzeigen lassen.

Verschlüsseln oder Entschlüsseln einzelner Laufwerke

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Drive Encryption**, und klicken Sie auf **Verschlüsselungsverwaltung**.
2. Klicken Sie auf die Schaltfläche **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 vorhergehenden Fortschritt wiederzugeben.

Sicherung und Wiederherstellung (Administrator-Aufgabe)

Im Fenster „Drive Encryption: Sichern und Wiederherstellen“ können Windows Administratoren Codierungsschlüssel sichern und wiederherstellen.

Erstellen von Sicherungsschlüsseln

ACHTUNG: Bewahren Sie das Speichergerät mit dem Chiffrierschlüssel-Backup an einem sicheren Ort auf. Wenn Sie Ihr Kennwort vergessen, können Sie nur mithilfe des Speichergeräts wieder auf Ihre Festplatte zugreifen.

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Drive Encryption**, und klicken Sie auf **Sichern und Wiederherstellen**.
2. Klicken Sie auf **Schlüssel sichern**.
3. Klicken Sie auf der Seite „Backup-Diskette auswählen“ auf den Namen des Geräts, auf dem Sie Ihren Chiffrierschlüssel sichern möchten, und klicken Sie dann auf **Weiter**.
4. Lesen Sie die Informationen auf der daraufhin angezeigten Seite, und klicken Sie auf **Weiter**.

   Der Chiffrierschlüssel wird auf dem ausgewählten Speichergerät gesichert.
5. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

HINWEIS: In der Online-Hilfe zu Drive Encryption for HP ProtectTools finden Sie weitere Informationen zur Verwaltung und Wiederherstellung.

7 Credential Manager for HP ProtectTools (Password Manager)

Mit Password Manager können Sie sich sehr viel schneller und sicherer bei Windows sowie bei Websites und Programmen anmelden.

Password Manager ermöglicht die Einrichtung von Anmeldebildschirmen für Websites und Programme, sodass Sie sich besonders schnell und sicher dort anmelden können. Zunächst speichert Password Manager Ihre Anmeldedaten sowie die Informationen, die Sie in die Felder der einzelnen Anmeldebildschirme eingeben. Wenn Sie danach diesen Anmeldebildschirm wieder aufrufen, trägt Password Manager nach der Bestätigung Ihrer Identität die betreffenden Daten automatisch ein und übergibt sie an das System.

Für einen noch schnelleren Zugriff können Sie ein Menü mit Ihren Anmeldedaten anzeigen, indem Sie eine konfigurierbare Tastenkombination (standardmäßig Strg+Windows+H) drücken. Wenn Sie in dem Menü bestimmte Anmeldedaten auswählen, startet Password Manager automatisch die zugehörige Website oder das Programm, wechselt zum entsprechenden Anmeldebildschirm und meldet Sie an.

Zur Überprüfung Ihrer Identität verwendet HP ProtectTools for Small Business Anmeldeinformationen wie beispielsweise Ihr Windows Kennwort. Sie verwenden also ein und dieselben Anmeldeinformationen, um sich bei allen konfigurierten Anmeldebildschirmen anzumelden. Auf diese Weise können Sie effizientere Kennwörter festlegen, ohne sich diese notieren oder merken zu müssen, um Ihre Konten zuverlässig zu schützen.

Mit Password Manager sehen Sie auf einen Blick, ob eines Ihrer Kennwörter ein Sicherheitsrisiko darstellt. Wenn dies der Fall ist, können Sie ein komplexeres Kennwort mit einer besseren Schutzwirkung festlegen, das dann für neue Sites verwendet wird.

Darüber hinaus können Sie in Password Manager Ihre Anmeldedaten und Kennwörter anzeigen lassen und jederzeit bearbeiten. Viele Funktionen von Password Manager können auch über das Password Manager Symbol aufgerufen werden, wenn der Anmeldebildschirm eines entsprechend konfigurierten Programms aktiv ist oder wenn der Anmeldebildschirm einer Website aktiv ist. Durch Klicken auf das Symbol wird ein Kontextmenü aufgerufen, in dem Ihnen die unten aufgeführten Optionen zur Auswahl stehen.

Websites und Programme, für die noch keine Anmeldedaten definiert wurden:

Das Kontextmenü enthält die folgenden Optionen:

- [beliebigeDomäne.de] zu Password Manager hinzufügen - Mit dieser Option können Sie Anmeldedaten für den aktuellen Anmeldebildschirm hinzufügen.
- Password Manager öffnen - Startet Security Manager auf der Seite „Password Manager“.

- Einstellungen für das Password Manager-Symbol - Ermöglicht die Definition von Bedingungen, unter denen das Password Manager Symbol angezeigt wird.
- Hilfe - Öffnet die Online-Hilfe zu der Password Manager Anwendung.

Websites und Programme, für die bereits Anmeldedaten definiert wurden:

Das Kontextmenü enthält die folgenden Optionen:

- Anmeldedaten eingeben - Übernimmt Ihre Anmeldedaten in die betreffenden Felder und übergibt die Seite dann an das System (wenn die Übergabe bei der Erstellung oder letzten Bearbeitung der Anmeldedaten festgelegt wurde).
- Anmeldedaten bearbeiten - Ermöglicht Ihnen die Bearbeitung Ihrer Anmeldedaten für diese Website.
- Anmeldedaten hinzufügen - Ermöglicht Ihnen, weitere Anmeldedaten für eine Website oder ein Programm hinzuzufügen.
- Password Manager öffnen - Startet das Security Manager Dashboard auf der Seite „Password Manager“.
- Hilfe - Öffnet die Online-Hilfe zu der Password Manager Anwendung.

Hinzufügen von Anmeldedaten

So fügen Sie Anmeldedaten hinzu:

1. Öffnen Sie den Anmeldebildschirm einer Website oder eines Programms.
2. Klicken Sie auf den Pfeil des Password Manager Symbols, und wählen Sie dann eine der folgenden Optionen aus, je nachdem, ob es sich um den Anmeldebildschirm für eine Website oder ein Programm handelt.
   - Website – Wählen Sie **[domain name] zu Password Manager hinzufügen**.
   - Programm – Wählen Sie **Diesen Anmeldebildschirm zu Password Manager hinzufügen**.
3. Geben Sie Ihre Anmeldedaten ein. Die Anmeldefelder auf dem Bildschirm und die entsprechenden Felder des Dialogfelds sind durch einen orangefarbenen Rahmen gekennzeichnet. Zur Anzeige dieses Dialogfelds können Sie auch andere Optionen wählen, wie beispielsweise „Anmeldedaten von Password Manager hinzufügen“ auf der Registerkarte **Verwalten**. Einige Optionen sind davon abhängig, welche Sicherheitsgeräte mit dem Computer verbunden sind; dies gilt z. B. für die Verwendung der Tastenkombination strg+H oder das Einsetzen einer Smart Card.
   - Wenn Sie auf die Pfeile rechts von einem Anmeldefeld klicken, können Sie eine der vorformatierten Auswahlmöglichkeiten in das Feld übernehmen.
   - Optional klicken Sie auf **Andere Felder wählen**, um weitere Felder des Bildschirms in die Anmeldedaten zu übernehmen.

- Deaktivieren Sie **Anmeldedaten senden**, wenn die Anmeldefelder zwar ausgefüllt, die Anmeldedaten jedoch nicht an das System übergeben werden sollen.
- Wenn Sie das Kennwort für die Anmeldedaten anzeigen lassen möchten, klicken Sie auf **Kennwort einblenden**.

4. Klicken Sie auf **OK**. Das Password Manager Symbol wird nun ohne Pluszeichen angezeigt und macht somit deutlich, dass die Anmeldedaten erstellt wurden.

Bei jedem Besuch der Website und jedem Aufrufen des Programms wird nun das Password Manager Symbol angezeigt. Es gibt an, dass Sie Ihre registrierten Anmeldeinformationen für die Anmeldung verwenden können.

Bearbeiten von Anmeldedaten

So bearbeiten Sie Anmeldedaten:

1. Öffnen Sie den Anmeldebildschirm einer Website oder eines Programms.
2. Klicken Sie auf den Pfeil des Password Manager Symbols, und wählen Sie **Anmeldedaten bearbeiten**, um ein Dialogfeld zu öffnen, in dem Sie Ihre Anmeldedaten bearbeiten können. Die Anmeldefelder auf dem Bildschirm und die entsprechenden Felder des Dialogfelds sind durch einen orangefarbenen Rahmen gekennzeichnet.
3. Geben Sie Ihre Anmeldedaten ein.
   - Wenn Sie auf die Pfeile rechts von einem Anmeldefeld klicken, können Sie eine der vorformatierten Auswahlmöglichkeiten in das Feld übernehmen.
   - Optional klicken Sie auf **Andere Felder wählen**, um weitere Felder des Bildschirms in die Anmeldedaten zu übernehmen.
   - Deaktivieren Sie **Kontodaten senden**, wenn die Anmeldefelder zwar ausgefüllt, die Anmeldedaten jedoch nicht an das System übergeben werden sollen.
   - Wenn Sie das Kennwort für die Anmeldedaten anzeigen lassen möchten, klicken Sie auf „Kennwort einblenden“.
4. Klicken Sie auf **OK**.

Verwenden des Menüs „Anmeldedaten“

Password Manager ermöglicht den schnellen und einfachen Start von Websites und Programmen, für die Sie Anmeldedaten definiert haben. Doppelklicken Sie hierfür einfach im Menü „Anmeldedaten“ auf die Anmeldedaten eines Programms oder einer Website. Alternativ können Sie auch in Passwort Manager auf die Registerkarte **Verwalten** klicken. Der zugehörige Anmeldebildschirm wird geöffnet, und Ihre Anmeldedaten werden übernommen. Standardmäßig werden die Daten sofort an die Website gesendet. Wenn Sie dies nicht möchten, deaktivieren Sie die Option **Kontodaten senden** bei der erstmaligen Konfiguration bzw. Bearbeitung der Anmeldedaten.

Wenn Sie Anmeldedaten definieren, werden diese automatisch in das Menü „Anmeldedaten“ von Password Manager aufgenommen.

Zur Anzeige des Menüs „Anmeldedaten“ drücken Sie die Tastenkombination für Password Manager. Dies ist standardmäßig strg+H. In **Password Manager** > **Einstellungen** können Sie jedoch auch eine andere Tastenkombination festlegen.

Zusammenfassen von Anmeldedaten in Kategorien

Mithilfe von Kategorien können Sie Ihre Anmeldedaten übersichtlich strukturieren. Dabei erstellen Sie einfach die gewünschte Zahl von Kategorien und übernehmen Ihre Anmeldedaten mittels Ziehen & Ablegen in die gewünschte Kategorie.

So fügen Sie eine Kategorie hinzu:

1. Wählen Sie im linken Fenster von Security Manager die Option **Password Manager**.
2. Wählen Sie die Registerkarte **Verwalten**, und klicken Sie dann auf **Kategorie hinzufügen**.
3. Geben Sie einen Namen für die Kategorie ein.
4. Klicken Sie auf **OK**.

So nehmen Sie Anmeldedaten in eine Kategorie auf:

1. Platzieren Sie den Mauszeiger über den gewünschten Anmeldedaten.
2. Halten Sie die linke Maustaste gedrückt.
3. Ziehen Sie die Anmeldedaten in die Liste der Kategorien. Wenn Sie mit der Maus über die Kategorien fahren, werden diese hervorgehoben dargestellt.
4. Lassen Sie die Maustaste los, wenn die gewünschte Kategorie markiert ist.

Die Anmeldedaten werden nicht in die ausgewählte Kategorie verschoben, sondern lediglich kopiert. Ein und dieselben Anmeldedaten können also in mehreren Kategorien enthalten sein. Außerdem können Sie durch Klicken auf **Alle** Ihre gesamten Anmeldedaten jederzeit anzeigen lassen.

Verwalten von Anmeldedaten

Mit Password Manager lassen sich Anmeldedaten wie Benutzernamen, Kennwörter und Konten mit Mehrfach-Anmeldung einfach und intuitiv von einer zentralen Stelle aus verwalten.

Sie finden Ihre Anmeldedaten auf der Registerkarte **Verwalten**. Wenn Sie für eine Website mehrere Anmeldedaten definiert haben, werden die einzelnen Daten unter dem Namen der Website sowie (eingerückt) in der Liste der Anmeldedaten geführt.

So verwalten Sie Ihre Anmeldedaten:

Wählen Sie im linken Fenster von Security Manager die Option **Password Manager** und klicken Sie auf die Registerkarte **Verwalten**.

- Hinzufügen von Anmeldedaten – Klicken Sie auf **Anmeldedaten hinzufügen**, und folgen Sie dann den Anleitungen auf dem Bildschirm.
- Bearbeiten von Anmeldedaten – Wählen Sie die gewünschten Anmeldedaten aus, und klicken Sie auf **Bearbeiten**. Nehmen Sie dann die erforderlichen Änderungen vor.
- Löschen von Anmeldedaten – Wählen Sie die gewünschten Anmeldedaten aus, und klicken Sie auf **Löschen**.

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

1. Öffnen Sie den Anmeldebildschirm der Website oder des Programms.
2. Klicken Sie auf das Symbol für Password Manager, um das zugehörige Kontextmenü aufzurufen.
3. Wählen Sie **Zusätzliche Anmeldedaten hinzufügen**, und folgen Sie dann den Anleitungen auf dem Bildschirm.

Überprüfen der Kennwortstärke

Die Verwendung effizienter Kennwörter bei der Anmeldung bei Websites und Programmen ist eine wichtige Voraussetzung für den wirksamen Identitätsschutz.

Password Manager ermöglicht die einfache Überprüfung und Verbesserung der Sicherheit durch die sofortige und vollautomatische Analyse der Kennwortstärke für alle Kennwörter, mit denen Sie sich bei Websites und Programmen anmelden. Zur Überprüfung der Kennwortstärke wählen Sie in Password Manager die Registerkarte **Kennwortstärke**.

Symboleinstellungen für Password Manager

Password Manager erkennt die Anmeldebildschirme für Websites und Programme. Wenn ein Bildschirm festgestellt wird, für den Sie noch keine Anmeldedaten erstellt haben, werden Sie von Password Manager aufgefordert, die entsprechenden Daten hinzuzufügen. Dies wird kenntlich gemacht, indem das Password Manager Symbol mit einem Pluszeichen (+) versehen wird.

Sie können die folgenden Einstellungen vornehmen:

- Immer auffordern - Wählen Sie diese Option, wenn Password Manager Sie zur Aufnahme von Anmeldedaten auffordern soll, sobald ein Anmeldebildschirm geöffnet wird, für den Sie noch keine Anmeldedaten eingerichtet haben.
- Aufforderung für diesen Bildschirm nicht anzeigen - Wählen Sie diese Option, wenn Sie von Password Manager nicht mehr zur Aufnahme von Anmeldedaten für diesen Bildschirm aufgefordert werden wollen.
- Nie auffordern - Wählen Sie diese Option, wenn Password Manager Sie bei der Anzeige von Anmeldebildschirmen ohne definierte Anmeldedaten nie zur Eingabe der Daten auffordern soll.

8 File Sanitizer for HP ProtectTools

File Sanitizer ist ein Tool, mit dem Sie kritische Dateien und Ordner (persönliche Daten oder Dateien, historische oder Internet-bezogene Daten sowie andere Datenkomponenten) auf Ihrem Computer sicher löschen und Ihre Festplatte regelmäßig bereinigen können.

HINWEIS: Zurzeit wird der Einsatz von File Sanitizer nur für Festplatten unterstützt.

Informationen zum Shreddern

Beim Löschen von Dateien und/oder Ordnern in Windwos wird der Inhalt nicht vollständig von der Festplatte entfernt. Windows löscht lediglich den Verweis. Der Inhalt bleibt so lange auf der Festplatte, bis eine andere Datei diesen Bereich auf der Festplatte mit neuen Daten überschreibt.

Das Shreddern unterscheidet sich vom üblichen Löschvorgang unter Windows (dieser wird in File Sanitizer auch als „einfaches Löschen“ bezeichnet), weil das Shreddern von Daten es quasi unmöglich macht, die Daten wiederherzustellen.

Wenn Sie ein Shred-Profil (Hohe Sicherheit, Mittlere Sicherheit oder Geringe Sicherheit) auswählen, werden automatisch eine vordefinierte Liste mit Dateien und/oder Ordnern sowie eine Löschmethode für den Shred-Vorgang festgelegt. Sie können ein Shred-Profil auch anpassen. Damit können Sie die Anzahl der Shred-Zyklen, die zu shreddernden Dateien, die Dateien, bei denen das Shreddern bestätigt werden muss, und die nicht zu shreddernden Dateien angeben.

Sie können einen Zeitplan zum automatischen Shreddern festlegen oder die Dateien und/oder Ordner zu einem beliebigen Zeitpunkt manuell shreddern.

Informationen zur Festplattenbereinigung.

Mit der Festplattenbereinigung können Sie gelöschte Dateien sicher mit Zufallsdaten überschreiben, sodass der ursprüngliche Inhalt der gelöschten Dateien nicht mehr angezeigt werden kann.

HINWEIS: Die Festplattenbereinigung ist für die Dateien gedacht, die Sie manuell oder über den Windows Papierkorb löschen. Sie bietet für geshredderte Dateien keine zusätzliche Sicherheit.

Sie haben die Möglichkeit, einen automatischen Zeitplan für das Bereinigen der Festplatte zu erstellen oder die Festplattenbereinigung über das Symbol HP ProtectTools im Infobereich der Taskleiste (rechts außen) manuell zu aktivieren.

Setup-Verfahren

Öffnen von File Sanitizer

So öffnen Sie File Sanitizer:

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

   – ODER –

- Doppelklicken Sie auf das Symbol **File Sanitizer**.

  – ODER –

- Klicken Sie im Infobereich ganz rechts in der Taskleiste mit der rechten Maustaste auf das Symbol für HP ProtectTools, und wählen Sie **File Sanitizer**; klicken Sie anschließend auf **File Sanitizer öffnen**.

Planen der Festplattenbereinigung

So erstellen Sie einen Zeitplan für die Festplattenbereinigung:

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, und klicken Sie dann auf **Bereinigung**.
2. Aktivieren Sie das Kontrollkästchen **Planer aktivieren**, geben Sie Ihr Windows Kennwort ein, und tragen Sie anschließend Tag und Uhrzeit für die Bereinigung der Festplatte ein.
3. Klicken Sie auf das Symbol **Speichern**.

HINWEIS: Die Festplattenbereinigung kann längere Zeit in Anspruch nehmen. Auch wenn der Bereinigungsvorgang im Hintergrund stattfindet, wird die Verarbeitungsleistung Ihres Computers unter Umständen durch die erhöhte Prozessorbeanspruchung beeinträchtigt.

Planen eines Shred-Vorgangs

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, und klicken Sie dann auf **Shreddern**.
2. Wählen Sie eine Shred-Option:
   - **Beim Herunterfahren von Windows** — Wählen Sie diese Option, um alle ausgewählten Dateien beim Herunterfahren von Windows zu shreddern.

     HINWEIS: Wenn Sie diese Option aktivieren, wird beim Herunterfahren ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob Sie mit dem Shreddern der ausgewählten Dateien fortfahren oder den Vorgang überspringen möchten. Klicken Sie auf „Ja“, um das Shreddern zu überspringen, auf „Nein“, wenn Sie mit dem Shred-Vorgang fortfahren möchten. Die gewünschte Option muss schnell gewählt werden, da Windows die Software während des Herunterfahrens schließt und dann eventuell ein Fehler auftritt. Wenn Sie mit „Nein“ den Shred-Vorgang fortsetzen möchten, zeigt Windows unter Umständen eine Fehlermeldung an, die angibt, dass File Sanitizer nicht reagiert. Warten Sie, bis File Sanitizer den Shred-Vorgang beendet hat, und leiten Sie dann das Herunterfahren erneut ein.
   - **Beim Öffnen eines Webbrowsers** — Wählen Sie diese Option, wenn Sie alle ausgewählten webbezogenen Dateien, wie den URL-Verlauf des Browsers, beim Öffnen eines Webbrowsers shreddern möchten.
   - **Beim Schließen eines Webbrowsers** — Wählen Sie diese Option, wenn Sie alle ausgewählten webbezogenen Dateien, wie den URL-Verlauf des Browsers, beim Schließen eines Webbrowsers shreddern möchten.
   - **Tastenfolge** — Wählen Sie diese Option, um das Shreddern unter Verwendung einer bestimmten Tastenfolge einzuleiten.
   - **Planer** — Aktivieren Sie das Kontrollkästchen „Planer aktivieren“, geben Sie Ihr Windows Kennwort ein, und legen Sie dann das Datum und die Uhrzeit fest, an dem bzw. zu der die ausgewählten Dateien geshreddert werden sollen.
3. Klicken Sie auf das Symbol **Speichern**.

Auswählen oder Erstellen eines Shred-Profils

Sie können eine Löschmethode festlegen und die zu shreddernden Dateien und/oder Ordner angeben, indem Sie ein vordefiniertes Profil auswählen 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 eine vordefinierte Löschmethode und eine Liste mit Dateien festgelegt. Sie können auf die Schaltfläche „Details anzeigen“ klicken, um die vordefinierte Liste mit Dateien anzuzeigen, die geshreddert werden sollen.

So wählen Sie ein vordefiniertes Shred-Profil aus:

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf ein vordefiniertes Shred-Profil.

3. Klicken Sie auf **Details anzeigen**, um die Liste mit Dateien anzuzeigen, die geshreddert werden sollen.
4. Aktivieren Sie unter **Folgende Elemente shreddern** das Kontrollkästchen neben den Dateien, bei denen der Shred-Vorgang bestätigt werden soll.
5. Klicken Sie auf **Übernehmen**.

Anpassen eines Shred-Profils für erhöhte Sicherheit

Beim Erstellen eines Shred-Profils geben Sie die Anzahl der Shred-Zyklen an sowie die zu shreddernden Dateien, die Dateien, bei denen das Shreddern bestätigt werden muss und die nicht zu shreddernden Dateien.

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, klicken Sie auf **Einstellungen**, wählen Sie **Einstellungen für erweiterte Sicherheit**, und klicken Sie dann auf **Details anzeigen**.

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

HINWEIS: Für jede Datei wird die ausgewählte Anzahl an Shred-Zyklen ausgeführt. Wenn Sie beispielsweise drei Shred-Zyklen gewählt haben, wird der Algorithmus, der die Daten löscht, drei Mal ausgeführt. Wenn Sie die Shred-Zyklen mit einer höheren Sicherheitsstufe wählen, kann der Shred-Vorgang sehr lange dauern. Allerdings ist der Computer umso besser geschützt, je höher die Anzahl der angegebenen Shred-Zyklen ist.

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

   a. Klicken Sie unter **Verfügbare Shred-Optionen** auf eine Datei und dann auf **Hinzufügen**.

   b. Zum Hinzufügen einer benutzerdefinierten Datei klicken Sie auf **Benutzerdefinierte Option hinzufügen**. Geben Sie anschließend einen Datei- oder Ordnernamen ein bzw. klicken Sie darauf, und klicken Sie dann auf **OK**. Klicken Sie auf die benutzerdefinierte Datei und anschließend auf **Hinzufügen**.

HINWEIS: Um eine Datei aus den verfügbaren Shred-Optionen zu entfernen, klicken Sie auf die Datei und dann auf **Löschen**.

4. Aktivieren Sie unter **Folgende Elemente shreddern** das Kontrollkästchen neben den Dateien, bei denen der Shred-Vorgang bestätigt werden soll.

HINWEIS: Um eine Datei aus der Liste der zu shreddernden Elemente zu entfernen, klicken Sie auf die Datei und dann auf **Entfernen**.

5. Klicken Sie unter **Folgende Elemente nicht shreddern** auf **Hinzufügen**, um die Dateien auszuwählen, die nicht geshreddert werden sollen.

6. Wenn Sie die Konfiguration des Shred-Profils abgeschlossen haben, klicken Sie auf **Übernehmen**.

Anpassen eines Profils für einfaches Löschen

Das einfache Löschprofil führt einen Standard-Dateilöschvorgang ohne Shreddern durch. Beim Anpassen eines einfachen Löschprofils geben Sie an, welche Dateien bei einem einfachen Löschen berücksichtigt werden sollen, bei welchen Dateien das einfache Löschen bestätigt werden muss und welche Dateien vom einfachen Löschen ausgeschlossen werden sollen.

HINWEIS: Bei Verwendung der Option für einfaches Löschen empfiehlt sich dringend die regelmäßige Durchführung einer Festplattenbereinigung.

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, klicken Sie auf **Einstellungen**, wählen Sie **Einstellungen für einfaches Löschen**, und klicken Sie dann auf **Details anzeigen**.
2. Wählen Sie die zu löschenden Dateien aus:
   a. Klicken Sie unter **Verfügbare Löschoptionen** auf eine Datei und dann auf **Hinzufügen**.
   b. Zum Hinzufügen einer benutzerdefinierten Datei klicken Sie auf **Benutzerdefinierte Option hinzufügen**. Geben Sie anschließend einen Datei- oder Ordnernamen ein bzw. klicken Sie darauf, und klicken Sie dann auf **OK**. Klicken Sie auf die benutzerdefinierte Datei und anschließend auf **Hinzufügen**.

   HINWEIS: Um eine Datei aus dem Bereich mit den verfügbaren Löschoptionen zu entfernen, klicken Sie auf die Datei und dann auf **Löschen**.
3. Aktivieren Sie unter **Folgende Elemente löschen** das Kontrollkästchen neben den Dateien, bei denen der Löschvorgang bestätigt werden soll.

HINWEIS: Um eine Datei aus der Liste der zu löschenden Elemente zu entfernen, klicken Sie auf die Datei und dann auf **Entfernen**.

4. Klicken Sie unter **Folgende Elemente nicht löschen** auf **Hinzufügen**, um die Dateien auszuwählen, die nicht geshreddert werden sollen.
5. Wenn Sie die Konfiguration des Profils für das einfache Löschen abgeschlossen haben, klicken Sie auf **Übernehmen**.

Allgemeine Aufgaben

Verwenden von Tastenfolgen zum Einleiten des Shred-Vorgangs

Gehen Sie folgendermaßen vor, um eine Tastenfolge festzulegen:

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, und klicken Sie dann auf **Shreddern**.
2. Aktivieren Sie das Kontrollkästchen **Tastenfolge**.
3. Geben Sie im entsprechenden Feld ein Zeichen ein, und aktivieren Sie anschließend **strg**, **alt** oder **Umschalttaste**, oder wählen Sie alle drei Optionen aus.

   Um zum Beispiel das automatische Shreddern mit der Tastenfolge Strg+Umschalttaste und S auszulösen, geben Sie in das dafür vorgesehene Feld den Buchstaben S ein und aktivieren die Optionen **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 Taste Strg, Alt, Umschalttaste oder eine von Ihnen festgelegte Tastenkombination gedrückt, und drücken Sie das gewünschte Zeichen.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Verwenden des Symbols „File Sanitizer“

△ **ACHTUNG:** Geshredderte Dateien lassen sich nicht wiederherstellen. Gehen Sie bei der Auswahl der manuell zu shreddernden Elemente daher vorsichtig vor.

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

Manuelles Shreddern eines Datenbestands

△ **ACHTUNG:** Geshredderte Dateien lassen sich nicht wiederherstellen. Gehen Sie bei der Auswahl der manuell zu shreddernden Elemente daher vorsichtig vor.

1. Klicken Sie im Infobereich ganz rechts in der Taskleiste mit der rechten Maustaste auf das Symbol **HP ProtectTools**, und wählen Sie **File Sanitizer**. Klicken Sie anschließend auf **Ein Element shreddern**.
2. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu der Datei, die Sie shreddern möchten, und klicken Sie anschließend auf **Öffnen**.

HINWEIS: Bei der ausgewählten Datei kann es sich um eine einzelne Datei oder um 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 **Shreddern**.
2. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu der Datei, die Sie shreddern möchten, und klicken Sie anschließend auf **OK**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, und klicken Sie dann auf **Shreddern**.
2. Klicken Sie auf die Schaltfläche **Durchsuchen**.
3. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu der Datei, die Sie shreddern möchten, und klicken Sie anschließend auf **Öffnen**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Shreddern aller ausgewählten Datenbestände

1. Klicken Sie im Infobereich ganz rechts in der Taskleiste mit der rechten Maustaste auf das Symbol **HP ProtectTools**, und wählen Sie **File Sanitizer**. Klicken Sie 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**.

Manuelles Aktivieren der Festplattenbereinigung

1. Klicken Sie im Infobereich ganz rechts in der Taskleiste mit der rechten Maustaste auf das Symbol **HP ProtectTools**, und wählen Sie **File Sanitizer**. Klicken Sie anschließend auf **Jetzt überschreiben**.
2. Das Programm bestätigt, dass der Überschreibvorgang gestartet wurde.

– ODER –

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, und klicken Sie dann auf **Bereinigung**.
2. Klicken Sie auf **Jetzt überschreiben**.
3. Das Programm bestätigt, dass der Überschreibvorgang gestartet wurde.

Abbrechen eines Shred-Vorgangs oder einer Festplattenbereinigung

Wenn der Shred- bzw. Bereinigungsvorgang bereits läuft, wird über dem Symbol für HP ProtectTools Security Manager im Infobereich eine Meldung angezeigt. Sie enthält Einzelheiten zum Shred- oder Festplattenbereinigungsvorgang (in Prozent) und gibt Ihnen die Möglichkeit, den Vorgang abzubrechen.

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 jede Festplattenbereinigung 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 Festplattenbereinigung bezieht.

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

Es wird eine Protokolldatei für Shred-Vorgänge und eine separate Protokolldatei für Festplattenbereinigungen erstellt. Beide Protokolldateien werden auf der Festplatte in den folgenden Ordnern gespeichert:

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

9 Device Access Manager for HP ProtectTools

Dieses Sicherheitstool steht nur den Administratoren zur Verfügung. Device Access Manager for HP ProtectTools bietet die folgenden Sicherheitsfunktionen, mit denen die am Computersystem angeschlossenen Geräte vor einem unbefugten Zugriff geschützt werden:

- Geräteprofile für jeden Benutzer, um den Gerätezugriff zu definieren
- Gerätezugriff, der auf der Grundlage der Gruppenmitgliedschaft gewährt oder verweigert werden kann

HINWEIS: Device Access Manager verwendet lokale Windows Benutzer und Gruppen für die Zugriffsverwaltung. Da Windows Home lokale Benutzer und Gruppen nicht unterstützt, funktioniert Device Access Manager nicht einwandfrei. Wenn Sie Device Access Manager unter Microsoft Windows Vista Home verwenden möchten, müssen Sie bei der Benutzereinrichtung mit DOS-Befehlen arbeiten. Weitere Informationen hierzu finden Sie in der Device Access Manager Online-Hilfe.

Starten des Hintergrunddienstes

Damit Geräteprofile übernommen werden, muss der Hintergrunddienst zum Sperren/Überwachen von HP ProtectTools Geräten ausgeführt werden. Beim ersten Versuch, Geräteprofile zu übernehmen, öffnet die HP ProtectTools Administrator-Konsole ein Dialogfeld, in dem Sie gefragt werden, ob Sie den Hintergrunddienst starten möchten. Klicken Sie auf **Ja**, um den Hintergrunddienst zu starten und so einzustellen, dass er bei jedem Systemstart automatisch gestartet wird.

Einfache Konfiguration

Device Access Manager legt bei der Initialisierung eine neue Benutzergruppe mit der Bezeichnung „Geräteadministratoren“ an. Diese Gruppe kann mit Administratorrechten auf Geräte zugreifen und diese verwalten. Nehmen Sie in diese Gruppe Benutzer auf, denen Sie einen Administratorzugriff auf die Geräte einräumen möchten, die über die einfache Konfiguration von Device Access Manager kontrolliert werden.

Mit dieser Funktion können Sie folgenden Geräteklassen den Zugriff verweigern:

- USB-Geräte für alle Nicht-Geräteadministratoren
- Alle Wechselmedien (Disketten, USB-Sticks usw.) für alle Nicht-Geräteadministratoren
- Alle DVD-/CD-ROM-Laufwerke für alle Nicht-Geräteadministratoren
- Alle seriellen und parallelen Anschlüsse für alle Nicht-Geräteadministratoren

So verweigern Sie allen Nicht-Geräteadministratoren den Zugriff auf eine Geräteklasse:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Device Access Manager** und anschließend auf **Einfache Konfiguration**.
3. Aktivieren Sie im rechten Fensterausschnitt das Kontrollkästchen eines Geräts, dem Sie den Zugriff verweigern möchten.
4. Klicken Sie auf das Symbol **Speichern**.

HINWEIS: Wenn der Hintergrunddienst noch nicht aktiv ist, versucht er jetzt, zu starten. Klicken Sie auf **Ja**, um dies zuzulassen.

5. Klicken Sie auf **OK**.

Geräteklassen-Konfiguration (erweitert)

Es stehen weitere Auswahlmöglichkeiten zur Verfügung, um bestimmten Benutzern oder Benutzergruppen den Zugriff auf bestimmte Gerätetypen zu gewähren oder zu verweigern.

Hinzufügen eines Benutzers oder einer Gruppe

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Erweitern Sie im linken Fenster die Option **Device Access Manager**, und klicken Sie dann auf **Geräteklassen-Konfiguration**.
3. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.
4. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Benutzer oder Gruppen auswählen** wird geöffnet.
5. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um die hinzuzufügenden Benutzer oder Gruppen zu suchen.
6. Klicken Sie auf einen Benutzer oder eine Gruppe, den/die Sie in die Liste der verfügbaren Benutzer bzw. Gruppen aufnehmen möchten. Klicken Sie dann auf **OK**.
7. Klicken Sie auf **OK**.

Entfernen eines Benutzers oder einer Gruppe

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Erweitern Sie im linken Fenster die Option **Device Access Manager**, und klicken Sie dann auf **Geräteklassen-Konfiguration**.
3. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.
4. Klicken Sie auf den Benutzer oder die Gruppe, der bzw. die entfernt werden soll, und klicken Sie anschließend auf **Entfernen**.

Verweigern oder Zulassen des Zugriffs durch einen Benutzer oder eine Gruppe

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Erweitern Sie im linken Fenster die Option **Device Access Manager**, und klicken Sie dann auf **Geräteklassen-Konfiguration**.
3. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.
4. Klicken Sie unter **Benutzer/Gruppen** auf den Benutzer oder die Gruppe, dem/der Sie den Zugriff verweigern möchten.
5. Klicken Sie neben dem Benutzer oder der Gruppe, welchem/welcher der Zugriff verweigert werden soll, auf **Verweigern**.
6. Klicken Sie auf das Symbol **Speichern** und anschließend auf **OK**.

Benutzerzugriffseinstellungen (erweitert)

Mit den Benutzerzugriffseinstellungen können Administratoren festlegen, welche Benutzer und Gruppen die Ansichten „Einfache Konfiguration“ und „Geräteklassen-Konfiguration“ verwenden dürfen.

Damit ein Benutzer oder eine Gruppe die Daten für die einfache oder Geräteklassen-Konfiguration anzeigen lassen kann, muss er/sie über das Zugriffsrecht **Konfigurationseinstellungen anzeigen (nur Lesezugriff)** verfügen.

Damit ein Benutzer oder eine Gruppe die Daten für die einfache oder Geräteklassen-Konfiguration ändern kann, muss er/sie über das Zugriffsrecht **Konfigurationseinstellungen ändern** verfügen.

Damit ein Benutzer oder eine Gruppe die Einstellungen in der Ansicht „Einfache Konfiguration“ oder „Geräteklassen-Konfiguration“ ändern kann, muss er/sie über das Zugriffsrecht **Alle Administrator-Benutzerrechte** verfügen.

Hinzufügen von Benutzern oder Gruppen

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Erweitern Sie im linken Fenster die Option **Device Access Manager**, und klicken Sie dann auf **Benutzerzugriffseinstellungen**.
3. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Benutzer oder Gruppen auswählen** wird geöffnet.
4. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um nach Benutzern oder Gruppen zu suchen, die hinzugefügt werden sollen.
5. Klicken Sie auf einen Benutzer oder eine Gruppe, der/die in die Liste der verfügbaren Benutzer und Gruppen aufgenommen werden soll, und danach auf **OK**.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf das Symbol **Speichern**.

Entfernen von Benutzern oder Gruppen

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Erweitern Sie im linken Fenster die Option **Device Access Manager**, und klicken Sie dann auf **Benutzerzugriffseinstellungen**.
3. Klicken Sie auf den Benutzer oder die Gruppe, den/die Sie entfernen möchten, und anschließend auf **Entfernen**.
4. Klicken Sie auf das Symbol **Speichern**.

Zulassen oder Verweigern von Berechtigungen

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Erweitern Sie im linken Fenster die Option **Device Access Manager**, und klicken Sie dann auf **Benutzerzugriffseinstellungen**.

3. Wählen Sie im Feld **Gruppen- oder Benutzernamen** den Namen eines Benutzers oder einer Gruppe aus.
4. Wählen Sie im Feld **Berechtigungen** die Kontrollkästchen **Zulassen** oder **Verweigern** für die betreffenden Berechtigungen.
5. Klicken Sie auf das Symbol **Speichern**.

Glossar

Administrator:
Siehe Windows Administrator.

Anmeldeinformationen:
Methode, bei der der Benutzer bei der Authentifizierung z. B. durch einen Benutzernamen und ein Kennwort beweist, dass er eine bestimmte Aufgabe ausführen darf.

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 Einschalten des Computers eine Form der Authentifizierung (z. B. ein Kennwort) erfordert.

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

Automatisches Shreddern:
Geplante Shred-Vorgänge, die der Benutzer in File Sanitizer for HP ProtectTools festlegt.

Bereinigen (Überschreiben von freiem Speicherplatz):
Siehe **Festplattenbereinigung**.

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

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.

Einfaches Löschen:
Sicheres Löschen sensibler Daten, einschließlich Dateien, Verlaufs- oder webbezogener Inhalte oder anderer vertraulicher Daten.

Festplattenbereinigung:
Das sichere Schreiben von Zufallsdaten über gelöschte Dateien auf die Festplatte, um den Inhalt der gelöschten Dateien zu verzerren und somit die Wiederherstellung der Daten zu erschweren.

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

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.

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.

Tastenfolge:
Eine Kombination aus bestimmten Tasten, die gedrückt wird, um einen automatischen Shred-Vorgang auszulösen, z. B. Strg+Alt+S.

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

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

Index