HP ProtectTools
Benutzerhandbuch

HP ProtectTools-Benutzerhandbuch

HP Compaq Business PC

Erste Ausgabe: Juli 2008

Teilenummer des Dokuments: 491163-041

Allgemeines

In diesem Handbuch finden Sie grundlegende Informationen für die Aufrüstung dieses Computermodells.

⚠ **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 ProtectTools Security Manager for Administrators bietet Sicherheitsfunktionen, um den unbefugten Zugriff auf den Computer sowie auf Netzwerke und kritische Daten zu verhindern. Folgende Softwaremodule bieten erweiterte Sicherheitsfunktionen:

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager für HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools

HINWEIS: Credential Manager, Java Card Security und Drive Encryption werden mit dem Security Manager-Installationsassistenten konfiguriert.

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.

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

HP ProtectTools Funktionen

Die folgende Tabelle nennt die wichtigsten Funktionen der HP ProtectTools Module:

Modul	Funktionen
HP ProtectTools Security Manager for Administrators	• Der Security Manager Installationsassistent wird von Administratoren verwendet, um Sicherheitsstufen und Sicherheits-Anmeldemethoden einzurichten und zu konfigurieren. • Benutzer können den Installationsassistenten auch zum Konfigurieren ihrer Anmeldemethoden verwenden. • Administratortools werden dazu verwendet, ProtectTools-Benutzer hinzuzufügen oder zu entfernen und den Benutzerstatus anzuzeigen. • Zum Sichern und Wiederherstellen von Sicherheitsmodulen aus installierten HP ProtectTools-Modulen.
Credential Manager for HP ProtectTools	• Credential Manager fungiert als persönlicher Kennwortspeicher und beschleunigt den Anmeldeprozess mithilfe der Single Sign On-Funktion, die automatisch Benutzerzugangsdaten speichert und anwendet. • Single Sign On bietet außerdem zusätzliche Sicherheit, weil es Kombinationen aus verschiedenen Sicherheitstechnologien erfordert, beispielsweise eine Java™ Card und biometrische Benutzerauthentifizierung. • Die Kennwortspeicherung wird durch eine Softwareverschlüsselung geschützt und kann durch den Einsatz eines TPM-Chips für integrierte Sicherheit und/oder Authentifizierung über ein Sicherheitsgerät wie Java Cards oder ein biometrisches Lesegerät noch sicherer gemacht werden.
Drive Encryption für HP ProtectTools	• Drive Encryption bietet eine vollständige Festplattenverschlüsselung für das gesamte Volume. • Drive Encryption erfordert die Authentifizierung vor dem Systemstart, um die Festplatte zu entschlüsseln und den Datenzugriff zu gewähren.
Privacy Manager für HP ProtectTools	• Privacy Manager ist ein Tool zum Generieren von Echtheitszertifikaten. Dieses Tool überprüft die Quelle, Integrität und Sicherheit der Verbindung, wenn Microsoft Mail, Microsoft Office-Dokumente und Live Messenger verwendet werden.
File Sanitizer for HP ProtectTools	• File Sanitizer ermöglicht das sichere Shreddern von digitalen Beständen (sicheres Löschen von sensiblen Informationen wie Anwendungsdateien, Verlaufsdaten oder webbezogener Content und andere vertrauliche Daten) auf dem Computer. Darüber hinaus ermöglicht File Sanitizer die regelmäßige Bereinigung der Festplatte (Überschreiben von Daten, die vorher gelöscht wurden, aber noch auf der Festplatte vorhanden sind, um die Wiederherstellung dieser Daten zu erschweren).

Modul	Funktionen
Java Card Security for HP ProtectTools	• Java Card Security ist eine Verwaltungsoberfläche für Java Card. Java Card ist ein persönliches Sicherheitsgerät, das Authentifizierungsdaten schützt, da es sowohl die Card als auch eine PIN-Nummer benötigt, um den Zugriff zu gewähren. Die Java Card kann verwendet werden, um auf Credential Manager, Drive Encryption, HP BIOS oder auf eine beliebige Anzahl von Access Points von Drittanbietern zuzugreifen. • Java Card Security konfiguriert die HP ProtectTools Java Card für die Benutzerauthentifizierung, bevor die Festplatte gestartet wird. Auf Java Card Security kann über Embedded Security, Java Card und Kennwörter zugegriffen werden. • Java Card Security konfiguriert separate Java Cards für Administrator und Benutzer.
BIOS Configuration for HP ProtectTools	• BIOS Configuration ermöglicht die Verwaltung der Benutzer- und Administratorkennwörter für den Systemstart. • BIOS Configuration stellt eine Alternative zum BIOS-Konfigurationsprogramm Computer Setup dar, das vor dem Systemstart aufgerufen werden kann. • Die Möglichkeit, in diesem Modul den automatischen DriveLock zu aktivieren, der durch den Chip für integrierte Sicherheit unterstützt wird, bietet einen Schutz der Festplatte gegen unbefugten Zugriff, auch wenn diese aus dem System ausgebaut wird. Der Benutzer muss hierzu keine zusätzlichen Kennwörter verwenden, lediglich das Benutzerkennwort für den Chip für integrierte Sicherheit.
Embedded Security for HP ProtectTools	• Embedded Security verwendet einen Trusted Platform Module (TPM) Chip für integrierte Sicherheit, um lokal auf einem PC gespeicherte sensible Benutzerdaten oder Anmeldeinformationen vor unbefugtem Zugriff zu schützen. • Mit Embedded Security kann ein PSD-Laufwerk (Personal Secure Drive) erstellt werden, das die Dateien und Ordner des Benutzers wirkungsvoll schützt. • Darüber hinaus unterstützt die Embedded Security Software Anwendungen von Fremdherstellern wie Microsoft® Outlook und Internet Explorer für geschützte digitale Zertifikatoperationen.
Device Access Manager for HP ProtectTools	• Device Access Manager ermöglicht es IT-Managern, den Zugriff auf Geräte (z. B. USB-Anschlüsse, optische Laufwerke usw.) basierend auf Benutzerprofilen zu steuern. • Device Access Manager verhindert, dass unbefugte Benutzer unter Verwendung externer Speichermedien Daten kopieren oder Viren über externe Medien in das System einschleppen. • Der Administrator kann Einzelpersonen oder Benutzergruppen den Zugriff auf beschreibbare Geräte untersagen.

Öffnen von HP ProtectTools Security

So erhalten Sie Zugriff auf HP ProtectTools Security Manager for Administrators über die Windows® Systemsteuerung:

- Klicken Sie unter Windows Vista® auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators**.

  – ODER –

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

HINWEIS: Wenn Sie kein HP ProtectTools Administrator sind, können Sie HP ProtectTools im Nicht-Administrator-Modus ausführen. Auf diese Weise können Sie die Informationen einsehen, aber nicht ändern.

HINWEIS: Nachdem Sie das Modul „Credential Manager“ konfiguriert haben, können Sie HP ProtectTools auch öffnen, indem Sie sich direkt über das Windows Anmeldefenster bei Credential Manager anmelden. Weitere Informationen finden Sie unter „Anmelden bei Windows mit dem Credential Manager“ auf Seite 29.

Lösungen für grundlegende Sicherheitsaufgaben

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

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

Schutz gegen Diebstahl

Ein Beispiel für ein solches Ereignis ist der gezielte Diebstahl eines Computers oder der auf diesem Computer befindlichen Daten und Kundendaten. Diebstähle dieser Art kommen häufig in offenen

Büroumgebungen oder ungeschützten Bereichen vor. Die folgenden Funktionen helfen beim Schutz der Daten, falls der Computer gestohlen wird:

- Wenn die Funktion für eine Authentifizierung vor dem Systemstart aktiviert ist, kann ein unbefugter Benutzer nicht auf das Betriebssystem zugreifen. Siehe auch die Vorgehensweisen für folgende Merkmale:
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- Mit DriveLock ist gewährleistet, dass auch dann nicht auf die Daten zugegriffen werden kann, wenn die Festplatte ausgebaut und in ein nicht gesichertes System wieder eingebaut wird.
- Die Personal Secure Drive Funktion des Moduls Embedded Security for HP ProtectTools verschlüsselt sensible Daten und sorgt so dafür, dass der Zugriff darauf nur nach einer erfolgreichen Authentifizierung möglich ist. Siehe auch die Vorgehensweisen für folgende Merkmale:
  - Embedded Security „Setup-Verfahren“ auf Seite 83
  - „PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk)“ auf Seite 85

Einschränken des Zugriffs auf sensible Daten

Wenn beispielsweise ein Wirtschaftsprüfer im Unternehmen die notwendigen Berechtigungen für den Zugriff auf sensible Finanzdaten erhält, soll aus Sicherheitsgründen verhindert werden, dass er diese Daten ausdrucken oder auf einem beschreibbaren Datenträger, wie beispielsweise einer CD, speichern kann. Mit den folgenden Funktionen kann der Datenzugriff beschränkt werden:

- Mit Device Access Manager für HP ProtectTools können IT-Manager den Zugriff auf beschreibbare Geräte einschränken, um das Drucken oder Kopieren von sensiblen Informationen von der Festplatte auf Wechseldatenträger zu verhindern. Siehe „Geräteklassen-Konfiguration (erweitert)“ auf Seite 92.
- Mit DriveLock ist gewährleistet, dass auch dann nicht auf die Daten zugegriffen werden kann, wenn die Festplatte ausgebaut und in ein nicht gesichertes System wieder eingebaut wird.

Verhindern des unbefugten Zugriffs von internen oder externen Standorten

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

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

- Wenn die Funktion für eine Authentifizierung vor dem Systemstart aktiviert ist, kann ein unbefugter Benutzer nicht auf das Betriebssystem zugreifen. Siehe auch die Vorgehensweisen für folgende Merkmale:
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- Embedded Security for HP ProtectTools schützt sensible Benutzerdaten oder Anmeldeinformationen, die lokal auf einem PC gespeichert sind, folgendermaßen vor unbefugtem Zugriff:
  - Embedded Security „Setup-Verfahren“ auf Seite 83
  - „PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk)“ auf Seite 85
- Mit den folgenden Vorgehensweisen sorgt Credential Manager for HP ProtectTools dafür, dass unbefugte Benutzer nicht an Kennwörter gelangen bzw. auf kennwortgeschützte Anwendungen zugreifen können:
  - Credential Manager „Setup-Verfahren“ auf Seite 24
  - „Verwenden von Single Sign On (Einmaliges Anmelden)“ auf Seite 29
- Mit Device Access Manager für HP ProtectTools können IT-Manager den Zugriff auf beschreibbare Geräte einschränken, um das Kopieren von sensiblen Informationen zu verhindern, die sich auf der Festplatte befinden. Siehe „Einfache Konfiguration“ auf Seite 90.
- Die Personal Secure Drive Funktion verschlüsselt sensible Daten und sorgt so dafür, dass der Zugriff darauf nur nach erfolgreicher Authentifizierung möglich ist. Dabei kommen die folgenden Vorgehensweisen zum Einsatz:
  - Embedded Security „Setup-Verfahren“ auf Seite 83
  - „PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk)“ auf Seite 85
- File Sanitizer ermöglicht das sichere Löschen von Daten, indem Bestände 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).
- Privacy Manager ist ein Tool zum Generieren von Echtheitszertifikaten, wenn Microsoft Mail, Microsoft Office-Dokumente und Live Messenger verwendet werden, damit wichtige Informationen sicher gesendet und gespeichert werden.

Erstellen von Richtlinien für den starken Kennwortschutz

Wenn für eine größere Zahl von webbasierten Anwendungen und Datenbanken ein besonders strikter Kennwortschutz benötigt wird, kann mit Credential Manager for HP ProtectTools ein geschütztes Repository für Kennwörter eingerichtet und die SSO-Funktionalität aktiviert werden. Die hierfür relevanten Vorgehensweisen werden in diesen Abschnitten beschrieben:

- Credential Manager „Setup-Verfahren“ auf Seite 24
- „Verwenden von Single Sign On (Einmaliges Anmelden)“ auf Seite 29

Für erhöhte Sicherheit schützt Embedded Security for HP ProtectTools das Repository der Benutzernamen und Kennwörter. Auf diese Weise können Benutzer mehrere sichere Kennwörter einrichten, ohne sich diese notieren oder merken zu müssen. Siehe „Embedded Security „Setup-Verfahren“ auf Seite 83.

Weitere Sicherheitselemente

Zuweisen von Sicherheitsrollen

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

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

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

- Sicherheitsmitarbeiter – Definiert die Sicherheitsstandards für das Unternehmen oder das Netzwerk und legt die anwendbaren Sicherheitsfunktionen fest, wie z. B. Java™ Cards, biometrische Lesegeräte oder USB-Tokens.
- IT-Administrator – Wendet die vom Sicherheitsmitarbeiter definierten Sicherheitsfunktionen an und verwaltet diese. Der IT-Administrator kann manche Funktionen auch aktivieren und deaktivieren. Wenn sich der Sicherheitsmitarbeiter z. B. für den Einsatz von Java Cards entscheidet, kann der IT-Administrator den Java Card BIOS-Sicherheitsmodus aktivieren.
- Benutzer – Verwendet die Sicherheitsfunktionen. Wenn der Sicherheitsmitarbeiter und der IT-Administrator z. B. Java Cards für das System aktiviert haben, kann der Benutzer die PIN für die Java Card festlegen und die Karte zur Authentifizierung verwenden.

Verwalten der Kennwörter für HP ProtectTools

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

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

HP ProtectTools Kennwort	In diesem HP ProtectTools Modul eingerichtet	Funktion
Credential Manager Anmeldekennwort	Credential Manager	Dieses Kennwort bietet 2 Optionen: • Es kann zur separaten Anmeldung für den Zugriff auf Credential Manager verwendet werden, nachdem Sie sich bei Windows angemeldet haben. • Es kann an Stelle des Windows Anmeldevorgangs verwendet werden, um den Zugriff auf Windows und Credential Manager gleichzeitig zu ermöglichen.
Kennwort für Wiederherstellungsdatei von Credential Manager	Credential Manager, vom IT-Administrator	Schützt den Zugriff auf die Wiederherstellungsdatei von Credential Manager.
Kennwort für allgemeinen Benutzerschlüssel	Embedded Security	Ermöglicht den Zugriff auf die Embedded Security Funktionen, wie sichere E-Mail-, Datei- und Ordnerverschlüsselung. Wenn

HP ProtectTools Kennwort	In diesem HP ProtectTools Modul eingerichtet	Funktion
HINWEIS: Auch bekannt als: Embedded Security Kennwort		dieses Kennwort für die Authentifizierung beim Einschalten verwendet wird, ermöglicht es auch den Zugriff auf die Daten im Computer, wenn der Computer eingeschaltet, neu gestartet oder der Ruhezustand beendet wird.
Kennwort für das Notfallwiederherstellungs-Token **HINWEIS:** Auch bekannt als: Kennwort für den Notfallwiederherstellungs-Schlüssel	Embedded Security, vom IT-Administrator	Schützt den Zugriff auf das Notfallwiederherstellungs-Token. Hierbei handelt es sich um eine Sicherungsdatei für den Chip für integrierte Sicherheit.
Eigentümerkennwort	Embedded Security, vom IT-Administrator	Schützt das System und den TPM-Chip vor unberechtigtem Zugriff auf alle Eigentümerfunktionen von Embedded Security.
Java™ Card-PIN	Java Card Security	Schützt den Zugriff auf die Daten der Java Card und authentifiziert Benutzer der Java Card. Wenn die Java Card-PIN für die Authentifizierung beim Einschalten verwendet wird, schützt sie auch den Zugriff auf Computer Setup Utility und auf die Daten im Computer. Authentifiziert Benutzer von Drive Encryption, wenn das Java Card-Token ausgewählt wird.
Kennwort für Computer Setup **HINWEIS:** Auch bekannt als BIOS-Administrator-, F10-Setup- oder Sicherheits-Setup-Kennwort	BIOS Configuration, vom IT-Administrator	Schützt den Zugriff auf Computer Setup Utility.
Systemstart-Kennwort	BIOS Configuration	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 oder auf der Java Card gespeichert 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 und Wiederherstellen von Zugangsdaten in HP ProtectTools

Zum Sichern und Wiederherstellen von Zugangsdaten aus allen unterstützten HP ProtectTools Modulen gehen Sie wie folgt vor:

Sichern von Zugangsdaten und Einstellungen

Sie können Zugangsdaten auf folgende Arten sichern:

- Wählen und sichern Sie die Zugangsdaten von HP ProtectTools über Drive Encryption for HP ProtectTools.

  Sie können sich auch beim Online-Dienst zur Schlüsselwiederherstellung von Drive Encryption registrieren. Dieser speichert eine Kopie des Sicherungs- bzw. Chiffrierschlüssels, mit dessen Hilfe Sie auf Ihren Computer zugreifen können, selbst wenn Sie das Kennwort vergessen und keinen Zugriff auf Ihre lokale Sicherungskopie haben.

  HINWEIS: Sie müssen über eine Internetverbindung und eine gültige E-Mail-Adresse verfügen, damit Sie sich registrieren und Ihr Kennwort über diesen Service wiederherstellen können.

- Sichern Sie die Zugangsdaten von HP ProtectTools über Embedded Security for HP ProtectTools.
- Verwenden Sie das Tool „Backup and Recovery“ in HP ProtectTools Security Manager for Administrators als zentralen Ort zum Sichern und Wiederherstellen von Sicherheitsinformationen aus installierten HP ProtectTools-Modulen.

2 HP ProtectTools Security Manager for Administrators

Info über HP ProtectTools Security Manager for Administrators

HP ProtectTools Security Manager for Administrators bietet Sicherheitsfunktionen, um den unbefugten Zugriff auf den Computer, Netzwerke und kritische Daten zu verhindern. Security Manager ist mit neuen Technologien zur Beseitigung von aktuellen Bedrohungen erweiterbar.

Verwenden Sie für das erste Sichherheitssetup das Modul „HP ProtectTools Security Manager for Administrators“. Die zentrale Benutzeroberfläche von Security Manager bietet folgende Funktionen:

- **Einführung** – Der Installationsassistent, der Administratoren von Windows Betriebssystemen durch die Konfiguration der Sicherheitsstufen und der Sicherheits-Anmeldemethoden leitet, die in einer Systemstartumgebung, in Credential Manager und in Drive Encryption verwendet werden. Benutzer können den Installationsassistenten auch zum Konfigurieren der Sicherheits-Anmeldemethoden verwenden. Weitere Informationen finden Sie unter „Getting Started (Einführung) – Konfigurieren von HP ProtectTools Security Manager for Administrators“ auf Seite 13 und „Getting Started (Einführung) – Konfigurieren der Sicherheits-Anmeldemethoden von Benutzern“ auf Seite 15.
- **Administrators Tools** – Ermöglicht Windows Administratoren das Hinzufügen und Entfernen von ProtectTools-Benutzern sowie das Anzeigen des Benutzerstatus. Weitere Hinweise erhalten Sie unter „Administrator Tools – Benutzerverwaltung (Administratoraufgabe)“ auf Seite 17.
- **Backup and Restore** (Sichern und Wiederherstellen) – Zum Sichern und Wiederherstellen der Sicherheitsinformationen aus installierten HP ProtectTools-Modulen. Weitere Hinweise erhalten Sie unter „Backup and Restore“ auf Seite 19.
- **Einstellungen** – Zum Anpassen des Verhaltens einer Vielzahl von Elementen. Weitere Hinweise erhalten Sie unter „Einstellungen“ auf Seite 23.

Die zentrale Benutzeroberfläche von Security Manager enthält auch eine Liste zusätzlicher Software-Module zur Verbesserung der Computersicherheit. Sie können beliebig viele Module auswählen und konfigurieren.

Getting Started (Einführung) – Konfigurieren von HP ProtectTools Security Manager for Administrators

Mit dem Installationsassistenten „Getting Started“ (Einführung) können Windows Administratoren Sicherheitsstufen und Sicherheits-Anmeldemethoden einrichten und/oder aktualisieren.

Auch die Sicherheits-Anmeldemethoden der Benutzer können mit dem Installations-Assistenten konfiguriert werden.

HINWEIS: Windows Administratoren können den Installationsassistenten zum Ändern der Sicherheitsstufen oder Sicherheits-Anmeldemethoden jederzeit ausführen.

Der Installationsassistent leitet Windows Administratoren durch die Konfiguration von Security Manager:

1. Klicken Sie in HP ProtectTools Security Manager for Administrators auf **Getting Started** (Einführung) und anschließend auf die Schaltfläche **Security Manager Setup**. Daraufhin wird möglicherweise eine Demo der Security Manager-Funktionen gestartet.
2. Deaktivieren Sie auf der Willkommensseite (falls verfügbar) das Kontrollkästchen **Automatically play video when wizard starts** (Video beim Start des Assistenten automatisch abspielen), wenn Sie die Demo der Security Manager-Funktionen bei der nächsten Ausführung des Installationsassistenten überspringen möchten.
3. Lesen Sie die Seite, und klicken Sie auf **Weiter**.
4. Wählen Sie die Sicherheitsstufen auf der Seite „Set Levels of Security“ (Sicherheitsstufen einstellen) aus. Sie können eine oder mehrere der folgenden Stufen auswählen:
   - HP Credential Manager – Schützt Ihr Windows Konto.
   - Pre-boot Security (Sicherheit vor dem Systemstart) (bestimmte Modelle) – Schützt den Computer, bevor Windows gestartet wird.
   - HP Drive Encryption – Schützt die Computerdaten durch Verschlüsselung der Festplatte. Wenn Sie diese Option wählen, müssen Sie den eindeutigen Codierungsschlüssel auf einem Wechseldatenträger sichern.

   HINWEIS: Die Sicherheitsanzeige verändert sich entsprechend Ihrer Auswahl. Je mehr Sicherheitsstufen Sie auswählen, desto geschützter ist Ihr Computer.

   Klicken Sie nach Auswahl der Sicherheitsstufen auf **Weiter**.

5. Es werden eine oder mehrere der folgenden Seiten angezeigt, je nachdem, welche Sicherheitsstufen Sie in Schritt 4 ausgewählt haben.

   - Protect your Windows account (Windows Konto schützen) – Das Windows Kennwort ist erforderlich, da Security Manager das Kennwort für jede einzelne Sicherheitsstufe synchronisieren muss.

     Geben Sie ein Windows Kennwort ein, und bestätigen Sie es, oder geben Sie Ihr Kennwort ein, falls Sie bereits ein Kennwort eingerichtet haben, und klicken Sie auf **Weiter**.

   - Protect your system before Windows start-up (System vor dem Windows Systemstart schützen) (optional) – Falls Sie oder der Benutzer das BIOS-Administratorkennwort kennen, geben Sie dieses Kennwort ein. Bei Eingabe des BIOS-Administratorkennworts wird der Windows Administrator oder -Benutzer als BIOS-Administrator angemeldet.

     HINWEIS: Falls kein BIOS-Administratorkennwort vorhanden ist, müssen Sie dieses Kennwort einrichten, um fortzufahren. Bei Eingabe des BIOS-Administratorkennworts werden Sie als BIOS-Administrator angemeldet.

     Geben Sie ein BIOS-Administratorkennwort ein, oder geben Sie Ihr Kennwort ein, falls Sie bereits ein Kennwort eingerichtet haben. Klicken Sie anschließend auf **Weiter**.

   - Protect your data by encrypting your hard drive (Daten durch Verschlüsselung der Festplatte schützen) – Sie müssen den Codierungsschlüssel auf einem USB-Datenträger speichern. Wählen Sie die zu verschlüsselnden Laufwerke aus (mindestens ein Laufwerk), setzen Sie den Datenträger in den entsprechenden Steckplatz ein, wählen Sie den Datenträger aus, auf dem der Codierungsschlüssel gespeichert wird, und klicken Sie auf **Weiter**.

6. Wählen Sie auf der Seite „Set Security Login Methods“ (Sicherheits-Anmeldemethoden einstellen) eine oder mehrere Sicherheits-Anmeldemethoden aus.

   a. Wählen Sie in Schritt 1 eine oder mehrere Sicherheits-Anmeldemethoden aus.

      HINWEIS: Die Auswahl bezieht sich sowohl auf Administratoren als auch auf Benutzer.

   b. Um die Sicherheit zu erhöhen, aktivieren Sie in Schritt 2 das Kontrollkästchen, damit *alle* in Schritt 1 ausgewählten Sicherheits-Anmeldemethoden bei der Anmeldung am Computer erforderlich sind.

      Wenn Sie möchten, dass eine *beliebige* der ausgewählten Sicherheits-Anmeldemethoden bei der Anmeldung am Computer zulässig ist, aktivieren Sie dieses Kontrollkästchen nicht.

      △ **ACHTUNG:** Wenn Sie das Kontrollkästchen aktivieren und ein Benutzer seine Anmeldemethoden (Windows Kennwort, Fingerabdruckauthentifizierung und/oder HP ProtectTools Java™ Card) noch nicht konfiguriert hat, kann sich dieser Benutzer nicht beim Computer anmelden. Es wird empfohlen, dass alle Benutzer zunächst ihre Anmeldemethoden konfigurieren, bevor diese Option gewählt wird.

   c. Klicken Sie auf **Weiter**. Eine Übersichtsseite wird angezeigt, auf der Sie Ihre Auswahl überprüfen können.

7. Klicken Sie auf der Seite „Review and Enable Security Settings“ (Sicherheitseinstellungen überprüfen und aktivieren) auf **Enable** (Aktivieren).

   Wenn sie auf **Enable** (Aktivieren) klicken, übernimmt der Computer die von Ihnen ausgewählten Sicherheitsoptionen. Sie können erst zu einer der vorherigen Seiten des Assistenten zurückkehren, wenn das Sicherheits-Setup abgeschlossen ist. Wenn Sie Ihre Einstellungen nach Beendigung des Assistenten ändern möchten, führen Sie den Assistenten noch einmal aus.

8. Es werden eine oder mehrere der folgenden Seiten angezeigt, je nachdem, welche Sicherheitsstufen Sie in Schritt 6 ausgewählt haben. Befolgen Sie die Anleitungen auf dem Bildschirm, und klicken Sie auf **Weiter**.

   - „Enroll your fingerprints“ (Fingerabdrücke registrieren) – Klicken Sie auf den Finger auf dem Bildschirm, der dem Finger entspricht, den Sie registrieren möchten (Sie müssen mindestens zwei Fingerabdrücke registrieren.). Streichen Sie mit dem ausgewählten Finger langsam über den Fingerabdrucksensor. Wiederholen Sie dies so lange, bis der Vorgang abgeschlossen ist. Wiederholen Sie diesen Vorgang, um einen zweiten Finger zu registrieren, und klicken Sie anschließend auf **Fertig stellen**.

   - „Register an HP ProtectTools Java Card“ (HP ProtectTools Java Card registrieren) – Legen Sie die HP ProtectTools Java Card ein, geben Sie die Java Card-PIN ein, und klicken Sie anschließend auf **Fertig stellen**.

9. Überprüfen Sie Ihre Auswahl auf der Seite „Congratulations“ (Herzlichen Glückwunsch), und klicken Sie anschließend auf **Fertig**.

Getting Started (Einführung) – Konfigurieren der Sicherheits-Anmeldemethoden von Benutzern

Nachdem der Windows Administrator die Sicherheitsstufen und Sicherheits-Anmeldemethoden konfiguriert hat, führt der Benutzer den Installationsassistenten aus, um als HP ProtectTools-Benutzer auf dem Computer registriert zu werden:

HINWEIS: Benutzer, die den Installationsassistenten ausführen, können die meisten Assistentenseiten anzeigen. Die Seiten „Set Levels of Security“ (Sicherheitsstufen einstellen) und „Set Security Login Methods“ (Sicherheits-Anmeldemethoden einstellen) sind jedoch nicht konfigurierbar, da sie nur Administratoraufgaben enthalten.

1. Melden Sie sich beim Computer an.

2. Klicken Sie in Security Manager auf **Getting Started** (Einführung) und anschließend auf die Schaltfläche **Security Manager Setup**.

3. Deaktivieren Sie auf der Willkommensseite das Kontrollkästchen **Automatically play video when wizard starts** (Video beim Start des Assistenten automatisch abspielen), wenn Sie die Demo der Security Manager-Funktionen bei der nächsten Ausführung des Installationsassistenten überspringen möchten.

4. Lesen Sie die Seite, und klicken Sie auf **Weiter**.

5. Klicken Sie auf der Seite „Set Levels of Security“ (Sicherheitsstufen einstellen) auf **Weiter**.

6. Es werden eine oder beide der folgenden Seiten angezeigt, je nachdem, welche Sicherheitsstufen vom Administrator eingestellt wurden.

   - Protect your Windows account (Schützen Sie Ihr Windows Konto) – Das Windows Kennwort ist erforderlich, da Security Manager das Kennwort für jede einzelne Sicherheitsstufe synchronisieren muss.

     HINWEIS: Wenn nur die Sicherheitsstufe „HP Credential Manager“ ausgewählt wurde, werden Sie nicht zur Eingabe des Windows Kennworts aufgefordert, da Credential Manager Ihr Windows Kennwort bereits kennt.

     Geben Sie ein Windows Kennwort ein, und bestätigen Sie es, oder geben Sie Ihr Kennwort ein, falls Sie bereits ein Kennwort eingerichtet haben. Klicken Sie anschließend auf **Weiter**.

   - Protect your system before Windows start-up (Schützen Sie Ihr System vor dem Windows Systemstart) (optional) – Falls Sie das BIOS-Administratorkennwort kennen, geben Sie dieses Kennwort ein. Bei Eingabe des BIOS-Administratorkennworts wird der Windows Administrator oder Benutzer als BIOS-Administrator angemeldet.

     HINWEIS: Falls kein BIOS-Administratorkennwort vorhanden ist, müssen Sie dieses Kennwort einrichten, um fortzufahren. Bei Eingabe des BIOS-Administratorkennworts werden Sie als BIOS-Administrator angemeldet.

     Geben Sie ein BIOS-Administratorkennwort ein, oder geben Sie Ihr Kennwort ein, falls Sie bereits ein Kennwort eingerichtet haben. Klicken Sie anschließend auf **Weiter**.

7. Klicken Sie auf der Seite „Set Security Login Methods“ (Sicherheits-Anmeldemethoden einstellen) auf **Weiter**.

8. Klicken Sie auf der Seite „Review and Enable Security Settings“ (Sicherheitseinstellungen überprüfen und aktivieren) auf **Enable** (Aktivieren).

9. Es werden eine oder beide der folgenden Seiten angezeigt, je nachdem, welche Sicherheits-Anmeldemethoden vom Administrator festgelegt wurden. Befolgen Sie die Anleitungen auf dem Bildschirm, und klicken Sie auf **Weiter**.

   - „Enroll your fingerprints“ (Fingerabdrücke registrieren) – Klicken Sie mit dem Finger auf den Bildschirm, der dem Finger entspricht, den Sie registrieren möchten (Sie müssen mindestens zwei Fingerabdrücke registrieren.) Streichen Sie mit dem ausgewählten Finger langsam über den Fingerabdrucksensor. Wiederholen Sie dies so lange, bis der Vorgang abgeschlossen ist. Wiederholen Sie diesen Vorgang, um einen zweiten Finger zu registrieren, und klicken Sie anschließend auf **Fertig stellen**.

   - „Register an HP ProtectTools Java Card“ (HP ProtectTools Java Card registrieren) – Legen Sie die HP ProtectTools Java Card ein, geben Sie die Java Card-PIN ein, und klicken Sie anschließend auf **Fertig stellen**.

10. Übrprüfen Sie Ihre Auswahl auf der Seite „Congratulations“ (Herzlichen Glückwunsch), und klicken Sie anschließend auf **Fertig**.

Anmelden nach der Konfiguration von Security Manager

Die Anmeldeszenarien variieren, je nachdem, welche Sicherheitsstufen und Sicherheits-Anmeldemethoden vom Administrator während der Konfiguration ausgewählt wurden. Folgende Szenarien sind möglich:

- Falls alle 3 Sicherheitsstufen konfiguriert wurden und *alle* Sicherheits-Anmeldemethoden erforderlich sind, muss sich der Benutzer unter Verwendung aller Konfigurationsmethoden anmelden, wenn der Computer zum ersten Mal eingeschaltet wird. Dieser Vorgang meldet den Benutzer bei Windows an.
- Falls alle 3 Sicherheitsstufen konfiguriert wurden und *beliebige* Sicherheits-Anmeldemethoden zulässig sind, kann sich der Benutzer unter Verwendung einer beliebigen konfigurierten Sicherheits-Anmeldemethode anmelden, wenn der Computer zum ersten Mal eingeschaltet wird. Dieser Vorgang meldet den Benutzer bei Windows an.
- Falls die Sicherheitsstufen „HP Drive Encryption“ und „HP Credential Manager“ konfiguriert wurden und *alle* Sicherheits-Anmeldemethoden erforderlich sind, müssen sich Benutzer unter Verwendung aller konfigurierten Methoden anmelden, wenn der Bildschirm „HP Drive Encryption“ angezeigt wird. Dieser Vorgang meldet den Benutzer bei Windows an.
- Falls die Sicherheitsstufen „HP Drive Encryption“ und „HP Credential Manager“ konfiguriert wurden und *beliebige* konfigurierte Sicherheits-Anmeldemethoden zulässig sind, können sich Benutzer unter Verwendung einer beliebigen Sicherheits-Anmeldemethode anmelden, wenn der Bildschirm „HP Drive Encryption“ angezeigt wird. Dieser Vorgang meldet den Benutzer bei Windows an.
- Falls die Sicherheitsstufe „HP Credential Manager“ konfiguriert wurde und *alle* Sicherheits-Anmeldemethoden erforderlich sind, müssen sich Benutzer unter Verwendung aller konfigurierten Methoden anmelden, wenn der Bildschirm „HP Credential Manager“ angezeigt wird. Dieser Vorgang meldet den Benutzer bei Windows an.
- Falls die Sicherheitsstufe „HP Credential Manager“ konfiguriert wurde und *beliebige* konfigurierte Sicherheits-Anmeldemethoden zulässig sind, können sich Benutzer unter Verwendung einer beliebigen Sicherheits-Anmeldemethode anmelden, wenn der Bildschirm „HP Credential Manager“ angezeigt wird. Dieser Vorgang meldet den Benutzer bei Windows an.

HINWEIS: Falls die Sicherheitsstufe „HP Credential Manager“ nicht konfiguriert wurde, müssen Benutzer am Windows Anmeldebildschirm ihr Windows Kennwort eingeben, unabhängig davon, welche Sicherheits-Anmeldemethoden von anderen Sicherheitsstufen angefordert werden.

Administrator Tools – Benutzerverwaltung (Administratoraufgabe)

Mit der Funktion „Administrator Tools“ können Windows Administratoren HP ProtectTools-Benutzer hinzufügen bzw. entfernen und den Benutzerstatus anzeigen.

Die unter „Administrator Tools“ enthaltenen Registerkarten „Administrator“ und „User“ (Benutzer) zeigen die ausgewählten Sicherheits-Anmeldemethoden sowie Informationen darüber an, ob ein Benutzer beliebige dieser Sicherheits-Anmeldemethoden auswählen kann oder alle verwenden muss. Um die Sicherheitsstufen oder Sicherheits-Anmeldemethoden zu ändern, müssen Sie den Installationsassistenten ausführen.

Hinzufügen eines Benutzers

Der Windows Administrator kann der Benutzerliste zusätzliche Administratoren oder „normale“ Benutzer hinzufügen. Die Vorgehensweise ist für beide identisch.

HINWEIS: Um einen Benutzer hinzufügen zu können, muss dieser Benutzer 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 Security Manager for Administrators**.
2. Klicken Sie auf **Administrator Tools**.
3. Klicken Sie auf die Schaltfläche **Manage Users** (Benutzer verwalten).
4. Wählen Sie die Registerkarte **Administrator** oder **User** (Benutzer).
5. Klicken Sie auf **Add** (Hinzufügen).
6. Klicken Sie auf den Benutzernamen für das Konto, das Sie hinzufügen möchten, oder geben Sie den Benutzernamen in das Feld **User Name** (Benutzername) ein. Klicken Sie anschließend auf **Weiter**.

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

7. Geben Sie das Windows Kennwort für das ausgewählte Konto ein, und klicken Sie auf **OK**.

   HINWEIS: Wenn sich der Benutzer über seinen Fingerabdruck und/oder die Sicherheits-Anmeldemethode „HP ProtectTools Java Card“ anmeldet, muss er sich jetzt beim Computer anmelden und den Installationsassistenten ausführen, um diese Sicherheits-Anmeldemethoden zu konfigurieren.

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.

So entfernen Sie einen Benutzer aus der Benutzerliste:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators**.
2. Klicken Sie auf **Administrator Tools**.
3. Klicken Sie auf die Schaltfläche **Manage Users** (Benutzer verwalten).
4. Wählen Sie die Registerkarte **Administrator** oder **User** (Benutzer).
5. Klicken Sie auf den Benutzernamen für das Konto, das Sie entfernen möchten, und klicken Sie anschließend auf **Entfernen**.

HINWEIS: Administratoren können nicht entfernt werden, wenn nur ein Administratoreintrag in der Liste besteht.

6. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Überprüfen des Benutzerstatus

Die unter „Administrator Tools“ enthaltenen Registerkarten „Administrator“ und „User“ (Benutzer) zeigen den aktuellen Status der einzelnen Benutzer an:

- **Grünes Häkchen** - Gibt an, dass der Benutzer die erforderliche(n) Sicherheits-Anmeldemethode(n) konfiguriert hat.
- **Gelbes Ausrufungszeichen** - Gibt an, dass der Benutzer eine oder mehrere erforderliche oder zulässige Sicherheits-Anmeldemethoden nicht konfiguriert hat. Wenn der Windows Administrator mindestens 2 erforderliche Sicherheits-Anmeldemethoden konfiguriert und angibt, dass beide Methoden für die Anmeldung beim Computer verwendet werden können, kann sich ein Benutzer, der eine dieser beiden Methoden bereits konfiguriert hat, unter Verwendung dieser Methode beim Computer anmelden. Das gelbe Ausrufungszeichen gibt dem Windows Administrator an, dass der Benutzer die andere Sicherheits-Anmeldemethode noch nicht 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.

Backup and Restore

HP ProtectTools Backup and Restore bietet einen zentralen Ort, über den Sie Sicherheitsinformationen aus installierten HP ProtectTools-Modulen sichern und wiederherstellen können.

Klicken Sie in Security Manager auf **Backup and Restore** und anschließend auf eine der folgenden Schaltflächen:

- Schaltfläche **Backup Options** (Sicherungsoptionen) – Zum Konfigurieren der Sicherungseinstellen. Weitere Informationen finden Sie unter „Verwenden des Sicherungsassistenten“ auf Seite 20.
- Schaltfläche **Backup** (Sichern) – Zum Durchführen einer sofortigen Sicherung aller Sicherheitsinformationen.

HINWEIS: Um eine Sicherung durchführen zu können, müssen Sie die Sicherungseinstellungen über die Schaltfläche **Backup Options** (Sicherungsoptionen) konfigurieren.

- Schaltfläche **Schedule Backups** (Sicherungen planen) – Zum Einrichten geplanter Sicherungen. Wenn Sie bei der Planung Hilfe benötigen, suchen Sie in der Windows Hilfe nach dem Thema „Planen einer Aufgabe“.

HINWEIS: Um eine Sicherung planen zu können, müssen Sie die Sicherungseinstellungen über die Schaltfläche **Backup Options** (Sicherungsoptionen) konfigurieren.

- Schaltfläche **Restore** (Wiederherstellen) – Zum Wiederherstellen vorher gesicherter Sicherheitsinformationen. Weitere Informationen finden Sie unter „Verwenden des Wiederherstellungsassistenten“ auf Seite 21.

△ **ACHTUNG:** Außerhalb von HP ProtectTools Backup and Restore erstellte Sicherungsdateien (z. B. von einem bestimmten Sicherheitsmodul erstellte Dateien) sind mit HP ProtectTools Backup and Restore nicht kompatibel und können daher auch nicht von HP ProtectTools Backup and Restore oder neuen Versionen der Sicherheitsmodule selbst wiederhergestellt werden. HP empfiehlt, dass Sie eine neue Sicherungsdatei mit HP ProtectTools Backup and Restore erstellen.

Verwenden des Sicherungsassistenten

1. Klicken Sie in Security Manager auf **Backup and Restore** (Sichern und Wiederherstellen), und klicken Sie anschließend auf **Backup Options** (Sicherungsoptionen), um den Sicherungsassistenten zu starten.
2. Deaktivieren Sie das Kontrollkästchen **Show Welcome Screen** (Willkommensbildschirm anzeigen), um die Seite „Welcome“ (Willkommen) zu überspringen, wenn Sie den Sicherungsassistenten das nächste Mal ausführen.
3. Klicken Sie auf **Weiter**. Die Seite „Security Modules“ (Sicherheitsmodule) wird geöffnet.
4. Weitere Informationen finden Sie in den nachstehenden Abschnitten.

Sicherheitsmodule

Um die zu sichernden Module auszuwählen, führen Sie folgende Schritte aus:

1. Aktivieren Sie das Kontrollkästchen am Beginn einer Zeile, um das zugehörige Modul zur Sicherungsliste hinzuzufügen. Klicken Sie auf **Alle auswählen** oder **Auswahl aufheben**, um alle Module schnell zur Sicherungsliste hinzuzufügen bzw. aus der Sicherungsliste zu entfernen. Die Spalte „Status“ für das jeweilige Modul muss „Ready“ (Bereit) oder „Needs Authentication“ (Authentifizierung erforderlich) anzeigen, um sie auswählen zu können.

HINWEIS: Das Kontrollkästchen ist nicht verfügbar, wenn das Modul nicht bereit ist. Nachdem Sie den Status eines Moduls aktualisiert haben, klicken Sie rechts in der Zeile auf die Schaltfläche **Aktualisieren**, um das Feld „Status“ zu aktualisieren. Klicken Sie auf die Schaltfläche **Alle aktualisieren**, um den Status für alle Module zu aktualisieren.

2. Geben Sie bei Bedarf für jedes ausgewählte Modul den erforderlichen Wert in die Spalte „Authentication“ (Authentifizierung) ein. Das Sicherheitsgerät erfordert möglicherweise die Eingabe von Authentifizierungswerten, um auf die Anmeldeinformationen des Geräts zuzugreifen. Bei diesen Werten kann es sich um Kennwörter, PINs usw. handeln.
3. Klicken Sie auf **Weiter**. Die Seite „File Location“ (Dateipfad) wird geöffnet.

Dateipfad

Auf der Seite „File Location“ (Dateipfad) können Sie den Speicherort der Sicherungsdatei und der Sicherheits-Token-Datei auswählen.

Die Sicherheits-Token-Datei speichert den zur Verschlüsselung der Sicherungsdatei verwendeten Schlüssel auf sichere Weise. Ein Kennwort verschlüsselt den Inhalt der Sicherheits-Token-Datei. Wenn Sie die Sicherheits-Token-Datei auf einem externen Datenträger (USB-Flash-Laufwerk, Diskette oder andere Datenträger) speichern, erhalten Sie einen zweistufigen Schutz, da Sie für den Zugriff auf die gesicherten Daten in der Speicherdatei die Sicherheits-Token-Datei *haben* und das Kennwort *kennen* müssen. Aus diesem Grund empfiehlt HP, die Speicherdatei und die Token-Datei auf zwei unterschiedlichen Wechseldatenträgern zu speichern, die an unterschiedlichen Standorten aufbewahrt werden.

So konfigurieren Sie den Speicherort der Datei:

1. Bestätigen oder ändern Sie den Dateinamen und den Speicherort, unter dem Sie die Speicherdatei und die Sicherheits-Token-Datei speichern möchten. Um den Speicherort zu ändern, klicken Sie auf die Schaltfläche **Bearbeiten** und geben den neuen Dateinamen ein. Wenn Sie auf **Durchsuchen** klicken, können Sie einen neuen Speicherort auswählen. Die Dateierweiterung .ptb wird automatisch an den Dateinamen angehängt.

   HINWEIS: In einer bestimmten Speicherdatei darf pro Modul nur jeweils nur ein Satz an Sicherungsdaten vorhanden sein. Wenn Sie eine bestehende Speicherdatei angeben, haben Sie die Möglichkeit, die Daten des ausgewählten Moduls innerhalb der Speicherdatei zu überschreiben oder eine andere Speicherdatei anzugeben. Wenn Sie eine bestehende Speicherdatei angeben, wird nicht die gesamte Datei überschrieben; es werden lediglich die Sicherungsdaten für das ausgewählte Modul überschrieben.

2. Um die Speicherdatei mit dem Sicherheits-Token und dem Kennwort zu verschlüsseln und zu schützen, klicken Sie auf **Password protect the storage file** (Kennwortschutz für Speicherdatei verwenden). Geben Sie dann das Kennwort zur Verschlüsselung der Sicherheits-Token-Datei ein, und bestätigen Sie es.

3. Klicken Sie auf **Remember all passwords and authentication values** (Alle Kennwörter und Authentifizierungswerte speichern), um das System so zu konfigurieren, dass Kennwörter sicher zwischengespeichert werden. Hierdurch werden unbeaufsichtigte Sicherungen aktiviert. Wenn Sie diese Funktion aktivieren, werden außerdem die in Sicherheitsmodulen eingegebenen Authentifizierungswerte zwischengespeichert.

4. Klicken Sie auf **Jetzt sichern**, um den Sicherungsvorgang zu starten, oder klicken Sie auf **Weiter**, um die Sicherungskonfiguration zu speichern, ohne eine Sicherung durchzuführen.

   Wenn Sie den Sicherungsvorgang starten, wird die Seite „Backup Complete“ (Sicherung abgeschlossen) nach Abschluss der Sicherung geöffnet.

Sicherung abgeschlossen

Die Seite „Backup Complete“ (Sicherung abgeschlossen) zeigt den Status des Sicherungsvorgangs an.

1. Klicken Sie auf **Protokoll anzeigen**, um weitere Einzelheiten zum Sicherungsvorgang anzuzeigen, einschließlich möglicher Fehler.

2. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

Verwenden des Wiederherstellungsassistenten

1. Klicken Sie in Security Manager auf **Backup and Restore** (Sichern und Wiederherstellen), und klicken Sie anschließend auf **Restore** (Wiederherstellen), um den Wiederherstellungsassistenten zu starten.

2. Deaktivieren Sie das Kontrollkästchen **Show Welcome Screen** (Willkommensbildschirm anzeigen), um die Seite „Welcome“ (Willkommen) zu überspringen, wenn Sie den Wiederherstellungsassistenten das nächste Mal ausführen.

3. Klicken Sie auf **Weiter**. Die Seite „File Location“ (Dateipfad) wird geöffnet.

4. Weitere Informationen finden Sie in den nachstehenden Abschnitten.

Dateipfad

Auf der Seite „File Location“ (Dateipfad) können Sie die Sicherungsdatei und die Sicherheits-Token-Datei (falls zutreffend) auswählen, welche die wiederherzustellenden Sicherheitsinformationen enthalten.

Um den Speicherort der Sicherungsdateien auszuwählen, führen Sie folgende Schritte aus:

1. Falls die Speicherdatei nicht auf der Seite angezeigt wird, klicken Sie auf die Schaltfläche **Bearbeiten** und anschließend auf die Schaltfläche **Durchsuchen**, um zu dieser Datei zu navigieren.
2. Falls die Sicherheits-Token-Datei nicht auf der Seite angezeigt wird, klicken Sie auf die Schaltfläche **Bearbeiten** und anschließend auf die Schaltfläche **Durchsuchen**, um zum Speicherort der Sicherheits-Token-Datei zu navigieren.
3. Falls erforderlich, geben Sie das Kennwort für die Datei ein.
4. Klicken Sie auf **Weiter**. Die Seite „Security Modules“ (Sicherheitsmodule) wird geöffnet.

Sicherheitsmodule

Diese Seite zeigt alle installierten Module an, für die gesicherte Daten in der Datei enthalten sind, die auf der Seite „File Location“ (Dateipfad) ausgewählt wurde.

So wählen Sie wiederherzustellende Module aus:

1. Aktivieren Sie das Kontrollkästchen am Beginn jeder Zeile, um das zugehörige Modul zur Wiederherstellungsliste hinzuzufügen. Klicken Sie auf **Alle auswählen** oder **Auswahl aufheben**, um alle Module schnell zur Wiederherstellungsliste hinzuzufügen bzw. aus der Wiederherstellungsliste zu entfernen. Die Spalte „Status“ für das jeweilige Modul muss „Ready“ (Bereit) oder „Needs Authentication“ (Authentifizierung erforderlich) anzeigen, um sie auswählen zu können.

   HINWEIS: Das Kontrollkästchen ist nicht verfügbar, wenn das Modul nicht bereit ist. Nachdem Sie den Status eines Moduls aktualisiert haben, klicken Sie rechts in der Zeile auf die Schaltfläche **Aktualisieren**, um das Feld „Status“ zu aktualisieren. Klicken Sie auf die Schaltfläche **Alle aktualisieren**, um den Status für alle Module zu aktualisieren.

2. Geben Sie bei Bedarf für jedes ausgewählte Modul den erforderlichen Wert in die Spalte „Authentication“ (Authentifizierung) ein. Für den Zugriff auf das Sicherheitsgerät sind möglicherweise Authentifizierungswerte erforderlich. Bei diesen Werten kann es sich um Kennwörter, PINs usw. handeln. Die in diese Felder eingegebenen Werte werden sofort überprüft.
3. Klicken Sie auf **Weiter**. Die Bestätigungsseite wird geöffnet.

Bestätigung

1. Zum Ändern der Wiederherstellungseinstellungen klicken Sie auf **Zurück**, um zu den Bildschirmen der Wiederherstellungskonfiguration zurückzukehren.
2. Bestätigen Sie, dass Sie die Anmeldeinformationen für die aufgelisteten Module wiederherstellen möchten, und klicken Sie anschließend auf **Jetzt wiederherstellen**, um den Wiederherstellungsvorgang zu starten.
3. Wählen Sie die wiederherzustellenden Dateien aus, und klicken Sie auf **Fertig stellen**.
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

△ **ACHTUNG:** Beim Wiederherstellen der Anmeldeinformationen werden die aktuellen Anmeldeinformationen überschrieben. Hierdurch kann es zu einem Datenverlust oder einer Systemsperrung kommen.

Wiederherstellung abgeschlossen

Die Seite „Restore Complete“ (Wiederherstellung abgeschlossen) zeigt den Status des Wiederherstellungsvorgangs an.

- Klicken Sie auf **Protokoll anzeigen**, um weitere Einzelheiten zum Wiederherstellungsvorgang anzuzeigen, einschließlich möglicher Fehler.
- Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

Einstellungen

Klicken Sie in HP ProtectTools Security Manager for Administrators auf **Einstellungen**, um die Einstellungsoptionen zu ändern.

Die folgenden Security Manager-Einstellungen sind verfügbar:

- Aktivieren des Kontrollkästchens **Show icon on the taskbar** (Symbol in Taskleiste anzeigen), über das Sie den Host starten und eine bestimmte Seite aktivieren bzw. eine bestimmte Anwendung starten können
- Aktivieren des Kontrollkästchens **Show Security Desktop Notifications** (Sicherheitsinfo auf Desktop anzeigen), um die Benachrichtigungen anzuzeigen, die von den installierten Modulen generiert werden
- Anzeigen oder Überspringen der Willkommensseite des Sicherungsassistenten
- Anzeigen oder Überspringen der Willkommensseite des Wiederherstellungsassistenten

3 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools enthält die folgenden Sicherheitsfunktionen, um Sie vor einem unberechtigten Zugriff auf Ihren Computer zu schützen.

- Alternativen zu Kennwörtern für die Anmeldung bei Windows, wie z. B. die Verwendung einer Java Card oder eines biometrischen Lesegeräts. Weitere Informationen finden Sie unter „Registrieren von Anmeldeinformationen“ auf Seite 25.
- SSO-Funktion (Single Sign On; Einmaliges Anmelden), die automatisch die Berechtigungen für den Zugriff auf Websites, Anwendungen und geschützte Ressourcen im Netzwerk speichert.
- Unterstützung für optionale Sicherheitsgeräte wie Java Cards und biometrische Lesegeräte.
- Unterstützung für zusätzliche Sicherheitseinstellungen, z. B. Authentifizierungsabfrage unter Verwendung eines optionalen Sicherheitsgeräts, um den Computerschutz aufzuheben.

Setup-Verfahren

Anmelden bei Credential Manager

Je nach Konfiguration haben Sie die folgenden Möglichkeiten, um sich beim Credential Manager anzumelden:

- Symbol „HP ProtectTools Security Manager for Administrators“ im Infobereich.
- Klicken Sie unter Windows Vista® auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators**.
- Klicken Sie unter Windows XP auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager**.

HINWEIS: In Windows Vista müssen Sie HP ProtectTools Security Manager für Administratoren starten, wenn Sie Änderungen vornehmen möchten.

Nachdem Sie sich bei Credential Manager angemeldet haben, können Sie zusätzliche Anmeldeinformationen, z. B. einen Fingerabdruck oder eine Java Card, registrieren. Weitere Informationen finden Sie unter „Registrieren von Anmeldeinformationen“ auf Seite 25.

Bei der nächsten Anmeldung können Sie die Anmeldeart wählen und eine beliebige Kombination der registrierten Anmeldeinformationen verwenden.

Verwenden des Anmeldeassistenten für den Credential Manager

Gehen Sie folgendermaßen vor, um sich mithilfe des Anmeldeassistenten beim Credential Manager anzumelden:

1. Öffnen Sie den Anmeldeassistenten für den Credential Manager mit einer der folgenden Vorgehensweisen:
   - Über den Windows Anmeldebildschirm.
   - Über den Infobereich, indem Sie auf das Symbol **HP ProtectTools Security Manager for Administrators** klicken.
   - Über die Seite „Credential Manager“ in HP ProtectTools Security Manager for Administrators, indem Sie in der oberen rechten Fensterecke auf den Link **Log On** (Anmelden) klicken.
2. Befolgen Sie die Anleitungen auf dem Bildschirm, um sich bei Credential Manager anzumelden.

Registrieren von Anmeldeinformationen

Auf der Seite „Meine Identität“ können Sie Ihre verschiedenen Authentifizierungsmethoden oder Anmeldeinformationen registrieren. Nach der Registrierung können Sie sich mit diesen Methoden beim Credential Manager anmelden.

Registrieren von Fingerabdrücken

Mit einem Fingerabdruck-Lesegerät können Sie sich bei Windows anmelden, indem Sie ihren Fingerabdruck anstatt eines Windows Kennworts zur Authentifizierung verwenden.

Einrichten des Fingerabdruck-Lesegeräts

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Meine Identität** und dann auf **Fingerabdrücke registrieren**.
3. Folgen Sie den Anleitungen auf dem Bildschirm, um Ihre Fingerabdrücke zu registrieren und das Fingerabdruck-Lesegerät einzurichten.
4. Um das Fingerabdruck-Lesegerät für einen anderen Windows Benutzer einzurichten, melden Sie diesen Benutzer bei Windows an, und wiederholen Sie die oben angegebenen Schritte mit dessen Fingerabdruck.

Verwenden des registrierten Fingerabdrucks zur Anmeldung bei Windows.

1. Starten Sie Windows neu, sobald Sie Ihre Fingerabdrücke registriert haben.
2. Streichen Sie beim Windows Willkommensbildschirm mit einem Ihrer registrierten Finger über den Sensor, um sich bei Windows anzumelden.

Registrieren einer Smart Card oder eines Tokens

Eine Smart Card ist eine Kunststoffkarte von der ungefähren Größe einer Visitenkarte mit einem integrierten Mikrochip, auf dem Daten gespeichert werden können. Smart Cards dienen dem Datenschutz und der Authentifizierung einzelner Benutzer. Wenn sich Benutzer mit einer Smart Card beim Netzwerk anmelden, kann dies eine starke Authentifizierungsform sein, wenn beim Anmelden eines Benutzers bei einer Domäne eine verschlüsselte Identifizierung und ein Besitznachweis verwendet werden.

Ein USB-Token ist einfach eine Smart Card in einer anderen Form. Der Chip ist dabei nicht auf einer flachen Kunststoffkarte, sondern in einem Kunststoffkörper integriert, der auch als USB-Schlüssel bezeichnet wird. Der Unterschied zwischen einer Smart Card und einem Token ist die Leseschnittstelle. Für eine Karte ist ein Lesegerät erforderlich, ein USB-Token dagegen kann direkt in einen USB-Anschluss gesteckt werden. Die Grundfunktionalität der Speicherung und Bereitstellung von Zugangsdaten bleibt dabei dieselbe.

Ein USB-Token wird für eine starke Authentifizierung verwendet. Es bietet erhöhte Sicherheit und einen sicheren Zugriff auf Informationen.

HINWEIS: Sie müssen ein Kartenlesegerät konfiguriert haben, um diesen Vorgang auszuführen. Wenn kein Lesegerät installiert ist, können Sie ein virtuelles Token registrieren, wie unter „Erstellen eines virtuellen Token“ auf Seite 27 beschrieben.

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Meine Identität** und dann auf **Smart Card oder Token registrieren**.
3. Klicken Sie im Dialogfeld **Gerätetyp** auf den gewünschten Datenträger und dann auf **Weiter**.
4. Wurde eine Smart Card oder ein USB-Token als Gerätetyp ausgewählt, muss die Karte oder das Token in die entsprechende Leseschnittstelle eingesetzt sein.

   HINWEIS: Ist die Smart Card bzw. das USB-Token nicht eingesetzt, dann ist im Dialogfeld **Select Token** (Token auswählen) die Schaltfläche Weiter deaktiviert.

5. Wählen Sie im Dialogfeld Gerätetyp die Option **Weiter**.

   Das Dialogfeld mit den Token-Eigenschaften wird angezeigt.

6. Geben Sie die Benutzer-PIN ein, wählen Sie **Register smart card or token for authentication** (Smart Card oder Token für Authentifizierung registrieren), und klicken Sie dann auf **Fertig stellen**.

Registrieren weiterer Anmeldeinformationen

1. Klicken Sie in HP ProtectTools Security Manager for Administrators auf **Credential Manager**.
2. Klicken Sie auf **Meine Identität** und dann auf **Anmeldeinformationen registrieren**.

   Der Credential Manager Registrierungsassistent wird geöffnet.

3. Folgen Sie den Anleitungen auf dem Bildschirm.

Allgemeine Aufgaben

Alle Benutzer haben Zugriff auf die Seite „Meine Identität“ im Credential Manager. Auf der Seite „Meine Identität“ können Sie die folgenden Aufgaben ausführen:

- Ändern des Windows Anmeldekennworts
- Ändern einer Token-PIN
- Sperren einer Arbeitsstation

HINWEIS: Diese Option ist nur verfügbar, wenn die standardmäßige Credential Manager-Anmeldeaufforderung aktiviert ist. Siehe „Beispiel 1 – Verwenden der Seite „Erweiterte Einstellungen“, um die Anmeldung bei Windows im Credential Manager zu ermöglichen“ auf Seite 36.

Erstellen eines virtuellen Token

Ein virtuelles Token funktioniert im Wesentlichen wie eine Java Card oder ein USB-Token. Das Token wird auf der Festplatte des Computers oder in der Windows Registrierung gespeichert. Wenn Sie sich mit einem virtuellen Token anmelden, wird zur Vervollständigung der Authentifizierung eine Benutzer-PIN angefordert.

So erstellen Sie ein neues virtuelles Token:

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Meine Identität** und dann auf **Smart Card oder Token registrieren**.
3. Klicken Sie im Dialogfeld Gerätetyp auf **Virtuelles Token**, und klicken Sie dann auf **Weiter**.
4. Geben Sie Namen und Speicherort des Tokens an, und klicken Sie dann auf **Weiter**.

   Ein neues virtuelles Token kann in einer Datei oder in der Registry-Datenbank von Windows gespeichert werden.
5. Geben Sie im Dialogfeld mit den Token-Eigenschaften für das neu erstellte Token die Master-PIN und die Benutzer-PIN ein, wählen Sie **Register smart card or token for authentication** (Smart Card oder Token für Authentifizierung registrieren), und klicken Sie dann auf **Fertig stellen**.

   Das Dialogfeld mit den Token-Eigenschaften wird angezeigt.
6. Geben Sie die Benutzer-PIN ein, wählen Sie **Register smart card or token for authentication** (Smart Card oder Token für Authentifizierung registrieren), und klicken Sie dann auf **Fertig stellen**.

Ändern des Windows Anmeldekennworts

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Meine Identität** und dann auf **Change Windows Password** (Windows Anmeldekennwort ändern).
3. Geben Sie das alte Kennwort in das Feld **Altes Kennwort** ein.

4. Geben Sie Ihr neues Kennwort in die Felder **Neues Kennwort** und **Kennwort bestätigen** ein.
5. Klicken Sie auf **Fertig stellen**.

Ändern einer Token-PIN

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Meine Identität** und dann auf **Token-PIN ändern**.
3. Klicken Sie im Dialogfeld Gerätetyp auf den gewünschten Datenträger, und klicken Sie dann auf **Weiter**.
4. Wählen Sie das Token aus, für das Sie die PIN ändern wollen, und klicken Sie auf **Weiter**.
5. Befolgen Sie die Anleitungen auf dem Bildschirm, um die Änderung der PIN durchzuführen.

HINWEIS: Wenn Sie mehrmals hintereinander die falsche PIN für das Token eingeben, wird das Token gesperrt. Sie können es nicht mehr verwenden, bis es entsperrt wird.

Sperren des Computers (der Arbeitsstation)

Diese Funktion ist verfügbar, wenn Sie sich über Credential Manager bei Windows anmelden. Sichern Sie Ihren Computer während Ihrer Abwesenheit mithilfe der Funktion „Arbeitsstation sperren“. Dadurch verhindern Sie, dass unbefugte Benutzer auf Ihren Computer zugreifen. Nur Sie und die Administratoren auf Ihrem Computer können die Sperre wieder aufheben.

HINWEIS: Diese Option ist nur verfügbar, wenn die standardmäßige Credential Manager-Anmeldeaufforderung aktiviert ist. Siehe „Beispiel 1 – Verwenden der Seite „Erweiterte Einstellungen“, um die Anmeldung bei Windows im Credential Manager zu ermöglichen“ auf Seite 36.

Für noch mehr Sicherheit können Sie die Funktion „Lock Workstation“ (Workstation sperren) konfigurieren, damit zum Entsperren des Computers eine Java Card, ein biometrisches Lesegerät oder ein Token erforderlich ist. Weitere Informationen finden Sie unter „Konfigurieren der Einstellungen des Credential Manager“ auf Seite 35.

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Meine Identität**.
3. Klicken Sie auf **Arbeitsstation sperren**, um den Computer sofort zu sperren.

   Sie müssen ein Windows Kennwort oder den Anmeldeassistenten für den Credential Manager verwenden, um den Schutz für den Computer aufzuheben.

Verwenden der Windows Anmeldung

Sie können sich im Credential Manager entweder auf einem lokalen Computer oder in einer Netzwerkdomäne bei Windows anmelden. Wenn Sie sich zum ersten Mal beim Credential Manager anmelden, fügt das System automatisch Ihr lokales Windows Benutzerkonto als Konto für den Windows Anmeldedienst hinzu.

Anmelden bei Windows mit dem Credential Manager

Sie können sich im Credential Manager bei einem Windows Netzwerk oder einem lokalen Konto anmelden.

1. Wenn Sie Ihren Fingerabdruck für die Anmeldung bei Windows registriert haben, streichen Sie mit Ihrem Finger über den Sensor, um sich anzumelden.
2. Windows XP: Wenn Sie Ihren Fingerabdruck nicht zum Anmelden bei Windows registriert haben, klicken Sie auf das Tastatursymbol links oben im Bildschirm neben dem Fingerabdrucksymbol. Der Credential Manager Anmeldeassistent wird geöffnet.

   Windows Vista: Wenn Sie Ihren Fingerabdruck nicht zum Anmelden bei Windows registriert haben, klicken Sie auf das Symbol **Credential Manager** im Anmeldebildschirm. Der Credential Manager Anmeldeassistent wird geöffnet.
3. Klicken Sie auf den Pfeil neben **Benutzername** und anschließend auf Ihren Namen.
4. Geben Sie in das Feld **Kennwort** Ihr Kennwort ein, und klicken Sie dann auf **Weiter**.
5. Wählen Sie **Mehr**, und klicken Sie dann auf **Wizard Options** (Optionen für Assistent).
   a. Wenn Sie möchten, dass dieser Name als Standardanmeldename für die nächste Anmeldung beim Computer verwendet wird, aktivieren Sie das Kontrollkästchen **Use last user name on next logon** (Letzten Benutzernamen bei nächster Anmeldung verwenden).
   b. Wenn Sie diese Anmeldemethode als Standard einrichten möchten, aktivieren Sie die Option **Use this policy next time you log on** (Diese Methode bei der nächsten Anmeldung verwenden).
6. Folgen Sie den Anleitungen auf dem Bildschirm. Wenn die Authentifizierungsinformationen korrekt sind, werden Sie bei Ihrem Windows Konto und beim Credential Manager angemeldet.

Verwenden von Single Sign On (Einmaliges Anmelden)

Der Credential Manager besitzt eine Funktion zur einmaligen Anmeldung (Single Sign On, SSO), die Benutzernamen und Kennwörter für mehrere Internet- und Windows Programme speichert und automatisch die Anmeldeinformationen einfügt, wenn Sie auf ein registriertes Programm zugreifen.

HINWEIS: Sicherheit und Datenschutz sind wichtige Funktionen von Single Sign On. Sämtliche Anmeldeinformationen werden verschlüsselt und sind erst nach erfolgreicher Anmeldung beim Credential Manager verfügbar.

HINWEIS: Sie können auch die einmalige Anmeldung (Single Sign On) aktivieren, um Ihre Authentifizierungsinformationen mit einer Java Card, einem Fingerabdruck-Lesegerät oder einem Token zu überprüfen, bevor Sie sich bei einer sicheren Website oder einem Programm anmelden. Dies ist insbesondere dann nützlich, wenn Sie sich bei Programmen oder Websites anmelden, die persönliche Informationen, wie z. B. Kontonummern, enthalten. Weitere Informationen finden Sie unter „Konfigurieren der Einstellungen des Credential Manager“ auf Seite 35.

Registrieren einer neuen Anwendung

Der Credential Manager fordert Sie auf, jede Anwendung zu registrieren, die Sie aufrufen, während Sie beim Credential Manager angemeldet sind. Sie können Anwendungen auch manuell registrieren.

Verwenden der automatischen Registrierung

1. Öffnen Sie eine Anwendung, für die Sie sich anmelden müssen.
2. Klicken Sie im Kennwortdialogfeld des Programms oder der Website auf das Credential Manager SSO-Symbol.
3. Geben Sie Ihr Kennwort für die Anwendung oder Website ein, und klicken Sie dann auf **OK**. Das Dialogfeld **Credential Manager Single Sign On** (Einmaliges Anmelden bei Credential Manager) wird geöffnet.
4. Klicken Sie auf **More** (Mehr), und wählen Sie eine der folgenden Optionen:
   - Verwenden Sie SSO nicht für diese Website oder Anwendung.
   - Fordern Sie zur Auswahl eines Kontos für diese Anwendung auf.
   - Geben Sie die Anmeldeinformationen ein, aber senden Sie sie nicht ab.
   - Authentifizieren Sie den Benutzer, bevor Sie die Anmeldeinformationen absenden.
   - Zeigen Sie die SSO-Verknüpfung für diese Anwendung an.
5. Klicken Sie auf **Ja**, um die Registrierung durchzuführen.

Verwenden der manuellen Registrierung (Drag & Drop)

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager** und anschließend auf **Services and Applications** (Dienste und Anwendungen).
2. Klicken Sie auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).

   Das Dialogfeld Credential Manager Single Sign-On wird geöffnet.
3. Um eine bereits registrierte Website oder Anwendung zu ändern oder zu löschen, wählen Sie den gewünschten Eintrag in der Liste.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Verwalten von Anwendungen und Anmeldeinformationen

Ändern der Anwendungseigenschaften

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager** und anschließend auf **Services and Applications** (Dienste und Anwendungen).
2. Klicken Sie auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).

   Das Dialogfeld Credential Manager Single Sign-On wird geöffnet.
3. Klicken Sie auf den Eintrag, den Sie ändern möchten, und anschließend auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Allgemein**, um den Namen und die Beschreibung der Anwendung zu ändern. Nehmen Sie die gewünschten Änderungen vor, indem Sie die Optionen neben den entsprechenden Einstellungen aktivieren bzw. deaktivieren.

5. Klicken Sie auf die Registerkarte **Skript**, um das SSO-Anwendungsskript anzuzeigen und zu bearbeiten.

6. Klicken Sie auf **OK**.

Entfernen einer Anwendung aus Single Sign On

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager** und anschließend auf **Services and Applications** (Dienste und Anwendungen).

2. Klicken Sie auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).

   Das Dialogfeld **Credential Manager Single Sign-On** wird geöffnet.

3. Klicken Sie auf die Anwendung, die Sie entfernen möchten, und anschließend auf **Entfernen**.

4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

5. Klicken Sie auf **OK**.

Exportieren einer Anwendung

Sie können Anwendungen exportieren, um eine Sicherungskopie des SSO-Anwendungsskripts zu erstellen. Diese Datei kann dann zur Wiederherstellung der SSO-Daten verwendet werden. Es handelt sich hierbei um eine Ergänzung der Identitätssicherungsdatei, die nur die Anmeldeinformationen enthält.

So exportieren Sie eine Anwendung:

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager** und anschließend auf **Services and Applications** (Dienste und Anwendungen).

2. Klicken Sie auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).

   Das Dialogfeld Credential Manager Single Sign-On wird geöffnet.

3. Klicken Sie die Anwendung, die Sie exportieren möchten, und anschließend auf **Mehr**.

4. Befolgen Sie die Anleitungen auf dem Bildschirm, um den Export durchzuführen.

5. Klicken Sie auf **OK**.

Importieren einer Anwendung

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager** und anschließend auf **Services and Applications** (Dienste und Anwendungen).

2. Klicken Sie auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).

   Das Dialogfeld Credential Manager Single Sign-On wird geöffnet.

3. Klicken Sie auf die Anwendung, die Sie importieren möchten, und anschließend auf **Mehr**.

4. Befolgen Sie die Anleitungen auf dem Bildschirm, um den Import durchzuführen.
5. Klicken Sie auf **OK**.

Ändern der Anmeldeinformationen

1. Klicken Sie in HP ProtectTools Security Manager for Administrators auf **Credential Manager** und anschließend auf **Services and Applications** (Dienste und Anwendungen).
2. Klicken Sie auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).

   Das Dialogfeld Credential Manager Single Sign-On wird geöffnet.
3. Klicken Sie auf den Eintrag, den Sie ändern möchten, und anschließend auf **More** (Mehr).
4. Es stehen unter anderem folgende Optionen zur Auswahl:
   - Anwendungen
     - Neue hinzufügen
     - Entfernen
     - Eigenschaften
     - Import Script (Skript importieren)
     - Export Script (Skript exportieren)
   - Anmeldeinformationen
     - Neu erstellen
   - View Password (Kennwort anzeigen)

   HINWEIS: Sie müssen Ihre Identität authentifizieren, bevor Sie das Kennwort anzeigen können.
5. Folgen Sie den Anleitungen auf dem Bildschirm.
6. Klicken Sie auf **OK**.

Verwenden des Anwendungsschutzes

Mit dieser Funktion können Sie den Zugriff auf Anwendungen konfigurieren. Sie können den Zugriff auf der Grundlage folgender Kriterien begrenzen:

- Benutzerkategorie
- Verwendungszeitpunkt
- Benutzerinaktivität

Einschränken des Zugriffs auf eine Anwendung

1. Klicken Sie unter HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager** und anschließend auf **Services and Applications** (Dienste und Anwendungen).
2. Klicken Sie auf **Application Protection** (Anwendungsschutz) und anschließend auf **Manage Protected Applications** (Geschützte Anwendungen verwalten).
3. Wählen Sie eine Benutzerkategorie, deren Zugriff Sie verwalten möchten.

HINWEIS: Wenn die Kategorie nicht „Jeder“ lautet, müssen Sie unter Umständen die Option **Override default settings** (Standardeinstellungen überschreiben) auswählen, um die Einstellungen für die Kategorie „Jeder“ zu überschreiben.

4. Klicken Sie auf **Hinzufügen**.

   Der Assistent zum Hinzufügen eines Programms wird geöffnet.
5. Folgen Sie den Anleitungen auf dem Bildschirm.

Entfernen des Schutzes für eine Anwendung

So entfernen Sie Einschränkungen von einer Anwendung:

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Dienste und Anwendungen**.
3. Klicken Sie auf **Application Protection** (Anwendungsschutz) und anschließend auf **Manage Protected Applications** (Geschützte Anwendungen verwalten).
4. Wählen Sie eine Benutzerkategorie, deren Zugriff Sie verwalten möchten.

HINWEIS: Wenn die Kategorie nicht „Jeder“ lautet, müssen Sie unter Umständen auf die Option **Override default settings** (Standardeinstellungen überschreiben) klicken, um die Einstellungen für die Kategorie „Jeder“ zu überschreiben.

5. Klicken Sie auf den Eintrag, den Sie entfernen möchten, und anschließend auf **Entfernen**.
6. Klicken Sie auf **OK**.

Ändern der Einschränkungseinstellungen für eine geschützte Anwendung

1. Klicken Sie auf **Application Protection** (Anwendungsschutz) und anschließend auf **Manage Protected Applications** (Geschützte Anwendungen verwalten).
2. Wählen Sie eine Benutzerkategorie, deren Zugriff Sie verwalten möchten.

HINWEIS: Wenn die Kategorie nicht „Jeder“ lautet, müssen Sie unter Umständen auf die Option **Override default settings** (Standardeinstellungen überschreiben) klicken, um die Einstellungen für die Kategorie „Jeder“ zu überschreiben.

3. Klicken Sie auf die Anwendung, die Sie ändern möchten, und klicken Sie anschließend auf **Eigenschaften**. Das Dialogfeld **Eigenschaften** für diese Anwendung wird geöffnet.

4. Klicken Sie auf die Registerkarte **Allgemein**. Wählen Sie eine der folgenden Einstellungen:

   - Disabled (Cannot be used) (Deaktiviert (kann nicht verwendet werden))
   - Enabled (Can be used without restrictions) (Aktiviert (kann ohne Einschränkung verwendet werden))
   - Restricted (Usage depends on settings) (Eingeschränkt (Verwendung hängt von Einstellungen ab))

5. Wenn Sie „Eingeschränkt“ wählen, sind die folgenden Einstellungen verfügbar:

   a. Wenn Sie die Nutzung nach Uhrzeit, Tag oder Datum einschränken möchten, klicken Sie auf die Registerkarte **Zeitplan**, und konfigurieren Sie die Einstellungen.

   b. Wenn Sie die Nutzung auf Grundlage der Inaktivität einschränken möchten, klicken Sie auf **Erweitert**, und wählen Sie die Zeitspanne für die Inaktivität.

6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für die Anwendung zu schließen.

7. Klicken Sie auf **OK**.

Erweiterte Aufgaben (nur für Administratoren)

Die Seiten „Multifactor Authentication“ (Mehrstufige Authentifizierung) und „Einstellungen“ im Credential Manager sind nur für Benutzer mit Administratorrechten verfügbar. Auf diesen Seiten können Sie folgende Aufgaben durchführen:

- Konfigurieren der Anmeldeeigenschaften
- Konfigurieren der Einstellungen des Credential Manager

Konfigurieren der Anmeldeeigenschaften

Auf der Seite „Multifactor Authentication“ (Mehrstufige Authentifizierung) können Sie eine Liste der verfügbaren Authentifizierungsmethoden anzeigen und die Einstellungen ändern.

So konfigurieren Sie die Anmeldeinformationen:

1. Klicken Sie unter HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Multifactor Authentication** (Mehrere Authentifizierungsmethoden).
3. Klicken Sie auf die Registerkarte **Anmeldeinformationen**.
4. Klicken Sie auf die Anmeldeart, die Sie ändern möchten. Sie haben dabei die folgenden Optionen:
   - Klicken Sie auf **Registrieren**, um die Anmeldeinformationen zu registrieren, und befolgen Sie anschließend die Anleitungen auf dem Bildschirm.
   - Klicken Sie auf **Löschen** und anschließend im Bestätigungsdialogfeld auf **Ja**, um die Anmeldeinformationen zu löschen.
   - Klicken Sie auf **Eigenschaften**, um die Anmeldeeigenschaften zu ändern, und befolgen Sie anschließend die Anleitungen auf dem Bildschirm.
5. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Konfigurieren der Einstellungen des Credential Manager

Auf der Seite „Einstellungen“ können Sie über die nachfolgenden Registerkarten verschiedene Einstellungen anzeigen und ändern.

- Allgemein – Hier können Sie die Einstellungen für die Grundkonfiguration ändern.
- Single Sign On – Hier können Sie die Einstellungen von Single Sign On für den aktuellen Benutzer ändern, z. B. Erkennung der Anmeldebildschirme, automatische Anmeldung bei registrierten Anmeldedialogfeldern und Anzeige von Kennwörtern.
- Dienste und Anwendungen – Hier können Sie die verfügbaren Dienste anzeigen und deren Einstellungen ändern.
- Sicherheit – Hier können Sie die Software für das Fingerabdruck-Lesegerät auswählen und seine Sicherheitsstufe anpassen.
- Smart Cards and Tokens (Smart Cards und Tokens) – Hier können Sie die Eigenschaften aller verfügbaren Java Cards und Tokens anzeigen und ändern.

So ändern Sie die Einstellungen des Credential Manager:

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Einstellungen**.
3. Klicken Sie auf die Registerkarte für die zu ändernden Einstellungen.
4. Befolgen Sie die Anleitungen auf dem Bildschirm, um die Einstellungen zu ändern.
5. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Beispiel 1 – Verwenden der Seite „Erweiterte Einstellungen“, um die Anmeldung bei Windows im Credential Manager zu ermöglichen

1. Klicken Sie in HP ProtectTools Security Manager for Administrators im linken Fenster auf **Credential Manager**.
2. Klicken Sie auf **Einstellungen**.
3. Klicken Sie auf die Registerkarte **Allgemein**.
4. Aktivieren Sie unter **Select the way users log on to Windows** (Methode für die Windows Anmeldung auswählen) das Kontrollkästchen **Use Credential Manager to log on to Windows** (Credential Manager für die Windows Anmeldung verwenden)
5. Klicken Sie auf **Übernehmen** und dann auf **OK**.
6. Starten Sie den Computer neu.

HINWEIS: Wenn Sie das Kontrollkästchen **Use Credential Manager to log on to Windows** (Credential Manager für die Windows Anmeldung verwenden) aktivieren, können Sie Ihren Computer sperren. Siehe „Sperren des Computers (der Arbeitsstation)“ auf Seite 28.

HINWEIS: Die oben beschriebene Vorgehensweise kann sich für Windows XP leicht unterscheiden.

Beispiel 2 – Verwenden der Seite „Erweiterte Einstellungen“, um vor der einmaligen Anmeldung eine Benutzerüberprüfung durchzuführen

1. Klicken Sie in HP ProtectTools Security Manager for Administrators auf **Credential Manager** und anschließend auf **Einstellungen**.
2. Klicken Sie auf die Registerkarte **Single Sign-On**.
3. Aktivieren Sie unter **When registered logon dialog or Web page is visited** (Bei Aufruf des registrierten Anmeldedialogfelds oder der registrierten Webseite) die Option **Validate user before submitting credentials** (Benutzer vor Senden der Anmeldeinformationen authentifizieren).
4. Klicken Sie auf **Übernehmen** und dann auf **OK**.
5. Starten Sie den Computer neu.

4 Drive Encryption für HP ProtectTools

△ **ACHTUNG:** Wenn Sie das Modul „Drive Encryption“ deinstallieren oder eine Sicherungs- und Wiederherstellungslösung verwenden, müssen Sie zunächst alle verschlüsselten Laufwerke entschlüsseln. Wenn Sie dies nicht tun, haben Sie nur Zugriff auf die verschlüsselten Laufwerke, wenn Sie sich beim HP Drive Encryption-Wiederherstellungsdienst registriert haben. 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 unter Windows Vista auf **Start**, **Alle Programme**, **HP ProtectTools Security Manager for Administrators** bzw. unter Windows XP auf **HP ProtectTools Security Manager**.
2. Klicken Sie auf **Drive Encryption**.

Allgemeine Aufgaben

Aktivieren von Drive Encryption

Verwenden Sie den Installationsassistenten für HP ProtectTools Security Manager for Administrators, um „Drive Encryption“ zu aktivieren.

Deaktivieren von Drive Encryption

Verwenden Sie den Installationsassistenten für HP ProtectTools Security Manager, 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) unter HP ProtectTools Security Manager for Administrators aktiviert hat, können Sie sich nach dem Einschalten des Computers direkt beim Computer anmelden, ohne dies im Drive Encryption-Anmeldebildschirm tun zu müssen.

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

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

Erweiterte Aufgaben

Verwalten von Drive Encryption (Administrator-Aufgabe)

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

Aktivieren eines TPM-geschützten Kennworts

Verwenden Sie Embedded Security for HP ProtectTools, um das TPM-geschützte Kennwort zu aktivieren. Nach der Aktivierung sind für die Anmeldung beim Drive Encryption-Anmeldebildschirm der Windows Benutzername und das Windows Kennwort erforderlich.

HINWEIS: Da das Kennwort durch einen TPM-Chip für integrierte Sicherheit geschützt ist, kann bei einem Wechsel der Festplatte auf einen anderen Computer erst dann auf die Daten zugegriffen werden, wenn die TPM-Einstellungen auf diesen Computer migriert werden.

1. Verwenden Sie Embedded Security für HP ProtectTools, um das TPM-geschützte Kennwort zu aktivieren.
2. Öffnen Sie Drive Encryption, und klicken Sie auf **Verschlüsselungsverwaltung**.
3. Aktivieren Sie das Kontrollkästchen **TPM-geschütztes Kennwort**.

Verschlüsseln oder Entschlüsseln einzelner Laufwerke

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

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

Sicherung und Wiederherstellung (Administrator-Aufgabe)

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

Erstellen von Sicherungsschlüsseln

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

1. Öffnen Sie Drive Encryption, und klicken Sie dann auf **Wiederherstellung**.
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**.

Registrieren für Online-Wiederherstellung

Der Online-Dienst zur Schlüsselwiederherstellung von Drive Encryption speichert eine Kopie des Sicherungs- bzw. Chiffrierschlüssels, mit dessen Hilfe Sie auf Ihren Computer zugreifen können, selbst wenn Sie das Kennwort vergessen und keinen Zugriff auf Ihren lokal abgelegten Sicherungsschlüssel haben.

HINWEIS: Sie müssen über eine Internetverbindung und eine gültige E-Mail-Adresse verfügen, damit Sie sich registrieren und Ihr Kennwort über diesen Service wiederherstellen können.

1. Öffnen Sie Drive Encryption, und klicken Sie dann auf **Wiederherstellung**.
2. Klicken Sie auf **Registrieren**.
3. Klicken Sie auf eine der folgenden Optionen:
   - Ich möchte ein neues Recovery-Konto für diesen PC erstellen. Wenn Sie diese Option wählen, geben Sie Ihre E-Mail-Adresse und andere persönliche Daten ein, und klicken Sie danach auf **Weiter**.
   - Ich möchte diesen PC meinem vorhandenen Web Recovery-Konto hinzufügen.
4. Erstellen und bestätigen Sie Ihr Kennwort, wählen Sie die gewünschten Sicherheitsfragen aus, geben Sie die Antworten ein, und klicken Sie danach auf **Weiter**.

   HINWEIS: Der Kontoaktivierungscode wird an die von Ihnen angegebene E-Mail-Adresse gesendet.
5. Geben Sie den Aktivierungscode ein, und klicken Sie auf **Weiter**.
6. Geben Sie die Seriennummer des Computers ein, und klicken Sie auf **Weiter**.

   HINWEIS: Um die Seriennummer Ihres Computers anzuzeigen, klicken Sie auf **Start** und dann auf **Hilfe und Support**.
7. Wenn Sie über keinen Abonnementcoupon verfügen, klicken Sie auf den Link **Zum Kaufen von Coupons hier klicken**.

   Über diesen Link gelangen Sie zur SafeBoot Recovery Service-Website. Beenden Sie den Assistenten nicht, während Sie auf dieser Site arbeiten.

8. Klicken Sie auf **Purchase Coupon Codes** (Couponcodes kaufen).
9. Wählen Sie Ihr Land und den Computertyp aus, und klicken Sie auf **Start**.
10. Klicken Sie neben der gewünschten Abonnementoption (ein oder drei Jahre) auf **Buy** (Kaufen).
11. Klicken Sie auf **Checkout** (Auschecken).
12. Lesen Sie die Nutzungsbestimmungen, und klicken Sie auf **Accept** (Akzeptieren).
13. Geben Sie Ihre Rechnungsdaten ein, und klicken Sie auf **Weiter**.
14. Geben Sie Ihre Kreditkarteninformationen ein, und klicken Sie auf **Make Payment** (Bezahlen).
15. Notieren Sie Ihren Couponcode, und kehren Sie zur Assistentenseite „Kontoaktivierung“ zurück.
16. Geben Sie Ihren Kontoaktivierungscode ein, und klicken Sie auf **Weiter**.
17. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

Verwalten eines vorhandenen Online-Wiederherstellungskontos

Nachdem Sie ein Online-Wiederherstellungskonto erstellt haben, können Sie auf der SafeBoot Recovery Service-Website folgende Aufgaben durchführen: Zugang zu Ihrem Computer wiederherstellen, falls Sie Ihr Kennwort vergessen haben, Ihre persönlichen Einstellungen ändern, das für Ihr Online-Wiederherstellungskonto verwendete Kennwort zurücksetzen und Ihr Konto anzeigen bzw. verlängern.

1. Öffnen Sie Drive Encryption, und klicken Sie dann auf **Wiederherstellung**.
2. Klicken Sie auf **Manage** (Verwalten).
3. Klicken Sie auf der SafeBoot Recovery Service-Website auf **Recovery Service Account** (Recovery Service-Konto) oder **Recovery Process** (Wiederherstellungsprozess).
4. Geben Sie auf der Anmeldeseite des Wiederherstellungsdienstes Ihre E-Mail-Adresse, Ihr Kennwort sowie die in dem Feld angegebene Buchstaben- und Zahlenfolge ein.
5. Klicken Sie auf **Logon** (Anmelden).
6. Klicken Sie auf **Profile** (Profil), wenn Sie Ihre persönlichen Daten, zum Beispiel Ihre Telefonnummer oder Rechnungsadresse, ändern möchten.

   – ODER –

   Klicken Sie auf **Reset Password** (Kennwort zurücksetzen), wenn Sie Ihr Kennwort zurücksetzen oder ändern möchten.

   – ODER –

   Klicken Sie auf **My Subscriptions** (Meine Abonnements), um Informationen zu Ihren aktuellen Abonnements anzuzeigen.

HINWEIS: Auf der Seite „My Subscriptions“ (Meine Abonnements) können Sie Ihr Abonnement auch verlängern. Klicken Sie dazu auf **Renew Subscription** (Abonnement verlängern).

Wiederherstellen des Systems

Lokale Wiederherstellung des Systems

1. Schalten Sie den Computer ein.
2. Setzen Sie den Wechseldatenträger ein, auf dem Ihr Sicherungsschlüssel gespeichert ist.
3. Klicken Sie im Anmeldedialogfeld für Drive Encryption for HP ProtectTools auf **Abbrechen**.
4. Klicken Sie in der unteren rechten Bildschirmecke auf **Optionen** und danach auf **Wiederherstellung**.
5. Klicken Sie auf **Lokale Wiederherstellung** und danach auf **Weiter**.
6. Wählen Sie die Datei mit Ihrem Sicherungsschlüssel aus, oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen, und klicken Sie danach auf **Weiter**.
7. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Damit ist die Wiederherstellung abgeschlossen und der Computer wird gestartet.

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

Online-Wiederherstellung des Systems

HINWEIS: In diesem Abschnitt wird die Online-Wiederherstellung beschrieben. Diese können Sie nur durchführen, wenn Sie Zugang zu einem anderen Computer mit Verbindung zum Internet haben. Steht Ihnen ein solcher Computer nicht zur Verfügung, wenden Sie sich an den technischen Support von HP.

1. Schalten Sie den Computer ein.
2. Klicken Sie im Anmeldedialogfeld für Drive Encryption for HP ProtectTools auf **Abbrechen**.
3. Klicken Sie in der unteren rechten Bildschirmecke auf **Optionen** und danach auf **Wiederherstellung**.
4. Klicken Sie auf **Web-Wiederherstellung** und danach auf **Weiter**.
5. Notieren Sie den Client-Code, und klicken Sie auf **Weiter**.
6. Rufen Sie die SafeBoot Recovery Service-Website unter http://www.safeboot-hp.com auf einem anderen Computer auf, der über eine Verbindung zum Internet verfügt.
7. Klicken Sie auf **Recovery Process** (Wiederherstellungsprozess).
8. Geben Sie auf der Anmeldeseite des Wiederherstellungsdienstes Ihre E-Mail-Adresse, Ihr Kennwort sowie die in dem Feld angegebene Buchstaben- und Zahlenfolge ein.
9. Klicken Sie auf **Logon** (Anmelden).
10. Klicken Sie auf **Recovery Process** (Wiederherstellungsprozess).
11. Geben Sie den Client-Code des Computers, den Sie wiederherstellen möchten, sowie die in dem Feld angegebene Buchstaben- und Zahlenfolge ein.
12. Klicken Sie auf **Submit** (Senden).
13. Notieren Sie den Antwortschlüssel Zeile für Zeile.

14. Geben Sie auf dem Computer, den Sie wiederherstellen, Zeile 1 des zuvor notierten Antwortschlüssels ein, und drücken Sie die **Eingabetaste**.
15. Geben Sie Zeile 2 des Antwortschlüssels ein, und drücken Sie die **Eingabetaste**.
16. Geben Sie Zeile 3 des Antwortschlüssels ein, und drücken Sie die **Eingabetaste**.
17. Geben Sie Zeile 4 des Antwortschlüssels ein, und drücken Sie die **Eingabetaste**.

    HINWEIS: Zeile 4 des Antwortschlüssels ist kürzer als die ersten drei Zeilen.

18. Klicken Sie auf **Fertig stellen**.

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

5 Privacy Manager für HP ProtectTools

Privacy Manager ist ein Tool zum Generieren von Echtheitszertifikaten. Dieses Tool überprüft die Quelle, Integrität und Sicherheit der Verbindung, wenn Microsoft Mail, Microsoft Office-Dokumente und Live Messenger verwendet werden.

Privacy Manager nutzt die von HP ProtectTools Security Manager for Administrators bereitgestellte Sicherheitsinfrastruktur, die folgende Sicherheits-Anmeldemethoden umfasst:

- Fingerabdruck-Authentifizierung
- Windows® Kennwort
- HP ProtectTools Java™ Card
- Virtuelles Token
- Allgemeiner Benutzerschlüssel für Embedded Security for HP ProtectTools

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

Aufrufen von Privacy Manager

So öffnen Sie Privacy Manager:

1. Klicken Sie unter Windows Vista auf **Start**, **Alle Programme**, **HP ProtectTools Security Manager for Administrators** bzw. unter Windows XP auf **HP ProtectTools Security Manager**.
2. Klicken Sie auf **Privacy Manager: Sign and Chat**.

– ODER –

Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich außen rechts in der Taskleiste. Wählen Sie **Privacy Manager: Sign and Chat**, und klicken Sie auf **Configuration** (Konfiguration).

– ODER –

Klicken Sie unter Microsoft Outlook in der Symbolleiste einer E-Mail-Nachricht neben **Send Securely** (Sicheres Senden) auf den Pfeil nach unten und anschließend auf **Certificate Manager** oder **Trusted Contact Manager**.

– ODER –

Klicken Sie in der Symbolleiste eines Microsoft Office-Dokuments neben **Sign and Encrypt** (Signieren und verschlüsseln) auf den Pfeil nach unten und anschließend auf **Certificate Manager** oder **Trusted Contact Manager**.

Setup-Verfahren

Verwalten von Privacy Manager-Zertifikaten

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

Anfordern und Installieren eines Privacy Manager-Zertifikats

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

Anfordern eines Privacy Manager-Zertifikats

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Certificate Manager**.
2. Klicken Sie auf **Request a Privacy Manager Certificate** (Ein Privacy Manager-Zertifikat anfordern).
3. Lesen Sie den Text auf der Begrüßungsseite, und klicken Sie dann auf **Weiter**.
4. Lesen Sie die Lizenzvereinbarung auf der Seite „License Agreement“ (Lizenzvereinbarung).
5. Aktivieren Sie das Kontrollkästchen neben **Check here to accept the terms of this license agreement** (Bedingungen dieser Lizenzvereinbarung akzeptieren), und klicken Sie anschließend auf **Weiter**.
6. Geben Sie auf der Seite „Your Certificate Details“ (Ihre Zertifikatdetails) die angeforderten Informationen ein, und klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite „Certificate Request Accepted“ (Zertifikatanforderung akzeptiert) auf **Fertig stellen**.

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

Installieren eines Privacy Manager-Zertifikats

1. Wenn Sie die E-Mail mit Ihrem Privacy Manager-Zertifikat erhalten haben, öffnen Sie sie, und klicken Sie unten rechts in der Nachricht auf die Schaltfläche **Setup** (Einrichten).
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
3. Klicken Sie auf der Seite „Certificate Installed“ (Zertifikat installiert) auf **Weiter**.
4. Geben Sie auf der Seite „Certificate Backup“ (Zertifikat-Backup) einen Speicherort und einen Namen für die Backup-Datei ein, oder klicken Sie auf **Durchsuchen**, um nach einem Speicherort zu suchen.

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

5. Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.
6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
7. Wenn Sie den Trusted Contact-Einladungsprozess starten möchten, befolgen Sie die Anleitungen auf dem Bildschirm.

   – ODER –

   Wenn Sie auf Abbrechen klicken, lesen Sie im Abschnitt „Verwalten von Trusted Contacts“ nach, wie Sie zu einem späteren Zeitpunkt einen Trusted Contact hinzufügen können.

Anzeigen von Details eines Privacy Manager-Zertifikats

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

Erneuern eines Privacy Manager-Zertifikats

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

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Certificate Manager**.
2. Klicken Sie auf ein **Privacy Manager-Zertifikat**.
3. Klicken Sie auf **Renew certificate** (Zertifikat erneuern).
4. Befolgen Sie die Anleitungen auf dem Bildschirm, um ein neues Privacy Manager-Zertifikat zu erwerben.

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

Festlegen eines Privacy Manager-Standardzertifikats

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

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

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Certificate Manager**.
2. Klicken Sie auf das Privacy Manager-Zertifikat, das als Standardzertifikat verwendet werden soll, und klicken Sie anschließend auf **Set default** (Als Standard festlegen).
3. Klicken Sie auf **OK**.

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

Löschen eines Privacy Manager-Zertifikats

Wenn Sie ein Privacy Manager-Zertifikat löschen, können Sie die Dateien nicht mehr öffnen oder die Daten nicht mehr anzeigen, die Sie mit diesem Zertifikat verschlüsselt haben. Wenn Sie versehentlich ein Privacy Manager-Zertifikat gelöscht haben, können Sie es mithilfe der Backup-Datei wiederherstellen, die Sie während der Installation des Zertifikats erstellt haben.

So löschen Sie ein Privacy Manager-Zertifikat:

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

Wiederherstellen eines Privacy Manager-Zertifikats

Wenn Sie versehentlich ein Privacy Manager-Zertifikat gelöscht haben, können Sie es mithilfe der Backup-Datei wiederherstellen, die Sie während der Installation oder beim Exportieren des Zertifikats erstellt haben:

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Migration**.
2. Klicken Sie auf **Import migration file** (Migrationsdatei importieren).
3. Klicken Sie auf der Seite „Migration File“ (Migrationsdatei) auf **Durchsuchen**, um nach der Datei mit der Erweiterung. dppsm zu suchen, die Sie während der Installation oder beim Exportieren des Privacy Manager-Zertifikats erstellt haben, und klicken Sie auf **Weiter**.
4. Klicken Sie auf der Seite „Migration File Import“ (Migrationsdatei-Import) auf **Beenden**.
5. Klicken Sie auf **Schließen** und dann auf **Übernehmen**.

HINWEIS: Weitere Informationen finden Sie in den Abschnitten „Installieren eines Privacy Manager-Zertifikats“ und „Exportieren von Privacy Manager-Zertifikaten und Trusted Contacts“.

Widerrufen Ihres Privacy Manager-Zertifikats

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

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

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Certificate Manager**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf das Privacy Manager-Zertifikat, das widerrufen werden soll, und anschließend auf **Revoke** (Widerrufen).
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.
5. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
6. Folgen Sie den Anleitungen auf dem Bildschirm.

Verwalten von Trusted Contacts

Trusted Contacts sind Benutzer, mit denen Sie Privacy Manager-Zertifikate ausgetauscht haben, sodass Sie sicher mit ihnen kommunizieren können.

Hinzufügen von Trusted Contacts

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

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

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

Hinzufügen eines Trusted Contact

1. Öffnen Sie Privacy Manager, klicken Sie auf **Trusted Contacts Manager** und anschließend auf **Invite Contacts** (Kontakte einladen).

   – ODER –

   Klicken Sie in Microsoft Outlook neben **Send Securely** (Sicheres Senden) in der Symbolleiste auf den Pfeil nach unten und anschließend auf **Invite Contacts** (Kontakte einladen).

2. Nach dem Öffnen des Dialogfelds **Select Certificate** (Zertifikat auswählen) klicken Sie auf das Privacy Manager-Zertifikat, das Sie verwenden möchten. Klicken Sie abschließend auf **OK**.
3. Lesen Sie den Text im Dialogfeld **Trusted Contact Invitation** (Trusted Contact-Einladung), und klicken Sie dann auf **OK**.

Es wird automatisch eine E-Mail erzeugt.

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

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

6. Klicken Sie auf **Senden**.

HINWEIS: Wenn Sie kein Privacy Manager-Zertifikat erhalten haben, informiert Sie eine Meldung darüber, dass Sie im Besitz eines Privacy Manager-Zertifikats sein müssen, um eine Trusted Contact-Einladung senden zu können. Klicken Sie auf **OK**, um den Assistenten zum Anfordern eines Zertifikats aufzurufen.

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

8. Wenn Sie eine E-Mail-Antwort von einem Empfänger erhalten, der die Einladung, ein Trusted Contact zu werden, annimmt, klicken Sie unten rechts in der E-Mail auf **Accept** (Akzeptieren).

   Ein Dialogfeld wird geöffnet, das bestätigt, dass der Empfänger erfolgreich zu Ihrer Trusted Contacts-Liste hinzugefügt wurde.

9. Klicken Sie auf **OK**.

Hinzufügen von Trusted Contacts unter Verwendung des Microsoft Outlook Adressbuchs

1. Öffnen Sie Privacy Manager, klicken Sie auf **Trusted Contacts Manager**, und anschließend auf **Invite Contacts** (Kontakte einladen).

   – ODER –

   Klicken Sie in Microsoft Outlook neben **Send Securely** (Sicheres Senden) in der Symbolleiste auf den Pfeil nach unten und anschließend auf **Invite All My Outlook Contacts** (Alle meine Outlook Kontakte einladen).

2. Wählen Sie nach dem Öffnen der Seite „Trusted Contact Invitation“ (Trusted Contact-Einladung) die E-Mail-Adressen der Empfänger aus, die Sie als Trusted Contacts hinzufügen möchten, und klicken Sie anschließend auf **Weiter**.

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

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

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

5. Klicken Sie auf **Senden**.

HINWEIS: Wenn Sie kein Privacy Manager-Zertifikat erhalten haben, informiert Sie eine Meldung darüber, dass Sie im Besitz eines Privacy Manager-Zertifikats sein müssen, um eine Trusted Contact-Einladung senden zu können. Klicken Sie auf **OK**, um den Assistenten zum Anfordern eines Zertifikats aufzurufen.

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

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

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

   Ein Dialogfeld wird geöffnet, das bestätigt, dass der Empfänger erfolgreich zu Ihrer Trusted Contacts-Liste hinzugefügt wurde.

8. Klicken Sie auf **OK**.

Anzeigen von Details zu Trusted Contacts

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

Löschen eines Trusted Contact

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Trusted Contacts Manager**.
2. Klicken Sie auf den Trusted Contact, der gelöscht werden soll.
3. Klicken Sie auf **Delete contact** (Kontakt löschen).
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Prüfen des Widerruf-Status für einen Trusted Contact

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Trusted Contacts Manager**.
2. Klicken Sie auf einen Trusted Contact.
3. Klicken Sie auf die Schaltfläche **Erweitert**.

   Das Dialogfeld **Advanced Trusted Contact Management** (Erweiterte Trusted Contact-Verwaltung) wird geöffnet.

4. Klicken Sie auf **Check Revocation** (Auf Widerruf prüfen).
5. Klicken Sie auf **Schließen**.

Allgemeine Aufgaben

Verwenden von Privacy Manager in Microsoft Office

Nach der Installation Ihres Privacy Manager-Zertifikats wird die Schaltfläche „Sign and Encrypt“ (Signieren und verschlüsseln) rechts in der Symbolleiste aller Microsoft Word, Microsoft Excel und Microsoft PowerPoint Dokumente angezeigt.

Konfigurieren von Privacy Manager in einem Microsoft Office Dokument

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

– ODER –

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

   – ODER –

   Klicken Sie in der Symbolleiste eines Microsoft Office-Dokuments neben **Sign and Encrypt** (Signieren und verschlüsseln) auf den Pfeil nach unten und anschließend auf **Einstellungen**.

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

Signieren eines Microsoft Office Dokuments

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

Wenn Sie das Dokument später bearbeiten möchten, müssen Sie wie folgt vorgehen:

1. Klicken Sie auf die Schaltfläche **Office** links oben auf dem Bildschirm.
2. Klicken Sie auf **Prepare** (Erstellen) und dann auf **Mark as Final** (Als endgültig markieren).
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**, und fahren Sie mit Ihrer Arbeit fort.
4. Wenn Sie die Bearbeitung abgeschlossen haben, signieren Sie das Dokument erneut.

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

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

1. Erstellen Sie in Microsoft Word oder Microsoft Excel ein Dokument, und speichern Sie es.
2. Klicken Sie auf das Menü **Home** (Startseite).
3. Klicken Sie neben **Sign and Encrypt** (Signieren und verschlüsseln) auf den Pfeil nach unten und anschließend auf **Add Signature Line Before Signing** (Signaturzeile vor Signieren hinzufügen).

   HINWEIS: Bei aktivierter Option ist das Kontrollkästchen neben „Add Signature Line Before Signing“ (Signaturzeile vor Signieren hinzufügen) aktiviert. Diese Option ist standardmäßig aktiviert.

4. Klicken Sie neben **Sign and Encrypt** (Signieren und verschlüsseln) auf den Pfeil nach unten und anschließend auf **Sign Document** (Dokument signieren).
5. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Hinzufügen empfohlener Signierer zu einem Microsoft Word oder Microsoft Excel Dokument

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

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

1. Erstellen Sie in Microsoft Word oder Microsoft Excel ein Dokument, und speichern Sie es.
2. Klicken Sie auf das Menü **Einfügen**.
3. Klicken Sie in der Gruppe **Text** in der Symbolleiste neben **Signature Line** (Signaturzeile) auf den Pfeil nach unten und anschließend auf **Privacy Manager Signature Provider**.

   Das Dialogfeld „Signature Setup“ (Einrichten der Signatur) wird geöffnet.
4. Geben Sie in das Feld unter **Suggested signer** (Empfohlener Signierer) den Namen des empfohlenen Signierers ein.
5. Geben Sie in das Feld unter **Instructions to the signer** (Anleitungen für den Signierer) eine Mitteilung für diesen empfohlenen Signierer ein.

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

6. Aktivieren Sie das Kontrollkästchen **Show sign date in signature line** (Signierungsdatum in Signaturzeile anzeigen), um das Datum anzuzeigen.
7. Aktivieren Sie das Kontrollkästchen **Show signer's title in signature line** (Titel des Signierers in Signaturzeile anzeigen), um den Titel anzuzeigen.

HINWEIS: Wenn die Kontrollkästchen **Show sign date in signature line** (Signierungsdatum in Signaturzeile anzeigen) und/oder **Show signer's title in signature line** (Titel des Signierers in Signaturzeile anzeigen) nicht aktiviert sind, sind die vom Dokumenteigentümer zugewiesenen, empfohlenen Signierer nicht in der Lage, das Datum und/oder den Titel in der Signaturzeile anzuzeigen, auch wenn die Dokumenteinstellungen des betreffenden empfohlenen Signierers entsprechend konfiguriert sind.

8. Klicken Sie auf **OK**.

Hinzufügen der Signaturzeile eines empfohlenen Signierers

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

So signieren Sie das Dokument:

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

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

Verschlüsseln eines Microsoft Office Dokuments

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

So verschlüsseln Sie ein Microsoft Office Dokument:

1. Erstellen Sie in Microsoft Word, Microsoft Excel oder Microsoft PowerPoint ein Dokument, und speichern Sie es.
2. Klicken Sie auf das Menü **Home** (Startseite).
3. Klicken Sie neben **Sign and Encrypt** (Signieren und verschlüsseln) auf den Pfeil nach unten und anschließend auf **Encrypt Document** (Dokument verschlüsseln).

   Das Dialogfeld „Select Trusted Contacts“ (Trusted Contacts auswählen) wird geöffnet.
4. Klicken Sie auf den Namen eines Trusted Contact, der in der Lage sein soll, das Dokument zu öffnen und seinen Inhalt anzuzeigen.

HINWEIS: Halten Sie zur Auswahl mehrerer Trusted Contacts die Taste Strg gedrückt, und klicken Sie auf die einzelnen Namen.

5. Klicken Sie auf **OK**.
6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Wenn Sie das Dokument später bearbeiten möchten, gehen Sie wie in Abschnitt **Signieren eines Microsoft Office Dokuments** beschrieben vor. Nach dem Entfernen der Verschlüsselung lässt sich das Dokument bearbeiten. Führen Sie die Schritte in diesem Abschnitt durch, um das Dokument erneut zu verschlüsseln.

Entfernen der Verschlüsselung für ein Microsoft Office Dokument

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

So entfernen Sie die Verschlüsselung für ein Microsoft Office Dokument

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

Senden eines verschlüsselten Microsoft Office Dokuments

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

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

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

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

Anzeigen eines signierten Microsoft Office Dokuments

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

Beim Öffnen eines signierten Microsoft Office Dokuments erscheint das Dialogfeld „Signatures“ (Signaturen) neben dem Dokument und gibt den Namen des Benutzers, der das Dokument signiert hat, sowie das Signierungsdatum an. Klicken Sie mit der rechten Maustaste auf den Namen, um zusätzliche Informationen anzuzeigen.

Anzeigen eines verschlüsselten Microsoft Office Dokuments

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

Ein Trusted Contact, der ein verschlüsseltes Microsoft Office Dokument anzeigen möchte, muss auf seinem Computer ein Privacy Manager-Zertifikat sowie Privacy Manager installiert haben. Außerdem muss der Trusted Contact vom Eigentümer des verschlüsselten Microsoft Office Dokuments ausgewählt worden sein.

Verwenden von Privacy Manager in Microsoft Outlook

Bei der Installation von Privacy Manager wird in der Symbolleiste von Microsoft Outlook eine Privacy-Schaltfläche angezeigt. Außerdem steht in der Symbolleiste jeder Microsoft Outlook E-Mail-Nachricht die Schaltfläche „Send Securely“ (Sicheres Senden) zur Verfügung.

Konfigurieren von Privacy Manager für Microsoft Outlook

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

   – ODER –

   Klicken Sie in der Hauptsymbolleiste von Microsoft Outlook neben **Privacy** auf den Pfeil nach unten und anschließend auf **Einstellungen**.

   – ODER –

   Klicken Sie in der Symbolleiste einer Microsoft Outlook E-Mail-Nachricht neben **Send Securely** (Sicheres Senden) auf den Pfeil nach unten und anschließend auf **Einstellungen**.

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

Signieren und Senden einer E-Mail-Nachricht

- Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
- Schreiben Sie Ihre E-Mail-Nachricht.
- Klicken Sie neben **Send Securely** (Sicheres Senden) auf den Pfeil nach unten und anschließend auf **Sign and Send** (Signieren und senden).
- Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Versiegeln und Senden einer E-Mail-Nachricht

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

So versiegeln und senden Sie eine E-Mail-Nachricht an einen Trusted Contact:

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Schreiben Sie Ihre E-Mail-Nachricht.
3. Klicken Sie neben **Send Securely** (Sicheres Senden) auf den Pfeil nach unten und anschließend auf **Seal for Trusted Contacts and Send** (Für Trusted Contacts versiegeln und senden).
4. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Anzeigen einer versiegelten E-Mail-Nachricht

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

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

Verwenden von Privacy Manager in Windows Live Messenger

Hinzufügen von Privacy Manager Chat

Gehen Sie folgendermaßen vor, um Privacy Manager Chat zu Windows Live Messenger hinzuzufügen:

1. Melden Sie sich an Windows Live Home an.
2. Klicken Sie auf das Symbol **Windows Live** und anschließend auf **Windows Live Services**.
3. Klicken Sie auf **Gallery** und dann auf **Messenger**.
4. Klicken Sie auf **Activities** (Aktivitäten) und weiter auf **Safety and Security** (Sicherheit).
5. Klicken Sie auf **Privacy Manager Chat**, und befolgen Sie die Anleitungen auf dem Bildschirm.

Starten von Privacy Manager Chat

HINWEIS: Um Privacy Manager Chat einsetzen zu können, müssen beide Parteien sowohl Privacy Manager als auch ein Privacy Manager-Zertifikat installiert haben. Näheres zur Installation eines Privacy Manager-Zertifikats finden Sie im Abschnitt „Anfordern und Installieren eines Privacy Manager-Zertifikats“ auf Seite 5.

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

   a. Klicken Sie mit der rechten Maustaste auf einen Online-Kontakt in Live Messenger, und wählen Sie **Start an Activity** (Eine Aktivität starten).

   b. Klicken Sie auf **Start Privacy Manager Chat** (Privacy Manager Chat starten).

   – ODER –

   a. Doppelklicken Sie auf einen Online-Kontakt in Live Messenger. Klicken Sie dann auf das Menü **Conversation** (Unterhaltung).

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

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

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

Konfigurieren von Privacy Manager Chat für Windows Live Messenger

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

   – ODER –

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

   – ODER –

   Klicken Sie in Privacy Manager History Viewer auf die Schaltfläche **Einstellungen**.

2. Um anzugeben, wie lange Privacy Manager Chat bis zum Sperren Ihrer Sitzung warten soll, wählen Sie im Feld **Lock session after _ minutes of inactivity** (Sitzung nach _ Minuten ohne Aktivität sperren) einen Zahlenwert aus.

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

4. Damit Ihre Sitzungen automatisch verschlüsselt und gespeichert werden, wenn Sie sie schließen, aktivieren Sie das Kontrollkästchen **Automatically save secure chat history** (Sicheres Chat-Protokoll automatisch speichern).

5. Klicken Sie auf **OK**.

Im Fenster „Privacy Manager Chat“ chatten

Nach dem Start von Privacy Manager Chat wird das Fenster „Privacy Manager Chat“ in Windows Live Messenger geöffnet. Die Verwendung von Privacy Manager Chat ist ähnlich der von Windows Live

Messenger, wobei die folgenden Funktionen zusätzlich im Fenster „Privacy Manager Chat“ verfügbar sind:

- **Speichern**: Klicken Sie auf diese Schaltfläche, um Ihre Chat-Sitzung in dem Ordner zu speichern, den Sie in den Konfigurationseinstellungen angegeben haben. Sie können Privacy Manager Chat auch so konfigurieren, dass automatisch jede Sitzung gespeichert wird, wenn Sie sie schließen.
- **Alles ausblenden** und **Alles anzeigen**: Klicken Sie auf die entsprechende Schaltfläche, um die Nachrichten, die im Fenster „Secure Communications“ (Sichere Kommunikation) angezeigt werden, ein- oder auszublenden. Sie können auch einzelne Nachrichten ausblenden oder anzeigen, indem Sie auf den Header der Nachricht klicken.
- **Sind Sie da?**: Klicken Sie auf diese Schaltfläche, um Ihren Kontakt zur Authentifizierung aufzufordern.
- **Sperren**: Klicken Sie auf diese Schaltfläche, um das Fenster „Privacy Manager Chat“ zu schließen und zum Fenster „Chat Entry“ (Chat-Einstieg) zurückzukehren. Zum erneuten Anzeigen des Fensters „Secure Communications“ (Sichere Kommunikation) klicken Sie auf **Sitzung fortsetzen**. Authentifizieren Sie sich anschließend mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
- **Senden**: Klicken Sie auf diese Schaltfläche, um eine verschlüsselte Nachricht an Ihren Kontakt zu senden.
- **Signiert senden:** Aktivieren Sie dieses Kontrollkästchen, um Ihre Nachrichten elektronisch zu signieren und zu verschlüsseln. Wird dann versucht, die Nachricht zu manipulieren, wird sie als ungültig gekennzeichnet, wenn sie der Empfänger erhält. Sie müssen sich jedes Mal authentifizieren, wenn Sie eine signierte Nachricht senden möchten.
- **Ausgeblendet senden**: Aktivieren Sie diese Option, um eine Nachricht zu verschlüsseln und zu senden, für die nur der Kopf angezeigt wird. Ihr Kontakt muss sich authentifizieren, um den Inhalt der Nachricht lesen zu können.

Anzeigen des Chat-Protokolls

Privacy Manager Chat History Viewer zeigt verschlüsselte Privacy Manager Chat-Sitzungsdateien an. Sie können die Sitzungen speichern, indem Sie im Fenster „Privacy Manager Chat“ auf Speichern klicken oder auf der Registerkarte „Chat“ in Privacy Manager die Funktion für automatisches Speichern konfigurieren. In Privacy Manager Chat History Viewer werden für jede Sitzung der (verschlüsselte) Contact Screen Name sowie Datum und Uhrzeit von Beginn und Ende der Sitzung angezeigt. Standardmäßig werden die Sitzungen für alle E-Mail-Konten angezeigt, die Sie eingerichtet haben. Über das Menü **Display history for** (Protokoll anzeigen für) können Sie bestimmte Konten zum Anzeigen auswählen.

Starten des Chat History Viewer

1. Klicken Sie unter Windows Vista auf **Start**, **Alle Programme**, **HP ProtectTools Security Manager for Administrators** bzw. unter Windows XP auf **HP ProtectTools Security Manager**.
2. Klicken Sie auf **Privacy Manager: Sign and Chat** und dann auf **Chat History Viewer**.

   – ODER –

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

   – ODER –

   ▲ Klicken Sie auf der Seite „Chat Configuration“ (Chat-Konfiguration) auf **Start Live Messenger History Viewer** (Live Messenger History Viewer starten).

Sichtbarmachen aller Sitzungen

Beim Sichtbarmachen aller Sitzungen werden der entschlüsselte Contact Screen Name für die aktuell ausgewählten Sitzungen sowie alle Sitzungen im selben Konto angezeigt.

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

   Die Contact Screen Names sind entschlüsselt.
3. Doppelklicken Sie auf eine Sitzung, um ihren Inhalt anzuzeigen.

Sichtbarmachen der Sitzungen für ein bestimmtes Konto

Beim Sichtbarmachen einer Sitzung wird der entschlüsselte Contact Screen Name für die aktuell ausgewählte Sitzung angezeigt.

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

   Die Contact Screen Names sind entschlüsselt.
3. Doppelklicken Sie auf die sichtbar gemachte Sitzung, um ihren Inhalt anzuzeigen.

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

Anzeigen einer Sitzungs-ID

- Klicken Sie in Chat History Viewer mit der rechten Maustaste auf eine sichtbar gemachte Sitzung, und wählen Sie dann die Option **View session ID** (Sitzungs-ID anzeigen).

Anzeigen einer Sitzung

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

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

   Der Sitzungsinhalt ist entschlüsselt.

Sitzungen nach bestimmtem Text durchsuchen

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

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

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

Löschen einer Sitzung

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

Hinzufügen oder Entfernen von Spalten

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

So fügen Sie der Ansicht Spalten hinzu:

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

So entfernen Sie Spalten aus der Ansicht:

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

Filtern der angezeigten Sitzungen

In Chat History Viewer wird eine Liste der Sitzungen für alle Ihre Konten angezeigt.

Anzeigen der Sitzungen für ein bestimmtes Konto

- Wählen Sie in Chat History Viewer ein Konto aus dem Menü **Display history for** (Protokoll anzeigen für) aus.

Anzeigen der Sitzungen für einen bestimmten Datumsbereich

1. Klicken Sie in Chat History View auf das Symbol **Advanced Filter** (Erweiterter Filter).

   Das Dialogfeld „Advanced Filter“ (Erweiterter Filter) wird geöffnet.
2. Aktivieren Sie das Kontrollkästchen **Display only sessions within specified date range** (Nur Sitzungen innerhalb des angegebenen Datumsbereichs anzeigen).
3. Geben Sie in die Felder **From date** (Von) und **To date** (Bis) Tag, Monat und/oder Jahr ein, oder klicken Sie auf den Pfeil neben dem Kalender, um die Datumswerte auszuwählen.
4. Klicken Sie auf **OK**.

Anzeigen der Sitzungen, die nicht im Standardordner gespeichert sind

1. Klicken Sie in Chat History View auf das Symbol **Advanced Filter** (Erweiterter Filter).
2. Aktivieren Sie das Kontrollkästchen **Use an alternate history files folder** (Alternativen Ordner für Protokolldateien verwenden).
3. Geben Sie den Pfad für den Ordner ein, oder klicken Sie auf **Durchsuchen**, um nach einem Ordner zu suchen.
4. Klicken Sie auf **OK**.

Erweiterte Aufgaben

Migrieren von Privacy Manager-Zertifikaten und Trusted Contacts auf einen anderen Computer

Sie können Ihre Privacy Manager-Zertifikate und Trusted Contacts sicher auf einen anderen Computer migrieren. Exportieren Sie dazu die Privacy Manager-Zertifikate und Trusted Contacts als kennwortgeschützte Datei in einen Netzwerkordner oder auf einen Wechseldatenträger, und importieren Sie anschließend die Datei auf dem neuen Computer.

Exportieren von Privacy Manager-Zertifikaten und Trusted Contacts

Gehen Sie folgendermaßen vor, um Ihre Privacy Manager-Zertifikate und Trusted Contacts in eine kennwortgeschützte Datei zu exportieren:

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

HINWEIS: Bewahren Sie dieses Kennwort an einem sicheren Ort auf, da Sie es benötigen, um die Migrationsdatei zu importieren.

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

Importieren von Privacy Manager-Zertifikaten und Trusted Contacts

Gehen Sie folgendermaßen vor, um Ihre Privacy Manager-Zertifikate und Trusted Contacts aus einer kennwortgeschützten Datei zu importieren:

1. Öffnen Sie Privacy Manager, und klicken Sie auf **Migration**.
2. Klicken Sie auf **Import migration file** (Migrationsdatei importieren).
3. Wählen Sie auf der Seite „Select Data“ (Daten auswählen) die Datenkategorien aus, die in die Migrationsdatei einbezogen werden sollen, und klicken Sie anschließend auf **Weiter**.
4. Geben Sie auf der Seite „Migration File“ (Migrationsdatei) einen Dateinamen ein, oder klicken Sie auf **Durchsuchen**, um nach einem Speicherort zu suchen, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf der Seite „Migration File Import“ (Migrationsdatei-Import) auf **Beenden**.

6 File Sanitizer for HP ProtectTools

Mit File Sanitizer können Sie Datenbestände (persönliche Informationen oder Dateien, Verlaufsdaten oder Web-bezogene Daten sowie sonstige Datenkomponenten) auf Ihrem Computer sicher vernichten und die Festplatte regelmäßig bereinigen.

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

Informationen zum Shreddern

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

Das so genannte Shreddern unterscheidet sich vom gewöhnlichen Löschvorgang unter Windows® (auch bekannt als einfaches Löschen in File Sanitizer). Beim Shreddern eines Datenbestands überschreibt ein Algorithmus die Daten, sodass es praktisch unmöglich ist, die Originaldaten wiederherzustellen.

Wenn Sie ein Shred-Profil (Hohe Sicherheit, Mittlere Sicherheit oder Niedrige Sicherheit) auswählen, werden automatisch eine vordefinierte Liste mit Datenbeständen sowie eine Löschmethode für das Shreddern aufgerufen. Sie haben auch die Möglichkeit, das Shred-Profil anzupassen, indem Sie die folgenden Informationen angeben: Anzahl der Shred-Zyklen, welche Datenbestände in den Shred-Vorgang einbezogen werden sollen, für welche Datenbestände das Shreddern vor dem Ausführen des Befehls bestätigt werden soll und welche Datenbestände vom Shred-Prozess ausgeschlossen werden sollen.

Sie können einen automatischen Shred-Zeitplan erstellen, aber auch jederzeit Datenbestände manuell shreddern.

Informationen zum Bereinigen der Festplatte

Bei der Bereinigung der Festplatte werden gelöschte Datenbestände sicher mit willkürlichen Daten überschrieben, sodass die Originalinhalte nicht mehr angezeigt werden können.

HINWEIS: Mithilfe einer Bereinigung können Sie die Datenbestände von der Festplatte entfernen, die Sie über den Windows Papierkorb oder manuell gelöscht haben. Die Festplattenbereinigung bietet jedoch keine zusätzliche Sicherheit für geshredderte Datenbestände.

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 unter Windows Vista auf **Start**, **Alle Programme**, **HP ProtectTools Security Manager for Administrators** bzw. unter Windows XP auf **HP ProtectTools Security Manager**.
2. Klicken Sie auf **File Sanitizer**.

   – ODER –

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

  – ODER –

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

Erstellen eines Zeitplans für die Festplattenbereinigung

HINWEIS: Das Bereinigen der Festplatte bietet sich für Datenbestände an, die Sie über den Windows Papierkorb oder manuell gelöscht haben. Die Festplattenbereinigung bietet jedoch keine zusätzliche Sicherheit für geshredderte Datenbestände.

So erstellen Sie einen Zeitplan für die Festplattenbereinigung:

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Free Space Bleaching** (Überschreiben von freiem Speicherplatz).
2. Aktivieren Sie das Kontrollkästchen **Activate Scheduler** (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 **Übernehmen** und anschließend auf **OK**.

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.

Auswählen oder Erstellen eines Shred-Profils

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

Auswählen eines vordefinierten Shred-Profils

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

So wählen Sie ein vordefiniertes Shred-Profil aus:

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

Anpassen eines Shred-Profils

Beim Erstellen eines Shred-Profils können Sie die folgenden Informationen angeben: Anzahl der Shred-Zyklen, welche Datenbestände in den Shred-Vorgang einbezogen werden sollen, für welche Datenbestände das Shreddern vor dem Ausführen des Befehls bestätigt werden soll und welche Datenbestände vom Shred-Prozess ausgeschlossen werden sollen.

1. Öffnen Sie File Sanitizer, und klicken Sie nacheinander auf **Einstellungen**, **Advanced Security Settings** (Erweiterte Sicherheitseinstellungen), **View Details** (Details anzeigen).

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

HINWEIS: Die angegebene Anzahl der Shred-Zyklen gilt für jeden Datenbestand. Wenn Sie beispielsweise drei Shred-Zyklen festlegen, wird dreimal ein Algorithmus zum Überschreiben der Daten ausgeführt. Eine höhere Anzahl von Shred-Zyklen zur Verbesserung der Sicherheit kann den Shred-Vorgang erheblich verlängern. Allerdings steigt die Sicherheit des Computers mit der Anzahl der Shred-Zyklen.

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

   a. Klicken Sie unter **Available shred options** (Verfügbare Shred-Optionen) auf einen Datenbestand und anschließend auf **Hinzufügen**.

   b. Zum Hinzufügen eines benutzerdefinierten Datenbestands klicken Sie auf **Add Custom Option** (Benutzerdefinierte Option hinzufügen). Geben Sie anschließend einen Datei- oder Ordnernamen ein, und klicken Sie auf **OK**. Klicken Sie auf den benutzerdefinierten Datenbestand und dann auf **Hinzufügen**.

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

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

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

5. Klicken Sie unter **Do not shred the following** (Folgende Elemente nicht shreddern) auf **Hinzufügen**, um die Datenbestände auszuwählen, die vom Shreddern ausgeschlossen werden sollen.

HINWEIS: Es können nur Dateierweiterungen vom Shreddern ausgeschlossen werden. Wenn Sie zum Beispiel die Dateierweiterung BMP hinzufügen, werden alle Dateien mit dieser Erweiterung vom Shred-Prozess ausgeschlossen.

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

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

Anpassen eines Profils für einfaches Löschen

Das Profil für einfaches Löschen führt einen Standardlöschvorgang für Datenbestände ohne Shreddern durch. Beim Anpassen eines Profils für einfaches Löschen können Sie angeben, welche Datenbestände in den einfachen Löschvorgang einbezogen werden sollen, für welche Datenbestände das Löschen vor dem Ausführen des Vorgangs bestätigt werden soll und welche Datenbestände vom Löschen auszuschließen sind.

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

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

   HINWEIS: Zum Löschen eines Datenbestands aus den verfügbaren Löschoptionen klicken Sie auf den betreffenden Datenbestand und anschließend auf **Löschen**.
3. Aktivieren Sie unter **Delete the following** (Folgende Elemente löschen) das Kontrollkästchen neben jedem Datenbestand, für den Sie das Löschen bestätigen möchten.

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

4. Klicken Sie unter **Do not shred the following** (Folgende Elemente nicht shreddern) auf **Hinzufügen**, um die Datenbestände auszuwählen, die vom Shreddern ausgeschlossen werden sollen.

HINWEIS: Es können nur Dateierweiterungen vom Löschen ausgeschlossen werden. Wenn Sie zum Beispiel die Dateierweiterung BMP hinzufügen, werden alle Dateien mit dieser Erweiterung vom Löschprozess ausgeschlossen.

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

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

Planen eines Shred-Vorgangs

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shred** (Shreddern).
2. Wählen Sie eine Shred-Option:
   - **Windows startup** (Beim Starten von Windows): Wenn diese Option aktiviert ist, werden alle ausgewählten Datenbestände beim Start von Windows geshreddert.
   - **Windows shutdown** (Beim Herunterfahren von Windows): Wenn diese Option aktiviert ist, werden alle ausgewählten Datenbestände beim Herunterfahren von Windows geshreddert.

     HINWEIS: Bei Auswahl dieser Option wird beim Herunterfahren ein Dialogfeld angezeigt. Sie können das Shreddern der ausgewählten Datenbestände bestätigen oder umgehen. Klicken Sie auf Ja, um das Shreddern zu umgehen, oder auf Nein, um mit dem Shreddern der Datenbestände fortzufahren.
   - **Web browser open** (Beim Öffnen eines Webbrowsers): Wählen Sie diese Option, um alle ausgewählten Web-bezogenen Datenbestände, z. B. URL-Verlauf des Browsers, zu shreddern, sobald ein Webbrowser geöffnet wird.
   - **Web browser quit** (Beim Schließen eines Webbrowsers): Wählen Sie diese Option, um alle ausgewählten Web-bezogenen Datenbestände, z. B. URL-Verlauf des Browsers, zu shreddern, sobald ein Webbrowser geschlossen wird.
   - **Scheduler** (Planer): Aktivieren Sie das Kontrollkästchen **Activate Scheduler** (Planer aktivieren), geben Sie Ihr Windows Kennwort ein, und tragen Sie anschließend Tag und Uhrzeit für das Shreddern bestimmter Datenbestände ein.
3. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Erstellen eines Zeitplans für die Festplattenbereinigung

HINWEIS: Das Bereinigen der Festplatte bietet sich für Datenbestände an, die Sie über den Windows Papierkorb oder manuell gelöscht haben. Die Festplattenbereinigung bietet jedoch keine zusätzliche Sicherheit für geshredderte Datenbestände.

So erstellen Sie einen Zeitplan für die Festplattenbereinigung:

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Free Space Bleaching** (Überschreiben von freiem Speicherplatz).
2. Aktivieren Sie das Kontrollkästchen **Activate Scheduler** (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 **Übernehmen** und anschließend auf **OK**.

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.

Auswählen oder Erstellen eines Shred-Profils

Auswählen eines vordefinierten Shred-Profils

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

So wählen Sie ein vordefiniertes Shred-Profil aus:

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

Anpassen eines Shred-Profils

Beim Erstellen eines Shred-Profils können Sie die folgenden Informationen angeben: Anzahl der Shred-Zyklen, welche Datenbestände in den Shred-Vorgang einbezogen werden sollen, für welche Datenbestände das Shreddern vor dem Ausführen des Befehls bestätigt werden soll und welche Datenbestände vom Shred-Prozess ausgeschlossen werden sollen.

1. Öffnen Sie File Sanitizer, und klicken Sie nacheinander auf **Einstellungen**, **Advanced Security Settings** (Erweiterte Sicherheitseinstellungen), **View Details** (Details anzeigen).
2. Geben Sie die Anzahl der Shred-Zyklen an.

HINWEIS: Die angegebene Anzahl der Shred-Zyklen gilt für jeden Datenbestand. Wenn Sie beispielsweise drei Shred-Zyklen festlegen, wird dreimal ein Algorithmus zum Überschreiben der Daten ausgeführt. Eine höhere Anzahl von Shred-Zyklen zur Verbesserung der Sicherheit kann den Shred-Vorgang erheblich verlängern. Allerdings steigt die Sicherheit des Computers mit der Anzahl der Shred-Zyklen.

3. Wählen Sie die Datenbestände aus, die geshreddert werden sollen:
   a. Klicken Sie unter **Available shred options** (Verfügbare Shred-Optionen) auf einen Datenbestand und anschließend auf **Hinzufügen**.
   b. Zum Hinzufügen eines benutzerdefinierten Datenbestands klicken Sie auf **Add Custom Option** (Benutzerdefinierte Option hinzufügen). Geben Sie anschließend einen Datei- oder Ordnernamen ein, und klicken Sie auf **OK**. Klicken Sie auf den benutzerdefinierten Datenbestand und dann auf **Hinzufügen**.

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

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

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

5. Klicken Sie unter **Do not shred the following** (Folgende Elemente nicht shreddern) auf **Hinzufügen**, um die Datenbestände auszuwählen, die vom Shreddern ausgeschlossen werden sollen.

HINWEIS: Es können nur Dateierweiterungen vom Shreddern ausgeschlossen werden. Wenn Sie zum Beispiel die Dateierweiterung BMP hinzufügen, werden alle Dateien mit dieser Erweiterung vom Shred-Prozess ausgeschlossen.

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

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

Anpassen eines Profils für einfaches Löschen

Das Profil für einfaches Löschen führt einen Standardlöschvorgang für Datenbestände ohne Shreddern durch. Beim Anpassen eines Profils für einfaches Löschen können Sie angeben, welche Datenbestände in den einfachen Löschvorgang einbezogen werden sollen, für welche Datenbestände das einfache Löschen vor dem Ausführen des Vorgangs bestätigt werden soll und welche Datenbestände vom einfachen Löschen auszuschließen sind.

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

1. Öffnen Sie File Sanitizer, und klicken Sie nacheinander auf **Einstellungen**, **Simple Delete Setting** (Einstellung für einfaches Löschen) und **View Details** (Details anzeigen).

2. Wählen Sie die zu löschenden Datenbestände aus:

   - Klicken Sie unter **Available delete options** (Verfügbare Löschoptionen) auf einen Datenbestand und anschließend auf **Hinzufügen**.

   - Zum Hinzufügen eines benutzerdefinierten Datenbestands klicken Sie auf **Add Custom Option** (Benutzerdefinierte Option hinzufügen). Geben Sie anschließend einen Datei- oder Ordnernamen ein, und klicken Sie auf **OK**. Klicken Sie auf den benutzerdefinierten Datenbestand und dann auf **Hinzufügen**.

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

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

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

4. Klicken Sie unter **Do not delete the following** (Folgende Elemente nicht löschen) auf **Hinzufügen**, um die Datenbestände auszuwählen, die vom Löschen ausgeschlossen werden sollen.

HINWEIS: Es können nur Dateierweiterungen vom Löschen ausgeschlossen werden. Wenn Sie zum Beispiel die Dateierweiterung BMP hinzufügen, werden alle Dateien mit dieser Erweiterung vom Löschprozess ausgeschlossen.

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

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

Allgemeine Aufgaben

Verwenden von Tastenfolgen zum Einleiten des Shred-Vorgangs

Gehen Sie folgendermaßen vor, um eine Tastenfolge festzulegen:

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shred** (Shreddern).
2. Aktivieren Sie das Kontrollkästchen **Key sequence** (Tastenfolge).
3. Geben Sie im entsprechenden Feld ein Zeichen ein, und aktivieren Sie anschließend **CTRL** (Strg), **ALT** oder **SHIFT** (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 **CTRL** (Strg) und **SHIFT** (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 Datenbestände können nicht wiederhergestellt werden. Gehen Sie daher bei der Auswahl von Datenbeständen für manuelles Shreddern mit Bedacht vor.

1. Navigieren Sie zu dem Dokument oder Ordner, das bzw. der geshreddert werden soll.
2. Ziehen Sie den Datenbestand auf das Symbol „File Sanitizer“ auf dem Desktop.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.
4. Wählen Sie **Ja**, um das Entfernen des ausgewählten Benutzers zu bestätigen.

Manuelles Shreddern eines Datenbestands

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

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **Shred One** (Ein Element shreddern).
2. Das Dialogfeld **Durchsuchen** wird geöffnet. Navigieren Sie zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.

HINWEIS: Als Datenbestand kann eine einzelne Datei oder ein einzelner Ordner ausgewählt werden.

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 **Shred One** (Ein Element shreddern).
2. Das Dialogfeld **Durchsuchen** wird geöffnet. Navigieren Sie zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shred** (Shreddern).
2. Klicken Sie auf die Schaltfläche **Durchsuchen**.
3. Das Dialogfeld **Durchsuchen** wird geöffnet. Navigieren Sie zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Shreddern aller ausgewählten Datenbestände

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

Manuelles Aktivieren der Festplattenbereinigung

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

– ODER –

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Free Space Bleaching** (Überschreiben von freiem Speicherplatz).
2. Klicken Sie auf **Bleach Now** (Jetzt überschreiben).
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Abbrechen eines Shred-Vorgangs oder einer Festplattenbereinigung

Wenn der Shred- bzw. Bereinigungsvorgang bereits läuft, wird über dem Symbol „HP ProtectTools Security Manager for Administrators“ im Infobereich eine Meldung angezeigt. Die Meldung 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

7 Java Card Security for HP ProtectTools

Mit Java Card Security for HP ProtectTools verwalten Sie die Java Card-Einrichtung und -Konfiguration für die Verwendung mit der HP Smart Card-Tastatur. Die HP Java Card ist ein persönliches Sicherheitsgerät, das Authentifizierungsdaten schützt, da es sowohl die Card als auch eine PIN-Nummer benötigt, um den Zugriff zu gewähren – wie bei der Verwendung einer Geldautomatenkarte mit einer PIN. Die Java Card kann verwendet werden, um auf Credential Manager, Drive Encryption, HP BIOS oder auf eine beliebige Anzahl von Access Points von Drittanbietern zuzugreifen.

Mit Java Card Security können Sie die folgenden Aufgaben ausführen:

- Zugriff auf Java Card-Sicherheitsfunktionen
- Aktivieren der Unterstützung für die Java Card-Authentifizierung beim Systemstart mit Hilfe von Computer Setup Utility
- Konfigurieren separater Java Cards für Administrator und Benutzer; damit das Betriebssystem geladen werden kann, muss der Benutzer die Java Card einlegen und eine PIN eingeben.
- Einstellen und Ändern der PIN zur Authentifizierung von Benutzern der Java Card

Allgemeine Aufgaben

Auf der Seite „Allgemein“ können Sie folgende Aufgaben ausführen:

- Ändern der Java Card-PIN
- Wählen Sie den Kartenleser oder die Smart Card-Tastatur

HINWEIS: Der Card Reader kann sowohl für Java Cards als auch für Smart Cards verwendet werden. Diese Funktion steht zur Verfügung, wenn mehrere Lesegeräte an den Computer angeschlossen sind.

Ändern der Java Card-PIN

So ändern Sie die Java Card-PIN:

HINWEIS: Die Java Card-PIN muss zwischen 4 und 8 numerische Zeichen enthalten.

1. Wählen Sie **Start** > **Alle Programme** > **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Java Card Security** (Java Card-Sicherheit) und dann auf **Allgemein**.
3. Legen Sie eine Java Card (mit einer vorhandenen PIN) in den Card Reader ein.

4. Klicken Sie im rechten Fensterausschnitt auf **Ändern**.
5. Geben Sie im Dialogfeld **PIN ändern** die aktuelle PIN in das Dialogfeld **Current PIN** (Aktuelle PIN) ein.
6. Geben Sie eine neue PIN in das Feld **Neue PIN** ein, und bestätigen Sie die PIN im Feld **Neue Pin bestätigen**.
7. Klicken Sie auf **OK**.

Auswählen des Card Readers

Vergewissern Sie sich, dass in Java Card Security der richtige Card Reader ausgewählt wurde, bevor Sie die Java Card verwenden. Wenn das falsche Lesegerät ausgewählt wurde, stehen einige Funktionen möglicherweise nicht zur Verfügung oder werden falsch angezeigt. Außerdem müssen die Treiber für das Lesegerät korrekt installiert worden sein. Dies kann im Windows Geräte-Manager überprüft werden.

So wählen Sie den Card Reader aus:

1. Wählen Sie **Start** > **Alle Programme** > **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Java Card Security** (Java Card-Sicherheit) und dann auf **Allgemein**.
3. Legen Sie die Java Card in den Card Reader ein.
4. Klicken Sie im rechten Fensterausschnitt unter **Selected Card Reader** (Ausgewählter Card Reader) auf das richtige Lesegerät.

Erweiterte Aufgaben (nur für Administratoren)

Auf der Seite „Erweitert“ können Sie folgende Aufgaben ausführen:

- Zuordnen einer Java Card-PIN;
- Zuordnen eines Namens zu einer Java Card-PIN;
- Einrichten der Authentifizierung beim Systemstart;
- Sichern und Wiederherstellen der Java Cards.

HINWEIS: Zur Anzeige der Seite „Advanced“ müssen Sie über Windows Administratorrechte verfügen.

Zuordnen einer Java Card-PIN

Sie müssen einer Java Card eine PIN zuordnen, bevor Sie die Java Card für die Authentifizierung beim Systemstart verwenden können.

So ordnen Sie einer Java Card eine PIN zu:

HINWEIS: Die Java Card-PIN muss zwischen 4 und 8 numerische Zeichen enthalten.

1. Wählen Sie **Start** > **Alle Programme** > **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Java Card Security** (Java Card-Sicherheit) und dann auf **Erweitert**.
3. Legen Sie eine neue Java Card in den Card Reader ein.
4. Wenn das Dialogfeld **Neue Karte** angezeigt wird, geben Sie einen neuen Namen in das Feld **Neuer Anzeigename** ein. Geben Sie anschließend in das Feld **Neue PIN** eine neue PIN ein, und bestätigen Sie die Eingabe in **Neue PIN bestätigen**.
5. Klicken Sie auf **OK**.

Zuordnen eines Namens zu einer Java Card-PIN

Sie müssen einer Java Card einen Namen zuordnen, bevor Sie die Java Card für die Authentifizierung beim Systemstart verwenden können.

So ordnen Sie einer Java Card einen Namen zu:

1. Wählen Sie **Start** > **Alle Programme** > **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Java Card Security** (Java Card-Sicherheit) und dann auf **Erweitert**.
3. Legen Sie die Java Card in das Karten-Lesegerät ein.

HINWEIS: Wenn Sie dieser Karte keine PIN zugeordnet haben, wird das Dialogfeld **Neue Karte** angezeigt, in das Sie einen neuen Namen und eine neue PIN eingeben können.

4. Klicken Sie im rechten Fensterausschnitt unter **Anzeigename** auf **Ändern**.
5. Geben Sie einen Namen für die Java Card in das Feld **Name** ein.
6. Geben Sie die aktuelle Java Card-PIN in das Feld **PIN** ein.
7. Klicken Sie auf **OK**.

Einrichten der Authentifizierung beim Systemstart

Wenn die Authentifizierung beim Systemstart aktiviert ist, benötigen Sie eine Java Card, um den Computer zu starten.

Für das Aktivieren der Authentifizierung beim Systemstart müssen Sie folgende Schritte ausführen:

1. Aktivieren der Java Card-Systemstart-Authentifizierungsfunktion in BIOS Configuration oder Computer Setup.
2. Aktivieren Sie die Java Card-Authentifizierung beim Systemstart in Java Card Security.
3. Erstellen und aktivieren Sie die Administrator-Java Card.

Aktivieren der Java Card-Authentifizierung beim Systemstart und Erstellen der Administrator-Java Card

So aktivieren Sie die Java Card-Authentifizierung beim Systemstart:

1. Wählen Sie **Start** > **Alle Programme** > **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Java Card Security** (Java Card-Sicherheit) und dann auf **Erweitert**.
3. Legen Sie die Java Card in das Karten-Lesegerät ein.

HINWEIS: Wenn Sie dieser Karte keinen Namen und keine PIN zugeordnet haben, wird das Dialogfeld **Neue Karte** angezeigt, in das Sie einen neuen Namen und eine neue PIN eingeben können.

4. Aktivieren Sie im rechten Fensterausschnitt unter **Power-on authentication** (Authentifizierung beim Systemstart) das Kontrollkästchen **Aktivieren**.
5. Geben Sie das Kennwort für Computer Setup in das Dialogfeld **Computer Setup Kennwort** ein. Klicken Sie anschließend auf **OK**.
6. Wenn Sie DriveLock nicht aktiviert haben, geben Sie die Java Card-PIN ein. Klicken Sie anschließend auf **OK**.

   – ODER –

   Wenn DriveLock aktiviert ist:

   a. Klicken Sie auf **Eindeutige Java Card-Identität festlegen**.

      – ODER –

      Klicken Sie auf **Java Card-Identität an DriveLock Kennwort angleichen**.

      HINWEIS: Wenn DriveLock auf dem Computer aktiviert ist, können Sie die Java Card-Identität mit dem DriveLock Benutzerkennwort gleichsetzen. Somit können Sie DriveLock und die Java Card nur mit der Java Card validieren, wenn Sie den Computer starten.

   b. Falls zutreffend, geben Sie das Benutzerkennwort für DriveLock in das Feld **DriveLock Password** (DriveLock Kennwort) ein. Geben Sie es anschließend erneut in das Feld **Kennwort bestätigen** ein.

   c. Geben Sie die Java Card-PIN ein.

   d. Klicken Sie auf **OK**.
7. Wenn Sie zum Erstellen einer Wiederherstellungsdatei aufgefordert werden, klicken Sie auf **Abbrechen**, falls Sie die Wiederherstellungsdatei zu einem späteren Zeitpunkt erstellen möchten. Alternativ klicken Sie auf **OK** und befolgen die Bildschirmanleitungen des HP ProtectTools Backup-Assistenten, um die Datei jetzt zu erstellen.

HINWEIS: Weitere Informationen finden Sie unter „Sichern und Wiederherstellen von Zugangsdaten in HP ProtectTools“ auf Seite 10.

Erstellen einer Java Card-PIN

HINWEIS: Um eine Benutzer-Java Card zu erstellen, müssen die Authentifizierung beim Systemstart und eine Administratorkarte eingerichtet sein.

So erstellen Sie eine Java Card:

1. Wählen Sie **Start** > **Alle Programme** > **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Java Card Security** (Java Card-Sicherheit) und dann auf **Erweitert**.
3. Legen Sie eine Java Card ein, die als Benutzerkarte verwendet wird.
4. Klicken Sie im rechten Fensterausschnitt unter **Power-on authentication** (Authentifizierung beim Systemstart) auf **Erstellen** neben **User card identity** (Benutzerkarten-ID).
5. Geben Sie eine PIN für die Benutzer-Java Card ein, und klicken Sie auf **OK**.

Deaktivieren der Java Card-Authentifizierung beim Systemstart

Wenn Sie die Java Card-Authentifizierung beim Systemstart deaktivieren, benötigen Sie keine Java Card, um den Computer zu starten.

1. Wählen Sie **Start** > **Alle Programme** > **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Java Card Security** (Java Card-Sicherheit) und dann auf **Erweitert**.
3. Legen Sie die Administrator-Java Card ein.
4. Deaktivieren Sie im rechten Fensterausschnitt unter **Power-on authentication** (Authentifizierung beim Systemstart) das Kontrollkästchen **Aktivieren**.
5. Geben Sie eine PIN für die Java Card ein, und klicken Sie auf **OK**.

8 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools ermöglicht den Zugriff auf die Sicherheits- und Konfigurationsfunktionen von Computer Setup. Sie bieten Benutzern den Zugriff über Windows auf Systemsicherheitsfunktionen, die von Computer Setup verwaltet werden. BIOS Configuration for HP ProtectTools bietet folgende Optionen:

- File (Datei)
- Storage (Speicher)
- Security (Sicherheit)
- Power (Stromzufuhr)
- Advanced (Erweitert)

HINWEIS: Je nach Hardwarekonfiguration werden unterschiedliche Computer Setup-Optionen unterstützt.

Mit BIOS Configuration können Sie verschiedene Computereinstellungen verwalten, die andernfalls nur zugänglich wären, wenn Sie beim Start die Taste F10 drücken und Computer Setup aktivieren. Mit BIOS Configuration können Sie die folgenden Ziele erreichen:

- Windows Systemstart-Kennwörter und Administratorkennwörter verwalten.
- Sonstige Authentifizierungsfunktionen für den Systemstart konfigurieren, z. B. Aktivieren der Embedded Security-Authentifizierung.
- Aktivieren und Deaktivieren von Hardwarefunktionen, wie beispielsweise das Starten von Wechseldatenträgern oder verschiedene Hardwareanschlüsse.
- Bootoptionen konfigurieren, z. B. Aktivieren von MultiBoot und Ändern der Bootreihenfolge.

HINWEIS: Alle in BIOS Configuration for HP ProtectTools enthaltenen Funktionen sind auch in F10 Setup verfügbar. Genaue Anleitungen zur Verwendung von F10 Setup finden Sie im *Computer Setup (F10) Utility-Handbuch*, das mit Ihrem Computer oder dem BIOS-Update geliefert wurde.

Allgemeine Aufgaben

Mit BIOS Configuration können Sie verschiedene Computereinstellungen verwalten, auf die Sie ansonsten nur durch Drücken der Taste F10 während des Starts zum Aufrufen des Computer Setup zugreifen könnten.

Zugriff auf BIOS Configuration

So greifen Sie auf BIOS Configuration zu:

1. Klicken Sie auf **Start**, dann auf **Einstellungen** und anschließend auf **Systemsteuerung**.
2. Klicken Sie auf **HP ProtectTools Security Manager for Administrators** und anschließend auf **BIOS Configuration**.

   Sie können auch über ein Symbol ganz rechts in der Taskleiste im Infobereich auf BIOS Configuration zugreifen.

   HINWEIS: Um das Symbol „HP ProtectTools Security Manager for Administrators“ anzuzeigen, müssen Sie im Infobereich möglicherweise auf **Ausgeblendete Symbole einblenden** (**<** oder **<<**) klicken.

   - Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools Security Manager for Administrators** im Infobereich.
   - Klicken Sie auf **BIOS Configuration**.
3. Geben Sie Ihr Windows Kennwort ein, wenn Sie Benutzer von HP ProtectTools sind.
   - Wenn Sie das Windows Kennwort richtig eingeben, aber kein BIOS-Administrator sind, haben Sie nur eingeschränkte Möglichkeiten zum Vornehmen von Änderungen. Diese entsprechen den Einstellungen für die Sicherheitsstufe.

     HINWEIS: Ein Benutzer von HP ProtectTools kann ein BIOS-Administrator sein oder auch nicht.
   - Wenn Sie das Windows Kennwort falsch eingeben, können Sie die BIOS-Konfigurationseinstellungen nur anzeigen, aber nicht ändern.
4. Wenn Sie kein Benutzer von HP ProtectTools sind, prüft die BIOS Configuration-Software, ob ein BIOS-Administrator-Kennwort eingerichtet wurde.
   - Wenn ein BIOS-Administrator-Kennwort eingerichtet wurde, müssen Sie es eingeben.
     - Wenn Sie das BIOS-Administrator-Kennwort richtig eingeben, können Sie die BIOS-Konfigurationseinstellungen anzeigen und ändern.
     - Wenn ein BIOS-Administrator-Kennwort eingerichtet wurde, Sie das Kennwort aber falsch oder überhaupt nicht eingeben, können Sie die BIOS-Konfigurationseinstellungen anzeigen, aber nicht ändern.
   - Wurde kein BIOS-Administrator-Kennwort eingerichtet, so können Sie die BIOS-Konfigurationseinstellungen sowohl anzeigen als auch ändern.

Anzeigen oder Ändern der Einstellungen

So zeigen Sie Konfigurationseinstellungen an oder ändern sie:

1. Klicken Sie auf eine der BIOS Configuration-Seiten.
2. Nehmen Sie die Änderungen vor, und klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.
3. Beenden Sie das Programm, und starten Sie den Computer neu.

   Die Änderungen werden beim Neustart des Computers wirksam.

HINWEIS: Kennwortänderungen werden ohne Neustart des Computers wirksam.

File (Datei)

Die Option File in BIOS Configuration for HP ProtectTools bietet Angaben zum System wie den Prozessortyp, den Namen und die Version des System-BIOS, Gehäuse, Seriennummer usw. Die einzige Dateiangabe, die bearbeitet werden kann, ist die Bestandsnummer. Alle anderen Daten sind schreibgeschützt.

HINWEIS: Weitere Informationen zu Dateioptionen finden Sie im *Computer Setup (F10) Utility-Handbuch*.

Storage (Speicher)

Die Option Storage in BIOS Configuration for HP ProtectTools liefert Informationen zu allen bootfähigen Geräten, die im Computersystem konfiguriert sind und ermöglicht es Ihnen, Einstellungen für diese Geräte festzulegen. Folgende Einstellungen stehen unter Storage zur Verfügung:

- Device Configuration (Gerätekonfiguration)
- Storage Options (Speicheroptionen)
- DPS Self-Test (DPS-Selbsttest)
- Boot Order (Startreihenfolge)

HINWEIS: Weitere Informationen zu Speicheroptionen finden Sie im *Computer Setup (F10) Utility-Handbuch*.

Security (Sicherheit)

Mit Hilfe der Option Security in BIOS Configuration for HP ProtectTools lassen sich zentral alle Einstellungen vornehmen, die sich auf Sicherheit und Kennwörter beziehen. Dabei handelt es sich um:

- Setup Password (Setup-Kennwort)
- Power-On Password (Kennwort für den Systemstart)
- Password Options (Kennwortoptionen)
- Smart Cover (bestimmte Modelle)
- Device Security (Gerätesicherheit)

- Network Service Boot (Starten über Netzwerk)
- System IDs (System-IDs)
- DriveLock Security (DriveLock-Sicherheitsfunktion)
- System Security (Systemsicherheit) (bestimmte Modelle)
- Setup Security Level (Setup-Schutzstufe)

HINWEIS: Weitere Informationen zu Sicherheitsoptionen finden Sie im *Computer Setup (F10) Utility-Handbuch*.

Power (Energieverwaltung)

Die Option Power in BIOS Configuration for HP ProtectTools umfasst Einstellungen, welche die Energieverwaltung auf Hardwareebene steuern. Dabei handelt es sich um folgende Einstellungen:

- OS Power Management (Betriebssystem-Energieverwaltung)
- Hardware Power Management (Hardware-Energieverwaltung)
- Thermal (Thermosensor)

HINWEIS: Weitere Informationen zu Energieoptionen finden Sie im *Computer Setup (F10) Utility-Handbuch*.

Advanced (Erweitert)

Die Einstellungen der Option Advanced in BIOS Configuration for HP ProtectTools richten sich an fortgeschrittene Benutzer. Dabei handelt es sich um folgende Einstellungen:

- Power-On Options (Optionen für den Systemstart)
- Execute Memory Test (Speichertest durchführen) (bestimmte Modelle)
- BIOS Power-On (BIOS-Aktivierung)
- Onboard Devices (Integrierte Komponenten)
- PCI Devices (PCI-Geräte)
- PCI VGA Configuration (PCI-VGA-Konfiguration)
- Bus Options (Busoptionen)
- Device Options (Geräteoptionen)
- Verwaltungsgeräte
- Verwaltungsvorgänge

HINWEIS: Weitere Informationen zu erweiterten Optionen finden Sie im *Computer Setup (F10) Utility-Handbuch*.

9 Embedded Security for HP ProtectTools

HINWEIS: Der TPM-Chip (Trusted Platform Module) für integrierte Sicherheit muss im Computer installiert sein, um Embedded Security for HP ProtectTools zu verwenden.

Embedded Security for HP ProtectTools schützt vor unberechtigtem Zugriff auf Benutzerdaten oder Berechtigungen. Dieses Softwaremodul enthält folgende Sicherheitsfunktionen:

- Enhanced Microsoft® Encryption File System (EFS)-Datei und Ordnerverschlüsselung
- Erstellen eines PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk) zum Schutz der Benutzerdaten
- Datenverwaltungsfunktionen, wie Sichern und Wiederherstellen der Haupthierarchie
- Unterstützung für Anwendungen von Fremdherstellern (wie Microsoft Outlook und Internet Explorer) für geschützte digitale Zertifikatoperationen bei der Verwendung der Embedded Security Software

Mit dem TPM-Sicherheitschip werden HP ProtectTools Security Manager for Administrators-Sicherheitsfunktionen erweitert und aktiviert. Credential Manager for HP ProtectTools kann den eingebetteten Chip beispielsweise als Authentifizierungsfaktor verwenden, wenn sich Benutzer bei Windows anmelden. Auf bestimmten Modellen aktiviert der TPM-Sicherheitschip auch erweiterte BIOS-Sicherheitsfunktionen, auf die über BIOS Configuration for HP ProtectTools zugegriffen wird.

Setup-Verfahren

△ **ACHTUNG:** Es wird dringend empfohlen, dass der IT-Administrator den Chip für integrierte Sicherheit unverzüglich initialisiert, um das Sicherheitsrisiko zu verringern. Andernfalls kann ein unberechtigter Benutzer, ein Computerwurm oder ein Virus den Computer übernehmen und Eigentümeraufgaben, wie Verwalten des Archivs für Notfallwiederherstellung und Konfigurieren der Benutzerzugriffseinstellungen, ausführen.

Führen Sie die in den folgenden beiden Abschnitten aufgeführten Schritte aus, und initialisieren Sie den Chip für integrierte Sicherheit.

Aktivieren des eingebetteten Sicherheitschips in Computer Setup.

Der eingebettete Sicherheitschip kann im Assistenten für die Schnellinitialisierung oder im Dienstprogramm „Computer Setup“ aktiviert werden (siehe unten). Dieser Vorgang kann nicht in BIOS Configuration for HP ProtectTools durchgeführt werden.

So aktivieren Sie den eingebetteten Sicherheitschip in Computer Setup:

1. Öffnen Sie Computer Setup, indem Sie den Computer einschalten oder neu starten und die Taste F10 drücken, während die Meldung „F10 = ROM Based Setup“ unten links auf dem Bildschirm angezeigt wird.
2. Wenn Sie noch kein Administratorkennwort eingerichtet haben, wählen Sie mit den Pfeiltasten die Option **Sicherheit** und dann **Setup password** (Setup-Kennwort) aus, und drücken Sie die Eingabetaste.
3. Geben Sie ein Kennwort in die Felder **Neues Kennwort** und **Neues Kennwort bestätigen** ein, und drücken Sie anschließend F10.
4. Wählen Sie im Menü **Sicherheit** mit den Pfeiltasten **TPM Embedded Security** aus, und drücken Sie die Eingabetaste.
5. Wählen Sie unter **Embedded Security** die Option **Verfügbar** aus, wenn das Gerät ausgeblendet ist.
6. Wählen Sie **Embedded security device state** (Gerätestatus für Embedded Security), und ändern Sie die Option in **Aktivieren**.
7. Drücken Sie F10, um die Änderungen an der Embedded Security-Konfiguration zu akzeptieren.
8. Um Ihre Einstellungen zu speichern und Computer Setup zu verlassen, wählen Sie mithilfe der Pfeiltasten die Option **Datei** und dann **Änderungen speichern und beenden**. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

Initialisieren des Chips für integrierte Sicherheit

Während des Initialisierungsvorgangs für Embedded Security führen Sie Folgendes aus:

- Richten Sie ein Eigentümerkennwort für den Chip für integrierte Sicherheit ein, um den Zugriff auf alle Eigentümerfunktionen auf dem Chip für integrierte Sicherheit zu schützen.
- Richten Sie das Archiv für die Notfallwiederherstellung ein. Hierbei handelt es sich um einen geschützten Speicherbereich, der die erneute Verschlüsselung der allgemeinen Benutzerschlüssel für alle Benutzer ermöglicht.

So initialisieren Sie den Chip für integrierte Sicherheit:

1. Klicken Sie im Infobereich, ganz rechts in der Taskleiste, mit der rechten Maustaste auf das Symbol „HP ProtectTools Security Manager for Administrators“, und wählen Sie **Embedded Security Initialization** (Embedded Security-Initialisierung).

   Der Assistent für die Initialisierung der HP ProtectTools Embedded Security wird geöffnet.

2. Folgen Sie den Anleitungen auf dem Bildschirm.

Einrichten von allgemeinen Benutzerkonten

Die Einrichtung eines allgemeinen Benutzerkontos in Embedded Security führt Folgendes aus:

- Erstellt einen allgemeinen Benutzerschlüssel, der die verschlüsselten Informationen schützt, und richtet ein Kennwort für den allgemeinen Benutzerschlüssel ein, um diesen zu schützen.
- Richtet ein PSD (Personal Secure Drive, persönliches Sicherheitslaufwerk) zum Speichern verschlüsselter Dateien und Ordner ein.

△ **ACHTUNG:** Bewahren Sie das Kennwort für den allgemeinen Benutzerschlüssel sorgfältig auf. Der Zugriff auf oder die Wiederherstellung von verschlüsselten Informationen ist ohne dieses Kennwort nicht möglich.

So richten Sie ein allgemeines Benutzerkonto ein und aktivieren die Sicherheitsfunktionen für den Benutzer:

1. Wenn der Assistent zur Benutzerinitialisierung bei Embedded Security nicht geöffnet ist, klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Benutzereinstellungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Embedded Security Features** (Embedded Security-Funktionen) auf **Konfigurieren**.

   Der Assistent für die Benutzerinitialisierung der Embedded Security wird geöffnet.

4. Folgen Sie den Anleitungen auf dem Bildschirm.

HINWEIS: Um die Funktionalität sicherer E-Mails verwenden zu können, müssen Sie zunächst Ihr E-Mail-Programm so konfigurieren, dass es ein digitales Zertifikat verwendet, das mit Embedded Security erstellt wurde. Wenn kein digitales Zertifikat verfügbar ist, müssen Sie eines von einer Zertifizierungsstelle beziehen. Anleitungen zur Konfiguration Ihres E-Mail-Programms und zum Bezug eines digitalen Zertifikats finden Sie in der Hilfe Ihres E-Mail-Programms.

Allgemeine Aufgaben

Nachdem das allgemeine Benutzerkonto eingerichtet wurde, können Sie folgende Aufgaben ausführen:

- Verschlüsseln von Dateien und Ordnern
- Senden und Empfangen verschlüsselter E-Mails

PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk)

Nachdem Sie das PSD eingerichtet haben, werden Sie aufgefordert, das Kennwort für den allgemeinen Benutzerschlüssel bei der nächsten Anmeldung einzugeben. Wenn Sie das Kennwort für den allgemeinen Benutzerschlüssel richtig eingegeben haben, können Sie im Windows Explorer direkt auf das PSD zugreifen.

Verschlüsseln von Dateien und Ordnern

Beachten Sie bei der Arbeit mit verschlüsselten Dateien die folgenden Regeln:

- Sie können nur Dateien und Ordner in NTFS-Partitionen verschlüsseln. Dateien und Ordner in FAT-Partitionen können nicht verschlüsselt werden.
- Systemdateien und komprimierte Dateien können nicht verschlüsselt werden. Verschlüsselte Dateien können nicht komprimiert werden.
- Temporäre Ordner müssen verschlüsselt werden, weil sich Hacker für diese interessieren.
- Wenn Sie eine Datei oder einen Ordner erstmals verschlüsseln, wird automatisch eine Richtlinie für die Wiederherstellung eingerichtet. Diese Richtlinie gewährleistet, dass Sie bei Verlust der Verschlüsselungszertifikate und privaten Schlüssel einen Wiederherstellungs-Agent zum Entschlüsseln Ihrer Informationen verwenden können.

So verschlüsseln Sie Dateien und Ordner:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die bzw. den Sie verschlüsseln möchten.
2. Klicken Sie auf **Verschlüsseln**.
3. Klicken Sie auf eine der folgenden Optionen:
   - **Änderungen nur für diesen Ordner übernehmen.**
   - **Änderungen für diesen Ordner, untergeordnete Ordner und Dateien übernehmen.**
4. Klicken Sie auf **OK**.

Senden und Empfangen verschlüsselter E-Mails

Embedded Security ermöglicht das Senden und Empfangen verschlüsselter E-Mails. Der genaue Vorgang ist jedoch von dem Programm abhängig, mit dem Sie Ihre E-Mails bearbeiten. Weitere Informationen hierzu finden Sie in der Hilfe von Embedded Security und Ihres E-Mail-Programms.

Ändern des Kennworts für den allgemeinen Benutzerschlüssel

So ändern Sie das Kennwort für den allgemeinen Benutzerschlüssel:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Benutzereinstellungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Basic User Key password** (Kennwort für allgemeinen Benutzerschlüssel) auf **Ändern**.
4. Geben Sie zuerst das alte Kennwort ein. Geben Sie dann das neue Kennwort ein, und bestätigen Sie das neue Kennwort.
5. Klicken Sie auf **OK**.

Erweiterte Aufgaben

Sichern und Wiederherstellen

Mit der Sicherungsfunktion von Embedded Security erstellen Sie ein Archiv, das Zertifizierungsinformationen enthält, die bei einem Notfall wiederhergestellt werden.

Erstellen einer Sicherungsdatei

So erstellen Sie eine Sicherungsdatei:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Fensterausschnitt auf **Sicherung**. Der HP Embedded Security for ProtectTools Backup-Assistent wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Wiederherstellen von Daten aus der Sicherungsdatei

So stellen Sie die Daten aus der Sicherungsdatei wieder her:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Fensterausschnitt auf **Wiederherstellen**. Der HP Embedded Security for ProtectTools Backup-Assistent wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Ändern des Eigentümerkennworts

So ändern Sie das Eigentümerkennwort:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Erweitert**.
3. Klicken Sie im rechten Fensterausschnitt unter **Owner Password** (Eigentümerkennwort) auf **Ändern**.
4. Geben Sie zuerst das alte Eigentümerkennwort ein. Geben Sie dann das neue Eigentümerkennwort ein, und bestätigen Sie das neue Kennwort.
5. Klicken Sie auf **OK**.

Erneutes Einrichten eines Benutzerkennworts

Der Administrator kann Benutzer beim Zurücksetzen vergessener Kennwörter unterstützen. Weitere Informationen finden Sie in der Software-Hilfe.

Aktivieren und Deaktivieren von Embedded Security

Sie können die Embedded Security-Funktionen deaktivieren, wenn Sie ohne die Sicherheitsfunktionen arbeiten möchten.

Sie können die Embedded Security-Funktionen auf 2 verschiedenen Stufen aktivieren oder deaktivieren:

- Temporary disabling (Vorübergehend deaktivieren) – Mit dieser Option wird Embedded Security automatisch reaktiviert, sobald Sie Windows erneut starten. Diese Option steht standardmäßig allen Benutzern zur Verfügung.
- Permanent disabling (Permanent deaktivieren) – Mit dieser Option wird Embedded Security erst reaktiviert, nachdem Sie das Eigentümerkennwort eingegeben haben. Diese Option steht nur den Administratoren zur Verfügung.

Permanentes Deaktivieren von Embedded Security

So deaktivieren Sie Embedded Security permanent:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Erweitert**.
3. Klicken Sie im rechten Fensterausschnitt unter **Embedded Security** auf **Deaktivieren**.
4. Geben Sie an der Eingabeaufforderung das Eigentümerkennwort ein, und klicken Sie dann auf **OK**.

Aktivieren von Embedded Security nach der permanenten Deaktivierung

So aktivieren Sie Embedded Security nach der permanenten Deaktivierung:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Erweitert**.
3. Klicken Sie im rechten Fensterausschnitt unter **Embedded Security** auf **Aktivieren**.
4. Geben Sie an der Eingabeaufforderung das Eigentümerkennwort ein, und klicken Sie dann auf **OK**.

Migrieren von Schlüsseln mithilfe des Migrationsassistenten

Bei der Migration handelt es sich um eine erweiterte Administratoraufgabe. Sie ermöglicht das Verwalten, Wiederherstellen und Übertragen von Schlüsseln und Zertifikaten.

Weitere Informationen zur Migration finden Sie in der Hilfe von Embedded Security.

10 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

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, wird von HP ProtectTools Security Manager for Administrators ein Dialogfeld geöffnet, 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

Mit dieser Funktion können Sie folgenden Geräteklassen den Zugriff verweigern:

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

Gehen Sie folgendermaßen vor, um den Zugriff auf eine Geräteklasse für alle Nicht-Administratoren zu verweigern:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Device Access Manager** und anschließend auf **Simple Configuration** (Einfache Konfiguration).
3. Aktivieren Sie im rechten Fensterausschnitt das Kontrollkästchen eines Geräts, dem Sie den Zugriff verweigern möchten.

4. Klicken Sie auf **Übernehmen**.

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 Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
3. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.
4. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Select Users or Groups** (Benutzer oder Gruppen auswählen) wird geöffnet.
5. Klicken Sie auf **Advanced** (Erweitert) und dann auf **Find Now** (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 Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Device Access Manager** und anschließend 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**.
5. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Verweigern des Zugriffs für einen Benutzer oder eine Gruppe

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager for Administrators** unter Windows Vista bzw. **HP ProtectTools Security Manager** unter Windows XP.
2. Klicken Sie im linken Fensterausschnitt auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
3. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.
4. Klicken Sie unter **User/Groups** (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 **Übernehmen** und dann auf **OK**.

11 Fehlerbeseitigung

Credential Manager for HP ProtectTools

Kurzbeschreibung	Einzelheiten	Lösung
Mit der Option „Network Accounts“ von Credential Manager kann ein Benutzer auswählen, bei welchem Domänenkonto er sich anmelden möchte. Wenn die TPM-Authentifizierung verwendet wird, steht diese Option nicht zur Verfügung. Alle übrigen Authentifizierungsmethoden stehen in vollem Umfang zur Auswahl.	Bei der TPM-Authentifizierung ist der Benutzer nur auf dem lokalen Computer angemeldet.	Die SSO-Tools von Credential Manager ermöglichen dem Benutzer auch die Authentifizierung anderer Konten.
Smart Cards und USB-Token sind in Credential Manager nicht verfügbar, wenn sie erst nach der Installation von Credential Manager installiert wurden.	Um Smart Cards oder USB-Token in Credential Manager verwenden zu können, muss die unterstützende Software (Treiber, PKCS#11-Anbieter usw.) vor der Installation von Credential Manager installiert werden. Wenn Sie Credential Manager bereits installiert haben, gehen Sie nach der Installation der Unterstützungssoftware für Smart Cards oder USB-Token folgendermaßen vor:	Melden Sie sich bei Credential Manager an. Wählen Sie im HP ProtectTools Security Manager die Option **Credential Manager**, klicken Sie auf **Erweiterte Einstellungen** und dann auf die Registerkarte **Smart Cards und Token**. Es wird eine Liste der verfügbaren Token angezeigt. Klicken Sie mit der rechten Maustaste auf den Knoten **Local Tokens** (Lokale Token), und wählen Sie im Popup-Menü die Option **Scan for New Smart Cards and Tokens** (Nach neuen Smart Cards und Token suchen). Starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.
Bestimmte Webseiten von Anwendungen erzeugen Fehler, infolge derer der Benutzer die gewünschten Aufgaben nicht durchführen oder abschließen kann.	Aufgrund der Single Sign On-Funktion wird die Ausführung bestimmter webbasierter Anwendungen beendet, und es werden Fehlermeldungen angezeigt. So weist im Internet Explorer ein **!** in einem gelben Dreieck z. B. darauf hin, dass ein Fehler aufgetreten ist.	Credential Manager Single Sign-On unterstützt nicht alle Web-Schnittstellen der Software. Deaktivieren Sie die Single Sign-On-Unterstützung für die jeweilige Web-Seite. Siehe dazu die vollständige Dokumentation über Single Sign-On in den Software-Hilfedateien des Credential Manager. Wenn sich Single Sign On für eine konkrete Anwendung nicht deaktivieren lässt, wenden Sie sich an den HP Techniksupport und bitten um Third-Level-Support über Ihren HP Service-Ansprechpartner.
Bei der Anmeldung wird die Option **Browse for Virtual Token** (Nach	Der Benutzer kann den Speicherort eines registrierten virtuellen Token in Credential Manager nicht ändern, da die	Durch die Entfernung der Durchsuchen-Option soll verhindert werden, dass unbefugte Benutzer Dateien

Kurzbeschreibung	Einzelheiten	Lösung
virtuellem Token suchen) nicht angezeigt.	Durchsuchen-Option aus Sicherheitsgründen entfernt wurde.	löschen oder umbenennen bzw. Windows nutzen können.
Domänenadministratoren können das Windows Kennwort selbst mit Autorisation nicht ändern.	Das Problem tritt auf, nachdem sich ein Domänenadministrator an einer Domäne angemeldet und die Domänenidentität unter Verwendung eines Kontos mit Administratorrechten für die Domäne und den lokalen Computer mit Credential Manager registriert hat. Wenn der Domänenadministrator versucht, das Windows Kennwort über Credential Manager zu ändern, wird folgender Anmeldungsfehler zurückgegeben: **User account restriction** (Benutzerkontenbeschränkung).	Credential Manager kann das Kontokennwort eines Domain-Benutzers nicht über die Funktion **Windows Anmeldekennwort ändern** ändern. Credential Manager kann nur die Kennwörter der lokalen PC-Accounts ändern. Der Domain-Benutzer kann sein Kennwort mithilfe der Option **Kennwort ändern** in **Windows Sicherheit** ändern, da er aber kein physikalisches Konto auf dem lokalen PC hat, kann Credential Manager nur das zum Anmelden verwendete Kennwort ändern.
Credential Manager ist mit dem GINA-Kennwortschutz in Corel WordPerfect 12 nicht kompatibel.	Wenn sich der Benutzer bei Credential Manager anmeldet, ein Dokument in WordPerfect erstellt und es mit Kennwortschutz speichert, kann Credential Manager weder eine manuelle noch eine automatische Erkennung des GINA-Kennworts durchführen.	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.
Credential Manager erkennt die Schaltfläche **Connect** (Verbinden) auf dem Bildschirm nicht.	Wenn für die SSO-Zugangsdaten für Remote Desktop Connection (RDP) beim erneuten Starten von Single Sign On **Connect** (Verbinden) festgelegt wurde, wird jedes Mal **Save As** (Speichern unter) anstelle von **Connect** (Verbinden) angezeigt.	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.
Die Benutzer können alle durch das TPM geschützten Zugangsdaten für Credential Manager verlieren.	Wenn das TPM-Modul entfernt oder beschädigt wird, verlieren die Benutzer alle durch das TPM geschützten Zugangsdaten.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Das TPM-Modul wurde für den Schutz der Credential Manager Zugangsdaten konzipiert. HP empfiehlt den Benutzern daher die Sicherung ihrer Credential Manager Identität, bevor sie das TPM-Modul entfernen.
Nach dem Wechsel vom Energiesparmodus (Sleep) in den Ruhezustand (Hibernation) kann sich der Benutzer nicht bei Credential Manager anmelden. Dies betrifft ausschließlich Systeme mit Windows XP Service Pack 1.	Nach dem Wechsel in den Ruhezustand oder den Energiesparmodus kann sich der Administrator oder Benutzer nicht bei Credential Manager anmelden, und der Windows Anmeldebildschirm wird angezeigt, unabhängig davon, welche Zugangsmethode (Kennwort, Fingerabdruck oder Java Card) ausgewählt werden.	Aktualisieren Sie Windows mithilfe der Windows Update-Funktion auf Service Pack 2. Zur Ursache des Problems siehe auch den Artikel Nummer 813301 in der Microsoft Knowledge Base unter http://www.microsoft.com. Für die Anmeldung muss der Benutzer Credential Manager auswählen und sich dann anmelden. Nach der Anmeldung bei Credential Manager wird der Benutzer aufgefordert, sich bei Windows anzumelden (hierfür muss er unter Umständen die Windows Anmeldeoption auswählen), um den Anmeldevorgang abzuschließen. Wenn sich der Benutzer zuerst bei Windows anmeldet, muss er sich im Anschluss daran manuell bei Credential Manager anmelden.
Bei der Wiederherstellung von Embedded Security	Die Registrierung der Zugangsdaten in Credential Manager schlägt fehl,	Der Zugriff von Credential Manager auf den TPM-Chip schlägt fehl, wenn der ROM nach der Installation von

Kurzbeschreibung	Einzelheiten	Lösung
schlägt Credential Manager fehl.	nachdem die Werkseinstellungen des ROM wiederhergestellt wurden.	Credential Manager auf die Werkseinstellungen zurückgesetzt wird. Der TPM-Chip für integrierte Sicherheit kann mit F10 Computer Setup, BIOS Configuration oder HP Client Manager aktiviert werden. Zur Aktivierung des Chips für integrierte Sicherheit mittels Computer Setup gehen Sie folgendermaßen vor: 1. Öffnen Sie Computer Setup, indem Sie den Computer einschalten oder neu starten und die Taste F10 drücken, während die Meldung **F10 = ROM Based Setup** unten links auf dem Bildschirm angezeigt wird. 2. Wählen Sie mit den Pfeiltasten die Option **Sicherheit** und dann **Setup-Kennwort**. Legen Sie ein Kennwort fest. 3. Wählen Sie **Embedded Security Device** (Chip für integrierte Sicherheit). 4. Wählen Sie mit den Pfeiltasten **Embedded Security Device – Disable** (Chip für integrierte Sicherheit – Deaktivieren). Ändern Sie die Einstellung mit den Pfeiltasten auf **Embedded Security Device – Enable** (Chip für integrierte Sicherheit – Aktivieren). 5. Klicken Sie auf **Aktivieren** und dann auf **Änderungen speichern und beenden**. HP arbeitet derzeitig an Lösungsmöglichkeiten für zukünftige Software-Versionen.
Beim Sicherheitsprozess **Restore Identity** (Identität wiederherstellen) geht die Verknüpfung mit dem virtuellen Token verloren.	Wenn der Benutzer die Identität wiederherstellt, kann es geschehen, dass Credential Manager die Verknüpfung mit dem Speicherort des virtuellen Token auf dem Anmeldebildschirm verliert. Obwohl Credential Manager das virtuelle Token registriert hat, muss der Benutzer es in diesem Fall erneut registrieren, um die Verknüpfung wiederherzustellen.	Dies ist zurzeit das beabsichtigte Standardverhalten der Anwendung. Wenn bei der Deinstallation von Credential Manager die Identitäten nicht beibehalten werden, wird der System- (bzw. Server-) Teil des Token eliminiert, so dass das Token nicht mehr für die Anmeldung verwendet werden kann. Dies gilt auch dann, wenn der Client-Teil des Token mittels Identitätswiederherstellung wiederhergestellt wird. HP untersucht langfristige Optionen zur Behebung des Problems.

Embedded Security for HP ProtectTools

Kurzbeschreibung	Einzelheiten	Lösung
Die Verschlüsselung von Ordnern, Unterordnern und Dateien auf einem PSD führt zur Anzeige einer Fehlermeldung.	Wenn der Benutzer Dateien und Ordner auf das PSD kopiert und versucht, Ordner/Dateien oder Ordner/Unterordner zu verschlüsseln, wird die Meldung **Error Applying Attributes** (Fehler bei der Attribut-Übernahme) angezeigt. Der Benutzer kann diese Dateien auf Laufwerk C:\ oder auf einer zusätzlich installierten Festplatte verschlüsseln.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Wenn die Dateien/Ordner auf das PSD verschoben werden, werden sie automatisch verschlüsselt. Eine doppelte Verschlüsselung ist überflüssig. Wenn der Benutzer auf dem PSD mittels EFS eine derartige doppelte Verschlüsselung versucht, wird die obige Fehlermeldung angezeigt.
Die Eigentumsrechte können auf einer Mehrfachboot-Plattform nicht in ein anderes Betriebssystem übernommen werden.	Wenn ein Laufwerk für den Start mehrerer Betriebssysteme eingerichtet ist, können die Eigentumsrechte nur vom Assistenten für die Plattforminitialisierung eines Betriebssystems übernommen werden.	Dies ist das aus Sicherheitsgründen vorgesehene Standardverhalten.
Ein unbefugter Administrator kann den Inhalt verschlüsselter EFS-Ordner anzeigen lassen, löschen, umbenennen und verschieben.	Inhalte verschlüsselter Ordner können von unbefugten Benutzern mit administrativen Rechten angezeigt, gelöscht oder verschoben werden.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Hierbei handelt es sich um eine Funktion von EFS und nicht des Embedded Security-TPM. Embedded Security verwendet Microsoft EFS-Software, die allen Administratoren Zugriffsrechte für Dateien und Ordner zuweist.
Dem Benutzer stehen keine Verschlüsselungsoptionen zur Verfügung, wenn er die Festplatte unter Verwendung des FAT32-Dateisystems verschlüsseln möchte.	Wenn der Benutzer versucht, die Festplatte unter Verwendung des FAT32-Dateisystems wiederherzustellen, stehen keine EFS-Verschlüsselungsoptionen für Dateien und Ordner zur Verfügung.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Software sollte nicht auf einem wiederhergestellten Laufwerk mit einer FAT32-Partition installiert werden. Microsoft EFS wird nur für NTFS- und nicht für FAT32-Partitionen unterstützt. Dies ist eine Funktion von Microsoft EFS und steht nicht mit der HP ProtectTools Software in Zusammenhang.
Der Benutzer kann die XML-Datei des Wiederherstellungsarchivs verschlüsseln bzw. löschen.	Die ACLs für diesen Ordner sind standardmäßig nicht definiert; somit kann ein Benutzer die Datei absichtlich oder nicht absichtlich verschlüsseln oder löschen, so dass kein Zugriff darauf mehr möglich ist. Nach der Verschlüsselung bzw. dem Löschen der Datei, kann die TPM-Software nicht mehr genutzt werden.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Die Benutzer sind zum Zugriff auf ein Notfallarchiv berechtigt, in dem sie die Sicherungskopie ihres allgemeinen Benutzerschlüssels sichern/aktualisieren zu können. Sie sollten darauf hingewiesen werden, dass die Dateien des Wiederherstellungsarchivs in keinem Fall verschlüsselt oder gelöscht werden dürfen.
Die Interaktion von Embedded Security EFS mit Symantec Antivirus oder McAfee Total Protection führt zu längeren Ver-/Entschlüsselungszeiten und Suchzeiten.	Verschlüsselte Dateien vertragen sich schlecht mit der Virensuche von Symantec Antivirus oder McAfee Total Protection. Die Verschlüsselung von Dateien mit Embedded Security EFS dauert länger, wenn Symantec Antivirus oder McAfee Total Protection ausgeführt wird.	Um die Scan-Dauer für Embedded Security EFS-Dateien zu verkürzen, kann der Benutzer entweder vor dem Scannen das Verschlüsselungskennwort eingeben oder die Dateien entschlüsseln. Um die Ver-/Entschlüsselungszeit mit Embedded Security EFS zu verkürzen, sollte der Benutzer die Auto-Protect-Funktion in Symantec Antivirus oder McAfee Total Protection deaktivieren.
Das Archiv für die Notfallwiederherstellung kann nicht auf einem	Wenn der Benutzer eine MultiMediaCard oder eine Secure Digital (SD) Memory Card einlegt, wenn er während der Initialisierung von Embedded Security	Dies ist das beabsichtigte Standardverhalten der Anwendung.

Kurzbeschreibung	Einzelheiten	Lösung
Wechselmedium gesichert werden.	den Pfad für das Notfallarchiv angibt, wird eine Fehlermeldung angezeigt.	Das Wiederherstellungsarchiv kann nicht auf Wechselmedien gespeichert werden. Eine Speicherung ist lediglich auf einem Netzlaufwerk oder einem anderen lokalen Laufwerk (nicht Laufwerk C:\) möglich.
Nachdem die Initialisierung von Embedded Security durch einen Stromausfall unterbrochen wurde, treten Fehler auf.	Nachdem es bei der Initialisierung des Chips für integrierte Sicherheit zu einem Stromausfall gekommen ist, treten die folgenden Fehler auf: • Beim Versuch, den Assistenten für die Initialisierung von Embedded Security zu starten, wird die folgende Fehlermeldung angezeigt: **The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner.** (Embedded Security kann nicht initialisiert werden, da für den Chip für integrierte Sicherheit bereits ein Embedded Security Eigentümer definiert wurde.) • Beim Versuch, den Assistenten für die Benutzerinitialisierung zu starten, wird die folgende Fehlermeldung angezeigt: **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.** (Embedded Security wurde nicht initialisiert. Sie können den Assistenten erst nach der Initialisierung von Embedded Security verwenden.)	Führen Sie nach einem Stromausfall folgende Aktionen durch: **HINWEIS:** Verwenden Sie die Pfeiltasten, um verschiedene Menüs und Menüoptionen auszuwählen und Werte zu ändern (sofern nicht anderweitig vorgegeben). 1. Starten Sie den Computer, oder führen Sie einen Neustart durch. 2. Drücken Sie F10, sobald die Meldung **F10=Setup** auf dem Bildschirm erscheint. 3. Wählen Sie die entsprechende Option aus. 4. Drücken Sie die Eingabetaste. 5. Wählen Sie **Security** (Sicherheit) und dann **Embedded Security** (Integrierte Sicherheit). 6. Setzen Sie die Option **Embedded Security Device** (Chip für integrierte Sicherheit) auf **Enable** (Aktivieren). 7. Drücken Sie F10, um die Änderung zu übernehmen. 8. Wählen Sie **File** (Datei) und dann **Save Changes and Exit** (Änderungen speichern und beenden). 9. Drücken Sie die Eingabetaste. 10. Drücken Sie F10, um die Änderungen zu speichern und das Dienstprogramm zu verlassen.
Das Kennwort für Computer Setup (F10) Utility kann entfernt werden, nachdem das TPM-Modul aktiviert wurde.	Zur Aktivierung des TPM-Moduls wird ein Kennwort für Computer Setup (F10) Utility benötigt. Nachdem das Modul aktiviert wurde, kann der Benutzer das Kennwort entfernen. Auf diese Weise kann allerdings jeder Benutzer mit direktem Zugriff auf das System das TPM-Modul zurücksetzen und somit einen Datenverlust verursachen.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Das Kennwort für Computer Setup (F10) Utility kann nur von einem Benutzer entfernt werden, der das betreffende Kennwort kennt. HP empfiehlt jedoch unbedingt, jederzeit einen optimalen Schutz des Kennworts für Computer Setup (F10) Utility sicherzustellen.
Das Feld für das PSD-Kennwort wird nicht mehr angezeigt, nachdem das System aus dem Standby- in den Normalbetrieb gewechselt ist.	Wenn sich ein Benutzer nach dem Erstellen eines PSD beim System anmeldet, fragt der Sicherheits-Chip nach dem allgemeinen Benutzerkennwort. Wenn der Benutzer das Kennwort nicht eingibt und das System in den Standby-Modus wechselt, wird das Dialogfeld zur Kennworteingabe auch dann nicht mehr angezeigt, wenn der Benutzer fortfahren möchte und das System wieder in den Normalbetrieb wechselt.	Dies entspricht dem Standardverhalten der Anwendung. Der Benutzer muss sich abmelden und dann erneut anmelden, um das Dialogfeld für das PSD-Kennwort wieder anzeigen zu lassen.

Kurzbeschreibung	Einzelheiten	Lösung
Zur Änderung der Richtlinien für die Sicherheitsplattform ist kein Kennwort erforderlich.	Für den Zugriff auf Sicherheitsplattformrichtlinien (Computer und Benutzer) benötigen Benutzer mit administrativen Rechten für das System kein TPM-Kennwort.	Dies entspricht dem Standardverhalten der Anwendung. Alle Administratoren können mit oder ohne Benutzerinitialisierung des TPM die Sicherheitsplattformrichtlinien ändern.
Bei der Anzeige eines Zertifikats wird dieses als „nicht vertrauenswürdig“ gekennzeichnet.	Nachdem HP ProtectTools eingerichtet und der Assistent für die Benutzerinitialisierung ausgeführt wurde, kann der Benutzer das betreffende Zertifikat anzeigen lassen. Dabei wird das Zertifikat jedoch als „nicht vertrauenswürdig“ eingestuft. Das ausgestellte Zertifikat kann nun zwar durch Klicken auf die Installationsschaltfläche installiert werden, es wird dadurch aber nicht automatisch als vertrauenswürdig eingestuft.	Selbst signierte Zertifikate sind nicht vertrauenswürdig. In einer ordnungsgemäß konfigurierten Unternehmensumgebung werden EFS-Zertifikate von Online-Zertifizierungsstellen ausgestellt und werden dann als vertrauenswürdig eingestuft.
Ein intermittierender Verschlüsselungs- und Entschlüsselungsfehler tritt auf: **The process cannot access the file because it is being used by another process.** (Der Prozess kann auf die Datei nicht zugreifen, da sie von einem anderen Prozess verwendet wird.)	Hierbei handelt es sich um einen immer wieder vorkommenden Fehler, der bei der Verschlüsselung und Entschlüsselung von Dateien vorkommt und auftritt, da die Datei von einem anderen Prozess verwendet wird, obwohl die Datei bzw. der Ordner weder vom Betriebssystem noch von anderen Anwendungen verwendet wird.	So beseitigen Sie den Fehler: 1. Starten Sie das System neu. 2. Melden Sie sich ab. 3. Melden Sie sich wieder an.
Bei einem Wechselmedium kommt es zu Datenverlust, wenn das Medium entfernt wird, bevor die Daten vollständig erzeugt oder übertragen wurden.	Wenn dagegen ein Speichermedium (z. B. eine MultiBay-Festplatte) entfernt wird, ist das PSD dennoch verfügbar, und beim Hinzufügen/Ändern von Daten auf dem PSD treten keine Fehler auf. Nach dem Neustart des Systems sind Dateiänderungen, die vorgenommen wurden, während das Wechselmedium nicht verfügbar war, auf dem PSD nicht enthalten.	Entfernen Sie ein PSD erst dann, wenn die Daten vollständig erzeugt bzw. übertragen wurden. Dieses Problem tritt nur dann auf, wenn der Benutzer auf das PSD zugreift und dann die Festplatte entfernt, bevor die betreffenden Daten vollständig erzeugt oder übertragen wurden. Wenn der Benutzer auf das PSD zugreifen möchte und kein Wechselmedium vorhanden ist, wird eine Fehlermeldung angezeigt, die besagt, dass das Gerät nicht bereit ist.
Wenn der Benutzer den allgemeinen Benutzerschlüssel nicht initialisiert hat und das Administration-Tool öffnet, steht bei der Deinstallation die Option **Deaktivieren** nicht zur Verfügung. Uninstaller fährt erst dann mit der Deinstallation fort, wenn das Tool geschlossen wurde.	Der Benutzer kann die Deinstallation entweder ohne Deaktivierung des TPM-Chips durchführen, oder er kann zuerst den TPM-Chip (mit dem Administrator-Tool) deaktivieren und anschließend die Deinstallation vornehmen. Für den Zugriff auf das Administration-Tool muss der allgemeine Benutzerschlüssel initialisiert werden. Wenn dies nicht der Fall ist, steht dem Benutzer keine der Optionen zur Verfügung. Da sich der Benutzer explizit für die Ausführung des Administration-Tools entschieden hat (indem er im Dialogfeld **Click Yes to open Embedded Security Administration tool** (Auf „Ja“ klicken, um das Embedded Security Administration-Tool zu öffnen) auf **Ja**	Das Administration-Tool dient zur Deaktivierung des TPM-Chips, wobei diese Option jedoch nur verfügbar ist, wenn der allgemeine Benutzerschlüssel initialisiert wurde. Wenn dies noch nicht der Fall ist, wählen Sie **OK** oder **Abbrechen**, um mit der Deinstallation fortzufahren.

Kurzbeschreibung	Einzelheiten	Lösung
	geklickt hat), wird die Deinstallation so lange ausgesetzt, bis das Tool geschlossen wurde. Wenn der Benutzer in dem Dialogfeld auf **Nein** klickt, wird das Tool nicht geöffnet und der Deinstallationsvorgang fährt fort.	
Wenn bei einer 128-MB-Systemkonfiguration ein PSD mit zwei Benutzerkonten erstellt und die Fast-User-Switching-Funktion verwendet wird, kommt es zu intermittierenden Systemabstürzen.	Wenn Fast-User-Switching mit einer minimalen RAM-Konfiguration verwendet wird, kann ein Fehler auftreten, bei dem anstelle des Begrüßungs- bzw. Anmeldebildschirms ein schwarzer Bildschirm angezeigt wird und weder Tastatur noch Maus auf Eingaben reagieren.	Die Ursache für diesen Fehler liegt vermutlich in der Zeitsteuerung bei Konfigurationen mit einem geringen Arbeitsspeicher. Die eingebaute Grafik arbeitet mit der UMA-Architektur und benötigt 8 MB RAM, so dass dem Benutzer lediglich 120 MB zur Verfügung stehen. Der Fehler tritt dann auf, wenn diese 120 MB von beiden angemeldeten Benutzern genutzt werden und die Benutzer die Fast-User-Switching-Funktion verwenden. Die Lösung für dieses Problem besteht darin, das System neu zu starten und das System mit mehr RAM zu konfigurieren (HP liefert keine 128-MB-Konfigurationen mit Sicherheitsmodulen aus).
Zeitüberschreitung bei der EFS-Benutzerauthentifizierung (Kennwortanforderung): **Access denied** (Zugriff verweigert).	Die Meldung bei der EFS-Benutzerauthentifizierung (Kennwortanforderung) wird erneut angezeigt, wenn der Benutzer auf **OK** klickt oder das System den Standby-Modus verlässt.	Dies entspricht dem Standardverhalten der Anwendung. Um Probleme mit Microsoft EFS zu verhindern, wurde zum Generieren dieser Fehlermeldung ein 30-Sekunden-Watchdog-Timer erstellt.
Bei der Einrichtung für Japanisch werden Funktionsbeschreibungen teilweise abgeschnitten.	Im Installationsassistenten sind bei der benutzerdefinierten Installation Funktionsbeschreibungen teilweise abgeschnitten.	HP wird dieses Problem in zukünftigen Versionen beheben.
Die EFS-Verschlüsselung funktioniert auch ohne Kennworteingabe.	Durch die Zeitüberschreitung bei der Eingabe eines Benutzerkennworts, lässt sich eine Datei oder ein Ordner auch ohne Kennworteingabe verschlüsseln.	Für die Verschlüsselung ist keine Kennwortauthentifizierung erforderlich, da es sich hierbei um eine Funktion der Microsoft EFS-Verschlüsselt handelt. Für die Entschlüsselung muss dagegen ein Benutzerkennwort eingegeben werden.
Sichere E-Mail wird auch dann unterstützt, wenn dies im Assistenten für die Benutzerinitialisierung anderweitig festgelegt wurde oder wenn eine sichere E-Mail-Konfiguration in den Benutzerrichtlinien deaktiviert ist.	Die Einstellungen eines E-Mail-Clients wie Outlook, Outlook Express oder Netscape werden nicht durch die Embedded Security Software oder den Assistenten gesteuert.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Die Konfiguration von TPM-E-Mail-Einstellungen schließt nicht aus, dass die Verschlüsselungseinstellungen auch direkt in einem E-Mail-Client vorgenommen werden können. Die Verwendung von sicherer E-Mail wird in Anwendungen von Drittherstellern festgelegt und durch diese gesteuert. Der HP Assistent sieht die Verknüpfung zu den drei Referenzanwendungen vor, um so eine unmittelbare individuelle Anpassung zu ermöglichen.
Wenn eine umfangreiche Installation ein zweites Mal auf dem gleichen Computer oder auf einem bereits initialisierten Computer durchgeführt wird, werden die Wiederherstellungs- und Token-Dateien überschrieben. Die neuen Dateien können nicht für	Wenn Large Scale Deployment auf einem bereits initialisierten HP ProtectTools Embedded Security System ausgeführt wird, können bestehende Wiederherstellungsarchive und -Tokens nicht mehr verwendet werden, da die betreffenden XML-Dateien überschrieben werden.	HP arbeitet daran, die Überschreibung der XML-Dateien zu verhindern, und wird in einem zukünftigen SoftPaq eine Lösung anbieten.

Kurzbeschreibung	Einzelheiten	Lösung
eine Wiederherstellung verwendet werden.		
Automatisierte Anmeldeskripte funktionieren nicht, wenn eine Benutzer-wiederherstellung in Embedded Security durchgeführt wird.	Dieser Fehler tritt auf, wenn der Benutzer: • Eigentümer und Benutzer in Embedded Security unter Verwendung des Standardspeicherorts **Eigene Dokumente** initialisiert hat. • den Chip im BIOS auf die Werkseinstellungen zurückgesetzt hat. • den Computer neu startet. • mit der Wiederherstellung von Embedded Security beginnt; während des Wiederherstellungsvorgangs fragt Credential Manager, ob das System die Anmeldung bei der Infineon TPM-Benutzerauthentifizierung automatisch ausführen kann. Wenn der Benutzer **Ja** auswählt, wird im Textfeld automatisch der Speicherort von SPEmRecToken angezeigt. Obwohl der Speicherort korrekt ist, wird die folgende Fehlermeldung angezeigt: **No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.** (Kein Wiederherstellungs-Token vorhanden. Wählen Sie den Speicherort des Wiederherstellungs-Token aus.).	Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um den Speicherort auszuwählen. Der Wiederherstellungsvorgang wird dann fortgesetzt.
PSDs für mehrere Benutzer funktionieren nicht in einer Fast-User-Switching-Umgebung.	Dieser Fehler tritt auf, wenn mehrere Benutzer angelegt wurden und ihnen ein PSD mit demselben Laufwerksbuchstaben zugewiesen wurde. Wenn bei geladenem PSD ein Fast-User-Switching zwischen den Benutzern versucht wird, steht das PSD des zweiten Benutzers nicht zur Verfügung.	Das PSD des zweiten Benutzers steht nur dann zur Verfügung, wenn es mit einem anderen Laufwerksbuchstaben neu konfiguriert wird oder wenn der erste Benutzer abgemeldet ist.
Das PSD ist deaktiviert und kann nach der Formatierung der Festplatte, auf der es angelegt wurde, nicht gelöscht werden.	Das PSD-Symbol wird immer noch angezeigt, obwohl beim Versuch des Zugriffs auf das PSD die Fehlermeldung **drive is not accessible** (Laufwerk nicht verfügbar) erscheint. Der Benutzer kann das PSD nicht löschen, und die folgende Meldung wird angezeigt: **your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process** (Ihr PSD wird noch	Dies entspricht dem Standardverhalten der Anwendung: Wenn ein Kunde den Speicherort der PSD-Daten bewusst löscht oder die Verbindung trennt, funktioniert die PSD-Laufwerksemulation von Embedded Security weiterhin und gibt auf Grund der fehlenden Kommunikation mit den zuvor gelöschten Daten Fehlermeldungen aus. Lösung: Nach dem nächsten Neustart werden die Emulationen nicht geladen. Der Benutzer kann die alte PSD-Emulation löschen und ein neues PSD erstellen.

Kurzbeschreibung	Einzelheiten	Lösung
	genutzt; bitte vergewissern Sie sich, dass Ihr PSD keine geöffneten Dateien enthält und dass kein anderer Prozess darauf zugreift). Der Benutzer muss das System neu starten, um das PSD zu löschen. Nach dem Neustart wird das PSD nicht mehr geladen.	
Ein interner Fehler tritt auf, wenn der Benutzer eine Wiederherstellung anhand des automatischen Wiederherstellungs-archivs vornimmt.	Wenn der Benutzer in Embedded Security auf die Option **Restore under Backup** (Aus Sicherung wiederherstellen) klickt, um Daten anhand des automatischen Wiederherstellungsarchivs wiederherzustellen, und dann die Datei **SPSystemBackup.xml** auswählt, tritt ein Fehler bei der Ausführung des Wiederherstellungsassistenten auf, und die folgende Fehlermeldung wird angezeigt: **The selected Backup Archive does not match the restore reason. Please select another archive and continue.** (Das ausgewählte Wiederherstellungsarchiv passt nicht zum angegebenen Wiederherstellungsgrund. Bitte wählen Sie ein anderes Archiv aus, und fahren Sie dann mit der Wiederherstellung fort.)	Wenn der Benutzer **SpSystemBackup.xml** auswählt, obwohl die Datei SpBackupArchive.xml benötigt wird, tritt bei der Ausführung des Embedded Security Assistenten ein Fehler auf, und die folgende Meldung wird angezeigt: **An internal Embedded Security error has been detected.** (Ein interner Embedded Security Fehler ist aufgetreten.) Der Benutzer muss die korrekte XML-Datei für den jeweiligen Wiederherstellungsgrund auswählen. Die Prozesse entsprechen dem Standardverhalten und werden ordnungsgemäß ausgeführt. Die interne Embedded Security Fehlermeldung ist jedoch unklar und sollte präziser sein. HP arbeitet daran, die Meldung für zukünftige Produkte zu verbessern.
Bei Vorhandensein von mehreren Benutzern zeigt das Embedded Security System einen Fehler an.	Wenn der Administrator beim Wiederherstellungsprozess Benutzer auswählt, können nicht ausgewählte Benutzer die Schlüssel bei einem späteren Wiederherstellungsversuch nicht wiederherstellen. Es wird eine Fehlermeldung darüber angezeigt, dass der Verschlüsselungsprozess fehlgeschlagen ist (**decryption process failed**).	Die nicht ausgewählten Benutzer können wiederhergestellt werden, indem vor der nächsten täglichen Standardsicherung der TPM-Chip zurückgesetzt wird, der Wiederherstellungsvorgang durchgeführt wird und alle Benutzer ausgewählt werden. Wenn die automatische Sicherung durchgeführt wird, werden die nicht wiederhergestellten Benutzer überschrieben, und es kommt zu einem Datenverlust. Wenn ein neues System-Backup gespeichert wird, können die zuvor nicht ausgewählten Benutzer dann nicht wiederhergestellt werden. Außerdem muss der Benutzer das gesamte System-Backup wiederherstellen. Ein Archiv-Backup kann dagegen separat wiederhergestellt werden.
Wenn der System-ROM auf die Standardwerte zurückgesetzt wird, ist der TPM-Chip nicht mehr sichtbar.	Durch das Zurücksetzen des System-ROM auf die Standardeinstellungen ist der TPM-Chip für Windows nicht mehr sichtbar. Dadurch ist die Funktionsweise der Sicherheitssoftware beeinträchtigt, und auf TPM-verschlüsselte Daten kann nicht mehr zugegriffen werden.	So blenden Sie den TPM-Chip im BIOS wieder ein: Öffnen Sie das Computer Setup (F10) Utility, navigieren Sie zu **Security** (Sicherheit) > **Device security** (Gerätesicherheit), und ändern Sie das Feld von **Hidden** (Verborgen) in **Available** (Verfügbar).
Die automatische Sicherung funktioniert nicht für das zugeordnete Laufwerk.	Wenn ein Administrator in Embedded Security eine automatische Sicherung einrichtet, wird in Windows ein geplanter Task eingerichtet. Dieser geplante Windows Task ist so eingerichtet, dass als Berechtigung für die Sicherung NT AUTHORITY\SYSTEM verwendet wird. Dies funktioniert für lokale Laufwerke einwandfrei.	Als Behelfslösung können Sie NT AUTHORITY \SYSTEM in (Computername)\(Administratorname) ändern. Dies ist die Standardeinstellung, wenn der geplante Task manuell erstellt wird. HP wird in zukünftigen Produktversionen Standardeinstellungen bereitstellen, die (Computername\Administratorname) enthalten.

Kurzbeschreibung	Einzelheiten	Lösung
	Wenn der Administrator den automatischen Sicherungsvorgang stattdessen so konfiguriert, dass Daten auf einem zugeordneten Laufwerk gespeichert werden, schlägt der Prozess fehl, da NT AUTHORITY\SYSTEM nicht über die entsprechenden Rechte zum Verwenden des zugeordneten Laufwerks verfügt. Wenn die automatische Sicherung beim Anmelden erfolgen soll, zeigt das Embedded Security TNA (Taskbar Notification Area)-Symbol die folgende Meldung an: **The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.** (Das Backup-Archiv ist derzeit nicht verfügbar. Klicken Sie hier, um die Daten so lange in einem temporären Archiv zu sichern, bis das Archiv wieder zur Verfügung steht.) Wenn die automatische Sicherung jedoch für einen bestimmten Zeitpunkt geplant ist, schlägt das Backup fehl, ohne dass eine entsprechende Meldung erscheint.	
Embedded Security lässt sich in der Embedded Security GUI nicht vorübergehend deaktivieren.	Die aktuelle Software-Version 4.0 wurde für HP Notebook 1.1B Implementierungen sowie HP Desktop 1.2 Implementierungen entworfen. Die Deaktivierungsoption wird weiterhin von der Software-Schnittstelle für TPM 1.1-Plattformen unterstützt.	HP wird dieses Problem in zukünftigen Versionen beheben.

Device Access Manager for HP ProtectTools

Kurzbeschreibung	Details	Lösung
Die Benutzer erhalten keinen Zugriff auf Geräte in Device Access Manager, obwohl die Geräte grundsätzlich verfügbar sind.	Device Access Manager wurde für **Einfache Konfiguration** und/oder **Geräteklassen-Konfiguration** eingerichtet, so dass den Benutzern der Zugriff auf Geräte verwehrt wird. Die Benutzer können jedoch trotzdem auf die Geräte zugreifen.	Vergewissern Sie sich, dass der Dienst HP ProtectTools Device Locking gestartet wurde. Melden Sie sich mit Administratorrechten an, und rufen Sie **Systemsteuerung** > **Verwaltung** > **Dienste** auf. Suchen Sie im Fenster **Dienste** den Dienst **HP ProtectTools Gerätesperre/Überwachung**. Vergewissern Sie sich, dass der Dienst gestartet ist und dass sein Autostarttyp **Automatisch** lautet.
Ein Benutzer erhält Zugriff auf ein Gerät bzw. ihm wird der Zugriff verweigert, ohne dass der Grund hierfür offensichtlich ist.	In Device Access Manager wurde den Benutzern der Zugriff auf bestimmte Geräte gestattet bzw. untersagt. Bei der Arbeit mit dem System stellen die Benutzer fest, dass sie unerwarteterweise auf einige Geräte zugreifen können, während dies bei anderen Geräten nicht der Fall ist, obwohl sie ihrer Meinung nach darauf Zugriff haben müssten.	Die Geräteeinstellungen für die einzelnen Benutzer sollte anhand der **Geräteklassen-Konfiguration** in Device Access Manager überprüft werden. Klicken Sie auf **Security Manager**, dann auf **Device Access Manager** und dann auf **Geräteklassen-Konfiguration**. Blenden Sie die Ebenen des Geräteklassenbaums ein, und überprüfen Sie die auf den Benutzer zutreffenden Einstellungen. Achten Sie auf „Verweigern“-Einträge für den betreffenden Benutzer oder eine Windows Gruppe, der er angehört, z. B. Benutzer, Administratoren.
Was hat Vorrang – die Zugriffserteilung oder die Zugriffsverweigerung?	Innerhalb der Geräteklassen-Konfiguration lauten die Einstellungen wie folgt: • Einer bestimmten Windows Gruppe (z. B. BUILTIN\Administrators) wurde der Zugriff erteilt, während einer andere Windows Gruppe (z. B. BUILTIN\Users) auf der gleichen Ebene der Geräteklassen-Hierarchie (z. B. DVD/CD-ROM Drives) der Zugriff verweigert wurde. Was hat Vorrang, wenn ein Benutzer beiden Gruppen angehört (z. B. bei einem Administrator)?	Der Benutzer erhält keinen Zugriff auf das Gerät. Die Zugriffsverweigerung hat stets Vorrang vor der Zugriffserteilung. Dies liegt in der Art und Weise begründet, wie Windows die jeweils gültige Berechtigung für das Gerät ermittelt. In dem beschriebenen Fall wird einer Gruppe der Zugriff erteilt, während er der anderen Gruppe verweigert wird. Der Benutzer gehört beiden Gruppen an. In diesem Fall wird dem Benutzer der Zugriff insgesamt verweigert, da die Zugriffsverweigerung Vorrang vor der Zugriffserteilung hat. Eine Lösungsmöglichkeit besteht darin, der Benutzer-Gruppe auf der DVD/CD-ROM-Laufwerksebene den Zugriff zu verweigern und ihn gleichzeitig der Administrator-Gruppe unterhalb der DVD/CD-ROM-Laufwerksebene zu gewähren. Alternativ können spezifische Windows Gruppen angelegt werden, wobei einer Gruppe der DVD/CD-Zugriff gewährt und der anderen dieser Zugriff verweigert wird. Diesen Gruppen können dann die gewünschten Benutzer zugewiesen werden.

Sonstiges

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
Security Manager — Warnmeldung: **The security application can not be installed until the HP ProtectTools Security Manager is installed**. (Die Sicherheitsanwendung kann erst installiert werden, nachdem HP ProtectTools Security Manager installiert wurde.)	Alle Sicherheitsanwendungen wie Embedded Security, Java Card Security und biometrische Lesegeräte sind erweiterbare Plug-In-Module für die Security Manager Schnittstelle. Security Manager muss daher installiert sein, bevor ein von HP genehmigtes Sicherheits-Plug-In geladen werden kann.	Die Security Manager Software muss installiert sein, bevor ein Sicherheits-Plug-In installiert werden kann.
TPM Firmware-Aktualisierungsprogramm für Modelle mit Broadcom-fähigen TPM-Chips – Das über die HP Support-Website erhältliche Tool zeigt die Meldung **ownership required** (Eigentumsrechte erforderlich) an.	Dies ist das Standardverhalten des TPM-Firmware-Aktualisierungsprogramms für Modelle mit Broadcom-fähigen TPM-Chips. Mit dem Firmware-Aktualisierungsprogramm kann der Benutzer die Firmware aktualisieren, unabhängig davon, ob ein so genannter Bestätigungsschlüssel (Endorsement Key, EK) vorhanden ist. Wenn kein Bestätigungsschlüssel verfügbar ist, ist für das Durchführen der Firmware-Aktualisierung keine Autorisierung erforderlich. Wenn ein Bestätigungsschlüssel vorhanden ist, muss auch ein TPM-Eigentümer vorhanden sein, da für den Aktualisierungsvorgang dann eine Benutzerautorisierung benötigt wird. Nach einer erfolgreichen Aktualisierung muss die Plattform neu gestartet werden, damit die neue Firmware wirksam wird. Wenn das BIOS-TPM auf die Werkseinstellungen zurückgesetzt wird, werden Eigentümerrechte entfernt, und die Firmware kann erst dann aktualisiert werden, wenn die Embedded Security-Softwareplattform und der Assistent für die Benutzerinitialisierung (User Initialization Wizard) konfiguriert wurden. **HINWEIS:** Nach der Ausführung der Firmware-Aktualisierung sollte stets ein Neustart erfolgen. Die Firmware-Version wird erst nach einem Neustart korrekt erkannt.	1. Führen Sie eine Neueinstallation von Embedded Security durch. 2. Führen Sie die Plattform und den Assistenten für die Benutzerkonfiguration aus. 3. Vergewissern Sie sich, dass auf dem System Microsoft .NET Framework 1.1 installiert ist: a. Klicken Sie auf **Start**. b. Klicken Sie auf **Systemsteuerung**. c. Klicken Sie auf **Software**. d. Überprüfen Sie, ob **Microsoft .NET Framework 1.1** in der Liste aufgeführt ist. 4. Überprüfen Sie die Hardware- und Softwarekonfiguration: a. Klicken Sie auf **Start**. b. Klicken Sie auf **Alle Programme**. c. Klicken Sie unter Windows Vista auf **HP ProtectTools Security Manager for Administrators** bzw. unter Windows XP auf **HP ProtectTools Security Manager**.

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
		d. Wählen Sie im Baummenü den Eintrag **Embedded Security**. **e.** Klicken Sie auf **More Details** (Weitere Details). Das System sollte folgende Konfiguration aufweisen: • Product version (Produktversion) = V4.0.1 • Embedded Security State (Embedded Security-Status): Chip State (Chip-Status) = Enabled (Aktiviert), Owner State (Eigentümerstatus) = Initialized (Initialisiert), User State (Benutzerstatus) = Initialized (Initialisiert) • Component Info (Komponenteninformation): TCG Spec. Version (Version TCG-Spez.) = 1.2 • Vendor (Anbieter) = Broadcom Corporation • FW Version (Firmware-Version) = 2.18 (oder höher) • TPM Device driver library version 2.0.0.9 (or greater) (TPM-Gerätetreiberbibliothek Version 2.0.0.9 (oder höher) 5. Wenn die FW-Version nicht mit 2.18 übereinstimmt, laden Sie die TPM-Firmware herunter, und führen Sie ein Update aus. Der TPM-Firmware-SoftPaq ist als Support-Download auf der HP Website unter http://www.hp.com verfügbar.
HP ProtectTools Security Manager – Beim Schließen der Security Manager-Schnittstelle wird zeitweilig ein Fehler zurückgegeben.	Wenn der Benutzer Security Manager über die Schließen-Schaltfläche in der oberen rechten Ecke des Bildschirms schließt, bevor alle Plug-In-Anwendungen vollständig geladen wurden, tritt zeitweilig (in einem von 12 Fällen) ein Fehler auf.	Dies ist auf eine Zeitsteuerungsabhängigkeit von Ladezeiten für Plug-In-Dienste beim Schließen und Neustarten von Security Manager zurückzuführen. Da die Datei **PTHOST.exe** die Shell für die anderen Anwendungen (Plug-Ins) bildet, ist sie davon abhängig, dass Plug-Ins ihre Ladezeiten (Dienste) regulär abschließen. Das Problem tritt dann auf, wenn die Shell geschlossen wird, bevor ein Plug-In erfolgreich geladen werden konnte. Warten Sie, bis Security Manager die Meldung über das Laden der Dienste (oben im Security Manager Fenster) abgeschlossen hat und alle in der linken Spalte aufgeführten Plug-Ins geladen sind. Um einen Fehler zu vermeiden warten Sie einige Sekunden, bis sämtliche Plug-Ins geladen wurden.

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
HP ProtectTools – Durch unbeschränkten Zugriff oder unkontrollierte Administratorrechte kommt es zu einem Sicherheitsrisiko.	Ein unbeschränkter Zugriff auf den Client-PC kann eine Vielzahl von Sicherheitsrisiken mit sich bringen, z. B.: • Löschen eines PSD • Unbefugte Änderungen von Benutzereinstellungen • Deaktivieren von Sicherheitsrichtlinien und -funktionen	Administratoren sollten empfohlene Verfahrensweisen anwenden, um Endbenutzerrechte und den Benutzerzugriff zu beschränken. Unautorisierte Benutzer sollten keine Administratorrechte erhalten.
Die Embedded Security Kennwörter für BIOS und Betriebssystem sind nicht synchronisiert.	Wenn ein Benutzer ein neues Kennwort nicht als das Embedded Security Kennwort für das BIOS validiert, wird das Embedded Security Kennwort für das BIOS über F10 BIOS auf das ursprüngliche Embedded Security Kennwort zurückgesetzt.	Dies entspricht dem Standardverhalten. Diese Kennwörter können erneut synchronisiert werden, indem das Basisbenutzerkennwort für das Betriebssystem geändert und an der Aufforderung zur Eingabe des Embedded Security-Kennworts für das BIOS authentifiziert wird.
Nach der Aktivierung der TPM-Preboot-Authentifizierung im BIOS kann sich nur ein Benutzer am System anmelden.	Die TPM-BIOS-PIN ist dem ersten Benutzer zugewiesen, der die Benutzereinstellung initialisiert. Wenn ein Computer über mehrere Benutzer verfügt, hat der erste Benutzer die Funktion eines Administrators. Der erste Benutzer muss seine TPM-Benutzer-PIN den anderen Benutzern mitteilen, damit diese sich ebenfalls anmelden können.	Dies entspricht dem Standardverhalten. HP empfiehlt, dass die IT-Abteilung des Kunden sinnvolle Sicherheitsrichtlinien anwenden sollte, um die Sicherheitslösung bereitzustellen und zu gewährleisten, dass das BIOS-Administratorkennwort von IT-Administratoren für den Schutz auf Systemebene konfiguriert wird.
Der Benutzer muss seine PIN ändern, damit die TPM-Preboot-Funktion nach einer TPM-Rücksetzung auf die Werkseinstellungen ausgeführt werden kann.	Der Benutzer muss seine PIN ändern oder einen anderen Benutzer anlegen, um seine Benutzereinstellung zu initialisieren und zu erreichen, dass die TPM-BIOS-Authentifizierung nach dem Rücksetzen funktioniert. Es steht keine Option zur Verfügung, mit der die Funktionsfähigkeit der TPM-BIOS-Authentifizierung realisiert werden kann.	Dies entspricht dem Standardverhalten. Durch das Zurücksetzen auf die Werkseinstellungen wird der allgemeine Benutzerschlüssel gelöscht. In der Folge muss der Benutzer seine Benutzer-PIN ändern oder einen neuen Benutzer anlegen, um den allgemeinen Benutzerschlüssel neu zu initialisieren.
Power-on authentication (Systemstart-Authentifizierung) wird bei Verwendung der Embedded Security Option **Reset to Factory Settings** (Auf Werkseinstellungen zurücksetzen) nicht auf den Standardwert zurückgesetzt.	In Computer Setup wird die Option **Power-on authentication support** (Systemstart-Authentifizierung) mit der Embedded Security-Chip-Option **Reset to Factory Settings** (Auf Werkseinstellungen zurücksetzen) nicht auf die Werkseinstellungen zurückgesetzt. Standardmäßig wird **Power-on authentication support** (Systemstart-Authentifizierung) auf **Disable** (Deaktivieren) eingestellt.	Die Option **Reset to Factory Settings** (Auf Werkseinstellungen zurücksetzen) deaktiviert Embedded Security Device (Chip für integrierte Sicherheit), wodurch auch die anderen Optionen von Embedded Security (einschließlich **Power-on authentication support** (Systemstart-Authentifizierung)) nicht sichtbar sind. Nach der erneuten Aktivierung von Embedded Security Device bleibt **Power-on authentication support** (Systemstart-Authentifizierung) jedoch aktiviert. HP arbeitet an einer Lösung, die in zukünftigen webbasierten ROM-SoftPaqs bereitgestellt wird.

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
Beim Startvorgang kommt es zu einer Überschneidung der Embedded Security Systemstart-Authentifizierung mit dem BIOS-Kennwort.	Bei der Systemstart-Authentifizierung wird der Benutzer aufgefordert, sich mit dem TPM-Kennwort beim System anzumelden. Wenn der Benutzer F10 drückt, um zum BIOS Setup zu gelangen, erhält er lediglich Lese-Rechte.	Um die BIOS-Einstellungen ändern zu können, muss der Benutzer im Fenster der Systemstart-Authentifizierung anstelle des TPM-Kennworts das BIOS-Kennwort eingeben.
Nach der Änderung des Eigentümerkennworts wird der Benutzer vom BIOS zur Eingabe des alten und des neuen Kennworts über Computer Setup Utility aufgefordert.	Nachdem in Embedded Security Windows Software das Eigentümerkennwort geändert wurde, wird der Benutzer vom BIOS zur Eingabe des alten und des neuen Kennworts über Computer Setup aufgefordert.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Die Ursache für dieses Problem liegt darin, dass das BIOS nach dem Starten des Betriebssystems nicht in der Lage ist, mit dem TPM-Chip zu kommunizieren und das TPM-Kennwort zu verifizieren.

Glossar

Administrator: Siehe Windows Administrator.

Aktivierung: Die Aufgabe, die ausgeführt werden muss, bevor Drive Encryption-Funktionen verfügbar sind. Drive Encryption wird mit dem Installationsassistenten für HP ProtectTools Security Manager for Administrators aktiviert. Nur ein einziger Administrator kann Drive Encryption aktivieren. Der Aktivierungsvorgang besteht darin, die Software zu aktivieren, das Laufwerk zu verschlüsseln, ein Benutzerkonto zu erstellen und den Verschlüsselungscode der ersten Sicherung auf einem Wechseldatenträger zu erstellen.

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

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

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

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.

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

Bereinigung: Siehe **Festplattenbereinigung**.

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

BIOS-Administrator-Kennwort: *Setup*-Kennwort für Computer Setup.

BIOS-Pofil: Gruppe von BIOS-Konfigurationseinstellungen, die gespeichert und auf andere Konten angewendet werden können.

BIOS-Sicherheitsmodus: Einstellung in Java Card Security, die bei Aktivierung die Verwendung einer Java Card und einer gültigen PIN zur Benutzerauthentifizierung erfordert.

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

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

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

Dienst zur Schlüsselwiederherstellung von Drive Encryption: Der SafeBoot Recovery Service. Dieser Dienst speichert eine Kopie des Chiffrierschlüssels, mit dessen Hilfe Sie auf Ihren Computer zugreifen können, selbst wenn Sie das Kennwort vergessen und keinen Zugriff auf Ihren lokal abgelegten Sicherungsschlüssel haben. Sie müssen ein Konto bei diesem Dienst erstellen, um den Online-Zugriff auf Ihren Sicherungsschlüssel einzurichten.

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

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

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

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

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

Einfaches Löschen: Das Löschen des Windows Verweises zu einem Datenbestand. Der Inhalt des Datenbestands verbleibt auf der Festplatte, bis die Daten im Rahmen der Festplattenbereinigung überschrieben werden.

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

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

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

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

Hohe Sicherheit: Sicherheitsmerkmal in der BIOS Konfiguration, das erweiterten Schutz für das Administratorkennwort und das Kennwort beim Systemstart sowie für weitere Arten der Authentifizierung beim Systemstart bietet.

Identität: Im HP ProtectTools Credential Manager ist das eine Gruppe von Anmeldeinformationen und Einstellungen, die wie ein Konto oder Profil für einen bestimmten Benutzer behandelt wird.

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

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

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

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

Migration: Eine Aufgabe, die das Verwalten, Wiederherstellen und Übertragen von Privacy Manager-Zertifikaten und Trusted Contacts ermöglicht.

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

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

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

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

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

Public Key-Infrastruktur (PKI) Standard, der die Oberflächen zum Erstellen, Verwenden und Verwalten von Zertifikaten und kryptografischen Schlüsseln definiert.

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

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

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

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

Shred-Profil: Eine spezielle Löschmethode mit einer Liste von Datenbeständen.

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

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

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

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

Single Sign-On: Funktion, die Authentifizierungsdaten speichert und den Zugriff auf Internet- und Windows Anwendungen mit Kennwortauthentifizierung über den Credential Manager ermöglicht.

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

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

Token: Siehe Sicherheits-Anmeldemethode.

TPM (Trusted Platform Module)-Sicherheitschip: Oberbegriff für den HP ProtectTools Embedded Security Chip. Ein TPM (Trusted Platform Module) authentifiziert einen Computer anstatt einen Benutzer, indem es hostsystem-spezifische Informationen wie Chiffrierschlüssel, digitale Zertifikate und Kennwörter speichert. Ein TPM minimiert das Risiko, dass Daten auf dem Computer durch physischen Diebstahl oder einen Angriff durch einen externen Hacker gefährdet werden.

Trusted Contact: Eine Person, die eine Trusted Contact-Einladung angenommen hat.

Trusted Contact-Einladung: Eine E-Mail-Nachricht, die an eine Person gesendet wird, um sie zu bitten, ein Trusted Contact zu werden.

Trusted Contact-Empfänger: Eine Person, die die Einladung erhält, ein Trusted Contact zu werden.

Trusted Contacts-Liste: Eine Liste der Trusted Contacts.

TXT: Trusted Execution Technology (Vertrauenswürdige Ausführungstechnologie). Hardware und Firmware, die Schutz vor Angriffen auf die Software und Daten eines Computers bietet.

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

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

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

Vertrauenswürdige IM-Kommunikation: Eine Kommunikationssitzung, während der vertrauenswürdige Nachrichten von einem vertrauenswürdigen Absender an einen Trusted Contact gesendet werden.

Vertrauenswürdige Nachricht: Eine Kommunikationssitzung, während der vertrauenswürdige Nachrichten von einem vertrauenswürdigen Absender an einen Trusted Contact gesendet werden.

Vertrauenswürdiger Absender: Ein Trusted Contact, der signierte und/oder verschlüsselte E-Mails und Microsoft Office-Dokumente versendet.

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

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

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.

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

Index