HP ProtectTools
Benutzerhandbuch

Zweite Ausgabe: Oktober 2007

Teilenummer des Dokuments: 451271-042

Inhaltsverzeichnis

1 Einführung in die Sicherheitsfunktionen

Die HP ProtectTools Security Manager Software enthält Sicherheitsfunktionen, die vor unberechtigtem Zugriff auf den Computer, Netzwerke und kritische Daten schützen. Folgende Softwaremodule enthalten erweiterte Sicherheitsfunktionen:

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

Die für Ihren Computer erhältlichen Softwaremodule hängen vom Computermodell ab. So steht das Softwaremodul Embedded Security for HP ProtectTools beispielsweise nur auf Computern zur Verfügung, auf denen der integrierte TPM-Sicherheits-Chip (Trusted Platform Module) installiert ist.

Die Module der HP ProtectTools-Software können vorinstalliert bzw. auf der Festplatte vorhanden sein, oder Sie können sie von der HP Website herunterladen. Für bestimmte HP Compaq Desktop-Modelle ist HP ProtectTools als Aftermarket-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
Credential Manager for HP ProtectTools	• Credential Manager erfüllt zwei Aufgaben: Er dient zum einen als Speicherort für das persönliche Kennwort und ermöglicht dadurch die einmalige Anmeldung. Zum anderen bietet er dem Benutzer die Möglichkeit, Funktionen für eine höhere Sicherheit bei der Benutzerauthentifizierung, die über die Eingabe eines Kennworts hinausgehen, zu definieren und auszuführen. • Das gespeicherte Kennwort wird verschlüsselt und kann durch die Verwendung eines integrierten TPM-Sicherheitschips noch zuverlässiger geschützt werden. • Neben der Funktion zum einmaligen Anmelden bietet Credential Manager die Möglichkeit, verschiedene Technologien zur sicheren Authentifizierung einsetzen. Dazu gehören zum Beispiel eine Java™ Card oder die biometrische Erkennung für die Benutzerauthentifizierung in Verbindung mit einem Kennwort.
Embedded Security for HP ProtectTools	• Embedded Security verwaltet Sicherheitsoptionen für Benutzer und Administrator zum Schutz verschiedener Verschlüsselungsschlüssel mit Hilfe der TPM-Technologie, wie zum Beispiel EFS (Encrypting File System), auf dem lokalen Computer. Personal Secure Drive (PSD) und digitale Zertifikate von Drittanbietern. • Embedded Security verwendet einen integrierten Trusted Platform Module (TPM)-Sicherheitschip zum Schutz vor unautorisiertem Zugriff auf wichtige Benutzer- oder Zugangsdaten, die lokal auf einem PC gespeichert sind. TPM bietet die sichere Speicherung von Verschlüsselungsschlüsseln und verfügt über Funktionen zur Schlüsselgenerierung. Zusätzlich bietet es sicheren Schutz vor Kennwortangriffen. • Embedded Security ermöglicht die Erstellung eines persönlichen sicheren Laufwerks (Personal Secure Drive, PSD), d. h. eines virtuellen Laufwerks, das im System ausgeblendet werden kann, um Benutzerdaten zu schützen. • Darüber hinaus unterstützt die Embedded Security Software Anwendungen von Fremdherstellern wie Microsoft® Outlook und Internet Explorer für geschützte digitale Zertifikatoperationen.
Java Card Security for HP ProtectTools	• 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. • 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.
BIOS Configuration for HP ProtectTools	• BIOS Configuration ermöglicht den Zugriff auf die Systemstart- und Administratorkennwörter. • BIOS Configuration stellt eine Alternative zum Pre-Boot BIOS Configuration-Dienstprogramm F10 Setup dar.

Modul	Funktionen
Drive Encryption for HP ProtectTools	• Drive Encryption ermöglicht eine umfassende Verschlüsselung der gesamten Festplatte. • Drive Encryption erfordert die Authentifizierung vor dem Systemstart, um die Festplatte zu entschlüsseln und den Datenzugriff zu gewähren. • Drive Encryption bietet ein Tool zur Authentifizierungsverwaltung, mit dem Partitionen sowie einzelne oder mehrere Festplatten verschlüsselt werden können.
Device Access Manager for HP ProtectTools	• Device Access Manager bietet die benutzerdefinierbare Steuerung von Datenspeichern und Übertragungsgeräten (USB, COM- und LPT-Ports, persönliche Musikwiedergabegeräte, CD-Laufwerke, Netzwerkschnittstellenkarten usw.). • Zusätzlich kann Device Access Manager Benutzer und Benutzergruppen verwalten, um den Lese- und Schreibzugriff zu ermöglichen und den Zugriff auf Daten auf der Hardware zuzulassen oder zu verweigern.

Öffnen von HP ProtectTools Security

So öffnen Sie HP ProtectTools Security über die Windows®-Systemsteuerung:

- Wählen Sie in Windows Vista **Start > Alle Programme > HP ProtectTools Security Manager** (oder **HP ProtectTools Security Manager for Administrators**).

HINWEIS: Nachdem Sie das Credential Manager Modul konfiguriert haben, können Sie HP ProtectTools auch öffnen, indem Sie sich direkt mithilfe des Windows-Anmeldebildschirms bei Credential Manager anmelden. Weitere Informationen finden Sie unter „Anmelden bei Windows mit Credential Manager“ auf Seite 18.

Unter Windows Vista muss der Administrator „HP ProtectTools Security Manager for Administrators“ beim Zugriff auf Drive Encryption verwenden.

Realisierung grundlegender Sicherheitsaufgaben

Die HP ProtectTools Module bieten zusammengenommen Lösungen für eine Vielzahl von Sicherheitsthemen, zu denen auch die folgenden grundlegenden Aufgaben gehören:

- Schutz gegen Diebstahl
- Einschränken des Zugriffs auf sensible Daten
- Verhindern des unbefugten Zugriffs von internen oder externen Standorten
- Erstellen und Verwenden von sicheren Kennwörtern

Schutz gegen Diebstahl

Ein Beispiel für diesen Ereignistyp wäre der gezielte Diebstahl eines Computers mit vertraulichen Daten und Kundendaten aus einem abgetrennten Bereich oder Großraumbüro. Die folgenden Funktionen helfen beim Schutz vor gezieltem Diebstahl:

- Wenn die Funktion für eine Authentifizierung vor dem Systemstart aktiviert ist, kann ein unbefugter Benutzer nicht auf das Betriebssystem zugreifen. Siehe auch die folgenden Vorgehensweisen:
  - „Zuordnen eines Namens zu einer Java Card-PIN“ auf Seite 36
  - „Device Access Manager for HP ProtectTools“ auf Seite 45
  - „Drive Encryption for HP ProtectTools“ auf Seite 50
- DriveLock gewährleistet, dass auch dann nicht auf Daten zugegriffen werden kann, wenn die Festplatte entfernt und in einem ungeschützten System installiert wird. Siehe „Security (Sicherheit)“ auf Seite 42.
- 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 folgenden Vorgehensweisen:
  - Embedded Security „Setup“ auf Seite 28
  - „PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk)“ auf Seite 30

Einschränken des Zugriffs auf sensible Daten

Angenommen, ein Vertragsprüfer arbeitet vor Ort und hat Zugriff auf die Computer erhalten, um vertrauliche Finanzdaten zu prüfen. Sie möchten nicht, dass der Prüfer die Dateien drucken oder auf einem beschreibbaren Medium wie einer CD speichern kann. Mit der folgenden Funktion kann der Zugriff auf Daten eingeschränkt werden:

- Device Access Manager for HP ProtectTools ermöglicht es IT-Managern, den Zugriff auf beschreibbare Geräte einzuschränken, damit wichtige Informationen nicht gedruckt oder von der Festplatte auf Wechseldatenträger kopiert werden können. Siehe „Geräteklassen-Konfiguration (erweitert)“ auf Seite 48.
- DriveLock hilft dabei, sicherzustellen, dass auch dann nicht auf Daten zugegriffen werden kann, wenn die Festplatte entfernt und in einem unsicheren System installiert wird. Siehe „Security (Sicherheit)“ auf Seite 42.

Verhindern des unbefugten Zugriffs von internen oder externen Standorten

Wenn von einem internen oder externen Standort auf einen PC zugegriffen wird, der vertrauliche Daten und Kundeninformationen enthält, könnten nicht autorisierte Benutzer unter Umständen Zugriff auf

Ressourcen im Unternehmensnetzwerk oder auf Daten von Finanzdiensten, eines Mitglieds der Geschäftsleitung oder der Forschungs- und Entwicklungsabteilung erhalten. Die folgenden Funktionen helfen dabei, nicht autorisierten Zugriff zu verhindern:

- Wenn die Funktion für eine Authentifizierung vor dem Systemstart aktiviert ist, kann ein unbefugter Benutzer nicht auf das Betriebssystem zugreifen. Siehe auch die folgenden Vorgehensweisen:
  - „Zuordnen eines Namens zu einer Java Card-PIN“ auf Seite 36
  - „Drive Encryption for HP ProtectTools“ auf Seite 50
- Embedded Security for HP ProtectTools schützt sensible Benutzerdaten oder Anmeldeinformationen, die lokal auf einem PC gespeichert sind, folgendermaßen vor unbefugtem Zugriff:
  - Embedded Security „Setup“ auf Seite 28
  - „PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk)“ auf Seite 30
- 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“ auf Seite 13
  - „Verwenden von Single Sign On (Einmaliges Anmelden)“ auf Seite 19
- Device Access Manager for HP ProtectTools ermöglicht es IT-Managern, den Zugriff auf beschreibbare Geräte einzuschränken, damit wichtige Informationen nicht von der Festplatte kopiert werden können. Siehe „Einfache Konfiguration“ auf Seite 47.
- 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“ auf Seite 28
  - „PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk)“ auf Seite 30

Erstellen und Verwenden von sicheren Kennwörtern

Bei der Flut von Kennwörtern, die für den regelmäßigen Zugriff auf Websites oder gesicherte Anwendungen erforderlich sind, neigen Benutzer dazu, ein einfaches Kennwort für alle Anwendungen und Websites zu verwenden. Oder sie werden kreativ und vergessen dann prompt, welches Kennwort für welche Anwendung gilt. Mit den folgenden Vorgehensweisen bietet Credential Manager for HP ProtectTools einen geschützten Speicherort für Kennwörter sowie einmalige Anmeldung:

- „Erstellen eines sicheren Kennworts“ auf Seite 8
- Credential Manager „Setup“ auf Seite 13
- „Verwenden von Single Sign On (Einmaliges Anmelden)“ auf Seite 19

Für eine optimale Sicherheit übernimmt Embedded Security for HP ProtectTools dann den zuverlässigen Schutz des Repository, in dem die Benutzernamen und Kennwörter abgelegt werden. Auf diese Weise lassen sich mehrere sichere Kennwörter verwalten, ohne dass die Benutzer sie notieren oder auswendig lernen müssen. Siehe Embedded Security „Setup“ auf Seite 28.

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.

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

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

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

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 dieses Kennwort für die Authentifizierung

HP ProtectTools Kennwort	In diesem HP ProtectTools Modul eingerichtet	Funktion
HINWEIS: Auch bekannt als: Embedded Security Kennwort		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-Token-Schlüssel	Embedded Security, vom IT-Administrator	Schützt den Zugriff auf das Notfallwiederherstellungs-Token. Hierbei handelt es sich um eine Sicherungsdatei für den integrierten Sicherheits-Chip.
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:** Wird auch als BIOS-Administrator-, F10 Setup- oder Sicherheits-Setup-Kennwort bezeichnet.	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.

Erstellen eines sicheren Kennworts

Das Erstellen von Kennwörtern ist nur möglich, wenn Sie die vom Programm festgelegten Anforderungen erfüllen. Beachten Sie im Allgemeinen folgende Richtlinien für das Erstellen 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.
- Erstellen Sie Wörter aus 2 oder mehreren 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.

HP ProtectTools Backup and Restore

Die Funktionen zum Sichern und Wiederherstellen von HP ProtectTools Backup and Restore ermöglichen die schnelle und einfache Sicherung und Wiederherstellung der Zugangsdaten für alle installierten HP ProtectTools Module.

Sichern von Zugangsdaten und Einstellungen

Sie können Zugangsdaten auf folgende Arten sichern:

- Indem Sie den HP ProtectTools Backup-Assistenten aufrufen, um HP ProtectTools Module auszuwählen und zu sichern.
- Indem Sie vorausgewählte HP ProtectTools Module sichern.

HINWEIS: Hierfür müssen Sie zunächst Sicherungsoptionen festlegen.

- Indem Sie Sicherungen planen.

HINWEIS: Hierfür müssen Sie zunächst Sicherungsoptionen festlegen.

Auswählen und Sichern von HP ProtectTools Modulen mit dem HP ProtectTools Backup-Assistenten

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **HP ProtectTools** und anschließend **Backup and Restore** (Sichern und Wiederherstellen).
3. Klicken Sie im rechten Fensterausschnitt auf **Backup Options** (Backup-Optionen). Der Backup-Assistent für HP ProtectTools wird geöffnet. Befolgen Sie die Anleitungen auf dem Bildschirm, um die Zugangsdaten zu sichern.

Einstellen der Sicherungsoptionen

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **HP ProtectTools** und anschließend **Backup and Restore** (Sichern und Wiederherstellen).
3. Klicken Sie im rechten Fensterausschnitt auf **Backup Options** (Backup-Optionen). Das Fenster „HP ProtectTools Backup Wizard“ wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

5. Nachdem Sie das **Storage File Password** (Kennwort für die Speicherdatei) definiert und bestätigt haben, klicken Sie auf **Remember all passwords and authentication values for future automated backups** (Alle Kennwörter und Authentifizierungswerte für künftige automatische Sicherungen speichern).

6. Klicken Sie auf **Save Settings** (Einstellungen speichern) und anschließend auf **Fertig stellen**.

Sichern von vorausgewählten HP ProtectTools Modulen

HINWEIS: Hierfür müssen Sie zunächst Sicherungsoptionen festlegen.

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.

2. Wählen Sie im linken Fensterausschnitt die Option **HP ProtectTools** und anschließend **Backup and Restore** (Sichern und Wiederherstellen).

3. Klicken Sie im rechten Fensterausschnitt auf **Sicherung**.

Planen von Sicherungen

HINWEIS: Hierfür müssen Sie zunächst Sicherungsoptionen festlegen.

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.

2. Wählen Sie im linken Fensterausschnitt die Option **HP ProtectTools** und anschließend **Backup and Restore** (Sichern und Wiederherstellen).

3. Klicken Sie im rechten Fensterausschnitt auf **Schedule Backups** (Backup-Zeitplan).

4. Klicken Sie auf der Registerkarte **Task** (Aufgabe) auf die Schaltfläche **Aktiviert**, um geplante Sicherungen zu aktivieren.

5. Klicken Sie auf **Set Password** (Kennwort festlegen), geben Sie das Kennwort im Dialogfeld **Set Password** (Kennwort festlegen) ein, und bestätigen Sie es anschließend durch eine erneute Eingabe. Klicken Sie auf **OK**.

6. Klicken Sie auf **Übernehmen**. Klicken Sie auf die Registerkarte **Schedule** (Zeitplan). Klicken Sie auf den Pfeil neben **Schedule Task** (Aufgabe planen), und wählen Sie aus, in welchen Zeitabständen das automatische Backup durchgeführt werden soll.

7. Wählen Sie unter **Start time** (Startzeit) mit den entsprechenden Pfeiltasten den genauen Zeitpunkt aus, zu dem das Backup beginnen soll.

8. Klicken Sie auf **Erweitert**, um ein Startdatum, ein Enddatum und andere Standardeinstellungen für die Aufgabe festzulegen. Klicken Sie auf **Übernehmen**.

9. Klicken Sie auf **Einstellungen**, und legen Sie die Einstellungen für **Scheduled Task Completed** (Abschluss der geplanten Aufgabe), **Idle Time** (Leerlaufzeit) und **Energieverwaltung** fest.

10. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Wiederherstellen von Anmeldeinformationen

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.

2. Wählen Sie im linken Fensterausschnitt die Option **HP ProtectTools** und anschließend **Backup and Restore** (Sichern und Wiederherstellen).

3. Klicken Sie im rechten Fensterausschnitt auf **Wiederherstellen**. Das Fenster „HP ProtectTools Restore Wizard“ wird geöffnet. Folgen Sie den Anleitungen auf dem Bildschirm.

Konfigurieren der Einstellungen

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **HP ProtectTools** und dann auf **Einstellungen**.
3. Wählen Sie im rechten Fensterausschnitt Ihre Einstellungen aus, und klicken Sie dann auf **OK**.

2 Credential Manager for HP ProtectTools

Credential Manager erfüllt zwei Aufgaben: Er bietet dem Benutzer die Möglichkeit, Funktionen für eine höhere Sicherheit bei der Benutzerauthentifizierung, die über die Eingabe eines Kennworts hinausgehen, zu definieren und auszuführen. Außerdem dient er als Speicherort für das persönliche Kennwort und ermöglicht dadurch die einmalige Anmeldung. Credential Manager for HP ProtectTools schützt Ihren Computer mit Hilfe der folgenden Sicherheitsfunktionen vor unautorisiertem Zugriff:

- Alternativen zu Kennwörtern für die Anmeldung bei Windows, wie eine Smart Card oder biometrische Lesegeräte. Weitere Informationen finden Sie unter „Registrieren von Anmeldeinformationen“ auf Seite 14.
- 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 Smart Cards und biometrische Lesegeräte.
- Unterstützung für zusätzliche Sicherheitseinstellungen, z. B. Authentifizierungsabfrage unter Verwendung eines optionalen Sicherheitsgeräts, um den Computerschutz aufzuheben.

Setup

Anmelden bei Credential Manager

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

- Über den Anmeldeassistenten für den Credential Manager (bevorzugte Methode)
- Symbol für HP ProtectTools Security Manager im Infobereich
- HP ProtectTools Security Manager

HINWEIS: Wenn Sie im Fenster der Windows-Anmeldung die Aufforderung zur Anmeldung bei Credential Manager verwenden, werden Sie gleichzeitig bei Windows angemeldet.

Melden Sie sich mit Ihrem normalen Windows-Anmeldekennwort an, wenn Sie den Credential Manager zum ersten Mal öffnen. Bei dieser Gelegenheit wird anhand Ihrer Windows-Anmeldeinformationen automatisch ein Credential Manager-Konto erstellt.

Nachdem Sie beim Credential Manager angemeldet sind, können Sie zusätzliche Anmeldeinformationen, z. B. einen Fingerabdruck oder eine Java Card, registrieren. Weitere Informationen finden Sie unter „Registrieren von Anmeldeinformationen“ auf Seite 14.

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 Anmelde-Assistenten bei Credential Manager anzumelden:

1. Öffnen Sie den Anmeldeassistenten für den Credential Manager mit einem der folgenden Vorgehensweisen:
   - über den Windows-Anmeldebildschirm.
   - über den Infobereich mit einem Doppelklick auf das **HP ProtectTools Security Manager**-Symbol.
   - über die Seite „Credential Manager“ des ProtectTools Security Manager, indem Sie auf den Link **Anmelden** in der rechten oberen Ecke des Fensters klicken.
2. Befolgen Sie die Anleitungen auf dem Bildschirm, um sich bei Credential Manager anzumelden.

Erste Anmeldung

Zunächst müssen Sie sich jedoch bei Windows als Administrator anmelden. Melden Sie sich aber noch nicht beim Credential Manager an.

1. Öffnen Sie HP ProtectTools Security Manager, indem Sie im Infobereich auf das HP ProtectTools Security Manager-Symbol doppelklicken. Daraufhin wird das Fenster „HP ProtectTools Security Manager“ geöffnet.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**, und klicken Sie dann in der oberen rechten Ecke des rechten Fensterausschnitts auf **Anmelden**. Der Anmeldeassistent für den Credential Manager wird aufgerufen.
3. Geben Sie in das Feld **Kennwort** Ihr Windows-Kennwort ein, und klicken Sie auf **Weiter**.

Registrieren von Anmeldeinformationen

Auf der Seite „My Identity“ (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 und anstatt eines Windows-Kennworts Ihren Fingerabdruck zur Authentifizierung verwenden.

Einrichten des Fingerabdruck-Lesegeräts

1. Nachdem Sie sich bei Credential Manager angemeldet haben, wischen Sie mit Ihrem Finger über das Fingerabdruck-Lesegerät. Der Registrierungsassistent für den Credential Manager wird aufgerufen.
2. Befolgen Sie die Anleitungen auf dem Bildschirm, um die Registrierung Ihres Fingerabdrucks abzuschließen und das Fingerabdruck-Lesegerät einzurichten.
3. Um das Fingerabdruck-Lesegerät für einen anderen Windows-Benutzer einzurichten, melden Sie diesen Benutzer bei Windows an und wiederholen die Schritte 1 und 2.

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, um sich bei Windows anzumelden.

Registrieren einer Java Card, eines USB eToken oder eines virtuellen Token

HINWEIS: Sie müssen ein Kartenlesegerät oder eine Smart Card-Tastatur konfiguriert haben, um diesen Vorgang auszuführen. Wenn Sie keine Smart Card verwenden möchten, können Sie ein virtuelles Token registrieren, wie unter „Erstellen eines virtuellen Token“ auf Seite 16 beschrieben.

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**.
3. Klicken Sie im rechten Fensterausschnitt auf **Register Smart Card or Token** (SmartCard oder Token registrieren). Der Registrierungsassistent für den Credential Manager wird aufgerufen.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Registrieren eines USB eToken

1. Stellen Sie sicher, dass die USB eToken-Treiber installiert sind.

   HINWEIS: Weitere Informationen finden Sie im Benutzerhandbuch zum USB eToken.

2. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
3. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**.
4. Klicken Sie im rechten Fensterausschnitt auf **Register Smart Card or Token** (SmartCard oder Token registrieren). Der Registrierungsassistent für den Credential Manager wird aufgerufen.
5. Folgen Sie den Anleitungen auf dem Bildschirm.

Registrieren weiterer Anmeldeinformationen

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**.
3. Klicken Sie im rechten Fensterausschnitt auf **Register Credentials** (Anmeldeinformationen registrieren). Der Registrierungsassistent für den Credential Manager wird aufgerufen.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Allgemeine Aufgaben

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

- Erstellen eines virtuellen Token
- Ändern des Windows-Anmeldekennworts
- Verwalten einer Token-PIN
- Verwalten der Identität
- Sperren des Computers

HINWEIS: Diese Option ist nur dann verfügbar, wenn die klassische Anmeldeaufforderung des Credential Manager aktiviert ist. Siehe „Beispiel 1 – Verwenden der Seite „Erweiterte Einstellungen“, um die Anmeldung bei Windows im Credential Manager zu ermöglichen“ auf Seite 26.

Erstellen eines virtuellen Token

Ein virtuelles Token funktioniert im Wesentlichen wie eine Java Card oder ein USB eToken. Das Token wird entweder auf der Festplatte des Computers oder in der Registrierungsdatei von Windows gespeichert. Wenn Sie sich mit einem virtuellen Token anmelden, werden Sie aufgefordert, eine Benutzer-PIN einzugeben, um die Authentifizierung durchzuführen.

So erstellen Sie ein neues virtuelles Token:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**.
3. Klicken Sie im rechten Fensterausschnitt auf **Virtual Token** (Virtuelles Token). Der Registrierungsassistent für den Credential Manager wird aufgerufen.

HINWEIS: Wenn es keine Option **Virtual Token** (Virtuelles Token) gibt, verwenden Sie die Vorgehensweise für „Registrieren weiterer Anmeldeinformationen“ auf Seite 15.

4. Folgen Sie den Anleitungen auf dem Bildschirm.

Ändern des Windows-Anmeldekennworts

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**.
3. Klicken Sie im rechten Fensterausschnitt auf **Change Windows Password** (Windows-Kennwort ändern).
4. Geben Sie das alte Kennwort in das Feld **Altes Kennwort** ein.
5. Geben Sie Ihr neues Kennwort in die Felder **Neues Kennwort** und **Kennwort bestätigen** ein.
6. Klicken Sie auf **Fertig stellen**.

Ändern einer Token-PIN

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**.
3. Klicken Sie im rechten Fensterausschnitt auf **Change Token PIN** (Token-PIN ändern).

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.

Verwalten der Identität

Entfernen einer Identität aus dem System

HINWEIS: Ihr Windows-Benutzerkonto bleibt von diesem Löschvorgang unberührt.

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**.
3. Klicken Sie im rechten Fensterausschnitt auf **Clear Identity for this Account** (Identität für dieses Konto löschen).
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**. Ihre Identität wird abgemeldet und aus dem System entfernt.

Sperren des Computers

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 dann verfügbar, wenn die klassische Anmeldeaufforderung des Credential Manager aktiviert ist. Siehe „Beispiel 1 – Verwenden der Seite „Erweiterte Einstellungen“, um die Anmeldung bei Windows im Credential Manager zu ermöglichen“ auf Seite 26.

Ein zusätzliches Maß an Sicherheit erhalten Sie, wenn Sie die Funktion zum Sperren der Arbeitsstation so konfigurieren, dass der Schutz des Computers nur mithilfe einer Java Card, eines biometrischen Lesegeräts oder eines Token aufgehoben werden kann. Weitere Informationen finden Sie unter „Konfigurieren der Einstellungen des Credential Manager“ auf Seite 25.

So sperren Sie den Computer:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager**.
3. Klicken Sie im rechten Fensterausschnitt auf **Arbeitsstation sperren**. Der Windows-Anmeldebildschirm wird angezeigt. 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 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, um sich anzumelden.
2. Wenn Sie nicht Ihren Fingerabdruck für die Anmeldung bei Windows registriert haben, klicken Sie in der oberen linken Ecke des Bildschirms auf das Tastatursymbol neben dem Fingerabdrucksymbol. Der Anmeldeassistent für den Credential Manager wird aufgerufen.
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 **More** (Weitere) **> Wizard Options** (Assistent-Optionen).
   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.

Hinzufügen eines Kontos

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt auf **Windows-Anmeldung**, und klicken Sie dann auf **Add a Network Account** (Netzwerkkonto hinzufügen). Daraufhin wird der Assistent zum Hinzufügen eines Netzwerkkontos geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Entfernen eines Kontos

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt auf **Windows-Anmeldung**, und klicken Sie dann auf **Manage Network Accounts** (Netzwerkkonten verwalten). Daraufhin wird das Dialogfeld **Manage Network Accounts** (Netzwerkkonten verwalten) geöffnet.
4. Klicken Sie auf das Konto, das entfernt werden soll, und anschließend auf **Entfernen**.
5. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
6. Klicken Sie auf **OK**.

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 Single Sign On auch so konfigurieren, dass Ihre Authentifizierungsinformationen vor der Anmeldung bei einer sicheren Website oder Anwendung mithilfe einer Java Card, eines Fingerabdruck-Lesegeräts oder eines Token überprüft werden. Diese Funktion ist besonders nützlich für die Anmeldung bei Programmen oder Websites, die persönliche Informationen wie Kontonummern enthalten. Weitere Informationen finden Sie unter „Konfigurieren der Einstellungen des Credential Manager“ auf Seite 25.

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 auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt auf **Single Sign On** (Einmaliges Anmelden) und anschließend auf **Register New Application** (Neue Anwendung registrieren). Daraufhin wird der SSO-Anwendungsassistent geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Verwalten von Anwendungen und Anmeldeinformationen

Ändern der Anwendungseigenschaften

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Single Sign On** (Einmaliges Anmelden) auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).
4. Klicken Sie auf den Eintrag, den Sie ändern möchten, und anschließend auf **Eigenschaften**.
5. 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.
6. Klicken Sie auf die Registerkarte **Skript**, um das SSO-Anwendungsskript anzuzeigen und zu bearbeiten.
7. Klicken Sie auf **OK**.

Entfernen einer Anwendung aus Single Sign On

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Single Sign On** (Einmaliges Anmelden) auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).
4. Klicken Sie auf den Eintrag, den Sie entfernen möchten, und anschließend auf **Entfernen**.
5. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
6. 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 auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Single Sign On** (Einmaliges Anmelden) auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).
4. Klicken Sie auf den Anwendungseintrag, den Sie exportieren möchten. Klicken Sie dann auf **More** (Weitere) **> Applications** (Anwendungen) **> Export Script** (Skript exportieren).
5. Befolgen Sie die Anleitungen auf dem Bildschirm, um den Export durchzuführen.
6. Klicken Sie auf **OK**.

Importieren einer Anwendung

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Single Sign On** (Einmaliges Anmelden) auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).
4. Klicken Sie auf den Anwendungseintrag, den Sie importieren möchten. Wählen Sie anschließend **More** (Weitere) **> Applications** (Anwendungen) **> Import Script** (Skript importieren).
5. Befolgen Sie die Anleitungen auf dem Bildschirm, um den Import durchzuführen.
6. Klicken Sie auf **OK**.

Ändern der Anmeldeinformationen

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Single Sign On** (Einmaliges Anmelden) auf **Manage Applications and Credentials** (Anwendungen und Anmeldeinformationen verwalten).
4. Klicken Sie auf den Eintrag, den Sie ändern möchten, und anschließend auf **More** (Mehr).
5. Wählen Sie eine der folgenden Optionen:
   - 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.
6. Folgen Sie den Anleitungen auf dem Bildschirm.
7. 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 auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Application Protection** (Anwendungsschutz) auf **Manage Protected Applications** (Geschützte Anwendungen verwalten). Das Dialogfeld **Application Protection Service** (Dienst zum Anwendungsschutz) wird geöffnet.
4. 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.

5. Klicken Sie auf **Hinzufügen**. Daraufhin wird der Assistent zum Hinzufügen eines Programms geöffnet.
6. Folgen Sie den Anleitungen auf dem Bildschirm.

Entfernen des Schutzes für eine Anwendung

So entfernen Sie Einschränkungen von einer Anwendung:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Application Protection** (Anwendungsschutz) auf **Manage Protected Applications** (Geschützte Anwendungen verwalten). Das Dialogfeld **Application Protection Service** (Dienst zum Anwendungsschutz) wird geöffnet.
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 **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Credential Manager** und anschließend **Dienste und Anwendungen**.

3. Klicken Sie im rechten Fensterausschnitt unter **Application Protection** (Anwendungsschutz) auf **Manage Protected Applications** (Geschützte Anwendungen verwalten). Das Dialogfeld **Application Protection Service** (Dienst zum Anwendungsschutz) wird geöffnet.

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

6. 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))

7. 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.

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

9. Klicken Sie auf **OK**.

Erweiterte Aufgaben (nur für Administratoren)

Die Seiten „Authentication and Credentials“ (Authentifizierung und Anmeldeinformationen) und „Erweiterte Einstellungen“ im Credential Manager stehen nur Benutzern mit Administratorrechten zur Verfügung. Auf der Seite „My Identity“ (Meine Identität) können Sie die folgenden Aufgaben ausführen:

- Festlegen der Anmeldung für Benutzer und Administratoren
- Konfigurieren benutzerdefinierter Authentifizierungsanforderungen
- Konfigurieren der Anmeldeeigenschaften
- Konfigurieren der Einstellungen des Credential Manager

Festlegen der Anmeldung für Benutzer und Administratoren

Auf der Seite „Authentication and Credentials“ (Authentifizierung und Anmeldeinformationen) können Sie die Art oder Kombination der Anmeldeinformationen für Benutzer oder Administratoren festlegen.

So legen Sie die Anmeldung für Benutzer und Administratoren fest:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager** und anschließend auf **Authentication and Credentials** (Authentifizierung und Anmeldeinformationen).
3. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Authentifizierung**.
4. Klicken Sie in der Kategorieliste auf die gewünschte Kategorie (**Benutzer** oder **Administratoren**).
5. Klicken Sie in der Liste auf die Art oder Kombination der zu verwendenden Authentifizierungsmethoden.
6. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Konfigurieren benutzerdefinierter Authentifizierungsanforderungen

Wenn die gewünschten Authentifizierungsinformationen nicht auf der Registerkarte „Authentifizierung“ auf der Seite „Authentication and Credentials“ (Authentifizierung und Anmeldeinformationen) aufgeführt sind, können Sie benutzerdefinierte Anforderungen erstellen.

So konfigurieren Sie benutzerdefinierte Anforderungen:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager** und anschließend auf **Authentication and Credentials** (Authentifizierung und Anmeldeinformationen).
3. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Authentifizierung**.
4. Klicken Sie in der Kategorieliste auf die gewünschte Kategorie (**Benutzer** oder **Administratoren**.
5. Klicken Sie in der Liste der Authentifizierungsmethoden auf **Benutzerdefiniert**.
6. Klicken Sie auf **Konfigurieren**.
7. Wählen Sie die zu verwendenden Authentifizierungsmethoden.

8. Legen Sie die Kombination der Methoden fest, indem Sie auf eine der folgenden Optionen klicken:

   - Verwenden Sie AND, um die Authentifizierungsmethoden zu kombinieren.

     (Die Benutzer müssen sich bei jeder Anmeldung mit allen ausgewählten Methoden authentifizieren.)

   - Verwenden Sie OR, um zwei oder mehr Authentifizierungsmethoden anzufordern.

     (Die Benutzer können bei jeder Anmeldung wählen, mit welcher der ausgewählten Methoden sie sich authentifizieren.)

9. Klicken Sie auf **OK**.

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

Konfigurieren der Anmeldeeigenschaften

Auf der Registerkarte „Anmeldeinformationen“ auf der Seite „Authentication and Credentials“ (Authentifizierung und Anmeldeinformationen) können Sie die Liste der verfügbaren Authentifizierungsmethoden anzeigen und die Einstellungen ändern.

So konfigurieren Sie die Anmeldeinformationen:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.

2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager** und anschließend auf **Authentication and Credentials** (Authentifizierung und Anmeldeinformationen).

3. Klicken Sie im rechten Fensterausschnitt 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 „Erweiterte Einstellungen“ haben Sie Zugriff auf verschiedene Einstellungen, die Sie über die folgenden Registerkarten ändern können:

- 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. Behandlung bei der Erkennung von Anmeldebildschirmen, 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 auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager** und dann auf **Einstellungen**.
3. Klicken Sie im rechten Fensterausschnitt auf die entsprechende Registerkarte für die Einstellungen, die Sie ändern möchten.
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 auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager** und dann auf **Einstellungen**.
3. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Allgemein**.
4. Aktivieren Sie unter **Select the way users log on to Windows (requires restart)** (Art der Benutzeranmeldung bei Windows wählen (Neustart erforderlich)) das Kontrollkästchen **Use Credential Manager with classic logon prompt** (Credential Manager mit klassischer Anmeldeaufforderung verwenden).
5. Klicken Sie auf **Übernehmen** und dann auf **OK**.
6. Starten Sie den Computer neu.

HINWEIS: Durch Aktivieren des Kontrollkästchens **Use Credential Manager with classic logon prompt** (Credential Manager mit klassischer Anmeldeaufforderung verwenden) können Sie Ihren Computer sperren. Siehe „Sperren des Computers“ auf Seite 17.

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

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Credential Manager** und dann auf **Einstellungen**.
3. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Single Sign On**.
4. 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).
5. Klicken Sie auf **Übernehmen** und dann auf **OK**.
6. Starten Sie den Computer neu.

3 Embedded Security for HP ProtectTools

HINWEIS: Der integrierte TPM-Sicherheits-Chip (Trusted Platform Module) 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:

- Erweitertes EFS (Encrypting File System, EFS) von Microsoft® für die Verschlüsselung von Ordnern und Dateien
- Erstellung eines PSD (Personal Secure Drive) zum Schützen von Benutzerdaten auf einem versteckten Laufwerk
- 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

Der integrierte TPM-Sicherheitschip erweitert und aktiviert weitere Funktionen von HP ProtectTools Security Manager. Credential Manager for HP ProtectTools kann z. B. den integrierten Chip als Authentifizierungsfaktor verwenden, wenn sich der Benutzer bei Windows anmeldet. Auf bestimmten Modellen aktiviert der integrierte TPM-Sicherheitschip zusätzlich erweiterte BIOS-Sicherheitsfunktionen, auf die über BIOS Configuration for HP ProtectTools zugegriffen wird.

Setup

△ **ACHTUNG:** Es wird dringend empfohlen, dass der IT-Administrator den integrierten Sicherheits-Chip 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 integrierten Sicherheits-Chip.

Aktivieren des integrierten Sicherheits-Chips

Der Embedded Security-Chip muss im Computer Setup Utility aktiviert werden. Dieser Vorgang kann nicht in BIOS Configuration for HP ProtectTools ausgeführt werden.

So aktivieren Sie den integrierten Sicherheits-Chip:

1. Öffnen Sie Computer Setup, indem Sie den Computer einschalten oder neu starten. Drücken Sie dann die Taste F10, während die Meldung **F10 = ROM Based Setup** (F10 = ROM-basiertes Setup) unten links auf dem Bildschirm angezeigt wird.
2. Wenn Sie kein Administratorkennwort festgelegt haben, verwenden Sie die Pfeiltasten, um **Sicherheit > Setup-Kennwort** zu wählen, und drücken Sie dann die Eingabetaste.
3. Geben Sie Ihr Kennwort in die Felder **Neues Kennwort** und **Neues Kennwort bestätigen** ein, und drücken Sie die Taste 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 Konfiguration von Embedded Security zu übernehmen.
8. Wenn Sie Ihre Einstellungen speichern und Computer Setup beenden möchten, verwenden Sie die Pfeiltasten, um **Datei > Änderungen speichern und beenden** zu wählen. Folgen Sie den Anleitungen auf dem Bildschirm.

Initialisieren des integrierten Sicherheits-Chips

Während des Initialisierungsvorgangs für Embedded Security führen Sie Folgendes aus:

- Richten Sie ein Eigentümerkennwort für den integrierten Sicherheits-Chip ein, um den Zugriff auf alle Eigentümerfunktionen auf dem integrierten Sicherheits-Chip 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 integrierten Sicherheits-Chip:

1. Klicken Sie mit der rechten Maustaste auf das Symbol „HP ProtectTools Security Manager“ im Infobereich (außen rechts in der Taskleiste), und wählen Sie dann **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 von Embedded Security nicht geöffnet ist, wählen Sie **Start > Alle Programme > HP ProtectTools Security Manager**.
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 E-Mail sicher zu verwenden, müssen Sie zuerst den E-Mail-Client so konfigurieren, dass ein digitales Zertifikat, das mit Embedded Security erstellt wurde, verwendet wird. Wenn kein digitales Zertifikat verfügbar ist, müssen Sie ein digitales Zertifikat von der Zertifizierungsstelle anfordern. Anleitungen zum Konfigurieren der E-Mail und Anfordern eines digitalen Zertifikats finden Sie in der Online-Hilfe des E-Mail-Clients.

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:

- Es können nur Dateien und Ordner auf Windows-Partitionen verschlüsselt werden. Dateien und Ordner auf MS-DOS-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 Ihnen, verschlüsselte E-Mails zu senden und zu empfangen. Die Verfahrensweise hängt jedoch vom Programm ab, das Sie für den Zugriff auf E-Mails verwenden. Weitere Informationen hierzu finden Sie in der Online-Hilfe zu Embedded Security und der Online-Hilfe zu Ihrem E-Mail-Programm.

Ändern des Kennworts für den allgemeinen Benutzerschlüssel

So ändern Sie das Kennwort für den allgemeinen Benutzerschlüssel:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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 > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Bereich auf **Backup** (Sichern). Daraufhin wird der Sicherungsassistent für Embedded Security 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 > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Bereich auf **Restore** (Wiederherstellen). Daraufhin wird der Sicherungsassistent für Embedded Security geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Ändern des Eigentümerkennworts

So ändern Sie das Eigentümerkennwort:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Erweitert**.
3. Klicken Sie im rechten Fensterausschnitt unter **Owner Password** (Besitzerkennwort) 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

Ein Administrator kann einem Benutzer helfen, ein vergessenes Kennwort erneut einzurichten. Weitere Informationen hierzu finden Sie in der Online-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 > HP ProtectTools Security Manager**.
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 > HP ProtectTools Security Manager**.
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 erhalten Sie in der Online-Hilfe zu Embedded Security.

4 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. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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 „HP ProtectTools Backup and Restore“ auf Seite 9.

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. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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**.

5 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 Funktionen in BIOS Configuration for HP ProtectTools stehen auch in F10 Setup zur Verfügung. Eine detaillierte Anleitung zur Verwendung von F10 Setup finden Sie in dem im Lieferumfang Ihres Computers oder im BIOS-Update enthaltenen Computer Setup (F10) Utility-Handbuch.

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.

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)

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)

Stromzufuhr

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)

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)
- AMT Options (AMT-Optionen)

6 Device Access Manager for HP ProtectTools

Dieses Sicherheitstool ist nur für Administratoren verfügbar. Device Access Manager ermöglicht die benutzerdefinierte Steuerung der Datenspeicher und Übertragungshardware (USB, COM- und LPT-Anschlüsse, CD-Laufwerke, Netzwerkschnittstellenkarten, persönliche Musikwiedergabegeräte usw.). Zusätzlich können mit Device Access Manager Benutzer und Benutzergruppen verwaltet werden, um den Lese- und Schreibzugriff zu ermöglichen und den Zugriff auf Daten auf der Hardware zuzulassen oder zu verweigern.

Starten des Hintergrunddienstes

Wenn Geräteprofile angewendet werden sollen, muss der HP ProtectTools Hintergrund-Service zum Sperren/Prüfen des Geräts ausgeführt werden. Wenn Sie erstmalig versuchen, Geräteprofile anzuwenden, öffnet HP ProtectTools Security Manager ein Dialogfeld, in dem Sie gefragt werden, ob Sie diesen Hintergrund-Service starten möchten. Klicken Sie auf **Yes** (Ja), um den Hintergrund-Service zu starten, und legen Sie fest, dass dieser Service bei jedem Systemstart automatisch aktiviert werden soll.

Einfache Konfiguration

Mit dieser Funktion können Sie folgenden Geräteklassen den Zugriff verweigern:

- Alle Wechseldatenträger (Disketten, USB-Speichersticks, USB usw.) für alle Nicht-Administratoren
- Alle DVD/CD-ROM-Laufwerke für Nicht-Administratoren
- Alle seriellen und parallelen Anschlüsse für Nicht-Administratoren
- Alle Bluetooth-, Infrarot-, Modem-, PCMCIA-Geräte, persönliche Musikwiedergabegeräte und alle 1394 (FireWire)-Geräte für alle 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 > HP ProtectTools Security Manager**.
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 sind weitere Auswahlmöglichkeiten verfügbar, um bestimmten Benutzern oder Benutzergruppen den Zugriff auf Gerätetypen zu gewähren oder zu verweigern. Einige Klassen ermöglichen die Konfiguration von schreibgeschütztem Zugriff oder Schreibzugriff.

Hinzufügen eines Benutzers oder einer Gruppe

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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. Wählen Sie **Advanced** (Erweitert) **> Find Now** (Jetzt suchen), um nach Benutzern oder Gruppen zu suchen, die hinzugefügt werden sollen.
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 > HP ProtectTools Security Manager**.
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 > HP ProtectTools Security Manager**.
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**.

Zulassen des Zugriffs auf eine Geräteklasse für einen Benutzer einer Gruppe

Sie können einem Benutzer den Zugriff auf eine Geräteklasse erlauben, während Sie allen anderen Mitgliedern dieser Benutzergruppe den Zugriff verweigern.

So erlauben Sie den Zugriff für einen Benutzer, jedoch nicht für die Gruppe:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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. Fügen Sie unter **User/Groups** (Benutzer/Gruppen) die Gruppe hinzu, welcher der Zugriff verweigert werden soll.
5. Klicken Sie neben der Gruppe, welcher der Zugriff verweigert werden soll, auf **Verweigern**.
6. Navigieren Sie zu dem Ordner unterhalb des Ordners für die erforderliche Klasse, und fügen Sie den bestimmten Benutzer hinzu. Klicken Sie auf **Zulassen**, um diesem Benutzer den Zugriff zu gewähren.
7. Klicken Sie auf **Übernehmen** und dann auf **OK**.

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

Sie können einem Benutzer den Zugriff auf ein bestimmtes Gerät erlauben, während Sie allen anderen Mitgliedern dieser Benutzergruppe den Zugriff auf alle Geräte in der Klasse verweigern.

So erlauben Sie den Zugriff auf ein bestimmtes Gerät für einen Benutzer, jedoch nicht für die Gruppe:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
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, und navigieren Sie dann zu dem untergeordneten Ordner.
4. Fügen Sie unter **User/Groups** (Benutzer/Gruppen) die Gruppe hinzu, welcher der Zugriff verweigert werden soll.
5. Klicken Sie neben der Gruppe, welcher der Zugriff verweigert werden soll, auf **Verweigern**.
6. Navigieren Sie in der Geräteliste zu dem bestimmten Gerät, das für den Benutzer zugelassen werden soll.
7. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Select Users or Groups** (Benutzer oder Gruppen auswählen) wird geöffnet.
8. Wählen Sie **Advanced** (Erweitert) **> Find Now** (Jetzt suchen), um nach Benutzern oder Gruppen zu suchen, die hinzugefügt werden sollen.
9. Klicken Sie auf einen Benutzer, dem der Zugriff gewährt werden soll, und klicken Sie dann auf **OK**.
10. Klicken Sie auf **Zulassen**, um diesem Benutzer den Zugriff zu gewähren.
11. Klicken Sie auf **Übernehmen** und dann auf **OK**.

7 Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools kann alle Informationen auf einer einzelnen Festplatte, einer Partition oder auf mehreren Festplatten verschlüsseln, so dass sie für unbefugte Personen nicht lesbar sind.

△ **ACHTUNG:** Wenn Sie das Modul Drive Encryption deinstallieren möchten, müssen zunächst alle verschlüsselten Laufwerke entschlüsselt werden. Wenn Sie die Entschlüsselung nicht vornehmen, können Sie nur dann auf die Daten der verschlüsselten Laufwerke zugreifen, wenn Sie beim Drive Encryption Wiederherstellungsdienst registriert sind (siehe „Wiederherstellung“ auf Seite 54). Auch nach einer Neuinstallation von Drive Encryption ist der Zugriff auf die verschlüsselten Laufwerke nicht möglich.

Verschlüsselungsverwaltung

Verschlüsseln eines Laufwerks

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **Encryption Management** (Verschlüsselungsverwaltung).
3. Klicken Sie im rechten Fensterausschnitt auf **Activate** (Aktivieren). Der Assistent für das Modul Drive Encryption for HP ProtectTools wird geöffnet.
4. Befolgen Sie die Anleitungen auf dem Bildschirm, um die Verschlüsselung zu aktivieren.

HINWEIS: Sie müssen eine Diskette, einen Flash-Datenträger oder ein anderes USB-Speichermedium angeben, auf der/dem die Wiederherstellungsdaten gespeichert werden sollen.

Ändern der Verschlüsselung

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **Encryption Management** (Verschlüsselungsverwaltung).
3. Klicken Sie im rechten Fensterausschnitt auf **Change encryption** (Verschlüsselung ändern). Wählen Sie im Dialogfeld **Change Encryption** (Verschlüsselung ändern) die zu verschlüsselnden Laufwerke aus, und klicken Sie dann auf **OK**.
4. Klicken Sie auf **OK**, um die Verschlüsselung zu starten.

Entschlüsseln eines Laufwerks

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **Encryption Management** (Verschlüsselungsverwaltung).
3. Klicken Sie im rechten Fensterausschnitt auf **Deactivate** (Deaktivieren).

Benutzerverwaltung

Hinzufügen eines Benutzers

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **User Management** (Benutzerverwaltung).
3. Klicken Sie im rechten Fensterausschnitt auf **Hinzufügen**. Klicken Sie in der Liste **User Name** (Benutzername) auf einen Benutzernamen, oder geben Sie in das Feld **Username** (Benutzername) einen Benutzernamen ein. Klicken Sie auf **Weiter**.
4. Geben Sie das Windows-Kennwort für den ausgewählten Benutzer ein, und klicken Sie dann auf **Weiter**.
5. Wählen Sie eine Authentifizierungsmethode für den neuen Benutzer, und klicken Sie anschließend auf **Fertig stellen**.

Entfernen eines Benutzers

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **User Management** (Benutzerverwaltung).
3. Klicken Sie im rechten Fensterausschnitt auf den Benutzernamen, der aus der Liste **User Name** (Benutzername) entfernt werden soll. Klicken Sie auf **Entfernen**.
4. Klicken Sie auf **Ja**, um zu bestätigen, dass der Benutzer entfernt werden soll.

Ändern eines Token

So ändern Sie die Authentifizierungsmethode für einen Benutzer:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **User Management** (Benutzerverwaltung).
3. Klicken Sie im rechten Fensterausschnitt auf einen Benutzernamen in der Liste **User Name** (Benutzername) und anschließend auf **Change Token** (Token ändern).
4. Geben Sie das Windows-Kennwort des Benutzers ein, und klicken Sie dann auf **Weiter**.
5. Wählen Sie eine neue Authentifizierungsmethode, und klicken Sie anschließend auf **Fertig stellen**.
6. Wenn Sie eine Java Card als Authentifizierungsmethode gewählt haben, geben Sie bei der entsprechenden Aufforderung das Java Card-Kennwort ein und klicken anschließend auf **OK**.

Einrichten eines Kennworts

So können Sie ein Kennwort für die Authentifizierungsmethode eines Benutzers einrichten bzw. ändern:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **User Management** (Benutzerverwaltung).
3. Wählen Sie im rechten Fensterausschnitt den Benutzernamen aus der Liste **User Name** (Benutzername) und anschließend **Set Password** (Kennwort einrichten).
4. Geben Sie das Windows-Kennwort des Benutzers ein, und klicken Sie dann auf **Weiter**.

5. Wählen Sie die neue Authentifizierungsmethode, und klicken Sie anschließend auf **Fertig stellen**.

6. Wenn Sie eine Java Card als Authentifizierungsmethode gewählt haben, geben Sie bei der entsprechenden Aufforderung das Java Card-Kennwort ein und klicken anschließend auf **OK**.

Wiederherstellung

Die folgenden beiden Optionen stehen zur Auswahl:

- Wenn Sie Ihr Kennwort vergessen haben, können Sie auf Ihre verschlüsselten Laufwerke nicht zugreifen. Durch eine Registrierung beim Drive Encryption Wiederherstellungsdienst erhalten Sie jedoch die Möglichkeit, auch dann auf Ihren Computer zuzugreifen, wenn Sie das Kennwort vergessen haben.
- Sie können die Drive Encryption Schlüssel auf einer Diskette, einem Flash-Datenträger oder einem anderweitigen USB-Speichermedium sichern.

Registrieren beim Drive Encryption Wiederherstellungsdienst

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **Wiederherstellen**.
3. Klicken Sie im rechten Fensterausschnitt auf **Click here to register** (Für Registrierung hier klicken). Geben Sie die erforderlichen Informationen ein, um die Registrierung abzuschließen.

Sichern der Drive Encryption Schlüssel

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fensterausschnitt die Option **Drive Encryption** und anschließend **Wiederherstellen**.
3. Klicken Sie im rechten Fensterausschnitt auf **Click here to backup your keys** (Für Schlüsselsicherung hier klicken).
4. Wählen Sie eine Diskette, einen Flash-Datenträger oder ein anderes USB-Speichermedium aus, auf der/dem die Wiederstellungsdaten gespeichert werden sollen, und klicken Sie dann auf **Weiter**. Der Assistent für das Modul Drive Encryption for HP ProtectTools wird geöffnet.
5. Befolgen Sie die Anleitungen auf dem Bildschirm, um die Schlüssel für Drive Encryption zu sichern.

HINWEIS: Sie müssen eine Diskette, einen Flash-Datenträger oder ein anderes USB-Speichermedium angeben, auf der/dem die Wiederstellungsdaten gespeichert werden sollen.

8 Fehlerbeseitigung

Credential Manager for HP ProtectTools

Kurzbeschreibung	Einzelheiten	Lösung
Mithilfe der Option **Credential Manager Network Accounts** (Credential Manager-Netzwerkkonten) kann ein Benutzer auswählen, an welchem Domänenkonto er sich anmeldet. Wenn die TPM-Authentifizierung verwendet wird, ist diese Option nicht verfügbar. Alle anderen Authentifizierungs-methoden funktionieren ordnungsgemäß.	Bei der TPM-Authentifizierung ist der Benutzer nur am lokalen Computer angemeldet.	Mit Tools zur einmaligen Anmeldung (Single-Sign-On) von Credential Manager können Benutzer andere Konten authentifizieren.
Die USB-Token-Zugangsdaten stehen für die Anmeldung bei Windows XP Service Pack 1 nicht zur Verfügung.	Nach der Installation der USB-Token-Software, der Registrierung der USB-Token-Zugangsdaten und dem Einrichten von Credential Manager als primäre Anmeldungsoption wird das USB-Token in der GINA-Anmeldung von Credential Manager weder aufgelistet, noch ist es dort verfügbar. Wenn Sie sich wieder bei Windows anmelden, sich bei Credential Manager abmelden und dann erneut bei Credential Manager anmelden und das Token als primäre Anmeldung wählen, funktioniert die Token-Anmeldung ordnungsgemäß.	Dieser Fehler tritt nur unter Windows XP Service Pack 1 auf. Aktualisieren Sie zur Fehlerbehebung Ihre Windows-Version mithilfe der Windows Update-Website auf Service Pack 2. Falls Sie weiterhin mit Service Pack 1 arbeiten möchten, melden Sie sich mit anderen Zugangsdaten (Windows-Kennwort) erneut bei Windows an, um sich bei Credential Manager abzumelden und dann wieder anzumelden.
Auf einigen Webseiten von Anwendungen treten Fehler auf, die Benutzer darin hindern, bestimmte Aufgaben auszuführen oder zu beenden.	Einige webbasierte Anwendungen stürzen ab und erzeugen Fehler, die auf das Deaktivierungsmuster der einmaligen Anmeldung zurückzuführen sind. In Internet Explorer wird beispielsweise beim Auftreten eines Fehlers ein **!** in einem gelben Dreieck angezeigt.	Die Single-Sign-On-Funktion von Credential Manager unterstützt nicht alle Software-Webschnittstellen. Deaktivieren Sie die Unterstützung für die Single-Sign-On-Funktion für eine bestimmte Webseite, indem Sie die entsprechende Option deaktivieren. Weitere Informationen finden Sie in der umfassenden Dokumentation zur Single-Sign-On-Funktion, die in den Hilfedateien von Credential Manager verfügbar ist. Wenn die Single-Sign-On-Funktion für eine bestimmte Anwendung nicht deaktiviert werden kann, wenden Sie sich an den Service und Support von HP, und fordern Sie über Ihren HP Service-Ansprechpartner Third-Level-Support an.
Die Option **Browse for Virtual Token** (Nach virtuellem Token suchen)	Der Benutzer kann den Speicherort des registrierten virtuellen Token in Credential Manager nicht ändern, da die	Die Option zum Durchsuchen wurde aus den aktuellen Produkten entfernt, da sie es unberechtigten Benutzern

Kurzbeschreibung	Einzelheiten	Lösung
ist während des Anmeldeprozesses nicht verfügbar.	Option zum Durchsuchen auf Grund von Sicherheitsrisiken entfernt wurde.	ermöglicht, Dateien zu löschen und umzubenennen und die Kontrolle über Windows zu übernehmen.
Bei der Anmeldung mit TPM-Authentifizierung steht die Option **Network Accounts** (Netzwerkkonten) nicht zur Verfügung.	Mit der Option **Network Accounts** (Netzwerkkonten) kann ein Benutzer das Domänenkonto auswählen, an dem er sich anmeldet. Wenn die TPM-Authentifizierung verwendet wird, ist diese Option nicht verfügbar.	HP arbeitet an einer Lösung für zukünftige Produkte.
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 Kennwort eines Domänenbenutzerkontos nicht über die Option **Change Windows password** (Windows-Kennwort ändern) ändern. Mit Credential Manager können nur die Kennwörter für Konten auf lokalen PCs geändert werden. Der Domänenbenutzer kann das eigene Kennwort über die Option **Windows security** (Windows-Sicherheit) **> Change password** (Kennwort ändern) ändern. Da der Domänenbenutzer jedoch kein Konto auf dem lokalen PC besitzt, kann Credential Manager nur das Anmeldekennwort ändern.
Die Funktion zum einmaligen Anmelden (Single-Sign-On) von Credential Manager sollte standardmäßig zur Kennworteingabe auffordern, um eine Schleife zu verhindern.	Standardmäßig protokolliert die Single-Sign-On-Funktion Benutzer automatisch. Beim Erstellen des zweiten Dokuments von zwei Dokumenten mit Kennwortschutz verwendet Credential Manager jedoch das letzte aufgezeichnete Kennwort, d. h. das Kennwort des ersten Dokuments.	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.
Inkompatibilitätsprobleme mit der GINA-Anmeldung für Corel WordPerfect 12.	Wenn sich ein Benutzer bei Credential Manager anmeldet, in WordPerfect ein Dokument erstellt und dieses mit einem Kennwortschutz belegt, kann Credential Manager weder manuell noch automatisch die GINA-Anmeldung erkennen.	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.
Credential Manager erkennt die Schaltfläche **Connect** (Verbinden) auf dem Bildschirm nicht.	Wenn die Zugangsdaten der Single-Sign-On-Funktion für Remote Desktop Connection (RDP) auf **Connect** (Verbinden) eingestellt sind, gibt die Single-Sign-On-Funktion bei Neustart stets **Save As** (Speichern unter) anstatt **Connect** (Verbinden) ein.	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.
Der ATI Catalyst-Konfigurationsassistent kann in Credential Manager nicht verwendet werden.	Die Single-Sign-On-Funktion von Credential Manager verursacht einen Konflikt mit dem ATI Catalyst-Konfigurationsassistenten.	Deaktivieren Sie die Single-Sign-On-Funktion für Credential Manager.
Wenn bei der Anmeldung mit TPM-Authentifizierung die Schaltfläche **Back** (Zurück) auf dem Bildschirm verwendet wird, kann keine andere Authentifizierungsmethode ausgewählt werden.	Wenn ein Benutzer bei der Anmeldung bei Credential Manager die TPM-Authentifizierung verwendet, das Kennwort eingibt und dann auf die Schaltfläche **Back** (Zurück) klickt, funktioniert diese nicht ordnungsgemäß. Anstatt eine Auswahl anderer Authentifizierungsmethoden anzuzeigen, wird sofort der Windows-Anmeldebildschirm angezeigt.	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.

Kurzbeschreibung	Einzelheiten	Lösung
Credential Manager wird aus dem Standby-Modus geöffnet, auch wenn das Programm nicht entsprechend konfiguriert ist.	Wenn **Use Credential Manager log on to Windows** (Credential Manager-Anmeldung für Windows verwenden) nicht als Option ausgewählt ist, sodass das System in den S3-Standby-Modus wechseln kann, wird bei erneuter Aktivierung des Systems die Credential Manager-Anmeldung für Windows geöffnet.	Wenn kein Administratorkennwort eingerichtet ist, können sich Benutzer auf Grund von Kontobeschränkungen von Credential Manager nicht über Credential Manager bei Windows anmelden. • Ohne Java Card/Token können die Benutzer die Credential Manager-Anmeldung abbrechen. Daraufhin wird die Microsoft Windows-Anmeldung angezeigt. Die Benutzer können sich an diesem Punkt anmelden. • Mit Java Card/Token können die Benutzer mit der folgenden Behelfslösung beim Einsetzen einer Java Card das Öffnen von Credential Manager aktivieren/deaktivieren. 1. Klicken Sie auf **Advanced Settings** (Erweiterte Einstellungen). 2. Klicken Sie auf **Service & Applications** (Service & Anwendungen). 3. Klicken Sie auf **Java Cards and Tokens** (Java Cards und Tokens). 4. Klicken Sie, wenn die Java Card/das Token eingesetzt wird. 5. Aktivieren Sie das Kontrollkästchen **Advise to log-on** (Benachrichtigung zur Anmeldung).
Die Benutzer verlieren alle durch das TPM geschützten Credential Manager-Zugangsdaten, wenn das TPM-Modul entfernt oder beschädigt wird.	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 ist so konzipiert, dass es die Credential Manager-Zugangsdaten schützt. HP empfiehlt, dass die Benutzer eine Sicherungskopie der Benutzeridentität in Credential Manager erstellen, bevor sie das TPM-Modul entfernen.
Credential Manager ist unter Windows 2000 nicht als primäre Anmeldung eingestellt.	Während der Installation von Windows 2000 wird die Anmelderichtlinie auf manuelle oder automatische Administratoranmeldung eingestellt. Wird die automatische Anmeldung gewählt, setzt die standardmäßige Windows-Registrierungseinstellung den Wert für die automatische Standard-Administratoranmeldung auf 1. Dieser Wert wird von Credential Manager nicht überschrieben.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Wenn der Benutzer die Betriebssystemeinstellungen für die Werte der automatischen Administratoranmeldung zum Überspringen ändern möchte, lautet der Pfad zum Bearbeiten folgendermaßen: `HKEY_LOCAL_MACHINE/ Software/Microsoft/ WindowsNT/ CurrentVersion/WinLogon`. **ACHTUNG:** Die Verwendung des Registrierungs-Editors erfolgt auf eigene Gefahr! Der falsche Einsatz des Registrierungs-Editors (regedit) kann zu schwerwiegenden Problemen führen. Im schlimmsten Fall müssen Sie das Betriebssystem neu installieren. Teilweise können die aufgetretenen Probleme so schwerwiegend sein, dass sie nicht gelöst werden können.
Es wird eine Meldung zur Anmeldung per Fingerabdruck angezeigt, unabhängig davon, ob das Lesegerät für Fingerabdrücke installiert oder registriert ist.	Wenn der Benutzer die Windows-Anmeldung wählt, wird in der Taskleiste von Credential Manager folgende Desktop-Warnung angezeigt: **You can place your finger on the fingerprint reader to log on to Credential Manager (Legen Sie Ihren Finger auf das Lesegerät für Fingerabdrücke, um**	Mit dieser Desktop-Warnung soll der Benutzer darauf hingewiesen werden, dass die Authentifizierung per Fingerabdruck verfügbar ist, wenn sie konfiguriert wurde.

Kurzbeschreibung	Einzelheiten	Lösung
	sich bei Credential Manager anzumelden).	
Im Anmeldefenster von Credential Manager für Windows 2000 wird der Benutzer aufgefordert, seine Karte einzusetzen (**insert card**), obwohl kein Lesegerät angeschlossen ist.	Auf der Windows-Willkommenseite in Credential Manager wird der Benutzer aufgefordert, seine Karte einzusetzen (**insert card**), obwohl kein Java Card-Lesegerät angeschlossen ist.	Mit dieser Meldung soll der Benutzer darauf hingewiesen werden, dass die Java Card-Authentifizierung verfügbar ist, wenn sie konfiguriert wurde.
Die Anmeldung bei Credential Manager schlägt fehl, nachdem das System in den Standby-Modus und dann in den Ruhezustand gewechselt ist. Dieser Fehler tritt nur unter Windows XP Service Pack 1 auf.	Nachdem das System in den Standby-Modus und dann in den Ruhezustand gewechselt ist, können sich Administratoren oder Benutzer nicht bei Credential Manager anmelden, und der Windows-Anmeldebildschirm wird unabhängig von den verwendeten Zugangsdaten (Kennwort, Fingerabdruck oder Java Card) angezeigt.	Dieses Problem scheint in Service Pack 2 von Microsoft behoben worden zu sein. Weitere Informationen zum Ursprung dieses Problems finden Sie unter http://www.microsoft.com in Artikel 813301 der Microsoft Knowledge Base. Zum Anmelden muss der Benutzer Credential Manager auswählen und sich dann anmelden. Nach der Anmeldung bei Credential Manager wird der Benutzer aufgefordert, sich bei Windows anzumelden (möglicherweise muss die entsprechende Option ausgewählt werden), um den Anmeldevorgang abzuschließen. Wenn sich die Benutzer zuerst bei Windows anmelden, müssen sie sich anschließend manuell bei Credential Manager anmelden.

Kurzbeschreibung	Einzelheiten	Lösung
Bei der Wiederherstellung von Embedded Security schlägt Credential Manager fehl.	Die Registrierung der Zugangsdaten in Credential Manager schlägt fehl, nachdem die Werkseinstellungen des ROM wiederhergestellt wurden.	HP Credential Manager for ProtectTools kann nicht auf das TPM zugreifen, falls das ROM nach der Installation von Credential Manager auf die Werkseinstellungen zurückgesetzt wurde. Der integrierte TPM-Sicherheitschip kann mit dem Dienstprogramm BIOS Computer Setup, BIOS Configuration for ProtectTools oder mit dem HP Client Manager aktiviert werden. So aktivieren Sie den integrierten TPM-Sicherheitschip: 1. Öffnen Sie Computer Setup, indem Sie den Computer einschalten oder neu starten. Drücken Sie dann die Taste F10, während die Meldung **F10 = ROM Based Setup** (F10 = ROM-basiertes Setup) unten links auf dem Bildschirm angezeigt wird. 2. Wählen Sie mithilfe der Pfeiltasten die Funktion **Sicherheit > Setup-Kennwort**. Legen Sie ein Kennwort fest. 3. Wählen Sie **Embedded Security Device** (Embedded Security-Chip). 4. Wählen Sie mit den Pfeiltasten **Embedded Security Device – Disable** (Embedded Security-Chip – Deaktivieren). Ändern Sie die Einstellung mit den Pfeiltasten auf **Embedded Security Device – Enable** (Embedded Security-Chip – Aktivieren). 5. Wählen Sie **Aktivieren > Änderungen speichern und beenden**. HP arbeitet derzeitig an Lösungsmöglichkeiten für zukünftige Software-Versionen.
Der Prozess **Restore Identity** (Identität wiederherstellen) verliert die Verknüpfung mit dem virtuellen Token.	Bei der Wiederherstellung der Benutzeridentität kann Credential Manager die Verknüpfung mit dem Speicherort des virtuellen Token im Anmeldebildschirm verlieren. Obgleich das virtuelle Token in Credential Manager registriert ist, muss der Benutzer das Token erneut registrieren, um die Verknüpfung wiederherzustellen.	Dies ist zurzeit das beabsichtigte Standardverhalten der Anwendung. Wenn Credential Manager deinstalliert wird, ohne dass Identitäten beibehalten werden, wird der systemseitige Teil (Server) des Token zerstört, sodass das Token für die Anmeldung nicht mehr verwendet werden kann, auch wenn der clientseitige Teil des Token während der Wiederherstellung der Identitäten wiederhergestellt wird. HP untersucht langfristige Optionen zur Behebung des Problems.

Embedded Security for HP ProtectTools

Kurzbeschreibung	Einzelheiten	Lösung
Das Verschlüsseln von Ordnern, Unterordnern und Dateien auf dem PSD verursacht eine Fehlermeldung.	Wenn der Benutzer Dateien und Ordner auf das PSD kopiert und versucht, Ordner und Dateien bzw. Ordner und Unterordner zu verschlüsseln, wird die Fehlermeldung **Error Applying Attributes** (Fehler beim Anwenden der Attribute) angezeigt. Der Benutzer kann jedoch die gleichen Dateien auf dem	Dies ist das beabsichtigte Standardverhalten der Anwendung. Beim Verschieben von Dateien und Ordnern auf das PSD werden diese automatisch verschlüsselt. Es besteht kein Grund, die Dateien und Ordner „doppelt“ zu verschlüsseln. Bei einer doppelten Verschlüsselung auf dem PSD mit EFS wird diese Fehlermeldung angezeigt.

Kurzbeschreibung	Einzelheiten	Lösung
	Laufwerk C:\ einer separat installierten Festplatte verschlüsseln.	
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 Sichheitsgründen vorgesehene Standardverhalten.
Ein nicht autorisierter Administrator kann den Inhalt von mit EFS verschlüsselten Ordnern anzeigen, löschen, umbenennen oder 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.
Mit EFS verschlüsselte Ordner werden unter Windows 2000 nicht in Grün angezeigt.	Mit EFS verschlüsselte Ordner werden unter Windows XP in Grün angezeigt, nicht aber unter Windows 2000.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Hierbei handelt es sich um eine Funktion von EFS. Verschlüsselte Ordner werden nicht unter Windows 2000, jedoch unter Windows XP hervorgehoben. Dies gilt sowohl für Installationen mit als auch ohne Embedded Security-TPM.
Bei EFS wird kein Kennwort benötigt, um verschlüsselte Dateien unter Windows 2000 anzuzeigen.	Wenn ein Benutzer Embedded Security einrichtet, sich als Administrator anmeldet, sich abmeldet und dann erneut als Administrator anmeldet, kann der Benutzer unter Windows 2000 Dateien und Ordner ohne Eingabe eines Kennworts anzeigen. Dies geschieht nur bei dem ersten Administratorkonto unter Windows 2000. Bei der Anmeldung mit einem zweiten Administratorkonto tritt dies nicht auf.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Hierbei handelt es sich um eine Funktion von EFS unter Windows 2000. Unter Windows XP kann ein Benutzer standardmäßig keine EFS-verschlüsselten Dateien und Ordner ohne Eingabe eines Kennworts öffnen.
Die Software sollte nicht auf einer Wiederherstellung mit FAT32-Partition installiert werden.	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. Microsoft EFS wird nur unter NTFS unterstützt, nicht unter FAT32. Hierbei handelt es sich eine Eigenschaft von Microsoft EFS, die in keinerlei Verbindung zur HP ProtectTools-Software steht.
Windows 2000-Benutzer können alle PSDs mit der versteckten Freigabe (durch das $-Zeichen gekennzeichnet) im Netzwerk freigeben.	Windows 2000-Benutzer können alle PSDs mit der versteckten Freigabe (durch das $-Zeichen gekennzeichnet) im Netzwerk freigeben. Auf diese versteckte Freigabe kann dann über das Netzwerk unter Verwendung der versteckten Freigabe ($) zugegriffen werden.	Das PSD wird normalerweise nicht im Netzwerk freigegeben. Ausschließlich unter Windows 2000 ist dies jedoch über die versteckte Freigabe ($) möglich. HP empfiehlt, das integrierte Administratorkonto immer mit einem Kennwortschutz zu belegen.
Die Benutzer können das Wiederherstellungsarchiv (XML-Datei) verschlüsseln oder löschen.	Standardmäßig sind die ACLs (Zugriffskontrolllisten) für diesen Ordner nicht eingerichtet, daher kann ein Benutzer die Datei unabsichtlich oder auch bewusst verschlüsseln oder löschen, sodass auf sie nicht mehr zugegriffen werden kann. Wurde die Datei verschlüsselt oder gelöscht, kann die TPM-Software nicht mehr verwendet werden.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Die Benutzer verfügen über Zugriffsrechte auf ein Wiederherstellungsarchiv, um eine Sicherungskopie ihres Basisbenutzerschlüssels zu speichern oder zu aktualisieren. Die Kunden sollten eine 'optimierte Vorgehensweise' für den Sicherheitsbereich einführen und die Benutzer anweisen, Wiederherstellungsarchivdateien niemals zu verschlüsseln oder zu löschen.

Kurzbeschreibung	Einzelheiten	Lösung
Die Interaktion von HP ProtectTools Embedded Security EFS mit Symantec Antivirus oder Norton AntiVirus führt zu verlängerten Verschlüsselungs-, Entschlüsselungs- und Scanzeiten.	Verschlüsselte Dateien verursachen einen Konflikt mit dem Virus-Scanner von Symantec Antivirus oder von Norton AntiVirus 2005. Während des Scan-Vorgangs wird der Benutzer jeweils nach etwa zehn Dateien zur Eingabe eines Basisbenutzerkennworts aufgefordert. Wenn der Benutzer kein Kennwort eingibt, wird die Eingabeaufforderung wegen Zeitüberschreitung beendet, sodass der Scanvorgang von Norton AntiVirus 2005 fortgesetzt werden kann. Das Verschlüsseln von Dateien mit HP ProtectTools Embedded Security EFS dauert länger, wenn Symantec Antivirus oder Norton AntiVirus ausgeführt wird.	Um die Scanzeit für EFS-Dateien in HP ProtectTools Embedded Security zu verkürzen, kann der Benutzer vor dem Scannen entweder das Verschlüsselungs-Kennwort eingeben oder die Dateien und Ordner entschlüsseln. Um beim Verschlüsseln und Entschlüsseln von Daten mit HP ProtectTools Embedded Security-EFS Zeit zu sparen, sollte der Benutzer die automatische Schutzfunktion von Symantec Antivirus oder Norton AntiVirus deaktivieren.
Das Wiederherstellungsarchiv kann nicht auf Wechsellaufwerken gespeichert werden.	Wenn der Benutzer beim Erstellen des Pfades für das Wiederherstellungsarchiv während der Initialisierung von Embedded Security eine MMC- oder SD-Karte einsetzt, wird eine Fehlermeldung angezeigt.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Das Speichern des Wiederherstellungsarchivs auf Wechsellaufwerken wird nicht unterstützt. Das Archiv kann auf einem Netzlaufwerk oder einem lokalen Laufwerk (jedoch nicht Laufwerk C) gespeichert werden.
Unter Windows 2000 mit dem Gebietsschema Französisch (Frankreich) können keine Daten verschlüsselt werden.	Beim Klicken mit der rechten Maustaste auf ein Dateisymbol steht die Option **Encrypt** (Verschlüsseln) nicht zur Verfügung.	Dies ist eine Einschränkung des Microsoft-Betriebssystems. Wenn das Gebietsschema auf eine andere Einstellung gesetzt wird (beispielsweise auf Französisch (Kanada)), steht die Option **Encrypt** (Verschlüsseln) zur Verfügung. Um das Problem zu umgehen, verschlüsseln Sie die Datei wie folgt: Klicken Sie mit der rechten Maustaste auf das Dateisymbol, und wählen Sie **Eigenschaften > Erweitert > Inhalt verschlüsseln**.
Wenn es während der Initialisierung von Embedded Security beim Übernehmen von Eigentümerrechten zu einem Stromausfall kommt, werden Fehlermeldungen zurückgegeben.	Wenn es während der Initialisierung des Embedded Security-Chips zu einem Stromausfall kommt, treten folgende Fehler auf: • Beim Versuch, den Assistenten für die Initialisierung von Embedded Security (Embedded Security Initialization Wizard) zu starten, wird der folgende Fehler angezeigt: **The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.** (Embedded Security kann nicht initialisiert werden, da der Embedded Security-Chip bereits über einen Embedded Security-Eigentümer verfügt.) • Beim Versuch, den Assistenten für die Benutzerinitialisierung (User Initialization Wizard) zu starten, wird der folgende Fehler angezeigt: **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.** (Embedded Security ist nicht initialisiert. Um den Assistenten zu verwenden,	Führen Sie nach einem Stromausfall folgende Aktionen durch: **HINWEIS:** Verwenden Sie die Pfeiltasten, um verschiedene Menüs und Menüelemente auszuwählen und Werte zu ändern (falls nicht anders angegeben). 1. Starten Sie den Computer, oder führen Sie einen Neustart durch. 2. Drücken Sie F10, wenn **F10=Setup** auf dem Bildschirm angezeigt wird (oder sobald die Monitor-LED grün leuchtet). 3. Wählen Sie die entsprechende Sprachoption aus. 4. Drücken Sie die Eingabetaste. 5. Wählen Sie **Sicherheit > Embedded Security**. 6. Setzen Sie die Option **Embedded Security Device** (Embedded Security-Chip) auf **Aktivieren**. 7. Drücken Sie F10, um die Änderung zu übernehmen. 8. Wählen Sie **Datei > Änderungen speichern und beenden**.

Kurzbeschreibung	Einzelheiten	Lösung
	muss Embedded Security zuerst initialisiert werden.)	9. Drücken Sie die Eingabetaste. 10. Drücken Sie F10, um die Änderungen zu speichern und Computer Setup zu beenden.
Das Kennwort für das Dienstprogramm Computer Setup (F10) kann nach der Aktivierung des TPM entfernt werden.	Zum Aktivieren des TPM ist ein Kennwort für das Dienstprogramm Computer Setup (F10) erforderlich. Sobald das Modul aktiviert ist, kann der Benutzer das Kennwort entfernen. Dadurch können alle Benutzer mit direktem Zugriff auf das System das TPM zurücksetzen, was unter Umständen zu einem Datenverlust führt.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Das Kennwort für das Dienstprogramm Computer Setup (F10) kann nur von einem Benutzer entfernt werden, der das Kennwort kennt. HP empfiehlt jedoch, das Dienstprogramm Computer Setup (F10) immer mit einem Kennwort zu schützen.
Das Dialogfeld für das PSD-Kennwort wird nicht mehr angezeigt, wenn das System aus dem Standby-Modus aktiviert wird.	Wenn sich ein Benutzer nach dem Erstellen eines PSD am System anmeldet, wird er vom TPM zur Eingabe des Basisbenutzerkennworts aufgefordert. Wenn der Benutzer das Kennwort nicht eingibt und das System in den Standby-Modus wechselt, ist das Dialogfeld zur Eingabe des Kennworts nicht mehr verfügbar, wenn das System wieder aktiviert wird.	Dies entspricht dem Standardverhalten der Anwendung. Der Benutzer muss sich abmelden und dann erneut anmelden, um das Dialogfeld für das PSD-Kennwort wieder anzuzeigen.
Zum Ändern der Sicherheitsplattform-richtlinien ist kein Kennwort erforderlich.	Für den Zugriff auf Sicherheitsplattformrichtlinien (Computer und Benutzer) ist für Benutzer, die über administrative Rechte für das System verfügen, kein TPM-Kennwort erforderlich.	Dies entspricht dem Standardverhalten der Anwendung. Alle Administratoren können mit oder ohne Benutzerinitialisierung des TPM die Sicherheitsplattformrichtlinien ändern.
Der Funktionsumfang von Microsoft EFS ist unter Windows 2000 eingeschränkt.	Ein Administrator kann ohne das richtige Kennwort auf verschlüsselte Informationen auf dem System zugreifen. Wenn der Administrator ein falsches Kennwort eingibt oder das Dialogfeld zur Eingabe des Kennworts ohne Eingabe schließt, wird die verschlüsselte Datei so geöffnet, als ob der Administrator das richtige Kennwort eingegeben hätte. Dies geschieht unabhängig der beim Verschlüsseln der Daten verwendeten Sicherheitseinstellungen. Unter Windows 2000 geschieht dies nur beim ersten Administratorkonto.	Die Datenwiederherstellungsrichtlinie wird automatisch für das Zuweisen eines Administrators als Wiederherstellungs-Agent konfiguriert. Wenn kein Benutzerschlüssel abgerufen werden kann (bei Eingabe eines falschen Kennworts oder beim Schließen des Dialogfelds **Enter Password** (Kennwort eingeben) ohne Eingabe), wird die Datei automatisch mit einem Wiederherstellungsschlüssel entschlüsselt. Dies ist auf Microsoft EFS zurückzuführen. Weitere Informationen finden Sie in Artikel Q257705 der Microsoft Knowledge Base unter http://www.microsoft.com. Die Dokumente können nicht von einem Benutzer ohne administrative Rechte geöffnet werden.
Beim Anzeigen eines Zertifikats wird dieses als nicht vertrauenswürdig eingestuft.	Nach dem Einrichten von HP ProtectTools und dem Ausführen des Assistenten für die Benutzerinitialisierung (User Initialization Wizard) kann der Benutzer das ausgestellte Zertifikat zwar anzeigen, es wird jedoch als nicht vertrauenswürdig eingestuft. Das Zertifikat kann an diesem Punkt installiert werden, indem der Benutzer auf die Schaltfläche zum Installieren klickt, jedoch wird das Zertifikat durch die Installation nicht vertrauenswürdig.	Selbst signierte Zertifikate sind nicht vertrauenswürdig. In einer ordnungsgemäß konfigurierten Unternehmensumgebung werden EFS-Zertifikate von Online-Zertifizierungsstellen ausgestellt und werden dann als vertrauenswürdig eingestuft.

Kurzbeschreibung	Einzelheiten	Lösung
Der folgende Fehler tritt zeitweilig bei Verschlüsselungs- und Entschlüsselungsvorgängen auf: **The process cannot access the file because it is being used by another process.** (Der Prozess kann nicht auf die Datei zugreifen, da sie von einem anderen Prozess verwendet wird.)	Extrem selten auftretender Fehler während der Verschlüsselung oder Entschlüsselung von Dateien. Er gibt an, dass die Datei von einem anderen Prozess verwendet wird, obgleich die entsprechende Datei oder der Ordner nicht vom Betriebssystem oder anderen Anwendungen verarbeitet wird.	So beseitigen Sie den Fehler: 1. Starten Sie das System neu. 2. Melden Sie sich ab. 3. Melden Sie sich wieder an.
Wenn ein Laufwerk entfernt wird, bevor neue Daten erzeugt oder übertragen werden konnten, kann dies zu einem Datenverlust auf den Wechsellaufwerken führen.	Beim Entfernen von Speichermedien wie einer MultiBay Festplatte bleibt das PSD weiterhin verfügbar, sodass beim Hinzufügen bzw. Ändern von Daten auf dem PSD keine Fehler auftreten. Nach dem Neustart des Systems werden Dateiänderungen, die vorgenommen wurden, während die Wechsellaufwerke nicht verfügbar waren, nicht angezeigt.	Dieses Problem tritt nur dann auf, wenn der Benutzer auf das PSD zugreift und die Festplatte entfernt, bevor neue Daten generiert oder übertragen wurden. Wenn der Benutzer versucht, auf das PSD zuzugreifen, wenn das Wechsellaufwerk nicht vorhanden ist, wird eine Fehlermeldung mit dem Hinweis **The device is not ready** (Das Gerät ist nicht bereit) ausgegeben.
Wenn der Benutzer während der Deinstallation das Administrations-Tool öffnet und den Basisbenutzerschlüssel nicht initialisiert hat, ist die Option **Disable** (Deaktivieren) nicht verfügbar. Das Deinstallationsprogramm wird erst dann fortgesetzt, wenn das Administrations-Tool geschlossen wird.	Der Benutzer kann entweder die Deinstallation ohne Deaktivieren des TPM-Chips durchführen oder zunächst den TPM-Chip deaktivieren (über das Adminstrations-Tool) und dann die Deinstallation durchführen. Um auf das Administrations-Tool zugreifen zu können, muss der Basisbenutzerschlüssel initialisiert werden. Wurde der Schlüssel nicht initialisiert, kann der Benutzer auf keine Option zugreifen. Wenn der Benutzer explizit das Öffnen des Administrations-Tools festgelegt hat, indem er im Dialogfeld mit der Aufforderung **Click Yes to open Embedded Security Administration tool** (Klicken Sie auf „Ja”, um das Embedded Security-Administrations-Tool zu öffnen) auf **Yes** (Ja) geklickt hat, wird der Deinstallationsprozess erst fortgesetzt, wenn das Administrations-Tool geschlossen wurde. Wenn der Benutzer in diesem Dialogfeld auf **No** (Nein) geklickt hat, wird das Administrations-Tool nicht geöffnet, und die Deinstallation wird fortgesetzt.	Das Administrations-Tool wird zum Deaktivieren des TPM-Chips verwendet. Diese Option steht jedoch nur dann zur Verfügung, wenn der Basisbenutzerschlüssel bereits initialisiert wurde. Wurde er nicht initialisiert, wählen Sie entweder **OK** oder **Cancel** (Abbrechen), um den Deinstallationsprozess fortzusetzen.
Das System wird nach dem Erstellen eines PSD für zwei Benutzerkonten und dem Verwenden von schnellem Benutzerwechsel in 128-MB-Systemkonfigurationen zeitweilig gesperrt.	Das Verwenden eines schnellen Benutzerwechsels bei minimalem RAM führt gelegentlich zu einer Systemsperre: Es wird kein Anmeldebildschirm angezeigt, der Bildschirm bleibt schwarz und die Tastatur funktioniert nicht mehr.	Die Ursache ist vermutlich ein Zeitsteuerungsproblem in Konfigurationen mit wenig Arbeitsspeicher. Der integrierte Grafikcontroller verwendet eine UMA-Architektur mit 8 MB RAM. Dadurch stehen den Benutzern nur noch 120 MB zur Verfügung. Diese 120 MB werden von den beiden gleichzeitig angemeldeten Benutzern gemeinsam genutzt. Bei einem schnellen Benutzerwechsel treten dann möglicherweise Fehler auf. Als Behelfslösung sollte das System neu gestartet werden, und die Benutzer sollten den Speicher vergrößern (HP liefert standardmäßig keine 128-MB-Konfigurationen mit Sicherheitsmodulen).

Kurzbeschreibung	Einzelheiten	Lösung
Zeitüberschreitung bei der EFS-Benutzerauthentifizierung (Kennwortanforderung): **Access denied** (Zugriff verweigert).	Die Kennwortaufforderung für die EFS-Benutzerauthentifizierung wird erneut geöffnet, wenn Sie auf **OK** klicken oder nach einer Zeitüberschreitung den Computer aus dem Standby-Modus wieder aktivieren.	Dies entspricht dem Standardverhalten der Anwendung. Um Probleme mit Microsoft EFS zu verhindern, wurde zum Generieren dieser Fehlermeldung ein 30-Sekunden-Watchdog-Timer erstellt.
In den Funktionsbeschreibungen für den Installationsprozess sind im Japanischen die Wörter teilweise abgeschnitten.	Im Installationsassistenten sind bei der benutzerdefinierten Installation Funktionsbeschreibungen teilweise abgeschnitten.	HP wird dieses Problem in zukünftigen Versionen beheben.
Die EFS-Verschlüsselung funktioniert ohne das Angeben eines Kennworts an der Eingabeaufforderung.	Bei einer Zeitüberschreitung zur Eingabe eines Benutzerkennworts können Verschlüsselungen immer noch für Dateien oder Ordner durchgeführt werden.	Zum Verschlüsseln von Dateien oder Ordnern ist keine Kennwortauthentifizierung erforderlich, da es sich hierbei um eine Funktion der Microsoft EFS-Verschlüsselung handelt. Zum Entschlüsseln wird jedoch das Benutzerkennwort benötigt.
Sichere E-Mail-Funktionen werden auch dann unterstützt, wenn die entsprechende Option im Assistenten für die Benutzerinitialisierung (User Initialization Wizard) oder die Konfiguration für sichere E-Mails in den Benutzerrichtlinien deaktiviert ist.	Die Embedded Security-Software und der Assistent steuern nicht die Einstellungen von E-Mail-Clients (Outlook, Outlook Express oder Netscape).	Dies ist das beabsichtigte Standardverhalten der Anwendung. Die Konfiguration der TPM-E-Mail-Einstellungen verhindert nicht die direkte Bearbeitung von Verschlüsselungseinstellungen im E-Mail-Client. Die Verwendung sicherer E-Mail-Funktionen wird mithilfe von Drittanbieteranwendungen gesteuert. Der HP Assistant ermöglicht zur sofortigen Anpassung der Funktionen die Verknüpfung mit den drei Referenzanwendungen.
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 eine Wiederherstellung verwendet werden.	Beim Ausführen einer umfangreichen Installation auf einem bereits initialisierten HP ProtectTools Embedded Security-System werden vorhandene Wiederherstellungs-archive und -Tokens für eine Wiederherstellung unbrauchbar, da die entsprechenden XML-Dateien überschrieben werden.	HP arbeitet an einer Lösung für dieses Überschreibungsproblem und wird in einem zukünftigen SoftPaq eine Lösung bereitstellen.
Die automatisierten Anmeldeskripte funktionieren bei Wiederherstellungsvorgängen durch den Benutzer in Embedded Security nicht.	Der Fehler tritt auf, nachdem 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 dem Wiederherstellen von Embedded Security begonnen hat. Während des Wiederherstellungsvorgangs wird der Benutzer von Credential Manager gefragt, ob das System die Anmeldung bei der Infineon	Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um den Speicherort auszuwählen. Der Wiederherstellungsvorgang wird dann fortgesetzt.

Kurzbeschreibung	Einzelheiten	Lösung
	TPM-Benutzerauthentifizierung automatisieren kann. Wenn der Benutzer **Yes** (Ja) auswählt, wird der Speicherort der Datei **SPEmRecToken.xml** automatisch im Textfeld 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.).	
PSDs für mehrere Benutzer funktionieren nicht in einer Umgebung mit schnellem Benutzerwechsel.	Dieser Fehler tritt auf, wenn mehreren erstellten Benutzern ein PSD mit demselben Laufwerksbuchstaben zugewiesen wurde. Bei dem Versuch, beim Laden des PSD einen schnellen Benutzerwechsel durchzuführen, ist das PSD des zweiten Benutzers nicht verfügbar.	Das PSD des zweiten Benutzers steht erst dann zur Verfügung, wenn ihm ein anderer Laufwerksbuchstabe zugewiesen wird oder wenn der erste Benutzer sich abmeldet.
Das PSD wird deaktiviert und kann nach dem Formatieren der Festplatte, auf der das PSD generiert wurde, nicht gelöscht werden.	Das PSD wird deaktiviert und kann nach dem Formatieren der sekundären Festplatte, auf der das PSD generiert wurde, nicht gelöscht werden. Das PSD-Symbol ist immer noch sichtbar, aber beim Versuch, auf das PSD zuzugreifen, wird die Fehlermeldung **Drive is not accessible** (Auf das Laufwerk kann nicht zugegriffen werden) angezeigt. Der Benutzer kann das PSD nicht löschen. Es wird folgende Meldung angezeigt: **Your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process**. (Das PSD wird noch verwendet. Stellen Sie sicher, dass auf Ihrem PSD keine Dateien geöffnet sind und es von keinem anderen Prozess verwendet wird.). Um das PSD zu löschen, muss der Benutzer das System neu starten. Nach dem Neustart wird das PSD nicht mehr geladen.	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.
Bei der Wiederherstellung aus dem automatischen Sicherungsarchiv ist ein interner Fehler aufgetreten.	Wenn der Benutzer • in HPPTSM auf die Embedded Security-Option **Restore under Backup** (Wiederherstellung von Sicherungskopie) zum Wiederherstellen aus einem automatischen Sicherungsarchiv klickt, • die Datei **SPSystemBackup.xml** auswählt, schlägt der Wiederherstellungs-Assistent (Restore Wizard) fehl, und die folgende Fehlermeldung wird angezeigt: **The selected Backup Archive does not match the restore reason. Please**	Wenn der Benutzer statt der erforderlichen Datei **SpBackupArchive.xml** die Datei **SpSystemBackup.xml** auswählt, gibt der Embedded Security-Assistent folgende Fehlermeldung zurück: **An internal Embedded Security error has been detected. (Ein interner Embedded Security-Fehler ist aufgetreten.)** Der Benutzer muss die richtige XML-Datei für den angegebenen Grund 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.

Kurzbeschreibung	Einzelheiten	Lösung
	select another archive and continue. (Das ausgewählte Sicherungsarchiv entspricht nicht dem Wiederherstellungsgrund. Wählen Sie ein anderes Archiv aus, um fortzufahren.)	
Wiederherstellungsfehler des Sicherheitssystems bei mehreren Benutzern.	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 der TPM-Chip zurückgesetzt wird, der Wiederherstellungsprozess ausgeführt wird und alle Benutzer ausgewählt werden, bevor die nächste tägliche Standardsicherungskopie angelegt wird. Beim Erstellen der automatischen Sicherungskopie werden die nicht wiederhergestellten Benutzer überschrieben, und ihre Daten gehen verloren. Wenn eine neue Sicherungskopie des Systems gespeichert wird, können die vorher nicht ausgewählten Benutzer nicht wiederhergestellt werden. Außerdem muss der Benutzer die gesamte Sicherungskopie des Systems wiederherstellen. Archivierte Sicherungskopien können einzeln wiederhergestellt werden.
Beim Zurücksetzen des System-ROM auf die Standardwerte wird der TPM-Chip verborgen.	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 Computer Setup (F10), gehen Sie zu **Sicherheit > Gerätesicherheit**, und ändern Sie die Einstellungen von **Hidden** (Gerät verborgen) auf **Available** (Gerät verfügbar).
Das automatische Erstellen einer Sicherungskopie ist für das zugeordnete Laufwerk nicht möglich.	Wenn ein Administrator das Erstellen einer automatischen Sicherungskopie in Embedded Security einrichtet, wird unter **Windows > Tasks > Scheduled Task** (Geplante Tasks) ein Eintrag erstellt. Dieser geplante Task ist so eingestellt, dass NT AUTHORITY\SYSTEM für Rechte zum Ausführen der Sicherung verwendet wird. Dieses Verfahren funktioniert ordnungsgemäß auf allen lokalen Laufwerken. 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 bei der Anmeldung ausgeführt werden soll, zeigt das Embedded Security-TNA-Symbol 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.** (Auf den Speicherort für das Sicherungsarchiv kann zurzeit nicht zugegriffen werden. Klicken Sie hier, falls Sie Sicherungskopien in einem temporären Archiv speichern möchten,	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
	bis das Sicherungsarchiv wieder verfügbar ist.) Ist die automatische Sicherung für einen bestimmten Zeitpunkt geplant, schlägt die Sicherung jedoch fehl, ohne dass eine entsprechende Fehlermeldung ausgegeben wird.	
Der Embedded Security-Status kann auf der grafischen Benutzeroberfläche von Embedded Security vorübergehend nicht deaktiviert werden.	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.

Verschiedenes

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
HP ProtectTools Security Manager – Es wird folgender Warnhinweis angezeigt: **The security application can not be installed until the HP Protect Tools Security Manager is installed**. (Die Sicherheitsanwendung kann erst dann installiert werden, wenn HP ProtectTools Security Manager installiert ist.)	Alle Sicherheitsanwendungen, wie Embedded Security, Java Card und biometrische Lesegeräte, sind erweiterbare Plug-Ins für die HP Security Manager-Schnittstelle. Security Manager muss installiert sein, bevor ein von HP getestetes und empfohlenes Sicherheits-Plug-In geladen werden kann.	Vor dem Installieren von Sicherheits-Plug-Ins muss die HP ProtectTools Security Manager-Software installiert werden.
HP ProtectTools TPM Firmware Update Utility für dc7600 und Modelle mit Broadcom-fähigen TPM-Chips – Das über die Support-Website von HP bereitgestellte Tool gibt die Meldung **ownership required** (Eigentumsrechte erforderlich) zurück.	Dies entspricht dem erwarteten Verhalten der TPM-Firmware für dc7600 und 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	1. Installieren Sie die HP ProtectTools Embedded Security-Software neu. 2. Führen Sie den Plattform and User Configuration Wizard (Assistenten für Plattform- und Benutzerkonfiguration) aus. 3. Stellen Sie sicher, dass Microsoft .NET Framework 1.1 auf dem System installiert ist: a. Klicken Sie auf **Start**. b. Klicken Sie auf **Systemsteuerung**. c. Klicken Sie auf **Software**. d. Stellen Sie sicher, dass **Microsoft .NET Framework 1.1** in der Liste enthalten ist. 4. Überprüfen Sie die Hardware- und Softwarekonfiguration: a. Klicken Sie auf **Start**. b. Klicken Sie auf **Alle Programme**. c. Klicken Sie auf **HP ProtectTools Security Manager**.

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
	die Firmware kann erst dann aktualisiert werden, wenn die Embedded Security-Softwareplattform und der Assistent für die Benutzerinitialisierung (User Initialization Wizard) konfiguriert wurden. *Nach einer Firmware-Aktualisierung sollte der Computer stets neu gestartet werden. Die Firmware-Version wird erst nach einem Neustart korrekt erkannt.	**d.** Wählen Sie **Embedded Security** aus. **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 Firmware-Version nicht 2.18 ist, laden Sie die entsprechende Version herunter, und aktualisieren Sie die TPM-Firmware. Das TPM-Firmware-SoftPaq ist als Support-Download 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. Alle Dienste müssen in Security Manager erfolgreich geladen (ein entsprechender Hinweis wird oben im Security Manager-Fenster angezeigt) und alle Plug-Ins in der linken Spalte angezeigt werden. Um Probleme zu vermeiden, räumen Sie entsprechend viel Zeit für das Laden dieser Plug-Ins ein.
HP ProtectTools * Allgemein – Unbeschränkte Zugriffs- oder Administratorrechte stellen ein Sicherheitsrisiko dar.	Folgende Risiken bestehen beim uneingeschränktem Zugriff auf den Client-PC: • Löschen von PSDs • Mutwilliges Ändern 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.

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
Die Embedded Security-Kennwörter für das BIOS und das Betriebssystem sind nicht synchronisiert.	Wenn der Benutzer ein neues Kennwort nicht als Embedded Security-Kennwort für das BIOS bestätigt, wird das ursprüngliche Embedded Security-Kennwort über Computer Setup (F10) für das BIOS wiederhergestellt.	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 PIN für das TPM-BIOS wird dem ersten Benutzer zugeordnet, der die Benutzereinstellung initialisiert. Bei einem Computer mit mehreren Benutzern ist der Administrator normalerweise der erste Benutzer. Dieser muss seine TPM-Benutzer-PIN an andere Benutzer weitergeben, damit diese sich 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 die PIN ändern, damit das TPM-Preboot nach dem Zurücksetzen auf die TPM-Werkseinstellungen funktioniert.	Der Benutzer muss die PIN ändern oder einen anderen Benutzer erstellen, um seine Benutzereinstellung zu initialisieren, damit die TPM-BIOS-Authentifizierung nach dem Zurücksetzen auf die Werkseinstellungen funktioniert. Es gibt keine Option zur Aktivierung der TPM-BIOS-Authentifizierung.	Dies entspricht dem Standardverhalten. Durch das Wiederherstellen der Werkseinstellungen wird der Basisbenutzerschlüssel gelöscht. Der Benutzer muss seine Benutzer-PIN ändern oder einen neuen Benutzer erstellen, um den Basisbenutzerschlüssel erneut zu initialisieren.
Die **Power-on authentication support** (Systemstartauthentifizierung) wird mit der Embedded Security-Funktion **Reset to Factory Settings** (Auf Werkseinstellungen zurücksetzen) nicht auf die Standardeinstellung zurückgesetzt.	In Computer Setup wird die Option **Power-on authentication support** (Systemstartauthentifizierung) 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.	Mit der Option **Reset to Factory Settings** (Auf Werkseinstellungen zurücksetzen) wird der Embedded Security-Chip deaktiviert. Dadurch werden die anderen Embedded Security-Optionen (einschließlich **Power-on authentication support** (Systemstart-Authentifizierung) ausgeblendet. Nach dem erneuten Aktivieren des Embedded Security-Chips bleibt die Option **Power-on authentication support** (Systemstart-Authentifizierung) jedoch aktiviert. HP arbeitet an einer Lösung, die in zukünftigen webbasierten ROM-SoftPaqs bereitgestellt wird.
Während der Startsequenz wird das BIOS-Kennwort von der Systemstart-Authentifizierung außer Kraft gesetzt.	Bei der Systemstart-Authentifizierung wird der Benutzer aufgefordert, sich mit dem TPM-Kennwort am System anzumelden. Wenn der Benutzer jedoch die Taste F10 drückt, um auf das BIOS zuzugreifen, wird nur Lesezugriff gewährt.	Damit der Benutzer in das BIOS schreiben kann, muss er im Fenster der Systemstart-Authentifizierung anstelle des TPM-Kennworts das BIOS-Kennwort eingeben.
Nach der Änderung des Eigentümerkennworts in der Embedded Security-Software für Windows wird der Benutzer vom BIOS zur Eingabe des alten und des neuen Kennworts in Computer Setup aufgefordert.	Nach der Änderung des Eigentümerkennworts in der Embedded Security-Software für Windows wird der Benutzer vom BIOS zur Eingabe des alten und des neuen Kennworts in Computer Setup aufgefordert.	Dies ist das beabsichtigte Standardverhalten der Anwendung. Der Grund hierfür ist, dass das BIOS nicht in der Lage ist, mit dem TPM zu kommunizieren, sobald das Betriebssystem aktiv ist, und das TPM-Kennwort anhand TPM-Schlüssel-BLOB zu bestätigen.

Glossar

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, wie 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.

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

BIOS-Profil 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.

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.

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

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.

DriveLock Sicherheitsmerkmal, das die Festplatte mit einem Benutzer verbindet und vom Benutzer verlangt, das DriveLock-Kennwort beim Starten des Computers korrekt einzugeben.

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.

FAT-Partition File Allocation Table (Dateizuordnungstabelle), eine Methode zum Indizieren von Speichermedien.

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 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.

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

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

Migration Eine Aufgabe, die das Verwalten, Wiederherstellen und Übertragen von Schlüsseln und Zertifikaten ermöglicht.

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

Neustart Neustarten des Computers.

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

NTFS-Partition NT File System (NT-Dateisystem), eine Methode zum Indizieren von Speichermedien. Diese Methode wird standardmäßig unter Windows Vista und Windows XP verwendet.

PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk) 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.

Single Sign On (Einmalanmeldung) Funktion, die die Authentifizierungsinformationen speichert und es Ihnen ermöglicht, den Credential Manager für den Zugang zum Internet und zu Windows-Anwendungen zu verwenden, die eine Kennwortauthentifizierung erfordern.

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.

Strenge Sicherheit Sicherheitsfunktion in BIOS Configuration, mit der der Schutz für das Kennwort beim Systemstart und das Administratorkennwort sowie für die weiteren Möglichkeiten zur Authentifizierung beim Einschalten erhöht wird.

Trusted Platform Module (TPM) integrierter Sicherheits-Chip (bestimmte Modelle) Integrierter Sicherheits-Chip, der streng vertrauliche Benutzerdaten vor böswilligen Angriffen schützen kann. Er bildet die Sicherheitsbasis in einer Plattform. Das TPM liefert kryptografische Algorithmen und Vorgänge, die die Vorgaben der Trusted Computing Group (TCG) erfüllen.

USB-Token Sicherheitsgerät, das Identifizierungsinformationen zu einem Benutzer 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.

Virtuelles Token Sicherheitsfunktion, deren Funktionsweise weitgehend der einer Java Card oder eines Lesegerätes entspricht. Das Token wird entweder auf der Festplatte des Computers oder in der Registrierungsdatei von Windows gespeichert. Wenn Sie sich mit einem virtuellen Token anmelden, werden Sie aufgefordert, eine Benutzer-PIN einzugeben, um die Authentifizierung durchzuführen.

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