

# HP ProtectTools Security Manager- Handbuch

---

HP Compaq Business Desktops



© Copyright 2006 Hewlett-Packard  
Development Company, L.P. Inhaltliche  
Änderungen dieses Dokuments behalten wir  
uns ohne Ankündigung vor.

Microsoft und Windows sind Marken der  
Microsoft Corporation in den USA und/oder  
anderen Ländern.

Intel und SpeedStep sind Marken der Intel  
Corporation in den USA und anderen  
Ländern.

Die Garantien für HP Produkte werden  
ausschließlich in der entsprechenden, zum  
Produkt gehörigen Garantieerklärung  
beschrieben. Aus dem vorliegenden  
Dokument sind keine weiter reichenden  
Garantieansprüche abzuleiten. Hewlett-  
Packard („HP“) haftet nicht für technische  
oder redaktionelle Fehler oder  
Auslassungen in diesem Dokument. Ferner  
übernimmt sie keine Haftung für Schäden,  
die direkt oder indirekt auf die Bereitstellung,  
Leistung und Nutzung dieses Materials  
zurückzuführen sind. Die Haftung für  
Schäden aus der Verletzung des Lebens,  
des Körpers oder der Gesundheit, die auf  
einer fahrlässigen Pflichtverletzung durch  
HP oder einer vorsätzlichen oder  
fahrlässigen Pflichtverletzung eines  
gesetzlichen Vertreters oder  
Erfüllungsgehilfen von HP beruhen, bleibt  
hierdurch unberührt. Ebenso bleibt hierdurch  
die Haftung für sonstige Schäden, die auf  
einer grob fahrlässigen Pflichtverletzung  
durch HP oder auf einer vorsätzlichen oder  
grob fahrlässigen Pflichtverletzung eines  
gesetzlichen Vertreters oder  
Erfüllungsgehilfen von HP beruht, unberührt.

Dieses Dokument enthält urheberrechtlich  
geschützte Informationen. Ohne schriftliche  
Genehmigung der Hewlett-Packard  
Company darf dieses Dokument weder  
kopiert noch in anderer Form vervielfältigt  
oder übersetzt werden.

HP ProtectTools Security Manager-  
Handbuch

HP Compaq Business Desktops

Erste Ausgabe (August 2006)

Dokumenten-Teilenummer: 431330-041

## Allgemeines

Dieses Handbuch enthält Anleitungen zur Konfiguration und Verwendung von HP ProtectTools Security Manager.



---

**ACHTUNG!** In dieser Form gekennzeichnete Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anleitungen hin.

---



---

**VORSICHT** In dieser Form gekennzeichnete Text weist auf die Gefahr von Hardware-Schäden oder Datenverlust bei Nichtbefolgen der Anleitungen hin.

---



---

**Hinweis** In dieser Form gekennzeichnete Text weist auf wichtige Zusatzinformationen hin.

---



# Inhaltsverzeichnis

## 1 Einführung

HP ProtectTools Security Manager .....	1
Zugreifen auf HP ProtectTools Security Manager .....	1
Erläuterungen zu Sicherheitsrollen .....	2
Verwalten von ProtectTools-Kennwörtern .....	2
Multifaktorauthentifizierung bei der Credential Manager-Anmeldung .....	5
Erstellen eines sicheren Kennworts .....	6
Erweiterte Aufgaben .....	7
Verwalten von ProtectTools-Einstellungen .....	7
Aktivieren bzw. Deaktivieren der Java Card-Systemstart-Authentifizierungsfunktion .....	7
Aktivieren bzw. Deaktivieren der Systemstart-Authentifizierungsfunktion für Embedded Security .....	7
Verwalten der Computer Setup-Kennwörter .....	8
Festlegen des Kennworts für den Systemstart (falls verfügbar) .....	8
Ändern des Kennworts für den Systemstart (falls verfügbar) .....	9
System-Setup .....	9
Ändern der Systemstart-Authentifizierungsfunktion .....	9
Ändern von Benutzerkonten .....	10
Festlegen des Administratorkennworts für Computer Setup .....	10
Ändern des Administratorkennworts für Computer Setup .....	11
Verhalten der Systemstart-Authentifizierung bei einem Wörterbuchangriff .....	12
Verteidigung gegen Wörterbuchangriffe .....	12

## 2 HP BIOS Configuration for ProtectTools

Grundkonzepte .....	13
Ändern der BIOS-Einstellungen .....	13

## 3 HP Embedded Security for ProtectTools

Grundkonzepte .....	15
Setup-Verfahren .....	16

## 4 HP Credential Manager for ProtectTools

Grundkonzepte .....	17
Startverfahren .....	17
Erstmalige Anmeldung .....	18

## 5 HP Java Card Security for ProtectTools

Grundkonzepte .....	19
<b>6 Lösungen von Drittanbietern</b>	
<b>7 HP Client Manager for Remote Deployment</b>	
Hintergrund .....	23
Initialisierung .....	23
Wartung .....	23
<b>8 Fehlerbeseitigung</b>	
Credential Manager for ProtectTools .....	25
Embedded Security for ProtectTools .....	30
Verschiedenes .....	39
<b>Glossar .....</b>	<b>43</b>
<b>Index .....</b>	<b>47</b>

# 1 Einführung

## HP ProtectTools Security Manager

Die ProtectTools Security Manager Software stellt Sicherheitsfunktionen zur Verfügung, die Schutz vor dem unberechtigten Zugriff auf Computer, Netzwerke und kritische Daten bieten. Dabei ist durch die folgenden Module eine optimale Sicherheit gewährleistet:

- HP BIOS Configuration for ProtectTools
- HP Embedded Security for ProtectTools
- HP Credential Manager for ProtectTools
- HP Java Card Security for ProtectTools

Welche Module für Ihren Computer zur Verfügung stehen, ist vom jeweiligen Modell abhängig. Die ProtectTools-Module können vorinstalliert oder auf der mit dem Computer gelieferten CD enthalten sein. Sie können sie aber auch auf der HP Website bestellen. Weitere Informationen hierzu finden Sie unter <http://www.hp.com>.



---

**Hinweis** Spezielle Anleitungen für die ProtectTools-Module finden Sie in der ProtectTools-Hilfe.

---

Um den TPM-Sicherheitschip (Trusted Platform Module) verwenden zu können, wird für Plattformen mit TPM sowohl ein TCG Software Stack (TSS) als auch Embedded Security-Software benötigt. Bei bestimmten Modellen ist TSS vorhanden. Andernfalls können Sie es bei HP kaufen. Darüber hinaus muss für manche Modelle separat Software erworben werden, die TPM aktiviert. Weitere Informationen finden Sie unter [Lösungen von Drittanbietern](#).

## Zugreifen auf HP ProtectTools Security Manager

So greifen Sie über die Systemsteuerung von Microsoft Windows auf ProtectTools Security Manager zu:

- ▲ Windows XP: Klicken Sie auf **Start > Systemsteuerung > Sicherheitscenter > ProtectTools Security Manager**.
- ▲ Windows 2000: Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.



---

**Hinweis** Nach der Konfiguration des Moduls Credential Manager können Sie sich im Windows-Anmeldefenster auch direkt bei Credential Manager anmelden. Weitere Informationen finden Sie unter [HP Credential Manager for ProtectTools](#).

---

## Erläuterungen zu Sicherheitsrollen

Bei der Verwaltung der Computersicherheit (insbesondere bei großen Organisationen) müssen Kompetenzen und Rechte auf verschiedene Administrator- und Benutzertypen verteilt werden.



**Hinweis** In einer kleinen Organisation oder bei einem einzelnen Benutzer hat möglicherweise nur eine Person diese Rollen inne.

Bei ProtectTools können die Sicherheitspflichten und -rechte auf die folgenden Rollen verteilt werden:

- Sicherheitsbeauftragter – Definiert die Schutzstufe für das Unternehmen oder das Netzwerk und legt die bereitzustellenden Sicherheitsfunktionen wie Java Cards, biometrische Lesegeräte oder USB-Tokens fest.



**Hinweis** Viele Funktionen von ProtectTools können vom Sicherheitsbeauftragten in Zusammenarbeit mit HP angepasst werden. Weitere Informationen finden Sie unter <http://www.hp.com>.

- IT-Administrator – Wendet die vom Sicherheitsbeauftragten definierten Sicherheitsfunktionen an und verwaltet diese. Kann bestimmte Funktionen auch aktivieren und deaktivieren. Wenn der Sicherheitsbeauftragte z. B. entschieden hat, Java Cards bereitzustellen, kann der IT-Administrator den Java Card-BIOS-Sicherheitsmodus aktivieren.
- Benutzer – Verwendet die Sicherheitsfunktionen. Wenn der Sicherheitsbeauftragte und der IT-Administrator z. B. Java Cards für das System aktiviert haben, kann der Benutzer die Java Card-PIN festlegen und die Karte zur Authentifizierung verwenden.


Administratoren wird empfohlen, Endbenutzerrechte und den Benutzerzugriff mithilfe sogenannter „Best Practices“ einzuschränken.

## Verwalten von ProtectTools-Kennwörtern

Die meisten Funktionen von ProtectTools Security Manager sind durch Kennwörter geschützt. In der folgenden Tabelle werden die üblicherweise verwendeten Kennwörter, das Softwaremodul, in dem das Kennwort festgelegt wird, und die Kennwortfunktion aufgeführt.

In dieser Tabelle werden auch die Kennwörter angegeben, die nur von IT-Administratoren festgelegt und verwendet werden. Alle übrigen Kennwörter können von normalen Benutzern oder Administratoren festgelegt werden.

**Tabelle 1-1** Kennwortverwaltung





ProtectTools-Kennwort	ProtectTools Module	Funktion
Administrator-Kennwort für Computer Setup	BIOS Configuration, durch IT-Administrator	Schützt den Zugriff auf das BIOS Computer Setup-Dienstprogramm und die Sicherheitseinstellungen.
 <b>Hinweis</b> Wird auch als BIOS-Administrator-, F10 Setup- oder Sicherheits-Setup-Kennwort bezeichnet.		
Systemstart-Kennwort	BIOS Configuration	Die Systemstart-Authentifizierung von HP ProtectTools ist ein TPM-basiertes Sicherheitstool, das beim Einschalten den unbefugten Zugriff auf den



**Tabelle 1-1** Kennwortverwaltung (Fortsetzung)

		Computer verhindern soll. Die Systemstart-Authentifizierung verwendet das Basisbenutzerkennwort für HP ProtectTools Embedded Security. Sobald in Computer Setup die Systemstart-Authentifizierungsfunktion aktiviert ist, wird das Kennwort festgelegt, wenn der erste/nächste Basisbenutzerschlüssel für Embedded Security initialisiert wird. Der Embedded Security TPM-Chip schützt das Kennwort für die Systemstart-Authentifizierung.
Java Card-Administratorkennwort	Java Card Security, durch IT-Administrator	Verknüpft die Java Card zum Zweck der Identifizierung mit dem Computer.
 <b>Hinweis</b> Wird auch als BIOS-Administrator-Kartenkennwort bezeichnet.		Gibt einem Computeradministrator die Möglichkeit, Computer Setup-Kennwörter zu aktivieren oder zu deaktivieren, eine neue Administratorkarte zu generieren und Wiederherstellungsdateien für die Wiederherstellung von Benutzer- oder Administratorkarten zu erstellen.
Java Card-PIN	Java Card Security	Schützt den Zugriff auf den Java Card-Inhalt und auf den Computer, wenn eine optionale Java Card und ein entsprechendes Lesegerät verwendet wird. Überprüft, ob das Java Card-Benutzerkennwort mit der PIN übereinstimmt; wird zur Registrierung der Java Card-Authentifizierung verwendet.
Kennwort für Java Card-Wiederherstellungsdatei (falls verfügbar)	Java Card Security	Schützt den Zugriff auf die Wiederherstellungsdatei, die die BIOS-Kennwörter enthält.
Java Card-Benutzerkennwort (falls verfügbar)	Java Card Security	Verknüpft die Java Card zum Zweck der Identifizierung mit dem Computer.
 <b>Hinweis</b> Wird auch als BIOS-Benutzer-Kartenkennwort bezeichnet.		Gibt einem Benutzer die Möglichkeit, zur Wiederherstellung einer Benutzerkarte eine Wiederherstellungsdatei zu erstellen.
Basisbenutzerkennwort	Embedded Security	Wird für den Zugriff auf Embedded Security-Funktionen wie sichere Verschlüsselung von E-Mails, Dateien und Ordnern verwendet. Wenn es als Kennwort für die BIOS-Systemstart-Authentifizierung aktiviert ist, wird beim Einschalten oder Neustart des Computers oder beim Beenden des Standby-Zustands der Zugriff auf den Inhalt des Computers geschützt. Dient auch der Authentifizierung des Personal Secure Drive (PSD) und zur Registrierung der TPM-Authentifizierung.
 <b>Hinweis</b> Wird auch folgendermaßen bezeichnet: Embedded Security-Kennwort, TPM Preboot-Kennwort		
Wiederherstellungs-Token-Kennwort	Embedded Security, durch IT-Administrator	Schützt den Zugriff auf das Wiederherstellungs-Token; dabei handelt es sich um eine Sicherungsdatei

**Tabelle 1-1** Kennwortverwaltung (Fortsetzung)

	<b>Hinweis</b> Wird auch als Wiederherstellungs-Token-Schlüssel bezeichnet.	für den integrierten TPM-Sicherheitschip.
Eigentümerkennwort	Embedded Security, durch IT-Administrator	Schützt das System und den TPM-Chip vor dem unbefugten Zugriff auf alle Eigentümerfunktionen von Embedded Security.
Credential Manager-Anmeldekennwort	Credential Manager	Dieses Kennwort bietet zwei Optionen: <ul style="list-style-type: none"> <li>• Es kann anstelle der Windows-Anmeldung verwendet werden und ermöglicht damit den gleichzeitigen Zugriff auf Windows und Credential Manager.</li> <li>• Es kann nach der Anmeldung bei Microsoft Windows in einer separaten Anmeldung für den Zugriff auf Credential Manager verwendet werden.</li> </ul>
Kennwort für die Credential Manager-Wiederherstellungsdatei	Credential Manager, durch IT-Administrator	Schützt den Zugriff auf die Wiederherstellungsdatei des Credential Manager.
Windows-Anmeldekennwort	Windows-Systemsteuerung	Kann bei der manuellen Anmeldung verwendet oder auf der Java Card gespeichert werden.
Kennwort für Sicherungsplanung	Embedded Security, durch IT-Administrator	Legt die Sicherungsplanung für Embedded Security fest.
	<b>Hinweis</b> Mit einem Windows-Benutzerkennwort wird die Sicherungsplanung für Embedded Security konfiguriert.	
PKCS #12 Import-Kennwort	Embedded Security, durch IT-Administrator	Kennwort, das als Verschlüsselungsschlüssel aus anderen Zertifikaten verwendet wird, falls Zertifikate importiert wurden.
	<b>Hinweis</b> Zu jedem importierten Zertifikat gibt es ein spezielles Kennwort.	 <b>Hinweis</b> Für den normalen Softwarebetrieb nicht erforderlich. Der Benutzer kann festlegen, dass dieses Kennwort erforderlich ist, wenn wichtige Zertifikate mit Embedded Security gesendet werden.
Token zum Zurücksetzen des Kennworts	Embedded Security, durch IT-Administrator	Vom Kunden bereitgestelltes Tool, mit dem der Eigentümer das Basisbenutzerkennwort zurücksetzen kann, falls dies verloren gegangen ist. Das Zurücksetzen wird mithilfe dieses Kennworts ausgeführt.
Administrator Kennwort für Microsoft-Wiederherstellungs-Agenten	Microsoft, durch IT-Sicherheitsadministrator	Stellen Sie sicher, dass PSD-verschlüsselte Daten (Personal Security Drive) wiederhergestellt werden können. Weitere Informationen finden Sie unter

**Tabelle 1-1** Kennwortverwaltung (Fortsetzung)

	<p><b>Hinweis</b> Jeder Administrator eines lokalen Computers kann Wiederherstellungs-Agent sein. Beim Erstellen des Wiederherstellungs-Agenten müssen Sie sich mit dem entsprechenden Administratorkonto anmelden und ein Kennwort eingeben. Der Wiederherstellungs-Agent kann die verschlüsselten Daten aller Benutzer entschlüsseln, indem er einfach die Daten öffnet (ein Assistent wird nicht benötigt).</p>	<p><a href="http://www.microsoft.com/technet/prodtechnol/winxppro/support/dataprot.mspix">http://www.microsoft.com/technet/prodtechnol/winxppro/support/dataprot.mspix</a>.</p>
Virtual Token-Master-PIN	Credential Manager	Kundenoption zum Speichern von Eigentümerzugangsdaten in Credential Manager.
Virtual Token-Benutzer-PIN	Credential Manager	Kundenoption zum Speichern von Eigentümerzugangsdaten in Credential Manager.
Kennwort des Backup Identity-Assistenten	Credential Manager, durch IT-Administrator	Schützt bei der Verwendung von Credential Manager den Zugriff auf eine Identitätssicherung.
Virtual Token-Authentifizierungskennwort	Credential Manager	Dient zur Registrierung der Virtual Token-Authentifizierung durch Credential Manager.
Alias für TPM-Authentifizierung	Credential Manager	Wird nach Wahl des Administrators oder Benutzers von Credential Manager anstelle des Basisbenutzerkennworts verwendet.
Anmeldung über Fingerabdruck	Credential Manager	Mithilfe von Credential Manager kann der Benutzer die Anmeldung mit dem Windows-Kennwort durch eine bequeme und sichere Anmeldung über den Fingerabdruck ersetzen. Im Gegensatz zu Kennwörtern können Fingerabdruck-Zugangsdaten nicht gemeinsam genutzt, weitergegeben, gestohlen oder erraten werden. Wird von Credential Manager verwendet.
USB-Token-Authentifizierung	Credential Manager	Wird von Credential Manager als Token-Authentifizierung anstelle eines Kennworts verwendet.

## Multifaktorauthentifizierung bei der Credential Manager-Anmeldung

Bei der Credential Manager-Anmeldung wird die Multifaktorauthentifizierung für die Anmeldung beim Windows-Betriebssystem aktiviert. Die Sicherheit der normalen Windows-Anmeldung per Kennwort wird angehoben, indem eine starke Multifaktorauthentifizierung verlangt wird. Zugleich wird die tägliche Anmeldung komfortabler, da sich die Benutzer keine Kennwörter mehr merken müssen. Eine besondere Funktion der Credential Manager-Anmeldung ist die Fähigkeit, mehrere Kontozugangsdaten zu einer Benutzeridentität zusammenzufassen. Die Multifaktorauthentifizierung muss nur einmal verwendet werden und ermöglicht dann über die gleichen Zugangsdaten den Zugriff auf verschiedene Windows-Konten.

Die Multifaktor-Benutzerauthentifizierung unterstützt alle Kombinationen von Benutzerkennwörtern, dynamischen oder nur einmal verwendeten Kennwörtern, TPM, Java Cards, USB-Tokens, virtuellen Tokens und biometrischen Daten. Credential Manager unterstützt außerdem weitere Authentifizierungsmethoden und ermöglicht damit die Verwendung mehrerer Benutzerzugriffsrechte für die gleiche Anwendung oder den gleichen Dienst. Ein Benutzer kann alle Zugangsdaten, Anwendungskennwörter und Netzwerkkonten zu einer Dateneinheit, der so genannten Benutzeridentität, zusammenfassen. Die Benutzeridentität wird stets mit der Multifaktorauthentifizierung verschlüsselt und geschützt.

## Erstellen eines sicheren Kennworts

Beim Erstellen von Kennwörtern müssen Sie zunächst alle vom Programm geforderten Spezifikationen beachten. Berücksichtigen Sie jedoch grundsätzlich die folgenden Hinweise, um sichere Kennwörter zu erstellen und das Risiko zu verringern, dass die Kennwortsicherheit beeinträchtigt wird:

- Verwenden Sie Kennwörter mit mehr als sechs Zeichen, vorzugsweise mit mehr als acht.
- Verwenden Sie im Kennwort sowohl Groß- als auch Kleinbuchstaben.
- Verwenden Sie Ziffern und Buchstaben gleichermaßen sowie Sonderzeichen und Satzzeichen.
- Ersetzen Sie Buchstaben in einem Schlüsselwort durch Sonderzeichen oder Zahlen. Sie können beispielsweise die Zahl 1 für die Buchstaben I oder L verwenden.
- Kombinieren Sie Wörter aus mindestens zwei Sprachen.
- Teilen Sie ein Wort oder einen Ausdruck durch Zahlen oder Sonderzeichen, z. B. „Mary22Cat45“.
- Verwenden Sie als Kennwort kein Wort aus einem Wörterbuch.
- Verwenden Sie als Kennwort nicht Ihren Namen oder andere persönliche Informationen wie Geburtsdatum, Namen von Haustieren oder den Mädchennamen Ihrer Mutter, auch dann nicht, wenn Sie diese rückwärts schreiben.
- Ändern Sie Kennwörter regelmäßig. Sie könnten z. B. nur einige Zeichen ändern, und dabei jedes Mal weitere Zeichen ändern.
- Wenn Sie sich Ihr Kennwort notieren, bewahren Sie es nicht an einem allgemein zugänglichen Platz in der Nähe des Computers auf.
- Speichern Sie das Kennwort nicht in einer Datei, z. B. einer E-Mail, auf dem Computer.
- Nutzen Sie Benutzerkonten nicht gemeinsam, und teilen Sie niemandem Ihr Kennwort mit.

# Erweiterte Aufgaben

## Verwalten von ProtectTools-Einstellungen

Einige Funktionen von ProtectTools Security Manager können in BIOS Configuration verwaltet werden.

### Aktivieren bzw. Deaktivieren der Java Card-Systemstart-Authentifizierungsfunktion

Wenn diese Option verfügbar ist und Sie sie aktivieren, können Sie beim Einschalten des Computers die Java Card für die Benutzerauthentifizierung verwenden.



**Hinweis** Zur vollständigen Aktivierung der Funktion für die Systemstart-Authentifizierung müssen Sie die Java Card auch mithilfe des Moduls Java Card Security for ProtectTools konfigurieren.

So aktivieren Sie die Java Card-Systemstart-Authentifizierungsfunktion:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Bereich auf **BIOS Configuration**.
3. Geben Sie an der Aufforderung zur Eingabe des BIOS-Administratorkennworts Ihr Administratorkennwort für Computer Setup ein, und klicken Sie auf **OK**.
4. Klicken Sie im linken Bereich auf **Security**.
5. Klicken Sie unter **Java Card Security** auf **Enable** (Aktivieren).



**Hinweis** Wenn Sie die Java Card-Systemstart-Authentifizierung deaktivieren möchten, wählen Sie **Disable** (Deaktivieren).

6. Klicken Sie auf **Apply** (Übernehmen), und klicken Sie anschließend im Fenster **ProtectTools** auf **OK**, um die Änderungen zu speichern.

### Aktivieren bzw. Deaktivieren der Systemstart-Authentifizierungsfunktion für Embedded Security

Wenn diese Option verfügbar ist und Sie sie aktivieren, kann das System beim Einschalten des Computers den integrierten TPM-Sicherheitschip für die Benutzerauthentifizierung verwenden.



**Hinweis** Zur vollständigen Aktivierung der Funktion für die Systemstart-Authentifizierung müssen Sie den integrierten TPM-Sicherheitschip zusätzlich mithilfe des Moduls Embedded Security for ProtectTools konfigurieren.

So aktivieren Sie die Systemstart-Authentifizierungsfunktion für Embedded Security:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Bereich auf **BIOS Configuration**.
3. Geben Sie an der Aufforderung zur Eingabe des BIOS-Administratorkennworts Ihr Administratorkennwort für Computer Setup ein, und klicken Sie auf **OK**.
4. Klicken Sie im linken Bereich auf **Security**.

5. Wählen Sie unter **Embedded Security** die Option **Enable Power-On Authentication Support** (Systemstart-Authentifizierungsfunktion aktivieren).



---

**Hinweis** Wenn Sie die Systemstart-Authentifizierung für Embedded Security deaktivieren möchten, wählen Sie **Disable** (Deaktivieren).

---

6. Klicken Sie auf **Apply** (Übernehmen), und klicken Sie anschließend im Fenster **ProtectTools** auf **OK**, um die Änderungen zu speichern.

## Verwalten der Computer Setup-Kennwörter

Mit BIOS Configuration können Sie die Kennwörter zum Einschalten und Einrichten des Computers in Computer Setup festlegen und ändern und verschiedene Kennworteinstellungen verwalten.



---

**VORSICHT** Die Kennwörter, die Sie auf der Seite **Passwords** (Kennwörter) in BIOS Configuration festlegen, werden sofort gespeichert, wenn Sie im Fenster **ProtectTools** auf die Schaltfläche **Apply** (Übernehmen) oder **OK** klicken. Merken Sie sich das festgelegte Kennwort, denn Sie können eine Kennworteinstellung nur rückgängig machen, wenn Sie das vorherige Kennwort eingeben.

---

Das Kennwort für den Systemstart kann den Computer vor unbefugtem Zugriff schützen.



---

**Hinweis** Nachdem Sie ein Kennwort für den Systemstart festgelegt haben, wird die Schaltfläche **Set** (Festlegen) auf der Seite **Passwords** (Kennwörter) durch die Schaltfläche **Change** (Ändern) ersetzt.

---

Das Administratorkennwort für Computer Setup schützt die Konfigurationseinstellungen und Systemidentifizierungsdaten in Computer Setup. Nachdem dieses Kennwort festgelegt wurde, muss es eingegeben werden, um auf Computer Setup zugreifen zu können.

Wenn Sie ein Administratorkennwort festgelegt haben, werden Sie vor dem Öffnen des Moduls BIOS Configuration von ProtectTools zur Eingabe des Kennworts aufgefordert.



---

**Hinweis** Nachdem Sie ein Administratorkennwort festgelegt haben, wird die Schaltfläche **Set** (Festlegen) auf der Seite **Passwords** (Kennwörter) durch die Schaltfläche **Change** (Ändern) ersetzt.

---

## Festlegen des Kennworts für den Systemstart (falls verfügbar)

So legen Sie das Systemstart-Kennwort fest:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Bereich auf **BIOS Configuration**, und wählen Sie anschließend **Security** (Sicherheit).
3. Klicken Sie im rechten Bereich neben **Power-On Password** (Systemstart-Kennwort) auf **Set** (Festlegen).
4. Geben Sie das Kennwort in das Feld **Enter Password** (Kennwort eingeben) ein, und bestätigen Sie es im Feld **Verify Password** (Kennwort bestätigen).

5. Klicken Sie im Dialogfeld **Passwords** (Kennwörter) auf **OK**.
6. Klicken Sie auf **Apply** (Übernehmen), und klicken Sie anschließend im Fenster **ProtectTools** auf **OK**, um die Änderungen zu speichern.

## Ändern des Kennworts für den Systemstart (falls verfügbar)

So ändern Sie das Systemstart-Kennwort:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Bereich auf **BIOS Configuration**, und wählen Sie anschließend **Security**.
3. Klicken Sie im rechten Bereich neben **Power-On Password** (Systemstart-Kennwort) auf **Change** (Ändern).
4. Geben Sie das aktuelle Kennwort in das Feld **Old Password** (Altes Kennwort) ein.
5. Legen Sie das neue Kennwort im Feld **Enter Password** (Kennwort eingeben) fest, und bestätigen Sie es im Feld **Verify New Password** (Neues Kennwort bestätigen).
6. Klicken Sie im Dialogfeld **Passwords** (Kennwörter) auf **OK**.
7. Klicken Sie auf **Apply** (Übernehmen), und klicken Sie anschließend im Fenster **ProtectTools** auf **OK**, um die Änderungen zu speichern.

## System-Setup

1. Initialisieren Sie HP ProtectTools Embedded Security.
2. Initialisieren Sie den Basisbenutzerschlüssel.

HP Power-On Authentication Support wird gestartet, sobald der Basisbenutzerschlüssel und das Basisbenutzerkennwort für den Systemstart festgelegt sind. Nach dem nächsten Neustart wird HP ProtectTools Power-On Authentication Support initialisiert, und zum Starten des Computers muss das Basisbenutzerkennwort eingegeben werden. Sobald die Systemstart-Authentifizierung funktioniert, wird die Option zum Aufrufen des BIOS Setup nicht mehr angezeigt. Wenn der Benutzer im Fenster der Systemstart-Authentifizierung das Setup-Kennwort eingibt, wird das BIOS aufgerufen.

Wenn das Basisbenutzerkennwort für Embedded Security bereits festgelegt ist, muss das Kennwort geändert werden, um den Kennwortschutz mithilfe der Systemstart-Authentifizierung festzulegen.

## Ändern der Systemstart-Authentifizierungsfunktion

Die Systemstart-Authentifizierung verwendet das Benutzerkennwort für Embedded Security. So ändern Sie das Kennwort:

1. Geben Sie F10 BIOS-Einstellungen ein (Sie müssen wie oben in den Setup-Schritten beschrieben das Setup-Kennwort eingeben), und navigieren Sie zu **Security** (Sicherheit) > **Embedded Security Device** (Embedded Security-Chip) > **Reset authentication credential** (Authentifizierungsdaten zurücksetzen).
2. Drücken Sie die Pfeiltaste, um die Einstellung von **Do not reset** (Nicht zurücksetzen) auf **Reset** (Zurücksetzen) zu ändern.
3. Navigieren Sie zu **Security Manager > Embedded Security > User Settings** (Benutzereinstellungen) > **Basic User Password** (Basisbenutzerkennwort) > **Change** (Ändern).

4. Geben Sie das alte Kennwort ein. Geben Sie dann das neue Kennwort ein, und bestätigen Sie es.
5. Führen Sie mit der Systemstart-Authentifizierungsfunktion einen Neustart durch.

Im Kennwortfenster wird der Benutzer aufgefordert, zuerst das alte Kennwort einzugeben.

6. Geben Sie das alte Kennwort und dann das neue Kennwort ein. (Wird drei Mal das falsche neue Kennwort eingegeben, wird ein neues Fenster mit der Meldung geöffnet, dass das Kennwort ungültig ist und dass für die Systemstart-Authentifizierung das ursprüngliche Embedded Security-Kennwort F1 = Boot wiederhergestellt wird.

An diesem Punkt sind die Kennwörter nicht synchronisiert, und der Benutzer muss das Embedded Security-Kennwort nochmals ändern, um die Kennwörter erneut zu synchronisieren.)

## Ändern von Benutzerkonten

Die Systemstart-Authentifizierung unterstützt jeweils nur einen Benutzer. Mit den folgenden Schritten können Sie Benutzerkonten ändern, die die Systemstart-Authentifizierung steuern.

1. Navigieren Sie zu **F10 BIOS > Security > Embedded Security Device > Reset authentication credential** (Authentifizierungsdaten zurücksetzen).
2. Drücken Sie die Pfeiltaste, um den Cursor seitlich zu bewegen, und drücken Sie anschließend eine beliebige Taste.
3. Drücken Sie die Taste **F10** zwei Mal und danach die **Eingabetaste**, um die Änderungen zu speichern und die Anwendung zu schließen.
4. Erstellen Sie einen Microsoft Windows-Benutzer, der geändert werden soll, bzw. melden Sie sich mit diesem Benutzernamen an.
5. Öffnen Sie Embedded Security, und initialisieren Sie einen Basisbenutzerschlüssel für das neue Windows-Benutzerkonto. Wenn ein Basisbenutzerschlüssel bereits vorhanden ist, ändern Sie das Basisbenutzerkennwort, um die Eigentümerrechte an der Funktion Systemstart-Authentifizierung zu übernehmen.

Die Systemstart-Authentifizierung akzeptiert jetzt nur das Basisbenutzerkennwort des neuen Benutzers.



**VORSICHT** Es gibt viele Produkte, die Daten durch Softwareverschlüsselung, Hardwareverschlüsselung und Hardware schützen. Die meisten Produkte werden mithilfe von Kennwörtern verwaltet. Wenn Sie diese Tools und Kennwörter nicht verwalten, kann dies zu Datenverlusten und zur Sperre der Hardware führen, so dass diese eventuell ersetzt werden muss. Lesen Sie vor der Verwendung dieser Tools die entsprechenden Hilfedateien.

## Festlegen des Administratorkennworts für Computer Setup

So legen Sie das Administratorkennwort für Computer Setup fest:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Bereich auf **BIOS Configuration**, und wählen Sie anschließend **Security** (Sicherheit).
3. Klicken Sie im rechten Bereich neben **Setup Password** (Setup-Kennwort) auf **Set** (Festlegen).
4. Geben Sie das Kennwort in das Feld **Enter Password** (Kennwort eingeben) ein, und bestätigen Sie es im Feld **Confirm Password** (Kennwort bestätigen).



5. Klicken Sie im Dialogfeld **Passwords** (Kennwörter) auf **OK**.
6. Klicken Sie auf **Apply** (Übernehmen), und klicken Sie anschließend im Fenster **ProtectTools** auf **OK**, um die Änderungen zu speichern.

## Ändern des Administratorkennworts für Computer Setup

So ändern Sie das Administratorkennwort für Computer Setup:

1. Klicken Sie auf **Start > Alle Programme > HP ProtectTools Security Manager**.
2. Klicken Sie im linken Bereich auf **BIOS Configuration**, und wählen Sie anschließend **Security** (Sicherheit).
3. Klicken Sie im rechten Bereich neben **Setup Password** (Setup-Kennwort) auf **Change** (Ändern).
4. Geben Sie das aktuelle Kennwort in das Feld **Old Password** (Altes Kennwort) ein.
5. Legen Sie das neue Kennwort im Feld **Enter Password** (Kennwort eingeben) fest, und bestätigen Sie es im Feld **Verify New Password** (Neues Kennwort bestätigen).
6. Klicken Sie im Dialogfeld **Passwords** (Kennwörter) auf **OK**.
7. Klicken Sie auf **Apply** (Übernehmen), und klicken Sie anschließend im Fenster **ProtectTools** auf **OK**, um die Änderungen zu speichern.

## Verhalten der Systemstart-Authentifizierung bei einem Wörterbuchangriff

Ein Wörterbuchangriff ist eine Methode zum Eindringen in Sicherheitssysteme, bei der systematisch alle in Betracht kommenden Kennwörter zum Aufbrechen eines Sicherheitssystems getestet werden. Bei einem Wörterbuchangriff gegen Embedded Security wird unter Umständen versucht, das Eigentümerkennwort, das Basisbenutzerkennwort oder kennwortgeschützte Schlüssel zu entdecken. Embedded Security verfügt über eine erweiterte Verteidigungsfunktion gegen Wörterbuchangriffe.

### Verteidigung gegen Wörterbuchangriffe

Die Verteidigungsfunktion von Embedded Security gegen Wörterbuchangriffe soll fehlgeschlagene Authentifizierungsversuche erkennen und das TPM vorübergehend deaktivieren, wenn eine bestimmte Anzahl von Fehlschlägen erreicht wurde. Sobald dieser Wert erreicht ist, wird nicht nur das TPM deaktiviert und ein Neustart verlangt, sondern es werden auch immer größere Sperr-Timeouts erzwungen. Während des Timeouts wird die Eingabe des richtigen Kennworts ignoriert. Bei Eingabe des falschen Kennworts wird der letzte Timeoutwert verdoppelt.

Dieser Prozess wird ausführlicher in der Hilfe zu Embedded Security beschrieben. Klicken Sie auf **Welcome to the HP Embedded Security for ProtectTools Solution** (Willkommen bei der Lösung HP Embedded Security for ProtectTools) > **Advanced Embedded Security Operation** (Erweiterter Embedded Security-Betrieb) > **Dictionary Attack Defense** (Verteidigung gegen Wörterbuchangriffe).



**Hinweis** Normalerweise erhält ein Benutzer die Warnung, dass er ein falsches Kennwort eingegeben hat. In der Warnung wird angegeben, wie viele weitere Versuche der Benutzer hat, bevor sich das TPM selbst deaktiviert.

Die Systemstart-Authentifizierung erfolgt im ROM noch vor dem Laden des Betriebssystems. Die Verteidigung gegen Wörterbuchangriffe ist aktiv, dem Benutzer wird als Warnung jedoch nur das X-Symbol angezeigt.

## 2 HP BIOS Configuration for ProtectTools

### Grundkonzepte

BIOS Configuration for ProtectTools bietet Zugriff auf die Sicherheits- und Konfigurationseinstellungen im Dienstprogramm Computer Setup. Dadurch erhalten Benutzer über Windows Zugriff auf Sicherheitsfunktionen des Systems, die durch Computer Setup verwaltet werden.

Mit BIOS Configuration haben Sie folgende Möglichkeiten

- Verwalten von Systemstart-Kennwörtern und Administratorkennwörtern
- Konfigurieren weiterer Funktionen der Systemstart-Authentifizierung, beispielsweise Aktivieren von Java Card-Kennwörtern und der Authentifizierungsfunktion für Embedded Security
- Aktivieren und Deaktivieren von Hardwarekomponenten, beispielsweise des CD-ROM-Startlaufwerks oder von verschiedenen Hardwareanschlüssen
- Konfigurieren von Startoptionen, z. B. Aktivieren von Mehrfach-Boot und Ändern der Startreihenfolge



---

**Hinweis** Viele Funktionen in BIOS Configuration für ProtectTools stehen auch in Computer Setup zur Verfügung.

---

### Ändern der BIOS-Einstellungen

Mit BIOS Configuration können Sie verschiedene Computereinstellungen verwalten, die andernfalls nur zugänglich wären, wenn Sie beim Start die Taste **F10** drücken und das Dienstprogramm Computer Setup aktivieren. Im *Computer Setup (F10) Utility-Handbuch* auf der mit dem Computer gelieferten *Documentation and Diagnostics CD* finden Sie Informationen zu Einstellungen und Funktionen. Wenn Sie auf die Hilfedateien für BIOS Configuration zugreifen möchten, klicken Sie auf **Security Manager > BIOS Configuration > Help** (Hilfe).



---

**Hinweis** Spezielle Anleitungen für ProtectTools BIOS Configuration finden Sie in der ProtectTools-Hilfe.

---



# 3 HP Embedded Security for ProtectTools

## Grundkonzepte

Falls verfügbar, schützt Embedded Security for ProtectTools vor dem unbefugten Zugriff auf Benutzerdaten oder Zugangsdaten. Dieses Modul verfügt über die folgenden Sicherheitsfunktionen:

- Erweitertes verschlüsselndes Dateisystem (Encrypting File System, EFS) von Microsoft für die Verschlüsselung von Ordnern und Dateien
- Erstellung eines PSD (Personal Security Drive) zum Verschlüsseln von Benutzerdaten
- Datenverwaltungsfunktionen wie Sichern und Wiederherstellen der Schlüsselhierarchie
- Unterstützung von Drittanbieterprogrammen, die MSCAPI verwenden (wie Microsoft Outlook und Microsoft Internet Explorer), und von Anwendungen, die PKCS#11 verwenden (wie Netscape), für geschützte digitale Zertifikatsvorgänge unter Verwendung der Embedded Security-Software

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

Die Hardware besteht aus einem TPM-Sicherheitschip, der den TCG-Anforderungen (Trusted Computing Group) der TPM 1.2-Standards entspricht. Der Chip ist in die Systemplatine integriert. Bei manchen TPM-Implementierungen (je nach dem gekauften Modell) ist TPM auf der Netzwerkkarte integriert. Bei diesen Netzwerkkarten-/TPM-Konfigurationen befinden sich der On-Chip- und Off-Chip-Speicher, -Funktionen und -Firmware in einem externen Flash-Speicher, der in die Systemplatine integriert ist. Alle TPM-Funktionen sind entweder verschlüsselt oder geschützt, um einen sicheren Flash-Speicher bzw. sichere Kommunikation zu gewährleisten.

Die Software bietet zudem die Funktion Personal Secure Drive (PSD). Diese Funktion ergänzt die EFS-basierte Datei- und Ordnerverschlüsselung und verwendet den AES-Verschlüsselungsalgorithmus (Advanced Encryption Standard). Wir weisen darauf hin, dass HP ProtectTools Personal Secure Drive nur ordnungsgemäß funktionieren kann, wenn das TPM nicht verborgen wird, durch eine mit Eigentümerrechten installierte Software aktiviert ist und wenn die Benutzerkonfiguration initialisiert ist.

# Setup-Verfahren

---



**VORSICHT** Zur Reduzierung des Sicherheitsrisikos sollte der IT-Administrator den integrierten TPM-Sicherheitschip sofort initialisieren. Wenn der integrierte TPM-Sicherheitschip nicht initialisiert wird, kann ein unbefugter Benutzer oder ein Computerwurm Zugriff auf den Computer erhalten, bzw. der integrierte TPM-Sicherheitschip könnte von einem Virus initialisiert werden, so dass der Zugriff auf den PC eingeschränkt wird.

---

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 **Security** (Sicherheit) > **Setup Password** (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 **Enable** > **Save Changes and Exit** (Aktivieren > Änderungen speichern und schließen).



**Hinweis** Spezielle Anleitungen für ProtectTools Embedded Security finden Sie in der ProtectTools-Hilfe.

---

# 4 HP Credential Manager for ProtectTools

## Grundkonzepte

Credential Manager for ProtectTools verfügt über Sicherheitsfunktionen, die eine sichere und komfortable Computerumgebung gewährleisten. Zu den Funktionen zählen unter anderem:

- Alternativen zu Kennwörtern für die Anmeldung bei Microsoft Windows, wie Java Card oder biometrische Lesegeräte
- Funktion für einmalige Anmeldung (Single-Sign-On), die sich automatisch Zugangsdaten (Benutzer-IDs und Kennwörter) für Websites, Anwendungen und geschützte Netzwerkressourcen merkt
- Unterstützung optionaler Sicherheitsgeräte, wie Java Cards und biometrische Lesegeräte
- Unterstützung zusätzlicher Sicherheitseinstellungen, wie Authentifizierung über ein optionales Sicherheitsgerät zum Entsperren des Computers und für den Zugriff auf Anwendungen
- Erweiterte Verschlüsselung für gespeicherte Kennwörter bei Implementierung über einen integrierten TPM-Sicherheitschip

## Startverfahren

So starten Sie Credential Manager, falls verfügbar:

1. Klicken Sie auf **Start > Systemsteuerung > Sicherheitscenter > ProtectTools Security Manager > Credential Manager**.
2. Klicken Sie oben rechts auf dem Bildschirm auf **Log On** (Anmelden).

Sie haben folgende Möglichkeiten, um sich bei Credential Manager anzumelden:

- Credential Manager-Anmelde-Assistent (bevorzugtes Verfahren)
- ProtectTools Security Manager



---

**Hinweis** Wenn Sie im Fenster der Windows-Anmeldung die Aufforderung zur Anmeldung bei Credential Manager verwenden, um sich bei Credential Manager anzumelden, werden Sie gleichzeitig bei Windows angemeldet.

---

## Erstmalige Anmeldung

Wenn Sie Credential Manager zum ersten Mal öffnen, melden Sie sich mit dem normalen Windows-Kennwort an. Anschließend wird automatisch ein Credential Manager-Konto mit Ihren Windows-Zugangsdaten angelegt.

Nach der Anmeldung bei Credential Manager können Sie weitere Zugangsdaten registrieren, beispielsweise einen Fingerabdruck oder eine Java Card.

Bei der nächsten Anmeldung können Sie die Anmelderrichtlinie auswählen und eine beliebige Kombination der registrierten Zugangsdaten verwenden.



**Hinweis** Spezielle Anleitungen für ProtectTools Security Manager finden Sie in der ProtectTools-Hilfe.

---



# 5 HP Java Card Security for ProtectTools

## Grundkonzepte

Mit Java Card Security for ProtectTools verwalten Sie die Java Card-Einrichtung und -Konfiguration für Computer, die mit einem optionalen Java Card-Lesegerät ausgestattet sind.

Mit Java Card Security for ProtectTools haben Sie folgende Möglichkeiten

- Zugriff auf Java Card Security-Funktionen.
- Initialisieren einer Java Card, so dass sie mit anderen ProtectTools-Modulen wie z. B. Credential Manager for ProtectTools verwendet werden kann.
- Verwenden des Dienstprogramms Computer Setup, um die Java Card-Authentifizierung in einer Preboot-Umgebung zu aktivieren und separate Java Cards für einen Administrator und einen Benutzer zu konfigurieren. Der Benutzer muss dann die Java Card einsetzen und optional eine PIN eingeben. Erst danach kann das Betriebssystem geladen werden.
- Festlegen und Ändern des Kennworts, mit dem die Benutzer der Java Card authentifiziert werden (falls verfügbar).
- Sichern und Wiederherstellen von Java Card-BIOS-Kennwörtern, die auf der Java Card gespeichert sind (falls verfügbar).
- Speichern des BIOS-Kennworts auf der Java Card (falls verfügbar).



---

**Hinweis** Spezielle Anleitungen für ProtectTools Security Manager finden Sie in der ProtectTools-Hilfe.

---



## 6 Lösungen von Drittanbietern

Plattformen mit TPM erfordern sowohl einen TCG Software Stack (TSS) als auch Embedded Security-Software. Der TSS steht auf allen Modellen zur Verfügung. Embedded Security-Software muss für manche Modelle separat erworben werden. Für diese Modelle steht ein NTRU TSS zur Verfügung, der vom Kunden erworbene integrierte Sicherheitssoftware von Drittanbietern unterstützt. Wir empfehlen Drittanbieterlösungen wie Wave Embassy Trust Suite.



# 7 HP Client Manager for Remote Deployment

## Hintergrund

HP Trustworthy-Plattformen, die mit einem Trusted Platform Module (TPM) ausgestattet sind, werden mit deaktiviertem TPM (Standardzustand) ausgeliefert. Das Aktivieren des TPM ist eine Administrator-Aufgabe und wird durch Richtlinien geschützt, die vom HP BIOS erzwungen werden. Der Administrator muss die BIOS-Konfigurationsoptionen (F10-Optionen) aufrufen und das TPM aktivieren. Die TCG-Spezifikationen (Trusted Computing Group) verlangen darüber hinaus, dass die Aktivierung eines TPM nur durch den expliziten Eingriff eines (physisch anwesenden) Benutzers erfolgt. Auf diese Weise wird sichergestellt, dass die Datenschutzrechte eines Benutzers respektiert werden (durch ein entsprechendes Anmeldemodell) und dass bösartige Anwendungen, Viren oder Trojaner das TPM nicht für böswillige Zwecke aktivieren. Die Tatsache, dass ein Administrator physisch und vor Ort anwesend sein muss, stellen eine große Herausforderung für IT-Manager dar, die diese Technologie in einem großen Unternehmen bereitstellen möchten.

## Initialisierung

HP Client Manager (HPCM) bietet die Möglichkeit, das TPM remote zu aktivieren und in einer Unternehmensumgebung zu verwalten. Bei dieser Methode muss der IT-Administrator nicht physisch anwesend sein; dennoch erfüllt sie die TCG-Anforderungen.

Mithilfe von HPCM stellt der IT-Administrator bestimmte BIOS-Optionen ein und startet das System anschließend neu, um das TPM auf dem Remote-System zu aktivieren. Bei diesem Neustart zeigt das BIOS standardmäßig eine Eingabeaufforderung an. Der Endbenutzer muss daraufhin eine Taste drücken, um, wie von den TCG-Spezifikationen verlangt, seine physische Anwesenheit zu belegen. Das Remote-System setzt danach den Startvorgang fort, das Skript wird ausgeführt, und der Benutzer übernimmt die Eigentümerrechte am TPM des Systems. Während dieses Vorgangs werden an einem vom IT-Administrator festgelegten Ort ein Wiederherstellungsarchiv und ein Wiederherstellungstoken für Notfälle erstellt.

Die TPM-Benutzerinitialisierung auf dem Remote-System wird nicht von HPCM ausgeführt, da der Benutzer die Möglichkeit haben muss, das Kennwort festzulegen. Die TPM-Benutzerinitialisierung muss vom Endbenutzer des betreffenden Systems ausgeführt werden.

## Wartung

Mit HP Client Manager kann das Benutzerkennwort remote zurückgesetzt werden, ohne dass dem IT-Administrator das Benutzerkennwort mitgeteilt werden muss. Mit HPCM können auch die Benutzerzugangsdaten remote wiederhergestellt werden. Für beide Funktionen müssen die richtigen Administratorkennwörter eingegeben werden.



# 8 Fehlerbeseitigung


## Credential Manager for ProtectTools

Kurzbeschreibung	Einzelheiten	Lösung
Mithilfe der Option <b>Credential Manager Network Accounts</b> (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 Authentifizierungsmethoden 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.	<p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p>
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.	<p>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.</p> <p>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.</p>

Kurzbeschreibung	Einzelheiten	Lösung
Die Option <b>Browse for Virtual Token</b> (Nach virtuellem Token suchen) ist während des Anmeldeprozesses nicht verfügbar.	Der Benutzer kann den Speicherort des registrierten virtuellen Token in Credential Manager nicht ändern, da die Option zum Durchsuchen auf Grund von Sicherheitsrisiken entfernt wurde.	Die Option zum Durchsuchen wurde aus den aktuellen Produkten entfernt, da sie es unberechtigten Benutzern ermöglicht, Dateien zu löschen und umzubenennen und die Kontrolle über Windows zu übernehmen.
Bei der Anmeldung mit TPM-Authentifizierung steht die Option <b>Network Accounts</b> (Netzwerkkonten) nicht zur Verfügung.	Mit der Option <b>Network Accounts</b> (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 Anwendungsfehler zurückgegeben: <b>User account restriction</b> (Benutzerkontenbeschränkung).	Credential Manager kann das Kennwort eines Domänenbenutzerkontos nicht über die Option <b>Change Windows password</b> (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 <b>Windows security</b> (Windows-Sicherheit) > <b>Change password</b> (Kennwort ändern) ändern. Da der Domänenbenutzer jedoch über kein Konto auf dem lokalen PC verfügt, 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 <b>Connect</b> (Verbinden) auf dem Bildschirm nicht.	Wenn die Zugangsdaten der Single-Sign-On-Funktion für Remote Desktop Connection (RDP) auf <b>Connect</b> (Verbinden) eingestellt sind, gibt die Single-Sign-On-Funktion bei Neustart stets <b>Save As</b> (Speichern unter) anstatt <b>Connect</b> (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 <b>Back</b> (Zurück) auf dem	Wenn ein Benutzer bei der Anmeldung bei Credential Manager die TPM-Authentifizierung verwendet, das Kennwort eingibt und dann auf die	HP untersucht mögliche Behelfslösungen, die in zukünftigen Produkten bereitgestellt werden könnten.



Kurzbeschreibung	Einzelheiten	Lösung
Bildschirm verwendet wird, kann keine andere Authentifizierungsmethode ausgewählt werden.	Schaltfläche <b>Back</b> (Zurück) klickt, funktioniert diese nicht ordnungsgemäß. Anstatt eine Auswahl anderer Authentifizierungsmethoden anzuzeigen, wird sofort der Windows-Anmeldebildschirm angezeigt.	
Credential Manager wird aus dem Standby-Modus geöffnet, auch wenn das Programm nicht entsprechend konfiguriert ist.	Wenn <b>Use Credential Manager log on to Windows</b> (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.	<p>Wenn kein Administratorkennwort eingerichtet ist, können sich Benutzer auf Grund von Kontobeschränkungen von Credential Manager nicht über Credential Manager bei Windows anmelden.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Mit Java Card/Token können die Benutzer mit der folgenden Behelfslösung beim Einsetzen einer Java Card das Öffnen von Credential Manager aktivieren/deaktivieren.</li> </ul> <ol style="list-style-type: none"> <li>1. Klicken Sie auf <b>Advanced Settings</b> (Erweiterte Einstellungen).</li> <li>2. Klicken Sie auf <b>Service &amp; Applications</b> (Service &amp; Anwendungen).</li> <li>3. Klicken Sie auf <b>Java Cards and Tokens</b> (Java Cards und Tokens).</li> <li>4. Klicken Sie, wenn die Java Card/das Token eingesetzt wird.</li> <li>5. Aktivieren Sie das Kontrollkästchen <b>Advise to log-on</b> (Benachrichtigung zur Anmeldung).</li> </ol>
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.	<p>Dies ist das beabsichtigte Standardverhalten der Anwendung.</p> <p>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.</p>
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.	<p>Dies ist das beabsichtigte Standardverhalten der Anwendung.</p> <p>Wenn der Benutzer die Betriebssystemeinstellungen für die Werte der automatischen Administratoranmeldung zum Überspringen ändern möchte, lautet der Pfad zum Bearbeiten folgendermaßen: <code>HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/WinLogon</code>.</p>


Kurzbeschreibung	Einzelheiten	Lösung
		 <p><b>VORSICHT</b> 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.</p>
<p>Es wird eine Meldung zur Anmeldung per Fingerabdruck angezeigt, unabhängig davon, ob das Lesegerät für Fingerabdrücke installiert oder registriert ist.</p>	<p>Wenn der Benutzer die Windows-Anmeldung wählt, wird in der Taskleiste von Credential Manager folgende Desktop-Warnung angezeigt: <b>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 sich bei Credential Manager anzumelden).</b></p>	<p>Mit dieser Desktop-Warnung soll der Benutzer darauf hingewiesen werden, dass die Authentifizierung per Fingerabdruck verfügbar ist, wenn sie konfiguriert wurde.</p>
<p>Im Anmeldefenster von Credential Manager für Windows 2000 wird der Benutzer aufgefordert, seine Karte einzusetzen (<b>insert card</b>), obwohl kein Lesegerät angeschlossen ist.</p>	<p>Auf der Windows-Willkommenseite in Credential Manager wird der Benutzer aufgefordert, seine Karte einzusetzen (<b>insert card</b>), obwohl kein Java Card-Lesegerät angeschlossen ist.</p>	<p>Mit dieser Meldung soll der Benutzer darauf hingewiesen werden, dass die Java Card-Authentifizierung verfügbar ist, wenn sie konfiguriert wurde.</p>
<p>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.</p>	<p>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.</p>	<p>Dieses Problem scheint in Service Pack 2 von Microsoft behoben worden zu sein. Weitere Informationen zum Ursprung dieses Problems finden Sie unter <a href="http://www.microsoft.com">http://www.microsoft.com</a> in Artikel 813301 der Microsoft Knowledge Base.</p> <p>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.</p> <p>Wenn sich die Benutzer zuerst bei Windows anmelden, müssen sie sich anschließend manuell bei Credential Manager anmelden.</p>
<p>Bei der Wiederherstellung von Embedded Security schlägt Credential Manager fehl.</p>	<p>Die Registrierung der Zugangsdaten in Credential Manager schlägt fehl, nachdem die Werkseinstellungen des ROM wiederhergestellt wurden.</p>	<p>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.</p> <p>Der integrierte TPM-Sicherheitschip kann mit dem Dienstprogramm BIOS Computer Setup, BIOS Configuration for ProtectTools oder mit dem HP Client</p>

Kurzbeschreibung	Einzelheiten	Lösung
Der Prozess <b>Restore Identity</b> (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.	<p>Manager aktiviert werden. So aktivieren Sie den integrierten TPM-Sicherheitschip:</p> <ol style="list-style-type: none"> <li>1. Öffnen Sie Computer Setup, indem Sie den Computer einschalten oder neu starten. Drücken Sie dann die Taste <b>F10</b>, während die Meldung <b>F10 = ROM Based Setup</b> (F10 = ROM-basiertes Setup) unten links auf dem Bildschirm angezeigt wird.</li> <li>2. Wählen Sie mithilfe der Pfeiltasten die Funktion <b>Security</b> (Sicherheit) &gt; <b>Setup Password</b> (Setup-Kennwort). Legen Sie ein Kennwort fest.</li> <li>3. Wählen Sie <b>Embedded Security Device</b> (Embedded Security-Chip).</li> <li>4. Wählen Sie mit den Pfeiltasten <b>Embedded Security Device – Disable</b> (Embedded Security-Chip – Deaktivieren). Ändern Sie die Einstellung mit den Pfeiltasten auf <b>Embedded Security Device – Enable</b> (Embedded Security-Chip – Aktivieren).</li> <li>5. Wählen Sie <b>Enable</b> (Aktivieren) &gt; <b>Save Changes and Exit</b> (Änderungen speichern und schließen).</li> </ol> <p>HP arbeitet derzeit an Lösungsmöglichkeiten für zukünftige Software-Versionen.</p>
		<p>Dies ist zurzeit das beabsichtigte Standardverhalten der Anwendung.</p> <p>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.</p> <p>HP untersucht langfristige Optionen zur Behebung des Problems.</p>

# Embedded Security for 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 <b>Error Applying Attributes</b> (Fehler beim Anwenden der Attribute) angezeigt. Der Benutzer kann jedoch die gleichen Dateien auf dem Laufwerk C:\ einer separat installierten Festplatte verschlüsseln.	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.
Die Eigentumsrechte können auf einer Mehrfachboot-Plattform nicht in ein anderes Betriebssystem übernommen werden.	Wenn ein Laufwerk für den Start mehrerer Betriebssysteme eingerichtet ist, können die Eigentumsrechte nur vom Assistenten für die Plattforminitialisierung eines Betriebssystems übernommen werden.	Dies ist das aus Sicherheitsgründen vorgesehene Standardverhalten.
Ein 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	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	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.

Kurzbeschreibung	Einzelheiten	Lösung
gekennzeichnet) im Netzwerk freigeben.	Netzwerk unter Verwendung der versteckten Freigabe (\$) zugegriffen werden.	
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.
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 Scanvorgangs 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 Verschlüsselungskennwort 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 <b>Encrypt</b> (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 <b>Encrypt</b> (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 <b>Eigenschaften &gt; Erweitert &gt; Inhalt verschlüsseln</b> .
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	Führen Sie nach einem Stromausfall folgende Aktionen durch:

Kurzbeschreibung	Einzelheiten	Lösung
	<p>Stromausfall kommt, treten folgende Fehler auf:</p> <ul style="list-style-type: none"> <li>Beim Versuch, den Assistenten für die Initialisierung von Embedded Security (Embedded Security Initialization Wizard) zu starten, wird der folgende Fehler angezeigt: <b>The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.</b> (Embedded Security kann nicht initialisiert werden, da der Embedded Security-Chip bereits über einen Embedded Security-Eigentümer verfügt.)</li> <li>Beim Versuch, den Assistenten für die Benutzerinitialisierung (User Initialization Wizard) zu starten, wird der folgende Fehler angezeigt: <b>The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.</b> (Embedded Security ist nicht initialisiert. Um den Assistenten zu verwenden, muss Embedded Security zuerst initialisiert werden.)</li> </ul>	 <p><b>Hinweis</b> Verwenden Sie die Pfeiltasten, um verschiedene Menüs und Menüelemente auszuwählen und Werte zu ändern (falls nicht anders angegeben).</p> <ol style="list-style-type: none"> <li>Starten Sie den Computer, oder führen Sie einen Neustart durch.</li> <li>Drücken Sie <b>F10</b>, wenn <b>F10=Setup</b> auf dem Bildschirm angezeigt wird (oder sobald die Monitor-LED grün leuchtet).</li> <li>Wählen Sie die entsprechende Sprachoption aus.</li> <li>Drücken Sie die <b>Eingabetaste</b>.</li> <li>Wählen Sie <b>Security</b> (Sicherheit) &gt; <b>Embedded Security</b>.</li> <li>Setzen Sie die Option <b>Embedded Security Device</b> (Embedded Security-Chip) auf <b>Enable</b> (Aktivieren).</li> <li>Drücken Sie <b>F10</b>, um die Änderung zu übernehmen.</li> <li>Wählen Sie <b>File</b> (Datei) &gt; <b>Save Changes and Exit</b> (Änderungen speichern und schließen).</li> <li>Drücken Sie die <b>Eingabetaste</b>.</li> <li>Drücken Sie <b>F10</b>, um die Änderungen zu speichern und Computer Setup zu beenden.</li> </ol>
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.	<p>Dies ist das beabsichtigte Standardverhalten der Anwendung.</p> <p>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.</p>
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.	<p>Dies entspricht dem Standardverhalten der Anwendung.</p> <p>Der Benutzer muss sich abmelden und dann erneut anmelden, um das Dialogfeld für das PSD-Kennwort wieder anzuzeigen.</p>
Zum Ändern der Sicherheitsplattformrichtlinien 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.	<p>Dies entspricht dem Standardverhalten der Anwendung.</p> <p>Alle Administratoren können mit oder ohne Benutzerinitialisierung des TPM die Sicherheitsplattformrichtlinien ändern.</p>

Kurzbeschreibung	Einzelheiten	Lösung
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 <b>Enter Password</b> (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 <a href="http://www.microsoft.com">http://www.microsoft.com</a> .  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.
Der folgende Fehler tritt zeitweilig bei Verschlüsselungs- und Entschlüsselungsvorgängen auf: <b>The process cannot access the file because it is being used by another process.</b> (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: <ol style="list-style-type: none"><li>1. Starten Sie das System neu.</li><li>2. Melden Sie sich ab.</li><li>3. Melden Sie sich wieder an.</li></ol>
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 <b>The device is not ready</b> (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 <b>Disable</b> (Deaktivieren) nicht	Der Benutzer kann entweder die Deinstallation ohne Deaktivieren des TPM-Chips durchführen oder zunächst den TPM-Chip deaktivieren (über das Administrations-Tool) und dann die Deinstallation durchführen. Um auf das Administrations-Tool zugreifen zu können, muss der Basisbenutzerschlüssel initialisiert	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 <b>OK</b> oder <b>Cancel</b> (Abbrechen), um den Deinstallationsprozess fortzusetzen.



Kurzbeschreibung	Einzelheiten	Lösung
<p>verfügbar. Das Deinstallationsprogramm wird erst dann fortgesetzt, wenn das Administrations-Tool geschlossen wird.</p>	<p>werden. Wurde der Schlüssel nicht initialisiert, kann der Benutzer auf keine Option zugreifen.</p> <p>Wenn der Benutzer explizit das Öffnen des Administrations-Tools festgelegt hat, indem er im Dialogfeld mit der Aufforderung <b>Click Yes to open Embedded Security Administration tool</b> (Klicken Sie auf „Ja“, um das Embedded Security-Administrations-Tool zu öffnen) auf <b>Yes</b> (Ja) geklickt hat, wird der Deinstallationsprozess erst fortgesetzt, wenn das Administrations-Tool geschlossen wurde. Wenn der Benutzer in diesem Dialogfeld auf <b>No</b> (Nein) geklickt hat, wird das Administrations-Tool nicht geöffnet, und die Deinstallation wird fortgesetzt.</p>	
<p>Das System wird nach dem Erstellen eines PSD für zwei Benutzerkonten und dem Verwenden von schnellem Benutzerwechsel in 128-MB-Systemkonfigurationen zeitweilig gesperrt.</p>	<p>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.</p>	<p>Die Ursache ist vermutlich ein Zeitsteuerungsproblem in Konfigurationen mit wenig Arbeitsspeicher.</p> <p>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.</p> <p>Als Behelfslösung sollte das System neu gestartet werden, und die Benutzer sollten den Speicher vergrößern (HP liefert standardmäßig keine 128-MB-Konfigurationen mit Sicherheitsmodulen).</p>
<p>Zeitüberschreitung bei der EFS-Benutzerauthentifizierung (Kennwortanforderung): <b>Access denied</b> (Zugriff verweigert).</p>	<p>Die Kennwortaufforderung für die EFS-Benutzerauthentifizierung wird erneut geöffnet, wenn Sie auf <b>OK</b> klicken oder nach einer Zeitüberschreitung den Computer aus dem Standby-Modus wieder aktivieren.</p>	<p>Dies entspricht dem Standardverhalten der Anwendung. Um Probleme mit Microsoft EFS zu verhindern, wurde zum Generieren dieser Fehlermeldung ein 30-Sekunden-Watchdog-Timer erstellt.</p>
<p>In den Funktionsbeschreibungen für den Installationsprozess sind im Japanischen die Wörter teilweise abgeschnitten.</p>	<p>Im Installationsassistenten sind bei der benutzerdefinierten Installation Funktionsbeschreibungen teilweise abgeschnitten.</p>	<p>HP wird dieses Problem in zukünftigen Versionen beheben.</p>
<p>Die EFS-Verschlüsselung funktioniert ohne das Angeben eines Kennworts an der Eingabeaufforderung.</p>	<p>Bei einer Zeitüberschreitung zur Eingabe eines Benutzerkennworts können Verschlüsselungen immer noch für Dateien oder Ordner durchgeführt werden.</p>	<p>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.</p>
<p>Sichere E-Mail-Funktionen werden auch dann unterstützt, wenn die entsprechende Option im Assistenten für die Benutzerinitialisierung (User Initialization Wizard)</p>	<p>Die Embedded Security-Software und der Assistent steuern nicht die Einstellungen von E-Mail-Clients (Outlook, Outlook Express oder Netscape).</p>	<p>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 Assistent ermöglicht zur sofortigen Anpassung der</p>



Kurzbeschreibung	Einzelheiten	Lösung
oder die Konfiguration für sichere E-Mails in den Benutzerrichtlinien deaktiviert ist.		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 Wiederherstellungsarchive 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.	<p>Der Fehler tritt auf, nachdem der Benutzer:</p> <ul style="list-style-type: none"> <li>Eigentümer und Benutzer in Embedded Security unter Verwendung des Standardspeicherorts <b>Eigene Dokumente</b> initialisiert hat</li> <li>den Chip im BIOS auf die Werkseinstellungen zurückgesetzt hat</li> <li>den Computer neu startet</li> <li>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 TPM-Benutzerauthentifizierung automatisieren kann. Wenn der Benutzer <b>Yes</b> (Ja) auswählt, wird der Speicherort der Datei <b>SPEmRecToken.xml</b> automatisch im Textfeld angezeigt.</li> </ul> <p>Obwohl der Speicherort korrekt ist, wird die folgende Fehlermeldung angezeigt: <b>No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.</b> (Kein Wiederherstellungs-Token vorhanden. Wählen Sie den Speicherort des Wiederherstellungs-Token aus.)</p>	Klicken Sie auf die Schaltfläche <b>Browse</b> (Durchsuchen), um den Speicherort auszuwählen. Der Wiederherstellungsvorgang wird dann fortgesetzt.
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	Das PSD des zweiten Benutzers steht erst dann zur Verfügung, wenn ihm ein anderer Laufwerksbuchstabe zugewiesen wird oder wenn der erste Benutzer sich abmeldet.

Kurzbeschreibung	Einzelheiten	Lösung
	<p>PSD des zweiten Benutzers nicht verfügbar.</p>	
<p>Das PSD wird deaktiviert und kann nach dem Formatieren der Festplatte, auf der das PSD generiert wurde, nicht gelöscht werden.</p>	<p>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 <b>Drive is not accessible</b> (Auf das Laufwerk kann nicht zugegriffen werden) angezeigt.</p> <p>Der Benutzer kann das PSD nicht löschen. Es wird folgende Meldung angezeigt: <b>Your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process.</b> (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.</p>	<p>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.</p> <p>Lösung: Nach dem nächsten Neustart werden die Emulationen nicht geladen. Der Benutzer kann die alte PSD-Emulation löschen und ein neues PSD erstellen.</p>
<p>Bei der Wiederherstellung aus dem automatischen Sicherungsarchiv ist ein interner Fehler aufgetreten.</p>	<p>Wenn der Benutzer</p> <ul style="list-style-type: none"> <li>in HPPTSM auf die Embedded Security-Option <b>Restore under Backup</b> (Wiederherstellung von Sicherungskopie) zum Wiederherstellen aus einem automatischen Sicherungsarchiv klickt,</li> <li>die Datei <b>SPSystemBackup.xml</b> auswählt,</li> </ul> <p>schlägt der Wiederherstellungs-Assistent (Restore Wizard) fehl, und die folgende Fehlermeldung wird angezeigt: <b>The selected Backup Archive does not match the restore reason. Please select another archive and continue.</b> (Das ausgewählte Sicherungsarchiv entspricht nicht dem Wiederherstellungsgrund. Wählen Sie ein anderes Archiv aus, um fortzufahren.)</p>	<p>Wenn der Benutzer statt der erforderlichen Datei <b>SpBackupArchive.xml</b> die Datei <b>SpSystemBackup.xml</b> auswählt, gibt der Embedded Security-Assistent folgende Fehlermeldung zurück: <b>An internal Embedded Security error has been detected. (Ein interner Embedded Security-Fehler ist aufgetreten.)</b></p> <p>Der Benutzer muss die richtige XML-Datei für den angegebenen Grund auswählen.</p> <p>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.</p>
<p>Wiederherstellungsfehler des Sicherheitssystems bei mehreren Benutzern.</p>	<p>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 (<b>decryption process failed</b>).</p>	<p>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</p>

Kurzbeschreibung	Einzelheiten	Lösung
		<p>ausgewählten Benutzer nicht wiederhergestellt werden.</p> <p>Außerdem muss der Benutzer die gesamte Sicherungskopie des Systems wiederherstellen. Archivierte Sicherungskopien können einzeln wiederhergestellt werden.</p>
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.	<p>So blenden Sie den TPM-Chip im BIOS wieder ein:</p> <p>Öffnen Sie das Dienstprogramm Computer Setup (F10), navigieren Sie zu <b>Security</b> (Sicherheit) &gt; <b>Device security</b> (Gerätesicherheit), und ändern Sie die Einstellungen von <b>Hidden</b> (Gerät verborgen) &gt; auf <b>Available</b> (Gerät verfügbar).</p>
Das automatische Erstellen einer Sicherungskopie ist für das zugeordnete Laufwerk nicht möglich.	<p>Wenn ein Administrator das Erstellen einer automatischen Sicherungskopie in Embedded Security einrichtet, wird unter <b>Windows &gt; Tasks &gt; Scheduled Task</b> (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.</p> <p>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.</p> <p>Wenn die automatische Sicherung bei der Anmeldung ausgeführt werden soll, zeigt das Embedded Security-TNA-Symbol folgende Meldung an: <b>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.</b> (Auf den Speicherort für das Sicherungsarchiv kann zurzeit nicht zugegriffen werden. Klicken Sie hier, falls Sie Sicherungskopien in einem temporären Archiv speichern möchten, 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.</p>	<p>Als Behelfslösung können Sie NT AUTHORITY \SYSTEM in (Computername)\(Administratorname) ändern. Dies ist die Standardeinstellung, wenn der geplante Task manuell erstellt wird.</p> <p>HP wird in zukünftigen Produktversionen Standardeinstellungen bereitstellen, die (Computername\Administratorname) enthalten.</p>
Der Embedded Security-Status kann auf der grafischen Benutzeroberfläche von	Die aktuelle Software-Version 4.0 wurde für HP Notebook 1.1B Implementierungen sowie HP Desktop 1.2 Implementierungen entworfen.	HP wird dieses Problem in zukünftigen Versionen beheben.

Kurzbeschreibung	Einzelheiten	Lösung
Embedded Security vorübergehend nicht deaktiviert werden.	Die Deaktivierungsoption wird weiterhin von der Software-Schnittstelle für TPM 1.1-Plattformen unterstützt.	

# Verschiedenes

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
<p>HP ProtectTools Security Manager – Es wird folgender Warnhinweis angezeigt: <b>The security application can not be installed until the HP Protect Tools Security Manager is installed.</b> (Die Sicherheitsanwendung kann erst dann installiert werden, wenn HP ProtectTools Security Manager installiert ist.)</p>	<p>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.</p>	<p>Vor dem Installieren von Sicherheits-Plug-Ins muss die HP ProtectTools Security Manager-Software installiert werden.</p>
<p>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 <b>ownership required</b> (Eigentumsrechte erforderlich) zurück.</p>	<p>Dies entspricht dem erwarteten Verhalten der TPM-Firmware für dc7600 und Modelle mit Broadcom-fähigen TPM-Chips.</p> <p>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.</p> <p>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.</p> <p>Wenn das BIOS-TPM auf die Werkseinstellungen zurückgesetzt wird, werden Eigentümerrechte entfernt, und die Firmware kann erst dann aktualisiert werden, wenn die Embedded Security-Softwareplattform und der Assistent für die Benutzerinitialisierung (User Initialization Wizard) konfiguriert wurden.</p> <p>*Nach einer Firmware-Aktualisierung sollte der Computer stets neu gestartet werden. Die Firmware-Version wird erst nach einem Neustart korrekt erkannt.</p>	<ol style="list-style-type: none"> <li>1. Installieren Sie die HP ProtectTools Embedded Security-Software neu.</li> <li>2. Führen Sie den Plattform and User Configuration Wizard (Assistenten für Plattform- und Benutzerkonfiguration) aus.</li> <li>3. Stellen Sie sicher, dass Microsoft .NET Framework 1.1 auf dem System installiert ist:             <ol style="list-style-type: none"> <li>a. Klicken Sie auf <b>Start</b>.</li> <li>b. Klicken Sie auf <b>Systemsteuerung</b>.</li> <li>c. Klicken Sie auf <b>Software</b>.</li> <li>d. Stellen Sie sicher, dass <b>Microsoft .NET Framework 1.1</b> in der Liste enthalten ist.</li> </ol> </li> <li>4. Überprüfen Sie die Hardware- und Softwarekonfiguration:             <ol style="list-style-type: none"> <li>a. Klicken Sie auf <b>Start</b>.</li> <li>b. Klicken Sie auf <b>Alle Programme</b>.</li> <li>c. Klicken Sie auf <b>HP ProtectTools Security Manager</b>.</li> <li>d. Wählen Sie <b>Embedded Security</b> aus.</li> <li>e. Klicken Sie auf <b>More Details</b> (Weitere Details). Das System sollte folgende Konfiguration aufweisen:                 <ul style="list-style-type: none"> <li>• Product version (Produktversion) = V4.0.1</li> <li>• Embedded Security State (Embedded Security-Status): Chip State (Chip-Status) = Enabled (Aktiviert), Owner State (Eigentümerstatus) = Initialized (Initialisiert), User State (Benutzerstatus) = Initialized (Initialisiert)</li> </ul> </li> </ol> </li> </ol>

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
		<ul style="list-style-type: none"> <li>• Component Info (Komponenteninformation): TCG Spec. Version (Version TCG-Spez.) = 1.2</li> <li>• Vendor (Anbieter) = Broadcom Corporation</li> <li>• FW Version (Firmware-Version) = 2.18 (oder höher)</li> <li>• TPM Device driver library version 2.0.0.9 (or greater) (TPM-Gerätetreiberbibliothek Version 2.0.0.9 (oder höher))</li> </ul> <p>5. Wenn die Firmware-Version nicht 2.18 ist, laden Sie die entsprechende Version herunter, und aktualisieren Sie die TPM-Firmware. Das TPM-Firmware-SoftPak ist als Support-Download unter <a href="http://www.hp.com">http://www.hp.com</a> verfügbar.</p>
<p>HP ProtectTools Security Manager – Beim Schließen der Security Manager-Schnittstelle wird zeitweilig ein Fehler zurückgegeben.</p>	<p>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.</p>	<p>Dies ist auf eine Zeitsteuerungsabhängigkeit von Ladezeiten für Plug-In-Dienste beim Schließen und Neustarten von Security Manager zurückzuführen. Da die Datei <b>PTHOST.exe</b> 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.</p> <p>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.</p>
<p>HP ProtectTools * Allgemein – Unbeschränkte Zugriffs- oder Administratorrechte stellen ein Sicherheitsrisiko dar.</p>	<p>Folgende Risiken bestehen beim uneingeschränktem Zugriff auf den Client-PC:</p> <ul style="list-style-type: none"> <li>• Löschen von PSDs</li> <li>• Mutwilliges Ändern von Benutzereinstellungen</li> <li>• Deaktivieren von Sicherheitsrichtlinien und -funktionen</li> </ul>	<p>Administratoren sollten empfohlene Verfahrensweisen anwenden, um Endbenutzerrechte und den Benutzerzugriff zu beschränken.</p> <p>Unautorisierte Benutzer sollten keine Administratorrechte erhalten.</p>
<p>Die Embedded Security-Kennwörter für das BIOS und das Betriebssystem sind nicht synchronisiert.</p>	<p>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.</p>	<p>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.</p>
<p>Nach der Aktivierung der TPM-Preboot-Authentifizierung im BIOS kann sich nur ein Benutzer am System anmelden.</p>	<p>Die PIN für das TPM-BIOS wird dem ersten Benutzer zugeordnet, der die Benutzereinstellung initialisiert. Bei einem Computer mit mehreren Benutzern ist der Administrator</p>	<p>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</p>

Betroffene Software – Kurzbeschreibung	Einzelheiten	Lösung
	normalerweise der erste Benutzer. Dieser muss seine TPM-Benutzer-PIN an andere Benutzer weitergeben, damit diese sich anmelden können.	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 <b>Power-on authentication support</b> (Systemstartauthentifizierung) wird mit der Embedded Security-Funktion <b>Reset to Factory Settings</b> (Auf Werkseinstellungen zurücksetzen) nicht auf die Standardeinstellung zurückgesetzt.	In Computer Setup wird die Option <b>Power-on authentication support</b> (Systemstartauthentifizierung) mit der Embedded Security-Chip-Option <b>Reset to Factory Settings</b> (Auf Werkseinstellungen zurücksetzen) nicht auf die Werkseinstellungen zurückgesetzt. Standardmäßig wird <b>Power-on authentication support</b> (Systemstart-Authentifizierung) auf <b>Disable</b> (Deaktivieren) eingestellt.	Mit der Option <b>Reset to Factory Settings</b> (Auf Werkseinstellungen zurücksetzen) wird der Embedded Security-Chip deaktiviert. Dadurch werden die anderen Embedded Security-Optionen (einschließlich <b>Power-on authentication support</b> (Systemstart-Authentifizierung)) ausgeblendet. Nach dem erneuten Aktivieren des Embedded Security-Chips bleibt die Option <b>Power-on authentication support</b> (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

**Advanced Encryption Standard (AES, Erweiterter Verschlüsselungsstandard)** Ein symmetrischer Verschlüsselungsalgorithmus mit einer Blockgröße von 128 Bit

**Application Programming Interface (API, Programmierschnittstelle)** Eine Reihe interner Betriebssystemfunktionen, mit deren Hilfe Anwendungen verschiedene Aufgaben ausführen können

**Authentifizierung** Prozess, mit dem überprüft wird, ob ein Benutzer zur Durchführung einer Aufgabe berechtigt ist, z. B. Zugriff auf einen Computer, Ändern von Einstellungen für ein bestimmtes Programm oder Anzeigen von geschützten Daten.

**Biometrisch** Kategorie von Authentifizierungsdaten, die zur Identifizierung eines Benutzers ein physisches Merkmal, beispielsweise einen Fingerabdruck, verwenden.

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

**BIOS-Sicherheitsmodus** Einstellung in Java Card Security for ProtectTools. Ist die Einstellung aktiviert, erfolgt die Benutzerauthentifizierung mittels einer Java Card und einer gültigen PIN.

**Cryptographic Service Provider (CSP, Kryptographiedienstleister)** Anbieter oder Bibliothek kryptographischer Algorithmen, die in einer gut definierten Schnittstelle für die Ausführung bestimmter kryptographischer Funktionen verwendet werden kann. Eine Software-Komponente mit einer Schnittstelle zu MSCAPI.

**Digitale Signatur** Daten, die zusammen mit einer Datei gesendet werden, die den Absender des Materials verifiziert und bestätigt, dass die Datei nach dem Signieren nicht modifiziert wurde.

**Digitales Zertifikat** Elektronische Zugangsdaten, die die Identität einer Person oder eines Unternehmens bestätigen, indem die Identität des Eigentümers des digitalen Zertifikats an ein Paar elektronischer Schlüssel gebunden wird, mit denen digitale Informationen signiert werden.

**Domäne** Gruppe von Computern, die Teil eines Netzwerks sind und eine gemeinsame Verzeichnisdatenbank verwenden. Domänen haben eindeutige Namen, und jede Domäne umfasst gemeinsame Regeln und Verfahren.

**Dringende Sicherheit** Sicherheitsfunktion in BIOS Configuration, die einen erweiterten Schutz für die Systemstart- und Administratorkennwörter sowie für andere Formen der Systemstart-Authentifizierung bietet.

**Encryption File System (EFS, Verschlüsselungssystem)** System, mit dem alle Dateien und Unterordner innerhalb des ausgewählten Ordners verschlüsselt werden. Ein unter Microsoft Windows 2000 oder höher verfügbarer transparenter Dateiverschlüsselungsdienst.

**Entschlüsselung** Verfahren der Kryptographie, mit dem verschlüsselte Daten in normalen Text umgewandelt werden.

**Identität** Im ProtectTools Credential Manager eine Gruppe von Zugangsdaten und Einstellungen, die wie ein Konto oder Profil eines bestimmten Benutzers behandelt werden.

**Integrierter Trusted Platform Module (TPM)-Sicherheitschip (nur in bestimmten Modellen enthalten)**

Integrierter Sicherheitschip, der sehr empfindliche Benutzerdaten vor böswilligen Angriffen schützen kann. Er bildet die Vertrauensgrundlage einer bestimmten Plattform. Der TPM-Sicherheitschip stellt kryptographische Algorithmen und Vorgänge bereit, die die Spezifikationen der Trusted Computing Group (TCG) erfüllen. TPM-Hardware und -Software erhöhen die Sicherheit von EFS und PSD durch den Schutz der Schlüssel, die von EFS und PSD verwendet werden. In Systemen ohne TPM werden diese Schlüssel normalerweise auf der Festplatte gespeichert. Dadurch sind die Schlüssel potenziell durch unberechtigte Zugriffe gefährdet. In Systemen mit TPM-Chip werden die TPM-internen Storage Root Keys, die immer im TPM-Chip vorhanden sind, zum „Tarnen“ bzw. zum Schutz der von EFS und PSD verwendeten Schlüssel verwendet. Es ist viel schwieriger, zum Extrahieren privater Schlüssel in das TPM-Modul einzudringen als in die Festplatte. Der TPM-Chip erweitert über S/MIME zudem die Sicherheit von E-Mails in Microsoft Outlook und Outlook Express. Der Chip fungiert als ein CPS (Cryptographic Service Provider). Schlüssel und Zertifikate werden von der TPM-Hardware generiert und/oder unterstützt und bieten so eine weitaus höhere Sicherheit als Implementierungen, die ausschließlich auf Software beruhen.

**Java Card** Kleine Hardwarekomponente von etwa der Größe und Form einer Kreditkarte, auf der identifizierende Informationen über den Eigentümer gespeichert sind. Dient zur Authentifizierung des Eigentümers auf einem Computer.

**Java Card-Administratorkennwort** Kennwort, das die Java Card eines Administrators in Computer Setup mit dem Computer verknüpft und zur Identifizierung des Administrators beim Systemstart oder beim Neustart dient. Dieses Kennwort kann manuell vom Administrator festgelegt oder durch einen Zufallsalgorithmus generiert werden.

**Java Card-Benutzerkennwort** Kennwort, das die Java Card eines Benutzers in Computer Setup mit dem Computer verknüpft und zur Identifizierung des Benutzers beim Systemstart oder beim Neustart dient. Dieses Kennwort kann manuell vom Administrator festgelegt oder durch einen Zufallsalgorithmus generiert werden.

**Kryptographie** Das Verschlüsseln und Entschlüsseln von Daten, sodass diese nur von bestimmten Personen dekodiert werden können.

**Low Pin Count (LPC, Niedrige Pin-Anzahl)** Definiert eine von HP ProtectTool Embedded Security verwendete Schnittstelle zum Plattform-Chipsatz. Der Bus besteht aus 4 Bit großen Adress-/Datenpins, ist mit 33 MHz getaktet und verfügt über mehrere Steuerungs-/Statuspins.

**Microsoft Cryptographic API oder CryptoAPI (MSCAPI)** Eine API von Microsoft, die für kryptographische Anwendungen eine Schnittstelle zum Windows-Betriebssystem bietet.

**Migration** Eine Aufgabe, die die Verwaltung, Wiederherstellung und Übertragung von Schlüsseln und Zertifikaten ermöglicht.

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

**Neustart** Neustart des Computers.

**Personal Secure Drive (PSD, Persönliches, sicheres Laufwerk)** Stellt einen geschützten Speicherbereich für empfindliche Daten bereit. Eine von HP ProtectTools Embedded Security bereitgestellte Funktion. Diese Anwendung erstellt ein virtuelles Laufwerk auf dem Computer des Benutzers, das dorthin verschobene Dateien und Ordner automatisch verschlüsselt.

**Public Key Cryptographic Standards (PKCS, kryptographische Standards für öffentliche Schlüssel)** Generierte Standards, die die Definition und Verwendung von öffentlichen und privaten Schlüsseln zur Verschlüsselung und Entschlüsselung bestimmen.

**Public Key Infrastructure (PKI, Infrastruktur öffentlicher Schlüssel)** Ein allgemeiner Begriff, der die Implementierung von Sicherheitssystemen definiert, die öffentliche und private Schlüssel zur Verschlüsselung und Entschlüsselung verwenden.

**Secure Multipurpose Internet Mail Extensions (S/MIME, Protokoll für den Austausch sicherer elektronischer Mails über das Internet)** Eine Spezifikation für sicheres elektronisches Messaging mithilfe von PKCS. S/MIME bietet Authentifizierung über digitale Signaturen und Datenschutz durch Verschlüsselung.

**Single Sign On (Funktion zum einmaligen Anmelden)** Funktion, die Authentifizierungsdaten speichert und Ihnen gestattet, über Credential Manager auf Internet- und Windows-Anwendungen zuzugreifen, die eine Kennwortauthentifizierung verlangen.

**Systemstart-Authentifizierung** Sicherheitsfunktion, die beim Einschalten des Computers eine bestimmte Form der Authentifizierung verlangt, beispielsweise eine Java Card, einen Sicherheitschip oder ein Kennwort.

**TCG Software Stack (TSS)** Stellt Dienste bereit, die den TPM-Chip nutzen, erfordert jedoch nicht den gleichen Schutz. Enthält eine Standard-Softwareschnittstelle für den Zugriff auf TPM-Funktionen. Zur vollen Nutzung der TPM-Fähigkeiten wie Schlüsselsicherung, Schlüsselmigration, Plattformauthentifizierung und -bestätigung schreiben die Anwendungen direkt in den TSS.

**Trusted Computing Group (TCG)** Industrieverband, der das Konzept eines „sicheren PCs“ fördert. TCG ist die Nachfolgeorganisation der TCPA (Trusted Computing Platform Alliance).

**Trusted Computing Platform Alliance (TCPA)** Organisation für einen „vertrauenswürdigen Computereinsatz“, die durch die TCG abgelöst wurde.

**USB-Token** Sicherheitsgerät, auf dem Identitätsinformationen über einen Benutzer gespeichert sind. Ebenso wie eine Java Card oder ein biometrisches Lesegerät dient das USB-Token zur Authentifizierung eines Eigentümers gegenüber einem Computer.

**Verschlüsselung** Verfahren, beispielsweise die Verwendung eines Algorithmus, mit dem in der Kryptographie normaler Text in Ziffern konvertiert wird, um unbefugte Empfänger daran zu hindern, die Daten zu lesen. Es gibt viele Arten der Datenverschlüsselung. Sie bilden die Grundlage der Netzwerksicherheit. Häufig verwendete Arten sind Datenverschlüsselungsstandard (Data Encryption Standard, DES) und Verschlüsselung mit öffentlichen Schlüsseln.

**Virtuelles Token** Sicherheitsfunktion, die ähnlich wie eine Java Card und ein entsprechendes Lesegerät funktioniert. Das Token wird entweder auf der Festplatte des Computers oder in der Windows-Registrierung gespeichert. Bei der Anmeldung über ein virtuelles Token werden Sie zum Abschließen der Authentifizierung zur Eingabe einer Benutzer-PIN aufgefordert.

**Wiederherstellungsarchiv** Geschützter Speicherbereich, der die erneute Verschlüsselung von Basisbenutzerschlüsseln von einem Plattformeigentümerschlüssel zu einem anderen ermöglicht.

**Windows-Benutzerkonto** Profil für einen Benutzer, der berechtigt ist, sich im Netzwerk oder an einem bestimmten Computer anzumelden.

**Zertifizierungsstelle** Dienst, der die für die Ausführung einer Infrastruktur öffentlicher Schlüssel benötigten Zertifikate ausgibt.

**Zugangsdaten** Methode, mit der ein Benutzer bei der Authentifizierung nachweist, dass er zur Ausführung einer bestimmten Aufgabe berechtigt ist.



# Index

## A

Alias für TPM-Authentifizierung 5  
Anmeldung über  
Fingerabdruck 5

## B

Basisbenutzer-Kennwort,  
Definition 3  
Betriebsanzeige  
Ändern des Kennworts 9  
Festlegen des Kennworts 8  
Kennwortdefinition 2  
Wörterbuchangriff 12

## BIOS

Administrator-Kartenkennwort,  
Definition 3  
Administrator-Kennwort,  
Definition 2  
Ändern von Einstellungen 13  
Benutzer-Kartenkennwort,  
Definition 3  
BIOS Configuration for  
ProtectTools 13

## C

Client Manager 23  
Computer Setup  
Administratorkennwort,  
ändern 11  
Administrator-Kennwort,  
Definition 2  
Einstellen des  
Administratorkennworts 10  
Kennwörter, verwalten 8  
Credential Manager  
Anmeldekennwort 4  
Anmelden 5, 18  
Fehlerbeseitigung 25

Installation 17  
Kennwort für die  
Wiederherstellungsdatei 4

## E

Eigentümerkennwort, Definition 4  
Embedded Security for  
ProtectTools  
Fehlerbeseitigung 30  
Kennwort 3  
Setup 16  
Systemstart-  
Authentifizierung 7  
Erweiterte Aufgaben 7

## F

F10-Setup-Kennwort 2  
Fehlerbeseitigung  
Credential Manager for  
ProtectTools 25  
Embedded Security for  
ProtectTools 30  
Verschiedenes 39

## I

Installation, Credential  
Manager 17

## J

Java Card  
Administratorkennwort,  
Definition 3  
Benutzerkennwort,  
Definition 3  
Kennwort für  
Wiederherstellungsdatei,  
Definition 3  
PIN, Definition 3

Security for ProtectTools 19  
Systemstart-  
Authentifizierung 7

## K

Kennwort des Backup Identity-  
Assistenten 5  
Kennwörter  
Alias für TPM-  
Authentifizierung 5  
Anmeldung über  
Fingerabdruck 5  
Backup Identity-Assistent 5  
Basisbenutzer 3  
Betriebsanzeige 2  
Computer Setup, verwalten 8  
Computer Setup-  
Administrator 2  
Computer Setup-Administrator,  
ändern 11  
Computer Setup-Administrator,  
festlegen 10  
Credential Manager-  
Anmeldung 4  
Credential Manager-  
Wiederherstellungsdatei 4  
Definitionen 2  
Eigentümer 4  
Hinweise 6  
Java Card-Administrator 3  
Java Card-Benutzer 3  
Java Card-PIN 3  
Java Card-  
Wiederherstellungsdatei 3  
PKCS #12 Import 4  
ProtectTools, Verwaltung 2  
Sicherheits-  
Wiederherstellungs-Agent 4  
Sicherungsplanung 4  
Systemstart, ändern 9

- Systemstart, festlegen 8
- Token zum Zurücksetzen des  
Kennworts 4
- USB-Token-  
Authentifizierung 5
- Virtual Token-  
Authentifizierung 5
- Virtual Token-Benutzer-PIN 5
- Virtual Token-Master-PIN 5
- Wiederherstellungs-Token 3
- Windows-Anmeldung 4
- Kennwort für Sicherheits-  
Wiederherstellungs-Agenten 4
- Kennwort für  
Sicherungsplanung 4

**L**  
Lösungen von Drittanbietern 21

**M**  
Multifaktorauthentifizierung bei der  
Credential Manager-  
Anmeldung 5

**P**  
PKCS #12 Import-Kennwort 4  
ProtectTools  
Credential Manager 17  
Embedded Security für 15  
Java Card Security 19  
Kennwortverwaltung 2  
Security Manager-Module 1  
Verwalten von  
Einstellungen 7  
Zugriff auf Security  
Manager 1

**R**  
Remote-Bereitstellung, Client  
Manager 23

**S**  
Security Manager, ProtectTools 1  
Sicherheit  
Embedded Security for  
ProtectTools 15  
Java Card 19  
Rollen 2  
Setup-Kennwort 2

Software  
ProtectTools Security  
Manager 1  
Systemstart-Authentifizierung  
Embedded Security 7  
Java Card 7

**T**  
TCG Software Stack (TSS) 1, 21  
Token zum Zurücksetzen des  
Kennworts 4  
TPM Preboot-Kennwort 3

**U**  
USB-Token-Authentifizierung 5

**V**  
Virtual Token-  
Authentifizierungskennwort 5  
Virtual Token-Benutzer-PIN 5  
Virtual Token-Master-PIN 5

**W**  
Wiederherstellungs-Token-  
Kennwort, Definition 3  
Windows  
Anmeldekennwort 4  
Wörterbuchangriff 12