HP ProtectTools

Einführung

Erste Ausgabe: August 2012

Teilenummer des Dokuments: 702113-041

Inhaltsverzeichnis

1 Einführung zum Thema Sicherheit

Die HP ProtectTools Security Manager Software bietet Sicherheitsfunktionen, die den Computer, Netzwerke und wichtige Daten vor nicht autorisiertem Zugriff schützen.

Anwendung	Funktionen
HP ProtectTools Security Manager Administrator-Konsole (für Administratoren)	• Für den Zugriff sind Administratorrechte unter Microsoft Windows® erforderlich. • Bietet Zugriff auf Module, die von einem Administrator konfiguriert werden und für Benutzer nicht verfügbar sind. • Ermöglicht eine erste Sicherheitseinrichtung und die Konfiguration von Optionen oder Anforderungen für alle Benutzer.
HP ProtectTools Security Manager Benutzer-Konsole (für Benutzer)	• Ermöglicht einem Benutzer, Optionen zu konfigurieren, die von einem Administrator bereitgestellt wurden. • Ermöglicht Administratoren, Benutzern die eingeschränkte Steuerung einiger HP ProtectTools Module zu ermöglichen.

Das für Ihren Computer verfügbare Softwaremodul kann je nach Computermodell unterschiedlich sein.

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

HINWEIS: Die Anleitungen in diesem Handbuch setzen voraus, dass die betreffenden Softwaremodule von HP ProtectTools bereits installiert sind.

Funktionen von HP ProtectTools

In der folgenden Tabelle werden wichtige Funktionen der HP ProtectTools Module beschrieben:

Modul	Wichtige Funktionen
HP ProtectTools Security Manager Administrator-Konsole	Administratoren können die folgenden Funktionen ausführen: • Den Installationsassistenten für Security Manager verwenden, um Sicherheitseinstellungen und Sicherheits-Anmeldemethoden einzurichten und zu konfigurieren. • Optionen, die für Benutzer nicht sichtbar sind, konfigurieren. • Drive Encryption und den Benutzerzugriff konfigurieren. • Richtlinien für Device Access Manager und den Benutzerzugriff konfigurieren. • Administratortools verwenden, um HP ProtectTools Benutzer hinzuzufügen oder zu entfernen und den Benutzerstatus anzuzeigen.

Modul	Wichtige Funktionen
HP ProtectTools Security Manager Benutzer-Konsole	Normale Benutzer können die folgenden Funktionen ausführen: • Einstellungen für Verschlüsselungsstatus und Device Access Manager anzeigen. • Computrace for HP ProtectTools aktivieren. • Voreinstellungen und Sicherungs- sowie Wiederherstellungsoptionen konfigurieren.
Credential Manager	Normale Benutzer können die folgenden Funktionen ausführen: • Benutzernamen und Kennwörter ändern. • Benutzeranmeldeinformationen, wie Windows Kennwort, Fingerabdruck, Gesichtsbilder, Smart Card, RFID-Karte oder Transponderkarte konfigurieren und ändern.
Password Manager	Normale Benutzer können die folgenden Funktionen ausführen: • Benutzernamen und Kennwörter verwalten und einrichten. • Stärkere Kennwörter für eine höhere Kontosicherheit erstellen. Password Manager füllt die Informationen automatisch aus und übermittelt sie. • Den Anmeldevorgang mit der Single Sign-On-Funktion beschleunigen, die Benutzeranmeldeinformationen automatisch speichert und anwendet.
Drive Encryption for HP ProtectTools (bestimmte Modelle)	• Bietet eine komplette Verschlüsselung der gesamten Festplatte. • Erzwingt eine Authentifizierung vor dem Systemstart zum Entschlüsseln und Zugreifen auf Daten. • Bietet die Option zur Aktivierung selbstverschlüsselnder Laufwerke (bestimmte Modelle):
Device Access Manager for HP ProtectTools (bestimmte Modelle)	• Ermöglicht IT-Managern die Zugriffssteuerung von Geräten auf Basis von Benutzerprofilen. • Verhindert, dass Daten von nicht autorisierten Benutzern auf externe Speichermedien kopiert werden und Viren über externe Medien in das System gelangen. • Ermöglicht Administratoren, den Zugriff auf Kommunikationsgeräte für bestimmte Personen oder Benutzergruppen zu sperren.
Wiederbeschaffung gestohlener Geräte (Computrace for HP ProtectTools, separat erhältlich)	• Für die Aktivierung ist ein separates Tracking- and Tracing-Abonnement erforderlich. • Bietet sichere Bestandsverfolgung. • Überwacht Benutzeraktivität sowie Hardware- und Softwareänderungen. • Bleibt aktiv, auch wenn die Festplatte neu formatiert oder ersetzt wird.

HP ProtectTools – Beschreibung und allgemeine Nutzungsbeispiele der Sicherheitsprodukte

Die meisten der HP ProtectTools Sicherheitsprodukte verfügen sowohl über die Benutzerauthentifizierung (normalerweise ein Kennwort) als auch über ein Administrator-Backup, um

den Zugriff zu gewährleisten, wenn Kennwörter verloren gehen, nicht verfügbar sind oder vergessen wurden, oder wenn die Unternehmenssicherheit einen Zugriff erforderlich macht.

HINWEIS: Einige der HP ProtectTools Sicherheitsprodukte dienen der Zugriffsbeschränkung auf Daten. Daten sollten verschlüsselt werden, wenn sie so wichtig sind, dass der Benutzer sie lieber verlieren würde, als sie an andere weiterzugeben. Es wird empfohlen, ein Backup aller Daten an einem sicheren Ort aufzubewahren.

Password Manager

Password Manager speichert Benutzernamen und Kennwörter und lässt sich für Folgendes einsetzen:

- Speichern von Anmeldenamen und Kennwörtern für den Internetzugriff und E-Mails.
- Automatische Anmeldung des Benutzers bei einer Website oder E-Mail.
- Verwalten und Organisieren von Authentifizierungen.
- Auswahl eines Web- oder Netzwerkbestands und direkter Zugriff auf den Link.
- Anzeigen von Namen und Kennwörtern, wenn erforderlich.

Beispiel 1: Die Einkaufssachbearbeiterin eines großen Herstellers tätigt die meisten ihrer Unternehmenstransaktionen über das Internet. Sie besucht auch häufig verschiedene Websites, für die Anmeldeinformationen erforderlich sind. Sie achtet genau auf Sicherheit, benutzt also nicht für jedes Konto das gleiche Kennwort. Die Einkaufssachbearbeiterin hat sich entschieden, Password Manager zu verwenden, um Weblinks mit verschiedenen Benutzernamen und Kennwörtern abzugleichen. Wenn sie sich auf einer Website anmeldet, übermittelt Password Manager automatisch die Zugriffsdaten. Wenn sie den Benutzernamen und das Kennwort abrufen möchte, kann Password Manager dazu konfiguriert werden, sie anzuzeigen.

Password Manager kann auch zum Verwalten und Organisieren der Authentifizierungen verwendet werden. Das Tool ermöglicht einem Benutzer die Auswahl eines Web- oder Netzwerkbestands und den direkten Zugriff auf den Link. Der Benutzer kann gegebenenfalls Namen und Kennwörter abrufen.

Beispiel 2: Ein Buchprüfer wurde befördert und leitet nun die gesamte Buchhaltung. Das Team muss sich bei einer Vielzahl von Client-Webkonten anmelden, für die verschiedene Anmeldeinformationen erforderlich sind. Diese Anmeldeinformationen werden mit anderen Angestellten gemeinsam genutzt, Vertraulichkeit ist also ein Thema. Der Buchhalter entscheidet sich, alle Weblinks, Benutzernamen im Unternehmen und Kennwörter mit Password Manager zu verwalten. Sobald er damit fertig ist, stellt der Buchhalter Password Manager für die Mitarbeiter bereit, so dass diese mit den Webkonten arbeiten können, ohne die von ihnen verwendeten Anmeldedaten zu kennen.

Drive Encryption for HP ProtectTools (bestimmte Modelle)

Drive Encryption dient zur Zugriffseinschränkung auf die Daten der gesamten Computerfestplatte oder eines Zweitlaufwerks. Drive Encryption kann auch selbstverschlüsselnde Laufwerke verwalten.

Beispiel 1: Ein Arzt möchte sicherstellen, dass nur er Zugriff auf die Daten auf seiner Computerfestplatte hat. Er aktiviert Drive Encryption, was eine Authentifizierung vor dem Systemstart erforderlich macht, noch vor der Anmeldung bei Windows. Nach der Einrichtung ist kein Zugriff auf die Festplatte ohne Angabe eines Kennworts vor dem Betriebssystemstart mehr möglich. Der Arzt kann die Laufwerkssicherheit noch weiter verbessern, wenn er die Daten mit der Option für selbstverschlüsselnde Laufwerke verschlüsselt.

Drive Encryption for HP ProtectTools verhindert den Zugriff auf die verschlüsselten Daten auch dann, wenn das Laufwerk entfernt wird, weil beide an die ursprüngliche Systemplatine gebunden sind.

Beispiel 2: Der Verwaltungschef eines Krankenhauses möchte sicherstellen, dass nur Ärzte und autorisierte Mitarbeiter auf die Daten auf ihrem lokalen Computer zugreifen können, ohne ihre persönlichen Kennwörter anderen preisgeben zu müssen. Die IT-Abteilung fügt den Administrator, die Ärzte und alle autorisierten Mitarbeiter als Drive Encryption-Benutzer hinzu. Jetzt können nur noch autorisierte Mitarbeiter den Computer oder die Domäne mit ihrem persönlichen Benutzernamen und Kennwort starten.

Device Access Manager for HP ProtectTools (bestimmte Modelle)

Device Access Manager for HP ProtectTools ermöglicht es einem Administrator, den Zugriff auf die Hardware einzuschränken und zu verwalten. Device Access Manager for HP ProtectTools kann dazu verwendet werden, den nicht autorisierten Zugriff auf USB-Flash-Laufwerke zu verhindern, wenn Daten kopiert werden könnten. Er kann auch den Zugriff auf CD/DVD-Laufwerke und die Steuerung von USB-Geräten, Netzwerkverbindungen usw. einschränken. Ein Beispiel wäre eine Situation, in der andere Hersteller Zugriff auf einen Unternehmenscomputer benötigen, aber nicht in der Lage sein sollen, Daten auf ein USB-Laufwerk zu kopieren.

Beispiel 1: Der Manager eines Unternehmens für medizinischen Bedarf arbeitet neben seinen Unternehmensdaten auch oft mit Krankenakten. Die Angestellten benötigen Zugriff auf diese Daten, es ist aber extrem wichtig, dass die Daten nicht mit einem USB-Laufwerk oder einem anderen externen Speichermedium vom Computer entfernt werden können. Das Netzwerk ist sicher, aber die Computer haben CD-Brenner und USB-Anschlüsse, die es ermöglichen, die Daten zu stehlen oder zu kopieren. Der Manager verwendet Device Access Manager, um die USB-Anschlüsse und CD-Brenner zu deaktivieren, damit sie nicht benutzt werden können. Obwohl die USB-Anschlüsse gesperrt sind, bleiben Maus und Tastatur funktionsfähig.

Beispiel 2: Ein Versicherungsunternehmen möchte verhindern, dass die Angestellten persönliche Software oder Daten von Zuhause installieren oder laden. Einige Angestellte benötigen auf allen Computern Zugriff auf den USB-Anschluss. Der IT-Manager verwendet Device Access Manager, um den Zugriff für einige Angestellte zu ermöglichen und gleichzeitig den externen Zugriff für andere zu sperren.

Computrace for HP ProtectTools (zuvor LoJack Pro) (separat zu erwerben)

Computrace for HP ProtectTools (separat erhältlich) ist ein Service, der die Position eines gestohlenen Computers bestimmen kann, sobald der Benutzer auf das Internet zugreift. Computrace for HP ProtectTools dient auch dazu, Computer per Fernzugriff zu verwalten und aufzufinden sowie die Nutzung von Computern und Anwendungen zu überwachen.

Beispiel 1: Ein Schuldirektor hat die IT-Abteilung damit beauftragt, alle Computer an seiner Schule zu verfolgen. Nach der Bestandsaufnahme der Computer hat der IT-Administrator alle Computer bei Computrace registriert, sodass sie sich im Fall eines Diebstahls verfolgen lassen. Kürzlich stellte die Schule fest, dass mehrere Computer fehlen. Der IT-Administrator setzte also die Behörden und Computrace-Mitarbeiter davon in Kenntnis. Die Computer wurden gefunden und von den Behörden der Schule zurückgebracht.

Beispiel 2: Eine Immobiliengesellschaft muss weltweit Computer verwalten und aktualisieren. Sie verwendet Computrace, um die Computer zu überwachen und zu aktualisieren, ohne dazu einen IT-Mitarbeiter zu jedem Computer schicken zu müssen.

Die wichtigsten Sicherheitsziele

HP ProtectTools Module können zusammenarbeiten, um Lösungen für verschiedene Sicherheitsprobleme zu bieten. Hierzu zählen folgende wichtige Sicherheitsziele:

- Schutz vor gezieltem Diebstahl
- Beschränken des Zugriffs auf sensible Daten
- Verhindern von nicht autorisiertem internen oder externen Zugriff
- Erstellen von Richtlinien für starke Kennwörter

Schutz vor gezieltem Diebstahl

Ein Beispiel für gezielten Diebstahl wäre der Diebstahl eines Computers der Sicherheitskontrolle am Flughafen, der vertrauliche Daten und Kundeninformationen enthält. Die folgenden Funktionen bieten Schutz vor gezieltem Diebstahl:

- Die Funktion zur Authentifizierung vor dem Systemstart verhindert den Zugriff auf das Betriebssystem.
    - Security Manager for HP ProtectTools – Siehe „HP ProtectTools Security Manager“ auf Seite 28.
    - Drive Encryption for HP ProtectTools – Siehe „Drive Encryption for HP ProtectTools (bestimmte Modelle)“ auf Seite 45.
- Mithilfe der Verschlüsselung kann sichergestellt werden, dass auf Daten auch dann nicht zugegriffen werden kann, wenn die Festplatte entfernt und auf einem ungesichterten System installiert wird.
- Computrace kann die Position eines Computers nach einem Diebstahl feststellen.
    - Computrace for HP ProtectTools – Siehe „Theft recovery (select models only)Aero verwalten (bestimmte Modelle)“ auf Seite 66.

Beschränken des Zugriffs auf sensible Daten

Nehmen wir an, ein Vertragsprüfer arbeitet vor Ort und hat Zugriff auf den Computer zur Überprüfung sensibler Finanzdaten erhalten. Es soll ihm aber nicht möglich sein, die Dateien zu drucken oder auf eine CD zu kopieren. Die folgende Funktion schränkt den Zugriff auf die Daten ein:

- Device Access Manager for HP ProtectTools ermöglicht es IT-Managern, den Zugriff auf Kommunikationsgeräte einzuschränken, sodass sensible Informationen nicht von der Festplatte kopiert werden können. Siehe „Geräteklassen-Konfiguration“ auf Seite 56.

Verhindern von nicht autorisiertem internen oder externen Zugriff

Der nicht autorisierte Zugriff auf einen nicht gesicherten Unternehmenscomputer stellt ein großes Risiko für die Ressourcen im Unternehmensnetzwerk dar, wie beispielsweise für die Daten von Finanzdienstleistern, einer Behörde oder der Abteilung für Forschung & Entwicklung, sowie für

vertrauliche Informationen wie Patientendatensätze oder persönliche Finanzdaten. Mithilfe der folgenden Funktionen kann der nicht autorisierte Zugriff verhindert werden:

- Die Funktion zur Authentifizierung vor dem Systemstart verhindert den Zugriff auf das Betriebssystem.
  - Security Manager for HP ProtectTools – Siehe „HP ProtectTools Security Manager“ auf Seite 28.
  - Drive Encryption for HP ProtectTools – Siehe „Drive Encryption for HP ProtectTools (bestimmte Modelle)“ auf Seite 45.
- Mit Security Manager kann sichergestellt werden, dass nicht autorisierte Benutzer keine Kennwörter und keinen Zugriff auf kennwortgeschützte Anwendungen erhalten. Siehe „HP ProtectTools Security Manager“ auf Seite 28.
- Device Access Manager for HP ProtectTools ermöglicht es IT-Managern, den Zugriff auf Schreibgeräte einzuschränken, sodass sensible Daten nicht von der Festplatte kopiert werden können. Siehe „Device Access Manager for HP ProtectTools (bestimmte Modelle)“ auf Seite 54.

Erstellen von Richtlinien für starke Kennwörter

Wenn eine Unternehmensrichtlinie in Kraft tritt, welche die Verwendung von starken Kennwörtern für webbasierte Anwendungen und Datenbanken erforderlich macht, bietet Security Manager ein geschütztes Repository für Kennwörter und Single Sign-On. Siehe „HP ProtectTools Security Manager“ auf Seite 28.

Zusätzliche Sicherheitselemente

Zuweisen von Sicherheitsrollen

Bei der Computersicherheitsverwaltung (besonders bei größeren Unternehmen) ist es wichtig, die Verantwortung und Rechte auf die verschiedenen Administrator- und Benutzertypen aufzuteilen.

HINWEIS: In kleineren Unternehmen oder bei Einzelpersonen können all diese Rollen derselben Person zugeteilt sein.

Bei HP ProtectTools können die Sicherheitspflichten und Rechte auf die folgenden Rollen aufgeteilt werden:

- Sicherheitsbeauftragter – Definiert die Sicherheitsstufe für das Unternehmen oder Netzwerk und bestimmt die Sicherheitsfunktionen, die bereitgestellt werden sollen, zum Beispiel Drive Encryption.

  HINWEIS: Viele der HP ProtectTools Funktionen können vom Sicherheitsbeauftragten in Zusammenarbeit mit Hewlett-Packard angepasst werden. Weitere Informationen finden Sie unter http://www.hp.com.
- IT-Administrator – Wendet die vom Sicherheitsbeauftragten definierten Sicherheitsfunktionen an und verwaltet sie. Er kann auch einige Funktionen aktivieren oder deaktivieren. Wenn der Sicherheitsbeauftragte zum Beispiel entschieden hat, Smart Cards bereitzustellen, kann der IT-Administrator das Kennwort und den Smart Card-Modus aktivieren.
- Benutzer – Nutzt die Sicherheitsfunktionen. Wenn der Sicherheitsbeauftragte und der IT-Administrator zum Beispiel Smart Cards für das System aktiviert haben, kann der Benutzer die PIN für die Smart Card festlegen und die Karte zur Authentifizierung benutzen.

⚠ **ACHTUNG:** Administratoren sollten beim Beschränken der Endbenutzer-Berechtigungen und des Benutzerzugriffs auf „Best Practices“ zurückgreifen.

Nicht autorisierten Benutzern sollten keine administrativen Rechte gewährt werden.

Verwalten von Kennwörtern in HP ProtectTools

Die meisten Funktionen von HP ProtectTools Security Manager sind kennwortgesichert. In der folgenden Tabelle werden häufig verwendete Kennwörter, das Softwaremodul, in dem das Kennwort festgelegt wird, und die Kennwortfunktion aufgelistet.

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

Kennwörter in HP ProtectTools	In folgendem Modul festgelegt	Funktion
Windows Anmeldekennwort	Windows Systemsteuerung oder HP ProtectTools Security Manager	Kann zur manuellen Anmeldung und zur Authentifizierung verwendet werden, um Zugriff auf verschiedene Security Manager-Funktionen zu erhalten.
Sicherungs- und Wiederherstellungskennwort für Security Manager	Security Manager, durch Einzelbenutzer	Schützt den Zugriff auf die Sicherungs- und Wiederherstellungsdatei für Security Manager.
Smart Card-PIN	Credential Manager	Kann zur Mehrfach-Authentifizierung verwendet werden. Kann zur Windows Authentifizierung verwendet werden. Authentifiziert Benutzer von Drive Encryption, wenn die Smart Card ausgewählt wird.

Erstellen eines sicheren Kennworts

Beim Erstellen eines Kennworts müssen Sie zuerst alle durch das Programm festgelegten Spezifikationen beachten. Mithilfe der folgenden Hinweise können Sie starke Kennwörter erstellen und die Wahrscheinlichkeit verringern, dass Ihr Passwort bekannt wird.

- Verwenden Sie Kennwörter mit mehr als sechs Zeichen, idealerweise mit mehr als acht.
- Verwenden Sie Groß- und Kleinbuchstaben in Ihrem Kennwort.
- Wenn möglich, verwenden Sie eine Kombination aus alphanumerischen Zeichen, Sonderzeichen und Satzzeichen.
- Ersetzen Sie Buchstaben durch Zahlen oder Sonderzeichen. Verwenden Sie beispielsweise die Zahl 1 für die Buchstaben I oder L.
- Kombinieren Sie Wörter aus zwei oder mehreren Fremdsprachen.
- Fügen Sie in der Mitte eines Wortes oder Ausdrucks Ziffern oder Sonderzeichen ein, wie in diesem Beispiel: „Mary2-2Cat45“.
- Verwenden Sie kein Kennwort, das in derselben Form in einem Wörterbuch zu finden ist.

- Benutzen Sie für das Kennwort weder Ihren Namen noch andere persönliche Informationen wie Ihr Geburtsdatum, Namen von Haustieren, Mädchenname der Mutter usw., auch nicht rückwärts geschrieben.
- Ändern Sie Ihre Kennwörter regelmäßig. Dabei können Sie auch nur ein paar Zeichen ändern.
- Wenn Sie ein Kennwort aufschreiben, bewahren Sie die Notiz nicht an einem leicht einsehbaren Platz in der Nähe des Computers auf.
- Speichern Sie das Kennwort nicht in einer Datei (z. B. E-Mail) auf dem Computer.
- Teilen Sie Benutzerkonten nicht mit anderen Personen, und geben Sie Ihr Kennwort niemandem weiter.

Sichern von Anmeldeinformationen und Einstellungen

Sie können Anmeldeinformationen auf folgende Arten sichern:

- Verwenden Sie Drive Encryption for HP ProtectTools, um HP ProtectTools Anmeldeinformationen auszuwählen und zu sichern.
- Verwenden Sie die Funktion zum Sichern und Wiederherstellen in HP ProtectTools Security Manager als zentralen Speicherort, von dem aus Sie Sicherheits-Anmeldeinformationen von einigen der installierten Module von HP ProtectTools sichern und wiederherstellen können.

2 Einführung

Zum Konfigurieren von Einstellungen für HP ProtectTools verwenden Sie den Installations-Assistent für HP Client Security oder den Installations-Assistent für HP ProtectTools Security Manager.

Nachdem Sie den Installations-Assistent für HP Client Security beendet haben, wird der Anwendungsstatus im HP Client Security Dashboard angezeigt.

Installations-Assistent für HP Client Security

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

Der Installations-Assistent für HP Client Security führt Sie durch die Einrichtung der am häufigsten genutzten Funktionen von Security Manager. Wenn Sie den Installations-Assistent für HP Client Security bisher noch nicht aufgerufen haben, können Sie ihn auf eine der folgenden Arten starten:

- Klicken oder tippen Sie auf dem Startbildschirm auf die Anwendung **HP Client Security**.

  – oder –

  Klicken oder tippen Sie auf dem Windows Desktop auf das Gadget **HP ProtectTools**.

Die Seiten des Assistenten werden in der folgenden Reihenfolge angezeigt:

1. **Windows Kennwort** – Geben Sie Ihre Windows Kennwort ein.

   So schützen Sie Ihre Windows Benutzerkonto mit starker Authentifizierung.

2. **SpareKey** – Um die SpareKey-Option zu aktivieren, wählen Sie drei Sicherheitsfragen aus.

3. **Fingerabdrücke registrieren** – Wenn ein Fingerabdruck-Lesegerät und der zugehörige Treiber installiert sind, können Sie Fingerabdrücke registrieren. Sie müssen mindesten zwei Fingerabdrücke auswählen und registrieren.

4. **Drive Encryption** – Wenn Drive Encryption for HP ProtectTools installiert ist, können Sie die Verschlüsselung für das primäre Laufwerk aktivieren:

   - Software-basierte Verschlüsselung für ein herkömmliches Festplattenlaufwerk
   - Hardware-basierte Verschlüsselung, sofern ein selbstverschlüsselndes Laufwerk erkannt wird

   Vor Aktivierung der Verschlüsselung müssen Sie einen Verschlüsselungsschlüssel unter Verwendung einer der beiden folgenden Optionen speichern:

HINWEIS: Wenn Sie die Ausführung des Assistenten zu diesem Zeitpunkt abbrechen, werden Sie nicht der Lage sein, die Windows Authentifizierung und die Authentifizierung auf Drive Encryption-Ebene zu aktivierenn.

- **Wechselmedien**, zum Beispiel ein mit FAT32 formatierters USB-Flash-Laufwerk.
  - Diese Option ist standardmäßig ausgewählt, wenn vor dem Anzeigen der Seite „Drive Encryption“ ein einzelnes Wechselmediengerät erkannt wurde.
  - Wenn mehrere Wechselmediengeräte erkannt wurden, wählen Sie eines der angezeigten Laufwerke aus.
- **SkyDrive** – Diese Option ist verfügbar, wenn eine bestehende Internetverbindung erkannt wurde.

  In diesem Fall ist eine Windows® Live ID erforderlich. Geben Sie Ihre ID und Ihr Kennwort ein, oder melden Sie sich an, um entsprechende Daten zugeteilt zu bekommen.

5. Auf der Seite „Fertig stellen“ wird eine Meldung über den erfolgreichen Abschluss des Assistenten angezeigt. Außerdem werden Sie zum Neustart des Systems aufgefordert, um Drive Encryption zu aktivieren.

Installations-Assistent für HP ProtectTools Security Manager

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

Der Installations-Assistent für HP ProtectTools Security Manager führt Sie durch die Einrichtung der Funktionen von HP ProtectTools Security Manager. Außer den Einstellungen im Assistenten können Administatoren zahlreiche zusätzliche Funktionen über die Administrator-Konsole konfigurieren. Diese Einstellungen gelten für den Computer und alle Benutzer, die den Computer verwenden.

So starten Sie den Installations-Assistent für HP ProtectTools Security Manager:

▲ Klicken Sie im linken Bereich der Administrator-Konsole auf **Installations-Assistent**, und befolgen Sie dann die Anweisungen auf dem Bildschirm bis zum Abschluss der Installation.

Administratoren können die Administrator-Konsole von der HP ProtectTools Security Manager Benutzer-Konsole aus starten. Weitere Informationen finden Sie unter „HP ProtectTools Security Manager Administrator-Konsole“ auf Seite 16.

Security Manager und die zugehörigen Anwendungen stehen allen Benutzern des Computers zur Verfügung.

HP Client Security Dashboard

So öffnen Sie HP Client Security, wenn Sie zuvor den Installations-Assistent für HP Client Security vollständig ausgeführt haben:

▲ Geben Sie auf dem Startbildschirm `hp` ein, und wählen Sie **HP Client Security** aus.

Das Dashboard bietet einen raschen Überblick über Funktionen und den Status aller Anwendungen.

▲ Klicken oder tippen Sie auf eine Anwendungszeile, um mehr Informationen zur ausgewählten Anwendung anzuzeigen.

- Die Schaltfläche **Jetzt konfigurieren** verweist darauf, dass eine Anwendung noch nicht konfiguriert ist. Klicken oder tippen Sie auf die Schaltfläche, um die Anwendungsseite zu öffnen und die Anwendung zu konfigurieren.
- Die Schaltfläche **Einstellungen** verweist auf eine ordnungsgemäß konfigurierte Anwendung. Klicken oder tippen Sie auf die Schaltfläche, um auf die Einstellungen für die Anwendung zuzugreifen.
- Die **Benutzer-Konsole** wird für eine Benutzerkonfiguration gestartet.
- Die **Administrator-Konsole** wird für eine Konfiguration gestartet, die Administratorberechtigungen erfordert.
- Das **Status-Dashboard** bleibt auch nach dem Starten der Benutzer- oder Administrator-Konsole geöffnet. Sobald Sie Einstellungen konfiguriert und die Konsole geschlossen haben, wird der Status im Dashboard aktualisiert.

3 Small Business – Kurzanleitung zur Einrichtung

Dieses Kapitel beschreibt die grundlegenden Schritte zur Aktivierung der häufigsten und hilfreichsten Optionen in HP ProtectTools for Small Business. Diese Software bietet eine Reihe von Tools und Optionen, die Ihnen eine Feinabstimmung der Voreinstellungen sowie Zugriffskontrolle ermöglichen. Diese Kurzanleitung zur Einrichtung dient dazu, jedes Modul mit einem möglichst geringen Zeit- und Arbeitsaufwand einzurichten und auszuführen. Wählen Sie für weitere Informationen das jeweilige Modul aus, und klicken Sie in der oberen rechten Ecke auf **?** oder auf die Schaltfläche für die Hilfe. Mithilfe dieser Schaltfläche erhalten Sie automatisch Informationen für das aktuell angezeigte Fenster.

Erste Schritte

1. Öffnen Sie HP ProtectTools Security Manager, indem Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools** doppelklicken.
2. Geben Sie Ihr Windows Kennwort ein, oder erstellen Sie ein Windows Kennwort.
3. Schließen Sie den Installationsassistenten ab.

HINWEIS: HP ProtectTools Security Manager ist standardmäßig für die starke Authentifizierung konfiguriert.

Diese Einstellung verhindert nicht autorisierten Zugriff, während Sie bei Windows angemeldet sind. Sie sollte verwendet werden, wenn ein hohes Maß an Sicherheit erforderlich ist, oder wenn Benutzer mehrmals täglich ihren Platz verlassen. Wenn Sie diese Einstellung ändern möchten, klicken Sie auf die Registerkarte „Sitzungsrichtlinie“, und nehmen Sie Ihre Auswahl vor.

Gehen Sie wie folgt vor, um HP ProtectTools Security Manager für die einmalige Authentifizierung während der Anmeldung bei Windows zu konfigurieren.

1. Öffnen Sie HP ProtectTools Security Manager, indem Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools** doppelklicken.
2. Klicken Sie im linken Bereich auf **Verwaltung** und anschließend auf **Administrator-Konsole**.
3. Wählen Sie im linken Bereich unter **System** die Option **Authentifizierung** aus der Gruppe **Sicherheit** aus.
4. Klicken Sie auf die Registerkarte **Sitzungsrichtlinie**, und wählen Sie die für die Sitzung erforderliche Anmeldeanforderungen aus. Um diese Auswahl rückgängig zu machen, klicken Sie auf **Standardeinstellungen wiederherstellen**.
5. Klicken Sie auf die Schaltfläche **Übernehmen**, wenn der Vorgang abgeschlossen ist.

Password Manager

Kennwörter! Wir alle haben eine ganze Reihe von ihnen, insbesondere, wenn wir regelmäßig auf Websites zugreifen oder Anwendungen benutzen, die eine Anmeldung erfordern. Der normale

Benutzer verwendet entweder dasselbe Kennwort für jede Anwendung und Website oder wird tatsächlich kreativ und vergisst prompt, welches Kennwort für welche Anwendung gilt.

Password Manager kann die Erinnerung der Kennwörter für Sie automatisieren oder Sie in die Lage versetzen, zwischen wichtigen Sites, für die Anmeldedaten verfügbar sein müssen, und unwichtigen Sites, für die das nicht gilt, zu unterscheiden. Sobald Sie sich am Computer anmelden, stellt Password Manager Ihre Kennwörter oder Anmeldeinformationen für ausgewählte Anwendungen oder Websites bereit.

Wenn Sie auf eine Anwendung oder Website zugreifen, die Anmeldeinformationen erfordert, erkennt Password Manager die Website automatisch und fordert Sie auf anzugeben, ob die Anmeldeinformationen von der Software gespeichert werden sollen. Wenn Sie bestimmte Websites ausschließen möchten, können Sie die Anfrage ablehnen.

So speichern Sie Websites, Benutzernamen und Kennwörter:

1. Navigieren Sie beispielsweise zu einer Website oder Anwendung, und klicken Sie dann auf das Password Manager-Symbol in der oberen linken Ecke der Webseite, um die Daten für die Webauthentifizierung hinzuzufügen.
2. Benennen Sie den Link (optional), und geben Sie einen Benutzernamen und ein Kennwort in Password Manager ein.

HINWEIS: Die Bereiche, die Password Manager aktuell und für künftige Besuche verwenden wird, werden hervorgehoben.

3. Klicken Sie auf die Schaltfläche **OK**, wenn der Vorgang abgeschlossen ist.
4. Password Manager kann auch Ihren Benutzernamen und Kennwörter für Netzwerkfreigaben oder zugeordnete Netzwerklaufwerke speichern

Anzeigen und Verwalten von gespeicherten Authentifizierungen in Password Manager

Password Manager ermöglicht das Anzeigen, Verwalten, Sichern und Starten Ihrer Authentifizierungen von einem zentralen Speicherort aus. Password Manager unterstützt außerdem das Starten von gespeicherten Websites von Windows aus.

Verwenden Sie zum Öffnen von Password Manager eine der beiden folgenden Optionen:

- Verwenden Sie die Tastenkombination strg+Windows Logo-Taste+h, um Password Manager zu öffnen. Klicken Sie danach auf **Öffnen**, um die gespeicherte Verknüpfung zu starten und zu authentifizieren.

  – oder –

- Klicken Sie in Password Manager auf die Registerkarte **Verwalten**, um HP ProtectTools Security Manager für die Bearbeitung der Anmeldeinformationen zu öffnen.

Die Password Manager-Optionen zum **Bearbeiten** ermöglichen es Ihnen, den Namen und den Anmeldenamen anzuzeigen und zu ändern und sogar die Kennwörter offenzulegen.

Mit HP ProtectTools for Small Business können alle Anmeldedaten und Einstellungen auf einem anderen Computer gesichert bzw. auf diesen kopiert werden.

Device Access Manager for HP ProtectTools

Device Access Manager bietet die Möglichkeit, die Verwendung von diversen internen und externen Speichergeräten einzuschränken. So kann sichergestellt werden, dass die Daten Ihr Unternehmen nicht verlassen und sicher auf der Festplatte bleiben. So kann ein Benutzer beispielsweise Zugriff auf

Ihre Daten haben, sie jedoch nicht auf eine CD, einen MP3-Player oder ein USB-Speichergerät kopieren. Im Folgenden wird erläutert, wie Sie dies einrichten können.

1. Öffnen Sie die HP ProtectTools Security Manager Benutzer-Konsole, indem Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools** doppelklicken.
2. Klicken Sie im linken Bereich von HP ProtectTools Security Manager auf **Verwaltung** und anschließend auf **Administrator-Konsole**.
3. Klicken Sie auf **Device Access Manager** und dann auf **Geräteklassen-Konfiguration**.
4. Im nächsten Schritt können Sie auswählen, wer weiterhin Zugriff hat, während der Zugriff für alle anderen gesperrt wird.
5. Wählen Sie die Hardwaregeräte aus, die Sie einschränken möchten, und klicken Sie dann auf die Schaltfläche **Übernehmen**, um den Vorgang abzuschließen.
6. Wählen Sie **Hinzufügen** aus, klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**.
7. Wählen Sie den gewünschten Benutzer aus, und klicken Sie auf **OK > OK > Übernehmen**.

   Ihre Auswahl wird im Feld **Benutzer/Gruppen** angezeigt.
8. Wählen Sie die **Geräteklasse** aus, die der Benutzer verwenden soll, wählen Sie **Erlauben** oder **Verweigern** aus,. und klicken Sie auf **Übernehmen**.

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools schützt Ihre Daten durch Verschlüsselung der gesamten Festplatte. Die Daten auf der Festplatte bleiben auch dann geschützt, wenn der PC gestohlen und/oder die Festplatte aus dem Originalcomputer entfernt und in einen anderen Computer eingebaut wird.

Ein zusätzlicher Sicherheitsvorteil ist, dass Sie von Drive Encryption gezwungen werden, sich vor dem Starten des Betriebssystems ordnungsgemäß unter Verwendung Ihres Benutzernamens und Ihres Kennworts zu authentifizieren. Dieser Vorgang wird „Authentifizierung vor dem Systemstart“ genannt.

Um diesen Vorgang zu vereinfachen, werden die Kennwörter von mehreren Softwaremodulen automatisch synchronisiert, z. B. für Windows Benutzerkonten, Domänen, Drive Encryption for HP ProtectTools, Password Manager und HP ProtectTools Security Manager.

Gehen Sie folgendermaßen vor, um Drive Encryption for HP ProtectTools problemlos zu aktivieren:

1. Öffnen Sie HP ProtectTools Security Manager, indem Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools** doppelklicken.
2. Klicken Sie im linken Bereich auf **Verwaltung** und anschließend auf **Administrator-Konsole**.
3. Klicken Sie im linken Fensterausschnitt auf **Installations-Assistent**.
4. Wählen Sie im Startbildschirm **Weiter** aus.
5. Geben Sie Ihr Windows Kennwort ein, um den Aktivierungsassistenten zu starten, und klicken Sie dann auf **Weiter**.
6. Überspringen Sie SpareKey, wenn er nicht erwünscht ist.
7. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.

8. Aktivieren Sie das Kontrollkästchen für die Festplatte, die verschlüsselt werden soll, und klicken Sie dann auf **Weiter**.

9. Das Konfigurationsfenster von Drive Encryption benötigt für die Speicherung des Wiederherstellungsschlüssels ein USB-Flash-Laufwerk oder ein anderes externes Gerät. Bewahren Sie diesen Wiederherstellungsschlüssel sicher auf, da er bei Verlust des für die Authentifizierung vor dem Systemstart erforderlichen Kennworts zur Wiederherstellung von Daten oder für Wiederherstellungsschlüsselden Zugriff auf das Laufwerk verwendet wird.

10. Klicken Sie auf **Weiter**, schließen Sie den Vorgang ab, und klicken Sie dann auf **Fertig stellen**. Entfernen Sie das USB-Flash-Laufwerk, und starten Sie danach den Computer neu.

11. Beim Systemstart werden Sie von Drive Encription aufgefordert, Ihr Windows Kennwort einzugeben. Geben Sie das Kennwort ein, und klicken Sie anschließend auf **OK**.

HINWEIS: Der Computer scheint während der Laufwerkverschlüsselung langsamer zu werden. Sobald die Verschlüsselung abgeschlossen ist, kehrt jedoch die normale Leistung zurück. Bei jedem Zugriff auf Daten, die sich auf dem Laufwerk befinden, werden diese gemäß den Vorgaben des Administrators ver- oder entschlüsselt.

Die Drive Encryption-Authentifizierung reicht das Ergebnis über die Windows Anmeldung direkt zum Windows Desktop weiter, so dass Sie Ihr Kennwort nicht zweimal eingeben müssen.

4 HP ProtectTools Security Manager Administrator-Konsole

Die HP ProtectTools Security Manager Software bietet Sicherheitsfunktionen, die den Computer, Netzwerke und wichtige Daten vor unberechtigtem Zugriff schützen. Die Verwaltung von HP ProtectTools Security Manager erfolgt über die Administrator-Konsole.

In der Security Manager Benutzer-Konsole sind zusätzliche Anwendungen verfügbar (nur bei bestimmten Modellen), die Ihnen bei der Wiedererlangung des Computers helfen, falls dieser verloren geht oder gestohlen wird.

Mithilfe der Administrator-Konsole kann der lokale Administrator die folgenden Aufgaben ausführen:

- Aktivieren oder Deaktivieren von Sicherheitsfunktionen
- Festlegen von erforderlichen Anmeldeinformationen zur Authentifizierung
- Verwalten der Benutzer des Computers
- Anpassen gerätespezifischer Parameter
- Konfigurieren installierter Security Manager Anwendungen

Erste Schritte

Zum Konfigurieren von Einstellungen für HP ProtectTools verwenden Sie den Installations-Assistent für HP Client Security oder den Installations-Assistent für HP ProtectTools Security Manager.

Nachdem Sie den Installations-Assistent für HP Client Security beendet haben, wird der Anwendungsstatus im HP Client Security Dashboard angezeigt.

Installations-Assistent für HP Client Security

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

Der Installations-Assistent für HP Client Security führt Sie durch die Einrichtung der am häufigsten genutzten Funktionen von Security Manager. Wenn Sie den Installations-Assistent für HP Client Security bisher noch nicht aufgerufen haben, können Sie ihn auf eine der folgenden Arten starten:

▲ Klicken oder tippen Sie auf dem Startbildschirm auf die Anwendung **HP Client Security**.

– oder –

Klicken oder tippen Sie auf dem Windows Desktop auf das Gadget **HP ProtectTools**.

Die Seiten des Assistenten werden in der folgenden Reihenfolge angezeigt:

1. **Windows Kennwort** – Geben Sie Ihre Windows Kennwort ein.

   So schützen Sie Ihre Windows Benutzerkonto mit starker Authentifizierung.

2. **SpareKey** – Um die SpareKey-Option zu aktivieren, wählen Sie drei Sicherheitsfragen aus.

3. **Fingerabdrücke registrieren** – Wenn ein Fingerabdruck-Lesegerät und der zugehörige Treiber installiert sind, können Sie Fingerabdrücke registrieren. Sie müssen mindesten zwei Fingerabdrücke auswählen und registrieren.

4. **Drive Encryption** – Wenn Drive Encryption for HP ProtectTools installiert ist, können Sie die Verschlüsselung für das primäre Laufwerk aktivieren:

   - Software-basierte Verschlüsselung für ein herkömmliches Festplattenlaufwerk
   - Hardware-basierte Verschlüsselung, sofern ein selbstverschlüsselndes Laufwerk erkannt wird

   Vor Aktivierung der Verschlüsselung müssen Sie einen Verschlüsselungsschlüssel unter Verwendung einer der beiden folgenden Optionen speichern:

   HINWEIS: Wenn Sie die Ausführung des Assistenten zu diesem Zeitpunkt abbrechen, werden Sie nicht der Lage sein, die Windows Authentifizierung und die Authentifizierung auf Drive Encryption-Ebene zu aktivierenn.

   - **Wechselmedien**, zum Beispiel ein mit FAT32 formatierters USB-Flash-Laufwerk.
     - Diese Option ist standardmäßig ausgewählt, wenn vor dem Anzeigen der Seite „Drive Encryption“ ein einzelnes Wechselmediengerät erkannt wurde.
     - Wenn mehrere Wechselmediengeräte erkannt wurden, wählen Sie eines der angezeigten Laufwerke aus.
   - **SkyDrive** – Diese Option ist verfügbar, wenn eine bestehende Internetverbindung erkannt wurde.

     In diesem Fall ist eine Windows® Live ID erforderlich. Geben Sie Ihre ID und Ihr Kennwort ein, oder melden Sie sich an, um entsprechende Daten zugeteilt zu bekommen.

5. Auf der Seite „Fertig stellen“ wird eine Meldung über den erfolgreichen Abschluss des Assistenten angezeigt. Außerdem werden Sie zum Neustart des Systems aufgefordert, um Drive Encryption zu aktivieren.

Installations-Assistent für HP ProtectTools Security Manager

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

Der Installations-Assistent für HP ProtectTools Security Manager führt Sie durch die Einrichtung der Funktionen von HP ProtectTools Security Manager. Außer den Einstellungen im Assistenten können Administatoren zahlreiche zusätzliche Funktionen über die Administrator-Konsole konfigurieren. Diese Einstellungen gelten für den Computer und alle Benutzer, die den Computer verwenden.

So starten Sie den Installations-Assistent für HP ProtectTools Security Manager:

▲ Klicken Sie im linken Bereich der Administrator-Konsole auf **Installations-Assistent**, und befolgen Sie dann die Anweisungen auf dem Bildschirm bis zum Abschluss der Installation.

Administratoren können die Administrator-Konsole von der HP ProtectTools Security Manager Benutzer-Konsole aus starten. Weitere Informationen finden Sie unter „HP ProtectTools Security Manager Administrator-Konsole“ auf Seite 16.

Security Manager und die zugehörigen Anwendungen stehen allen Benutzern des Computers zur Verfügung.

HP Client Security Dashboard

So öffnen Sie HP Client Security, wenn Sie zuvor den Installations-Assistent für HP Client Security vollständig ausgeführt haben:

▲ Geben Sie auf dem Startbildschirm `hp` ein, und wählen Sie **HP Client Security** aus.

Das Dashboard bietet einen raschen Überblick über Funktionen und den Status aller Anwendungen.

▲ Klicken oder tippen Sie auf eine Anwendungszeile, um mehr Informationen zur ausgewählten Anwendung anzuzeigen.

- Die Schaltfläche **Jetzt konfigurieren** verweist darauf, dass eine Anwendung noch nicht konfiguriert ist. Klicken oder tippen Sie auf die Schaltfläche, um die Anwendungsseite zu öffnen und die Anwendung zu konfigurieren.
- Die Schaltfläche **Einstellungen** verweist auf eine ordnungsgemäß konfigurierte Anwendung. Klicken oder tippen Sie auf die Schaltfläche, um auf die Einstellungen für die Anwendung zuzugreifen.
- Die **Benutzer-Konsole** wird für eine Benutzerkonfiguration gestartet.
- Die **Administrator-Konsole** wird für eine Konfiguration gestartet, die Administratorberechtigungen erfordert.
- Das **Status-Dashboard** bleibt auch nach dem Starten der Benutzer- oder Administrator-Konsole geöffnet. Sobald Sie Einstellungen konfiguriert und die Konsole geschlossen haben, wird der Status im Dashboard aktualisiert.

Öffnen der HP ProtectTools Administrator-Konsole

Verwenden Sie die HP ProtectTools Administrator-Konsole für administrative Aufgaben wie das Festlegen von Systemrichtlinien oder das Konfigurieren von Software. Der Zugriff auf die Administrator-Konsole erfolgt über HP ProtectTools Security Manager:

1. Doppelklicken Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools**.

   – oder –

   Klicken Sie in der **Systemsteuerung** auf **System und Sicherheit**, und wählen Sie **HP ProtectTools Security Manager** aus.

2. Klicken Sie im linken Bereich der Security Manager Benutzer-Konsole auf **Verwaltung** und anschließend auf **Administrator-Konsole**.

Verwenden der Administrator-Konsole

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

1. Doppelklicken Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools**.

   – oder –

   Klicken Sie in der **Systemsteuerung** auf **System und Sicherheit**, und wählen Sie **HP ProtectTools Security Manager** aus.

2. Klicken Sie im linken Bereich der Security Manager Benutzer-Konsole auf **Verwaltung** und anschließend auf **Administrator-Konsole**.

Auf der linken Seite der Administrator-Konsole werden unter „Startseite“ folgende Auswahlmöglichkeiten angezeigt:

- **System** – Ermöglicht mithilfe der folgenden Optionen die Konfiguration von Sicherheits- und Authentifizierungseinstellungen für Benutzer und Geräte.
  - **Sicherheit**
  - **Benutzer**
  - **Anmeldeinformationen**
- **Anwendungen** – Ermöglicht die Konfiguration der Einstellungen für HP ProtectTools Security Manager und für Security Manager-Anwendungen.
- **Daten** – Ermöglicht die Konfiguration von Einstellungen für Drive Encryption (nur bei bestimmten Modellen).
- **Computer** – Ermöglicht die Konfiguration von Einstellungen für Device Access Manager.
- **Installations-Assistent** – Führt Sie durch die Einrichtung von HP ProtectTools Security Manager.
- **Info** – Zeigt Informationen zu HP ProtectTools Security Manager, wie etwa Versionsnummer und Copyright-Hinweis, an.
- **Hauptbereich** – Zeigt anwendungsspezifische Inhalte an.

  ? – Zeigt die Hilfe zur Administrator-Konsole an. Das Hilfe-Symbol befindet sich rechts oben im Fensterrahmen neben den Symbolen für die Minimierung und Maximierung der Fensteranzeige.

Konfigurieren des Systems

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

Die folgenden Anwendungen sind in der Gruppe **System** enthalten:

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

Einrichten der Authentifizierung für Ihren Computer

In der Authentifizierungsanwendung können Sie Richtlinien für den Zugriff auf den Computer festlegen. Sie können Anmeldeinformationen festlegen, die für die Authentifizierung jeder Benutzerklasse für die Anmeldung bei Windows oder auf Websites und Programmen während einer Benutzersitzung benötigt werden.

So richten Sie eine Authentifizierung auf Ihrem Computer ein:

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Authentifizierung**.
2. Zur Konfiguration der Anmeldeauthentifizierung klicken Sie auf die Registerkarte **Anmelderichtlinie**, nehmen die Änderungen vor und klicken dann auf **Übernehmen**.
3. Zur Konfiguration der Sitzungsauthentifizierung klicken Sie auf die Registerkarte **Sitzungsrichtlinie**, nehmen die Änderungen vor und klicken dann auf **Übernehmen**.

Anmelderichtlinie

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

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Authentifizierung**.
2. Wählen Sie auf der Registerkarte **Anmelderichtlinie** eine Benutzerkategorie, wie zum Beispiel Administratoren oder Standardbenutzer, aus.
3. Klicken Sie auf eine Anmeldeinformation, um das Dialogfeld zur Bearbeitung der Information zu öffnen.
4. Wenn Sie eine Kombination von zwei Anmeldeinformationen zur Authentifizierung aktivieren möchten, klicken Sie auf den Pfeil nach unten, um die jeweiligen Anmeldeinformationen auszuwählen, und anschließend auf **OK**.
5. Klicken Sie auf **X**, um eine Anmeldeinformation zu entfernen, oder klicken Sie mit der rechten Maustaste auf die jeweilige Anmeldeinformation und anschließend auf **Löschen**.
6. Klicken Sie im Konfigurationsdialogfeld auf **Ja**.
7. Um festzustellen, ob sich Benutzer anmelden können, klicken Sie auf **Prüfen, ob die Anmeldung über HP ProtectTools möglich ist**.
8. Zum Wiederherstellen der ursprünglichen Einstellungen klicken Sie auf **Standardeinstellungen wiederherstellen**.
9. Klicken Sie auf **Übernehmen**.

Sitzungsrichtlinie

So legen Sie Richtlinien fest, die regulieren, welche Anmeldedaten zur Authentifizierung während einer Windows Sitzung erforderlich sind:

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Authentifizierung**.
2. Wählen Sie auf der Registerkarte **Sitzungsrichtlinie** eine Benutzerkategorie, wie zum Beispiel Administratoren oder Standardbenutzer, aus.
3. Klicken Sie auf eine Anmeldeinformation, um das Dialogfeld zur Bearbeitung der Information zu öffnen.

4. Wenn Sie eine Kombination von zwei Anmeldeinformationen zur Authentifizierung aktivieren möchten, klicken Sie auf den Pfeil nach unten, um die jeweiligen Anmeldeinformationen auszuwählen, und anschließend auf **OK**.
5. Klicken Sie auf **X**, um eine Anmeldeinformation zu entfernen, oder klicken Sie mit der rechten Maustaste auf die jeweilige Anmeldeinformation und anschließend auf **Löschen**.
6. Klicken Sie im Konfigurationsdialogfeld auf **Ja**.
7. Um festzustellen, ob sich Benutzer anmelden können, klicken Sie auf **Prüfen, ob die Anmeldung über HP ProtectTools möglich ist**.
8. Zum Wiederherstellen der ursprünglichen Einstellungen klicken Sie auf **Standardeinstellungen wiederherstellen**.
9. Klicken Sie auf **Übernehmen**.

Einstellungen

So ermöglichen Sie es Benutzern dieses Computers, die Windows Anmeldung zu überspringen, wenn die Authentifizierung auf der Ebene von BIOS oder Drive Encryption bereits erfolgt ist:

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Einstellungen**.
2. **One Step-Anmeldung zulassen** – Verwenden Sie zum Aktivieren oder Deaktivieren der One Step-Anmeldung dieses Kontrollkästchen.
3. Klicken Sie auf **Übernehmen**.

Verwalten von Benutzern

In der Anwendung „Benutzer“ können Sie die HP ProtectTools Benutzer dieses Computers überwachen und verwalten.

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

Zum Verwalten von Benutzern wählen Sie die folgenden Einstellungen aus:

- Um weitere Benutzer hinzuzufügen, klicken Sie auf **Hinzufügen**.
- Um einen Benutzer zu löschen, klicken Sie auf den Benutzer und danach auf **Löschen**.
- Um zusätzliche Anmeldeinformationen für den Benutzer einzurichten, klicken Sie auf **Registrieren**.
- Um die Richtlinien für einen bestimmten Benutzer anzuzeigen, wählen Sie den Benutzer aus. Die Richtlinien werden dann im unteren Fenster angezeigt.

Anmeldeinformationen

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

SpareKey

Sie können einstellen, ob Sie die SpareKey-Authentifizierung für die Windows Anmeldung zulassen möchten oder nicht, und die Sicherheitsfragen verwalten, die den Benutzern bei der SpareKey-Anmeldung gestellt werden.

1. Wählen Sie die Sicherheitsfragen aus, die den Benutzern bei der SpareKey-Anmeldung gestellt werden.

   Sie können bis zu drei benutzerdefinierte Fragen angeben, oder Sie können Benutzern die Möglichkeit einräumen, ihre eigene Passphrase einzugeben.

2. Aktivieren Sie das entsprechende Kontrollkästchen, um die Sicherung von SpareKey für die Windows Anmeldung zuzulassen.

3. Klicken Sie auf **Übernehmen**.

Fingerabdrücke

Wenn der Computer über ein integriertes oder angeschlossenes Fingerabdruck-Lesegerät verfügt, werden auf der Seite „Fingerabdrücke“ folgende Registerkarten angezeigt:

- **Registrierung** – Wählen Sie die Mindest- und die Maximalanzahl an Fingerabdrücken, die ein Benutzer registrieren kann, aus.

  Sie können ebenfalls alle Daten vom Fingerabdruck-Lesegerät löschen.

  ACHTUNG: Wenn Sie alle Daten aus dem Fingerabduck-Lesegerät löschen, werden die Fingerabdruckdaten aller Benutzer gelöscht, einschließlich des Administrators. Falls die Anmelderichtlinie nur die Authentifizierung per Fingerabdruck vorsieht, kann dies dazu führen, dass sich keiner der Benutzer mehr an diesem Computer anmelden kann.

- **Empfindlichkeit** – Bewegen Sie den Schieberegler, um die Empfindlichkeit anzupassen, mit der Fingerabdrücke beim Streichen über den Sensor vom Fingerabdruck-Lesegerät erkannt werden.

  Wenn Ihr Fingerabdruck nicht konsistent erkannt wird, müssen Sie ggf. die Empfindlichkeit vermindern. Eine höhere Einstellung erhöht die Empfindlichkeit für Abweichungen bei der Registrierung von Fingerabdrücken durch Streichen über den Sensor und verringert dadurch die Möglichkeit eines fälschlicherweise zugelassenen Zugriffs. Die Einstellung **Mittel-hoch** bietet eine gute Mischung aus Sicherheit und Komfort.

- **Erweitert** – Wählen Sie eine der folgenden Optionen aus, um das Fingerabdruck-Lesegerät so zu konfigurieren, dass Strom gespart und das visuelle Feedback verbessert wird:

  - **Optimiert** – Das Fingerabdruck-Lesegerät wird aktiviert, wenn es benötigt wird. Bei der ersten Verwendung des Geräts kann es zu einer leichten Verzögerung kommen.
  - **Geringer Stromverbrauch** – Das Fingerabdruck-Lesegerät reagiert langsamer, bei dieser Einstellung wird jedoch deutlich weniger Strom benötigt.
  - **Normaler Stromverbrauch** – Das Fingerabdruck-Lesegerät ist jederzeit einsatzbereit, bei dieser Einstellung wird jedoch am meisten Strom benötigt.

Gesicht

Wenn der Computer über eine integrierte oder angeschlossene Webcam verfügt, und wenn das Gesichtserkennungsprogramm installiert ist, können Administratorene die Sicherheitsstufe für die

Gesichtserkennung so einstellen, dass ein Gleichgewicht zwischen Nutzungskomfort und Computersicherheit hergestellt wird.

1. Klicken Sie auf **Anmeldeinformationen** und dann auf **Gesicht**.
2. Für mehr Komfort bewegen Sie den Schieberegler nach links, für mehr Genauigkeit bewegen Sie den Schieberegler nach rechts.
   - **Komfort** – Um registrierten Benutzern den Zugriff in Grenzsituationen zu erleichtern, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Komfort**.
   - **Balance** – Um ein gutes Gleichgewicht zwischen Sicherheit und Komfort herzustellen, oder wenn auf dem Computer kritische Informationen gespeichert sind bzw. sich der Computer in einer Umgebung befindet, in der unberechtigte Anmeldeversuche möglich sind, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Balance**.
   - **Genauigkeit** – Um den Zugriff für Benutzer zu erschweren, wenn die registrierten Szenen oder aktuellen Lichtbedingungen unter dem Normalwert liegen und fälschlicherweise zugelassene Zugriffe möglich sind, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Genauigkeit**.
3. Um die Einstellungen auf die ursprünglichen Werte zurückzusetzen, klicken Sie auf **Standardeinstellungen wiederherstellen**.
4. Klicken Sie auf **Übernehmen**.

Smart Card

Administratoren müssen die Smart Card initialisieren, bevor sie für die Authentifizierung verwendet werden kann. Die meisten standardmäßigen CSP- und PKCS11-Smart Cards werden von Windows unterstützt.

Initialisieren der Smart Card

HP ProtectTools Security Manager kann eine Reihe verschiedener Smart Cards unterstützen. Die Anzahl und Art der Zeichen, die für die PIN verwendet werden, können variieren. Der Hersteller der Smart Card stellt normalerweise Tools für die Installation eines Sicherheitszertifikats und einer Verwaltungs-PIN bereit, die HP ProtectTools in seinem Sicherheitsalgorithmus verwendet.

HINWEIS: Smart Card Middleware muss installiert werden.

1. Installieren Sie Middleware für die verwendete Smart Card (z. B. ActivClient 6.x für eine ActivIdentity Smart Card).
2. Führen Sie die Smart Card in das Lesegerät ein.
3. Initialisieren (formatieren) Sie die Smart Card.
   a. Starten Sie das Initialisierungstool für die Smart Card. Das Tool wird möglicherweise auch angezeigt, wenn Sie die Smart Card in das Lesegerät einführen.
   b. Folgen Sie den Anleitungen auf dem Bildschirm, um eine PIN einzurichten.
   c. Notieren Sie sich den Entsperrungscode für später.
4. Erstellen Sie ein Schlüsselpaar und ein Zertifikat.
   a. Starten Sie **HP ProtectTools Administor-Konsole**.
   b. Klicken Sie auf **Anmeldeinformationen**, **Smart Card** und anschließend auf die Registerkarte **Verwaltung**.

c. Vergewissern Sie sich, dass **Smart Card initialisieren** ausgewählt ist.

d. Geben Sie Ihre PIN ein, klicken Sie auf **Übernehmen**, und folgen Sie dann den Anleitungen auf dem Bildschirm.

Nachdem die Smart Card erfolgreich initialisiert wurde, muss sie noch registriert werden.

Registrieren der Smart Card

Nach der Initialisierung der Smart Card können Administratoren die Karte als Authentifizierungsmethode in der HP ProtectTools Administrator-Konsole registrieren:

1. Klicken Sie auf **Installations-Assistent**.
2. Klicken Sie auf der Seite **Willkommen!** auf **Weiter**.
3. Geben Sie Ihr Windows Kennwort ein, und klicken Sie dann auf **Weiter**.
4. Klicken Sie auf der Seite **SpareKey** auf **SpareKey-Setup überspringen**, es sei denn, Sie möchten die SpareKey-Informationen aktualisieren. Klicken Sie anschließend auf **Weiter**.
5. Klicken Sie auf der Seite **Sicherheitsfunktionen aktivieren** auf **Weiter**.
6. Vergewissern Sie sich, dass auf der Seite **Anmeldeinformationen auswählen** die Option **Smart Card** ausgewählt ist, und klicken Sie dann auf **Weiter**.
7. Geben Sie auf der Seite **Smart Card** Ihre PIN ein, und klicken Sie dann auf **Weiter**.
8. Klicken Sie auf **Fertig stellen**.

Benutzer können eine Smart Card auch in der Benutzer-Konsole von Security Manager registrieren. Weitere Informationen erhalten Sie in der Hilfe zur Software HP ProtectTools Security Manager, indem Sie rechts oben auf der Seite für die Smart Card auf das blaue **?**-Symbol klicken.

Konfigurieren der Smart Card

Wenn der Computer über ein integriertes oder angeschlossenes Lesegerät für Smart Cards verfügt, werden auf der Seite „Smart Card“ folgende Registerkarten angezeigt:

- **Einstellungen** – Durch Aktivierung des Kontrollkästchens **Computer beim Entfernen der Smart Card sperren** können Sie den Computer so konfigurieren, dass dieser beim Entfernen der Smart Card automatisch gesperrt wird. Klicken Sie anschließend auf **Übernehmen**.

HINWEIS: Der Computer wird jedoch nur dann gesperrt, wenn die Smart Card als Anmeldeinformation zur Authentifizierung bei der Windows Anmeldung genutzt wurde. Wenn eine Smart Card entfernt wird, die nicht für die Windows Anmeldung verwendet wurde, wird der Computer nicht gesperrt.

- **Verwaltung** – Wählen Sie eine der folgenden Optionen aus:
  - **Smart Card initialisieren** – Bereitet eine Smart Card für die Verwendung mit HP ProtectTools vor. Wenn eine Smart Card zuvor bereits außerhalb von HP ProtectTools initialisiert wurde (und ein asymmetrisches Schlüsselpaar sowie das zugehörige Zertifikat enthält), muss sie nicht erneut initialisiert werden, es sei denn, es wird eine Initialisierung mit einem bestimmten Zertifikat gewünscht.
  - **Smart Card-PIN ändern** – Hiermit können Sie die In Verbindung mit der Smart Card verwendete PIN ändern.

- **Nur HP ProtectTools Daten löschen** – Löscht nur das während der Karteninitialisierung erstellte HP ProtectTools Zertifikat. Es werden keine anderen Daten auf der Karte gelöscht.
- **Alle Daten auf der Smart Card löschen** – Löscht alle Daten auf der angegebenen Smart Card. Die Karte kann dann nicht mehr mit HP ProtectTools oder anderen Anwendungen verwendet werden.

HINWEIS: Funktionen, die von Ihrer Smart Card oder der zugehörigen Middleware nicht unterstützt werden, sind nicht verfügbar.

▲ Klicken Sie auf **Übernehmen**.

Transponderkarte

Eine Transponderkarte ist eine kleine Plastikkarte mit integriertem Computerchip. Wenn ein Lesegerät für eine Transponderkarte an den Computer angeschlossen ist, der damit verbundene Treiber des Herstellers installiert und eine Transponderkarte als Anmeldeinformation ausgewählt wurde, können Sie Ihre Transponderkarte zur Authentifizierung nutzen. Die folgenden Arten von Transponderkarten werden von HP ProtectTools unterstützt:

- HID iCLASS Transponderspeicherkarten
- MiFare Classic Transponderkarten (1k, 4k) und Mini-Speicherkarten

▲ Zum Einrichten der Transponderkarte halten Sie diese sehr nah an das Lesegerät, folgen Sie den Anleitungen auf dem Bildschirm, und klicken Sie anschließend auf **Übernehmen**.

RFID-Karte

Eine RFID-Karte ist eine kleine Plastikkarte mit integriertem Computerchip. Wenn ein Lesegerät für eine RFID-Karte an den Computer angeschlossen ist, der damit verbundene Treiber des Herstellers installiert und eine RFID-Karte als Anmeldeinformation zur Authentifizierung ausgewählt wurde, können Sie eine RFID-Karte in Verbindung mit anderen Anmeldeinformationen für zusätzliche Sicherheit nutzen.

▲ Zum Einrichten der RFID-Karte halten Sie sie sehr nah an das Lesegerät, und klicken Sie anschließend auf **Übernehmen**.

Bluetooth

Sofern der Computer mit Bluetooth® -Funktion ausgestattet ist, Bluetooth als Anmeldeinformation zur Authentifizierung ausgewählt und ein Bluetooth-Telefon mit dem Computer gekoppelt wurde, können Sie Ihr Bluetooth Telefon in Verbindung mit anderen Anmeldeinformationen für zusätzliche Sicherheit nutzen. Legen Sie die Bluetooth Einstellungen fest.

▲ Aktivieren Sie das entsprechende Kontrollkästchen, um unbeaufsichtigte Authentifizierung zuzulassen, und klicken Sie anschließend auf **Übernehmen**.

PIN

Wenn PIN als Anmeldeinformation zur Authentifizierung aktiviert wurde, können Sie eine PIN in Verbindung mit anderen Anmeldeinformationen für zusätzliche Sicherheit nutzen. Legen Sie die PIN-Einstellungen fest:

1. Klicken Sie auf den Pfeil nach unten oder nach oben, um die Mindestlänge der PIN festzulegen.

   Die maximale Länge beträgt 8 Ziffern.

2. Klicken Sie auf **Übernehmen**.

Anwendungen

Die Seite „Einstellungen“ unter Anwendungen auf der linken Seite der Administrator-Konsole enthält zwei Registerkarten, mit denen Sie das Verhalten der derzeit installierten HP ProtectTools Security Manager Anwendungen anpassen können.

▲ Klicken Sie auf der linken Seite der Administrator-Konsole unter **Anwendungen** auf **Einstellungen**.

Registerkarte „Allgemein“

Die folgenden Einstellungen stehen auf der Registerkarte **Allgemein** zur Verfügung:

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

1. Zum Aktivieren/Deaktivieren einer bestimmten Einstellung verwenden Sie das entsprechende Kontrollkästchen.
2. Klicken Sie auf **Übernehmen**.

Registerkarte „Anwendungen”

Administratoren können die folgenden Anwendungen aktivieren oder deaktivieren:

- **Status** — Verwenden Sie dieses Kontrollkästchen zum Aktivieren oder Deaktivieren aller Anwendungen.
- **Password Manager** – Aktiviert den Password Manager für alle Benutzer des Computers.

1. Zum Aktivieren/Deaktivieren einer bestimmten Einstellung verwenden Sie das entsprechende Kontrollkästchen.
2. Klicken Sie auf **Übernehmen**.

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

Daten

Der Abschnitt „Daten“ im linken Bereich der Administrator-Konsole ermöglicht es Ihnen, Einstellungen für die folgende Anwendung zu konfigurieren:

- **Drive Encryption** – Konfigurieren der Einstellungen und Anzeigen des Laufwerksstatus. Weitere Informationen erhalten Sie in der Hilfe zur Software Drive Encryption, indem Sie rechts oben auf der Seite für Drive Encryption auf das blaue **?**-Symbol klicken.

Computer

Der Bereich „Computer“ auf der linken Seite der Administrator-Konsole ermöglicht es Ihnen, Einstellungen für die Device Access Manager Anwendung zu konfigurieren:

- Einfache Konfiguration
- Geräteklassen-Konfiguration

- Konfiguration der Just-In-Time (JITA)-Authentifizierung
- Erweiterte Einstellungen

Weitere Informationen erhalten Sie in der Hilfe zur Device Access Manager Software, indem Sie auf das blaue Symbol **?** rechts oben auf der Device Access Manager Seite klicken.

5 HP ProtectTools Security Manager

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

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

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

Öffnen von Security Manager

Security Manager lässt sich auf folgenden Arten starten:

▲ Doppelklicken Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools**.

– oder –

Klicken Sie in der **Systemsteuerung** auf **System und Sicherheit**, und wählen Sie **HP ProtectTools Security Manager** aus.

Verwenden der Security Manager Benutzer-Konsole

Die Security Manager Benutzer-Konsole ist der zentrale Ausgangspunkt für den Zugriff auf Funktionen, Anwendungen und Einstellungen von Security Manager. Folgende Komponenten werden in der Benutzer-Konsole angezeigt:

- **ID-Card** – Zeigt den Windows Benutzernamen und ein Bild zur Identifizierung des angemeldeten Benutzerkontos an.
- **Sicherheitsanwendungen** – Zeigt ein erweitertes Menü mit Links an, über die folgende Sicherheitskategorien konfiguriert werden können:
  - **Startseite** – Ermöglicht die Verwaltung von Kennwörtern, die Einrichtung von Authentifizierungsinformationen und die Überprüfung des Status der Sicherheitsanwendungen.
  - **Wiederbeschaffung gestohlener Geräte** – Computrace for HP ProtectTools (separat erhältlich)
- **Meine Anmeldungen** – Ermöglicht die Verwaltung der verschiedenen Anmeldeinformationen zur Authentifizierung mit Password Manager und Credential Manager.

- **Meine Daten** – Ermöglicht die Verwaltung der Datensicherheit mit Drive Encryption.

HINWEIS: Diese Komponene wird nicht angezeigt, wenn die Anwendung nicht installiert ist.

- **Arbeitsplatz** – Ermöglicht die Verwaltung der Sicherheit Ihres Computers mit Device Access Manager.

HINWEIS: Diese Komponene wird nicht angezeigt, wenn die Anwendung nicht installiert ist.

- **Verwaltung** – Ermöglicht Administratoren den Zugriff auf die **Administrator-Konsole** zur Verwaltung von Sicherheit und Benutzern.
- **Erweitert** – Bietett Befehle für den Zugriff auf zusätzliche Funktionen, wie beispielsweise:
  - **Voreinstellungen** – Ermöglicht die Personalisierung der Security Manager-Einstellungen.
  - **Sichern und Wiederherstellen** – Ermöglicht die Sicherung und Wiederherstellung von Daten.
  - **Info** – Zeigt Informationen zu HP ProtectTools Security Manager, wie etwa Versionsnummer und Copyright-Hinweis, an.
- **Hauptbereich** – Zeigt anwendungsspezifische Inhalte an.
- **?** — Öffnet die Hilfe für die Security Manager Benutzer-Konsole. Das Hilfe-Symbol befindet sich rechts oben im Fensterrahmen neben den Symbolen für die Minimierung und Maximierung der Fensteranzeige.

Ihre persönliche ID-Card

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

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

So ändern Sie den angezeigten Namen:

1. Öffnen Sie die Security Manager Benutzer-Konsole. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
2. Klicken Sie auf die ID-Card links oben in der Benutzer-Konsole.
3. Klicken Sie auf das Feld mit Ihrem Windows Benutzernamen für dieses Konto, geben Sie einen neuen Namen ein, und klicken Sie dann auf **Speichern**.

My Logons (Meine Anmeldeinformationen)

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

- **Password Manager** – Erstellt und verwaltet Verknüpfungen, über die Sie Websites und Programme starten und sich bei diesen anmelden können, indem Sie sich mit Ihrem Windows Kennwort, Ihrem Fingerabdruck, Ihrem Gesicht, einer Smart Card, einer Transponderkarte, einer RFID-Karte, einem Bluetooth Telefon oder Ihrer PIN authentifizieren.
- **Credential Manager** – Hier können Sie ganz einfach Ihr Windows Kennwort ändern, Ihre Fingerabdrücke oder Ihr Gesicht registrieren oder eine Smart Card, eine Transponderkarte, eine RFID-Karte, ein Bluetooth Telefon oder eine PIN einrichten.

Administratoren erhalten Informationen zu weiteren verfügbaren Sicherheitsanwendungen, indem Sie auf **Verwaltung** und anschließend auf **Zentrale Verwaltung** links unten im Dashboard klicken.

Password Manager

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

Password Manager bietet folgende Optionen:

Registerkarte „Verwalten“

- Anmeldungen hinzufügen, bearbeiten oder löschen
- Verwenden von Verknüpfungen zum Starten Ihres Standardbrowsers und Anmelden bei beliebigen Websites oder Programmen (nach entsprechender Einrichtung).
- Verschieben von Verknüpfungen per Drag and Drop, um diese nach Belieben in Kategorien einzuordnen.
- Auf einen Blick erkennen, ob eines Ihrer Kennwörter ein Sicherheitsrisiko birgt.

Registerkarte „Kennwortsicherheit“

- Überprüfen der Sicherheit einzelner Kennwörter, die für Websites und Anwendungen verwendet werden, sowie der allgemeinen Kennwortsicherheit.
- Die Kennwortsicherheit wird mittels roter, gelber oder grüner Statusindikatoren dargestellt.

Das **Password Manager**-Symbol befindet sich links oben auf einer Website oder dem Anmeldebildschirm einer Anwendung. Wenn noch keine Anmeldedaten für die Website oder Anwendung festgelegt wurden, enthält das Symbol ein Pluszeichen.

▲ Klicken Sie auf das **Password Manager**-Symbol, um ein Kontextmenü anzuzeigen, in dem Sie aus den im Folgenden genannten Optionen wählen können:

- [beliebigeDomäne.de] zu Password Manager hinzufügen
- Password Manager öffnen
- Symboleinstellungen
- Hilfe

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

Folgende Optionen werden im Kontextmenü angezeigt:

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

Für Webseiten oder Programme, für die bereits Anmeldedaten festgelegt wurden

Folgende Optionen werden im Kontextmenü angezeigt:

- **Anmeldedaten eingeben** – Zeigt die Seite „Identität bestätigen“ an. Bei erfolgreicher Authentifizierung werden Ihre Anmeldedaten in die Anmeldefelder eingefügt und die Seite wird übermittelt (wenn die Übermittlung beim Erstellen oder bei der letzten Änderung der Anmeldedaten festgelegt wurde).
- **Anmeldedaten bearbeiten** – Hier können Sie Ihre Anmeldedaten für diese Website bearbeiten.
- **Anmeldedaten hinzufügen** – Hier können Sie ein Konto zu Password Manager hinzufügen.
- **Password Manager öffnen** – Startet Password Manager.
- **Hilfe** – Öffnet die Hilfe für Security Manager.

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

Hinzufügen von Anmeldedaten

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

So fügen Sie Anmeldedaten hinzu:

1. Öffnen Sie den Anmeldebildschirm für eine Website oder ein Programm.
2. Klicken Sie auf den Pfeil am Symbol **Password Manager**, und klicken Sie dann auf eine der folgenden Optionen, je nachdem, ob es sich um den Anmeldebildschirm einer Website oder eines Programms handelt.
   - Klicken Sie im Falle einer Website auf **[Domänenname] zu Password Manager hinzufügen**.
   - Klicken Sie im Falle eines Programms auf **Diesen Anmeldebildschirm zu Password Manager hinzufügen**.
3. Geben Sie Ihre Anmeldedaten ein. Anmeldefelder auf dem Bildschirm und ihre entsprechenden Felder im Dialogfeld sind mit einer fett formatierten orangefarbenen Umrandung gekennzeichnet. Sie können dieses Dialogfeld ebenfalls anzeigen, indem Sie in der

Registerkarte **Password Manager** auf **Anmeldung hinzufügen** klicken, die Tastenkombination strg+Windows Logo-Taste+h verwenden oder mit dem Finger über den Sensor streichen.

a. Um ein Anmeldefeld mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken Sie auf die Pfeile rechts vom Feld.

b. Um das Kennwort für diese Anmeldedaten anzuzeigen, klicken Sie auf **Kennwort einblenden**.

c. Um die Anmeldefelder automatisch auszufüllen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldedaten automatisch senden**.

d. Klicken Sie auf **OK**, um die gewünschte Authentifizierungsmethode zu wählen (Fingerabdruck, Gesicht, Smart Card, RFID-Karte, Transponderkarte, Bluetooth Telefon, PIN oder Kennwort). Melden Sie sich dann mit dieser Methode an.

Das Pluszeichen wird aus dem **Password Manager**-Symbol entfernt, um anzugeben, dass die Anmeldedaten erstellt wurden.

e. Falls Password Manager die Anmeldedaten nicht erkennt, klicken Sie auf **Weitere Felder**.

- Aktivieren Sie das Kontrollkästchen für jedes Feld, das für die Anmeldung erforderlich ist, oder deaktivieren Sie das Kontrollkästchen für alle Felder, die nicht für die Anmeldung erforderlich sind.
- Klicken Sie auf **Schließen**.

Bei jedem Aufrufen dieser Website oder dieses Programms wird das **Password Manager**-Symbol links oben auf der Website bzw. dem Anmeldebildschirm der Anwendung angezeigt. Es gibt an, dass Sie Ihre registrierten Anmeldeinformationen für die Anmeldung verwenden können.

Bearbeiten von Anmeldedaten

Gehen Sie folgendermaßen vor, um Anmeldedaten zu bearbeiten:

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

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

Verwenden des Menüs „Password Manager Verknüpfungen“

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

Wenn Sie Anmeldedaten festlegen, werden diese automatisch in das Menü **Verknüpfungen** von Password Manager übernommen.

So zeigen Sie das Menü **Verknüpfungen** an:

1. Drücken Sie die Tastenkombination für **Password Manager** (die Werkseinstellung lautet strg+Windows Logo-Taste+h). Zum Ändern der Tastenkombination klicken Sie in der Security Manager Benutzer-Konsole auf **Password Manager** und anschließend auf **Einstellungen**.
2. Scannen Sie Ihren Fingerabdruck (bei Computern mit integriertem oder angeschlossenem Fingerabdruck-Lesegerät), oder geben Sie Ihr Windows Kennwort ein.

Organisieren von Anmeldedaten in Kategorien

Erstellen Sie zum Ordnen Ihrer Anmeldedaten eine oder mehrere Kategorien. Verschieben Sie dann die Anmeldedaten per Drag & Drop in die gewünschten Kategorien.

So fügen Sie eine Kategorie hinzu:

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

So fügen Sie Anmeldedaten einer Kategorie hinzu:

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

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

Verwalten Ihrer Anmeldedaten

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

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

So verwalten Sie Ihre Anmeldedaten:

▲ Klicken Sie in der Security Manager Benutzer-Konsole auf **Password Manager** und anschließend auf die Registerkarte **Verwalten**.

- **Anmeldedaten hinzufügen** – Klicken Sie auf **Anmeldedaten hinzufügen**, und befolgen Sie die Anweisungen auf dem Bildschirm.
- **Ihre Anmeldedaten** – Klicken Sie auf vorhandene Anmeldedaten, wählen Sie eine der folgenden Optionen aus, und befolgen Sie dann die Anweisungen auf dem Bildschirm:
  - **Öffnen** –Öffnet eine Website oder Anwendung, für die Anmeldedaten vorhanden sind.
  - **Hinzufügen** – Fügt Anmeldedaten hinzu. Weitere Informationen finden Sie unter „Hinzufügen von Anmeldedaten“ auf Seite 31.
  - **Bearbeiten** – Ermöglicht die Bearbeitung von Anmeldedaten. Weitere Informationen finden Sie unter „Bearbeiten von Anmeldedaten“ auf Seite 32.
  - **Löschen** –Löscht den Eintrag für eine Website oder Anwendung, für die Anmeldedaten vorhanden sind.
- **Kategorie hinzufügen** – Klicken Sie auf **Kategorie hinzufügen** — und befolgen Sie dann die Anweisungen auf dem Bildschirm. Weitere Informationen finden Sie unter „Organisieren von Anmeldedaten in Kategorien“ auf Seite 33.

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

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

Einschätzen der Kennwortsicherheit

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

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

Auf der Registerkarte **Kennwortsicherheit** zeigen rote, gelbe oder grüne Statusindikatoren die Sicherheit einzelner Kennwörter, die für Websites und Anwendungen verwendet werden, sowie die allgemeine Kennwortsicherheit an.

Einstellungen für das Password Manager Symbol

Password Manager versucht, Anmeldebildschirme für Websites und Programme zu identifizieren. Wenn ein Anmeldebildschirm erkannt wird, für den Sie noch keine Anmeldedaten erstellt haben,

fordert Sie Password Manager auf, Anmeldedaten für diesen Bildschirm zu erstellen, indem das **Password Manager**-Symbol mit einem Pluszeichen angezeigt wird.

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

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

     So fügen Sie Anmeldedaten für einen neuen Bildschirm hinzu:

     - Öffnen Sie den zuvor ausgeschlossenen Anmeldebildschirm für eine Website oder Anwendung, öffnen Sie dann die Security Manager Benutzer-Konsole, und klicken Sie auf **Password Manager**.
     - Klicken Sie auf **Anmeldedaten hinzufügen**.

       Das Dialogfeld „Anmeldedaten hinzufügen“ wird geöffnet, wobei der Anmeldebildschirm für die Website oder das Programm im Feld **Aktueller Bildschirm** aufgeführt wird.
     - Klicken Sie auf **Weiter**.

       Der Bildschirm „Anmeldedaten zu Password Manager hinzufügen“ wird angezeigt.
     - Folgen Sie den Anleitungen auf dem Bildschirm. Weitere Informationen finden Sie unter „Hinzufügen von Anmeldedaten“ auf Seite 31.
     - Das **Password Manager**-Symbol wird bei jedem Öffnen dieses Website-Anmeldebildschirms bzw. Programmbildschirms angezeigt.

   Nicht zum Hinzufügen von Anmeldedaten für Anmeldebildschirm auffordern – Aktivieren Sie das Optionsfeld.

2. Um auf weitere Password Manager-Einstellungen zuzugreifen, doppelklicken Sie auf **Password Manager** und klicken Sie anschließend in der Security Manager Benutzer-Konsole auf **Einstellungen**.

Einstellungen

Sie können Einstellungen zur Personalisierung von Password Manager vornehmen:

1. **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern** – Das **Password Manager**-Symbol wird immer dann mit einem Pluszeichen angezeigt, wenn der Anmeldebildschirm einer Website oder eines Programms erkannt wird. Dies zeigt an, dass Sie Anmeldedaten für diesen Bildschirm im Menü **Anmeldedaten** hinterlegen können. Wenn diese Funktion nicht ausgeführt werden soll, deaktivieren Sie das Kontrollkästchen neben **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern**.
2. **Password Manager mit strg+win+h öffnen** – Die Standardtastenkombination zum Öffnen des Menüs **Password Manager Verknüpfungen** — lautet strg+Windows Logo-Taste+h. Zum Ändern der Tastenkombination klicken Sie auf diese Option und geben eine neue Tastenkombination ein. Die Kombinationen können sich aus folgenden Elementen zusammensetzen: strg, alt oder Umschalttaste plus eine beliebige Buchstaben- oder Zifferntaste.
3. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Credential Manager

Sie können Security Manager-Anmeldedaten zur Überprüfung Ihrer Identität verwenden. Der Administrator dieses Computers kann einstellen, anhand welcher Anmeldedaten Sie Ihre Identität bei Ihrem Windows Konto, bei Websites oder Programmen nachweisen können.

Die verfügbaren Anmeldedaten können je nach integrierten oder an den Computer angeschlossenen Sicherheitsgeräten variieren. Zur Anzeige der unterstützten Anmeldedaten, Anforderungen sowie des aktuellen Status klicken Sie unter **Meine Anmeldedaten** auf **Credential Manager**. Folgende Optionen stehen zur Auswahl:

- Kennwort
- SpareKey
- Fingerabdrücke
- Gesicht
- Smart Card
- Transponderkarte
- RFID-Karte
- Bluetooth
- PIN

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

Ändern Ihres Windows Kennworts

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

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

1. Klicken Sie in der Security Manager Benutzer-Konsole auf **Credential Manager** und anschließend auf **Kennwort**.
2. Geben Sie in das Textfeld **Aktuelles Windows Kennwort** Ihr aktuelles Kennwort ein.
3. Geben Sie in das Textfeld **Neues Windows Kennwort** ein neues Kennwort ein, und wiederholen Sie dieses im Textfeld **Neues Kennwort bestätigen**.
4. Klicken Sie auf **Ändern**, um Ihr aktuelles Kennwort sofort durch das soeben eingegebene Kennwort zu ersetzen.

Einrichten eines SpareKey

Die SpareKey-Funktion ermöglicht Ihnen (auf unterstützten Plattformen) den Zugriff auf Ihren Computer, indem Sie drei Sicherheitsfragen aus einer Liste beantworten, die zuvor vom Administrator definiert wurden.

Bei der Ersteinrichtung mithilfe des Installations-Assistenten werden Sie von HP ProtectTools Security Manager zur Einrichtung Ihres persönlichen SpareKey aufgefordert.

So richten Sie einen persönlichen SpareKey ein:

1. Wählen Sie auf der SpareKey-Seite des Assistenten drei Sicherheitsfragen aus, und beantworten Sie sie.
2. Klicken Sie auf **Erstellen**.

Auf der SpareKey-Seite von **Credential Manager** können Sie andere Fragen auswählen bzw. Ihre Antworten ändern.

Nach der Einrichtung können Sie mit dem SpareKey von einem Systemstart-Anmeldebildschirm oder dem Windows Startbildschirm aus auf Ihren Computer zugreifen.

Registrieren Ihrer Fingerabdrücke

Wenn der Administrator Fingerabdrücke auf der Seite **Anmeldeinformationen auswählen** ausgewählt hat oder wenn Ihr Computer über ein integriertes oder angeschlossenes Fingerabdruck-Lesegerät verfügt, leitet Sie der Installations-Assistent für HP ProtectTools Security Manager durch die Konfiguration bzw. Registrierung Ihrer Fingerabdrücke: Sie können Ihre Fingerabdrücke auch auf der Seite „Fingerabdruck“ in der Security Manager Benutzer-Konsole unter **Credential Manager** registrieren.

1. Auf der Seite „Fingerabdrücke“ des Assistenten wird der Umriss zweier Hände angezeigt. Bereits registrierte Finger sind hervorgehoben. Klicken Sie auf einen Finger in der Darstellung.

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

2. Sie werden aufgefordert, mit dem Finger über den Sensor zu streichen, bis der Fingerabdruck erfolgreich registriert wurde. Ein registrierter Finger wird in der Abbildung hervorgehoben.
3. Sie müssen mindestens zwei Finger registrieren, wobei Zeige- und Mittelfinger vorzuziehen sind. Wiederholen Sie die Schritte 1 und 2 für einen weiteren Finger.
4. Klicken Sie auf **Weiter**, und befolgen Sie die Anweisungen auf dem Bildschirm.

ACHTUNG: Bei der Registrierung der Fingerabdrücke über den Assistenten werden die Fingerabdruck-Informationen erst gespeichert, wenn Sie auf **Weiter** klicken. Wenn der Computer eine Zeit lang inaktiv ist oder das Programm geschlossen wird, werden die von Ihnen vorgenommenen Änderungen **nicht** gespeichert.

Registrieren von Gesichtsszenen für die Gesichtserkennung

Wenn Sie sich für die Anmeldung per Gesichtserkennung entscheiden und Ihr Computer über eine integrierte oder angeschlossene Webcam verfügt, fordert Sie der Installations-Assistent für HP ProtectTools Security Manager auf, Gesichtsszenen zu registrieren. Sie können Ihre Szenen auch auf der Seite für die Gesichtserkennung in der Security Manager Benutzer-Konsole unter **Credential Manager** registrieren.

Um die Anmeldung per Gesichtserkennung nutzen zu können, müssen Sie mindestens eine Gesichtsszene registrieren. Nachdem Sie sich erfolgreich registriert haben, können Sie auch eine neue Szene registrieren, falls während der Anmeldung Probleme auftreten, die mit Änderungen der folgenden Bedingungen zusammenhängen:

- Ihr Gesicht hat sich im Vergleich zur letzten Registrierung erheblich verändert.
- Die Beleuchtung unterscheidet sich wesentlich von der Beleuchtung vorheriger Registrierungen.
- Sie haben bei der letzten Registrierung eine (oder keine) Brille getragen.

HINWEIS: Wenn Sie Schwierigkeiten beim Registrieren von Szenen haben, versuchen Sie, Ihren Abstand zur Webcam zu verringern.

So registrieren Sie eine neue Szene mit dem Installations-Assistenten für HP ProtectTools Security Manager:

1. Klicken Sie auf der Seite für die Gesichtserkennung des Assistenten auf **Erweitert**, und konfigurieren Sie zusätzliche Optionen. Weitere Informationen finden Sie unter „Erweiterte Benutzereinstellungen“ auf Seite 40.
2. Klicken Sie auf **OK**.
3. Klicken Sie auf **Start** oder – falls Sie bereits Gesichtsszenen registriert haben – auf **Neue Szene registrieren**.
4. Während der Szenenregistrierung können Sie durch Klicken auf **Video abspielen** ein Demonstrationsvideo abspielen.

   Wenn es sich dabei um die Erstregistrierung handelt, wird ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob Sie sich das Demonstrationsvideo ansehen möchten. Klicken Sie entweder auf **Ja** oder auf **Nein**.
5. Bei geringem Licht kann die Software den Bildschirm automatisch aufhellen. Sie können jedoch auch auf das Symbol **Glühbirne** klicken, um die Hintergrundbeleuchtung zu ändern.
6. Klicken Sie auf das **Kamera**-Symbol, und folgen Sie den Anleitungen auf dem Bildschirm, um eine Gesichtsszene zu registrieren.

   HINWEIS: Schauen Sie auf Ihr Bild, und drehen Sie Ihren Kopf entsprechend, während die Szenen aufgezeichnet werden.
7. Klicken Sie auf **Weiter**.

Sie können Gesichtsszenen auch in der Security Manager Benutzer-Konsole registrieren:

1. Öffnen Sie die Security Manager Benutzer-Konsole. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
2. Klicken Sie unter **Meine Anmeldedaten** auf **Credential Manager** und dann auf **Gesicht**.
3. Klicken Sie auf **Erweitert**, um zusätzliche Optionen zu konfigurieren. Weitere Informationen finden Sie unter „Erweiterte Benutzereinstellungen“ auf Seite 40.
4. Klicken Sie auf **OK**.

5. Klicken Sie auf **Start** oder – falls Sie bereits Gesichtsszenen registriert haben – auf **Neue Szene registrieren**.
6. Wenn Sie aufgefordert werden, Ihr Windows Kennwort einzugeben, geben Sie es ein, und klicken Sie dann auf **Weiter**.
7. Während der Szenenregistrierung können Sie durch Klicken auf **Video abspielen** ein Demonstrationsvideo abspielen.

   Wenn es sich dabei um die Erstregistrierung handelt, wird ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob Sie sich das Demonstrationsvideo ansehen möchten. Klicken Sie entweder auf **Ja** oder auf **Nein**.
8. Bei geringem Licht kann die Software den Bildschirm automatisch aufhellen. Sie können jedoch auch auf das Symbol **Glühbirne** klicken, um die Hintergrundbeleuchtung zu ändern.
9. Klicken Sie auf das **Kamera**-Symbol, und folgen Sie den Anleitungen auf dem Bildschirm, um eine Gesichtsszene zu registrieren.

HINWEIS: Schauen Sie auf Ihr Bild, und drehen Sie Ihren Kopf entsprechend, während die Szenen aufgezeichnet werden.

Weitere Informationen erhalten Sie in der Hilfe zur Face Recognition Software, indem Sie auf das blaue Symbol **?** rechts oben auf der Seite für die Gesichtserkennung klicken.

Authentifizierung

Nachdem Sie eine oder mehrere Szenen registriert haben, können Sie die Gesichtserkennung verwenden, um sich beim Computer anzumelden oder eine neue Windows Sitzung zu starten.

1. Wenn der Authentifizierungsbildschirm angezeigt wird und die Kamera Ihr Gesicht erkennt, haben Sie fünf Sekunden Zeit, um den Anmeldevorgang zu starten. Wenn Ihr Gesicht erfolgreich authentifiziert wird, können Sie auf den Computer zugreifen.
2. Läuft das Zeitlimit für die Gesichtserkennung ab, so wird Face Recognition angehalten. Klicken Sie auf das Symbol **Kamera**, um den Authentifizierungsvorgang fortzusetzen.

HINWEIS: Falls die Beleuchtung nicht ausreicht und Sie sich über Face Recognition nicht anmelden können, können Sie Ihr Windows Kennwort eingeben, um sich am Computer anzumelden.

3. Wenn Face Recognition Sie nach dem Anmelden am Computer fragt, ob zusätzliche Szenen zur Verbesserung der Anmeldefähigkeit für zukünftige Anmeldungen hinzugefügt werden sollen, klicken Sie auf **Ja**.

Dunkelmodus

Ist die Beleuchtung während des Anmeldevorgangs per Gesichtserkennung zu dunkel, so wechselt die Hintergrundfarbe des Bildschirms für die Gesichtserkennung automatisch zu Weiß, um die Beleuchtung des Gesichts zu optimieren.

Um die Hintergrundfarbe des Bildschirms für die Gesichtserkennung manuell zu ändern, klicken Sie auf das Symbol **Glühbirne**.

Lernprozess

Wenn die Gesichtserkennung nicht erfolgreich ist, Sie jedoch Ihr Kennwort erfolgreich eingeben, werden Sie möglicherweise aufgefordert, eine Bilderserie zu speichern, um die Wahrscheinlichkeit einer erfolgreichen Anmeldung per Gesichtserkennung zukünftig zu erhöhen.

Löschen einer Szene

So löschen Sie eine registrierte Szene:

1. Öffnen Sie die Security Manager Benutzer-Konsole. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
2. Klicken Sie unter **Meine Anmeldungen** auf **Credential Manager** und dann auf **Gesicht**.
3. Klicken Sie auf die zu löschende Szene und anschließend auf das Symbol **Papierkorb**.
4. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

Erweiterte Benutzereinstellungen

1. Öffnen Sie die Security Manager Benutzer-Konsole. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
2. Klicken Sie unter **Meine Anmeldedaten** auf **Credential Manager** und dann auf **Gesicht**.
3. Klicken Sie auf **Erweitert**, um die folgenden Optionen zu konfigurieren:

   Registerkarte **Sonstige Einstellungen** – Aktivieren Sie die entsprechenden Kontrollkästchen, um eine oder mehrere der folgenden Optionen auszuwählen, oder deaktivieren Sie das entsprechende Kontrollkästchen, um die zugehörige Option zu deaktivieren. Die hier vorgenommenen Einstellungen gelten nur für den aktuellen Benutzer.

   - **Klang bei Gesichtserkennungsereignissen abspielen** – Wenn die Gesichtserkennung erfolgreich ist bzw. fehlschlägt, erklingt ein Signalton.
   - **Bei fehlgeschlagener Anmeldung zum Aktualisieren von Szenen auffordern** – Wenn die Gesichtserkennung fehlgeschlagen ist, Sie Ihr Kennwort jedoch erfolgreich eingegeben haben, werden Sie unter Umständen zum Speichern der einzelnen aufgezeichneten Gesichtsszenen aufgefordert, um die Chancen einer erfolgreichen Gesichtserkennung in der Zukunft zu erhöhen.
   - **Bei fehlgeschlagener Anmeldung zum Registrieren einer neuen Szene auffordern** – Wenn die Gesichtserkennung zwar fehlgeschlagen ist, Sie Ihr Kennwort jedoch erfolgreich eingegeben haben, werden Sie unter Umständen zur Registrierung einer neuen Szene aufgefordert, um die Chancen einer erfolgreichen Gesichtserkennung in der Zukunft zu erhöhen.

4. Um die Einstellungen auf die ursprünglichen Werte zurückzusetzen, klicken Sie auf **Standardeinstellungen wiederherstellen**.
5. Klicken Sie auf **OK**.

Einrichten einer Smart Card

Wenn ein Smart Card-Lesegerät integriert oder an Ihren Computer angeschlossen ist und der Administrator eine Smart Card als Anmeldeinformation zur Authentifizierung aktiviert und die in der Hilfe für die Software HP ProtectTools Administrator-Konsole beschriebenen Schritte ausgeführt hat, werden Sie vom Installations-Assistenten für HP ProtectTools Security Manager dazu aufgefordert, eine Smart Card einzuführen und diese einzurichten. Sie können die Smart Card auch in der Security Manager Benutzer-Konsole unter **Credential Manager** auf der Seite „Smart Card“ einrichten.

HINWEIS: Ein Administrator mussn die Smart Card initialisieren, bevor sie für die Authentifizierung verwendet werden kann.

Initialisieren der Smart Card

HP ProtectTools Security Manager kann eine Reihe verschiedener Smart Cards unterstützen. Die Anzahl und Art der Zeichen, die für die PIN verwendet werden, können variieren. Der Hersteller der Smart Card stellt normalerweise Tools für die Installation eines Sicherheitszertifikats und einer PIN-Verwaltung bereit, die HP ProtectTools in seinem Sicherheitsalgorithmus verwendet.

Administratoren können die Smart Card mithilfe der Software des Herstellers und der HP ProtectTools Administrator-Konsole initialisieren. Weitere Informationen finden Sie in der Hilfe zur Software HP ProtectTools Security Administrator-Konsole.

Registrieren der Smart Card

Nach der Initialisierung der Smart Card kann sie der Benutzer in Security Manager registrieren:

1. Öffnen Sie die Security Manager Benutzer-Konsole. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
2. Klicken Sie auf **Credential Manager** und dann auf **Smart Card**.
3. Vergewissern Sie sich, dass **Einrichten** ausgewählt ist.
4. Geben Sie Ihr Windows Kennwort und Ihre PIN ein, und klicken Sie dann auf **Speichern**.

Administratoren können die Smart Card auch über die HP ProtectTools Administrator-Konsole registrieren. Weitere Informationen finden Sie in der Hilfe zur Software der HP ProtectTools Security Administrator-Konsole.

Ändern der Smart Card-PIN

So ändern Sie Ihre Smart Card-PIN:

1. Legen Sie eine formatierte und initialisierte Smart Card ein.
2. Wählen Sie **Smart Card-PIN ändern**.
3. Geben Sie Ihre bisherige PIN ein. Geben Sie dann eine neue PIN ein, und bestätigen Sie Ihre Eingabe.

Transponderkarte

Eine Transponderkarte ist eine kleine Plastikkarte mit integriertem Computerchip. Wenn ein Lesegerät für eine Transponderkarte an den Computer angeschlossen ist, der Administrator den damit verbundenen Treiber des Herstellers installiert und eine Transponderkarte als Anmeldeinformation zur Authentifizierung aktiviert hat, können Sie eine Transponderkarte als Anmeldeinformation zur Authentifizierung nutzen. Die folgenden Arten von Transponderkarten werden von HP ProtectTools unterstützt:

- HID iCLASS Transponderspeicherkarten
- MiFare Classic Transponderkarten (1k, 4k) und Mini-Speicherkarten

▲ Zum Einrichten der Transponderkarte halten Sie diese sehr nah an das Lesegerät, befolgen Sie die Anweisungen auf dem Bildschirm, und klicken Sie anschließend auf **Übernehmen**.

RFID-Karte

Eine RFID-Karte ist eine kleine Plastikkarte mit integriertem Computerchip. Wenn ein Lesegerät für eine RFID-Karte an den Computer angeschlossen ist, der Administrator den damit verbundenen Treiber des Herstellers installiert und eine RFID-Karte als Anmeldeinformation zur Authentifizierung

aktiviert hat, können Sie eine RFID-Karte in Verbindung mit anderen Anmeldeinformationen für zusätzliche Sicherheit nutzen.

- ▲ Zum Einrichten der Transponderkarte halten Sie diese sehr nah an das Lesegerät, befolgen Sie die Anweisungen auf dem Bildschirm, und klicken Sie anschließend auf **Übernehmen**.

Bluetooth

Wenn der Administrator Bluetooth als Anmeldeinformation zur Authentifizierung aktiviert hat, können Sie ein Bluetooth Telefon in Verbindung mit anderen Anmeldeinformationen für zusätzliche Sicherheit einrichten.

HINWEIS: Es werden nur Bluetooth Telefone unterstützt.

1. Vergewissern Sie sich, dass die Bluetooth Funktion auf dem Computer aktiviert ist und sich das Bluetooth Telefon im Erkennungsmodus befindet. Um eine Verbindung zu dem Telefon herstellen zu können, werden Sie möglicherweise dazu aufgefordert, einen automatisch erzeugten Code auf dem Bluetooth Gerät einzugeben. Möglicherweise ist ein Vergleich zwischen den Pairing-Codes des Computers und des Telefons erforderlich. Dies hängt von den Konfigurationseinstellungen des Bluetooth Geräts ab.
2. Wählen Sie das zu registrierende Telefon aus, und klicken Sie auf **Registrieren**.
3. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

PIN

Wenn der Administrator eine PIN als Anmeldeinformation zur Authentifizierung aktiviert hat, können Sie eine PIN in Verbindung mit anderen Anmeldeinformationen für zusätzliche Sicherheit einrichten.

- ▲ Zum Einrichten einer neuen PIN geben Sie die PIN ein, und bestätigen Sie diese anschließend durch erneute Eingabe.

Verwaltung

Administratoren können auf die Administrator-Konsole und die zentrale Verwaltung zugreifen, indem sie auf **Verwaltung** klicken und dann im linken unteren Bereich der HP ProtectTools Security Manager Benutzer-Konsole **Administrator-Konsole** auswählen..

Weitere Informationen finden Sie in der Hilfe zur Software HP ProtectTools Security Administrator-Konsole.

Erweitert

Sie können auf die folgenden Optionen zugreifen, indem Sie im linken unteren Bereich der Benutzer-Konsole auf **Erweitert** klicken:

- **Voreinstellungen** – Ermöglicht die Personalisierung der Security Manager-Einstellungen.
- **Sichern und Wiederherstellen** – Ermöglicht die Sicherung und Wiederherstellung von Security Manager Daten.
- **Info** – Zeigt Versionsinformationen zu Security Manager an.

Festlegen der Einstellungen

Sie können die Einstellungen für HP ProtectTools Security Manager personalisieren. Klicken Sie in der Security Manager Benutzer-Konsole auf **Erweitert** und anschließend auf **Voreinstellungen**. Die

verfügbaren Einstellungen werden auf zwei Registerkarten angezeigt: **Allgemein** und **Fingerabdruck**.

Registerkarte „Allgemein“

Darstellung – Symbol im Infobereich der Taskleiste anzeigen

- Um die Anzeige des Symbols in der Taskleiste zu aktivieren, aktivieren Sie dieses Kontrollkästchen.
- Um die Anzeige des Symbols in der Taskleiste zu deaktivieren, deaktivieren Sie dieses Kontrollkästchen.

Registerkarte „Fingerabdruck“

HINWEIS: Die Registerkarte **Fingerabdruck** ist nur verfügbar, wenn der Computer über ein Fingerabdruck-Lesegerät verfügt und der korrekte Treiber installiert ist.

- **Schnellaktionen** – Hiermit können Sie die Security Manager-Aufgaben auswählen, die ausgeführt werden sollen, wenn Sie eine bestimmte Taste gedrückt halten, während Sie mit dem Finger über den Sensor streichen.

  Um eine Schnellaktion zu einer der aufgelisteten Tastenkombinationen hinzuzufügen, klicken Sie auf eine der Optionen **(Taste) + Fingerabdruck**, und wählen Sie eine der verfügbaren Aufgaben aus dem Menü aus.

- **Fingerabdruckscan-Feedback** – Wird nur angezeigt, wenn ein Fingerabdruck-Lesegerät verfügbar ist. Verwenden Sie diese Einstellung, um das Feedback anzupassen, das Sie erhalten, wenn Sie mit dem Finger über den Sensor streichen.

  - **Sound-Feedback aktivieren** – Security Manager gibt akustische Signale aus, wenn ein Fingerabdruck durch Streichen über den Sensor registriert wurde, wobei für spezifische Programmereignisse verschiedene Signale verwendet werden. Sie können diesen Ereignissen auf der Registerkarte **Sounds** in der Einstellung „Sound“ der Windows Systemsteuerung andere Töne zuweisen oder akustische Signale ausschalten, indem Sie diese Option deaktivieren.
  - **Feedback zur Scanqualität anzeigen**

    Um alle Scans unabhängig von der Qualität anzuzeigen, aktivieren Sie das Kontrollkästchen.

    Um nur Scans guter Qualität anzuzeigen, deaktivieren Sie das Kontrollkästchen.

Sichern und Wiederherstellen Ihrer Daten

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

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

HINWEIS: Von dieser Funktion werden nur Password Manager- und Face Recognition-Daten gesichert. Drive Encryption benutzt eine eigene Sicherungsmehode. Von Daten des Device Access Manager und der Authentifizierung per Fingerabdruck wird keine Sicherung erstellt.

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

So sichern Sie Ihre Daten:

1. Öffnen Sie die Security Manager Benutzer-Konsole. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
2. Klicken Sie im linken Bereich der Benutzer-Konsole auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Daten sichern**.
4. Wählen Sie die Module aus, die gesichert werden sollen. In den meisten Fällen empfiehlt es sich, alle Module auszuwählen.
5. Identität bestätigen.
6. Geben Sie einen Namen für die Speicherdatei ein. Die Datei wird standardmäßig im Ordner „Dokumente“ gespeichert. Klicken Sie auf **Durchsuchen**, um einen anderen Speicherort anzugeben.
7. Geben Sie ein Kennwort ein, um die Datei zu schützen.
8. Klicken Sie auf **Fertig stellen**.

So stellen Sie Ihre Daten wieder her:

1. Öffnen Sie die Security Manager Benutzer-Konsole. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
2. Klicken Sie im linken Bereich der Benutzer-Konsole auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Daten wiederherstellen**.
4. Wählen Sie die zuvor erstellte Speicherdatei aus. Geben Sie den Pfad in das entsprechende Feld ein, oder klicken Sie auf **Durchsuchen**.
5. Geben Sie das zuvor verwendete Kennwort zum Schützen der Datei ein.
6. Wählen Sie die Module aus, deren Daten wiederhergestellt werden sollen. In den meisten Fällen empfiehlt es sich, alle aufgeführten Module auszuwählen.
7. Bestätigen Sie Ihr Windows Kennwort.
8. Klicken Sie auf **Fertig stellen**.

6 Drive Encryption for HP ProtectTools (bestimmte Modelle)

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

Mit HP ProtectTools Security Manager (HP Client Security Setup Wizard, Advanced Setup Wizard oder Administrator-Konsole) können Windows Administratoren Drive Encryption aktivieren, den Verschlüsselungsschlüssel sichern und Laufwerke bzw. Partitionen auswählen oder deaktivieren. Weitere Informationen finden Sie in der Hilfe zur Software HP ProtectTools Security Manager.

Die folgenden Aufgaben können mit Drive Encryption durchgeführt werden:

- Auswählen von Einstellungen für Drive Encryption:
  - TPM-geschütztes Kennwort aktivieren
  - Einzelne Laufwerke oder Partitionen mit der Software-Verschlüsselung verschlüsseln oder entschlüsseln
  - Einzelne selbstverschlüsselnde Laufwerke mit der Hardware-Verschlüsselung verschlüsseln oder entschlüsseln
  - Für zusätzliche Sicherheit durch Deaktivieren des Energiespar- oder Standby-Modus sorgen, um sicherzustellen, dass stets die Systemstart-Authentifizierung in Drive Encryption erforderlich ist

HINWEIS: Es können nur interne SATA- und externe eSATA-Festplatten verschlüsselt werden.

- Erstellen von Sicherungsschlüsseln
- Wiederherstellen des Zugriffs auf einen verschlüsselten Computer mithilfe von Sicherungsschlüsseln und HP SpareKey
- Aktivieren der Systemstart-Authentifizierung von Drive Encryption per Kennwort, registriertem Fingerabdruck oder Smart Card-PIN für ausgewählte Smart Cards

Öffnen von Drive Encryption

Administratoren können durch Öffnen der HP ProtectTools Security Manager Benutzer-Konsole auf Drive Encryption zugreifen.

1. Doppelklicken Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools**.

   – oder –

   Klicken Sie in der **Systemsteuerung** auf **System und Sicherheit**, und wählen Sie **HP ProtectTools Security Manager** aus.

2. Klicken Sie im linken Bereich der Benutzer-Konsole auf **Verwaltung** und anschließend auf **Administrator-Konsole**.

3. Klicken Sie im linken Bereich der HP ProtectTools Administrator-Konsole auf **Drive Encryption**.

Allgemeine Aufgaben

Aktivieren von Drive Encryption für Standard-Festplatten

Standard-Festplatten werden mithilfe der Software-Verschlüsselung verschlüsselt. Gehen Sie folgendermaßen vor, um Drive Encryption zu aktivieren:

1. Starten Sie **HP ProtectTools Administor-Konsole**. Weitere Informationen finden Sie unter „Öffnen der HP ProtectTools Administrator-Konsole“ auf Seite 18.

2. Klicken Sie im linken Bereich auf **Installations-Assistent**.

3. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.

4. Schließen Sie zum Sichern des Verschlüsselungsschlüssels ein externes Gerät an, auf dem der Schlüssel gespeichert werden soll. Dieser Schlüssel muss für den Datenzugriff verwendet werden, wenn anderen Methoden fehlschlagen.

5. Aktivieren Sie unter **Drive Encryption-Schlüssel sichern** das Kontrollkästchen für das Speichergerät, auf dem der Verschlüsselungsschlüssel gespeichert werden soll.

6. Klicken Sie auf **Weiter**.

HINWEIS: Sie werden dazu aufgefordert, den Computer neu zu starten. Nach dem Einleiten des Neustarts wird der Bildschirm für den Systemstart von Drive Encryption angezeigt, über den Sie sich vor dem Start von Windows authentifizieren müssen.

Drive Encryption wurde aktiviert. Die Verschlüsselung der ausgewählten Laufwerkspartitionen kann einige Stunden dauern. Dies hängt von der Anzahl und der Größe der jeweiligen Partitionen ab.

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

Aktivieren von Drive Encryption für selbstverschlüsselnde Laufwerke

Selbstverschlüsselnde Laufwerke, die den OPAL-Spezifikationen der Trusted Computing Group für die Verwaltung von selbstverschlüsselnden Laufwerken entsprechen, können entweder mit der Software- oder der Hardware-Verschlüsselung verschlüsselt werden. Gehen Sie folgendermaßen vor, um Drive Encryption für selbstverschlüsselnde Laufwerke zu aktivieren:

HINWEIS: Hardware-Verschlüsselung ist nur verfügbar, wenn es sich bei ALLEN Laufwerken auf Ihrem Computer um selbstverschlüsselnde Laufwerke handelt, die den OPAL-Spezifikationen der Trusted Computing Group für die Verwaltung selbstverschlüsselnder Laufwerke entsprechen. In diesem Fall ist die Option **Hardware-Verschlüsselung für Laufwerk verwenden** verfügbar, und es kann sowohl die Hardware-Verschlüsselung als auch die Software-Verschlüsselung durchgeführt werden.

Wenn sowohl selbstverschlüsselnde als auch Standardfestplatten vorhanden sind, ist die Option **Hardware-Verschlüsselung für Laufwerk verwenden** nicht verfügbar. Nur die Software-Verschlüsselung kann verwendet werden. Weitere Informationen finden Sie unter „Aktivieren von Drive Encryption für Standard-Festplatten“ auf Seite 46.

- Verwenden Sie den Installations-Assistenten von HP ProtectTools Security Manager, um Drive Encryption zu aktivieren.

– oder –

Software-Verschlüsselung

1. Starten Sie **HP ProtectTools Administor-Konsole**. Weitere Informationen finden Sie unter „Öffnen der HP ProtectTools Administrator-Konsole“ auf Seite 18.
2. Klicken Sie im linken Bereich auf **Installations-Assistent**.
3. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.

   HINWEIS: Wenn die Option **Hardware-Verschlüsselung für Laufwerk verwenden** unten im Bildschirm angezeigt wird, deaktivieren Sie das Kontrollkästchen.
4. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die zu verschlüsselnde Festplatte, und klicken Sie dann auf **Weiter**.
5. Um den Verschlüsselungsschlüssel zu sichern, schließen Sie das Speichergerät an den entsprechenden Steckplatz an.
6. Aktivieren Sie unter **Drive Encryption-Schlüssel sichern** das Kontrollkästchen für das Speichergerät, auf dem der Verschlüsselungsschlüssel gespeichert werden soll.
7. Klicken Sie auf **Übernehmen**.

   HINWEIS: Der Computer wird neu gestartet.

   Drive Encryption ist aktiviert. Die Verschlüsselung des Laufwerks kann je nach Größe des Laufwerks einige Stunden in Anspruch nehmen.

Hardware-Verschlüsselung

1. Starten Sie **HP ProtectTools Administor-Konsole**. Weitere Informationen finden Sie unter „Öffnen der HP ProtectTools Administrator-Konsole“ auf Seite 18.
2. Klicken Sie im linken Bereich auf **Installations-Assistent**.
3. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.
4. Wenn das Kontrollkästchen **Hardware-Verschlüsselung für Laufwerk verwenden** unten im Bildschirm angezeigt wird, vergewissern Sie sich, dass es aktiviert ist.

   Wenn das Kontrollkästchen deaktiviert ist oder nicht angezeigt wird, wird die Software-Verschlüsselung durchgeführt. Weitere Informationen finden Sie unter „Aktivieren von Drive Encryption für Standard-Festplatten“ auf Seite 46.

5. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die zu verschlüsselnde Festplatte, und klicken Sie dann auf **Weiter**.

HINWEIS: Wenn nur ein Laufwerk angezeigt wird, wird das Kontrollkästchen für das Laufwerk automatisch ausgewählt und abgeblendet.

Wird mehr als ein Laufwerk angezeigt, so wird Datenträger 0 ebenfalls automatisch ausgewählt und ausgeblendet. Die Option für die Auswahl weiterer Festplatten für die Hardware-Verschlüsselung ist jedoch verfügbar.

Die Schaltfläche **Weiter** ist nur dann verfügbar, wenn mindestens ein Laufwerk ausgewählt ist.

6. Um den Verschlüsselungsschlüssel zu sichern, schließen Sie das Speichergerät an den entsprechenden Steckplatz an.
7. Aktivieren Sie unter **Drive Encryption-Schlüssel sichern** das Kontrollkästchen für das Speichergerät, auf dem der Verschlüsselungsschlüssel gespeichert werden soll.
8. Klicken Sie auf **Übernehmen**.

HINWEIS: Sie werden dazu aufgefordert, den Computer neu zu starten. Es wird der Systemstart von Drive Encryption angezeigt, über den Sie sich vor dem Start von Windows authentifizieren müssen.

Drive Encryption ist aktiviert. Die Verschlüsselung des Laufwerks kann einige Minuten in Anspruch nehmen.

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

Deaktivieren von Drive Encryption

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

1. Starten Sie **HP ProtectTools Administor-Konsole**. Weitere Informationen finden Sie unter „Öffnen der HP ProtectTools Administrator-Konsole“ auf Seite 18.
2. Klicken Sie im linken Bereich auf **Installations-Assistent**.
3. Deaktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.

Die Deaktivierung von Drive Encryption wird gestartet.

HINWEIS: Wenn Software-Verschlüsselung verwendet wurde, wird die Entschlüsselung gestartet. Dies kann einige Stunden dauern, je nach der Größe der verschlüsselten Festplattenpartitionen. Sobald die Entschlüsselung abgeschlossen ist, wird Drive Encryption deaktiviert.

Wenn Hardware-Verschlüsselung verwendet wurde, wird das Laufwerk sofort entschlüsselt. Nach ein paar Minuten wird Drive Encryption deaktiviert.

Nach der Deaktivierung von Drive Encryption werden Sie dazu aufgefordert, den Computer herunterzufahren (bei Hardware-Verschlüsselung), oder den Computer neu zu starten (bei Software-Verschlüsselung).

Anmelden, nachdem Drive Encryption aktiviert wurde

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

HINWEIS: Bei der Reaktivierung aus dem Standby- oder dem Energiesparmodus wird die Systemstart-Authentifizierung von Drive Encryption sowohl bei Software- als auch bei Hardware-Verschlüsselung nicht angezeigt. Bei der Hardware-Verschlüsselung steht die Option **Energiesparmodus für höhere Sicherheit deaktivieren** zur Verfügung. Mit dieser Option wird verhindert, dass der Standby- oder Energiesparmodus eingeleitet wird.

Bei der Reaktivierung aus dem Ruhezustand wird die Systemstart-Authentifizierung von Drive Encryption sowohl bei Software- als auch bei Hardware-Verschlüsselung angezeigt.

HINWEIS: Wenn der Windows Administrator die BIOS-Authentifizierung vor dem Systemstart in HP ProtectTools Security Manager aktiviert hat und wenn die One Step-Anmeldung (standardmäßig) aktiviert ist, können Sie sich unmittelbar nach der BIOS-Authentifizierung vor dem Systemstart am Computer anmelden. Eine erneute Authentifizierung beim Drive Encryption-Anmeldebildschirm ist nicht erforderlich.

Anmeldung eines einzelnen Benutzers:

- Melden Sie sich auf der Seite **Anmelden** an, indem Sie entweder Ihr Windows Kennwort, Ihre Smart Card-PIN oder Ihren SpareKey eingeben oder mit einem registrierten Finger über den Sensor streichen oder in die Kamera blicken.

Anmeldung mehrerer Benutzer:

1. Wählen Sie auf der Seite **Benutzer für Anmeldung auswählen** den Benutzer aus der Dropdown-Liste aus, und klicken Sie anschließend auf **Weiter**.
2. Geben Sie auf der Seite **Anmelden** Ihr Windows Kennwort oder Ihre Smart Card-PIN ein, oder streichen Sie mit einem registrierten Finger über den Sensor.

HINWEIS: Folgende Smart Cards werden unterstützt:

Unterstützte Smart Cards

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

HINWEIS: Wenn der Wiederherstellungsschlüssel für die Anmeldung im Drive Encryption-Anmeldebildschirm verwendet wird, sind zusätzliche Anmeldedaten für die Anmeldung bei Windows erforderlich, um Zugriff auf Benutzerkonten zu erhalten.

Schützen Ihrer Daten durch Verschlüsselung der Festplatte

Es wird empfohlen, den Installations-Assistenten von HP ProtectTools Security Manager zu verwenden, um Daten durch Verschlüsselung der Festplatte zu schützen. Nach der Aktivierung können alle hinzugefügten Festplatten oder Partitionen folgendermaßen verschlüsselt werden:

1. Klicken Sie im linken Bereich auf das Symbol **+** links neben **Drive Encryption**, um die verfügbaren Optionen anzuzeigen.
2. Klicken Sie auf **Einstellungen**.
3. Wählen Sie für Laufwerke mit Software-Verschlüsselung die zu verschlüsselnden Laufwerkspartitionen aus.

HINWEIS: Dies trifft auch auf ein Szenario mit verschiedenen Laufwerken zu, bei dem eine oder mehrere Standard-Festplatten und ein oder mehrere selbstverschlüsselnde Laufwerke vorhanden sind.

– oder –

▲ Bei Laufwerken mit Hardware-Verschlüsselung wählen Sie die zusätzlichen Laufwerke für die Verschlüsselung aus.

Erweiterte Aufgaben

Verwalten von Drive Encryption (Administrator-Aufgabe)

Auf der Seite „Einstellungen“ unter Drive Encryption können Administratoren den Status von Drive Encryption anzeigen und ändern (aktiviert, deaktiviert oder Hardware-Verschlüsselung wurde aktiviert) und den Verschlüsselungsstatus aller Festplatten auf dem Computer anzeigen.

HINWEIS: Auf der Seite „Drive Encryption Einstellungen“ können nur zusätzliche Festplatten für die Hardware-Verschlüsselung ausgewählt oder deaktiviert werden.

- Wenn der Status deaktiviert ist, wurde Drive Encryption noch nicht vom Windows Administrator aktiviert, und der Festplattenschutz ist nicht aktiv. Verwenden Sie den Installations-Assistenten von HP ProtectTools Security Manager, um Drive Encryption zu aktivieren.
- Wenn der Status „Aktiviert“ lautet, wurde Drive Encryption aktiviert und konfiguriert. Das Laufwerk befindet sich in einem der folgenden Zustände:

Software-Verschlüsselung

- Nicht verschlüsselt
- Verschlüsselt
- Wird gerade verschlüsselt
- Wird gerade entschlüsselt

Hardware-Verschlüsselung

- Verschlüsselt
- Nicht verschlüsselt (für zusätzliche Laufwerke)

Nutzung von erweiterten Sicherheitsfunktionen mit TPM (bestimmte Modelle)

Wenn Sie das Trusted Platform Module (TPM) aktiviert und Drive Encryption Enhanced Security mit TPM -Funktionalität ausgewählt haben, wird das Drive Encryption-Kennwort durch den TPM-Sicherheitschip geschützt. Der Zugriff auf das Laufwerk wird verweigert, sobald die Festplatte entfernt und in einen anderen Computer eingebaut wird.

ACHTUNG: Die TPM-Besitzrechte können nicht mit der Windows TPM-Verwaltung (TPM.msc) geteilt werden.

HINWEIS: Das Kennwort ist durch den TPM-Sicherheitschip (TPM) geschützt. Wenn die Festplatte an einen anderen Computer angeschlossen wird, ist der Zugriff auf die Daten nur dann möglich, wenn die TPM-Einstellungen auf diesen Computer migriert werden.

HINWEIS: Die TPM-Option muss im BIOS-Setup aktiviert sein.

Ver- und Entschlüsseln einzelner Laufwerkspartitionen (nur für Software-Verschlüsselung)

Administratoren können auf der Seite „Drive Encryption Einstellungen“ eine oder mehrere Festplattenpartitionen auf dem Computer verschlüsseln oder bereits verschlüsselte Laufwerkspartitionen entschlüsseln.

1. Starten Sie **HP ProtectTools Administor-Konsole**. Weitere Informationen finden Sie unter „Öffnen der HP ProtectTools Administrator-Konsole“ auf Seite 18.
2. Klicken Sie im linken Bereich auf das Symbol **+** links neben **Drive Encryption**, um die verfügbaren Optionen anzuzeigen.
3. Klicken Sie auf **Einstellungen**.
4. Aktivieren oder deaktivieren Sie unter **Laufwerkstatus** das Kontrollkästchen neben dem entsprechenden zu ver- oder entschlüsselnden Laufwerk, und klicken Sie dann auf **Übernehmen**.

HINWEIS: Wenn eine Partition gerade verschlüsselt oder entschlüsselt wird, wird eine Fortschrittsanzeige angezeigt, auf der zu sehen ist, zu wieviel Prozent die Partition bereits verschlüsselt ist und wie lange der Vorgang noch dauern wird.

HINWEIS: Dynamische Partitionen werden nicht unterstützt. Wenn eine Partition als verfügbar angezeigt wird, jedoch nach Auswahl nicht verschlüsselt werden kann, handelt es sich um eine dynamische Partition. Eine dynamische Partition ist das Ergebnis einer Partitionsverkleinerung, um in der Datenträgerverwaltung eine neue Partition zu erstellen.

Wenn eine Partition in eine dynamische Partition konvertiert werden soll, wird eine Warnung angezeigt.

Sicherung und Wiederherstellung (Administrator-Aufgabe)

Wenn Drive Encryption aktiviert ist, können Administratoren die Seite „Sichern von Verschlüsselungsschlüssel“ verwenden, um Verschlüsselungsschlüssel auf Wechselmedien zu sichern und von dort wiederherzustellen.

Sichern von Verschlüsselungsschlüsseln

Administratoren können den Verschlüsselungsschlüssel für ein verschlüsseltes Laufwerk auf einem Wechselmedium sichern.

ACHTUNG: Bewahren Sie das Speichergerät mit dem Sicherungsschlüssel an einem sicheren Ort auf. Wenn Sie das Kennwort vergessen, Ihre Smart Card verlieren oder keinen Fingerabdruck registriert haben, haben Sie nur mit diesem Gerät Zugriff auf den Computer. Der Aufbewahrungsort sollte für unbefugte Personen nicht zugänglich sein, denn das Speichergerät ermöglicht den Zugriff auf Windows.

HINWEIS: Zum Speichern des Verschlüsselungsschlüssels müssen Sie ein USB-Speichergerät mit FAT32 oder FAT16 verwenden. Für die Sicherung kann ein USB Memory Stick, eine Secure Digital (SD) Memory Card oder eine MultiMedia Card (MMC) verwendet werden.

1. Starten Sie **HP ProtectTools Administor-Konsole**. Weitere Informationen finden Sie unter „Öffnen der HP ProtectTools Administrator-Konsole“ auf Seite 18.
2. Klicken Sie im linken Bereich auf das Symbol **+** links neben **Drive Encryption**, um die verfügbaren Optionen anzuzeigen.
3. Klicken Sie auf **Sichern von Verschlüsselungsschlüsseln**.

4. Schließen Sie das für die Sicherung des Verschlüsselungsschlüssels gewünschte Speichergerät an.

HINWEIS: Zum Speichern des Verschlüsselungsschlüssels müssen Sie ein USB-Speichergerät mit FAT32-Formatierung verwenden. Für die Sicherung kann ein USB Memory Stick, eine Secure Digital (SD)-Speicherkarte oder eine MultiMedia Card (MMC) verwendet werden. In einigen Fällen kann auch SkyDrive verwendet werden.

5. Aktivieren Sie unter **Laufwerk** das Kontrollkästchen für das Gerät, auf dem Ihr Verschlüsselungsschlüssel gesichert werden soll.

6. Klicken Sie auf **Schlüssel sichern**.

7. Lesen Sie den Text auf der angezeigten Seite, und klicken Sie dann auf **OK**. Der Verschlüsselungsschlüssel wird auf dem von Ihnen ausgewählten Speichergerät gespeichert.

Wiederherstellen des Zugriffs auf einen Computer, auf dem Drive Encryption aktiviert ist, mithilfe von Sicherungsschlüsseln

Administratoren können eine Wiederherstellung mithilfe des Drive Encryption-Schlüssels durchführen, der bei der Aktivierung auf einem Wechselmediengerät gesichert wird, oder indem sie die Option **Sichern der Drive Encryption Schlüssel** in Security Manager auswählen.

1. Schließen Sie das Wechselmediengerät an, das Ihren Sicherungsschlüssel enthält.

2. Schalten Sie den Computer ein.

3. Klicken Sie im Anmeldedialogfeld von Drive Encryption for HP ProtectTools auf **Optionen**.

4. Klicken Sie auf **Wiederherstellung**.

5. Geben Sie den Pfad oder den Namen der Datei ein, die Ihren Sicherungsschlüssel enthält, und klicken Sie anschließend auf **Wiederherstellen**.

   – oder –

   Klicken Sie auf **Durchsuchen**, um nach der erforderlichen Sicherungsdatei zu suchen. Klicken Sie dann auf **OK** und anschließend auf **Wiederherstellen**.

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

   Der Anmeldebildschirm von Windows wird angezeigt.

HINWEIS: Wenn der Wiederherstellungsschlüssel für die Anmeldung im Drive Encryption-Anmeldebildschirm verwendet wird, sind zusätzliche Anmeldedaten für die Anmeldung bei Windows erforderlich, um Zugriff auf Benutzerkonten zu erhalten. Nach der Wiederherstellung sollten Sie Ihr Kennwort unbedingt zurücksetzen.

Durchführen einer HP SpareKey-Wiederherstellung

Für die SpareKey-Wiederherstellung während des Systemstarts mit Drive Encryption ist es erforderlich, dass Sie zunächst die Sicherheitsfragen richtig beantworten, bevor Sie auf den Computer zugreifen können. Weitere Informationen zum Einrichten der SpareKey-Wiederherstellung finden Sie in der Hilfe zur Security Manager-Software.

So führen Sie eine HP SpareKey-Wiederherstellung durch, wenn Sie Ihr Kennwort vergessen haben:

1. Schalten Sie den Computer ein.

2. Wenn die Seite „Drive Encryption for HP ProtectTools“ angezeigt wird, navigieren Sie zu der Seite für die Benutzeranmeldung.

3. Klicken Sie auf **SpareKey**.

HINWEIS: Wenn der SpareKey noch nicht in Security Manager initialisiert wurde, ist die Schaltfläche **SpareKey** nicht verfügbar.

4. Geben Sie die richtigen Antworten auf die angezeigten Fragen ein, und klicken Sie anschließend auf **Anmelden**.

   Der Anmeldebildschirm von Windows wird angezeigt.

HINWEIS: Wenn der SpareKey für die Anmeldung auf dem Drive Encryption-Anmeldebildschirm verwendet wird, sind zusätzliche Anmeldedaten für die Anmeldung bei Windows erforderlich, um Zugriff auf Benutzerkonten zu erhalten. Nach der Wiederherstellung sollten Sie Ihr Kennwort unbedingt zurücksetzen.

Anzeigen des Verschlüsselungsstatus

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

HINWEIS: Administratoren können den Drive Encryption-Status mithilfe von HP ProtectTools Administrator-Konsole ändern.

1. Starten Sie die **HP ProtectTools Benutzer-Konsole**. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
2. Klicken Sie unter **Meine Daten** auf **Drive Encryption**.

   Bei Software- oder Hardware-Verschlüsselung wird eine der folgenden Statusmeldungen für die Laufwerksverschlüsselung angezeigt:

   - Aktiviert
   - Deaktiviert

   Bei der Software-Verschlüsselung wird eine der folgenden Statusmeldungen für die Laufwerksverschlüsselung jeder einzelnen Festplatte oder Festplattenpartition angezeigt:

   - Nicht verschlüsselt
   - Verschlüsselt
   - Wird gerade verschlüsselt
   - Wird gerade entschlüsselt

   Bei der Hardware-Verschlüsselung wird eine der folgenden Statusmeldungen für die Laufwerksverschlüsselung angezeigt:

   - Nicht verschlüsselt
   - Verschlüsselt

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

7 Device Access Manager for HP ProtectTools (bestimmte Modelle)

Mithilfe von HP ProtectTools Device Access Manager kann der Datenzugriff gesteuert werden, indem Datenübertragungsgeräte deaktiviert werden.

HINWEIS: Einige Schnittstellen/Eingabegeräte für die Benutzerinteraktion, wie Maus, Tastatur, TouchPad und Fingerabdruck-Lesegeräte, können nicht über Device Access Manager gesteuert werden. Weitere Informationen finden Sie unter „Nicht verwaltete Geräteklassen“ auf Seite 64.

Windows® Administratoren verwenden HP ProtectTools Device Access Manager, um den Zugriff auf die Geräte eines Systems zu steuern und einen unbefugten Zugriff zu verhindern:

- Für jeden Benutzer werden Geräteprofile erstellt. Diese definieren, auf welche Geräte der Benutzer Zugriff bzw. keinen Zugriff hat.
- Mittels Just-In-Time-Authentifizierung (JITA) können sich vordefinierte Benutzer authentifizieren, um Zugriff auf Geräte zu erhalten, die normalerweise gesperrt sind.
- Administratoren und vertrauenswürdige Benutzer können aus den Beschränkungen für den Gerätezugriff durch Device Access Manager ausgenommen werden, indem sie zur Gruppe „Geräte-Administratoren“ hinzugefügt werden. Die Mitgliedschaft in dieser Gruppe wird über „Erweiterte Einstellungen“ verwaltet.
- Der Gerätezugriff kann auf der Grundlage der Gruppenzugehörigkeit bzw. für einzelne Benutzer erteilt oder verweigert werden.
- Für Geräteklassen, wie z. B. CD-ROM- und DVD-Laufwerke, können unterschiedliche Rechte für Lese- und Schreibzugriff erteilt werden.

Öffnen von Device Access Manager

1. Melden Sie sich als Administrator an.
2. Starten Sie **HP ProtectTools Security Manager** vom **HP Client Security Dashboard** aus.

   – oder –

   Doppelklicken Sie auf dem Windows Desktop im Infobereich ganz rechts in der Taskleiste auf das Symbol **HP ProtectTools**.

   – oder –

   Klicken Sie in der **Systemsteuerung** auf **System und Sicherheit**, und wählen Sie **HP ProtectTools Security Manager** aus.
3. Klicken Sie im linken Bereich der HP ProtectTools Security Manager Benutzer-Konsole auf **Verwaltung** und anschließend auf **Administrator-Konsole**.
4. Klicken Sie im linken Bereich der Administrator-Konsole auf **Device Access Manager**.

Ein Standardbenutzer kann die HP ProtectTools Device Access Manager-Richtlinie mit HP ProtectTools Security Manager anzeigen. Mit dieser Konsole ist nur eine schreibgeschützte Ansicht möglich.

Setup-Verfahren

Konfigurieren von Zugriffrechten auf Geräte

In HP ProtectTools Device Access Manager sind vier Ansichten verfügbar:

- **Einfache Konfiguration** – Zum Erteilen oder Verweigern des Zugriffs auf Geräteklassen auf der Grundlage der Mitgliedschaft in der Gruppe „Geräte-Administratoren“.
- **Geräteklassen-Konfiguration** – Zum Erteilen oder Verweigern des Zugriffs auf Gerätetypen oder bestimmte Geräte für bestimmte Benutzer oder Gruppen.
- **JITA-Konfiguration** – Zum Konfigurieren der Just-In-Time-Authentifizierung (JITA), um ausgewählten Benutzern den Zugriff auf DVD-/CD-ROM-Laufwerke oder Wechselmedien zu erlauben, wenn sie sich authentifizieren.
- **Erweiterte Einstellungen** – Zum Konfigurieren einer Liste mit Laufwerksbuchstaben, für die der Zugriff durch Device Access Manager nicht beschränkt wird, wie beispielsweise das Laufwerk C (Systemlaufwerk). In dieser Ansicht kann außerdem die Mitgliedschaft in der Gruppe „Geräte-Administratoren“ verwaltet werden.

Einfache Konfiguration

Administratoren können die Ansicht **Einfache Konfiguration** verwenden, um den Zugriff auf die folgenden Geräteklassen für alle Benutzer, die keine Geräteadministratoren sind, zu erteilen oder zu verweigern:

- Alle Wechselmedien (Disketten, USB-Flash-Laufwerke usw.)
- Alle DVD-/CD-ROM-Laufwerke
- Alle seriellen und parallelen Anschlüsse
- Alle Bluetooth-Geräte

HINWEIS: Wenn Bluetooth Geräte als Authentifizierungsinformationen genutzt werden, sollte der Zugriff auf Bluetooth Geräte in der Device Access Manager-Richtlinie nicht eingeschränkt werden.

- Alle Modems
- Alle PCMCIA-/ExpressCard-Geräte
- Alle 1394-Geräte

So erteilen oder verweigern Sie allen Benutzern, die keine Geräte-Administratoren sind, den Zugriff auf eine Geräteklasse:

1. Klicken Sie im linken Bereich der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Einfache Konfiguration**.
2. Um den Zugriff zu verweigern, aktivieren Sie im rechten Fensterausschnitt das Kontrollkästchen für eine Geräteklasse oder ein bestimmtes Gerät. Deaktivieren Sie das Kontrollkästchen, um den Zugriff auf die Geräteklasse oder das Gerät zu erteilen.

   Wenn ein Kontrollkästchen abgeblendet dargestellt wird, wurden die Werte, die sich auf das Zugriffsszenario auswirken, innerhalb der Ansicht **Geräteklassen-Konfiguration** geändert. Klicken Sie zum Wiederherstellen der Werkseinstellungen in der Ansicht **Geräteklassen-Konfiguration** auf **Zurücksetzen**.

3. Klicken Sie auf **Übernehmen**.

HINWEIS: Wenn der Hintergrunddienst nicht aktiv ist, werden Sie gefragt, ob Sie den Dienst starten möchten. Klicken Sie auf **Ja**.

4. Klicken Sie auf **OK**.

Starten des Hintergrunddienstes

Wenn das erste Mal eine neue Richtlinie festgelegt und angewendet wird, startet der Hintergrunddienst „HP ProtectTools Gerätesperre/Überwachung“ automatisch und ist so eingestellt, dass er bei jedem Systemstart automatisch startet.

HINWEIS: Bevor die Eingabeaufforderung für den Hintergrunddienst angezeigt wird, muss ein Geräteprofil definiert werden.

Administratoren können diesen Dienst auch starten oder stoppen.

Wenn Sie den Dienst „Gerätesperre/Überwachung“ stoppen, bleibt die Gerätesperre erhalten. Die Gerätesperre wird durch zwei Komponenten in Kraft gesetzt:

- Den Dienst „Gerätesperre/Überwachung“
- Den Treiber DAMDrv.sys

Wenn Sie den Dienst starten, wird auch der Gerätetreiber gestartet. Der Treiber jedoch nicht gestoppt, wenn Sie den Dienst stoppen.

Um festzustellen, ob der Hintergrunddienst aktiv ist, öffnen Sie ein Eingabeaufforderungsfenster, und geben Sie `sc query flcdlock` ein.

Um festzustellen, ob der Gerätetreiber aktiv ist, öffnen Sie ein Eingabeaufforderungsfenster, und geben Sie `sc query damdrv` ein.

Geräteklassen-Konfiguration

Administratoren können Listen mit Benutzern und Gruppen, die Zugriff bzw. keinen Zugriff auf Geräteklassen oder bestimmte Geräte haben, anzeigen und ändern.

Die Ansicht **Geräteklassen-Konfiguration** besteht aus den folgenden Bereichen:

- **Geräteliste** – Zeigt alle Geräteklassen und Geräte an, die auf dem System installiert sind oder bereits auf dem System installiert waren.
  - In der Regel erstreckt sich der Schutz auf eine Geräteklasse. Ein ausgewählter Benutzer oder eine ausgewählte Gruppe kann auf alle Geräte der Geräteklasse zugreifen.
  - Es besteht außerdem die Möglichkeit, bestimmte Geräte zu schützen.
- **Benutzerliste** – Zeigt alle Benutzer und Gruppen an, denen Zugriff auf die gewählte Geräteklasse bzw. ein bestimmtes Gerät gewährt oder verweigert wurde.
  - Der Eintrag in der Benutzerliste kann sich auf einen bestimmten Benutzer oder auf eine Gruppe beziehen, zu der der Benutzer gehört.
  - Wenn ein Benutzer- oder Gruppeneintrag in der Benutzerliste nicht verfügbar ist, wurden die Einstellungen übernommen, die für die Geräteklasse in der Geräteliste oder im Ordner „Klassen“ festgelegt wurden.
  - Der Zugriff auf einige Geräteklassen (z. B. DVD- und CD-ROM-Laufwerke) kann auch gesteuert werden, indem unterschiedliche Rechte für Lese- und Schreibzugriff erteilt werden.

Für andere Geräte und Klassen können die Rechte für Lese- und Schreibzugriff übernommen werden. Beispielsweise kann der Lesezugriff von einer höheren Klasse übernommen werden, aber der Schreibzugriff kann speziell für einen Benutzer oder eine Gruppe verweigert werden.

HINWEIS: Ein deaktiviertes Kontrollkästchen **Lesen** bedeutet, dass der Eintrag für die Zugriffssteuerung keine Auswirkung auf den Lesezugriff auf das Gerät hat. Der Lesezugriff wird jedoch nicht verweigert.

HINWEIS: Die Gruppe „Administratoren“ kann nicht zur „Benutzerliste“ hinzugefügt werden. Verwenden Sie stattdessen die Gruppe „Geräte-Administratoren“.

Beispiel 1: Einem Benutzer oder einer Gruppe wird Schreibzugriff auf ein Gerät oder eine Geräteklasse verweigert:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Schreib- oder Lese-/Schreibzugriff für ein Gerät erteilt werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Beispiel 2: Einem Benutzer oder einer Gruppe wird Schreibzugriff auf ein Gerät oder eine Geräteklasse gewährt:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Schreib- oder Lese-/Schreibzugriff für das Gerät selbst oder ein Gerät verweigert werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Beispiel 3: Einem Benutzer oder einer Gruppe wird Lesezugriff auf ein Gerät oder eine Geräteklasse gewährt:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Lese- oder Lese-/Schreibzugriff für das Gerät selbst oder ein Gerät verweigert werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Beispiel 4: Einem Benutzer oder einer Gruppe wird Lesezugriff auf ein Gerät oder eine Geräteklasse verweigert:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Lese- oder Lese-/Schreibzugriff für ein Gerät erteilt werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Beispiel 5: Einem Benutzer oder einer Gruppe wird Lese-/Schreibzugriff auf ein Gerät oder eine Geräteklasse gewährt:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Schreib- oder Lese-/Schreibzugriff für das Gerät selbst oder ein Gerät verweigert werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Beispiel 6: Einem Benutzer oder einer Gruppe wird Lese-/Schreibzugriff auf ein Gerät oder eine Geräteklasse verweigert:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Lese- oder Lese-/Schreibzugriff für ein Gerät erteilt werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Zugriff für Benutzer oder Gruppe verweigern

Gehen Sie folgendermaßen vor, um einem Benutzer oder einer Gruppe den Zugriff auf ein Gerät oder eine Geräteklasse zu verwehren:

1. Klicken Sie im linken Bereich der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die konfiguriert werden soll.
   - **Geräteklasse**
   - **Alle Geräte**
   - **Einzelnes Gerät**
3. Wählen Sie unter **Benutzer/Gruppen** den Benutzer bzw. die Gruppe aus, der/die keinen Zugriff erhalten soll, und klicken Sie dann auf **Verweigern**.
4. Klicken Sie auf **Übernehmen**.

HINWEIS: Wenn für einen Benutzer auf derselben Geräteebene Zugriff verweigert und erteilt wird, hat die Zugriffsverweigerung Vorrang.

Zugriff für Benutzer oder Gruppe erteilen

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

1. Klicken Sie im linken Bereich der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf eines der folgenden Elemente:
   - **Geräteklasse**
   - **Alle Geräte**
   - **Einzelnes Gerät**
3. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Benutzer oder Gruppen auswählen** wird geöffnet.
4. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um nach Benutzern und Gruppen zu suchen, die hinzugefügt werden sollen.
5. Klicken Sie auf einen Benutzer oder eine Gruppe, der bzw. die zur Liste der verfügbaren Benutzer und Gruppen hinzugefügt werden soll, und klicken Sie anschließend auf **OK**.
6. Klicken Sie erneut auf **OK**.
7. Klicken Sie auf **Zulassen**, um diesem Benutzer Zugriff zu gewähren.
8. Klicken Sie auf **Übernehmen**.

Einem Benutzer einer Gruppe Zugriff auf eine Geräteklasse erteilen

Gehen Sie folgendermaßen vor, um einem Benutzer Zugriff auf eine Gerätklasse zu erteilen, während Sie allen anderen Mitgliedern der Gruppe den Zugriff verweigern:

1. Klicken Sie im linken Bereich der **HP ProtectTools Administrator-Konsole** auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die konfiguriert werden soll.
   - **Geräteklasse**
   - **Alle Geräte**
   - **Einzelnes Gerät**
3. Wählen Sie unter **Benutzer/Gruppen** die Gruppe aus, die keinen Zugriff erhalten soll, und klicken Sie dann auf **Verweigern**.
4. Navigieren Sie zu dem Ordner unter dem der erforderlichen Klasse, und fügen Sie den entsprechenden Benutzer hinzu.
5. Klicken Sie auf **Zulassen**, um diesem Benutzer Zugriff zu gewähren.
6. Klicken Sie auf **Übernehmen**.

Einem Benutzer einer Gruppe Zugriff auf ein bestimmtes Gerät erteilen

Administratoren können einem Benutzer den Zugriff auf ein bestimmtes Gerät gewähren, während sie allen anderen Mitgliedern der Gruppe den Zugriff auf alle Geräte verweigern, die in der Klasse enthalten sind:

1. Klicken Sie im linken Bereich der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die konfiguriert werden soll, und navigieren Sie zu dem Ordner darunter.
3. Klicken Sie unter **Benutzer/Gruppen** neben der Gruppe, die Zugriff erhalten soll, auf **Zulassen**.
4. Klicken Sie neben der Gruppe, die keinen Zugriff erhalten soll, auf **Verweigern**.
5. Navigieren Sie in der Geräteliste zu dem Gerät, auf das der Benutzer Zugriff erhalten soll.
6. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Benutzer oder Gruppen auswählen** wird geöffnet.
7. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um nach Benutzern und Gruppen zu suchen, die hinzugefügt werden sollen.
8. Klicken Sie auf einen Benutzer, der Zugriff erhalten soll, und dann auf **OK**.
9. Klicken Sie auf **Zulassen**, um diesem Benutzer Zugriff zu gewähren.
10. Klicken Sie auf **Übernehmen**.

Entfernen von Einstellungen für einen Benutzer oder eine Gruppe

So entziehen Sie einem Benutzer oder einer Gruppe die Zugriffsberechtigung für ein Gerät oder eine Geräteklasse:

1. Klicken Sie im linken Bereich der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die konfiguriert werden soll.
   - **Geräteklasse**
   - **Alle Geräte**
   - **Einzelnes Gerät**
3. Klicken Sie unter **Benutzer/Gruppen** auf den Benutzer bzw. die Gruppe, der bzw. die entfernt werden soll, und klicken anschließend auf **Entfernen**.
4. Klicken Sie auf **Übernehmen**.

Zurücksetzen der Konfiguration

ACHTUNG: Beim Zurücksetzen der Konfiguration werden alle Änderungen an der Gerätekonfiguration verworfen, und alle Werkseinstellungen werden wiederhergestellt.

HINWEIS: Die Seite „Erweiterte Einstellungen“ wird nicht zurückgesetzt.

So setzen Sie die Konfigurationseinstellungen auf die Werkseinstellungen zurück:

1. Klicken Sie im linken Bereich der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie auf **Zurücksetzen**.
3. Klicken Sie in der Bestätigungsaufforderung auf **Ja**.
4. Klicken Sie auf **Übernehmen**.

JITA-Konfiguration

Mithilfe der JITA-Konfiguration kann der Administrator Listen mit Benutzern und Gruppen anzeigen und bearbeiten, die unter Verwendung der Just-In-Time-Authentifizierung (JITA) auf Geräte zugreifen dürfen.

JITA-aktivierte Benutzer können auf einige Geräte zugreifen, für die in der Ansicht **Geräteklassen-Konfiguration** oder **Einfache Konfiguration** erstellte Richtlinien beschränkt wurden.

- **Szenario** – Eine Richtlinie für eine einfache Konfiguration wird konfiguriert, um allen Benutzern, die keine Geräte-Administratoren sind, Zugriff auf das DVD-/CD-ROM-Laufwerk zu verweigern.
- **Ergebnis** – Ein JITA-fähiger Benutzer, der auf das DVD-/CD-ROM-Laufwerk zugreifen möchte, erhält dieselbe Meldung aufgrund verweigerten Zugriffs wie ein Benutzer, der nicht für die Verwendung von JITA konfiguriert ist. Anschließend wird eine Ballon-Nachricht angezeigt mit der Frage, ob der Benutzer JITA-Zugriff möchte. Wenn der Benutzer auf den Ballon klickt, wird das Dialogfeld für die Benutzerauthentifizierung angezeigt. Gibt der Benutzer seine Anmeldeinformationen erfolgreich ein, wird der Zugriff auf das DVD-/CD-ROM-Laufwerk erteilt.

Der JITA-Zeitraum kann für eine festgelegte Anzahl an Minuten oder 0 Minuten genehmigt sein. Ein JITA-Zeitraum von 0 Minuten kann nicht ablaufen. Benutzer können ab dem Zeitpunkt der Authentifizierung bis zur Abmeldung vom System auf das Gerät zugreifen.

Der JITA-Zeitraum kann bei entsprechender Konfiguration auch verlängert werden. In diesem Szenario können Benutzer 1 Minute vor Ablauf des JITA-Zeitraums auf die Aufforderung klicken, um ihren Zugriff ohne erneute Authentifizierung zu verlängern.

Unabhängig davon, ob der Benutzer einen beschränkten oder unbeschränkten JITA-Zeitraum zur Verfügung hat, läuft der JITA-Zeitraum ab, wenn sich der Benutzer vom System abmeldet bzw. sich ein anderer Benutzer anmeldet. Wenn der Benutzer sich das nächste Mal anmeldet und versucht, auf ein JITA-aktiviertes Gerät zuzugreifen, wird eine Aufforderung zur Eingabe der Anmeldeinformationen angezeigt.

JITA ist für die folgenden Geräteklassen verfügbar:

- DVD-/CD-ROM-Laufwerke
- Wechselmedien

Erstellen einer JITA für einen Benutzer oder eine Gruppe

Administratoren können Benutzern oder Gruppen Zugriff auf Geräte mit der Just-In-Time-Authentifizierung erteilen.

1. Klicken Sie im linken Fensterausschnitt der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **JITA-Konfiguration**.
2. Wählen Sie im Dropdown-Menü des Geräts entweder **Wechselmedien** oder **DVD/CD-ROM-Laufwerke** aus.
3. Klicken Sie auf **+**, um einen Benutzer oder eine Gruppe zur JITA-Konfiguration hinzuzufügen.

4. Wählen Sie das Kontrollkästchen **Aktiviert** aus.
5. Legen Sie den JITA-Zeitraum auf den gewünschten Wert fest.
6. Klicken Sie auf **Übernehmen**.

Der Benutzer muss sich abmelden und erneut anmelden, damit die neue JITA-Einstellung übernommen wird.

Erstellen einer verlängerbaren JITA für einen Benutzer oder eine Gruppe

Administratoren können einen Benutzer- oder Gruppenzugriff auf Geräte mit Just-In-Time-Authentifizierung erteilen, die der Benutzer verlängern kann, bevor sie abläuft.

1. Klicken Sie im linken Fensterausschnitt der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **JITA-Konfiguration**.
2. Wählen Sie im Dropdown-Menü des Geräts entweder **Wechselmedien** oder **DVD/CD-ROM-Laufwerke** aus.
3. Klicken Sie auf **+**, um einen Benutzer oder eine Gruppe zur JITA-Konfiguration hinzuzufügen.
4. Wählen Sie das Kontrollkästchen **Aktiviert** aus.
5. Legen Sie den JITA-Zeitraum auf den gewünschten Wert fest.
6. Wählen Sie das Kontrollkästchen **Verlängerbar** aus.
7. Klicken Sie auf **Übernehmen**.

Der Benutzer muss sich abmelden und erneut anmelden, damit die neue JITA-Einstellung übernommen wird.

Deaktivieren einer JITA für einen Benutzer oder eine Gruppe

Administratoren können den Zugriff von Benutzern oder Gruppen auf Geräte mit der Just-In-Time-Authentifizierung deaktivieren.

1. Klicken Sie im linken Fensterausschnitt der HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **JITA-Konfiguration**.
2. Wählen Sie im Dropdown-Menü des Geräts entweder **Wechselmedien** oder **DVD/CD-ROM-Laufwerke** aus.
3. Wählen Sie den Benutzer oder die Gruppe, für den/die JITA deaktiviert werden soll.
4. Deaktivieren Sie das Kontrollkästchen **Aktiviert**.
5. Klicken Sie auf **Übernehmen**.

Wenn sich der Benutzer anmeldet und versucht, auf das Gerät zuzugreifen, wird der Zugriff verweigert.

Erweiterte Einstellungen

Mit „Erweiterte Einstellungen“ stehen Ihnen die folgenden Funktionen zur Verfügung:

- Verwaltung der Gruppe „Geräte-Administratoren“
- Verwaltung von Laufwerksbuchstaben, für die Device Access Manager nie den Zugriff verweigert

Die Gruppe „Geräte-Administratoren“ wird verwendet, um vertrauenswürdige Benutzer (vertrauenswürdig im Hinblick auf den Gerätezugriff) von den Beschränkungen durch eine Device Access Manager Richtlinie auszunehmen. Systemadministratoren gehören üblicherweise zu den vertrauenswürdigen Benutzern. Weitere Informationen finden Sie unter „Gruppe „Geräte-Administratoren““ auf Seite 63.

In der Ansicht **Erweiterte Einstellungen** kann der Administrator zudem eine Liste mit Laufwerksbuchstaben konfigurieren, für die Device Access Manager den Zugriff für Benutzer nicht beschränkt.

HINWEIS: Die Hintergrunddienste für Device Access Manager müssen ausgeführt werden, wenn die Liste mit den Laufwerksbuchstaben konfiguriert wird.

So starten Sie diese Dienste:

1. Wenden Sie eine Richtlinie für eine einfache Konfiguration an, wie beispielsweise die Zugriffsverweigerung auf Wechselmedien für alle Benutzer, die keine Geräte-Administratoren sind.

   – oder –

   Öffnen Sie mit Administratorrechten ein Eingabeaufforderungsfenster, und geben Sie Folgendes ein:

   ```
   sc start flcdlock
   ```

   Drücken Sie die Eingabetaste.

2. Sobald die Dienste gestartet wurden, kann die Laufwerksliste bearbeitet werden. Geben Sie die Laufwerksbuchstaben von Geräten ein, die nicht von Device Access Manager gesteuert werden sollen.

   Die Laufwerksbuchstaben werden für physische Festplatten oder Partitionen angezeigt.

HINWEIS: Unabhängig davon, ob sich das Systemlaufwerk (üblicherweise C) in der Liste befindet, wird der Zugriff darauf nie für Benutzer verweigert.

Gruppe „Geräte-Administratoren“

Bei der Installation von Device Access Manager wird die Gruppe „Geräte-Administratoren” erstellt.

Die Gruppe „Geräte-Administratoren“ wird verwendet, um vertrauenswürdige Benutzer (vertrauenswürdig im Hinblick auf den Gerätezugriff) von den Beschränkungen durch eine Device Access Manager Richtlinie auszunehmen. Systemadministratoren gehören üblicherweise zu den vertrauenswürdigen Benutzern.

HINWEIS: Die Aufnahme eines Benutzers in die Gruppe „Geräte-Administratoren“ berechtigt ihn nicht automatisch zum Gerätezugriff. Wenn der Gruppe „Benutzer“ in der Ansicht **Geräteklassen-Konfiguration** der Zugriff auf ein Gerät verweigert wird, muss der Gruppe „Geräte-Administratoren“ der Zugriff erlaubt werden, damit Mitglieder der Gruppe Zugriff auf das Gerät haben. Die Ansicht **Einfache Konfiguration** kann jedoch verwendet werden, um allen Benutzern, die kein Mitglied der Gruppe „Geräte-Administratoren“ sind, den Zugriff auf Geräteklassen zu verweigern.

So fügen Sie Benutzer zur Gruppe „Geräte-Administratoren“ hinzu:

1. Klicken Sie in der Ansicht **Erweiterte Einstellungen** auf **+**.
2. Geben Sie den Benutzernamen des vertrauenswürdigen Benutzers ein.
3. Klicken Sie auf **OK**.
4. Klicken Sie auf **Übernehmen**.

eSATA-Gerätesupport

Damit Device Access Manager eSATA-Geräte steuern kann, muss Folgendes konfiguriert werden:

1. Das Laufwerk muss verbunden werden, wenn das System startet.
2. Stellen Sie über die Ansicht **Erweiterte Einstellungen** sicher, dass der Buchstabe des eSATA-Laufwerks nicht in der Liste der Laufwerke enthalten ist, für die Device Access Manager den Zugriff nicht verweigert. Wenn der Buchstabe des eSATA-Laufwerks aufgeführt ist, löschen Sie den Laufwerksbuchstaben, und klicken Sie dann auf **Übernehmen**.
3. Das Gerät kann über die Ansicht **Einfache Konfiguration** oder **Geräteklassen-Konfiguration** anhand der Geräteklasse „Wechselmedien“ gesteuert werden.

Nicht verwaltete Geräteklassen

HP ProtectTools Device Access Manager verwaltet die folgenden Geräteklassen nicht:

- Eingabe-/Ausgabegeräte
  - Biometrisches Gerät
  - Maus
  - Tastatur
  - Drucker
  - Plug-and-Play (PnP)-Drucker
  - Drucker-Upgrade
  - Infrarot-Schnittstelle für die Benutzerinteraktion
  - Smart Card-Lesegerät
  - Serieller Multi-Port
  - Datenträgerlaufwerk
  - Disketten-Controller (FDC)
  - Festplatten-Controller (HDC)
  - Schnittstelle für die Benutzerinteraktion (HID)
- Energie
  - Akku
  - Support für erweiterte Energieverwaltung (APM)
- Sonstiges
  - Computer
  - Decoder
  - Display
  - Prozessor
  - System
  - Unbekannt

- Lautstärke
- Volume-Schnappschuss
- Sicherheitsgerät
- Sicherheitsbeschleuniger
- Vereinheitlichter Display-Treiber von Intel®
- Medientreiber
- Medienwechselgerät
- Multifunktionsgerät
- Legacard
- Netz-Client
- Netzdienst
- Netzübertragung
- SCSI-Adapter

8 Theft recovery (select models only)Aero verwalten (bestimmte Modelle)

Mit Computrace for HP ProtectTools (separat erhältlich) können Sie Ihren Computer per Fernzugriff überwachen, verwalten und wiederfinden.

Nach der Aktivierung wird Computrace for HP ProtectTools vom Absolute Software-Kundencenter konfiguriert. Vom Kundencenter aus kann der Administrator Computrace for HP ProtectTools konfigurieren, um den Computer zu überwachen oder zu verwalten. Wenn der Computer verloren geht oder gestohlen wird, kann das Kundencenter die lokalen Behörden bem Auffinden und bei der Wiederbeschaffung des Computers unterstützen. Nach der Konfiguration bleibt Computrace auf dem Computer auch dann aktiv, wenn die Festplatte gelöscht oder ausgetauscht wird.

So aktivieren Sie Computrace for HP ProtectTools:

1. Stellen Sie eine Verbindung zum Internet her.
2. Öffnen Sie die Security Manager Benutzer-Konsole. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 28.
3. Klicken Sie auf der linken Seite von Security Manager auf **Theft Recovery** (Wiedererlangen bei Diebstahl).
4. Zum Starten des Computrace Aktivierungsassistenten klicken Sie auf **Los geht's**.
5. Geben Sie Ihre Kontakt- und Kreditkarteninformationen oder einen bereits gekauften Produktschlüssel ein.

Der Aktivierungsassistent verarbeitet die Transaktion auf sichere Weise und richtet Ihr Benutzerkonto auf der Website des Absolute Software-Kundencenters ein. Anschließend erhalten Sie eine Bestätigungs-E-Mail mit den Informationen zu Ihrem Kundencenter-Konto.

Wenn Sie den Computrace Aktivierungsassistenten schon einmal ausgeführt haben und bereits über ein Kundencenter-Benutzerkonto verfügen, können Sie zusätzliche Lizenzen erwerben. Weitere Informationen erhalten Sie von Ihrem HP Kundenberater.

So melden Sie sich beim Kundencenter an:

1. Rufen Sie folgende Adresse auf: https://cc.absolute.com/.
2. Geben Sie in die Felder **Anmelde-ID** und **Kennwort** die Anmeldeinformationen ein, die Sie in der Bestätigungs-E-Mail erhalten haben, und klicken Sie auf die Schaltfläche **Anmelden**.

Im Kundencenter können Sie:

- Ihre Computer überwachen.
- Ihre Remote-Daten schützen.
- Den Diebstahl von Computern melden, die durch Computrace geschützt sind.

▲ Klicken Sie auf **Weitere Informationen**, um zusätzliche Informationen über Computrace for HP ProtectTools zu erhalten.

9 Ausnahmen für lokalisierte Kennwörter

Auf der Ebene von Pre-Boot Security bzw. HP Drive Encryption wird die Kennwortlokalisierung nur beschränkt unterstützt. Dies wird in den folgenden Abschnitten beschrieben.

Vorgehensweise, wenn das Kennwort abgelehnt wird

Kennwörter können aus folgenden Gründen abgelehnt werden:

- Ein Benutzer verwendet einen nicht unterstützten IME. Dies kommt häufig bei Doppelbyte-Sprachen vor (Koreanisch, Japanisch, Chinesisch). So beheben Sie dieses Problem:

  1. Fügen Sie über die **Systemsteuerung** ein unterstütztes Tastaturlayout hinzu (zum Beispiel ein US-Tastaturlayout, wenn Chinesisch als Eingabesprache festgelegt ist).
  2. Legen Sie die unterstützte Tastatur als Standard-Eingabegebietsschema fest.
  3. Starten Sie HP ProtectTools neu, und geben Sie dann das Kennwort erneut ein.

- Ein Benutzer verwendet ein nicht unterstütztes Zeichen. So beheben Sie dieses Problem:

  1. Ändern Sie das Windows -Kennwort, sodass es nur unterstützte Zeichen enthält. Weitere Informationen zu nicht unterstützten Zeichen finden Sie in der Hilfe zur Software HP ProtectTools Security Administrator-Konsole.
  2. Führen Sie den Installations-Assistenten für HP ProtectTools Security Manager erneut aus, und geben Sie dann das neue Windows Kennwort ein.

Windows IMEs werden weder auf der Ebene von Pre-Boot Security noch auf der Ebene von HP Drive Encryption unterstützt

In Windows kann der Benutzer mit einem IME (Input Method Editor, Eingabemethoden-Editor) komplexe Zeichen und Symbole wie beispielsweise japanische oder chinesische Zeichen über eine westliche Standardtastatur eingeben.

IMEs werden weder auf der Ebene von Pre-Boot Security noch auf der Ebene von HP Drive Encryption unterstützt. Ein IME kann nicht dazu verwendet werden, ein Windows Kennwort im Anmeldebildschirm für Pre-Boot Security oder HP Drive Encryption einzugeben. Die Eingabe über einen IME kann zu einer Sperrung führen. In manchen Fällen zeigt Microsoft® Windows den IME nicht an, wenn der Benutzer das Kennwort eingibt.

Die Lösung besteht darin, eines der folgenden unterstützten Tastaturlayouts auszuwählen, die dem Tastaturlayout 00000411 entsprechen:

- Microsoft IME für Japanisch
- Das japanische Tastaturlayout
- Office 2007 IME für Japanisch – Wenn Microsoft oder ein Dritter den Begriff IME oder Input Method Editor verwendet, handelt es sich bei der Eingabemethode nicht unbedingt um einen IME. Dies kann zu Verwirrung führen, aber die Software liest die Hexadezimaldarstellung des

Codes. Aus diesem Grund kann HP ProtectTools die Konfiguration unterstützen, wenn ein IME einem unterstützten Tastaturlayout zugeordnet ist.

VORSICHT! Wenn HP ProtectTools bereitgestellt wurde, werden mit Windows IME eingegebene Kennwörter abgelehnt.

Ändern des Kennworts mit einem Tastaturlayout, das ebenfalls unterstützt wird

Wenn das Kennwort beispielsweise zunächst mit einem Tastaturlayout für US-Englisch (409) festgelegt wird und der Benutzer anschließend das Kennwort mit einem anderen Tastaturlayout ändert, das ebenfalls unterstützt wird, wie z. B. Lateinamerikanisches Spanisch (080A), funktioniert die Kennwortänderung zwar in HP Drive Encryption, jedoch nicht im BIOS, wenn der Benutzer Zeichen des spanischen Tastaturlayouts verwendet, die im amerikanischen Layout nicht vorhanden sind (zum Beispiel ē).

HINWEIS: Administratoren können dieses Problem lösen, indem sie die Funktion **Benutzer verwalten** in HP ProtectTools verwenden, das gewünschte Tastaturlayout im Betriebssystem auswählen und anschließend den Installationsassistenten für Security Manager für den gleichen Benutzer erneut ausführen. Das gewünschte Tastaturlayout wird im BIOS gespeichert, und Kennwörter, die mit diesem Tastaturlayout eingegeben werden können, werden im BIOS korrekt festgelegt.

Ein weiteres potenzielles Problem ist die Verwendung verschiedener Tastaturlayouts, die die gleichen Zeichen erzeugen können. So kann sowohl mit dem Tastaturlayout US-International (20409) als auch mit dem lateinamerikanischen Tastaturlayout (080A) das Zeichen é erzeugt werden, obwohl dafür möglicherweise eine unterschiedliche Abfolge von Tasten gedrückt werden muss. Wird ein Kennwort zunächst mit dem lateinamerikanischen Tastaturlayout festgelegt, so ist das lateinamerikanische Tastaturlayout im BIOS eingestellt. Dies ist auch dann der Fall, wenn das Kennwort anschließend mit dem Tastaturlayout US-International geändert wird.

Behandeln von Sonderzeichen

- Chinesisch, Slowakisch, kanadisches Französisch und Tschechisch

  Wenn ein Benutzer eines der oben genannten Tastaturlayouts auswählt und dann ein Kennwort (beispielsweise abcdef) eingibt, muss in BIOS Pre-Boot Security oder HP Drive Encryption das gleiche Kennwort eingegeben werden, während die Umschalttaste für Kleinschreibung bzw. die Umschalttaste und die Feststelltaste für Großschreibung gedrückt werden. Bei der Eingabe von numerischen Kennwörtern muss der Nummernblock verwendet werden.

- Koreanisch

  Wenn ein Benutzer ein koreanisches Tastaturlayout auswählt und dann ein Kennwort eingibt, muss in BIOS Pre-Boot Security oder HP Drive Encryption das gleiche Kennwort eingegeben werden, während die rechte alt-Taste für Kleinschreibung und die rechte alt-Taste und die Feststelltaste für Großschreibung gedrückt werden.

- Die nicht unterstützten Zeichen sind in der folgenden Tabelle aufgeführt:

Sprache	Windows	BIOS	Drive Encryption
Arabisch	Die Tasten ﻷ ,ﻹ, und ﻵ erzeugen zwei Zeichen.	Die Tasten ﻷ ,ﻹ, und ﻵ erzeugen ein Zeichen.	Die Tasten ﻷ ,ﻹ, und ﻵ erzeugen ein Zeichen.

Sprache	Windows	BIOS	Drive Encryption
Französisch (Kanada)	ç, è, à und é mit Feststelltaste entsprechen Ç, È, À und É in Windows.	ç, è, à und é mit Feststelltaste entsprechen ç, è, à und é bei der BIOS-Authentifizierung vor dem Systemstart.	ç, è, à und é mit Feststelltaste entsprechen ç, è, à und é in HP Drive Encryption.
Spanisch	40a wird zwar nicht unterstützt, funktioniert aber trotzdem, da es von der Software zu c0a konvertiert wird. Aufgrund geringfügiger Unterschiede zwischen den Tastaturlayouts wird jedoch empfohlen, dass Spanisch sprechende Benutzer zum Tastaturlayout 1040a (spanische Variation) oder 080a (lateinamerikanisches Spanisch) wechseln.	N/V	N/V
US-International	◦ Die Tasten ¡, ¤, ‘, ’, ¥ und × in der oberen Reihe werden abgelehnt. ◦ Die Tasten å, ® und Þ in der zweiten Reihe werden abgelehnt. ◦ Die Tasten á, ð und ø in der dritten Reihe werden abgelehnt. ◦ Die Taste æ in der unteren Reihe wird abgelehnt.	N/V	N/V
Tschechisch	◦ Die Taste ğ wird abgelehnt. ◦ Die Taste į wird abgelehnt. ◦ Die Taste ų wird abgelehnt. ◦ Die Tasten ė, ı und ż werden abgelehnt. ◦ Die Tasten ģ, ķ, ļ, ņ und ţ werden abgelehnt.	N/V	N/V
Slowakisch	Die Taste ż wird abgelehnt.	◦ Die Tasten š, ś und ş; werden abgelehnt, wenn sie über die Tastatur eingegeben werden, jedoch bei Eingabe über die Bildschirmtastatur angenommen. ◦ Die unbelegte Taste ţ erzeugt zwei Zeichen.	N/V

Sprache	Windows	BIOS	Drive Encryption
Ungarisch	Die Taste ż wird abgelehnt.	Die unbelegte Taste ţ erzeugt zwei Zeichen.	N/V
Slowenisch	Die Taste źŻ wird in Windows abgelehnt, und die alt-Taste erzeugt im BIOS eine unbelegte Taste.	Die Tasten ú, Ú, ů, Ů, ş, Ş, ś, Ś, š und Š werden im BIOS abgelehnt.	N/V
Japanisch	Wenn verfügbar, sollte Microsoft Office 2007 IME verwendet werden. Trotz des IME-Namens handelt es sich hier um das unterstützte Tastaturlayout 411.	N/V	N/V

Glossar

Administrator
Siehe *Windows Administrator*.

Administrator-Konsole
Ein zentraler Bereich, in dem Administratoren auf die Funktionen und Einstellungen von HP ProtectTools zugreifen und diese verwalten können.

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

Anmeldedaten
Ein Objekt in Security Manager, das aus einem Benutzernamen und einem Kennwort (und möglicherweise anderen ausgewählten Informationen) besteht, die für die Anmeldung auf Websites oder bei anderen Programmen verwendet werden.

Anmeldeinformationen
Die Mittel, mit denen ein Benutzer seine Berechtigung für eine bestimmte Aufgebe während der Authentifizierung beweist.

Authentifizierung
Die Prüfung, ob ein Benutzer zur Durchführung einer Task wie Zugriff auf einen Computer, Ändern von Programmeinstellungen oder Abrufen gesicherter Daten autorisiert ist.

Authentifizierung beim Systemstart
Eine Sicherheitsfunktion, die beim Einschalten des Computers eine Art von Authentifizierung erfordert, wie eine Smart Card, einen Sicherheitschip oder ein Kennwort.

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

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

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

Domäne
Eine Gruppe von Computern, die Teil eines Netzwerks sind und gemeinsam eine Verzeichnisdatenbank benutzen. Domänen sind einheitlich benannt, und jede verfügt über allgemeine Regeln und Prozeduren.

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

Drive Encryption Anmeldebildschirm
Ein Logo-Bildschirm, der angezeigt wird, bevor Windows startet. Benutzer müssen ihren Windows Benutzernamen und das Kennwort oder ihre Smart Card-PIN eingeben oder mit dem registrierten Finger über den Sensor streichen. In den meisten Fällen ermöglicht die Eingabe der korrekten Informationen auf dem Drive Encryption-Anmeldebildschirm den direkten Zugriff auf Windows ohne die erneute Anmeldung auf dem Windows Anmeldebildschirm.

DriveLock
Eine Sicherheitsfunktion, die die Festplatte mit einem Benutzer verknüpft, der das DriveLock-Kennwort beim Computerstart dann korrekt eingeben muss.

Encryption File System (EFS)
Ein System, das alle Dateien und Unterordner innerhalb des ausgewählten Ordners verschlüsselt.

Entschlüsselung
Eine in der Kryptographie verwendete Prozedur zur Konvertierung von verschlüsselten Daten in Klartext.

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

Geräteklasse
Alle Geräte eines bestimmten Typs, beispielsweise Laufwerke.

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

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

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

HP SpareKey-Wiederherstellung
Die Möglichkeit, auf Ihren Computer zuzugreifen, indem Sie die Sicherheitsfragen richtig beantworten.

ID-Card
Windows Desktop-Minianwendung, mit der Ihr Desktop anhand Ihres Benutzernamens und eines ausgewählten Bildes visuell identifiziert werden kann.

Identität
In HP ProtectTools Security Manager eine Gruppe von Anmeldedaten und Einstellungen, die wie ein Konto oder ein Profil für einen bestimmten Benutzer gehandhabt werden.

JITA
Just-In-Time-Authentifizierung.

Kryptographie
Das Ver- und Entschlüsseln von Daten, damit diese nur von bestimmten Personen decodiert werden können.

Kryptographiediensteanbieter (Cryptographic Service Provider = CSP)
Ein Dienstanbieter oder eine Bibliothek von Verschlüsselungsalgorithmen, die in einer gut definierten Schnittstelle dazu benutzt werden können, bestimmte Verschlüsselungsfunktionen auszuüben.

Netzwerkkonto

Ein Konto eines Benutzers oder Administrators unter Windows, entweder auf einem lokalen Computer, in einer Arbeitsgruppe oder einer Domäne.

Neustart
Der Neustart des Computers.

Notfallwiederherstellungsarchiv
Ein geschützter Speicherbereich, der die Neuverschlüsselung der einfachen Benutzerschlüssel von einem Plattform-Eigentümerschlüssel zu einem anderen ermöglicht.

PIN
Persönliche Identifikationsnummer.

PKI
Der Public Key Infrastructure-Standard, der die Schnittstellen für die Erstellung, Verwendung und Verwaltung von Zertifikaten und kryptographischen Schlüsseln definiert.

SATA-Gerätemodus
Ein Datenübertragungsmodus zwischen einem Computer und Massenspeichergeräten wie Festplatten und optischen Laufwerken.

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

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

Smart Card
Ein kleines Stück Hardware, in Größe und Form einer Kreditkarte ähnlich, auf dem identifizierende Informationen zum Eigentümer gespeichert sind. Dient zur Authentifizierung des Benutzers an einem Computer.

SSO (Single Sign On)
Eine Funktion, die Authentifizierungsinformationen speichert und es Ihnen ermöglicht, Security Manager für den Zugriff auf das Internet und auf Windows Anwendungen zu verwenden, die eine Kennwortauthentifizierung erfordern.

Szene
Ein Bild eines registrierten Benutzers, das zur Authentifizierung verwendet werden kann.

TPM-Sicherheitschip (Trusted Platform Module)
Der allgemeine Ausdruck für den HP ProtectTools Embedded Security-Chip. Ein TPM-Chip authentifiziert einen Computer anstelle eines Benutzers, indem für das Host-System typische Informationen gespeichert werden, wie Verschlüsselungsschlüssel, digitale Zertifikate und Kennwörter. Ein TPM-Chip senkt das Risiko, dass die Informationen auf dem Computer durch Diebstahl oder einen Hackerangriff preisgegeben werden.

TXT
Trusted Execution Technology.

Verschlüsselung
Ein Verfahren ähnlich einer Algorithmusanwendung, das im Bereich der Kryptografie zur Umwandlung eines einfachen Texts in einen verschlüsselten Text angewendet wird, damit unbefugte Empfänger die darin enthaltenen Daten nicht lesen können. Es gibt viele verschiedene Arten der Datenverschlüsselung. Sie bilden die Basis für die Netzwerksicherheit. Zu den häufig verwendeten Verschlüsselungstechniken zählen die Standarddatenverschlüsselung und die Verschlüsselung mit einem öffentlichen Schlüssel.

Widerruf-Kennwort

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

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

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

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

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

Zertifizierungsstelle (CA)
Ein Service, der Zertifikate ausstellt, die zum Betreiben einer öffentlichen Schlüsselinfrastruktur erforderlich sind.

Index

W

Z