HP ProtectTools Sicherheitssoftware, Version 6.0

Benutzerhandbuch

HP ProtectTools Sicherheitssoftware – Benutzerhandbuch

Dritte Ausgabe: November 2010

Teilenummer des Dokuments: 581746-043

Allgemeines

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

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

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

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

Inhaltsverzeichnis

1 Einführung in die Sicherheitsfunktionen

Die HP ProtectTools Sicherheitssoftware enthält Sicherheitsfunktionen, die vor unberechtigtem Zugriff auf den Computer, auf Netzwerke und kritische Daten schützen. Eine Reihe von HP ProtectTools Softwaremodulen bieten erweiterte Sicherheitsfunktionen.

HP ProtectTools steht in zwei Versionen zur Verfügung: HP ProtectTools Security Manager Administrator-Konsole und HP ProtectTools Security Manager (für Standardbenutzer ohne Administratorrechte). Die Administrator- sowie die Benutzerversion sind verfügbar im Menü **Start** > **Alle Programme** > **HP**.

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

HINWEIS: Password Manager, Smart Card Security, Face Recognition und Drive Encryption werden mit dem Security Manager Installationsassistenten konfiguriert. HP Professional Desktop Systeme unterstützen derzeit keine Fingerabdruck-Lesegeräte.

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

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

HP ProtectTools Funktionen

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

Modul	Funktionen
HP ProtectTools Security Manager Administrator-Konsole	• Der Security Manager Installationsassistent wird von Administratoren verwendet, um Sicherheitsstufen und Sicherheits-Anmeldemethoden einzurichten und zu konfigurieren. • Ermöglicht die Konfiguration von Optionen, die Standardbenutzern nicht angezeigt werden. • Ermöglicht die Aktivierung von Drive Encryption und die Konfiguration des Benutzerzugriffs. • Ermöglicht die Konfiguration von Device Access Manager und des Benutzerzugriffs. • Mit den Administrator-Tools können HP ProtectTools Benutzer hinzugefügt oder entfernt und der Benutzerstatus angezeigt werden.
HP ProtectTools Security Manager für Standardbenutzer ohne Administratorrechte	• Ermöglicht die Konfiguration und Änderung von File Sanitizer Funktionen für das Shreddern und Bereinigen sowie von File Sanitizer Einstellungen. • Ermöglicht die Anzeige der Einstellungen für den Verschlüsselungsstatus sowie Device Access Manager. • Verwenden Sie Privacy Manager, um die Sicherheit von E-Mails und Dokumenten zu erhöhen. • Aktivieren Sie Computrace for HP ProtectTools. • Ermöglicht die Konfiguration von Einstellungen sowie von Sicherungs- und Wiederherstellungsoptionen.
Credential Manager for HP ProtectTools (Teil von Security Manager)	• Ermöglicht die Verwaltung, Einrichtung und Änderung von Benutzernamen und -kennwörtern. • Ermöglicht die Konfiguration und Änderung von Anmeldeinformationen wie beispielsweise Windows und Smart Card-Kennwort. • Dient als persönliches Kennwortarchiv und vereinfacht den Anmeldeprozess anhand der Single Sign On-Funktion, die Anmeldeinformationen von Benutzern automatisch speichert und übernimmt. • Ermöglicht die Einrichtung und Verwaltung von Single Sign On-Benutzernamen und -kennwörtern.
Drive Encryption for HP ProtectTools	• Ermöglicht die vollständige Datenträgerverschlüsselung für eine Festplatte. • Erfordert die Authentifizierung vor dem Systemstart, um die Festplatte zu entschlüsseln und den Datenzugriff zu gewähren. • Bietet die Möglichkeit zur Aktivierung von SED-Laufwerken (Self Encrypting Drives, selbstverschlüsselnde Laufwerke), wenn sie vorhanden sind.
Privacy Manager for HP ProtectTools	• Generiert Echtheitszertifikate, mit denen die Quelle, Integrität und Sicherheit der Verbindung überprüft wird, wenn Microsoft-E-Mail- und Microsoft Office-Dokumente verwendet werden.

Modul	Funktionen
File Sanitizer for HP ProtectTools	• Ermöglicht das sichere Shreddern von digitalen Beständen (sicheres Löschen von sensiblen Informationen wie Anwendungsdateien, Verlaufsdaten oder webbezogener Content und andere vertrauliche Daten) auf dem Computer. Darüber hinaus ermöglicht File Sanitizer die regelmäßige Bereinigung der Festplatte (Überschreiben von Daten, die vorher gelöscht wurden, aber noch auf der Festplatte vorhanden sind, um die Wiederherstellung dieser Daten zu erschweren).
Smart Card Security (Teil von Security Manager)	• Bietet eine Management-Softwareschnittelle für Smart Card. HP ProtectTools Smart Card ist ein persönliches Sicherheitsgerät, das Authentifizierungsdaten schützt, da für den Zugriff sowohl die betreffende Karte als auch eine PIN-Nummer erforderlich ist. Die Smart Card kann für den Zugriff auf Password Manager, Drive Encryption oder eine beliebige Anzahl von Access Points verwendet werden, die von Drittanbietern bereitgestellt werden. • Ermöglicht die PIN-Änderung.
Embedded Security for HP ProtectTools	• Nutzt einen integrierten TPM (Trusted Platform Module)-Chip (wenn vorhanden), um den unberechtigten Zugriff auf sensible Benutzerdaten oder Anmeldeinformationen zu verhindern, die lokal auf einem PC gespeichert sind. • Ermöglicht die Erzeugung eines PSD (Personal Secure Drive)-Laufwerks, mit dem sich Informationen in Benutzerdateien und –ordnern wirksam schützen lassen. • Unterstützt Anwendungen von Drittanbietern wie Microsoft Outlook und Internet Explorer für geschützte Vorgänge, bei denen digitale Zertifikate zum Einsatz kommen.
Device Access Manager for HP ProtectTools	• Ermöglicht IT-Managern und Administratoren, den Zugriff auf Geräte (z. B. USB-Anschlüsse, optische Laufwerke, persönliche Music Player usw.) anhand von Benutzerprofilen festzulegen. • Verhindert, dass unberechtigte Benutzer Daten von externen Speichermedien entfernen und Computerviren von externen Medien in das System gelangen. • Der Administrator kann Einzelpersonen oder Benutzergruppen den Zugriff auf beschreibbare Geräte untersagen. • Ermöglicht dem Administrator zu planen, wann Zugriff auf die Hardware möglich ist.
Computrace for HP ProtectTools	• Ermöglicht die sichere Verfolgung von Datenbeständen. • Ermöglicht die Überwachung der Benutzeraktivität sowie von Hardware- und Softwaremodifizierungen. • Bleibt auch dann aktiv, wenn die Festplatte neu formatiert oder ausgetauscht wird. • Für die Aktivierung ist ein separates Tracking- und Tracing-Abonnement erforderlich.

HP ProtectTools Sicherheitsprodukte und Verwendungsbeispiele

Die meisten der HP ProtectTools Sicherheitsprodukte verfügen sowohl über ein Benutzerauthentifizierungs-Backup (normalerweise ein Kennwort) als auch über ein Administrator-

Backup. Damit kann der Zugriff wiederhergestellt werden, wenn Kennwörter verloren gehen, nicht verfügbar sind oder vergessen werden oder die Unternehmenssicherheit einen Zugriff erforderlich macht.

HINWEIS: Einige der HP ProtectTools Sicherheitsprodukte sind so konzipiert, dass sie den Zugriff auf Daten einschränken. Die Verschlüsselung von Daten ist sinnvoll, wenn die Daten so wichtig sind, dass der Benutzer lieber deren Verlust anstelle von unberechtigtem Zugriff in Kauf nimmt. Es ist empfehlenswert, ein Backup aller Daten an einem sicheren Ort aufzubewahren.

Credential Manager (Password Manager) for HP ProtectTools

Credential Manager (Bestandteil von Security Manager) ist ein Repository für Benutzernamen und Kennwörter. Es wird in den meisten Fällen zum Speichern von Anmeldenamen und Kennwörtern für den Internet- oder Webmail-Zugang verwendet. Credential Manager kann den Benutzer automatisch auf einer Website oder bei einem E-Mail-Konto anmelden.

Beispiel 1: Eine Mitarbeiterin der Einkaufsabteilung eines großen Herstellungsunternehmens wickelt die meisten geschäftlichen Transaktionen über das Internet ab. Sie besucht auch regelmäßig gängige Websites, bei denen eine Anmeldung erforderlich ist. Sicherheit ist ihr sehr wichtig. Aus diesem Grund verwendet sie nicht immer dasselbe Kennwort. Sie verwendet Credential Manager, um Web-Links mit unterschiedlichen Benutzernamen und Kennwörtern abzugleichen. Beim Anmelden auf einer Website werden die Anmeldeinformationen von Credential Manager automatisch ausgefüllt. Wenn sie den Benutzernamen und das Kennwort sehen möchte, kann Credential Manager so eingestellt werden, dass die Daten sichtbar sind.

Mit Credential Manager können die Authentifizierungsdaten auch verwaltet werden. Der Benutzer wählt den gewünschten Web- oder Netzwerkzugang aus, und Credential Manager greift automatisch auf den Link zu. Benutzernamen und Kennwörter können bei Bedarf auch angezeigt werden.

Beispiel 2: Ein engagierter Buchprüfer ist befördert worden und leitet nun die gesamte Buchhaltungsabteilung. Das Team muss sich bei einer großen Zahl von Kunden-Internetkonten anmelden, wobei für jedes Konto unterschiedliche Anmeldedaten erforderlich sind. Die Anmeldedaten werden gemeinsam mit anderen Mitarbeitern benutzt. Vertraulichkeit spielt daher eine wichtige Rolle. Der Buchprüfer beschließt, alle Internet-Links, Benutzernamen der Firmen und Kennwörter mit Credential Manager for HP ProtectTools zu verwalten. Nach der Einrichtung gibt der Buchprüfer Credential Manager an die Mitarbeiter weiter. Sie können sich nun bei den Internetkonten anmelden, ohne die Anmeldedaten einsehen zu können.

Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools ermöglicht das Erstellen eines PSD (Personal Secure Drive, persönliches sicheres Laufwerk). Mithilfe dieser Funktion kann der Benutzer eine virtuelle Laufwerkspartition auf dem PC erstellen, die vollständig ausgeblendet ist, bis darauf zugegriffen wird. Embedded Security kann immer verwendet werden, wenn ausgeblendete Daten geschützt werden sollen, während die restlichen Daten nicht verschlüsselt sind.

Beispiel 1: Ein Lagerverwalter hat einen Computer, auf den im Laufe des Tages mehrere Mitarbeiter immer wieder zugreifen. Der Verwalter möchte vertrauliche Lagerdaten auf dem Computer verschlüsseln und ausblenden. Die Daten sollen so gesichert sein, dass sie selbst im Falle eines Diebstahls der Festplatte nicht entschlüsselt oder gelesen werden können. Der Lagerverwalter beschließt Embedded Security zu aktivieren, und verschiebt die vertraulichen Daten auf das PSD. Er kann ein Kennwort eingeben und wie auf einer herkömmlichen Festplatte auf die vertraulichen Daten zugreifen. Nach dem Abmelden vom PSD oder einem Neustart lässt sich das Laufwerk nicht ohne das richtige Kennwort anzeigen oder öffnen. Die Mitarbeiter sehen somit niemals die vertraulichen Daten, wenn sie auf den Computer zugreifen.

Embedded Security schützt Verschlüsselungsschlüssel in einem Hardware-TPM (Trusted Computing Module)-Chip, der sich auf der Hauptplatine befindet. Es handelt sich dabei um das einzige Verschlüsselungstool, das den Mindestanforderungen für den Kennwortschutz entspricht, falls der Versuch unternommen wird, das Verschlüsselungskennwort zu erraten. Mit Embedded Security ist außerdem die vollständige Verschlüsselung des Laufwerks und von E-Mails möglich.

Beispiel 2: Eine Börsenmaklerin möchte äußerst wichtige Daten mithilfe einer tragbaren Festplatte auf einen anderen Computer übertragen. Dabei soll sichergestellt werden, dass das Laufwerk nur auf diesen beiden Computern geöffnet werden kann, selbst wenn unbefugte Personen im Besitz des Kennworts sind. Die Börsenmaklerin verwendet die TPM-Migration in Embedded Security, damit ein zweiter Computer über die erforderlichen Schlüssel zum Dekodieren der Daten verfügt. Während der Übertragung können nur diese beiden physischen Computer die Daten entschlüsseln – selbst wenn das Kennwort bekannt ist.

Drive Encryption for HP ProtectTools

Drive Encryption wird meist verwendet, um den Zugriff auf Daten auf der kompletten Festplatte des Computers oder einer sekundären Festplatte einzuschränken. Drive Encryption kann auch SED-Laufwerke (Self Encrypting Drive) verwalten.

Beispiel 1: Ein Arzt möchte sicherstellen, dass nur er auf die Daten auf der Festplatte seines Computers zugreifen kann. Er aktiviert Drive Encryption, das die Authentifizierung vor dem Systemstart oder der Windows-Anmeldung aktiviert. Nach der Einrichtung kann die Festplatte bereits für den Start des Betriebssystems nicht ohne Kennwort geöffnet werden. Der Arzt kann die Laufwerksicherheit verbessern, indem er die Daten mit der SED-Option (Self Encrypting Drive) verschlüsselt.

Sowohl Embedded Security als auch Drive Encryption for HP ProtectTools ermöglichen keinen Zugriff auf die verschlüsselten Daten, selbst wenn das Laufwerk entfernt wurde, da sie beide an die ursprüngliche Hauptplatine gebunden sind.

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

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools wird verwendet, um Daten wie den Webbrowserverlauf, temporäre Dateien, bereits gelöschte Daten oder andere Informationen dauerhaft zu löschen. File Sanitizer kann so konfiguriert werden, dass er manuell oder automatisch auf der Grundlage eines benutzerdefinierten Zeitplans ausgeführt wird.

Beispiel 1: Ein Anwalt hat oft mit wichtigen Kundendaten zu tun und möchte sicherstellen, dass Daten aus gelöschten Dateien nicht wiederhergestellt werden können. Er verwendet File Sanitizer, um gelöschte Dateien zu shreddern. Damit ist es so gut wie unmöglich, die Dateien wiederherzustellen.

Wenn in Windows Daten gelöscht werden, werden sie normalerweise nicht von der Festplatte entfernt. Stattdessen wird der Festplattensektor als verfügbar markiert. Bis die Daten überschrieben werden, können sie problemlos mithilfe von gängigen, im Internet verfügbaren Tools wiederhergestellt werden. File Sanitizer überschreibt die Sektoren mit zufällig ausgewählten Daten (auch mehrmals, falls nötig) und hinterlässt dabei die gelöschten Daten unlesbar und unwiederherstellbar.

Beispiel 2: Eine Forscherin möchte gelöschte Daten, temporäre Dateien, den Browserverlauf usw. beim Abmelden automatisch shreddern. Sie verwendet File Sanitizer, um das Shreddern zu planen. Dabei kann sie die gemeinsamen Dateien oder beliebige benutzerdefinierte Dateien auswählen, die automatisch dauerhaft entfernt werden sollen.

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools kann verwendet werden, um den unautorisierten Zugriff auf USB-Flash-Laufwerke zu blockieren und damit das Kopieren von Daten zu verhindern. Außerdem kann der Zugriff auf CD/DVD-Laufwerke und die Kontrolle von USB-Geräten, Netzwerkverbindungen usw. eingeschränkt werden. Ein Administrator kann zusätzlich planen, wann und für lange auf Laufwerke zugegriffen werden kann. Ein Beispiel dafür ist eine Situation, in der ein externer Vendor Zugriff auf Firmencomputer benötigt, aber nicht in der Lage sein soll, die Daten auf ein USB-Laufwerk zu kopieren. Mithilfe von Device Access Manager for HP ProtectTools kann ein Administrator den Zugriff auf Hardware einschränken und verwalten.

Beispiel 1: Der Manager eines Zulieferers für Medizinprodukte arbeitet häufig neben den eigenen Firmeninformationen auch mit persönlichen medizinischen Datensätzen. Die Mitarbeiter benötigen Zugriff auf diese Daten; es ist jedoch äußerst wichtig, dass die Daten nicht mithilfe eines USB-Laufwerks oder eines anderen externen Speichermediums entfernt werden. Das Netzwerk ist sicher, aber die Computer verfügen über CD-Brenner und USB-Anschlüsse, über die die Daten kopiert oder entwendet werden können. Der Manager verwendet Device Access Manager, um die USB-Anschlüsse und CD-Brenner zu deaktivieren. So können sie nicht verwendet werden. Auch wenn die USB-Anschlüsse blockiert sind, funktionieren Maus und Tastatur weiterhin.

Beispiel 2: Ein Versicherungsunternehmen möchte nicht, dass seine Mitarbeiter persönliche Software oder Daten von zuhause installieren oder laden. Einige Mitarbeiter benötigen Zugriff auf die USB-Anschlüsse an allen Computern. Der IT-Manager verwendet Device Access Manager, um den Zugriff für einige Mitarbeiter zu ermöglichen und für alle anderen zu blockieren.

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools wird verwendet, wenn die Kommunikation per E-Mail über das Internet sicher sein muss. Der Benutzer kann E-Mails erstellen und senden, die nur von einem authentifizierten Empfänger geöffnet werden können. Mit Privacy Manager kann nicht unerlaubt auf die Informationen zugegriffen werden. Außerdem können Betrüger sie nicht abfangen.

Beispiel 1: Ein Börsenmakler möchte sicherstellen, dass seine E-Mails ausschließlich an bestimmte Kunden gesendet werden und niemand das E-Mail-Konto fälschen und E-Mails abfangen kann. Der Börsenmakler registriert sich und seine Kunden in Privacy Manager. In Privacy Manager wird ein Certificate of Authentication (CA) für jeden Benutzer ausgestellt. Mithilfe dieses Tools müssen sich der Börsenmakler und seine Kunden authentifizieren, bevor eine E-Mail ausgetauscht wird.

Privacy Manager for HP ProtectTools erleichtert das Senden und Empfangen von E-Mails mit Verifizierung und Authentifizierung des Empfängers. Der E-Mail-Dienst kann auch verschlüsselt werden. Der Verschlüsselungsprozess ist mit dem Prozess vergleichbar, der für allgemeine Internetkäufe mit Kreditkarte verwendet wird.

Beispiel 2: Ein Geschäftführer möchte sichergehen, dass nur die Mitglieder des Aufsichtsrats die Informationen anzeigen können, die er per E-Mail sendet. Er verwendet die Option, um die an die Aufsichtsräte gesendeten E-Mails und die von ihnen empfangen zu verschlüsseln. Das Certificate of Authentication in Privacy Manager stellt dem Geschäftsführer und den Aufsichtsräten eine Kopie des Verschlüsselungsschlüssels zur Verfügung, sodass nur sie vertrauliche E-Mails entschlüsseln können.

Computrace for HP ProtectTools (zuvor als LoJack Pro bekannt)

Computrace for HP ProtectTools ist ein Dienst, mithilfe dessen ein entwendeter Computer geortet werden kann, sobald der Benutzer auf das Internet zugreift.

Beispiel 1: Der Direktor einer Schule wies die IT-Abteilung an, eine Übersicht aller Computer an seiner Schule zu erstellen. Nach der Bestandsaufnahme der PCs registrierte der IT-Administrator alle Computer in Computrace, sodass sie im Falle eines Diebstahls geortet werden können. Vor Kurzem wurde in der Schule festgestellt, dass einige Computer fehlten. Der IT-Administrator alarmierte daher die Polizei und die zuständigen Personen für Computrace. Die Computer wurden geortet und von der Polizei zur Schule zurückgebracht.

Computrace for HP ProtectTools kann auch bei der Remote-Verwaltung und -Ortung von Computern sowie bei der Überwachung der Computerverwendung und -anwendungen behilflich sein.

Beispiel 2: Ein Immobilienunternehmen muss weltweit Computer verwalten und aktualisieren. Dabei wird Computrace für die Überwachung und Aktualisierung der Computer verwendet, ohne dass ein IT-Mitarbeiter tatsächlich zu den jeweiligen Computern geschickt werden muss.

Öffnen von HP ProtectTools Security

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

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

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

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

HINWEIS: Nachdem Sie das Modul „Password Manager“ konfiguriert haben, können Sie HP ProtectTools auch öffnen, indem Sie sich direkt über das Windows Anmeldefenster bei Credential Manager anmelden.

Lösungen für grundlegende Sicherheitsaufgaben

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

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

Schutz gegen Diebstahl

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

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

- Die Authentifizierung vor dem Systemstart verhindert den unberechtigten Zugriff auf das Betriebssystem. Siehe auch folgende Kapitel:
  - „Password Manager for HP ProtectTools“ auf Seite 27
  - „Embedded Security for HP ProtectTools“ auf Seite 56
  - „Drive Encryption for HP ProtectTools“ auf Seite 32
- Mit DriveLock ist gewährleistet, dass auch dann nicht auf die Daten zugegriffen werden kann, wenn die Festplatte ausgebaut und in ein nicht gesichertes System wieder eingebaut wird.
- Die PSD-Funktion (Personal Secure Drive, Persönliches sicheres Laufwerk) des Moduls „Embedded Security for HP ProtectTools“ verschlüsselt sensible Daten und verhindert so den unberechtigten Zugriff darauf. Siehe auch folgendes Kapitel:
  - „Embedded Security for HP ProtectTools“ auf Seite 56
- Mit Computrace kann der Standort des Computers nach einem Diebstahl ermittelt werden. Siehe auch folgendes Kapitel:
  - „Computrace for HP ProtectTools“ auf Seite 67

Einschränken des Zugriffs auf sensible Daten

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

Mit Device Access Manager für HP ProtectTools können IT-Manager den Zugriff auf beschreibbare Geräte einschränken, um das Drucken oder Kopieren von sensiblen Informationen von der Festplatte auf Wechseldatenträger zu verhindern. Siehe „Geräteklassen-Konfiguration (erweitert)“ auf Seite 63.

Verhindern des unbefugten Zugriffs von internen oder externen Standorten

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

- Wenn die Authentifizierung vor dem Systemstart aktiviert ist, verhindert sie den Zugriff auf das Betriebssystem. Siehe auch folgende Kapitel:
  - „Password Manager for HP ProtectTools“ auf Seite 27
  - „Embedded Security for HP ProtectTools“ auf Seite 56
  - „Drive Encryption for HP ProtectTools“ auf Seite 32
- Embedded Security for HP ProtectTools sorgt für den optimalen Schutz sensibler Benutzerdaten oder Anmeldeinformationen, die lokal auf einem PC gespeichert sind. Siehe auch folgendes Kapitel:
  - „Embedded Security for HP ProtectTools“ auf Seite 56
- Password Manager for HP ProtectTools stellt sicher, dass unberechtigte Benutzer nicht in den Besitz von Kennwörtern gelangen oder auf kennwortgeschützte Anwendungen zugreifen können. Siehe auch folgendes Kapitel:
  - „Password Manager for HP ProtectTools“ auf Seite 27
- Mit Device Access Manager for HP ProtectTools können IT-Manager den Zugriff auf beschreibbare Geräte einschränken, um das Kopieren von sensiblen Informationen zu verhindern, die sich auf der Festplatte befinden. Siehe auch folgendes Kapitel:
  - „Device Access Manager for HP ProtectTools“ auf Seite 62
- Die PSD-Funktion (Personal Secure Drive, Persönliches sicheres Laufwerk) verschlüsselt sensible Daten und verhindert so den unberechtigten Zugriff darauf. Siehe auch folgendes Kapitel:
  - „Embedded Security for HP ProtectTools“ auf Seite 56
- File Sanitizer ermöglicht das sichere Löschen von Daten, indem kritische Dateien und Ordner geshreddert werden oder die Festplatte bereinigt wird (Überschreiben von Daten, die vorher gelöscht wurden, aber noch auf der Festplatte vorhanden sind, um die Wiederherstellung dieser Daten zu erschweren). Siehe auch folgendes Kapitel:
  - „File Sanitizer for HP ProtectTools“ auf Seite 49
- Privacy Manager ist ein Tool zur Erstellung von Echtheitszertifikaten, wenn Microsoft Mail, Microsoft Office-Dokumente und Instant Messenger verwendet werden, damit wichtige Informationen sicher gesendet und gespeichert werden. Siehe auch folgendes Kapitel:
  - „Privacy Manager for HP ProtectTools“ auf Seite 36

Erstellen von Richtlinien für den starken Kennwortschutz

Wenn für Dutzende von webbasierten Anwendungen und Datenbanken ein strenger Kennwortschutz festgelegt wird, steht mit Password Manager for HP ProtectTools ein geschütztes Repository für Kennwörter und die Single Sign On-Anmeldung zur Verfügung. Siehe auch folgendes Kapitel:

- „Password Manager for HP ProtectTools“ auf Seite 27

Weitere Sicherheitselemente

Zuweisen von Sicherheitsrollen

Bei der Verwaltung der Computersicherheit werden Zuständigkeiten und Berechtigungen häufig auf verschiedene Arten von Administratoren und Benutzern verteilt.

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

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

- Sicherheitsbeauftragter – definiert die Sicherheitsstufe für das Unternehmen oder Netzwerk und bestimmt die anzuwendenden Sicherheitsfunktionen, wie beispielsweise Drive Encryption oder Embedded Security.
- IT-Administrator – wendet die Sicherheitsfunktionen, die von dem Sicherheitsbeauftragten definiert wurden, an und verwaltet sie. Kann manche Funktionen auch aktivieren und deaktivieren. Wenn der Sicherheitsbeauftragte z. B. Smart Cards bereitstellt, kann der IT-Administrator den Kennwort- und den Smart Card-Modus aktivieren.
- Benutzer – verwendet die Sicherheitsfunktionen. Wenn der Sicherheitsbeauftragte und der IT-Administrator z. B. Smart Cards für das System aktiviert haben, kann der Benutzer die Karte zur Authentifizierung verwenden.

Verwalten der Kennwörter für HP ProtectTools

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

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

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

HP ProtectTools Kennwort	In diesem HP ProtectTools Modul eingerichtet	Funktion
Kennwort für allgemeinen Benutzerschlüssel **HINWEIS:** Auch bekannt als: Embedded Security Kennwort	Embedded Security	Ermöglicht den Zugriff auf die Embedded Security Funktionen, wie sichere E-Mail-, Datei- und Ordnerverschlüsselung. Wenn dieses Kennwort für die Authentifizierung beim Einschalten verwendet wird, ermöglicht es auch den Zugriff auf die Daten im Computer, wenn der Computer eingeschaltet, neu gestartet oder der Ruhezustand beendet wird.
Kennwort für das Notfallwiederherstellungs-Token **HINWEIS:** Auch bekannt als: Kennwort für den Notfallwiederherstellungs-Schlüssel	Embedded Security, vom IT-Administrator	Schützt den Zugriff auf das Notfallwiederherstellungs-Token. Hierbei handelt es sich um eine Sicherungsdatei für den Chip für integrierte Sicherheit.
Eigentümerkennwort	Embedded Security, vom IT-Administrator	Schützt das System und den TPM-Chip vor unberechtigtem Zugriff auf alle Eigentümerfunktionen von Embedded Security.
Smart Card-PIN	Smart Card-Sicherheit	Kann als Option für die mehrstufige Authentifizierung (Multifactor Authentication) verwendet werden. Kann als Windows-Authentifizierung verwendet werden. Authentifiziert Benutzer von Drive Encryption, wenn das Smart Card-Token ausgewählt wird.
Kennwort für Computer Setup **HINWEIS:** Auch bekannt als BIOS-Administrator-, F10-Setup- oder Sicherheits-Setup-Kennwort	BIOS (durch IT-Administrator)	Schützt den Zugriff auf Computer Setup Utility.
Systemstart-Kennwort	BIOS	Schützt den Zugriff auf die Daten auf dem Computer, wenn der Computer eingeschaltet oder neu gestartet wird bzw. wenn der Ruhezustand beendet wird.
Windows Anmeldekennwort	Windows Systemsteuerung	Kann für die manuelle Anmeldung verwendet werden.

Einrichten eines sicheren Kennworts

Das Einrichten von Kennwörtern ist nur möglich, wenn Sie die vom Programm festgelegten Anforderungen erfüllen. Beachten Sie im Allgemeinen folgende Richtlinien für das Einrichten von sicheren Kennwörtern, um die Risiken in Bezug auf Kennwörter zu verringern:

- Verwenden Sie Kennwörter mit mehr als 6 Zeichen, vorzugsweise mehr als 8 Zeichen.
- Verwenden Sie Groß- und Kleinschreibung innerhalb des Kennworts.
- Verwenden Sie nach Möglichkeit alphanumerische als auch Sonderzeichen und Interpunktionszeichen.

- Ersetzen Sie Buchstaben in einem Kennwort durch Sonderzeichen oder Zahlen. Sie können z. B. die Zahl 1 für den Buchstaben I oder L verwenden.
- Mischen Sie im Kennwort zwei oder mehrere Sprachen.
- Trennen Sie ein Wort oder einen Begriff durch Zahlen oder Sonderzeichen in der Mitte, z. B. „Mary2-2Cat45“.
- Verwenden Sie kein Kennwort, das in einem Wörterbuch vorkommt.
- Verwenden Sie nicht Ihren Namen oder andere persönliche Informationen, wie Geburtstage, Namen von Haustieren oder den Mädchennamen der Mutter, selbst dann nicht, wenn Sie diese rückwärts buchstabieren.
- Ändern Sie das Kennwort regelmäßig. Es genügt, wenn Sie nur einige Zeichen ändern.
- Wenn Sie Ihr Kennwort aufschreiben, bewahren Sie es auf keinen Fall sichtbar in der Nähe des Computers auf.
- Speichern Sie das Kennwort nicht in einer Datei, wie z. B. einer E-Mail, auf dem Computer.
- Nutzen Sie das Konto nicht gemeinsam mit anderen Benutzern, und geben Sie Ihr Kennwort nicht weiter.

Sichern von Zugangsdaten und Einstellungen

Sie können Zugangsdaten auf folgende Arten sichern:

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

  Sie können sich auch beim Online-Dienst zur Schlüsselwiederherstellung von Drive Encryption registrieren. Dieser speichert eine Kopie des Sicherungs- bzw. Chiffrierschlüssels, mit dessen Hilfe Sie auf Ihren Computer zugreifen können, selbst wenn Sie das Kennwort vergessen und keinen Zugriff auf Ihre lokale Sicherungskopie haben.
- Sichern Sie die Zugangsdaten von HP ProtectTools über Embedded Security for HP ProtectTools.
- Verwenden Sie das Tool „Backup and Recovery“ in HP ProtectTools Security Manager als zentralen Ort zum Sichern und Wiederherstellen von Sicherheitsinformationen aus installierten HP ProtectTools Modulen.

2 HP ProtectTools Security Manager Administrator-Konsole

Informationen zur HP ProtectTools Administrator-Konsole

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

Sie bietet dem lokalen Administrator folgende Möglichkeiten:

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

Verwenden der Administrator-Konsole

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

So öffnen Sie die Konsole:

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

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

Das linke Fenster der Administrator-Konsole enthält folgende Elemente:

- **Startseite** - Ermöglicht den einfachen Zugriff auf gängige Aufgaben wie die Aktivierung von Sicherheitsfunktionen, die Festlegung von Sicherheitsinformationen und die Verwaltung von Benutzern.
- **System** - Hier kann die Konfiguration von systemweiten Sicherheitsfunktionen, Benutzern und Authentifizierungsgeräten wie Smart Card-Lesegeräten verwaltet werden.
- **Anwendungen** - Beinhaltet Tools, mit denen sich das Verhalten von Security Manager und den zugehörigen Anwendungen konfigurieren lässt.
- **Daten** - Hier finden Sie Tools für das Verwalten von Laufwerksverschlüsselungen und das Sichern bzw. Wiederherstellen von Codierungsschlüsseln.
- **Computer** - Device Access Manager stellt erweiterte Sicherheitsoptionen bereit, mit denen verschiedenen Arten von Geräten, die eine Gefahr für die PC-Sicherheit darstellen könnten, selektiv der Zugriff untersagt werden kann. Außerdem können hier Berechtigungen für diverse Benutzer und Gruppen festgelegt werden.

- **Mitteilungen** (Communications) - Privacy Manager ermöglicht Benutzern, Zertifikate von Drittanbietern zur E-Mail-Authentifizierung zu verwalten. Embedded Security ermöglicht dem Benutzer, TPM-verschlüsselte E-Mails zu senden und zu empfangen.
- **Management-Tools** - Öffnet mithilfe des Standardbrowsers eine Website, auf der Sie weitere Verwaltungsanwendungen und –tools finden, die das Funktionsspektrum von Security Manager ergänzen. Außerdem finden Sie auf dieser Website Informationen zu neuen Anwendungen und Updates.
- **Links** - Bietet die folgenden Optionen:
  - **Installationsassistent** - Startet den Installationsassistenten, der Sie durch die Erstkonfiguration von Security Manager führt.
  - **Hilfe** - Öffnet die Online-Hilfe mit nützlichen Informationen zu Security Manager und den zugehörigen Anwendungen.
  - **Info** - Zeigt wichtige Informationen zu HP ProtectTools Security Manager einschließlich der Versionsnummer und dem Copyright-Vermerk an.

Einführung in den Installationsassistenten

Die Verwaltung von HP ProtectTools Security Manager erfordert Administratorrechte.

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

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

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

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

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

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

Systemkonfiguration

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

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

Die System-Gruppe umfasst die folgenden Anwendungen:

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

Aktivieren von Sicherheitsfunktionen

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

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

Festlegen der Security Manager Authentifizierungsrichtlinien

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

Registerkarte „Anmelden“

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

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Sicherheit**, und klicken Sie dann auf **Authentifizierung**.
2. Wählen Sie in der Registerkarte **Anmelden** eine Benutzerkategorie aus der Dropdown-Liste aus.
3. Legen Sie unter **Richtlinie** die Anmeldeinformationen für die ausgewählte Benutzerkategorie fest, indem Sie das/die Kontrollkästchen neben den betreffenden Anmeldeinformationen aktivieren. Es muss mindestens eine Anmeldeinformation festgelegt werden.
4. Wählen Sie in der Dropdown-Liste unter **Richtlinie** aus, ob „EINE BELIEBIGE“ (d. h. nur eine) der festgelegten Anmeldeinformationen oder aber ALLE festgelegten Anmeldeinformationen für eine Authentifizierung benötigt werden.
5. Klicken Sie auf **Übernehmen**.

HINWEIS: Wenn Sie für die Richtlinie die Option „ALLE angegebenen Anmeldeinformationen sind für die Authentifizierung erforderlich“ wählen, das System für Kennwort und Smart Card konfiguriert ist und die Smart Card beschädigt wird oder verloren geht, kann Windows für alle Administratoren gesperrt werden, sodass diese spezielle Tools benötigen, um wieder Zugriff zu erhalten.

Registerkarte „Sitzung“

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

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Sicherheit**, und klicken Sie dann auf **Authentifizierung**.
2. Wählen Sie auf der Registerkarte **Sitzung** eine Benutzerkategorie aus.
3. Legen Sie unter **Richtlinie** die Anmeldeinformationen für die ausgewählte Benutzerkategorie fest, indem Sie das/die Kontrollkästchen neben den betreffenden Anmeldeinformationen aktivieren. Es muss mindestens eine Anmeldeinformation festgelegt werden.
4. Wählen Sie in der Dropdown-Liste unter **Richtlinie** aus, ob „EINE BELIEBIGE“ (d. h. nur eine) der festgelegten Anmeldeinformationen oder aber ALLE festgelegten Anmeldeinformationen für eine Authentifizierung benötigt werden.
5. Klicken Sie auf **Übernehmen**.

Definieren von Einstellungen

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

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Sicherheit**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf das betreffende Kontrollkästchen, um eine Einstellung zu aktivieren bzw. zu deaktivieren.
3. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

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

Verwalten von Benutzern

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

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

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

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

Hinzufügen eines Benutzers

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

So fügen Sie der Benutzerliste einen Benutzer hinzu:

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

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

Entfernen eines Benutzers

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

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

Überprüfen des Benutzerstatus

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

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

Festlegen von Geräteeinstellungen

In der Anwendung „Geräte“ können Sie den Computer so konfigurieren, dass er beim Entfernen einer Smart Card automatisch gesperrt wird. Allerdings ist dies nur dann der Fall, wenn die Smart Card zur Authentifizierung bei der Windows Anmeldung verwendet wurde.

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Geräte**, und klicken Sie dann auf **Smart Card**.
3. Klicken Sie auf das Kontrollkästchen, um festzulegen, ob der Computer beim Entfernen einer Smart Card gesperrt werden soll.

Konfigurieren von Anwendungseinstellungen

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

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

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

Verschlüsseln von Laufwerken

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

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

Weitere Informationen zur Verwendung von Drive Encryption for HP ProtectTools finden Sie unter „Drive Encryption for HP ProtectTools“ auf Seite 32.

Verwalten des Gerätezugriffs

Device Access Manager for HP ProtectTools stellt erweiterte Sicherheitsfunktionen bereit, mit denen verschiedenen Arten von Geräten, die eine Gefahr für die PC-Sicherheit darstellen könnten, selektiv der Zugriff verweigert werden kann. Weitere Informationen zur Verwendung von Device Access Manager for HP ProtectTools finden Sie unter „Device Access Manager for HP ProtectTools“ auf Seite 62.

3 HP ProtectTools Security Manager

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

- Verwalten von Anmeldedaten und Kennwörtern
- Einfaches Ändern des Windows Kennworts
- Einrichten von Authentifizierungsinformationen einschließlich einer Smart Card
- Verbessern von Datenschutz und Sicherheit von E-Mails, Dokumenten und Instant Messaging
- Shreddern von Datenbeständen und Bereinigen der Festplatte
- Anzeige des Verschlüsselungsstatus eines Laufwerks
- Anzeige der Einstellungen für den Gerätezugriff
- Aktivieren von Diebstahlschutz-Software
- Sichern und Wiederherstellen von Security Manager Daten

Anmelden nach der Konfiguration von Security Manager

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

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

konfigurierten Methoden anmelden, wenn der Bildschirm „HP Password Manager“ angezeigt wird. Dieser Vorgang meldet den Benutzer bei Windows an.

- Falls die Sicherheitsstufe „HP Password Manager“ konfiguriert wurde und *beliebige* konfigurierte Sicherheits-Anmeldemethoden zulässig sind, können sich Benutzer unter Verwendung einer beliebigen Sicherheits-Anmeldemethode anmelden, wenn der Bildschirm „HP Password Manager“ angezeigt wird. Dieser Vorgang meldet den Benutzer bei Windows an.

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

Verwalten von Kennwörtern

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

Weitere Informationen zur Kennwortverwaltung finden Sie unter „Password Manager for HP ProtectTools“ auf Seite 27.

Festlegen von Anmeldeinformationen

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

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

Ändern des Windows Kennworts

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

So ändern Sie Ihr Windows Kennwort:

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

Einrichten einer Smart Card

Smart Card ist ein integrierter Teil von Security Manager. Die Smart Card-Einrichtung und -Konfiguration wird über die HP Smart Card-Tastatur durchgeführt. Smart Card ist ein persönliches Sicherheitsgerät, das Authentifizierungsdaten schützt, da für den Zugriff ähnlich wie bei einer Bankkarte sowohl die betreffende Karte als auch eine PIN-Nummer erforderlich ist. Smart Card kann für den Zugriff auf Password Manager, Drive Encryption PreBoot oder zukünftige Access Points

verwendet werden, die von Drittanbietern bereitgestellt werden. Die Smart Card-Optionen bleiben ausgeblendet, bis das Smart Card-Lesegerät erkannt wird.

Mit der Smart Card-Sicherheit, können die folgenden Aufgaben durchgeführt werden:

- Auf Smart Card-Sicherheitsfunktionen zugreifen
- Mit dem Dienstprogramm „Security Manager Setup“ arbeiten, um die Smart Card-Authentifizierung zu aktivieren
- Smart Card kann als authentische Methode für Drive Encryption Preboot verwendet werden
- Smart Card kann zusammen mit anderen Authentifizierungsmethoden verwendet werden
- Administrator-Konsole kann die PIN initialisieren

Initialisierung der Smart Card

HP ProtectTools Security Manager kann mehrere verschiedene Smart Cards unterstützen. Die Anzahl und Art der Zeichen, die als PIN-Nummer verwendet werden, können variieren. Der Hersteller der Smart Card sollte Tools zur Installation eines Sicherheitszertifikats und einer Management-PIN bereitstellen, die von ProtectTools in seinem Sicherheitsalgorithmus verwendet werden.

HINWEIS: Die Smart Card-Software des Herstellers stellt in der Regel einen Freischaltschlüssel bereit. Die meisten Smart Cards werden gesperrt, wenn die PIN fünfmal falsch eingegeben wird. Mithilfe des Freischaltschlüssels kann die Karte entsperrt werden.

1. Wenn die Smart Card mit der Software Herstellers eingerichtet wurde, stecken Sie die Karte in das Lesegerät.
2. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
3. Klicken Sie in der Administrator-Konsole auf **Geräte**, **Verwendung der Smart Card konfigurieren** (Configure the use of the smart card) und anschließend auf die Registerkarte **Smart Card einrichten** (Setup a Smart Card).
4. Stellen Sie sicher, dass die Option **Smart Card initialisieren** (Initialize the smart card) ausgewählt ist.
5. Geben Sie Ihre **PIN**-Nummer ein, klicken Sie auf die Schaltfläche **Übernehmen** und befolgen Sie die Anweisungen auf dem Bildschirm.
6. Nachdem die Smart Card erfolgreich initialisiert wurde, fahren Sie mit der Registrierung der Smart Card fort.

Registrieren der Smart Card

Nach der Initialisierung der Smart Card können Administratoren die Karte in der Administrator-Konsole als Authentifizierungsmethode registrieren oder Benutzer können sie im Security Manager registrieren.

Registrieren der Smart Card in der Administrator-Konsole:

1. Klicken Sie in der Administrator-Konsole unten links auf **Installations-Assistent**.
2. Klicken Sie auf dem **Willkommensbildschirm** auf **Weiter** und geben Sie Ihr Windows-Kennwort ein.
3. Klicken Sie im Fenster **SpareKey** auf **SpareKey-Einrichtung überspringen** (Skip SpareKey Setup) (außer, Sie möchten die SpareKey-Informationen aktualisieren).

4. Klicken Sie im Fenster **Sicherheitsfunktionen aktivieren** (Enable security features) auf **Weiter**.
5. Stellen sie sicher, dass im Fenster **Anmeldeinformationen auswählen** (Choose your credential) die Option **Smart Card** ausgewählt ist und klicken Sie auf **Weiter**.
6. Geben Sie im Fenster **Smart Card** Ihre **PIN**-Nummer ein und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.

Registrieren der Smart Card im Security Manager:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Erweitern Sie im Security Manager die **Anmeldeinformationen** und klicken Sie auf **Smart Card**.
3. Geben sie Ihr Windows-Kennwort und Ihre **PIN**-Nummer ein und klicken Sie anschließend auf **Speichern**.

Verwalten des Datenschutzes bei Verbindungen

Privacy Manager for HP ProtectTools ermöglicht die Verwendung erweiterter Sicherheits-Anmeldemethoden (Authentifizierungsmethoden), mit denen die Quelle, Integrität und Sicherheit der Verbindung überprüft wird, wenn E-Mails, Microsoft Office-Dokumente oder Instant Messaging (IM) verwendet werden.

Weitere Informationen zur Verwendung von Privacy Manager for HP ProtectTools finden Sie unter „Privacy Manager for HP ProtectTools“ auf Seite 36.

Shreddern und Bereinigen von Dateien

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

Weitere Informationen zur Verwendung von File Sanitizer for HP ProtectTools finden Sie unter „File Sanitizer for HP ProtectTools“ auf Seite 49.

Anzeigen des Verschlüsselungsstatus eines Laufwerks

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

So lassen Sie den Verschlüsselungsstatus eines Laufwerks anzeigen:

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

Anzeigen des Gerätezugriffs

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

So lassen Sie die Einstellungen für den Gerätezugriff anzeigen:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Erweitern Sie im linken Fenster von Security Manager die Option **Device Access Manager**.
3. Um anzeigen zu lassen, welchen Geräten der Zugriff verweigert ist, klicken Sie auf **Einfache Konfiguration**. Geräte mit verweigertem Zugriff sind durch ein Häkchen gekennzeichnet.
4. Um anzeigen zu lassen, welchen Benutzern oder Gruppen der Zugriff verweigert ist, klicken Sie auf **Geräteklassen-Konfiguration**.
5. Durch Klicken auf ein Gerät können Sie anzeigen lassen, welchen Benutzern oder Gruppen der Zugriff auf ein Gerät verwehrt bzw. gestattet ist.

Aktivieren der Diebstahlschutzfunktion

HP ProtectTools nutzt die von Absolute Software entwickelte Anwendung Computrace, um Computer remote zu überwachen, zu verwalten und zu verfolgen. Bei Verlust oder Diebstahl eines Computers kooperiert das Absolute-Team mit den zuständigen Behörden, um ihn wieder aufzufinden.

Weitere Information über die Verwendung von Computrace finden Sie unter „Computrace for HP ProtectTools“ auf Seite 67.

Hinzufügen von Anwendungen

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

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Wählen Sie im linken Fenster von Security Manager das Dropdown-Menü **Administration** aus und klicken Sie auf **Mehr erfahren**.

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

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

Festlegen von Einstellungen

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

So rufen Sie die Seite „Einstellungen“ auf:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fenster von Security Manager auf **Erweitert** und anschließend auf **Einstellungen**.
3. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Symbol in der Taskleiste anzeigen**, und klicken Sie dann auf **Übernehmen**.

Sichern und Wiederherstellen

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

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

Wenn Sie die Sicherungsdatei auf einem anderen Computer oder aber auf dem ursprünglichen Computer nach der Neuinstallation des Betriebssystems wiederherstellen, muss vor der Wiederherstellung der Daten aus der Sicherungsdatei HP ProtectTools Security Manager installiert worden sein.

Sichern von Daten

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

So sichern Sie Ihre Daten:

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

Wiederherstellen von Daten

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

So stellen Sie Ihre Daten wieder her:

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

Ändern von Windows Benutzername und Bild

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

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

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

4 Password Manager for HP ProtectTools

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

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

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

Zur Überprüfung Ihrer Identität verwendet HP ProtectTools Anmeldeinformationen wie beispielsweise Ihr Windows Kennwort oder eine Smart Card, wobei die genaue Vorgehensweise von der Konfiguration des Computers abhängig ist. Sie verwenden also ein und dieselben Anmeldeinformationen, um sich bei allen konfigurierten Anmeldebildschirmen anzumelden. Auf diese Weise können Sie effizientere Kennwörter festlegen, ohne sich diese notieren oder merken zu müssen, um Ihre Konten zuverlässig zu schützen.

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

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

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

Das Kontextmenü enthält die folgenden Optionen:

- [beliebigeDomäne.de] zu Password Manager hinzufügen - Mit dieser Option können Sie Anmeldedaten für den aktuellen Anmeldebildschirm hinzufügen.
- Password Manager öffnen - Startet Security Manager auf der Seite „Password Manager“.
- Einstellungen für das Password Manager-Symbol - Ermöglicht die Definition von Bedingungen, unter denen das Password Manager Symbol angezeigt wird.
- Hilfe - Öffnet die Online-Hilfe zu der Password Manager Anwendung.

Websites und Programme, für die bereits Anmeldedaten definiert wurden:

Das Kontextmenü enthält die folgenden Optionen:

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

HINWEIS: Unter Umständen hat Ihr Computeradministrator festgelegt, dass Security Manager mehrere Anmeldeinformationen benötigt, um Ihre Identität zu bestätigen.

Hinzufügen von Anmeldedaten

Anmeldedaten für eine Website oder ein Programm lassen sich schnell und einfach hinzufügen. Sie müssen die Anmeldedaten lediglich einmal auf der Website oder in dem Programm eingeben. Danach fügt Password Manager die betreffenden Daten automatisch für Sie ein. Sie können diese Anmeldedaten verwenden, nachdem Sie die Website oder das Programm durchsucht haben, oder Sie können einfach Anmeldedaten aus dem Anmeldemenü auswählen, um zu veranlassen, dass Password Manager die Website oder das Programm öffnet und Sie dort anmeldet.

So fügen Sie Anmeldedaten hinzu:

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

4. Klicken Sie auf **OK**. Das Password Manager-Symbol wird nun ohne Pluszeichen angezeigt und macht somit deutlich, dass die Anmeldedaten erstellt wurden.
5. Geben Sie das Windows-Kennwort ein, und klicken Sie auf den grünen Pfeil.

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

Bearbeiten von Anmeldedaten

So bearbeiten Sie Anmeldedaten:

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

Verwenden des Menüs „Anmeldedaten“

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

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

Zur Anzeige des Menüs „Anmeldedaten“ drücken Sie die Tastenkombination für Password Manager. Dies ist standardmäßig Strg+Win+H. In **Password Manager** unter „Windows-Kennwort“ > grüner Pfeil > **Einstellungen** können Sie jedoch auch eine andere Tastenkombination festlegen.

Zusammenfassen von Anmeldedaten in Kategorien

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

So fügen Sie eine Kategorie hinzu:

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

So nehmen Sie Anmeldedaten in eine Kategorie auf:

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

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

Verwalten von Anmeldedaten

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

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

So verwalten Sie Ihre Anmeldedaten:

Wählen Sie im linken Fenster von Security Manager die Option **Password Manager** und klicken Sie auf die Registerkarte **Verwalten**. Wählen Sie die Website, das Sie bearbeiten möchten.

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

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

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

Überprüfen der Kennwortstärke

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

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

Symboleinstellungen für Password Manager

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

Sie können die folgenden Einstellungen vornehmen:

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

Zur Konfiguration weiterer Einstellungen für Privacy Manager wählen Sie in Security Manager die Option **Password Manager** > „Windows-Kennwort“ > grüner Pfeil > **Einstellungen**.

5 Drive Encryption for HP ProtectTools

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

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

Drive Encryption for HP ProtectTools ist die branchenweit erste Software für die vollständige Datenträgerverschlüsselung, die als sofort einsatzbereite Lösung vorliegt. Durch die Verschlüsselung der Festplatte bietet sie einen umfassenden Datenschutz. Wenn Drive Encryption aktiviert ist, müssen Sie sich am Drive Encryption Anmeldebildschirm anmelden; dieser Bildschirm wird vor dem Starten von Windows angezeigt.

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

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

Drive Encryption:

- Ermöglicht die Verschlüsselung sämtlicher Daten auf den internen Festplatten des betreffenden Computers.
- Ermöglicht den einfachen Kennwortzugriff und die Authentifizierung vor dem Systemstart.
- Unterstützt Microsoft Windows XP, Windows Vista und Windows 7.
- Nutzen Sie den integrierten TPM (Trusted Platform Module)-Chip, wenn dieser vorhanden ist und eine Konfiguration mit TPM durchgeführt wurde.

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

- Verwalten von Drive Encryption
  - Aktivieren eines TPM-geschützten Kennworts
  - Verschlüsseln bzw. Entschlüsseln einzelner Laufwerke
  - Aktivieren eines SED-Laufwerks (Self Encrypting Drive)
- Sichern und Wiederherstellen
  - Erstellen von Sicherungsschlüsseln
  - Registrieren für die Online-Wiederherstellung
  - Verwalten eines vorhandenen Kontos für die Online-Wiederherstellung
  - Durchführen einer Wiederherstellung

△ **ACHTUNG:** Wenn Sie das Modul „Drive Encryption“ deinstallieren oder eine Sicherungs- und Wiederherstellungslösung verwenden, müssen Sie zunächst alle verschlüsselten Laufwerke entschlüsseln. Wenn Sie dies nicht tun, haben Sie nur Zugriff auf die verschlüsselten Laufwerke, wenn Sie sich beim HP Drive Encryption-Wiederherstellungsdienst registriert haben. Auch wenn Sie das Modul „Drive Encryption“ erneut installieren, haben Sie keinen Zugriff auf die verschlüsselten Daten.

Setup-Verfahren

Aufrufen von Drive Encryption

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

Allgemeine Aufgaben

Aktivieren von Drive Encryption

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

Deaktivieren von Drive Encryption

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

Anmelden, nachdem Drive Encryption aktiviert wurde

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

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

1. Wählen Sie Ihren Benutzernamen aus, und geben Sie dann Ihr Windows-Kennwort oder die PIN Ihrer Smart Card ein.
2. Klicken Sie auf **OK**.

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

Erweiterte Aufgaben

Verwalten von Drive Encryption (Administrator-Aufgabe)

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

Aktivieren eines TPM-geschützten Kennworts

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

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

1. Verwenden Sie Embedded Security für HP ProtectTools, um das TPM-geschützte Kennwort zu aktivieren.
2. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Drive Encryption**, und klicken Sie auf **Verschlüsselungsverwaltung**.
3. Aktivieren Sie das Kontrollkästchen **Sicherheit mit TPM erhöhen**.

Verschlüsseln oder Entschlüsseln einzelner Laufwerke

1. Erweitern Sie im linken Fenster der Administrator-Konsole die Option **Drive Encryption**, und klicken Sie auf **Verschlüsselungsverwaltung**.
2. Klicken Sie auf die Schaltfläche **Verschlüsselung ändern**.
3. Aktivieren oder deaktivieren Sie im Dialogfeld „Verschlüsselung ändern“ das Kontrollkästchen neben den einzelnen Festplatten, die Sie verschlüsseln oder entschlüsseln möchten, und klicken Sie dann auf **OK**.

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

Sicherung und Wiederherstellung (Administrator-Aufgabe)

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

Erstellen von Sicherungsschlüsseln

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

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

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

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

6 Privacy Manager for HP ProtectTools

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

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

- Windows Kennwort
- Smart Card

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

Aufrufen von Privacy Manager

So öffnen Sie Privacy Manager:

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

– ODER –

Klicken Sie im Infobereich ganz rechts in der Taskleiste mit der rechten Maustaste auf das Symbol **HP ProtectTools**, und wählen Sie **Privacy Manager for HP ProtectTools**. Klicken Sie anschließend auf **Konfiguration**.

– ODER –

Klicken Sie unter Microsoft Outlook in der Symbolleiste einer E-Mail-Nachricht neben **Sicher senden** auf den Pfeil nach unten und anschließend auf **Certificate Manager** oder **Trusted Contact Manager**.

– ODER –

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

Setup-Verfahren

Verwalten von Privacy Manager-Zertifikaten

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

eine Authentifizierung mit einem Verschlüsselungsschlüssel. Privacy Manager garantiert das sichere Speichern und Senden wichtiger Informationen.

Anfordern und Installieren eines Privacy Manager-Zertifikats

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

Anfordern eines Privacy Manager-Zertifikats

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf **Privacy Manager-Zertifikat anfordern**.
3. Lesen Sie den Text auf der Begrüßungsseite, und klicken Sie dann auf **Weiter**.
4. Lesen Sie die Lizenzvereinbarung auf der Seite „Lizenzvereinbarung“.
5. Aktivieren Sie das Kontrollkästchen neben **Hier aktivieren, um die Bedingungen dieses Lizenzvertrags zu akzeptieren**, und klicken Sie anschließend auf **Weiter**.
6. Geben Sie auf der Seite „Ihre Zertifikatdetails“ die angeforderten Informationen ein, und klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite „Zertifikatanforderung akzeptiert“ auf **Fertig stellen**.

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

Installieren eines Privacy Manager-Zertifikats

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

   △ **ACHTUNG:** Speichern Sie die Datei nicht auf der Festplatte, und bewahren Sie das Speichermedium an einem sicheren Platz auf. Diese Datei ist ausschließlich zu Ihrer Verwendung bestimmt und wird benötigt, wenn Sie Ihr Privacy Manager-Zertifikat und die zugehörigen Schlüssel wiederherstellen müssen.
5. Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.
6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
7. Wenn Sie den Trusted Contact-Einladungsprozess starten möchten, befolgen Sie die Anleitungen auf dem Bildschirm.

   – ODER –

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

Anzeigen von Details eines Privacy Manager-Zertifikats

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Certificate Manager**.
2. Klicken Sie auf ein **Privacy Manager-Zertifikat**.
3. Klicken Sie auf **Zertifikatdetails**.
4. Klicken Sie auf **OK**, um die Anzeige der Details zu schließen.

Erneuern eines Privacy Manager-Zertifikats

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

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Certificate Manager**.
2. Klicken Sie auf ein **Privacy Manager-Zertifikat**.
3. Klicken Sie auf **Zertifikat erneuern**.
4. Befolgen Sie die Anleitungen auf dem Bildschirm, um ein neues Privacy Manager-Zertifikat zu erwerben.

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

Festlegen eines Privacy Manager-Standardzertifikats

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

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

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Certificate Manager**.
2. Klicken Sie auf das Privacy Manager-Zertifikat, das als Standardzertifikat verwendet werden soll, und klicken Sie anschließend auf **Als Standard festlegen**.
3. Klicken Sie auf **OK**.

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

Löschen eines Privacy Manager-Zertifikats

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

So löschen Sie ein Privacy Manager-Zertifikat:

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

Wiederherstellen eines Privacy Manager-Zertifikats

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

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Migration**.
2. Klicken Sie auf **Wiederherstellen**.
3. Klicken Sie auf der Seite „Migrationsdatei“ auf **Durchsuchen**, um nach der .dppsm-Datei zu suchen, die Sie bei der Installation oder beim Export des Privacy Manager-Zertifikats erstellt haben. Klicken Sie dann auf **Weiter**.
4. Klicken Sie auf der Seite „Migrationsdatei importieren“ auf **Beenden**.
5. Klicken Sie auf **Schließen** und dann auf **Übernehmen**.

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

Widerrufen Ihres Privacy Manager-Zertifikats

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

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

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

Verwalten von Trusted Contacts

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

Hinzufügen von Trusted Contacts

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

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

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

Hinzufügen eines Trusted Contact

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, klicken Sie auf **Trusted Contacts** und anschließend auf **Kontakte einladen**.

   – ODER –

   Klicken Sie in Microsoft Outlook neben **Sicher senden** in der Symbolleiste auf den Pfeil nach unten und anschließend auf **Kontakte einladen**.
2. Nach dem Öffnen des Dialogfelds **Zertifikat auswählen** klicken Sie auf das Privacy Manager-Zertifikat, das Sie verwenden möchten. Klicken Sie abschließend auf **OK**.
3. Lesen Sie den Text im Dialogfeld **Trusted Contact-Einladung**, und klicken Sie dann auf **OK**.

   Es wird automatisch eine E-Mail erzeugt.

4. Geben Sie die E-Mail-Adressen der Empfänger ein, die Sie als Trusted Contacts hinzufügen möchten.
5. Bearbeiten Sie den Text, und unterschreiben Sie mit Ihrem Namen (optional).
6. Klicken Sie auf **Senden**.

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

7. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
8. Wenn Sie eine E-Mail-Antwort von einem Empfänger erhalten, der die Einladung, ein Trusted Contact zu werden, annimmt, klicken Sie unten rechts in der E-Mail auf **Akzeptieren**.

   Ein Dialogfeld wird geöffnet, das bestätigt, dass der Empfänger erfolgreich zu Ihrer Trusted Contacts-Liste hinzugefügt wurde.
9. Klicken Sie auf **OK**.

Hinzufügen von Trusted Contacts unter Verwendung des Microsoft Outlook-Adressbuchs

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, klicken Sie auf **Trusted Contact** und anschließend auf **Kontakte einladen**.

   – ODER –

   Klicken Sie in Microsoft Outlook neben **Sicher senden** in der Symbolleiste auf den Pfeil nach unten und anschließend auf **Meine Outlook-Kontakte einladen**.
2. Wählen Sie nach dem Öffnen der Seite „Trusted Contact-Einladung“ die E-Mail-Adressen der Empfänger aus, die Sie als Trusted Contacts hinzufügen möchten, und klicken Sie anschließend auf **Weiter**.
3. Wenn die Seite „Einladung wird gesendet“ geöffnet wird, klicken Sie auf **Beenden**.

   Es wird automatisch eine E-Mail mit den ausgewählten Microsoft Outlook-E-Mail-Adressen erzeugt.
4. Bearbeiten Sie den Text, und unterschreiben Sie mit Ihrem Namen (optional).
5. Klicken Sie auf **Senden**.

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

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

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

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

   Ein Dialogfeld wird geöffnet, das bestätigt, dass der Empfänger erfolgreich zu Ihrer Trusted Contacts-Liste hinzugefügt wurde.
8. Klicken Sie auf **OK**.

Anzeigen von Details zu Trusted Contacts

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Trusted Contacts Manager**.
2. Klicken Sie auf einen Trusted Contact.
3. Klicken Sie auf **Kontaktdetails**.
4. Klicken Sie auf **OK**, um die Anzeige der Details zu schließen.

Löschen eines Trusted Contact

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Trusted Contacts Manager**.
2. Klicken Sie auf den Trusted Contact, der gelöscht werden soll.
3. Klicken Sie auf **Kontakt löschen**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Prüfen des Widerruf-Status für einen Trusted Contact

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Trusted Contacts Manager**.
2. Klicken Sie auf einen Trusted Contact.
3. Klicken Sie auf die Schaltfläche **Erweitert**.

   Das Dialogfeld **Erweiterte Trusted Contact-Verwaltung** wird geöffnet.
4. Klicken Sie auf **Auf Widerruf prüfen**.
5. Klicken Sie auf **Schließen**.

Allgemeine Aufgaben

Verwenden von Privacy Manager in Microsoft Office

Nach der Installation des Privacy Manager-Zertifikats wird rechts in der Werkzeugliste aller mit Microsoft Office 2007 Word, Excel und PowerPoint erstellten Dokumente eine Schaltfläche „Signieren und Verschlüsseln“ angezeigt.

HINWEIS: Wenn Sie Microsoft Office 2007 verwenden, müssen alle Microsoft Updates installiert sein, da andernfalls einige signierte E-Mails im Spam-Ordner abgelegt werden.

Konfigurieren von Privacy Manager in einem Microsoft Office-Dokument

1. Klicken Sie im Infobereich ganz rechts in der Taskleiste mit der rechten Maustaste auf das Symbol **HP ProtectTools**, und wählen Sie **File Sanitizer**. Klicken Sie anschließend auf **Jetzt shreddern**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, klicken Sie auf **Einstellungen** und anschließend auf die Registerkarte **Dokumente**.

   – ODER –

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

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

Signieren eines Microsoft Office-Dokuments

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

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

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

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

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

1. Erstellen Sie in Microsoft Word oder Microsoft Excel ein Dokument, und speichern Sie es.
2. Klicken Sie auf das Menü **Startseite**.
3. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Signaturzeile vor Signieren hinzufügen**.

   HINWEIS: Bei aktivierter Option ist das Kontrollkästchen neben „Signaturzeile vor Signieren hinzufügen“ aktiviert. Diese Option ist standardmäßig aktiviert.

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

Hinzufügen empfohlener Signierer zu einem Microsoft Word- oder Microsoft Excel-Dokument

Sie können mehrere Signaturzeilen zu Ihrem Dokument hinzufügen, indem Sie empfohlene Signierer benennen. Ein empfohlener Signierer ist ein Benutzer, den der Eigentümer eines Microsoft Word- oder Microsoft Excel-Dokuments für das Hinzufügen einer Signaturzeile zu dem Dokument benennt. Bei empfohlenen Signierern kann es sich um Sie selbst oder eine andere Person, die Ihr Dokument signieren soll, handeln. Wenn Sie beispielsweise ein Dokument erstellen, das von allen Mitgliedern

Ihrer Abteilung signiert werden muss, können Sie für diese Benutzer am Ende der letzten Seite des Dokuments Signaturzeilen hinzufügen mit der Anleitung, das Dokument bis zu einem bestimmten Datum zu signieren.

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

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

   Das Dialogfeld „Einrichten der Signatur“ wird geöffnet.
4. Geben Sie in das Feld unter **Empfohlener Signierer** den Namen des empfohlenen Signierers ein.
5. Geben Sie in das Feld unter **Anleitungen für Signierer** eine Mitteilung für diesen empfohlenen Signierer ein.

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

6. Aktivieren Sie das Kontrollkästchen **Signierungsdatum in Signaturzeile anzeigen**, um das Datum anzuzeigen.
7. Aktivieren Sie das Kontrollkästchen **Titel des Signierers in Signaturzeile anzeigen**, um den Titel anzuzeigen.

HINWEIS: Wenn die Kontrollkästchen **Signierungsdatum in Signaturzeile anzeigen** und/oder **Titel des Signierers in Signaturzeile anzeigen** nicht aktiviert sind, sind die vom Dokumenteigentümer zugewiesenen, empfohlenen Signierer nicht in der Lage, das Datum und/oder den Titel in der Signaturzeile anzuzeigen, auch wenn die Dokumenteinstellungen des betreffenden empfohlenen Signierers entsprechend konfiguriert sind.

8. Klicken Sie auf **OK**.

Hinzufügen der Signaturzeile eines empfohlenen Signierers

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

So signieren Sie das Dokument:

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

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

Verschlüsseln eines Microsoft Office-Dokuments

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

So verschlüsseln Sie ein Microsoft Office-Dokument:

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

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

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

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

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

Entfernen der Verschlüsselung für ein Microsoft Office-Dokument

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

So entfernen Sie die Verschlüsselung für ein Microsoft Office-Dokument

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

Senden eines verschlüsselten Microsoft Office-Dokuments

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

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

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

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Schreiben Sie Ihre E-Mail-Nachricht.

3. Hängen Sie das Microsoft Office-Dokument an.
4. Weitere Anleitungen finden Sie im Abschnitt „Versiegeln und Senden einer E-Mail-Nachricht“.

Anzeigen eines signierten Microsoft Office-Dokuments

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

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

Anzeigen eines verschlüsselten Microsoft Office-Dokuments

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

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

Verwenden von Privacy Manager in Microsoft Outlook

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

HINWEIS: Wenn Sie Microsoft Office 2007 verwenden, müssen alle Microsoft Updates installiert sein, da andernfalls einige signierte E-Mails im Spam-Ordner abgelegt werden.

Konfigurieren von Privacy Manager für Microsoft Outlook

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, klicken Sie auf **Einstellungen** und anschließend auf die Registerkarte **E-Mail**.

   – ODER –

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

   – ODER –

   Klicken Sie in der Symbolleiste einer Microsoft Outlook-E-Mail-Nachricht neben **Sicher senden** auf den Pfeil nach unten und anschließend auf **Einstellungen**.
2. Wählen Sie die Aktionen aus, die ausgeführt werden sollen, wenn Sie eine sichere E-Mail senden, und klicken Sie anschließend auf **OK**.

Signieren und Senden einer E-Mail-Nachricht

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Geben Sie den E-Mail-Text ein.
3. Klicken Sie auf den Pfeil nach unten neben **Sicher senden** und dann auf **Signieren und Senden**.
4. Authentifizieren Sie sich unter Verwendung der ausgewählten Sicherheits-Anmeldemethode.

Versiegeln und Senden einer E-Mail-Nachricht

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

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

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

Anzeigen einer versiegelten E-Mail-Nachricht

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

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

Erweiterte Aufgaben

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

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

Exportieren von Privacy Manager-Zertifikaten und Trusted Contacts

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

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Migration**.
2. Klicken Sie auf **Migrationsdatei exportieren**.
3. Wählen Sie auf der Seite „Daten auswählen“ die Datenkategorien aus, die in die Migrationsdatei einbezogen werden sollen, und klicken Sie anschließend auf **Weiter**.
4. Geben Sie auf der Seite „Migrationsdatei“ einen Dateinamen ein, oder klicken Sie auf **Durchsuchen**, um nach einem Speicherort zu suchen, und klicken Sie dann auf **Weiter**.
5. Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.

   HINWEIS: Bewahren Sie dieses Kennwort an einem sicheren Ort auf, da Sie es benötigen, um die Migrationsdatei zu importieren.
6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
7. Klicken Sie auf der Seite „Migrationsdatei gespeichert“ auf **Beenden**.

Importieren von Privacy Manager-Zertifikaten und Trusted Contacts

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

1. Erweitern Sie im linken Fenster von Security Manager die Option **Privacy Manager**, und klicken Sie dann auf **Migration**.
2. Klicken Sie auf **Migrationsdatei importieren**.
3. Wählen Sie auf der Seite „Daten auswählen“ die Datenkategorien aus, die in die Migrationsdatei einbezogen werden sollen, und klicken Sie anschließend auf **Weiter**.
4. Geben Sie auf der Seite „Migrationsdatei“ einen Dateinamen ein, oder klicken Sie auf **Durchsuchen**, um nach einem Speicherort zu suchen, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf der Seite „Migrationsdatei importieren“ auf **Beenden**.

7 File Sanitizer for HP ProtectTools

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

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

Informationen zum Shreddern

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

Das Shreddern unterscheidet sich vom üblichen Löschvorgang unter Windows (dieser wird in File Sanitizer auch als „einfaches Löschen“ bezeichnet), da beim Shreddern von Datenbeständen ein spezieller Algorithmus zum Einsatz kommt, der die Daten verbirgt und es quasi unmöglich macht, sie nachträglich wiederherzustellen.

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

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

Informationen zur Festplattenbereinigung.

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

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

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

Setup-Verfahren

Öffnen von File Sanitizer

So öffnen Sie File Sanitizer:

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

– ODER –

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

  – ODER –

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

Planen der Festplattenbereinigung

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

So erstellen Sie einen Zeitplan für die Festplattenbereinigung:

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

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

Planen eines Shred-Vorgangs

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, und klicken Sie dann auf **Shreddern**.
2. Wählen Sie eine Shred-Option:

   - **Beim Herunterfahren von Windows**: Wenn diese Option aktiviert ist, werden alle ausgewählten Datenbestände beim Herunterfahren von Windows geshreddert.

     HINWEIS: Wenn Sie diese Option aktivieren, wird beim Herunterfahren ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob Sie mit dem Shreddern der ausgewählten Datenbestände fortfahren oder den Vorgang überspringen möchten. Klicken Sie auf „Ja“, um das Shreddern zu überspringen, auf „Nein“, wenn Sie mit dem Shred-Vorgang fortfahren möchten. Die gewünschte Option muss schnell gewählt werden, da Windows die Software während des Herunterfahrens schließt und dann eventuell ein Fehler auftritt. Wenn Sie mit „Nein“ den Shred-Vorgang fortsetzen möchten, zeigt Windows unter Umständen eine Fehlermeldung an, die angibt, dass File Sanitizer nicht reagiert. Warten Sie, bis File Sanitizer den Shred-Vorgang beendet hat, und leiten Sie dann das Herunterfahren erneut ein.

   - **Beim Öffnen eines Webbrowsers**: Wählen Sie diese Option, um alle ausgewählten Web-bezogenen Datenbestände, z. B. URL-Verlauf des Browsers, zu shreddern, sobald ein Webbrowser geöffnet wird.
   - **Beim Schließen eines Webbrowsers**: Wählen Sie diese Option, um alle ausgewählten Web-bezogenen Datenbestände, z. B. URL-Verlauf des Browsers, zu shreddern, sobald ein Webbrowser geschlossen wird.

- **Tastenfolge**: Wählen Sie diese Option, um das Shreddern unter Verwendung einer bestimmten Tastenfolge einzuleiten.
- **Planer**: Aktivieren Sie das Kontrollkästchen **Planer aktivieren**, geben Sie Ihr Windows Kennwort ein, und tragen Sie anschließend Tag und Uhrzeit für das Shreddern bestimmter Datenbestände ein.

3. Klicken Sie auf das Symbol **Speichern**.

Auswählen oder Erstellen eines Shred-Profils

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

Auswählen eines vordefinierten Shred-Profils

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

So wählen Sie ein vordefiniertes Shred-Profil aus:

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf ein vordefiniertes Shred-Profil.
3. Klicken Sie auf **Details anzeigen**, um die Liste der Datenbestände, die für den Shred-Vorgang ausgewählt wurden, anzuzeigen.
4. Aktivieren Sie unter **Folgende Elemente shreddern** das Kontrollkästchen neben jedem Datenbestand, für den Sie das Shreddern bestätigen möchten.
5. Klicken Sie auf **Übernehmen**.

Anpassen eines Shred-Profils für erhöhte Sicherheit

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

1. Erweitern Sie im linken Fenster von Security Manager die Option **File Sanitizer**, klicken Sie auf **Einstellungen**, wählen Sie **Einstellungen für erweiterte Sicherheit**, und klicken Sie dann auf **Details anzeigen**.
2. Geben Sie die Anzahl der Shred-Zyklen an.

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

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

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

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

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

5. Klicken Sie unter **Folgende Elemente nicht shreddern** auf **Hinzufügen**, um die Datenbestände auszuwählen, die vom Shreddern ausgeschlossen werden sollen.
6. Wenn Sie die Konfiguration des Shred-Profils abgeschlossen haben, klicken Sie auf **Übernehmen**.

Anpassen eines Profils für einfaches Löschen

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

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

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

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

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

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

Allgemeine Aufgaben

Verwenden von Tastenfolgen zum Einleiten des Shred-Vorgangs

Gehen Sie folgendermaßen vor, um eine Tastenfolge festzulegen:

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

   Um zum Beispiel das automatische Shreddern mit der Tastenfolge Strg+Umschalttaste und S auszulösen, geben Sie in das dafür vorgesehene Feld den Buchstaben S ein und aktivieren die Optionen **strg** und **Umschalttaste**.

HINWEIS: Achten Sie darauf, keine bereits für andere Zwecke konfigurierte Tastenfolge zu verwenden.

So leiten Sie den Shred-Vorgang mit einer Tastenfolge ein:

1. Halten Sie die Taste Strg, Alt, Umschalttaste oder eine von Ihnen festgelegte Tastenkombination gedrückt, und drücken Sie das gewünschte Zeichen.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Verwenden des Symbols „File Sanitizer“

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

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

Manuelles Shreddern eines Datenbestands

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

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

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

3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Desktop, und klicken Sie dann auf **Shreddern**.
2. Das Dialogfeld **Durchsuchen** wird geöffnet. Navigieren Sie zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

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

Manuelles Shreddern aller ausgewählten Datenbestände

1. Klicken Sie im Infobereich ganz rechts in der Taskleiste mit der rechten Maustaste auf das Symbol **HP ProtectTools**, und wählen Sie **File Sanitizer**. Klicken Sie anschließend auf **Jetzt shreddern**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Desktop, und klicken Sie dann auf **Jetzt shreddern**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Aktivieren der Festplattenbereinigung

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

– ODER –

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

Abbrechen eines Shred-Vorgangs oder einer Festplattenbereinigung

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

So brechen Sie den Vorgang ab:

▲ Klicken Sie auf die Meldung und anschließend auf **Stop**, um den Vorgang abzubrechen.

Anzeigen der Protokolldateien

Für jeden Shred-Vorgang und jede Festplattenbereinigung werden Protokolldateien erzeugt, die eventuell während der Ausführung aufgetretene Fehler aufzeichnen. Die Protokolldateien werden immer wieder aktualisiert, sodass sich ihr Inhalt jeweils auf den letzten Shred-Vorgang bzw. die letzte Festplattenbereinigung bezieht.

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

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

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

8 Embedded Security for HP ProtectTools

HINWEIS: Der integrierte TPM-Sicherheits-Chip (Trusted Platform Module) muss auf Ihrem Computer installiert sein, damit Sie Embedded Security for HP ProtectTools verwenden können. Die meisten kommerziellen HP Desktop-Computer verfügen über den Infineon TPM, der der einzige zertifizierte Chip mit gemeinsamen Kriterien ist, der die TCG-Spezifikationen erfüllt.

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

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

Mit dem TPM-Sicherheitschip werden die Sicherheitsfunktionen von HP ProtectTools Security Manager erweitert und aktiviert. Drive Encryption for HP ProtectTools kann den eingebetteten Chip beispielsweise als Authentifizierungsfaktor verwenden, wenn sich Benutzer bei Windows anmelden.

Setup-Verfahren

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

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

Installieren von Embedded Security for HP ProtectTools (wenn erforderlich)

So installieren Sie Embedded Security for HP ProtectTools:

1. Klicken Sie auf **Start**, **Alle Programme** und anschließend auf **HP ProtectTools Security Manager installieren**.
2. **Akzeptieren** Sie die UAC-Warnung.
3. Klicken Sie auf **Weiter**, und geben Sie dann den Benutzernamen sowie ggf. den Unternehmensnamen ein.

4. Klicken Sie auf **Weiter** und danach auf **Installieren**. Nach Abschluss der Installation klicken Sie auf **Fertig stellen**.
5. Wenn die Aufforderung zum Systemneustart angezeigt wird, wählen Sie **Ja** oder **Nein**.

Aktivieren des eingebetteten Sicherheitschips in Computer Setup

Der eingebettete Sicherheitschip kann im Assistenten für die Schnellinitialisierung oder im Dienstprogramm „Computer Setup“ aktiviert werden (siehe unten).

So aktivieren Sie den eingebetteten Sicherheitschip in Computer Setup:

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

Initialisieren des Chips für integrierte Sicherheit

Während des Initialisierungsvorgangs für Embedded Security führen Sie Folgendes aus:

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

So initialisieren Sie den Chip für integrierte Sicherheit:

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

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

2. Folgen Sie den Anleitungen auf dem Bildschirm.

Einrichten von allgemeinen Benutzerkonten

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

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

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

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

1. Wenn der Assistent zur Benutzerinitialisierung bei Embedded Security nicht geöffnet ist, klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließen auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Benutzereinstellungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Embedded Security Funktionen** auf **Konfigurieren**.

   Der Assistent für die Benutzerinitialisierung der Embedded Security wird geöffnet.

4. Folgen Sie den Anleitungen auf dem Bildschirm.

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

Allgemeine Aufgaben

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

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

PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk)

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

Verschlüsseln von Dateien und Ordnern

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

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

HINWEIS: Unter Windows Home wird die Verschlüsselung von Dateien und Ordnern nicht unterstützt.

So verschlüsseln Sie Dateien und Ordner:

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

Senden und Empfangen verschlüsselter E-Mails

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

Erweiterte Aufgaben

Sichern und Wiederherstellen

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

Erstellen einer Sicherungsdatei

So erstellen Sie eine Sicherungsdatei:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Fenster auf **Konfigurieren**. Der Sicherungsassistent für HP Embedded Security for HP ProtectTools wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Wiederherstellen von Daten aus der Sicherungsdatei

So stellen Sie die Daten aus der Sicherungsdatei wieder her:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Fenster auf **Alle wiederherstellen**. Der Sicherungsassistent für HP Embedded Security for HP ProtectTools wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Ändern des Eigentümerkennworts

So ändern Sie das Eigentümerkennwort:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Erweitert**.
3. Klicken Sie im rechten Fensterausschnitt unter **Besitzer-Kennwort** auf **Ändern**.
4. Geben Sie zuerst das alte Eigentümerkennwort ein. Geben Sie dann das neue Eigentümerkennwort ein, und bestätigen Sie das neue Kennwort.
5. Klicken Sie auf **OK**.

Erneutes Einrichten eines Benutzerkennworts

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

Migrieren von Schlüsseln mithilfe des Migrationsassistenten

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

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

9 Device Access Manager for HP ProtectTools

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

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

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

Starten des Hintergrunddienstes

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

Einfache Konfiguration

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

Mit dieser Funktion können Sie folgenden Geräteklassen den Zugriff verweigern:

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

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

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Device Access Manager** und anschließend auf **Einfache Konfiguration**.

3. Aktivieren Sie im rechten Fensterausschnitt das Kontrollkästchen eines Geräts, dem Sie den Zugriff verweigern möchten.
4. Klicken Sie auf das Symbol **Speichern**.

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

5. Klicken Sie auf **OK**.

Geräteklassen-Konfiguration (erweitert)

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

Hinzufügen eines Benutzers oder einer Gruppe

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

Entfernen eines Benutzers oder einer Gruppe

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

Verweigern oder Zulassen des Zugriffs durch einen Benutzer oder eine Gruppe

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Erweitern Sie im linken Fenster die Option **Device Access Manager**, und klicken Sie dann auf **Geräteklassen-Konfiguration**.
3. Klicken Sie in der Geräteliste auf die Geräteklasse, die Sie konfigurieren möchten.

4. Klicken Sie unter **Benutzer/Gruppen** auf den Benutzer oder die Gruppe, dem/der Sie den Zugriff verweigern möchten.
5. Klicken Sie neben dem Benutzer oder der Gruppe, welchem/welcher der Zugriff verweigert werden soll, auf **Verweigern**.
6. Klicken Sie auf das Symbol **Speichern** und anschließend auf **OK**.

Just In Time Authentication Configuration (JITA)

Die Seite „JITA Configuration“ ermöglicht dem Administrator, Listen von Benutzern und Gruppen anzuzeigen und zu ändern, die Just In Time Authentication (JITA) nutzen dürfen. JITA-aktivierte Benutzer können auf Geräte zugreifen, die durch Richtlinien eingeschränkt sind, die in der Ansicht „Device Class Configuration“ oder „Simple Configurations“ erstellt wurden.

Fall: Eine Simple Configuration-Richtlinie wird konfiguriert, damit Administratoren, die nicht für das Gerät registriert sind, nicht auf das DVD/CD-ROM-Laufwerk zugreifen können.

Ergebnis: Ein JITA-aktivierte Benutzer versucht, auf ein DVD/CD-ROM-Laufwerk zuzugreifen, und erhält ebenso wie ein Nicht-JITA-aktivierter Benutzer die Meldung, dass der Zugriff verweigert wurde. Zusätzlich wird der Benutzer in einem Popup-Fenster nach seinen Anmeldeinformationen gefragt. Sobald sich der Benutzer erfolgreich beim Security Manager identifiziert hat, erhält er Zugriff auf das DVD/CD-ROM-Laufwerk.

Der autorisierte JITA-Zeitraum kann für eine bestimmt Anzahl von Minuten oder für 0 Minuten festgelegt werden. Ein JITA-Zeitraum von 0 Minuten läuft nicht ab. Der Benutzer erhält vom Zeitpunkt der Authentifizierung bis zur Abmeldung vom System Zugriff auf das Gerät.

Der JITA-Zeitraum kann auch erweitert werden. In diesem Fall kann der Benutzer eine Minute vor dem Ablauf des JITA-Zeitraums auf die angezeigte Eingabeaufforderung klicken und die Zugriffszeit verlängern, ohne sich erneut authentifizieren zu müssen.

Unabhängig davon, ob der Benutzer einen begrenzten oder unbegrenzten JITA-Zeitraum erhält, läuft der Zeitraum ab, sobald der Benutzer sich vom System abmeldet oder sich mit einem anderen Benutzernamen anmeldet. Wenn sich der Benutzer das nächste Mal anmeldet und auf das JITA-aktivierte Gerät zugreift, wird er nach seinen Anmeldeinformationen gefragt. JITA ist derzeit für die folgenden Geräteklassen verfügbar:

- DVD/CD-ROM
- Wechseldatenträger

Dieser Abschnitt enthält Informationen zu folgenden Themen:

- Erstellen von JITA für einen Benutzer oder eine Gruppe
- Erstellen eines erweiterbaren JITA-Zugriffs für einen Benutzer oder eine Gruppe
- Deaktivieren von JITA für einen Benutzer oder eine Gruppe

Erstellen von JITA für einen Benutzer oder eine Gruppe

Administratoren können Benutzern oder Gruppen mithilfe der Just In Time Authentication Zugriff auf Geräte gewähren.

1. Klicken Sie im linken Fenster der HP ProtectTools Administrative Console auf **Device Access Manager** und anschließend auf **JITA Configuration**.
2. Wählen Sie im Dropdown-Menü des Geräts **Wechseldatenträger** oder **DVD/CD-ROM-Laufwerke**.

3. Fügen Sie mithilfe der **+**-Schaltfläche der JITA Configuration einen Benutzer oder eine Gruppe hinzu.
4. Klicken Sie auf das Kontrollkästchen **Aktiviert**.
5. Legen Sie die erforderliche Zeit für den JITA-Zeitraum fest.
6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Der ausgewählte Benutzer kann sich jetzt anmelden, beim Security Manager authentifizieren und auf das Gerät zugreifen.

Erstellen eines erweiterbaren JITA-Zugriffs für einen Benutzer oder eine Gruppe

Administratoren können Benutzern oder Gruppen mithilfe der Just In Time Authentication Zugriff auf Geräte gewähren.

1. Klicken Sie im linken Fenster der HP ProtectTools Administrative Console auf **Device Access Manager**und anschließend auf **JITA Configuration**.
2. Wählen Sie im Dropdown-Menü des Geräts **Wechseldatenträger** oder **DVD/CD-ROM-Laufwerke**.
3. Fügen Sie mithilfe der **+**-Schaltfläche der JITA Configuration einen Benutzer oder eine Gruppe hinzu.
4. Klicken Sie auf das Kontrollkästchen **Aktiviert**.
5. Legen Sie die erforderliche Zeit für den JITA-Zeitraum fest.
6. Klicken Sie auf das Kontrollkästchen **Erweiterbar** (Extendable).
7. Klicken Sie auf die Schaltfläche **Übernehmen**.

Der ausgewählte Benutzer kann sich jetzt anmelden, beim Security Manager authentifizieren und auf das Gerät zugreifen. Eine Minute vor dem Ablauf des JITA-Zeitraums wird der Benutzer dazu aufgefordert, den JITA-Zeitraum zu verlängern.

Deaktivieren von JITA für einen Benutzer oder eine Gruppe

Administratoren können Benutzern oder Gruppen mithilfe der Just In Time Authentication Zugriff auf Geräte verweigern.

1. Klicken Sie im linken Fenster der HP ProtectTools Administrative Console auf **Device Access Manager** und anschließend auf **JITA Configuration**.
2. Wählen Sie im Dropdown-Menü des Geräts **Wechseldatenträger** oder **DVD/CD-ROM-Laufwerke**.
3. Wählen Sie den Benutzer aus, dessen JITA-Zugriff Sie deaktivieren möchten.
4. Klicken Sie auf das Kontrollkästchen **Aktiviert**, um es zu deaktivieren.
5. Klicken Sie auf die Schaltfläche **Übernehmen**.

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

Erweiterte Einstellungen

Die Seite „Erweiterte Einstellungen“ bietet die folgenden Funktionen:

- Verwaltung der Geräteadministratorgruppe
- Verwaltung der Laufwerkbuchstaben auf die der Zugriff durch den Device Access Manager immer erlaubt wird.

Die Geräteadministratorgruppe wird verwendet, um vertrauenswürdige Benutzer (im Rahmen des Zugriffs auf das Gerät) von den Einschränkungen durch die Device Access Manager-Richtlinie auszuschließen. Geeignete Benutzer sind in der Regel Systemadministratoren.

Die Ansicht „Erweiterte Einstellungen“ ermöglicht dem Administrator auch, eine Liste von Laufwerkbuchstaben zu konfigurieren zu denen der Zugriff durch den Device Access Manager für keinen Benutzer eingeschränkt wird. Um die Liste von Laufwerkbuchstaben zu konfigurieren, müssen die Hintergrunddienste des Device Access Manager ausgeführt werden. Diese Dienste können am einfachsten mithilfe einer Simple Configuration-Richtlinie gestartet werden, die allen Nicht-Geräte-Administratoren den Zugriff auf Wechseldatenträger verweigert.

10 Computrace for HP ProtectTools

Computrace for HP ProtectTools ist ein Tool, das die Remote-Überwachung, -Verwaltung und -Verfolgung von Computern ermöglicht.

Nach der Aktivierung wird Computrace for HP ProtectTools über das Absolute Software Customer Center konfiguriert. Von dort aus kann der Administrator Computrace for HP ProtectTools für die Überwachung oder Verwaltung des Computers konfigurieren. Bei Verlust oder Diebstahl des Systems unterstützen die Experten des Customer Center die zuständigen Behörden bei der Lokalisierung und Sicherstellung des Computers. Bei entsprechender Konfiguration funktioniert Computrace auch dann, wenn die Festplatte des Computers gelöscht oder ausgetauscht wurde.

So aktivieren Sie Computrace for HP ProtectTools:

1. Stellen Sie eine Internetverbindung her.
2. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
3. Klicken Sie im linken Fenster von Security Manager auf **Wiedererlangen bei Diebstahl**.
4. Zum Starten des Aktivierungsassistenten von Computrace klicken Sie auf die Schaltfläche **Jetzt aktivieren**.
5. Geben Sie Ihre Kontaktdaten sowie Ihre Kreditkartendaten oder einen vorab erworbenen Produktschlüssel ein.

Der Aktivierungsassistent führt die Transaktion sicher durch und richtet auf der Website des Absolute Software Customer Center Ihr Benutzerkonto ein. Im Anschluss daran erhalten Sie eine Bestätigungs-E-Mail mit Ihren Kontodaten.

Wenn Sie den Aktivierungsassistenten von Computrace bereits ausgeführt haben und beim Customer Center schon ein Benutzerkonto für Sie existiert, können Sie von Ihrem zuständigen HP Ansprechpartner zusätzliche Lizenzen erwerben.

So melden Sie sich beim Customer Center an:

1. Besuchen Sie die Website https://cc.absolute.com/.
2. Geben Sie in den Feldern **Anmelde-ID** und **Kennwort** die Anmeldeinformationen ein, die Sie mit der Bestätigungs-E-Mail erhalten haben. Klicken Sie dann auf **Anmelden**.

Das Customer Center bietet Ihnen folgende Möglichkeiten:

- Überwachung Ihrer Computer
- Schutz Ihrer Remote-Daten
- Melden Sie den Diebstahl von Computern mit Computrace-Diebstahlschutz.

Klicken Sie auf **Weitere Informationen**, um mehr über Computrace for HP ProtectTools zu erfahren.

Glossar

Administrator:
Siehe Windows Administrator.

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

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

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

Authentifizierung beim Systemstart:
Sicherheitsfunktion, die ein Kennwort erfordert, wenn der Computer eingeschaltet wird.

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

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

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

Bereinigung:
Siehe **Festplattenbereinigung**.

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

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

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

Digitales Zertifikat:

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

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

Drive Encryption-Anmeldebildschirm:
Ein Anmeldebildschirm wird vor dem Windows-Start angezeigt. Benutzer müssen ihren Windows-Benutzernamen und ihr Kennwort oder ihre Smart Card-PIN eingeben. Wenn Sie die richtigen Informationen auf dem Drive Encryption-Anmeldebildschirm eingeben, erhalten sie in der Regel direkten Zugriff auf Windows, ohne sich erneut auf dem Windows-Anmeldebildschirm anmelden zu müssen.

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

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

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

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

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

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

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

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

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

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

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

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

Notfallwiederherstellungsarchiv:

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

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

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

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

Schaltfläche „Sicher senden“:
Eine Softwareschaltfläche in der Symbolleiste von Microsoft Outlook-E-Mail-Nachrichten. Klicken Sie auf diese Schaltfläche, um eine Microsoft Outlook-E-Mail-Nachricht zu signieren und/oder zu verschlüsseln.

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

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

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

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

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

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

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

Smart Card.
Eine tragbare Karte, die in den Computer gesteckt wird. Sie enthält Identifikationsinformationen für die Anmeldung. Bei der Anmeldung mit Smart Card über den Drive Encryption-Anmeldebildschirm müssen Sie Ihre Smart Card in den Computer stecken und Ihren Benutzernamen und Ihre Smart Card-PIN eingeben.

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

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

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

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

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

Trusted Contacts-Liste:
Eine Liste der Trusted Contacts.

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

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

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

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

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

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

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

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

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

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

Index