

HP ProtectTools

Einführung

© Copyright 2011 Hewlett-Packard
Development Company, L.P.

Bluetooth ist eine Marke ihres Inhabers und wird von Hewlett-Packard Company in Lizenz verwendet. Intel ist eine Marke der Intel Corporation in den USA und anderen Ländern und wird in Lizenz verwendet. Microsoft, Windows und Windows Vista sind eingetragene Marken der Microsoft Corporation in den USA.

HP haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument. Ferner übernimmt sie keine Haftung für Schäden, die direkt oder indirekt auf die Bereitstellung, Leistung und Nutzung dieses Materials zurückzuführen sind. HP haftet – ausgenommen für die Verletzung des Lebens, des Körpers, der Gesundheit oder nach dem Produkthaftungsgesetz – nicht für Schäden, die fahrlässig von HP, einem gesetzlichen Vertreter oder einem Erfüllungsgehilfen verursacht wurden. Die Haftung für grobe Fahrlässigkeit und Vorsatz bleibt hiervon unberührt.

Inhaltliche Änderungen dieses Dokuments behalten wir uns ohne Ankündigung vor. Die Informationen in dieser Veröffentlichung werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt. Insbesondere enthalten diese Informationen keinerlei zugesicherte Eigenschaften. Alle sich aus der Verwendung dieser Informationen ergebenden Risiken trägt der Benutzer.

Die Garantien für HP Produkte und Services werden ausschließlich in der zum Produkt bzw. Service gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten.

Erste Ausgabe: Januar 2011

Teilenummer des Dokuments: 638391-041

Inhaltsverzeichnis

1 Einführung in die Sicherheitsfunktionen	1
HP ProtectTools Funktionen	2
HP ProtectTools – Beschreibung und allgemeine Nutzungsbeispiele der Sicherheitsprodukte	4
Credential Manager for HP ProtectTools	4
Drive Encryption for HP ProtectTools	4
File Sanitizer for HP ProtectTools	5
Device Access Manager for HP ProtectTools	5
Privacy Manager for HP ProtectTools	6
Computrace for HP ProtectTools (zuvor LoJack Pro)	6
Embedded Security for HP ProtectTools (nur ausgewählte Modelle)	7
Lösungen für grundlegende Sicherheitsaufgaben	8
Schutz vor gezieltem Diebstahl	8
Einschränken des Zugriffs auf sensible Daten	8
Verhindern des unbefugten Zugriffs von internen oder externen Standorten	8
Erstellen von Richtlinien für starke Kennwörter	10
Weitere Sicherheitselemente	11
Zuweisen von Sicherheitsrollen	11
Verwalten der Kennwörter für HP ProtectTools	11
Erstellen eines sicheren Kennworts	13
Sichern und Wiederherstellen von HP ProtectTools Anmeldedaten	13
2 Einführung in den Installations-Assistenten	14
3 HP ProtectTools Security Manager Administrator-Konsole	17
Öffnen von HP ProtectTools Administrator-Konsole	18
Verwenden der Administrator-Konsole	19
Konfigurieren des Systems	20
Einrichten der Authentifizierung für Ihren Computer	20
Anmelderichtlinie	20
Sitzungsrichtlinie	21
Einstellungen	21

Verwalten von Benutzern	21
Anmeldeinformationen	22
SpareKey	22
Fingerabdrücke	23
Smart Card	24
Gesicht	24
Konfigurieren der Anwendungen	26
Registerkarte „Allgemein“	26
Registerkarte „Anwendungen“	26
Zentrale Verwaltung	27

4 HP ProtectTools Security Manager 28

Öffnen von Security Manager	29
Verwenden des Security Manager Dashboards	30
Status der Sicherheitsanwendungen	32
My Logons (Meine Anmeldedaten)	33
Password Manager	33
Für Webseiten oder Programme, für die noch keine Anmeldedaten festgelegt wurden	33
Für Webseiten oder Programme, für die bereits Anmeldedaten festgelegt wurden	34
Hinzufügen von Anmeldedaten	34
Bearbeiten von Anmeldedaten	35
Verwenden des Menüs „Anmeldedaten“	36
Organisieren von Anmeldedaten in Kategorien	36
Verwalten Ihrer Anmeldedaten	37
Einschätzen der Kennwortsicherheit	38
Einstellungen für das Password Manager Symbol	38
VeriSign Identity Protection (VIP)	39
Einstellungen	40
Credential Manager	40
Ändern Ihres Windows Kennworts	41
Einrichten eines SpareKey	41
Registrieren Ihrer Fingerabdrücke	41
Einrichten einer Smart Card	42
Initialisieren der Smart Card	42
Registrieren der Smart Card	43
Konfigurieren der Smart Card	43
Registrieren von Gesichtsszenen für die Gesichtserkennung	44
Erweiterte Benutzereinstellungen	46
Ihre persönliche ID-Card	48

Festlegen der Einstellungen	48
Sichern und Wiederherstellen Ihrer Daten	49
5 Drive Encryption for HP ProtectTools (nur ausgewählte Modelle)	51
Öffnen von Drive Encryption	51
Allgemeine Aufgaben	52
Aktivieren von Drive Encryption für Standard-Festplatten	52
Aktivieren von Drive Encryption für selbstverschlüsselnde Festplatten	52
Deaktivieren von Drive Encryption	54
Anmelden, nachdem Drive Encryption aktiviert wurde	55
Schützen Ihrer Daten durch Verschlüsselung der Festplatte	56
Anzeigen der Verschlüsselungsstatus	56
Erweiterte Aufgaben	57
Verwalten von Drive Encryption (Administrator-Aufgabe)	57
Ver- und Entschlüsseln einzelner Laufwerke (nur Softwareverschlüsselung) ..	58
Sicherung und Wiederherstellung (Administrator-Aufgabe)	58
Sichern von Verschlüsselungsschlüsseln	58
Wiederherstellen von Verschlüsselungsschlüsseln	59
6 Privacy Manager for HP ProtectTools (bestimmte Modelle)	60
Öffnen von Privacy Manager	61
Setup-Verfahren	62
Verwalten von Privacy Manager Zertifikaten	62
Anfordern eines Privacy Manager-Zertifikats	62
Abrufen eines vorab zugewiesenen Privacy Manager-Unternehmenszertifikats	63
Einrichten eines Privacy Manager-Zertifikats	63
Importieren eines Zertifikats von einem anderen Anbieter	63
Anzeigen der Details eines Privacy Manager-Zertifikats	64
Erneuern eines Privacy Manager-Zertifikats	64
Festlegen eines Privacy Manager-Standardzertifikats	66
Löschen eines Privacy Manager-Zertifikats	66
Wiederherstellen eines Privacy Manager-Zertifikats	66
Widerrufen eines Privacy Manager-Zertifikats	67
Verwalten vertrauenswürdiger Kontakte	67
Hinzufügen von vertrauenswürdigen Kontakten	67
Hinzufügen eines vertrauenswürdigen Kontakts	68
Hinzufügen von vertrauenswürdigen Kontakten unter Verwendung der Microsoft Outlook-Kontakte	68
Anzeigen von Details zu vertrauenswürdigen Kontakten	69
Löschen eines vertrauenswürdigen Kontakts	69

Prüfen des Widerruf-Status für einen vertrauenswürdigen Kontakt	69
Allgemeine Aufgaben	71
Verwenden von Privacy Manager in Microsoft Outlook	71
Konfigurieren von Privacy Manager für Microsoft Outlook	71
Signieren und Senden einer E-Mail-Nachricht	72
Versiegeln und Senden einer E-Mail-Nachricht	72
Anzeigen einer versiegelten E-Mail-Nachricht	72
Verwenden von Privacy Manager in einem Microsoft Office 2007 Dokument	72
Konfigurieren von Privacy Manager für Microsoft Office	73
Signieren eines Microsoft Office-Dokuments	73
Hinzufügen einer Signaturzeile beim Signieren eines Microsoft Word- oder Microsoft Excel-Dokuments	73
Hinzufügen eines empfohlenen Signierers zu einem Microsoft Word- oder Microsoft Excel-Dokument	74
Hinzufügen der Signaturzeile eines empfohlenen Signierers	74
Verschlüsseln eines Microsoft Office-Dokuments	75
Eine Verschlüsselung von einem Microsoft Office-Dokument entfernen	75
Versenden eines verschlüsselten Microsoft Office-Dokuments	76
Anzeigen eines signierten Microsoft Office-Dokuments	76
Anzeigen eines verschlüsselten Microsoft Office-Dokuments	76
Erweiterte Aufgaben	77
Migrieren von Privacy Manager Zertifikaten und vertrauenswürdigen Kontakten en auf einen anderen Computer	77
Sichern von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten	77
Wiederherstellen von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten	77
Zentrale Verwaltung von Privacy Manager	78
7 File Sanitizer for HP ProtectTools	79
Shreddern	80
Überschreiben von freiem Speicherplatz	81
Öffnen von File Sanitizer	82
Setup-Verfahren	83
Festlegen eines Shred-Zeitplans	83
Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz	83
Auswählen und Ändern eines Shred-Profiles	84
Auswählen eines vordefinierten Shred-Profiles	84
Anpassen eines Shred-Profiles	84
Anpassen eines Profils für das einfache Löschen	86
Allgemeine Aufgaben	87

Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs	87
Verwenden des File Sanitizer-Symbols	88
Manuelles Shreddern von Datenbeständen	88
Manuelles Shreddern aller ausgewählter Elemente	89
Manuelles Aktivieren des Überschreibens von freiem Speicherplatz	89
Abbrechen eines Shred- oder Überschreibungsvorgangs	89
Anzeigen der Protokolldateien	89
8 Device Access Manager for HP ProtectTools (bestimmte Modelle)	91
Öffnen von Device Access Manager	91
Setup-Verfahren	92
Konfigurieren von Zugriffsrechten auf Geräte	92
Einfache Konfiguration	92
Starten des Hintergrunddienstes	93
Geräteklassen-Konfiguration	93
Zugriff für Benutzer oder Gruppe verweigern	95
Zugriff für Benutzer oder Gruppe erteilen	95
Einem Benutzer einer Gruppe Zugriff auf eine Geräteklasse erteilen	96
Einem Benutzer einer Gruppe Zugriff auf ein bestimmtes Gerät erteilen	97
Entfernen von Einstellungen für einen Benutzer oder eine Gruppe	97
Zurücksetzen der Konfiguration	97
JITA-Konfiguration	98
Erstellen einer JITA für einen Benutzer oder eine Gruppe	99
Erstellen einer verlängerbaren JITA für einen Benutzer oder eine Gruppe	99
Deaktivieren einer JITA für einen Benutzer oder eine Gruppe	99
Erweiterte Einstellungen	101
Gruppe „Geräte-Administratoren“	101
eSATA-Support	102
Nicht verwaltete Geräteklassen	102
9 Wiederbeschaffung gestohlener Geräte	105
10 Embedded Security for HP ProtectTools (bestimmte Modelle)	107
Setup-Verfahren	108
Aktivieren des integrierten Sicherheitschips in Computer Setup	108
Initialisieren des integrierten Sicherheitschips	109
Einrichten eines einfachen Benutzerkontos	110

Allgemeine Aufgaben	111
Verwenden des persönlichen, sicheren Laufwerks	111
Verschlüsseln von Dateien und Ordnern	111
Senden und Empfangen verschlüsselter E-Mails	111
Ändern des Kennworts des einfachen Benutzerschlüssels	112
Erweiterte Tasks	113
Sichern und Wiederherstellen	113
Erstellen einer Sicherungsdatei	113
Wiederherstellen von Daten aus der Sicherungsdatei	113
Ändern des Eigentümerkennworts	114
Erneutes Einrichten eines Benutzerkennworts	114
Migrieren von Schlüsseln mithilfe des Migrationsassistenten	115
11 Ausnahmen für lokalisierte Kennwörter	116
Windows IMEs werden weder auf der Ebene von Pre-Boot Security noch auf der Ebene von HP Drive Encryption unterstützt.	117
Ändern des Kennworts mit einem Tastaturlayout, das ebenfalls unterstützt wird	118
Behandeln von Sonderzeichen	119
Vorgehensweise, wenn das Kennwort abgelehnt wird	122
Glossar	123
Index	129

1 Einführung in die Sicherheitsfunktionen

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

Anwendung	Funktionen
HP Protect Tools Administrator-Konsole (für Administratoren)	<ul style="list-style-type: none">• Administratorrechte unter Microsoft Windows sind für den Zugriff erforderlich.• Bietet Zugriff auf Module, die von einem Administrator konfiguriert werden und für Benutzer nicht verfügbar sind.• Ermöglicht eine erste Sicherheitseinrichtung und die Konfiguration von Optionen oder Anforderungen für alle Benutzer.
HP ProtectTools Security Manager (für Benutzer)	<ul style="list-style-type: none">• Ermöglicht einem Benutzer, Optionen zu konfigurieren, die von einem Administrator bereitgestellt wurden.• Ermöglicht Administratoren, Benutzern die eingeschränkte Steuerung einiger HP ProtectTools Softwaremodule zu ermöglichen.

Welche Softwaremodule für Ihren Computer verfügbar sind, ist vom Modell abhängig.

Die HP ProtectTools Softwaremodule sind möglicherweise vorinstalliert oder bereits geladen, oder sie sind auf der HP Website zum Download verfügbar. Weitere Informationen 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

In der folgenden Tabelle finden Sie nähere Informationen zu den HP ProtectTools Modulen.

Modul	Funktionen
HP ProtectTools Administrator-Konsole (für Administratoren)	<ul style="list-style-type: none">• Sicherheitsebenen und Sicherheits-Anmeldemethoden mithilfe des Installations-Assistenten von Security Manager einrichten und konfigurieren.• Optionen, die für Benutzer nicht sichtbar sind, konfigurieren.• Device Access Manager Konfigurationen und Benutzerzugriffseinstellungen einrichten.• HP ProtectTools Benutzer hinzufügen und entfernen und Benutzerstatus mithilfe der Funktion Administrator-Tools anzeigen.
HP ProtectTools Security Manager (für Benutzer)	<ul style="list-style-type: none">• Kennwörter verwalten, einrichten und ändern.• Benutzerberechtigungen, wie Windows Kennwort, Fingerabdruck oder Smart Card, konfigurieren und ändern.• Optionen zum Shreddern und Überschreiben in File Sanitizer und andere Einstellungen konfigurieren und ändern.• Einstellungen für Device Access Manager anzeigen.• Computrace for HP ProtectTools konfigurieren.• Voreinstellungen und Sicherungs- sowie Wiederherstellungsoptionen konfigurieren.
Credential Manager for HP ProtectTools (Password Manager)	<ul style="list-style-type: none">• Benutzernamen und Kennwörter sichern, verwalten und schützen.• Anmeldebildschirme von Websites und Programmen für den schnellen und sicheren Zugriff einrichten.• Website-Benutzernamen und -Kennwörter speichern, indem sie in Password Manager eingegeben werden. Wenn Sie diese Website das nächste Mal besuchen, gibt Password Manager die Daten automatisch ein und übermittelt sie.• Stärkere Kennwörter für eine höhere Kontosicherheit erstellen. Password Manager füllt die Informationen automatisch aus und übermittelt sie.
Drive Encryption for HP ProtectTools (bestimmte Modelle)	<ul style="list-style-type: none">• Bietet eine komplette Verschlüsselung der gesamten Festplatte.• Erzwingt eine Authentifizierung vor dem Systemstart zum Entschlüsseln und Zugreifen auf Daten.
File Sanitizer for HP ProtectTools	<ul style="list-style-type: none">• Shreddert digitale Bestände (sensible Informationen wie Anwendungsdateien, historischen oder Web-bezogenen Inhalt und andere vertrauliche Daten) auf Ihrem Computer und überschreibt von Zeit zu Zeit Datenbestände auf der Festplatte.

Modul	Funktionen
Device Access Manager for HP ProtectTools (nur ausgewählte Modelle)	<ul style="list-style-type: none"> • Ermöglicht IT-Managern die Zugriffssteuerung von Geräten auf Basis von Benutzerprofilen. • Verhindert, dass Daten von nicht autorisierten Benutzern auf externe Speichermedien kopiert werden und Viren über externe Medien in das System gelangen. • Ermöglicht Administratoren, den Zugriff auf beschreibbare Geräte für bestimmte Personen oder Benutzergruppen zu sperren.
Privacy Manager for HP ProtectTools (bestimmte Modelle)	<ul style="list-style-type: none"> • Generiert Echtheitszertifikate, mit denen die Quelle, Integrität und Sicherheit der Verbindung überprüft wird, wenn Microsoft E-Mail und Microsoft Office-Dokumente verwendet werden.
Computrace for HP ProtectTools (separat erhältlich)	<ul style="list-style-type: none"> • Bietet sichere Bestandsverfolgung. • Überwacht Benutzeraktivität sowie Hardware- und Softwareänderungen. • Bleibt aktiv, auch wenn die Festplatte neu formatiert oder ersetzt wird. • Für die Aktivierung ist ein separates Tracking- and Tracing-Abonnement erforderlich.
Embedded Security for HP ProtectTools (nur ausgewählte Modelle)	<ul style="list-style-type: none"> • Verwendet einen integrierten TPM-Sicherheitsschip (Trusted Platform Module) zum Schutz gegen den nicht autorisierten Zugriff auf Benutzerdaten und Anmeldeinformationen, die auf einem Computer gespeichert sind. • Ermöglicht die Erstellung eines persönlichen sicheren Laufwerks (PSD, Personal Secure Drive), 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.

HP ProtectTools – Beschreibung und allgemeine Nutzungsbeispiele der Sicherheitsprodukte

Die meisten der HP ProtectTools Sicherheitsprodukte verfügen sowohl über die Benutzerauthentifizierung (normalerweise ein Kennwort) als auch über ein Administrator-Backup, um den Zugriff zu gewährleisten, wenn Kennwörter verloren gehen, nicht verfügbar sind oder vergessen wurden, oder wenn die Unternehmenssicherheit einen Zugriff erforderlich macht.



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

Credential Manager for HP ProtectTools

Credential Manager (Teil von Security Manager) speichert Benutzernamen und Kennwörter und lässt sich für Folgendes einsetzen:

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

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

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

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

Drive Encryption for HP ProtectTools

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

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

Sowohl Embedded Security for HP ProtectTools als auch Drive Encryption for HP ProtectTools sperren den Zugriff auf die verschlüsselten Daten, auch wenn das Laufwerk entfernt wird, weil beide an die Original-Hauptplatine gebunden sind.

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

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools wird verwendet, um Daten permanent zu löschen, einschließlich Internet-Browseraktivität, temporären Dateien, bereits gelöschten Dateien und anderen Informationen. File Sanitizer kann so konfiguriert werden, dass er entweder manuell oder automatisch nach einem benutzerdefinierten Zeitplan läuft.

Beispiel 1: Ein Anwalt hat oft mit sensiblen Klienteninformationen zu tun und möchte sicherstellen, dass gelöschte Dateien nicht wiederhergestellt werden können. Er verwendet File Sanitizer, um gelöschte Dateien zu „shreddern“, so dass es nahezu unmöglich ist, sie wiederherzustellen.

Wenn Daten unter Windows gelöscht werden, werden sie normalerweise nicht von der Festplatte entfernt. Stattdessen werden die entsprechenden Sektoren der Festplatte für die zukünftige Verwendung als verfügbar gekennzeichnet. Bis die Daten überschrieben werden, können sie mit Tools, die im Internet verfügbar sind, wiederhergestellt werden. File Sanitizer überschreibt die Sektoren mit Zufallsdaten (mehrmals, wenn nötig) und macht sie so unlesbar und nicht wiederherstellbar.

Beispiel 2: Eine Forscherin möchte gelöschte Daten, temporäre Dateien, Browseraktivität usw. automatisch löschen, sobald sie sich abmeldet. Sie verwendet File Sanitizer, um das Shreddern zeitlich zu planen, und kann so allgemeine Dateien oder bestimmte Dateien auswählen, die automatisch gelöscht werden sollen.

Device Access Manager for HP ProtectTools

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

Beispiel 1: Der Manager eines Unternehmens für medizinischen Bedarf arbeitet neben seinen Unternehmensdaten auch oft mit Krankenakten. Die Angestellten benötigen Zugriff auf diese Daten, es ist aber extrem wichtig, dass die Daten nicht mit einem USB-Laufwerk oder einem anderen externen Speichermedium vom Computer entfernt werden können. Das Netzwerk ist sicher, aber die

Computer haben CD-Brenner und USB-Anschlüsse, die es ermöglichen, die Daten zu stehlen oder zu kopieren. Der Manager verwendet Device Access Manager, um die USB-Anschlüsse und CD-Brenner zu deaktivieren, damit sie nicht benutzt werden können. Obwohl die USB-Anschlüsse gesperrt sind, bleiben Maus und Tastatur funktionsfähig.

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

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools wird verwendet, wenn die E-Mail-Kommunikation über Internet gesichert werden muss. Der Benutzer kann E-Mails erstellen und senden, die sich nur von einem authentifizierten Empfänger öffnen lassen. Privacy Manager verhindert, dass die Informationen durch einen Betrüger abgefangen oder gefährdet werden.

Beispiel 1: Ein Börsenmakler möchte sicherstellen, dass seine E-Mails nur an bestimmte Kunden gesendet werden und dass niemand das E-Mail-Konto manipulieren oder Informationen abfangen kann. Der Börsenmakler meldet sich und seine Kunden bei Privacy Manager an. Privacy Manager stellt jedem Benutzer ein Authentifizierungszertifikat (CA) aus. Mit diesem Tool müssen der Börsenmakler und seine Kunden sich authentifizieren, bevor E-Mails ausgetauscht werden können.

Mit Privacy Manager for HP ProtectTools können E-Mails auf einfache Weise gesendet und empfangen werden, wenn der Empfänger verifiziert und authentifiziert wurde. Der Mailservice lässt sich auch verschlüsseln. Die Verschlüsselung verläuft ähnlich wie bei Kreditkartenkäufen über das Internet.

Beispiel 2: Ein Vorstandschef möchte sicherstellen, dass nur die Mitglieder des Vorstands Informationen anzeigen können, die er per E-Mail versendet. Er verwendet die Option zur Verschlüsselung von E-Mails, die von den Vorstandsmitgliedern empfangen und an ihn gesendet werden. Ein Privacy Manager Authentifizierungszertifikat ermöglicht es allen Vorstandsmitgliedern, eine Kopie des Verschlüsselungsschlüssels zu besitzen, damit nur sie die vertraulichen E-Mails entschlüsseln können.

Computrace for HP ProtectTools (zuvor LoJack Pro)

Computrace for HP ProtectTools ist ein Service (separat erhältlich), der die Position eines gestohlenen Computers bestimmen kann, sobald der Benutzer auf das Internet zugreift.

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

Computrace for HP ProtectTools dient auch dazu, Computer per Fernzugriff zu verwalten und aufzufinden sowie die Nutzung von Computern und Anwendungen zu überwachen.

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

Embedded Security for HP ProtectTools (nur ausgewählte Modelle)

Embedded Security for HP ProtectTools bietet die Möglichkeit, ein persönliches sicheres Laufwerk anzulegen. Diese Funktion ermöglicht es dem Benutzer, eine virtuelle Laufwerkspartition auf dem PC einzurichten, die bis zum Zugriff komplett verborgen bleibt. Embedded Security kann überall verwendet werden, wo ein Teil der Daten geheim geschützt werden muss, ohne den Rest der Daten zu verschlüsseln.

Beispiel 1: Der Manager eines Lagerhauses hat einen Computer, auf welchen den ganzen Tag lang verschiedene Angestellte zugreifen. Der Manager möchte vertrauliche Daten des Lagerhauses auf dem Computer verschlüsseln und ausblenden. Er möchte, dass die Daten so sicher sind, dass sie auch bei einem Diebstahl der Festplatte nicht entschlüsselt und gelesen werden können. Er beschließt, Embedded Security zu aktivieren, und verschiebt die vertraulichen Daten auf das persönliche sichere Laufwerk. Der Manager kann ein Kennwort eingeben und auf die vertraulichen Daten wie auf jedes andere Laufwerk zugreifen. Wenn er sich abmeldet oder das persönliche sichere Laufwerk neu startet, können die Daten ohne Angabe des Kennworts nicht abgerufen werden. Die Angestellten bekommen die vertraulichen Daten nie zu Gesicht, wenn sie auf den Computer zugreifen.

Embedded Security schützt Verschlüsselungsschlüssel innerhalb eines TPM-Chips (Trusted Platform Module), der sich auf der Hauptplatine befindet. Es ist das einzige Verschlüsselungstool, das den Mindestanforderungen genügt, um Kennwortattacken zu widerstehen, wenn jemand versucht, das Verschlüsselungskennwort zu erraten. Embedded Security kann auch die gesamte Festplatte und E-Mails verschlüsseln.

Beispiel 2: Eine Börsenmaklerin möchte extrem sensible Daten mit einem portablen Laufwerk auf einen anderen Computer übertragen. Sie möchte sicherstellen, dass nur diese beiden Computer das Laufwerk öffnen können, selbst wenn das Kennwort bekannt wird. Sie verwendet die TPM-Migration von Embedded Security, um einem zweiten Computer zu ermöglichen, die Verschlüsselungsschlüssel zum Entschlüsseln der Daten zu besitzen. Während der Übertragung können auch mit Kennwort nur diese beiden physischen Computer die Daten entschlüsseln.

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

Schutz vor gezieltem Diebstahl

Ein Beispiel für gezielten Diebstahl ist der Diebstahl eines Computers mit vertraulichen Daten und Kundeninformationen an einer Sicherheitskontrolle eines Flughafens. Die folgenden Merkmale helfen Ihnen, Ihren Computer vor gezieltem Diebstahl zu schützen:

- Die Funktion zur Authentifizierung vor dem Systemstart verhindert den Zugriff auf das Betriebssystem. Siehe die folgenden Kapitel:
 - Security Manager for HP ProtectTools
 - Embedded Security for HP ProtectTools
 - Drive Encryption for HP ProtectTools
- Die Funktion des persönlichen sicheren Laufwerks, die vom Modul Embedded Security for HP ProtectTools bereitgestellt wird, verschlüsselt sensible Daten, um sicherzustellen, dass niemand ohne Authentifizierung darauf zugreifen kann. Nähere Informationen dazu erhalten Sie im Kapitel:
 - Embedded Security for HP ProtectTools
- Computrace kann die Position eines Computers nach einem Diebstahl feststellen. Nähere Informationen dazu erhalten Sie im Kapitel:
 - Computrace for HP ProtectTools

Einschränken des Zugriffs auf sensible Daten

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

- Device Access Manager for HP ProtectTools ermöglicht es IT-Managern, den Zugriff auf Schreibgeräte einzuschränken, so dass sensible Daten nicht gedruckt oder von der Festplatte auf ein Wechselmedium kopiert werden können.

Verhindern des unbefugten Zugriffs von internen oder externen Standorten

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

vertrauliche Informationen wie Patientendatensätze oder persönliche Finanzdaten. Die folgende Funktion verhindert den unautorisierten Zugriff:

- Die Funktion zur Authentifizierung vor dem Systemstart verhindert den Zugriff auf das Betriebssystem. Siehe die folgenden Kapitel:
 - Password Manager for HP ProtectTools
 - Embedded Security for HP ProtectTools
 - Drive Encryption for HP ProtectTools
- Mit Password Manager können Sie sicherstellen, dass unberechtigte Benutzer keine Kennwörter bzw. keinen Zugriff auf kennwortgeschützte Anwendungen erhalten.
- Device Access Manager for HP ProtectTools ermöglicht es IT-Managern, den Zugriff auf Schreibgeräte einzuschränken, so dass sensible Daten nicht von der Festplatte kopiert werden können.
- File Sanitizer ermöglicht das sichere Löschen von Daten durch Shreddern kritischer Dateien und Ordner bzw. Überschreiben von gelöschten Beständen auf der Festplatte (Daten, die gelöscht wurden, aber wiederherstellbar sind, werden überschrieben).
- Privacy Manager ist ein Tool zur Erstellung von Echtheitszertifikaten, wenn Sie Microsoft E-Mail oder Microsoft Office-Dokumente verwendet werden, damit wichtige Informationen sicher gesendet und gespeichert werden.

Erstellen von Richtlinien für starke Kennwörter

Wenn eine Unternehmensrichtlinie in Kraft tritt, die das Benutzen starker Kennwörter für Web-basierte Anwendungen und Datenbanken erforderlich macht, bietet Security Manager ein geschütztes Repository für Kennwörter und Single Sign-On.

Weitere Sicherheitselemente

Zuweisen von Sicherheitsrollen

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

 **HINWEIS:** In kleineren Unternehmen oder im heimischen Büro können diese Rollen selbstverständlich auch alle von einer Person wahrgenommen werden.

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

- Der Sicherheitsbeauftragte definiert die Sicherheitsstufe für das Unternehmen oder Netzwerk und bestimmt die Sicherheitsfunktionen, die bereitgestellt werden sollen, wie Drive Encryption oder Embedded Security.

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

- Der IT-Administrator wendet die vom Sicherheitsbeauftragten definierten Sicherheitsfunktionen an und verwaltet sie. Er kann auch einige Funktionen aktivieren oder deaktivieren. Wenn der Sicherheitsbeauftragte zum Beispiel entschieden hat, Smart Cards bereitzustellen, kann der IT-Administrator das Kennwort und den Smart Card-Modus aktivieren.
- Der Benutzer nutzt die Sicherheitsfunktionen. Wenn der Sicherheitsbeauftragte und der IT-Administrator zum Beispiel Smart Cards für das System aktiviert haben, kann der Benutzer die PIN für die Smart Card festlegen und die Karte zur Authentifizierung benutzen.

 **ACHTUNG:** Administratoren wird geraten, gemäß den „Best Practices“ die Rechte für Endbenutzer und den Benutzerzugriff einzuschränken.

Unberechtigte Benutzer sollten nicht über Administratorrechte verfügen.

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	Wird in diesem Modul eingerichtet	Funktion
Windows Anmeldekennwort	Windows® Systemsteuerung oder HP ProtectTools Security Manager	Zur manuellen Anmeldung oder zur Authentifizierung, um auf verschiedene Security Manager Funktionen zuzugreifen.
Sicherungs- und Wiederherstellungskennwort für Security Manager	Security Manager, vom Benutzer selbst	Schützt den Zugriff auf die Security Manager Sicherungs- und Wiederherstellungsdatei.

HP ProtectTools Kennwort	Wird in diesem Modul eingerichtet	Funktion
Smart Card-PIN	Credential Manager	<p>Kann zur Mehrfach-Authentifizierung verwendet werden.</p> <p>Kann zur Windows Authentifizierung verwendet werden.</p> <p>Authentifiziert Benutzer von Drive Encryption, wenn das Smart Card-Token ausgewählt wird.</p>
Kennwort für Notfallwiederherstellungs-Token	Embedded Security, durch IT-Administrator	Schützt den Zugriff auf das Notfallwiederherstellungs-Token, eine Sicherungsdatei für den integrierten Sicherheitschip.
Kennwort des Eigentümers	Embedded Security, durch IT-Administrator	Schützt das System und den TPM-Chip vor nicht autorisiertem Zugriff auf alle Eigentümerfunktionen von Embedded Security.
BIOS-Administrator-Kennwort	Computer Setup, durch IT-Administrator	Schützt den Zugriff auf Computer Setup Utility.

Erstellen 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.
- Mischen Sie im gesamten Kennwort Klein- und Großbuchstaben.
- Verwenden Sie nach Möglichkeit sowohl 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.
- Benutzen Sie für das Kennwort weder Ihren Namen noch andere persönliche Informationen wie Ihr Geburtsdatum, Namen von Haustieren, Mädchenname der Mutter usw., auch nicht rückwärts geschrieben.
- Ändern Sie das Kennwort regelmäßig. Es genügt, wenn Sie nur einige Zeichen ändern.
- Wenn Sie Ihr Kennwort aufschreiben, bewahren Sie es auf keinen Fall sichtbar in der Nähe des Computers auf.
- Speichern Sie das Kennwort nicht in einer Datei, wie z. B. einer E-Mail, auf dem Computer.
- Nutzen Sie das Konto nicht gemeinsam mit anderen Benutzern, und geben Sie Ihr Kennwort nicht weiter.

Sichern und Wiederherstellen von HP ProtectTools Anmeldedaten

Sie können das Merkmal Sichern und Wiederherstellen von HP ProtectTools verwenden, um HP ProtectTools Anmeldeinformationen und zugehörige Einstellungen auszuwählen und diese zu sichern.

2 Einführung in den Installations-Assistenten

Der Installations-Assistent für Security Manager führt Sie durch den Vorgang zum Aktivieren der Sicherheitsfunktionen, die für alle Benutzer des Computers gelten. Sie können diese Funktionen auch auf der Seite mit den Sicherheitsfunktionen in der Administrator-Konsole verwalten.

So richten Sie im Installations-Assistenten für Security Manager die Sicherheitsfunktionen ein:

1. Öffnen Sie den HP ProtectTools Security Manager über das Symbol der HP ProtectTools Desktop-Minianwendung in der Windows Randleiste oder über das Symbol in der Taskleiste im Infobereich, ganz rechts auf der Taskleiste.



Die Farbe des Banners der Desktop-Minianwendung HP ProtectTools zeigt eine der folgenden Bedingungen an:

- Rot – HP ProtectTools wurde nicht eingerichtet, oder eine Fehlerbedingung mit einem der ProtectTools Module liegt vor.
- Gelb – Auf der Seite für den Status der Anwendungen in Security Manager wird angezeigt, welche Einstellungen geändert werden müssen.
- Blau – HP ProtectTools wurde eingerichtet und funktioniert ordnungsgemäß.

Wenn eine der folgenden Bedingungen erfüllt ist, wird am unteren Rand des Symbols der Minianwendung eine entsprechende Meldung angezeigt:

- **Jetzt einrichten** – Der Administrator muss auf das Symbol der Minianwendung klicken, um den Security Manager Installations-Assistenten zu starten und Authentifizierungsinformationen für den Computer zu konfigurieren.

Der Installations-Assistent ist eine eigenständige Anwendung.

- **Jetzt registrieren** – Benutzer müssen auf das Symbol der Minianwendung klicken, um den Security Manager-Einführungsassistenten zu starten und Authentifizierungsinformationen zu registrieren.

Der Einführungsassistent wird auf dem Security Manager Dashboard angezeigt.

- **Jetzt suchen** – Klicken Sie auf das Symbol der Minianwendung, um weitere Details auf der Seite „Status der Sicherheitsanwendungen“ anzeigen zu lassen.



HINWEIS: Die Desktop-Minianwendung HP ProtectTools ist in Windows XP nicht verfügbar.

– ODER –

Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**. Klicken Sie im linken Fensterausschnitt auf **Installations-Assistent**.

2. Lesen Sie den Startbildschirm, und klicken Sie dann auf **Weiter**.
3. Bestätigen Sie Ihre Identität, indem Sie Ihr Windows Kennwort eingeben und anschließend auf **Weiter** klicken.

Wenn Sie noch kein Windows Kennwort eingerichtet haben, werden Sie aufgefordert, eines einzurichten. Ein Windows Kennwort ist erforderlich, um Ihr Windows Konto vor Zugriffen von unbefugten Personen zu schützen und um die HP ProtectTools Security Manager Funktionen zu verwenden.

4. Wählen Sie auf der SpareKey-Seite drei Sicherheitsfragen aus, geben Sie zu jeder Frage eine Antwort ein, und klicken Sie auf **Weiter**.

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



HINWEIS: Diese SpareKey-Einrichtung ist nur für Administratoren verfügbar.

5. Aktivieren Sie die Sicherheitsfunktionen durch Auswahl der entsprechenden Kontrollkästchen, und klicken Sie dann auf **Weiter**.

Je mehr Funktionen Sie auswählen, desto sicherer ist Ihr Computer.



HINWEIS: Die hier vorgenommenen Einstellungen gelten für alle Benutzer. Wenn Kontrollkästchen nicht aktiviert sind, wird der Benutzer vom Installations-Assistenten nicht aufgefordert, diese Anmeldedaten zu registrieren.

- **Windows Anmeldesicherheit** – Schützt Ihre Windows Konten, indem es dafür sorgt, dass der Zugriff nur mit bestimmten Anmeldedaten möglich ist.
- **Drive Encryption** schützt Ihre Daten durch die Verschlüsselung Ihrer Festplatten, so dass Informationen für Personen ohne die entsprechende Berechtigung nicht lesbar sind.
- **Pre-Boot Security** schützt Ihren Computer, indem es den Zugriff unbefugter Personen verhindert, bevor Windows gestartet wird.



HINWEIS: Pre-Boot Security steht nur dann zur Verfügung, wenn diese Funktion vom BIOS unterstützt wird.

6. Sie werden vom Installations-Assistenten aufgefordert, sich zu registrieren oder sich anderweitig zu authentifizieren.

Wenn weder ein Fingerabdruck-Lesegerät noch eine Smart Card noch eine Webcam zur Verfügung steht, werden Sie aufgefordert, Ihr Windows Kennwort einzugeben. Nach der Registrierung können Sie beliebige registrierte Benutzerdaten verwenden, um bei Bedarf Ihre Identität zu verifizieren.



HINWEIS: Die Registrierung dieser Anmeldedaten ist nur für Administratoren verfügbar.

7. Klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Die Startseite des Security Manager Dashboard wird angezeigt.

3 HP ProtectTools Security Manager Administrator-Konsole

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

Im Security Manager Dashboard sind zusätzliche Anwendungen verfügbar (bestimmte Modelle), die Ihnen bei der Wiedererlangung des Computers helfen, falls dieser verloren geht oder gestohlen wird.

Mittels dieser Konsole kann der lokale Administrator die folgenden Aufgaben ausführen:

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

Öffnen von HP ProtectTools Administrator-Konsole

Für Administrationsaufgaben wie z. B. das Einrichten von Systemrichtlinien oder die Konfiguration von Software öffnen Sie die Konsole folgendermaßen:

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

– oder –

Klicken Sie auf der linken Seite von Security Manager auf **Verwaltung** und anschließend auf **Administrator-Konsole**.

Verwenden der Administrator-Konsole

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

- ▲ Zum Öffnen von HP ProtectTools Administrator-Konsole klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.

– oder –

Klicken Sie auf der linken Seite von Security Manager auf **Verwaltung** und anschließend auf **Administrator-Konsole**.

Die Konsole setzt sich aus den folgenden Komponenten zusammen:

- **Startseite** – Hier können Sie die folgenden Sicherheitsoptionen konfigurieren:
 - **Systemsicherheit erhöhen**
 - **Starke Authentifizierung erforderlich**
 - **HP ProtectTools Benutzer verwalten**
 - **Informationen zur zentralen Verwaltung von HP ProtectTools**
- **System** – Ermöglicht die Konfiguration der folgenden Sicherheitsfunktionen und die Authentifizierung für Benutzer und Geräte:
 - **Sicherheit**
 - **Benutzer**
 - **Anmeldeinformationen**
- **Anwendungen** – Ermöglicht die Konfiguration der Einstellungen für HP ProtectTools Security Manager und für Security Manager-Anwendungen.
- **Daten** – Enthält ein erweitertes Menü mit Links zu den Security Manager-Anwendungen, die Ihre Daten schützen.
- **Zentrale Verwaltung** – Zeigt Registerkarten für den Zugriff auf zusätzliche Lösungen, Produktaktualisierungen und Meldungen an.
- **Installations-Assistent** – Führt Sie durch die Installation von HP ProtectTools Security Manager.
- **Info** – Zeigt Informationen zu HP ProtectTools Security Manager, wie etwa Versionsnummer und Copyright-Hinweis, an.
- **Hauptbereich** – Zeigt anwendungsspezifische Bildschirme an.
 - ? – Zeigt Softwarehilfe zur Administrator-Konsole an. Das Hilfe-Symbol befindet sich rechts oben im Fensterrahmen, neben den Symbolen für die Minimierung und Maximierung der Fensteranzeige.

Konfigurieren des Systems

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

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

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

Einrichten der Authentifizierung für Ihren Computer

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

So richten Sie eine Authentifizierung auf Ihrem Computer ein:

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

Anmelderichtlinie

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

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Authentifizierung**.
2. Klicken Sie auf der Registerkarte **Anmelderichtlinie** auf den Pfeil nach unten, und wählen Sie eine Benutzerkategorie:
 - **Für Administratoren dieses Computers**
 - **Für Benutzer ohne Administratorrechte**
3. Geben Sie die für die ausgewählte Benutzerkategorie benötigten Anmeldeinformationen zur Authentifizierung an.
4. Wählen Sie aus, ob EINE BELIEBIGE (nur eine) der angegebenen Anmeldeinformationen erforderlich ist oder ob ALLE angegebenen Anmeldeinformationen für die Authentifizierung eines Benutzers erforderlich sind.
5. Klicken Sie auf **Übernehmen**.

Sitzungsrichtlinie

So bestimmen Sie Richtlinien, die regulieren, welche Anmeldedaten für den Zugriff auf HP ProtectTools Anwendungen in einer Windows Sitzung erforderlich sind:

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Authentifizierung**.
2. Klicken Sie auf der Registerkarte **Sitzungsrichtlinie** auf den Pfeil nach unten, und wählen Sie eine Benutzerkategorie:
 - **Für Administratoren dieses Computers**
 - **Für Benutzer ohne Administratorrechte**
3. Klicken Sie auf den Pfeil nach unten, und wählen Sie die erforderlichen Authentifizierungsinformationen für die gewählte Benutzerkategorie aus:
 - **Eine der angegebenen Anmeldeinformationen ist erforderlich**

 **HINWEIS:** Das Deaktivieren der Kontrollkästchen für alle Anmeldeinformationen hat dieselbe Wirkung wie das Auswählen der Option **Authentifizierung ist nicht erforderlich**.

 - **Alle der angegebenen Anmeldeinformationen sind erforderlich**
 - **Authentifizierung ist nicht erforderlich** – Bei Auswahl dieser Option werden alle Anmeldeinformationen aus dem Fenster gelöscht.
4. Klicken Sie auf **Übernehmen**.

Einstellungen

1. Zum Aktivieren/Deaktivieren der folgenden Einstellung verwenden Sie das entsprechende Kontrollkästchen.

One-Step Logon zulassen – Ermöglicht es den Benutzern dieses Computers, die Windows Anmeldung zu überspringen, wenn die Authentifizierung im BIOS oder über eine verschlüsselte Festplatte erfolgt ist.
2. Klicken Sie auf **Übernehmen**.

Verwalten von Benutzern

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

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

Zum Verwalten von Benutzern wählen Sie die folgenden Einstellungen aus:

- Um weitere Benutzer hinzuzufügen, klicken Sie auf **Hinzufügen**.
- Um einen Benutzer zu löschen, klicken Sie auf den Benutzer und danach auf **Löschen**.

- Um zusätzliche Anmeldeinformationen für den Benutzer einzurichten, klicken Sie auf **Registrieren**.
- Um die Richtlinien für einen bestimmten Benutzer anzuzeigen, wählen Sie den Benutzer aus. Die Richtlinien werden dann im unteren Fenster angezeigt.

Anmeldeinformationen

In der Anwendung „Anmeldeinformationen“ können Sie Einstellungen für integrierte oder angeschlossene Sicherheitsgeräte, die von HP ProtectTools Security Manager erkannt werden, festlegen.

SpareKey

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

1. Aktivieren oder deaktivieren Sie das Kontrollkästchen, um die SpareKey-Authentifizierung für die Windows Anmeldung zu aktivieren oder zu deaktivieren.
2. Wählen Sie die Sicherheitsfragen aus, die den Benutzern bei der SpareKey-Anmeldung gestellt werden. Sie können bis zu drei benutzerdefinierte Fragen angeben, oder Sie können Benutzern ermöglichen, ihre eigene Passphrase einzugeben.
3. Klicken Sie auf **Übernehmen**.

Fingerabdrücke

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

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

Sie können ebenfalls alle Daten vom Fingerabdruck-Lesegerät löschen.

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

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

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

- **Erweitert** – Wählen Sie eine der folgenden Optionen, um das Fingerabdruck-Lesegerät so zu konfigurieren, dass Strom gespart und Bildschirmmeldungen verbessert werden:
 - **Optimiert** – Das Fingerabdruck-Lesegerät wird aktiviert, wenn es benötigt wird. Bei der ersten Verwendung des Geräts kann es zu einer leichten Verzögerung kommen.
 - **Geringer Stromverbrauch** – Das Fingerabdruck-Lesegerät reagiert langsamer, bei dieser Einstellung wird jedoch deutlich weniger Strom benötigt.
 - **Normaler Stromverbrauch** – Das Fingerabdruck-Lesegerät ist jederzeit einsatzbereit, bei dieser Einstellung wird jedoch am meisten Strom benötigt.

Smart Card

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

- **Einstellungen** – Sie können den Computer so einstellen, dass er beim Entfernen einer Smart Card automatisch gesperrt wird.



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

- **Verwaltung** – Wählen Sie eine der folgenden Optionen:
 - **Initialize the smart card** (Smart Card initialisieren) – Bereitet eine Smart Card für die Verwendung mit HP Protect Tools vor. Wenn eine Smart Card zuvor bereits außerhalb von HP ProtectTools initialisiert wurde (und ein asymmetrisches Schlüsselpaar sowie das zugehörige Zertifikat enthält), muss sie nicht erneut initialisiert werden, es sei denn, es wird eine Initialisierung mit einem bestimmten Zertifikat gewünscht.
 - **Change smart card PIN** (Smart Card-PIN ändern) – Hiermit können Sie die mit der Smart Card verwendete PIN ändern.
 - **Erase HP ProtectTools data only** (Nur HP ProtectTools Daten löschen) – Löscht nur das während der Karteninitialisierung erstellte HP ProtectTools Zertifikat. Es werden keine anderen Daten von der Karte gelöscht.
 - **Erase all data on the smart card** (Alle Daten von der Smart Card löschen) – Löscht alle Daten von der angegebenen Smart Card. Die Karte kann dann nicht mehr mit HP ProtectTools oder anderen Anwendungen verwendet werden.



HINWEIS: Funktionen, die von Ihrer Smart Card nicht unterstützt werden, sind nicht verfügbar.

- ▲ Klicken Sie auf **Übernehmen**.

Gesicht

Wenn der Computer über eine integrierte oder angeschlossene Webcam verfügt, und wenn das Gesichtserkennungsprogramm installiert ist, können Sie die Sicherheitsstufe für die Gesichtserkennung so einstellen, dass ein Gleichgewicht zwischen Nutzungskomfort und Computersicherheit hergestellt wird.

1. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie auf **Anmeldeinformationen** und dann auf **Gesicht**.

3. Für mehr Komfort bewegen Sie den Schieberegler nach links, für mehr Genauigkeit bewegen Sie den Schieberegler nach rechts.
 - **Komfort** – Um registrierten Benutzern den Zugriff in Grenzsituationen zu erleichtern, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Komfort**.
 - **Balance** – Um ein gutes Gleichgewicht zwischen Sicherheit und Komfort herzustellen, oder wenn auf dem Computer kritische Informationen gespeichert sind bzw. sich der Computer in einer Umgebung befindet, in der unberechtigte Anmeldeversuche möglich sind, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Balance**.
 - **Genauigkeit** – Um den Zugriff für Benutzer zu erschweren, wenn die registrierten Szenen oder aktuellen Lichtbedingungen unter dem Normalwert liegen und fälschlicherweise zugelassene Zugriffe möglich sind, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Genauigkeit**.
4. Klicken Sie auf **Erweitert**, und konfigurieren Sie zusätzliche Sicherheitsoptionen. Weitere Informationen finden Sie unter [„Erweiterte Benutzereinstellungen“ auf Seite 46](#).
5. Klicken Sie auf **Übernehmen**.

Konfigurieren der Anwendungen

Sie können die Einstellungen nutzen, um das Verhalten der installierten HP ProtectTools Security Manager Anwendungen anzupassen.

So bearbeiten Sie die Anwendungseinstellungen:

1. Klicken Sie auf der linken Seite der Administrator-Konsole unter **Anwendungen** auf **Einstellungen**.
2. Zum Aktivieren/Deaktivieren einer bestimmten Einstellung verwenden Sie das entsprechende Kontrollkästchen.
3. Klicken Sie auf **Übernehmen**.

Registerkarte „Allgemein“

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

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

Registerkarte „Anwendungen“

Die hier dargestellten Einstellungen können sich ändern, wenn neue Anwendungen zu Security Manager hinzugefügt werden. Standardmäßig werden jedoch mindestens die folgenden Einstellungen angezeigt:

- **Status der Anwendungen** – Aktiviert die Anzeige des Status für alle Anwendungen.
- **Password Manager** – Aktiviert den Password Manager für alle Benutzer des Computers.
- **Privacy Manager** – Aktiviert den Privacy Manager für alle Benutzer des Computers.
- **Verknüpfung für zentrale Verwaltung aktivieren** – Ermöglicht es allen Benutzern dieses Computers, Anwendungen zu HP ProtectTools Security Manager hinzuzufügen, indem sie auf die Schaltfläche **Zentrale Verwaltung** klicken.

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

Zentrale Verwaltung

Möglicherweise sind zusätzliche Anwendungen verfügbar, um neue Management-Tools in Security Manager aufzunehmen. Der Administrator dieses Computers kann diese Funktion auf der Seite „Einstellungen“ deaktivieren. Auf der Seite „Zentrale Verwaltung“ befinden sich zwei Registerkarten:

- **Unternehmenslösungen** – Falls eine Internetverbindung verfügbar ist, können Sie auf der DigitalPersona Website (<http://www.digitalpersona.com/>) nach neuen Anwendungen suchen.
- **Updates und Nachrichten**
 - Um Informationen zu neuen Anwendungen und Updates anzufordern, aktivieren Sie das Kontrollkästchen **Über neue Anwendungen und Updates informieren**.
 - Zum Einrichten eines Zeitplans für automatische Updates wählen Sie die Anzahl der Tage.
 - Zum Suchen nach Updates klicken Sie auf **Jetzt suchen**.

4 HP ProtectTools Security Manager

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

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

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

Öffnen von Security Manager

Security Manager lässt sich auf folgende Arten starten:

- Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Security Manager**.
- Doppelklicken Sie auf das Symbol **HP ProtectTools** im Infobereich außen rechts in der Taskleiste.
- Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** und anschließend auf **HP ProtectTools Security Manager öffnen**.
- Klicken Sie auf die Desktop-Minianwendung **HP ProtectTools**.
- Drücken Sie die Tastenkombination **strg+Windows Logo-Taste+h**, um das Menü **Security Manager Quick Links** (Security Manager Verknüpfungen) zu öffnen.

Weitere Informationen zum Ändern der Tastenkombination finden Sie unter [„Einstellungen“ auf Seite 40](#).

Verwenden des Security Manager Dashboards

Das Security Manager Dashboard ist die zentrale Zugriffsstelle auf die Funktionen, Anwendungen und Einstellungen von Security Manager.

- ▲ Zum Öffnen des Security Manager Dashboards klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Security Manager**.

Das Dashboard enthält die folgenden Komponenten:

- **ID-Card** – Zeigt den Windows Benutzernamen und ein ausgewähltes Bild zur Ermittlung des angemeldeten Benutzerkontos an.
- **Sicherheitsanwendungen** – Zeigt ein erweitertes Menü mit Links an, über die folgende Sicherheitskategorien konfiguriert werden können:
 - **Startseite** – Ermöglicht die Verwaltung von Kennwörtern, die Einrichtung von Authentifizierungsinformationen und die Überprüfung des Status der Sicherheitsanwendungen.
 - **Status** – Ermöglicht die Überprüfung des Status der HP ProtectTools Sicherheitsanwendungen.



HINWEIS: Nicht auf dem Computer installierte Anwendungen werden in der folgenden Liste nicht aufgeführt.

- **My Logons** (Meine Anmeldedaten) – Ermöglicht die Verwaltung der verschiedenen Authentifizierungsinformationen (Password Manager, Credential Manager, Kennwort, SpareKey, Smart Card, Gesichtserkennung, Fingerabdruck).
- **Meine Daten** – Ermöglicht die Verwaltung der Datensicherheit mit Drive Encryption und File Sanitizer.
- **Arbeitsplatz** – Ermöglicht die Verwaltung der Sicherheit Ihres Computers mit Device Access Manager.
- **Meine Kommunikation** – Ermöglicht die Verwaltung der Kommunikationssicherheit mit Privacy Manager.
- **Verwaltung** – Ermöglicht Administratoren den Zugriff auf folgende Optionen:
 - **Administrator-Konsole** – Ermöglicht Administratoren die Verwaltung von Sicherheit und Benutzern.
 - **Zentrale Verwaltung** – Ermöglicht Administratoren des Zugriff auf zusätzliche Lösungen, Produktaktualisierungen und Meldungen.
- **Erweitert** – Enthält Befehle für den Zugriff auf zusätzliche Funktionen, wie beispielsweise:
 - **Voreinstellungen** – Ermöglicht die Personalisierung der Security Manager Einstellungen.
 - **Sichern und Wiederherstellen** – Ermöglicht die Sicherung und Wiederherstellung von Daten.
 - **Info** – Zeigt Informationen zu HP ProtectTools Security Manager, wie etwa Versionsnummer und Copyright-Hinweis, an.

- **Hauptbereich** – Zeigt anwendungsspezifische Bildschirme an.
- **?** – Öffnet die Softwarehilfe zu Security Manager. Das Hilfe-Symbol befindet sich rechts oben im Fenster, neben den Symbolen für die Minimierung und Maximierung der Fensteranzeige.

Status der Sicherheitsanwendungen

Der Status Ihrer installierten Sicherheitsanwendungen wird an zwei Stellen angezeigt:

- In der **HP ProtectTools Desktop-Minianwendung**

Die Farbe des Banners ganz oben im Symbol der HP ProtectTools Minianwendung ändert sich je nach Gesamtstatus der installierten Sicherheitsanwendungen.

- **Rot** – Vorsicht
- **Gelb** – Achtung: nicht konfiguriert
- **Blau** – OK

Wenn eine der folgenden Bedingungen erfüllt ist, wird am unteren Rand des Symbols der Minianwendung eine entsprechende Meldung angezeigt:

- **Jetzt einrichten** – Der Administrator muss auf das Symbol der Minianwendung klicken, um den Security Manager Installations-Assistenten zu starten und Authentifizierungsinformationen für den Computer zu konfigurieren.

Der Installations-Assistent ist eine eigenständige Anwendung.

- **Jetzt registrieren** – Benutzer müssen auf das Symbol der Minianwendung klicken, um den Security Manager-Einführungsassistenten zu starten und Authentifizierungsinformationen zu registrieren.

Der Einführungsassistent wird auf dem Security Manager Dashboard angezeigt.

- **Jetzt suchen** – Klicken Sie auf das Symbol der Minianwendung, um weitere Details auf der Seite „Status der Sicherheitsanwendungen“ anzuzeigen.
- Seite **Status der Sicherheitsanwendungen** – Klicken Sie im Security Manager Dashboard auf **Status**, um den Gesamtstatus Ihrer installierten Sicherheitsanwendungen sowie den Status der einzelnen Anwendungen anzuzeigen.

My Logons (Meine Anmeldedaten)

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

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

Administratoren können weitere Anwendungen hinzufügen, indem Sie auf **Verwaltung** und anschließend auf **Zentrale Verwaltung** links unten im Dashboard klicken.

Password Manager

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

Password Manager bietet folgende Optionen:

- Hinzufügen, Bearbeiten oder Löschen von Anmeldedaten über die Registerkarte **Verwalten**.
- Verwenden von Verknüpfungen zum Starten Ihres Standardbrowsers und Anmelden bei beliebigen Websites oder Programmen (nach entsprechender Einrichtung).
- Verschieben von Verknüpfungen per Drag and Drop, um diese nach Belieben in Kategorien einzuordnen.
- Auf einen Blick erkennen, ob eines Ihrer Kennwörter ein Sicherheitsrisiko birgt, und automatisch komplexe Kennwörter mit hoher Sicherheit für neue Websites generieren.

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

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

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

Folgende Optionen werden im Kontextmenü angezeigt:

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

Für Webseiten oder Programme, für die bereits Anmeldedaten festgelegt wurden

Folgende Optionen werden im Kontextmenü angezeigt:

- **Anmeldedaten eingeben** – Fügt Ihre Anmeldedaten in die Anmeldefelder ein und sendet sie an die Seite (wenn das Senden beim Erstellen oder bei der letzten Änderung der Anmeldedaten festgelegt wurde).
- **Anmeldedaten bearbeiten** – Hier können Sie Ihre Anmeldedaten für diese Website bearbeiten.
- **Anmeldedaten hinzufügen** – Hier können Sie ein Konto zu Anmeldedaten hinzufügen.
- **Password Manager öffnen** – Startet Password Manager.
- **Hilfe** – Öffnet die Softwarehilfe zu Security Manager.



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

Hinzufügen von Anmeldedaten

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

So fügen Sie Anmeldedaten hinzu:

1. Öffnen Sie den Anmeldebildschirm für eine Website oder ein Programm.
2. Klicken Sie auf den Pfeil am **Password Manager**-Symbol, und klicken Sie dann auf eine der folgenden Optionen, je nachdem, ob es sich um den Anmeldebildschirm einer Website oder eines Programms handelt.
 - Klicken Sie im Falle einer Website auf **[Domänenname] zu Password Manager hinzufügen**.
 - Klicken Sie im Falle eines Programms auf **Diesen Anmeldebildschirm zu Password Manager hinzufügen**.
3. Geben Sie Ihre Anmeldedaten ein. Anmeldefelder auf dem Bildschirm und ihre entsprechenden Felder im Dialogfeld sind mit einer fett formatierten orangefarbenen Umrandung gekennzeichnet. Sie können dieses Dialogfeld auch anzeigen, indem Sie auf der Registerkarte **Verwalten** von Password Manager auf **Anmeldedaten hinzufügen** klicken. Bei einigen Optionen kommt es darauf an, welche Sicherheitsgeräte an den Computer angeschlossen sind; dies gilt z. B. für die Tastenkombination **strg+Windows Logo-Taste+h**, das Streichen mit dem Finger über den Sensor oder das Einsetzen einer Smart Card.
 - a. Um ein Anmeldefeld mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken Sie auf die Pfeile rechts vom Feld.
 - b. Um das Kennwort für diese Anmeldedaten anzuzeigen, klicken Sie auf **Kennwort einblenden**.
 - c. Um die Anmeldefelder automatisch auszufüllen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldedaten automatisch senden**.

- d. Zur Aktivierung der VeriSign VIP-Sicherheit aktivieren Sie das Kontrollkästchen **I want VIP security on this site** (Ich möchte VIP-Sicherheit auf dieser Website).

Diese Option wird nur auf Websites angezeigt, die die VeriSign Identity Protection (VIP)-Funktion unterstützen. Wenn die VIP-Sicherheit von der betreffenden Website unterstützt wird, können Sie zudem festlegen, dass zusätzlich zur üblichen Authentifizierungsmethode auch Ihr VIP-Sicherheitscode eingegeben wird.

- e. Klicken Sie auf **OK** und anschließend auf die gewünschte Authentifizierungsmethode (Fingerabdruck, Kennwort, Gesichtserkennung). Melden Sie sich dann mit dieser Methode an.

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

- f. Falls Password Manager die Anmeldedaten nicht erkennt, klicken Sie auf **Weitere Felder**.
- Aktivieren Sie das Kontrollkästchen für jedes Feld, das für die Anmeldung erforderlich ist, oder deaktivieren Sie das Kontrollkästchen für alle Felder, die nicht für die Anmeldung erforderlich sind.
 - Wenn Password Manager nicht alle Anmeldefelder erkennen kann, werden Sie gefragt, ob Sie fortfahren möchten. Klicken Sie auf **Ja**.
 - Ein Dialogfeld mit Ihren Anmeldedaten wird angezeigt. Klicken Sie auf das Symbol für jedes Feld, und ziehen Sie es zum entsprechenden Anmeldefeld. Klicken Sie anschließend auf die Schaltfläche, um sich bei der Website anzumelden.



HINWEIS: Wenn Sie sich einmal für die Verwendung des manuellen Modus entschieden haben, um Anmeldedaten für eine Website einzugeben, müssen Sie diese Methode auch für künftige Anmeldungen bei dieser Website verwenden.

HINWEIS: Der manuelle Modus zur Eingabe von Anmeldedaten ist nur in Verbindung mit Internet Explorer 8 verfügbar.

- Klicken Sie auf **Schließen**.

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

Bearbeiten von Anmeldedaten

Gehen Sie folgendermaßen vor, um Anmeldedaten zu bearbeiten:

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

Sie können dieses Dialogfeld auch anzeigen, indem Sie auf der Registerkarte **Verwalten** im **Password Manager** auf **Für gewünschte Anmeldedaten bearbeiten** klicken.

3. Bearbeiten Sie Ihre Anmeldedaten.

- Um ein Anmeldefeld **Benutzername** mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken Sie auf den Abwärtspfeil rechts von dem Feld.
- Um ein Anmeldefeld **Kennwort** mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken Sie auf den Abwärtspfeil rechts von dem Feld.
- Zur Aktivierung der VeriSign VIP-Sicherheit aktivieren Sie das Kontrollkästchen **I want VIP security on this site** (Ich möchte VIP-Sicherheit auf dieser Website).

Diese Option wird nur auf Websites angezeigt, die die VeriSign VIP-Funktion unterstützen. Wenn die VIP-Sicherheit von der betreffenden Website unterstützt wird, können Sie zudem festlegen, dass zusätzlich zur üblichen Authentifizierungsmethode auch Ihr VIP-Sicherheitscode eingegeben wird.

- Um weitere Felder vom Bildschirm zu Ihren Anmeldedaten hinzuzufügen, klicken Sie auf **Weitere Felder**.
- Um das Kennwort für diese Anmeldedaten anzuzeigen, klicken Sie auf **Kennwort einblenden**.
- Um die Anmeldefelder automatisch auszufüllen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldedaten automatisch senden**.

4. Klicken Sie auf **OK**.

Verwenden des Menüs „Anmeldedaten“

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

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

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

1. Drücken Sie die Tastenkombination für **Password Manager** (die Werkseinstellung lautet **strg** +Windows Logo-Taste+h). Zum Ändern der Tastenkombination klicken Sie im Security Manager Dashboard auf **Password Manager** und anschließend auf **Einstellungen**.
2. Streichen Sie mit Ihrem Finger über den Sensor (bei Computern mit integriertem oder angeschlossenem Fingerabdruck-Lesegerät), oder geben Sie Ihr Windows Kennwort ein.

Organisieren von Anmeldedaten in Kategorien

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

So fügen Sie eine Kategorie hinzu:

1. Klicken Sie im Security Manager Dashboard auf **Password Manager**.
2. Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Kategorie hinzufügen**.

3. Geben Sie einen Namen für die Kategorie ein.
4. Klicken Sie auf **OK**.

So fügen Sie Anmeldedaten einer Kategorie hinzu:

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

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

Verwalten Ihrer Anmeldedaten

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

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

So verwalten Sie Ihre Anmeldedaten:

- ▲ Klicken Sie im Security Manager-Dashboard auf **Password Manager** und anschließend auf die Registerkarte **Verwalten**.
 - **Anmeldedaten hinzufügen** – Klicken Sie auf **Anmeldedaten hinzufügen**, und folgen Sie den Anleitungen auf dem Bildschirm.
 - **Ihre Anmeldedaten** – Klicken Sie auf vorhandene Anmeldedaten, wählen Sie eine der folgenden Optionen aus, und folgen Sie dann den Anleitungen auf dem Bildschirm:
 - **Öffnen** – Öffnet eine Website oder ein Programm, für die/das Sie Anmeldedaten erstellt haben.
 - **Hinzufügen** – Fügt Anmeldedaten hinzu. Weitere Informationen finden Sie unter [„Hinzufügen von Anmeldedaten“ auf Seite 34](#).
 - **Bearbeiten** – Ermöglicht die Bearbeitung von Anmeldedaten. Weitere Informationen finden Sie unter [„Bearbeiten von Anmeldedaten“ auf Seite 35](#).
 - **Löschen** – Löscht eine Website oder ein Programm, für die/das Sie Anmeldedaten festgelegt haben.
 - **Kategorie hinzufügen** – Klicken Sie auf **Kategorie hinzufügen**, und folgen Sie dann den Anleitungen auf dem Bildschirm. Weitere Informationen finden Sie unter [„Organisieren von Anmeldedaten in Kategorien“ auf Seite 36](#).

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

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

Einschätzen der Kennwortsicherheit

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

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

Einstellungen für das Password Manager Symbol

Password Manager versucht, Anmeldebildschirme für Websites und Programme zu identifizieren. Wenn ein Anmeldebildschirm erkannt wird, für den Sie noch keine Anmeldedaten erstellt haben, fordert Sie Password Manager auf, Anmeldedaten für diesen Bildschirm zu erstellen, indem das **Password Manager**-Symbol mit einem Pluszeichen angezeigt wird.

1. Klicken Sie auf das Pfeilsymbol und anschließend auf **Symboleinstellungen**, um festzulegen, wie Password Manager mögliche Anmelde-Sites behandelt.
 - **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern** – Klicken Sie auf diese Option, wenn Sie möchten, dass Password Manager Sie zum Erstellen von Benutzerdaten auffordert, wenn ein Anmeldebildschirm angezeigt wird, für den noch keine Anmeldedaten eingerichtet sind.
 - **Diesen Bildschirm ausschließen** – Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht erneut von Password Manager aufgefordert werden möchten, Anmeldedaten für diesen Anmeldebildschirm hinzuzufügen.

So fügen Sie Anmeldedaten für einen neuen Bildschirm hinzu:

- Öffnen Sie den Website-Anmeldebildschirm oder die Programmseite, für die noch keine Anmeldedaten eingerichtet wurden; öffnen Sie dann das Security Manager Dashboard, und klicken Sie auf **Password Manager**.
- Klicken Sie auf **Anmeldedaten hinzufügen**.

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

Der Bildschirm „Anmeldedaten zu Password Manager hinzufügen“ wird angezeigt.

- Folgen Sie den Anleitungen auf dem Bildschirm. Weitere Informationen finden Sie unter [„Hinzufügen von Anmeldedaten“ auf Seite 34](#).
 - Das **Password Manager**-Symbol wird bei nun jedem Öffnen dieses Website-Anmeldebildschirms bzw. Programmbildschirms angezeigt.
2. Wenn keine Aufforderung zum Hinzufügen von Anmeldedaten angezeigt werden soll, deaktivieren Sie das betreffende Kontrollkästchen.
 3. Für den Zugriff auf weitere Password Manager-Einstellungen klicken Sie auf **Password Manager** und anschließend im Security Manager-Dashboard auf **Einstellungen**.

VeriSign Identity Protection (VIP)

Für Websites, die die VeriSign VIP-Funktion unterstützen, können Sie VeriSign VIP-Zugriffstoken erzeugen. Anhand dieser Token erstellt Password Manager automatische Anmeldedaten, bei denen die Token mittels Drag & Drop in Anmeldebildschirme mit VeriSign VIP-Unterstützung übernommen bzw. von Hand in vorgegebene Felder eingegeben werden.

Die Aktivierung der VeriSign VIP-Funktion und die Erzeugung eines Tokens kann im Security Manager Dashboard oder auf einer beliebigen Website mit VeriSign VIP-Unterstützung vorgenommen werden. Zur Verwendung des Tokens müssen Sie sich auf jeder Website registrieren, auf der das Token genutzt werden soll.

Nach der Registrierung und vor dem ersten Gebrauch können Sie das Token (optional) an Ihre regulären Anmeldedaten koppelt und mit diesen verwenden. Falls die betreffende Website eine Koppelung der Anmeldedaten mit einem Token nicht zulässt, können Sie die Token-Daten auch manuell in das betreffende Feld ziehen und dort ablegen.

So aktivieren Sie VeriSign VIP und erzeugen ein VeriSign VIP-Token im Security Manager Dashboard:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter [„Öffnen von Security Manager“ auf Seite 29](#).
2. Klicken Sie auf **Password Manager** und anschließend auf **VIP**.
3. Klicken Sie auf **Get VIP** (VIP abrufen).

Ein VeriSign VIP-Token wird erzeugt und auf der VeriSign VIP-Seite angezeigt. Das Token wird nun bei jedem Zugriff auf diese Seite angezeigt.

So aktivieren Sie VeriSign VIP und erzeugen ein VeriSign VIP-Token auf einer Website:

1. Wenn Sie eine Website mit VeriSign VIP-Unterstützung besuchen, zeigt Password Manager eine entsprechende Meldung an.
2. Erstellen Sie Anmeldedaten für den Bildschirm. Weitere Informationen finden Sie unter [„Hinzufügen von Anmeldedaten“ auf Seite 34](#).
3. Wählen Sie im Dialogfeld „Anmeldedaten erstellen“ die Option **I want additional account protection with VIP** (Ich möchte zusätzlichen VIP-Schutz für mein Konto) aus.

So registrieren Sie ein VeriSign VIP-Token bei einer Website:

1. Melden Sie sich manuell oder mithilfe der Password Manager Anmeldedaten bei einer VeriSign VIP-fähigen Website an.
2. Klicken Sie auf das VeriSign VIP-Ballonsymbol, um Anmeldedaten für diese Website zu erstellen.
3. Aktivieren Sie im Dialogfeld „Anmeldedaten zu Password Manager hinzufügen“ das Kontrollkästchen **I want VIP security on this site** (Ich möchte VIP-Sicherheit auf dieser Website).

Diese Option wird nur auf Websites angezeigt, die die VeriSign VIP-Funktion unterstützen. Wenn die VIP-Sicherheit von der betreffenden Website unterstützt wird, können Sie zudem festlegen, dass zusätzlich zur üblichen Authentifizierungsmethode auch Ihr VIP-Sicherheitscode eingegeben wird.

Einstellungen

Sie können Einstellungen zur Personalisierung von HP ProtectTools Security Manager vornehmen:

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

Credential Manager

Mit den Security Manager-Anmeldedaten weisen Sie Ihre Identität nach. Der Administrator dieses Computers kann einstellen, anhand welcher Anmeldedaten Sie Ihre Identität bei Ihrem Windows Konto, bei Websites oder Programmen nachweisen können.

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

- Kennwort
- SpareKey
- Fingerabdrücke
- Smart Card
- Gesicht

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

Ändern Ihres Windows Kennworts

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

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

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

Einrichten eines SpareKey

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

Bei der Ersteinrichtung mithilfe des Einführungsassistenten werden Sie von HP ProtectTools zur Einrichtung Ihres persönlichen SpareKey aufgefordert.

So richten Sie einen persönlichen SpareKey ein:

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

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

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

Registrieren Ihrer Fingerabdrücke

Wenn Ihr Computer über ein integriertes oder angeschlossenes Fingerabdruck-Lesegerät verfügt, leitet Sie der Einführungsassistent von HP ProtectTools Security Manager bei der Ersteinrichtung durch die Konfiguration oder „Registrierung“ Ihrer Fingerabdrücke. Sie können Ihre Fingerabdrücke

auch auf der Seite „Fingerabdruck“ im Security Manager Dashboard unter **Credential Manager** registrieren.

1. Es wird eine Abbildung von zwei Händen angezeigt. Finger, die bereits registriert wurden, werden grün dargestellt. Klicken Sie auf einen Finger in der Darstellung.



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

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



ACHTUNG: Bei der Registrierung der Fingerabdrücke in der Einführungsphase werden die Fingerabdruckdaten erst mit einem Klick auf **Weiter** gespeichert. Wenn der Computer eine Zeit lang inaktiv ist oder das Programm geschlossen wird, werden die von Ihnen vorgenommenen Änderungen **nicht** gespeichert.

Einrichten einer Smart Card

Administratoren müssen die Smart Card initialisieren und registrieren, bevor sie für die Authentifizierung verwendet werden kann.

Initialisieren der Smart Card

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



HINWEIS: Die Software ActivIdentity muss installiert werden.

1. Legen Sie die Karte in das Lesegerät ein.
2. Klicken Sie auf **Start, Alle Programme** und dann auf **ActivClient PIN Initialization Tool**.
3. Geben Sie eine PIN ein, und bestätigen Sie diese.
4. Klicken Sie auf **Weiter**.

Die Smart Card-Software stellt Ihnen einen Entsperrschlüssel zur Verfügung. Die meisten Smart Cards sperren sich selbst, wenn die PIN fünfmal falsch eingegeben wird. Der Schlüssel wird zum Entsperrern der Karte verwendet.

5. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
6. Klicken Sie auf **Anmeldeinformationen** und dann auf **Smart Card**.
7. Klicken Sie auf die Registerkarte **Verwaltung**.
8. Vergewissern Sie sich, dass **Smart Card einrichten** ausgewählt ist.

9. Geben Sie Ihre PIN ein, klicken Sie auf **Übernehmen**, und folgen Sie dann den Anleitungen auf dem Bildschirm.
10. Nachdem die Smart Card erfolgreich initialisiert wurde, muss sie noch registriert werden.

Registrieren der Smart Card

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

1. Klicken Sie unter **Zentrale Verwaltung** auf **Installations-Assistent**.
2. Klicken Sie auf der Willkommenseite auf **Weiter**, und geben Sie dann Ihr Windows Kennwort ein.
3. Klicken Sie auf der SpareKey-Seite auf **Skip SpareKey Setup** (SpareKey-Einrichtung überspringen), außer Sie möchten die SpareKey-Informationen aktualisieren.
4. Klicken Sie auf der Seite zum Aktivieren der Sicherheitsfunktionen auf **Weiter**.
5. Vergewissern Sie sich, dass auf der Seite zur Auswahl der Anmeldeinformationen die Option **Smart Card einrichten** ausgewählt ist, und klicken Sie dann auf **Weiter**.
6. Geben Sie auf der Smart Card-Seite Ihre PIN ein, und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.

Benutzer können eine Smart Card in Security Manager registrieren. Weitere Informationen finden Sie in der Hilfe zu Software Security Manager for HP ProtectTools.

Konfigurieren der Smart Card

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

- **Einstellungen** – Sie können den Computer so einstellen, dass er beim Entfernen einer Smart Card automatisch gesperrt wird.



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

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

- **Erase HP ProtectTools data only** (Nur HP ProtectTools Daten löschen) – Löscht nur das während der Karteninitialisierung erstellte HP ProtectTools Zertifikat. Es werden keine anderen Daten von der Karte gelöscht.
- **Erase all data on the smart card** (Alle Daten von der Smart Card löschen) – Löscht alle Daten von der angegebenen Smart Card. Die Karte kann dann nicht mehr mit HP ProtectTools oder anderen Anwendungen verwendet werden.

 **HINWEIS:** Funktionen, die von Ihrer Smart Card nicht unterstützt werden, sind nicht verfügbar.

- ▲ Klicken Sie auf **Übernehmen**.

Registrieren von Gesichtsszenen für die Gesichtserkennung

Wenn Ihr Computer über eine integrierte oder angeschlossene Webcam verfügt, leitet Sie der Einführungsassistent von HP ProtectTools Security Manager bei der Ersteinrichtung durch die Konfiguration oder „Registrierung“ Ihrer Gesichtsszenen. Sie können Ihre Gesichtsszenen auch auf der Seite für die Gesichtserkennung im Security Manager Dashboard unter **Credential Manager** registrieren.

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

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

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

So registrieren Sie eine Gesichtsszene mit dem Einführungsassistenten:

1. Klicken Sie auf der Seite „Gesicht“ des Assistenten auf **Erweitert**, und konfigurieren Sie zusätzliche Sicherheitsoptionen. Weitere Informationen finden Sie unter [„Erweiterte Benutzereinstellungen“ auf Seite 46](#).
2. Klicken Sie auf **OK**.
3. Klicken Sie auf **Start** oder – falls Sie bereits Gesichtsszenen registriert haben – auf **Neue Szene registrieren**.
4. Wenn Sie keine zusätzlichen Sicherheitsoptionen auswählen, werden Sie zur Auswahl einer zusätzlichen Sicherheitsoption aufgefordert. Folgen Sie den Anleitungen auf dem Bildschirm, und klicken Sie dann auf **Weiter**. Weitere Informationen finden Sie unter [„Erweiterte Benutzereinstellungen“ auf Seite 46](#).
5. Klicken Sie auf das **Kamera**-Symbol, und folgen Sie den Anleitungen auf dem Bildschirm, um eine Gesichtsszene zu registrieren.

Folgen Sie den Anleitungen auf dem Bildschirm, und schauen Sie auf Ihr Bild, während die Szenen aufgezeichnet werden.

6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.

Sie können Gesichtsszenen auch im Security Manager Dashboard registrieren:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter [„Öffnen von Security Manager“ auf Seite 29](#).
2. Klicken Sie unter **Meine Anmeldeinformationen** auf **Credential Manager** und dann auf **Gesicht**.
3. Klicken Sie auf **Erweitert**, und konfigurieren Sie zusätzliche Sicherheitsoptionen. Weitere Informationen finden Sie unter [„Erweiterte Benutzereinstellungen“ auf Seite 46](#).
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Start** oder – falls Sie bereits Gesichtsszenen registriert haben – auf **Neue Szene registrieren**.
6. Wenn Sie keine zusätzlichen Sicherheitsoptionen auswählen, werden Sie zur Auswahl einer zusätzlichen Sicherheitsoption aufgefordert. Folgen Sie den Anleitungen auf dem Bildschirm, und klicken Sie dann auf **Weiter**. Weitere Informationen finden Sie unter [„Erweiterte Benutzereinstellungen“ auf Seite 46](#).
7. Klicken Sie auf das **Kamera**-Symbol, und folgen Sie den Anleitungen auf dem Bildschirm, um eine Gesichtsszene zu registrieren.

Folgen Sie den Anleitungen auf dem Bildschirm, und schauen Sie auf Ihr Bild, während die Szenen aufgezeichnet werden.

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

Erweiterte Benutzereinstellungen

Diese Optionen werden auch auf der Seite „Zusätzliche Sicherheit“ angezeigt, wenn keine weiteren Sicherheitsoptionen ausgewählt wurden.

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter [„Öffnen von Security Manager“ auf Seite 29](#).
2. Klicken Sie unter **Meine Anmeldedaten** auf **Credential Manager** und dann auf **Gesicht**.
3. Klicken Sie auf **Erweitert**, um die folgenden Sicherheitsoptionen zu konfigurieren:
 - a. Registerkarte **Sicherheit** – Wählen Sie eine der folgenden Optionen aus:
 - **No additional security** (Keine zusätzliche Sicherheitsoption) – Wählen Sie diese Option aus, falls Sie keine zusätzliche Sicherheitsoption für die Gesichtserkennung definieren möchten.
 - **Use PIN for additional security** (PIN für zusätzliche Sicherheit verwenden) – Wählen Sie diese Option aus, falls eine benutzerspezifische PIN für die Gesichtserkennung erforderlich sein soll.
 - Klicken Sie auf **PIN erstellen**.
 - Geben Sie Ihr Windows Kennwort ein.
 - Geben Sie die neue PIN ein, und bestätigen Sie sie, indem Sie die Eingabe wiederholen.

Nach der PIN-Erstellung stehen die folgenden Optionen zur Auswahl: **Ändern**, **Zurücksetzen** und **PIN entfernen**.
 - **Use PIN for additional security** (PIN für zusätzliche Sicherheit verwenden) – Wählen Sie diese Option, falls Ihr Bluetooth-fähiges Telefon mit der Gesichtserkennung gekoppelt werden soll. Nachdem bei der Windows Anmeldung Ihr Gesicht erkannt wurde, überprüft Face Recognition, ob das gekoppelte Bluetooth Telefon vorhanden ist. Wenn es vorhanden (und Bluetooth aktiviert) ist, können Sie sich bei Windows anmelden.
 - Vergewissern Sie sich, dass Bluetooth sowohl am Computer als auch am Telefon aktiviert ist.

Wenn kein Telefon mit aktivierter Bluetooth Funktion vorhanden ist, werden Sie aufgefordert, das gekoppelte Bluetooth Telefon zu aktivieren und den Anmeldevorgang zu wiederholen. Nach 30 Sekunden wird die Anzeige des Face Recognition Anmeldefensters beendet. Zum Starten des Anmeldevorgangs klicken Sie auf das **Kamera**-Symbol. Wenn kein Telefon mit aktivierter Bluetooth Funktion vorhanden ist, können Sie sich auch mit Ihrem normalen Windows Kennwort anmelden.
 - Klicken Sie auf **Hinzufügen**.
 - Wenn Ihr Bluetooth Gerät angezeigt wird, wählen Sie es aus und klicken dann auf **Weiter**.
 - b. Registerkarte **Sonstige Einstellungen** – Aktivieren Sie die Kontrollkästchen, um eine oder mehrere der folgenden Optionen auszuwählen. Wenn Sie eine Funktion nicht auswählen

Klicken Sie auf **OK**.

möchten, deaktivieren Sie das betreffende Kontrollkästchen. Die hier vorgenommenen Einstellungen gelten nur für den aktuellen Benutzer.

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

Klicken Sie auf **OK**.

Ihre persönliche ID-Card

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

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

So ändern Sie den angezeigten Namen:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter [„Öffnen von Security Manager“ auf Seite 29](#).
2. Klicken Sie auf die ID-Card links oben im Dashboard.
3. Klicken Sie auf das Feld mit Ihrem Windows Benutzernamen für dieses Konto, geben Sie einen neuen Namen ein, und klicken Sie dann auf **Speichern**.

So ändern Sie das angezeigte Bild:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter [„Öffnen von Security Manager“ auf Seite 29](#).
2. Klicken Sie auf die ID-Card links oben im Dashboard.
3. Klicken Sie auf **Bild wählen**; klicken Sie dann auf ein Bild und anschließend auf **Speichern**.

Festlegen der Einstellungen

Sie können die Einstellungen für HP ProtectTools Security Manager personalisieren. Klicken Sie im Security Manager-Dashboard auf **Erweitert** und anschließend auf **Voreinstellungen**. Die verfügbaren Einstellungen werden auf zwei Registerkarten angezeigt: **Allgemein** und **Fingerabdruck**.

Registerkarte „Allgemein“

Darstellung – Show icon in taskbar notification area (Symbol im Infobereich der Taskleiste anzeigen)

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

Registerkarte „Fingerabdruck“



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

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

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

- **Fingerabdruckscan-Feedback** – Wird nur angezeigt, wenn ein Fingerabdruck-Lesegerät verfügbar ist. Verwenden Sie diese Einstellung, um das Feedback anzupassen, das Sie erhalten, wenn Sie mit dem Finger über den Sensor streichen.
 - **Sound-Feedback aktivieren** – Security Manager gibt akustische Signale aus, wenn ein Fingerabdruck durch Streichen über den Sensor registriert wurde, wobei für spezifische Programmereignisse verschiedene Signale verwendet werden. Sie können diesen Ereignissen auf der Registerkarte **Sounds** in der Windows Systemsteuerung andere Töne zuweisen oder akustische Signale ausschalten, indem Sie diese Option deaktivieren.
 - **Feedback zur Scanqualität anzeigen**

Um alle durch Streichen über den Sensor registrierten Fingerabdrücke unabhängig von der Qualität anzuzeigen, aktivieren Sie das Kontrollkästchen.

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

Sichern und Wiederherstellen Ihrer Daten

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

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



HINWEIS: Mit dieser Funktion werden nur die Daten gesichert.

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

So sichern Sie Ihre Daten:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter [„Öffnen von Security Manager“ auf Seite 29](#).
2. Klicken Sie links im Dashboard auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Daten sichern**.
4. Wählen Sie die Module aus, die gesichert werden sollen. In den meisten Fällen empfiehlt es sich, alle Module auszuwählen.
5. Identität bestätigen.

6. Geben Sie einen Namen für die Speicherdatei ein. Die Datei wird standardmäßig im Ordner „Dokumente“ gespeichert. Klicken Sie auf **Durchsuchen**, um einen anderen Speicherort anzugeben.
7. Geben Sie ein Kennwort ein, um die Datei zu schützen.
8. Klicken Sie auf **Fertig stellen**.

So stellen Sie Ihre Daten wieder her:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter [„Öffnen von Security Manager“ auf Seite 29](#).
2. Klicken Sie links im Dashboard auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Daten wiederherstellen**.
4. Wählen Sie die zuvor erstellte Speicherdatei aus. Geben Sie den Pfad in das entsprechende Feld ein, oder klicken Sie auf **Durchsuchen**.
5. Geben Sie das zuvor verwendete Kennwort zum Schützen der Datei ein.
6. Wählen Sie die Module aus, deren Daten wiederhergestellt werden sollen. In den meisten Fällen empfiehlt es sich, alle aufgeführten Module auszuwählen.
7. Bestätigen Sie Ihr Windows Kennwort.
8. Klicken Sie auf **Fertig stellen**.

5 Drive Encryption for HP ProtectTools (nur ausgewählte Modelle)

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

Mit dem Installations-Assistenten für HP ProtectTools Security Manager können Windows Administratoren Drive Encryption aktivieren, den Verschlüsselungsschlüssel sichern und Laufwerke auswählen oder deaktivieren. Weitere Informationen finden Sie in der Hilfe zur HP ProtectTools Security Manager-Software.

Die folgenden Aufgaben können mit Drive Encryption durchgeführt werden:

- Auswahl der Drive Encryption-Einstellungen:
 - Aktivieren eines TPM-geschützten Kennworts
 - Ver- und Entschlüsseln einzelner Laufwerke oder Partitionen mit Software-Verschlüsselung
 - Ver- und Entschlüsseln einzelner selbstverschlüsselnder Laufwerke mit Hardware-Verschlüsselung
 - Erhöhen der Sicherheit durch Deaktivierung von Standby und Energiesparmodus um sicherzustellen, dass die Systemstart-Authentifizierung von Drive Encryption immer erforderlich ist



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

- Erstellen von Sicherungsschlüsseln
- Wiederherstellen eines Drive Encryption-Schlüssels
- Aktivieren der Systemstart-Authentifizierung von Drive Encryption per Kennwort, registriertem Fingerabdruck oder Smart Card-PIN

Öffnen von Drive Encryption

Administratoren können auf Drive Encryption über HP ProtectTools Administrator-Konsole zugreifen.

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

Allgemeine Aufgaben

Aktivieren von Drive Encryption für Standard-Festplatten

Standard-Festplatten werden mit Softwareverschlüsselung verschlüsselt. Um Drive Encryption zu aktivieren, führen Sie die folgenden Schritte aus:

1. Verwenden Sie den Installations-Assistenten von HP ProtectTools Security Manager, um Drive Encryption zu aktivieren.
2. Folgen Sie den Anleitungen auf dem Bildschirm, bis die Seite **Sicherheitsfunktionen aktivieren** angezeigt wird, und fahren Sie anschließend mit Schritt 4 unten fort.

– oder –

1. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Sicherheit**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Funktionen**.
4. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.

 **HINWEIS:** Wenn keine Festplatte zur Verschlüsselung ausgewählt ist, wird die Systemstart-Authentifizierung von Drive Encryption aktiviert, aber die Festplatte(n) wird/werden nicht verschlüsselt.

5. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die Festplatte, die verschlüsselt werden soll, und klicken Sie dann auf **Weiter**
6. Um den Verschlüsselungsschlüssel zu sichern, schließen Sie das Speichergerät an den richtigen Steckplatz an.

 **HINWEIS:** Um den Verschlüsselungsschlüssel zu speichern, müssen Sie ein USB-Speichergerät im FAT32-Format verwenden. Zur Sicherung kann eine Diskette, ein USB Memory Stick, eine Secure Digital (SD) Memory Card oder eine MMC verwendet werden.

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

 **HINWEIS:** Der Computer wird neu gestartet.

Drive Encryption wurde aktiviert. Die Verschlüsselung der Festplatte kann, je nach Größe des Laufwerks, einige Stunden dauern.

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

Aktivieren von Drive Encryption für selbstverschlüsselnde Festplatten

Selbstverschlüsselnde Laufwerke nach den OPAL-Spezifikationen der Trusted Computing Group für die Verwaltung selbstverschlüsselnder Laufwerke lassen sich entweder mit Software- oder mit

Hardwareverschlüsselung verschlüsseln. Gehen Sie wie folgt vor, um Drive Encryption für selbstverschlüsselnde Laufwerke zu aktivieren:

1. Verwenden Sie den Installations-Assistenten von HP ProtectTools Security Manager, um Drive Encryption zu aktivieren.
2. Folgen Sie den Anleitungen auf dem Bildschirm, bis die Seite **Sicherheitsfunktionen aktivieren** angezeigt wird, und fahren Sie anschließend mit Schritt 4 entweder unter „Softwareverschlüsselung“ oder unter „Hardwareverschlüsselung“ fort.

 **HINWEIS:** Wenn Ihr Computer nicht über ein selbstverschlüsselndes Laufwerk verfügt, das den OPAL-Spezifikationen der Trusted Computing Group für die Verwaltung selbstverschlüsselnder Laufwerke entspricht, ist die Option Hardwareverschlüsselung nicht verfügbar, und es wird die Softwareverschlüsselung verwendet.

Bei einer Mischung selbstverschlüsselnder und Standard-Laufwerke ist die Option Hardwareverschlüsselung nicht verfügbar, und es wird die Softwareverschlüsselung verwendet.

– oder –

Softwareverschlüsselung

1. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Sicherheit**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Funktionen**.
4. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.
5. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die Festplatte, die verschlüsselt werden soll, und klicken Sie dann auf **Weiter**.
6. Um den Verschlüsselungsschlüssel zu sichern, schließen Sie das Speichergerät an den richtigen Steckplatz an.

 **HINWEIS:** Um den Verschlüsselungsschlüssel zu speichern, müssen Sie ein USB-Speichergerät im FAT32-Format verwenden. Zur Sicherung kann eine Diskette, ein USB Memory Stick, eine Secure Digital (SD) Memory Card oder eine MMC verwendet werden.

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

 **HINWEIS:** Der Computer wird neu gestartet.

Drive Encryption wurde aktiviert. Die Verschlüsselung der Festplatte kann, je nach Größe des Laufwerks, einige Stunden dauern.

Hardwareverschlüsselung

1. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Sicherheit**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Funktionen**.
4. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.

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

Wenn mehr als ein Laufwerk angezeigt wird, werden die Kontrollkästchen automatisch ausgewählt, aber nicht abgeblendet.

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

5. Vergewissern Sie sich, dass das Kontrollkästchen **Hardwareverschlüsselung für Laufwerk verwenden** unten im Bildschirm markiert ist.
6. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die Festplatte, die verschlüsselt werden soll, und klicken Sie dann auf **Weiter**.
7. Um den Verschlüsselungsschlüssel zu sichern, schließen Sie das Speichergerät an den richtigen Steckplatz an.

 **HINWEIS:** Um den Verschlüsselungsschlüssel zu speichern, müssen Sie ein USB-Speichergerät im FAT32-Format verwenden. Zur Sicherung kann eine Diskette, ein USB Memory Stick, eine Secure Digital (SD) Memory Card oder eine MMC verwendet werden.

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

 **HINWEIS:** Der Computer muss neu gestartet werden.

Drive Encryption wurde aktiviert. Die Verschlüsselung des Laufwerks kann einige Minuten dauern.

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

Deaktivieren von Drive Encryption

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

- ▲ Folgen Sie den Anleitungen auf dem Bildschirm, bis die Seite **Sicherheitsfunktionen aktivieren** angezeigt wird, und fahren Sie anschließend mit Schritt 4 unten fort.

– ODER –

1. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Sicherheit**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Funktionen**.
4. Entfernen Sie die Markierung des Kontrollkästchens **Drive Encryption**, und klicken Sie dann auf **Weiter**.

Die Deaktivierung der Verschlüsselung wird gestartet.

 **HINWEIS:** Wenn Softwareverschlüsselung verwendet wurde, wird die Entschlüsselung gestartet. Dies kann, je nach Größe des Laufwerks, einige Stunden dauern. Sobald die Entschlüsselung abgeschlossen ist, wird Drive Encryption deaktiviert.

Wenn Hardwareverschlüsselung verwendet wurde, wird das Laufwerk sofort entschlüsselt. Dies kann ein paar Minuten dauern. Anschließend wird Drive Encryption deaktiviert.

Sobald das Laufwerk deaktiviert ist, muss der Computer neu gestartet werden.

Anmelden, nachdem Drive Encryption aktiviert wurde

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

 **HINWEIS:** Stellen Sie bei Hardwareverschlüsselung sicher, dass der Computer ausgeschaltet wird. Wenn der Computer nicht ausgeschaltet und dann neu gestartet wird, wird der Bildschirm für die Systemstart-Authentifizierung von Drive Encryption nicht angezeigt.

HINWEIS: Bei einem Start aus dem Standby- oder dem Energiesparmodus wird die Systemstart-Authentifizierung von Drive Encryption für Software- und Hardwareverschlüsselung nicht angezeigt, es sei denn, diese sind deaktiviert.

Bei einem Start aus dem Ruhezustand wird die Systemstart-Authentifizierung von Drive Encryption angezeigt.

HINWEIS: Wenn der Windows Administrator die Systemstartsicherheit in HP ProtectTools Security Manager aktiviert hat, können Sie sich sofort nach dem Einschalten am Computer anmelden, statt erst im Anmeldebildschirm von Drive Encryption.

1. Klicken Sie auf Ihren Benutzernamen, und geben Sie anschließend Ihr Windows Kennwort oder Ihre Smart Card-PIN ein, oder streichen Sie mit einem registrierten Finger über den Sensor.

 **HINWEIS:** Folgende Smart Cards werden unterstützt:

Smart Cards

- ActivIdentity 64K V2C Smart Card
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB key V3.0 ZFG-48001-A

PCMCIA-Lesegeräte

- Express Card 54 SCR3340, internes Lesegerät
- SCR 201
- SCR 243 (auch von HP)
- ActivCard
- Omnikey 4040
- Cisco

USB-Lesegeräte

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- HP Smart Card-Terminal

2. Klicken Sie auf **OK**.



HINWEIS: Wenn Sie einen Wiederherstellungsschlüssel zur Anmeldung beim Anmeldebildschirm von Drive Encryption verwenden, müssen Sie sich mit Ihrem Kennwort, Ihrer Smart Card-PIN oder einem registrierten Fingerabdruck beim Windows Anmeldebildschirm anmelden.

Schützen Ihrer Daten durch Verschlüsselung der Festplatte

Es wird empfohlen, den Installations-Assistenten von HP ProtectTools Security Manager zu verwenden, um Daten durch Verschlüsselung der Festplatte zu schützen:

1. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Drive Encryption**, um die verfügbaren Optionen aufzurufen.
2. Klicken Sie auf **Einstellungen**.
3. Bei Laufwerken mit Softwareverschlüsselung wählen Sie die Laufwerkspartitionen für die Verschlüsselung aus.



HINWEIS: Dies gilt auch für den Fall, dass eine oder mehrere Standardfestplatten und ein oder mehrere selbstverschlüsselnde Laufwerke vorhanden sind.

– oder –

- ▲ Bei Laufwerken mit Hardwareverschlüsselung wählen Sie das/die Laufwerk(e) für die Verschlüsselung aus. Mindestens ein Laufwerk muss ausgewählt werden.

Anzeigen der Verschlüsselungsstatus

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



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

1. Öffnen Sie HP ProtectTools Security Manager.
2. Klicken Sie unter **Meine Daten** auf **Drive Encryption**.

Bei Softwareverschlüsselung wird einer der folgenden Statuscodes unter **Laufwerkstatus** angezeigt:

- Aktiviert
- Deaktiviert
- Nicht verschlüsselt
- Verschlüsselt
- Wird gerade verschlüsselt
- Wird gerade entschlüsselt

Bei Hardwareverschlüsselung wird der folgende Statuscode unter **Laufwerkstatus** angezeigt:

- Verschlüsselt

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

Erweiterte Aufgaben

Verwalten von Drive Encryption (Administrator-Aufgabe)

Auf der Einstellungsseite von Drive Encryption können Administratoren den Status von Drive Encryption anzeigen und ändern (Aktiviert, Deaktiviert oder Hardwareverschlüsselung wurde aktiviert) und den Verschlüsselungsstatus aller Festplatten auf dem Computer anzeigen.



HINWEIS: Die Hardwareverschlüsselung kann auf der Einstellungsseite nicht geändert werden.

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

Softwareverschlüsselung

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

Hardwareverschlüsselung

- Verschlüsselt

Ver- und Entschlüsseln einzelner Laufwerke (nur Softwareverschlüsselung)

Administratoren können auf der Einstellungsseite eine oder mehrere Festplatten auf dem Computer verschlüsseln oder ein bereits verschlüsseltes Laufwerk entschlüsseln.

1. Öffnen Sie HP ProtectTools Administrator-Konsole.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol + links von **Drive Encryption**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Einstellungen**.
4. Aktivieren oder deaktivieren Sie unter **Laufwerkstatus** das Kontrollkästchen für die Festplatte, die verschlüsselt oder entschlüsselt werden soll, und klicken Sie dann auf **Übernehmen**



HINWEIS: Wenn die Festplatte gerade verschlüsselt oder entschlüsselt wird, wird eine Fortschrittsanzeige mit der noch verbleibenden Zeit bis zum Abschluss der aktuellen Sitzung angezeigt.

Wenn der Computer während der Verschlüsselung heruntergefahren wird oder in den Standby- oder Energiesparmodus oder den Ruhezustand wechselt und dann neu gestartet wird, wird die Zeit auf der Fortschrittsanzeige auf den Beginn zurückgesetzt, die Verschlüsselung wird aber dort fortgesetzt, wo sie unterbrochen wurde. Die Fortschrittsanzeige in Prozent und die verbleibende Zeit ändern sich schneller, was auf den vorhergehenden Prozess zurückzuführen ist.

HINWEIS: Dynamische Partitionen werden nicht unterstützt. Wenn eine Partition als verfügbar angezeigt wird, sich aber nicht verschlüsseln lässt, so handelt es sich um eine dynamische Partition. Eine dynamische Partition entsteht, wenn eine vorhandene Partition zum Erstellen einer neuer Partition in der Festplattenverwaltung geschrumpft wird.

Eine Warnmeldung wird angezeigt, wenn eine Partition in eine dynamische Partition umgewandelt wird.

Sicherung und Wiederherstellung (Administrator-Aufgabe)

Wenn Drive Encryption aktiviert ist, können Administratoren die Sicherungsseite für den Verschlüsselungsschlüssel verwenden, um Verschlüsselungsschlüssel auf Wechselmedien zu sichern und eine Wiederherstellung durchzuführen.

Sichern von Verschlüsselungsschlüsseln

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

 **ACHTUNG:** Das Speichergerät mit dem Verschlüsselungsschlüssel muss an einem sicheren Ort aufbewahrt werden, denn wenn Sie das Kennwort vergessen, Ihre Smart Card verlieren oder keinen Fingerabdruck registriert haben, stellt dieses Gerät die einzige Zugriffsmöglichkeit auf die Festplatte dar.

1. Öffnen Sie HP ProtectTools Administrator-Konsole.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol + links von **Drive Encryption**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Encryption Key Backup** (Sichern des Sicherungsschlüssels).
4. Schließen Sie das Speichergerät an, das zur Sicherung des Verschlüsselungsschlüssels verwendet werden soll.
5. Aktivieren Sie unter **Laufwerk** das Kontrollkästchen für das Gerät, auf dem der Verschlüsselungsschlüssel gesichert werden soll.
6. Klicken Sie auf **Schlüssel sichern**.
7. Lesen Sie den dargestellten Text, und klicken Sie dann auf **Weiter**. Der Verschlüsselungsschlüssel wird auf dem von Ihnen ausgewählten Speichergerät gespeichert.

Wiederherstellen von Verschlüsselungsschlüsseln

Administratoren können einen Verschlüsselungsschlüssel von einem Wechselmediengerät aus wiederherstellen, auf dem er zuvor gesichert wurde:

1. Schalten Sie den Computer ein.
2. Schließen Sie das Wechselmediengerät an, das Ihren Sicherungsschlüssel enthält.
3. Klicken Sie im Anmeldedialogfeld für Drive Encryption for HP ProtectTools auf **Optionen**.
4. Klicken Sie auf **Wiederherstellung**.
5. Wählen Sie die Datei aus, die Ihren Sicherungsschlüssel enthält, oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen, und klicken Sie danach auf **Weiter**.
6. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

Ihr Computer wird gestartet.

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

6 Privacy Manager for HP ProtectTools (bestimmte Modelle)

Privacy Manager für HP ProtectTools ermöglicht Ihnen die Nutzung von erweiterten Sicherheits-Anmeldemethoden (Authentifizierung), um die Quelle, die Integrität und die Sicherheit bei der Übertragung von E-Mails oder Microsoft® Office-Dokumenten zu überprüfen.

Privacy Manager ergänzt die Sicherheitsinfrastruktur von HP ProtectTools Security Manager, die die folgenden Sicherheits-Anmeldemethoden umfasst:

- Fingerabdruck-Authentifizierung
- Windows® Kennwort
- Smart Card
- Gesichtserkennung

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

Öffnen von Privacy Manager

So öffnen Sie Privacy Manager:

- Sie erhalten Zugriff auf Outlook-spezifische Funktionen in Microsoft Outlook, indem Sie auf der Registerkarte **Nachricht** in der Gruppe **Datenschutz** auf **Sicher senden** klicken.
- Sie erhalten Zugriff auf die meisten Funktionen in Microsoft Office-Dokumenten, indem Sie auf der Registerkarte **Startseite** in der Gruppe **Datenschutz** auf **Signieren und verschlüsseln** klicken.
- Zugriff auf zusätzliche Funktionen erhalten Sie über das HP ProtectTools Security Manager-Dashboard.
 - Klicken Sie auf **Start, Alle Programme, HP, HP ProtectTools Security Manager** und danach auf **Privacy Manager**.
– oder –
 - Klicken Sie auf die Desktop-Minianwendung **HP ProtectTools**.
– oder –
 - Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **Privacy Manager** und anschließend auf **Konfiguration**.

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.

Mit dem Certificate Manager können Sie folgende Aufgaben ausführen:

- [„Anfordern eines Privacy Manager-Zertifikats“ auf Seite 62](#)
- [„Abrufen eines vorab zugewiesenen Privacy Manager-Unternehmenszertifikats“ auf Seite 63](#)
- [„Festlegen eines Privacy Manager-Standardzertifikats“ auf Seite 66](#)
- [„Importieren eines Zertifikats von einem anderen Anbieter“ auf Seite 63](#)
- [„Anzeigen der Details eines Privacy Manager-Zertifikats“ auf Seite 64](#)
- [„Erneuern eines Privacy Manager-Zertifikats“ auf Seite 64](#)
- [„Festlegen eines Privacy Manager-Standardzertifikats“ auf Seite 66](#)
- [„Löschen eines Privacy Manager-Zertifikats“ auf Seite 66](#)
- [„Wiederherstellen eines Privacy Manager-Zertifikats“ auf Seite 66](#)
- [„Widerrufen eines Privacy Manager-Zertifikats“ auf Seite 67](#)

Anfordern eines Privacy Manager-Zertifikats

Um Zugriff auf die Privacy Manager-Funktionen zu erhalten, muss zunächst ein Privacy Manager-Zertifikat (aus Privacy Manager heraus) mit einer gültigen E-Mail-Adresse angefordert und installiert werden. Die E-Mail-Adresse muss als Konto von Microsoft Outlook auf dem Computer eingerichtet sein, von dem aus das Privacy Manager-Zertifikat angefordert wird.

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf **Privacy Manager-Zertifikat anfordern**.
3. Lesen Sie den Text auf dem Anfangsbildschirm, und klicken Sie dann auf **Weiter**.
4. Lesen Sie den Lizenzvertrag auf der Seite „Lizenzvertrag“.
5. Aktivieren Sie das Kontrollkästchen neben **Check here to accept the terms of this license agreement** (Hier klicken, um die Lizenzvereinbarung anzunehmen), und klicken Sie dann auf **Weiter**.
6. Geben Sie auf der Seite „Ihre Zertifikatsdetails“ die erforderlichen Angaben ein, und klicken Sie dann 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.

Abrufen eines vorab zugewiesenen Privacy Manager-Unternehmenszertifikats

1. Öffnen Sie in Outlook die E-Mail, in der Sie darüber informiert wurden, dass Ihnen ein Unternehmenszertifikat vorab zugewiesen wurde.
2. Klicken Sie auf **Abrufen**.

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

Informationen zum Installieren des Zertifikats finden Sie unter [„Einrichten eines Privacy Manager-Zertifikats“ auf Seite 63](#).

Einrichten eines Privacy Manager-Zertifikats

1. Wenn Sie die E-Mail mit Ihrem Privacy Manager-Zertifikat erhalten haben, öffnen Sie sie, und klicken Sie auf die Schaltfläche **Setup**. Diese befindet sich in Outlook 2007 bzw. Outlook 2010 unten rechts und in Outlook 2003 oben links in der Nachricht.
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 Sicherungsdatei 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 Einladungsvorgang für vertrauenswürdige Kontakte starten möchten, folgen Sie den Anleitungen auf dem Bildschirm beginnend mit Schritt 2 unter [„Hinzufügen von vertrauenswürdigen Kontakten unter Verwendung der Microsoft Outlook-Kontakte“ auf Seite 68](#).

– oder –

Wenn Sie auf **Abbrechen** klicken, finden Sie unter [„Verwalten vertrauenswürdiger Kontakte“ auf Seite 67](#) Informationen darüber, wie Sie zu einem späteren Zeitpunkt einen vertrauenswürdigen Kontakt hinzufügen können.

Importieren eines Zertifikats von einem anderen Anbieter

Sie können das Zertifikat eines anderen Anbieters möglicherweise mithilfe des Assistenten zum Importieren eines Zertifikats in Privacy Manager importieren.

Damit Sie diese Funktion nutzen können, muss auf der Seite „Einstellungen“ unter **Privacy Manager** in HP ProtectTools Administrator-Konsole die Einstellung **Verwendung von Zertifikaten anderer Anbieter zulassen** aktiviert sein.

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Wählen Sie die Registerkarte **Certificate Manager** aus, und klicken Sie dann auf **Zertifikate importieren**.

Diese Schaltfläche wird nicht angezeigt, wenn das Importieren von Zertifikaten nicht zulässig ist.

3. Wählen Sie ein bereits auf dem Computer installiertes Zertifikat oder eine PFX-Datei (Datei für den privaten Informationsaustausch/PKCS#12) für den Import aus, und klicken Sie danach auf **Weiter**.
 - Um ein bereits auf dem Computer installiertes Zertifikat zu importieren, wählen Sie das gewünschte Zertifikat aus, und klicken Sie danach auf **Weiter**.
 - Zum Auswählen eines PFX-Zertifikats klicken Sie auf **Durchsuchen**, navigieren Sie zu dem Speicherort der PFX-Datei, und klicken Sie dann auf **Weiter**. Geben Sie das Passwort für die PFX-Datei ein, und klicken Sie anschließend auf **Weiter**.
4. Nach Abschluss des Importvorgangs klicken Sie auf **Weiter**.
5. Sie haben die Möglichkeit, das importierte Zertifikat zu sichern.

Es wird empfohlen, das Zertifikat an einem anderen Speicherort als auf der Festplatte Ihres Computers zu sichern.

Anzeigen der Details eines Privacy Manager-Zertifikats

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf ein Privacy Manager-Zertifikat.
3. Klicken Sie auf **Zertifikatdetails**.
4. Wenn Sie die Details gelesen haben, klicken Sie auf **OK**.

Erneuern eines Privacy Manager-Zertifikats

Sie werden vor Ablauf Ihres Privacy Manager-Zertifikats daran erinnert, dass Sie das Zertifikat erneuern müssen:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf **Zertifikat erneuern**.
3. Folgen Sie den Anleitungen auf dem Bildschirm, um ein neues Privacy Manager-Zertifikat zu erhalten.



HINWEIS: Durch die Erneuerung Ihres Privacy Manager-Zertifikats wird Ihr altes Privacy Manager-Zertifikat nicht ersetzt. Sie müssen ein neues Privacy Manager-Zertifikat anfordern und dann die gleichen Schritte wie unter [„Anfordern eines Privacy Manager-Zertifikats“ auf Seite 62](#) beschrieben ausführen.

Bei Unternehmenszertifikaten, die von Ihrem Unternehmen mithilfe von Microsoft Certificate Authority ausgestellt wurden, muss der CA-Administrator Ihr Zertifikat mit demselben privaten Schlüssel erneuern, der auch für das ursprüngliche Zertifikat verwendet wurde. Er kann aber auch ein neues Zertifikat unter Verwendung desselben privaten Schlüssels ausstellen.

Festlegen eines Privacy Manager-Standardzertifikats

In Privacy Manager werden nur Privacy Manager-Zertifikate angezeigt, selbst dann, wenn zusätzliche Zertifikate von anderen Zertifizierungsstellen auf Ihrem Computer installiert sind.

Wenn Sie mehr als ein Privacy Manager-Zertifikat auf Ihrem Computer über Privacy Manager installiert haben, können Sie eines davon wie folgt als Standardzertifikat festlegen:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf das Privacy Manager-Zertifikat, das Sie als Standardzertifikat festlegen möchten, und klicken Sie dann auf **Als Standard festlegen**.
3. Klicken Sie auf **OK**.



HINWEIS: Sie müssen das Privacy Manager-Zertifikat nicht nutzen. Bei den verschiedenen Privacy Manager-Funktionen können Sie jeweils das von Ihnen gewünschte Privacy Manager-Zertifikat auswählen.

Löschen eines Privacy Manager-Zertifikats

Wenn Sie ein Privacy Manager-Zertifikat löschen, können Sie keine Dateien mehr öffnen oder Daten anzeigen, die Sie mit diesem Zertifikat verschlüsselt haben. Wenn Sie ein Privacy Manager-Zertifikat unbeabsichtigt gelöscht haben, können Sie es mithilfe der Sicherungsdatei wiederherstellen, die Sie beim Installieren des Zertifikats erstellt haben. Weitere Informationen finden Sie unter [„Wiederherstellen eines Privacy Manager-Zertifikats“ auf Seite 66](#).

So löschen Sie ein Privacy Manager-Zertifikat:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf das Privacy Manager-Zertifikat, das sie löschen möchten, und klicken Sie anschließend auf **Erweitert**.
3. Klicken Sie auf **Löschen**.
4. Klicken Sie im Bestätigungsdiaologfeld auf **Ja**.
5. Klicken Sie auf **Schließen** und dann auf **Übernehmen**.

Wiederherstellen eines Privacy Manager-Zertifikats

Bei der Installation des Privacy Manager-Zertifikats müssen Sie eine Sicherungskopie des Zertifikats erstellen. Sie können auch von der Migrationsseite aus eine Sicherungskopie erstellen. Diese Sicherungskopie kann verwendet werden, wenn Sie die Anwendung auf einen anderen Computer migrieren oder ein Zertifikat auf demselben Computer wiederherstellen.

1. Öffnen Sie 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 Datei mit der Erweiterung DPPSM zu suchen, die Sie während des Sicherungsprozesses erstellt haben, und klicken Sie auf **Weiter**.
4. Geben Sie das Kennwort ein, das Sie beim Erstellen der Sicherungsdatei verwendet haben, und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Fertig stellen**.

Weitere Informationen finden Sie unter [„Einrichten eines Privacy Manager-Zertifikats“ auf Seite 63](#) oder [„Sichern von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten“ auf Seite 77](#).

Widerrufen eines Privacy Manager-Zertifikats

Wenn Sie vermuten, dass die Sicherheit Ihres Privacy Manager-Zertifikats nicht mehr gegeben ist, können Sie Ihr eigenes Zertifikat widerrufen.



HINWEIS: Ein widerrufenes Privacy Manager-Zertifikat wird nicht gelöscht. Mithilfe des Zertifikats können auch nach dem Widerruf verschlüsselte Dateien angezeigt werden.

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf das Privacy Manager-Zertifikat, das Sie widerrufen möchten, und klicken Sie anschließend auf **Widerrufen**.
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
5. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
6. Folgen Sie den Anleitungen auf dem Bildschirm.

Verwalten vertrauenswürdiger Kontakte

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

Mit dem Trusted Contacts Manager können Sie folgende Aufgaben ausführen:

- Anzeigen von Details zu vertrauenswürdigen Kontakten
- Löschen von vertrauenswürdigen Kontakten
- Prüfen des Widerruf-Status für vertrauenswürdige Kontakte (erweitert)

Hinzufügen von vertrauenswürdigen Kontakten

Das Hinzufügen von vertrauenswürdigen Kontakten erfolgt in drei Schritten:

1. Sie senden per E-Mail eine Einladung an vertrauenswürdige Kontakte an einen gewünschten Empfänger.
2. Der Empfänger der Einladung antwortet auf die E-Mail.
3. Sie erhalten von diesem Empfänger eine Antwort per E-Mail. Klicken Sie auf **Akzeptieren**.

Sie können Einladungen an vertrauenswürdige Kontakte per E-Mail an verschiedene Empfänger senden, oder Sie können die Einladungen an alle Kontakte in Ihrem Microsoft Outlook-Adressbuch senden.

Nachstehend erfahren Sie, wie Sie vertrauenswürdige Kontakte hinzufügen.



HINWEIS: Die Empfänger einer Einladung an vertrauenswürdige Kontakte müssen auf ihrem Computer Private Manager oder den entsprechenden Client installiert haben, um auf Ihre Einladung zu antworten und zu einem vertrauenswürdigen Kontakt zu werden. Weitere Informationen für die Installation dieses Clients finden Sie auf der DigitalPersona-Website unter <http://digitalpersona.com/privacymanager/download>.

Hinzufügen eines vertrauenswürdigen Kontakts

1. Öffnen Sie **Privacy Manager**, klicken Sie auf **Trusted Contacts Manager** 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 **Einladung an vertrauenswürdige Kontakte**, 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 vertrauenswürdige Kontakte hinzufügen möchten.
5. Bearbeiten Sie den Text, und unterschreiben Sie mit Ihrem Namen (optional).
6. Klicken Sie auf **Senden**.



HINWEIS: Wenn Sie noch kein Privacy Manager-Zertifikat erworben haben, wird eine Benachrichtigung angezeigt, dass Sie ein Privacy Manager-Zertifikat benötigen, um eine Anfrage bezüglich eines vertrauenswürdigen Kontakts zu senden. Klicken Sie auf **OK**, um den Assistenten zum Anfordern eines Zertifikats zu starten. Weitere Informationen finden Sie unter [„Anfordern eines Privacy Manager-Zertifikats“ auf Seite 62](#).

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



HINWEIS: Nach Erhalt muss der Empfänger der Anfrage die E-Mail öffnen und unten rechts in der E-Mail auf **Akzeptieren** und in dem daraufhin angezeigten Bestätigungsdialogfeld auf **OK** klicken.

8. Wenn Sie eine E-Mail-Antwort von einem Empfänger erhalten, der die Einladung, ein vertrauenswürdiger Kontakt 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 Liste vertrauenswürdiger Kontakte hinzugefügt wurde.

9. Klicken Sie auf **OK**.

Hinzufügen von vertrauenswürdigen Kontakten unter Verwendung der Microsoft Outlook-Kontakte

1. Öffnen Sie Privacy Manager, klicken Sie auf **Trusted Contacts Manager** 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 „Einladung an vertrauenswürdige Kontakte“ die E-Mail-Adressen der Empfänger aus, die Sie als vertrauenswürdige Kontakte 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 noch kein Privacy Manager-Zertifikat erworben haben, wird eine Benachrichtigung angezeigt, dass Sie ein Privacy Manager-Zertifikat benötigen, um eine Anfrage bezüglich eines vertrauenswürdigen Kontakts zu senden. Klicken Sie auf **OK**, um den Assistenten zum Anfordern eines Zertifikats zu starten. Weitere Informationen finden Sie unter [„Anfordern eines Privacy Manager-Zertifikats“ auf Seite 62](#).

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



HINWEIS: Nach Erhalt muss der Empfänger der Anfrage die E-Mail öffnen und unten rechts in der E-Mail auf **Akzeptieren** und in dem daraufhin angezeigten Bestätigungsdialogfeld auf **OK** klicken.

7. Wenn Sie eine E-Mail-Antwort von einem Empfänger erhalten, der die Einladung, ein vertrauenswürdiger Kontakt 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 Liste der vertrauenswürdigen Kontakte hinzugefügt wurde.

8. Klicken Sie auf **OK**.

Anzeigen von Details zu vertrauenswürdigen Kontakten

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Vertrauenswürdige Kontakte**.
2. Klicken Sie auf einen vertrauenswürdigen Kontakt.
3. Klicken Sie auf **Kontaktdetails**.
4. Klicken Sie auf **OK**, um die Anzeige der Details zu schließen.

Löschen eines vertrauenswürdigen Kontakts

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Vertrauenswürdiger Kontakt**.
2. Klicken Sie auf den vertrauenswürdigen Kontakt, die gelöscht werden soll.
3. Klicken Sie auf **Kontakt löschen**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Prüfen des Widerruf-Status für einen vertrauenswürdigen Kontakt

So stellen Sie fest, ob ein vertrauenswürdiger Kontakt ihr Privacy Manager-Zertifikat widerrufen hat:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Vertrauenswürdiger Kontakt**.
2. Klicken Sie auf einen vertrauenswürdigen Kontakt.
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

Sie können Privacy Manager mit den folgenden Microsoft Produkten verwenden:

- Microsoft Outlook
- Microsoft Office

Verwenden von Privacy Manager in Microsoft Outlook

Nach der Installation von Privacy Manager wird die Schaltfläche „Datenschutz“ auf der Symbolleiste von Microsoft Outlook angezeigt, und die Schaltfläche „Sichern senden“ wird auf der Symbolleiste jeder E-Mail-Nachricht in Microsoft Outlook angezeigt. Wenn Sie neben **Datenschutz** oder **Sicher senden** auf den Pfeil nach unten klicken, können Sie zwischen folgenden Optionen auswählen:

- **Nachricht signieren und senden** (nur für die Schaltfläche „Sicher senden“) – Diese Option fügt Ihrer E-Mail eine digitale Signatur hinzu und versendet sie, sobald die Authentifizierung über die von Ihnen ausgewählte Sicherheits-Anmeldemethode erfolgt ist.
- **Für vertrauenswürdige Kontakte versiegeln und senden** (nur für die Schaltfläche „Sicher senden“) – Diese Option fügt Ihrer E-Mail eine digitale Signatur hinzu, verschlüsselt sie und versendet die E-Mail, sobald die Authentifizierung über die von Ihnen ausgewählte Sicherheits-Anmeldemethode erfolgt ist.
- **Kontakte einladen** – Mit dieser Option können Sie eine Einladung an vertrauenswürdige Kontakte versenden. Weitere Informationen finden Sie unter [„Hinzufügen eines vertrauenswürdigen Kontakts“ auf Seite 68](#).
- **Meine Outlook-Kontakte einladen** – Mit dieser Option können Sie eine Einladung an alle Kontakte in Ihrem Microsoft Outlook-Adressbuch senden. Weitere Informationen finden Sie unter [„Hinzufügen von vertrauenswürdigen Kontakten unter Verwendung der Microsoft Outlook-Kontakte“ auf Seite 68](#).
- **Privacy Manager-Software öffnen** – Mit Zertifikaten, vertrauenswürdigen Kontakten und Einstellungsoptionen können Sie die Privacy Manager-Software öffnen, um aktuelle Einstellungen hinzuzufügen, anzuzeigen oder zu aktualisieren. Weitere Informationen finden Sie unter [„Verwalten von Privacy Manager Zertifikaten“ auf Seite 62](#), [„Verwalten vertrauenswürdiger Kontakte“ auf Seite 67](#) oder [„Konfigurieren von Privacy Manager für Microsoft Outlook“ auf Seite 71](#).

Konfigurieren von Privacy Manager für Microsoft Outlook

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

– ODER –

Klicken Sie in der Hauptsymbolleiste von Microsoft Outlook neben **Sicher senden** (**Datenschutz** in Outlook 2003) 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. Schreiben Sie Ihre E-Mail-Nachricht.
3. Klicken Sie neben **Sicher senden (Datenschutz** in Outlook 2003) auf den Pfeil nach unten und anschließend auf **Signieren und senden**.
4. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Versiegeln und Senden einer E-Mail-Nachricht

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

So versiegeln und senden Sie eine E-Mail-Nachricht an einen vertrauenswürdigen Kontakt:

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 (**Datenschutz** in Outlook 2003) und anschließend auf **Für vertrauenswürdige Kontakte versiegeln und senden**.
4. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Anzeigen einer versiegelten E-Mail-Nachricht

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

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

Verwenden von Privacy Manager in einem Microsoft Office 2007 Dokument

Nach der Installation Ihres Privacy Manager-Zertifikats wird die Schaltfläche „Signieren und verschlüsseln“ rechts in der Symbolleiste aller Microsoft Word-, Microsoft Excel- und Microsoft PowerPoint-Dokumente angezeigt. Wenn Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten klicken, können Sie eine der folgenden Optionen auswählen:

- **Dokument signieren** – Mithilfe dieser Option können Sie Ihre digitale Signatur zu dem Dokument hinzufügen.
- **Signaturzeile vor Signieren hinzufügen** (nur für Microsoft Word und Microsoft Excel) – Beim Signieren oder Verschlüsseln eines Microsoft Word- oder Microsoft Excel-Dokuments wird standardmäßig eine Signaturzeile hinzugefügt. Zum Deaktivieren dieser Optionen klicken Sie auf **Signaturzeile hinzufügen**, und entfernen Sie das Häkchen.
- **Dokument verschlüsseln** – Mithilfe dieser Option können Sie Ihre digitale Signatur zu dem Dokument hinzufügen und es verschlüsseln.

- **Verschlüsselung entfernen** – Mithilfe dieser Option entfernen Sie die Verschlüsselung des Dokuments.
- **Privacy Manager-Software öffnen** – Mit Zertifikaten, vertrauenswürdigen Kontakten und Einstellungsoptionen können Sie die Privacy Manager-Software öffnen, um aktuelle Einstellungen hinzuzufügen, anzuzeigen oder zu aktualisieren. Weitere Informationen finden Sie unter [„Verwalten von Privacy Manager Zertifikaten“ auf Seite 62](#), [„Verwalten vertrauenswürdiger Kontakte“ auf Seite 67](#) oder [„Konfigurieren von Privacy Manager für Microsoft Office“ auf Seite 73](#).

Konfigurieren von Privacy Manager für Microsoft Office

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

– ODER –
Klicken Sie in der Symbolleiste eines Microsoft Office-Dokuments neben **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 Bestätigungsdiaologfeld, 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 Bestätigungsdiaologfeld 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 oder speichern Sie ein Dokument in Microsoft Word oder Microsoft Excel.
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“ markiert. 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 eines empfohlenen Signierers zu einem Microsoft Word- oder Microsoft Excel-Dokument

Sie können mehr als eine Signaturzeile zu Ihrem Dokument hinzufügen, indem Sie empfohlene Signierer bestimmen. Bei einem empfohlenen Signierer handelt es sich um einen Benutzer, der von dem Eigentümer eines Microsoft Word- oder Microsoft Excel-Dokuments dazu bestimmt wird, dem Dokument eine Signaturzeile hinzuzufügen. Der empfohlene Signierer können entweder Sie selbst sein oder eine andere Person, die Ihr Dokument für Sie signieren soll. Wenn sie z. B. ein Dokument vorbereiten, das von allen Mitgliedern Ihrer Abteilung signiert werden soll, können Sie Signaturzeilen für diese Benutzer unten auf der letzten Seite des Dokuments mit der Angabe einfügen, bis zu welchem Datum das Dokument signiert werden muss.

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



HINWEIS: Der Eigentümer des Dokuments weist seinem Dokument empfohlene Signierer zu. Die Kontrollkästchen **Signierungsdatum in Signaturzeile anzeigen** und/oder **Titel des Signierers in Signaturzeile anzeigen** müssen aktiviert sein, damit der empfohlene Signierer das Datum und/oder den Titel in der Signaturzeile anzeigen kann.

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 selbst und für Ihre vertrauenswürdigen Kontakte verschlüsseln. Nachdem Sie ein Dokument verschlüsselt und geschlossen haben, muss es von Ihnen und den aus der Liste ausgewählten vertrauenswürdigen Kontakten authentifiziert werden, bevor es erneut geöffnet werden kann.

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 klicken Sie anschließend auf **Dokument verschlüsseln**.

Das Dialogfeld **Vertrauenswürdigen Kontakt auswählen** wird geöffnet.

4. Klicken Sie auf den Namen eines vertrauenswürdigen Kontakts, der in der Lage sein soll, das Dokument zu öffnen und seinen Inhalt anzuzeigen.



HINWEIS: Um mehrere Namen vertrauenswürdiger Kontakte auszuwählen, drücken Sie die Taste **strg**, und klicken Sie anschließend auf die Namen der entsprechenden Personen.

5. Klicken Sie auf **OK**.

Für ein späteres Überarbeiten des Dokuments folgen Sie der Anleitung unter [„Eine Verschlüsselung von einem Microsoft Office-Dokument entfernen“ auf Seite 75](#). Sie können das Dokument überarbeiten, nachdem die Verschlüsselung entfernt wurde. Zur erneuten Verschlüsselung des Dokuments folgen Sie der Anleitung in diesem Abschnitt.

Eine Verschlüsselung von einem Microsoft Office-Dokument entfernen

Wenn Sie die Verschlüsselung für ein Microsoft Office-Dokument entfernen, ist weder für Sie noch für Ihre vertrauenswürdigen Kontakte 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 klicken Sie anschließend auf **Verschlüsselung entfernen**.

Versenden eines verschlüsselten Microsoft Office-Dokuments

Sie können ein verschlüsseltes Microsoft Office-Dokument an eine E-Mail-Nachricht anhängen, ohne dabei die E-Mail selbst zu signieren oder zu verschlüsseln. Sie erstellen und senden eine E-Mail mit einem signierten oder verschlüsselten Dokument als Anhang genau so, wie Sie eine reguläre E-Mail mit Anhang versenden würden.

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 Informationen erhalten Sie unter [„Versiegeln und Senden einer E-Mail-Nachricht“ auf Seite 72](#).

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 wird das Symbol für digitale Signaturen in der Statusleiste unten im Dokumentfenster angezeigt.

1. Klicken Sie auf das Symbol **Digitale Signatur**, um auf die Anzeige des Signatur-Dialogfelds umzuschalten, in dem die Namen aller Benutzer angezeigt werden, die das Dokument signiert haben, sowie das Datum, an dem die einzelnen Signaturen vorgenommen wurden.
2. Weitere Details zu den einzelnen Signaturen werden angezeigt, wenn Sie mit der rechten Maustaste auf einen Namen im Signatur-Dialogfeld klicken und dann **Signaturdetails** auswählen.

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 wiederherstellen, das für die Verschlüsselung der Datei verwendet wurde.

Wenn Ihr Zertifikat verloren gegangen ist, müssen Sie das zur Verschlüsselung der Datei verwendete Privacy Manager-Zertifikat wiederherstellen, um ein verschlüsseltes Microsoft Office-Dokument anzeigen zu können.

Ein vertrauenswürdiger Kontakt, der ein verschlüsseltes Microsoft Office Dokument anzeigen möchte, muss über ein installiertes Privacy Manager Zertifikat sowie über Privacy Manager auf ihrem Computer verfügen. Außerdem muss der vertrauenswürdige Kontakt vom Eigentümer des verschlüsselten Microsoft Office Dokuments ausgewählt worden sein.

Erweiterte Aufgaben

Migrieren von Privacy Manager Zertifikaten und vertrauenswürdigen Kontakten auf einen anderen Computer

Sie können Ihre Privacy Manager-Zertifikate und vertrauenswürdigen Kontakte sicher auf einen anderen Computer migrieren oder Sicherungskopien Ihrer Daten anlegen. Sichern Sie dazu die Privacy Manager-Zertifikate und die vertrauenswürdigen Kontakte als kennwortgeschützte Datei in einen Netzwerkordner oder auf einen Wechseldatenträger, und stellen Sie anschließend die Datei auf dem neuen Computer wieder her.

Sichern von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten

Gehen Sie folgendermaßen vor, um Ihre Privacy Manager-Zertifikate und vertrauenswürdigen Kontakte in einer kennwortgeschützten Datei zu sichern:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Migration**.
2. Klicken Sie auf **Sicherung**.
3. Wählen Sie auf der Seite „Daten auswählen“ die Datenkategorien aus, die in die Migrationsdatei mit aufgenommen 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. Klicken Sie anschließend 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 zum Wiederherstellen der Migrationsdatei benötigen.

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

Wiederherstellen von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten

Gehen Sie folgendermaßen vor, um Ihre Privacy Manager-Zertifikate und vertrauenswürdigen Kontakte als Teil des Migrationsprozesses auf einem anderen Computer oder auf demselben Computer wiederherzustellen:

1. Öffnen Sie 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 Datei zu suchen. Klicken Sie anschließend auf **Weiter**.
4. Geben Sie das Kennwort ein, das Sie beim Erstellen der Sicherungsdatei verwendet haben, und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite „Migrationsdatei“ auf **Beenden**.

Zentrale Verwaltung von Privacy Manager

Bei Ihrer Installation von Privacy Manager kann es sich um einen Teil einer zentralen Installation handeln, die von Ihrem Administrator benutzerdefiniert angepasst wurde. Eine oder mehrere der folgenden Funktionen können entweder aktiviert oder deaktiviert sein:

- **Richtlinien zur Zertifikatsverwendung** – Es kann eine Beschränkung auf die Verwendung von Privacy Manager-Zertifikaten vorliegen, die von Comodo ausgegeben wurden, oder Sie können zur Nutzung digitaler Zertifikate anderer Zertifizierungsstellen berechtigt sein.
- **Verschlüsselungsrichtlinien** – Verschlüsselungsfunktionen können in Microsoft Office oder Outlook individuell aktiviert oder deaktiviert werden.

7 File Sanitizer for HP ProtectTools

Mit File Sanitizer können Sie Datenbestände auf Ihrem Computer (z. B. persönliche Daten oder Dateien, Verlaufsdaten, Internet-bezogene und anderweitige Daten) sicher shreddern und von Zeit zu Zeit die Daten auf Ihrer Festplatte überschreiben.



HINWEIS: Die vorliegende Version von File Sanitizer unterstützt lediglich das Überschreiben der Computerfestplatte.

Shreddern

Das Shreddern von Daten ist nicht mit einem Standard-Löschvorgang unter Windows® gleichzusetzen; dieser Vorgang wird in File Sanitizer als „einfaches Löschen“ bezeichnet. Beim Shreddern von Datenbeständen mit File Sanitizer werden die Dateien mit bedeutungslosen Daten überschrieben. Damit ist quasi ausgeschlossen, dass der ursprüngliche Datenbestand wiederhergestellt werden kann. Bei einem Löschvorgang unter Windows verbleiben die Dateien bzw. Datenbestände dagegen auf der Festplatte oder können anhand datenforensischer Methoden wiedergewonnen werden.

Wenn Sie ein Shred-Profil auswählen (**Hohe Sicherheit**, **Mittlere Sicherheit** oder **Geringe Sicherheit**), wird für das Shreddern automatisch eine voreingestellte Liste von Datenbeständen sowie eine Löschmethode ausgewählt. Sie können ein Shred-Profil auch individuell anpassen. Dabei können Sie die Anzahl der Shred-Zyklen festlegen und angeben, welche Datenbestände geshreddert werden sollen bzw. welche Datenbestände nur nach vorheriger Bestätigung oder überhaupt nicht geshreddert werden sollen. Weitere Informationen finden Sie unter [„Auswählen und Ändern eines Shred-Profiles“ auf Seite 84](#).

Sie können einen automatischen Shred-Zeitplan erstellen oder das Shreddern manuell mithilfe des Symbols **HP ProtectTools** aktivieren, das sich im Infobereich ganz rechts in der Taskleiste befindet. Weitere Informationen finden Sie unter [„Festlegen eines Shred-Zeitplans“ auf Seite 83](#), [„Manuelles Shreddern von Datenbeständen“ auf Seite 88](#) oder [„Manuelles Shreddern aller ausgewählter Elemente“ auf Seite 89](#).



HINWEIS: .dll-Dateien werden nur dann geshreddert und vom System entfernt, wenn sie zuvor in den Papierkorb verschoben wurden.

Überschreiben von freiem Speicherplatz

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.

Beim Überschreiben von freiem Speicherplatz werden gelöschte Datenbestände sicher mit willkürlichen Daten überschrieben, sodass die Originalinhalte nicht mehr angezeigt werden können.



HINWEIS: Das Überschreiben von freiem Speicherplatz kann von Zeit zu Zeit für Datenbestände erfolgen, die Sie mit der File Sanitizer Option **Einstellungen für einfaches Löschen**, durch Verschieben in den Papierkorb oder manuell gelöscht haben. Das Überschreiben von freiem Speicherplatz bietet keine zusätzliche Sicherheit für geshredderte Datenbestände.

Sie können einen Zeitplan für das automatische Überschreiben von freiem Speicherplatz erstellen oder das Überschreiben manuell mithilfe des Symbols **HP ProtectTools** aktivieren, das sich im Infobereich ganz rechts in der Taskleiste befindet. Weitere Informationen finden Sie unter [„Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz“ auf Seite 83](#) oder [„Manuelles Aktivieren des Überschreibens von freiem Speicherplatz“ auf Seite 89](#).

Öffnen von File Sanitizer

1. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Security Manager**.

2. Klicken Sie auf **File Sanitizer**.

– oder –

▲ Doppelklicken Sie auf das **File Sanitizer**-Symbol auf dem Desktop.

– oder –

▲ Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich ganz rechts in der Taskleiste. Klicken Sie auf **File Sanitizer** und anschließend auf **File Sanitizer öffnen**.

Setup-Verfahren

Festlegen eines Shred-Zeitplans

Sie können ein vordefiniertes Shred-Profil auswählen oder Ihr eigenes Profil erstellen. Weitere Informationen finden Sie unter [„Auswählen und Ändern eines Shred-Profiles“ auf Seite 84](#). Datenbestände lassen sich außerdem jederzeit manuell shreddern. Weitere Informationen finden Sie unter [„Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs“ auf Seite 87](#).

 **HINWEIS:** Eingeplante Aufgaben werden zu einem bestimmten Zeitpunkt durchgeführt. Wenn das System zu diesem Zeitpunkt ausgeschaltet ist oder sich im Standby- oder Energiesparmodus befindet, versucht File Sanitizer nicht, die Aufgabe zu einem späteren Zeitpunkt durchzuführen.

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shreddern**.
2. Wählen Sie die gewünschten Shred-Optionen aus:
 - **Beim Herunterfahren von Windows** – Shreddert alle ausgewählten Datenbestände beim Herunterfahren von Windows.

 **HINWEIS:** Beim Herunterfahren wird ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob Sie mit dem Shreddern ausgewählter Datenbestände fortfahren oder den Vorgang übergehen möchten.

Klicken Sie auf **Ja**, um das Shreddern zu übergehen, bzw. auf **Nein**, wenn die Daten geshreddert werden sollen.

 - **Beim Öffnen eines Webbrowsers** – Shreddert beim Öffnen eines Webbrowsers alle Internet-bezogenen Datenbestände, wie beispielsweise das URL-Protokoll des Browsers.
 - **Beim Schließen eines Webbrowsers** – Shreddert beim Schließen eines Webbrowsers alle Internet-bezogenen Datenbestände, wie beispielsweise das URL-Protokoll des Browsers.
 - **Tastenfolge** – Ermöglicht die Definition einer Tastenfolge, die den Shred-Vorgang einleitet. Ausführliche Informationen zu diesem Thema finden Sie unter [„Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs“ auf Seite 87](#).

 **HINWEIS:** .dll-Dateien werden nur dann geshreddert und vom System entfernt, wenn sie zuvor in den Papierkorb verschoben wurden.
3. Wenn Sie ausgewählte Datensätze zu einem späteren Zeitpunkt shreddern möchten, aktivieren Sie das Kontrollkästchen **Planer aktivieren**, geben Ihr Windows Kennwort ein und wählen dann einen Tag und eine Uhrzeit aus.
4. Klicken Sie auf **Übernehmen**.

Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz

Das Überschreiben von freiem Speicherplatz kann von Zeit zu Zeit für Datenbestände erfolgen, die Sie mit der File Sanitizer Option **Einstellungen für einfaches Löschen**, durch Verschieben in den Papierkorb oder manuell gelöscht haben. Das Überschreiben von freiem Speicherplatz bietet keine zusätzliche Sicherheit für geshredderte Datenbestände.

 **HINWEIS:** Eingeplante Aufgaben werden zu einem bestimmten Zeitpunkt durchgeführt. Wenn das System zu diesem Zeitpunkt ausgeschaltet ist oder sich im Standby- oder Energiesparmodus befindet, versucht File Sanitizer nicht, die Aufgabe zu einem späteren Zeitpunkt durchzuführen.

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Überschreiben**.
2. Wenn Sie gelöschte Bestände auf Ihrer Festplatte zu einem späteren Zeitpunkt überschreiben möchten, aktivieren Sie das Kontrollkästchen **Planer aktivieren**, geben Ihr Windows Kennwort ein und wählen dann einen Tag und eine Uhrzeit aus.
3. Klicken Sie auf **Übernehmen**.

 **HINWEIS:** Das Überschreiben von freiem Speicherplatz kann einige Zeit in Anspruch nehmen. Obwohl der Vorgang im Hintergrund ausgeführt wird, kann die Computerleistung durch die zusätzliche Prozessorbeltung beeinträchtigt werden.

Auswählen und Ändern eines Shred-Profiles

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

Auswählen eines vordefinierten Shred-Profiles

Wenn Sie ein vordefiniertes Shred-Profil auswählen, werden automatisch eine vordefinierte Löschmethode und eine Liste von Datenbeständen ausgewählt. Sie können die vordefinierte Liste der für das Shreddern vorgesehenen Datenbestände anzeigen lassen.

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Einstellungen**.
2. Klicken Sie auf ein vordefiniertes Shred-Profil:
 - **Hohe Sicherheit**
 - **Mittlere Sicherheit**
 - **Geringe Sicherheit**
3. Zur Anzeige der für das Shreddern vorgesehenen Datenbestände klicken Sie auf **Details anzeigen**.
 - a. **Ausgewählte Elemente werden geshreddert, und eine Bestätigungsmeldung wird angezeigt. Nicht ausgewählte Elemente werden geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.** – Wählen Sie das Kontrollkästchen aus, um eine Bestätigungsmeldung anzuzeigen, bevor das Element geshreddert wird. Wenn Sie das Kontrollkästchen nicht auswählen, wird das Element geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.

 **HINWEIS:** Auch wenn das Kontrollkästchen für ein Element nicht angekreuzt ist, wird das Element geshreddert.

- b. Klicken Sie auf **Übernehmen**.
4. Klicken Sie auf **Übernehmen**.

Anpassen eines Shred-Profiles

Beim Erstellen eines Shred-Profiles können Sie die folgenden Informationen angeben: Anzahl der Shred-Zyklen, welche Datenbestände in den Shred-Vorgang einbezogen werden sollen, für welche

Datenbestände das Shreddern vor dem Ausführen des Befehls bestätigt werden soll und welche Datenbestände vom Shred-Prozess ausgeschlossen werden sollen.

1. Öffnen Sie File Sanitizer, klicken Sie auf **Einstellungen, Einstellungen für erhöhte Sicherheit** und anschließend auf **Details anzeigen**.
2. Wählen Sie die Anzahl der Shred-Zyklen aus.



HINWEIS: Der ausgewählte Wert legt fest, wie häufig der Shred-Zyklus auf die einzelnen Datenbestände angewendet wird. So wird der Shred-Algorithmus bei Auswahl von „3“ insgesamt drei Mal ausgeführt. Wenn Sie sich für eine höhere Sicherheit mit häufigeren Shred-Zyklen entscheiden, kann der Shred-Vorgang erheblich länger dauern. Allerdings wird es mit steigender Anzahl der Shred-Zyklen immer schwieriger, die Daten wiederherzustellen, so dass die Sicherheit zunimmt.

3. So wählen Sie die zu shreddernden Datenbestände aus:
 - 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**. Suchen Sie dann den Pfad zu der Datei oder dem Ordner, oder tippen Sie ihn ein.
 - c. Klicken Sie auf **Öffnen** und dann auf **OK**.
 - d. Klicken Sie unter **Verfügbare Shred-Optionen** auf einen Datenbestand und anschließend auf **Hinzufügen**.

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

4. **Ausgewählte Elemente werden geshreddert, und eine Bestätigungsmeldung wird angezeigt. Nicht ausgewählte Elemente werden geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.** – Wählen Sie das Kontrollkästchen aus, um eine Bestätigungsmeldung anzuzeigen, bevor das Element geshreddert wird. Wenn Sie das Kontrollkästchen nicht auswählen, wird das Element geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.



HINWEIS: Auch wenn das Kontrollkästchen für ein Element nicht angekreuzt ist, wird das Element geshreddert.

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

5. So schließen Sie Dateien und Ordner vom automatischen Shreddern aus:
 - a. Klicken Sie unter **Folgende Elemente nicht shreddern** auf **Hinzufügen**. Suchen Sie dann den Pfad zu der Datei oder dem Ordner, oder tippen Sie ihn ein.
 - b. Klicken Sie auf **Öffnen** und dann auf **OK**.

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

6. Klicken Sie auf **Übernehmen**.

Anpassen eines Profils für das einfache Löschen

Das Profil für einfaches Löschen umfasst das standardmäßige Löschen von Datenbeständen ohne Shreddern der Daten. Sie können ein Profil für das einfache Löschen auch individuell anpassen. Dabei können Sie angeben, welche Datenbestände gelöscht werden sollen, für welche Datensätze vor dem Löschen eine Bestätigung notwendig ist, und welche Datensätze nicht gelöscht werden sollen.



HINWEIS: Mit der Option **Einstellungen für einfaches Löschen** können Sie das Bereinigen der Festplatte von Zeit zu Zeit für Datenbestände durchführen, die Sie über den Windows Papierkorb oder manuell gelöscht haben.

1. Öffnen Sie File Sanitizer, klicken Sie auf **Einstellungen, Einstellungen für einfaches Löschen** und anschließend 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**. Suchen Sie dann den Pfad zu der Datei oder dem Ordner, oder tippen Sie ihn ein. Klicken Sie abschließend auf **OK**.
 - c. Klicken Sie auf den benutzerdefinierten Datenbestand und anschließend auf **Hinzufügen**.

Zum Entfernen eines Datenbestands aus den verfügbaren Löschoptionen klicken Sie auf den betreffenden Datenbestand und dann auf **Löschen**.

3. **Ausgewählte Elemente werden geshreddert, und eine Bestätigungsmeldung wird angezeigt. Nicht ausgewählte Elemente werden geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.** – Wählen Sie das Kontrollkästchen aus, um eine Bestätigungsmeldung anzuzeigen, bevor das Element geshreddert wird. Wenn Sie das Kontrollkästchen nicht auswählen, wird das Element geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.



HINWEIS: Auch wenn das Kontrollkästchen für ein Element nicht angekreuzt ist, wird das Element geshreddert.

Zum Entfernen eines Datenbestands aus der Liste der zu löschenden Datenbestände klicken Sie auf den betreffenden Datenbestand und anschließend auf **Entfernen**.

4. So schließen Sie Datenbestände vom automatischen Löschen aus:
 - a. Klicken Sie unter **Folgende Elemente nicht löschen** auf **Hinzufügen**. Suchen Sie dann den Pfad zu der Datei oder dem Ordner, oder tippen Sie ihn ein.
 - b. Klicken Sie auf **Öffnen** und dann auf **OK**.

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

5. Klicken Sie auf **Übernehmen**.

Allgemeine Aufgaben

Sie können mit File Sanitizer die folgenden Aufgaben ausführen:

- Einleiten des Shred-Vorgangs über eine Tastenfolge – Mit dieser Funktion können Sie eine Tastenfolge (z. B. **strg+alt+s**) zum Einleiten des Shred-Vorgangs festlegen. Nähere Informationen zu diesem Thema finden Sie unter [„Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs“ auf Seite 87](#).
- Einleiten des Shred-Vorgangs über das Symbol „File Sanitizer“ – Diese Funktion ist vergleichbar mit der Funktion Ziehen und Ablegen unter Windows. Nähere Informationen zu diesem Thema finden Sie unter [„Verwenden des File Sanitizer-Symbols“ auf Seite 88](#).
- Manuelles Shreddern eines bestimmten Datenbestands oder aller ausgewählten Datenbestände – Diese Funktionen ermöglichen das manuelle Shreddern außerhalb des Shred-Zeitplans. Nähere Informationen zu diesem Thema finden Sie unter [„Manuelles Shreddern von Datenbeständen“ auf Seite 88](#) oder [„Manuelles Shreddern aller ausgewählter Elemente“ auf Seite 89](#).
- Manuelles Aktivieren des Überschreibens von freiem Speicherplatz – Mithilfe dieser Funktion können Sie das Überschreiben von freiem Speicherplatz auf der Festplatte manuell aktivieren. Nähere Informationen zu diesem Thema finden Sie unter [„Manuelles Aktivieren des Überschreibens von freiem Speicherplatz“ auf Seite 89](#).
- Abbrechen eines Shred-Vorgangs oder einer Überschreibung von freiem Speicherplatz – Über diese Funktion haben Sie die Möglichkeit, den aktuellen Shred-Vorgang oder das Überschreiben von freiem Speicherplatz auf der Festplatte abzubrechen. Nähere Informationen zu diesem Thema finden Sie unter [„Abbrechen eines Shred- oder Überschreibungsvorgangs“ auf Seite 89](#).
- Anzeigen der Protokolldateien – Mit dieser Funktion zeigen Sie die Protokolldateien für Shred-Vorgänge und Überschreibungsvorgänge von freiem Speicherplatz an, die sämtliche Fehler für den letzten Shred-Vorgang bzw. die letzte Überschreibung von freiem Speicherplatz enthalten. Nähere Informationen zu diesem Thema finden Sie unter [„Anzeigen der Protokolldateien“ auf Seite 89](#).



HINWEIS: Der Shred-Vorgang oder die Überschreibung von freiem Speicherplatz kann viel Zeit in Anspruch nehmen. Auch wenn das Shreddern und das Überschreiben im Hintergrund stattfinden, wird die Verarbeitungsleistung Ihres Computers unter Umständen durch die erhöhte Prozessorbeanspruchung beeinträchtigt.

Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shreddern**.
2. Aktivieren Sie das Kontrollkästchen **Tastenfolge**.
3. Geben Sie ein Zeichen in das entsprechende Feld ein.
4. Markieren Sie das Kontrollkästchen **STRG** oder **ALT**, und markieren Sie dann die Option **UMSCHALTTASTE**.

Um zum Beispiel das automatische Shreddern mit der Tastenfolge **s** und **strg+Umschalttaste** auszulösen, geben Sie in das dafür vorgesehene Feld den Buchstaben **s** ein und markieren die Kontrollkästchen **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 **umschalttaste** und entweder die Taste **strg** oder **alt** (oder eine andere festgelegte Kombination) gedrückt, während Sie die Taste für das ausgewählte Zeichen drücken.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdiaologfeld auf **Ja**.

Verwenden des File Sanitizer-Symbols

 **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 **File Sanitizer**-Symbol auf dem Desktop.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdiaologfeld auf **Ja**.

Manuelles Shreddern von Datenbeständen

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

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **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: Bei dem von Ihnen ausgewählten Datenbestand kann es sich um eine einzelne Datei oder einen einzelnen Ordner handeln.

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

– ODER –

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

– ODER –

1. Öffnen Sie File Sanitizer, und klicken Sie 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 Bestätigungsdiaologfeld auf **Ja**.

Manuelles Shreddern aller ausgewählter Elemente

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

– ODER –

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shreddern**.
2. Klicken Sie auf die Schaltfläche **Jetzt shreddern**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Aktivieren des Überschreibens von freiem Speicherplatz

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

– ODER –

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Festplattenbereinigung**.
2. Klicken Sie auf **Jetzt überschreiben**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Abbrechen eines Shred- oder Überschreibungsvorgangs

Während eines Shred- oder Überschreibungsvorgangs wird über dem Symbol von HP ProtectTools Security Manager im Infobereich ganz rechts in der Taskleiste eine entsprechende Meldung angezeigt. Sie enthält Details zum laufenden Vorgang (Prozentsatz der Fertigstellung) sowie eine Option zum Abbrechen des Shred-/Überschreibungsvorgangs.

- ▲ Zum Abbrechen des Vorgangs klicken Sie auf die Meldung und anschließend auf **Stopp**.

Anzeigen der Protokolldateien

Für jeden Shred-Vorgang und jedes Überschreiben von freiem Speicherplatz 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 Überschreibung bezieht.



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

Das System erzeugt eine Protokolldatei für Shred- und eine für Überschreibungsvorgänge. Beide Protokolldateien befinden sich auf der Festplatte in folgenden Verzeichnissen:

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

Bei 64-Bit-Systemen sind die Protokolldateien auf der Festplatte in diesen Verzeichnissen abgelegt:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer\[Benutzername]_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer\[Benutzername]_DiskBleachLog.txt

8 Device Access Manager for HP ProtectTools (bestimmte Modelle)

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



HINWEIS: Einige Schnittstellen/Eingabegeräte für die Benutzerinteraktion, wie Maus, Tastatur, TouchPad und Fingerabdruck-Lesegeräte, können nicht über Device Access Manager gesteuert werden. Weitere Informationen finden Sie unter [„Nicht verwaltete Geräteklassen“ auf Seite 102](#).

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

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

Öffnen von Device Access Manager

1. Melden Sie sich als Administrator an.
2. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
3. Klicken Sie im linken Fensterausschnitt auf **Device Access Manager**.

Benutzer mit eingeschränkten Rechten können die HP ProtectTools Device Access Manager Richtlinie mit HP ProtectTools Security Manager anzeigen. Mit dieser Konsole ist nur eine schreibgeschützte Ansicht möglich.

Setup-Verfahren

Konfigurieren von Zugriffrechten auf Geräte

In HP ProtectTools Device Access Manager sind vier Ansichten verfügbar:

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

Einfache Konfiguration

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

- Alle Wechselmedien (Disketten, USB-Flash-Laufwerke usw.)
- Alle DVD-/CD-ROM-Laufwerke
- Alle seriellen und parallelen Anschlüsse
- Alle Bluetooth®-Geräte
- Alle Modems
- Alle PCMCIA-/ExpressCard-Geräte
- Alle 1394-Geräte

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

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

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

3. Klicken Sie auf **Übernehmen**.



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

4. Klicken Sie auf **OK**.

Starten des Hintergrunddienstes

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



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

Administratoren können diesen Dienst auch starten oder stoppen:

1. Klicken Sie unter Windows 7 auf **Start, Systemsteuerung** und anschließend auf **System und Sicherheit**.

– oder –

Klicken Sie unter Windows Vista® auf **Start, Systemsteuerung** und anschließend auf **System und Wartung**.

– oder –

Klicken Sie unter Windows XP auf **Start, Systemsteuerung** und anschließend auf **Leistung und Wartung**.

2. Klicken Sie auf **Verwaltung** und dann auf **Dienste**.
3. Wählen Sie den Dienst **HP ProtectTools Gerätesperre/Überwachung**.
4. Klicken Sie zum Starten des Diensts auf **Start**.

– oder –

Klicken Sie zum Stoppen des ausgeführten Diensts auf **Stopp**.

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

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

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

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

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

Geräteklassen-Konfiguration

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

Zugriff für Benutzer oder Gruppe verweigern

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

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

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

Zugriff für Benutzer oder Gruppe erteilen

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

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

Das Dialogfeld **Benutzer oder Gruppen auswählen** wird geöffnet.

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

Einem Benutzer einer Gruppe Zugriff auf eine Geräteklasse erteilen

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

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

Einem Benutzer einer Gruppe Zugriff auf ein bestimmtes Gerät erteilen

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

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

Das Dialogfeld **Benutzer oder Gruppen auswählen** wird geöffnet.

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

Entfernen von Einstellungen für einen Benutzer oder eine Gruppe

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

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

Zurücksetzen der Konfiguration

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

So setzen Sie die Konfigurationseinstellungen auf die Werkseinstellungen zurück:

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

JITA-Konfiguration

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

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

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

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

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

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

JITA ist für die folgenden Geräteklassen verfügbar:

- DVD-/CD-ROM-Laufwerke
- Wechselmedien

Erstellen einer JITA für einen Benutzer oder eine Gruppe

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

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

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

Erstellen einer verlängerbaren JITA für einen Benutzer oder eine Gruppe

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

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

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

Deaktivieren einer JITA für einen Benutzer oder eine Gruppe

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

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

4. Deaktivieren Sie das Kontrollkästchen **Aktiviert**.
5. Klicken Sie auf **Übernehmen**.

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

Erweiterte Einstellungen

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

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

Die Gruppe „Geräte-Administratoren“ wird verwendet, um vertrauenswürdige Benutzer (vertrauenswürdig im Hinblick auf den Gerätezugriff) von den Beschränkungen durch eine Device Access Manager Richtlinie auszunehmen. Systemadministratoren gehören üblicherweise zu den vertrauenswürdigen Benutzern. Weitere Informationen finden Sie unter [„Gruppe „Geräte-Administratoren““ auf Seite 101](#).

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

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

So starten Sie diese Dienste:

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

– oder –

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

```
sc start flcdlock
```

Drücken Sie die [Eingabetaste](#).

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

Die Laufwerksbuchstaben werden für physische Festplatten oder Partitionen angezeigt.

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

Gruppe „Geräte-Administratoren“

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

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



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

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

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

Alternative Methoden zum Verwalten der Mitgliedschaft in dieser Gruppe sind u. a.:

- Unter Windows 7 Professional oder Windows Vista können Benutzer über das Standard-Snap-In von Microsoft Management Console (MMC) „Lokale Benutzer und Gruppen“ zu dieser Gruppe hinzugefügt werden.
- Für die Home-Versionen von Windows 7, Windows Vista oder Windows XP geben Sie den folgenden Befehl über ein Administratorkonto in ein Eingabeaufforderungsfenster ein:

```
net localgroup "Geräte-Administratoren" benutzername /Add
```

In diesem Befehl ist „benutzername“ der Benutzername des Benutzers, der zu dieser Gruppe hinzugefügt werden soll.

eSATA-Support

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

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

Nicht verwaltete Geräteklassen

HP ProtectTools Device Access Manager verwaltet die folgenden Geräteklassen nicht:

- Eingabe-/Ausgabegeräte
 - Biometrisches Gerät
 - Maus
 - Tastatur
 - Drucker

- Plug-and-Play (PnP)-Drucker
- Drucker-Upgrade
- Infrarot-Schnittstelle für die Benutzerinteraktion
- Lesegerät für Smart Cards
- Serieller Multi-Port
- Datenträgerlaufwerk
- Disketten-Controller (FDC)
- Festplatten-Controller (HDC)
- Schnittstelle für die Benutzerinteraktion (HID)
- Energie
 - Akku
 - Support für erweiterte EnergiEVERWALTUNG (APM)
- Sonstiges
 - Computer
 - Decoder
 - Display
 - Prozessor
 - System
 - Unbekannt
 - Lautstärke
 - Volume-Schnappschuss
 - Sicherheitsgerät
 - Sicherheitsbeschleuniger
 - Vereinheitlichter Anzeigetreiber von Intel®
 - Medientreiber
 - Medienwechselgerät
 - Multifunktionsgerät
 - Legacard
 - Netz-Client
 - Netzdienst

- Netzübertragung
- SCSI-Adapter

9 Wiederbeschaffung gestohlener Geräte

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

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

So aktivieren Sie Computrace for HP ProtectTools:

1. Stellen Sie eine Verbindung zum Internet her.
2. Klicken Sie auf **Start, Alle Programme, HP** und anschließend auf **HP ProtectTools Security Manager**.
3. Klicken Sie auf der linken Seite von Security Manager auf **Theft Recovery** (Wiedererlangen bei Diebstahl).
4. Zum Starten des Computrace Aktivierungsassistenten klicken Sie auf die Schaltfläche **Activate Now** (Jetzt aktivieren).
5. Geben Sie Ihre Kontakt- und Kreditkarteninformationen oder einen bereits gekauften Produktschlüssel ein.

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

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

So melden Sie sich beim Kundencenter an:

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

Im Kundencenter können Sie:

- Ihre Computer überwachen.
- Ihre Remote-Daten schützen.
- Den Diebstahl von Computern melden, die durch Computrace geschützt sind.
- ▲ Klicken Sie auf **Weitere Informationen**, um zusätzliche Informationen über Computrace for HP ProtectTools zu erhalten.

10 Embedded Security for HP ProtectTools (bestimmte Modelle)



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

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

- Enhanced Microsoft® Encryption File System (EFS)-Datei und Ordnerschlüsselung
- 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

Die integrierte TPM-Sicherheitschip aktiviert und unterstützt weitere Sicherheitsfunktionen von HP ProtectTools Security Manager. Zum Beispiel kann Credential Manager for HP ProtectTools den integrierten Chip als Authentifizierungsfaktor verwenden, wenn sich der Benutzer bei Windows anmeldet.

Setup-Verfahren

⚠ ACHTUNG: Um Sicherheitsrisiken zu vermeiden, wird empfohlen, dass der IT-Administrator den integrierten Sicherheitschip sofort initialisiert. Geschieht dies nicht, so kann ein nicht autorisierter Benutzer, ein Computerwurm oder ein Virus die Steuerung des Computers und der Eigentümertasks übernehmen, wie zum Beispiel die Verwendung des Notfall-Wiederherstellungsarchivs und die Konfiguration von Benutzerzugriffseinstellungen.

Befolgen Sie die Schritte in den folgenden Absätzen, um den integrierten Sicherheitschip zu aktivieren und zu initialisieren.

Aktivieren des integrierten Sicherheitschips in Computer Setup

Der integrierte Sicherheitschip muss im Schnell-Initialisierungsassistenten oder mit dem Computer Setup Utility aktiviert werden.

So aktivieren Sie den integrierten 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“ (f10 = ROM-basiertes 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** (Kennwort einrichten) 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 unter **Embedded Security** die Option **Available** (Verfügbar) aus, wenn das Gerät ausgeblendet ist.
6. Wählen Sie **Embedded security device state** (Status des integrierten Sicherheitsgeräts) aus, und ändern Sie die Einstellung auf **Enable** (Aktivieren).
7. Drücken Sie **f10**, um die Änderungen an der Embedded Security-Konfiguration zu akzeptieren.
8. Um Ihre Einstellungen zu speichern und Computer Setup zu verlassen, wählen Sie mit den Pfeiltasten **File** (Datei) und dann **Save Changes and Exit** (Änderungen speichern und beenden) aus und folgen anschließend den Anleitungen auf dem Bildschirm.

Initialisieren des integrierten Sicherheitschips

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 mit der rechten Maustaste auf das Symbol **HP ProtectTools Security Manager** im Infobereich der Taskleiste (rechts außen). Wählen Sie dann **Embedded Security Initialization** (Initialisierung von Embedded Security) aus.

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

2. Folgen Sie den Anleitungen auf dem Bildschirm.

Einrichten eines einfachen Benutzerkontos

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 Initialisierungsassistent von Embedded Security nicht geöffnet ist, 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 **Benutzereinstellungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Embedded Security Features** (Embedded Security-Funktionen) auf **Konfigurieren**.

Der Assistent für die Benutzerinitialisierung der Embedded Security wird geöffnet.

4. Folgen Sie den Anleitungen auf dem Bildschirm.

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

Verwenden des persönlichen, sicheren Laufwerks

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

Verschlüsseln von Dateien und Ordnern

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

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

So verschlüsseln Sie Dateien und Ordner:

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

Senden und Empfangen verschlüsselter E-Mails

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

Ändern des Kennworts des einfachen Benutzerschlüssels

So ändern Sie das Kennwort des einfachen Benutzerschlüssels:

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 **Benutzereinstellungen**.
3. Klicken Sie im rechten Fensterbereich unter **Basic User password** (Kennwort des einfachen Benutzerschlüssels) auf **Ändern**.
4. Geben Sie zuerst das alte Kennwort ein. Geben Sie dann das neue Kennwort ein, und bestätigen Sie das neue Kennwort.
5. Klicken Sie auf **OK**.

Erweiterte Tasks

Administratoren können in Embedded Security die folgenden Aufgaben ausführen:

- Anmeldeinformationen, Embedded Security-Einstellungen und PSDs (Personal Secure Drives, Persönliche sichere Laufwerke) sichern und wiederherstellen
- Kennwort des Eigentümers ändern
- Benutzerkennwort zurücksetzen
- Sicherheitsanmeldeinformationen des Benutzers auf sichere Weise von einer Quellplattform auf eine Zielplattform migrieren

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 Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Fensterbereich auf **Konfigurieren**. HP Embedded Security for 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 Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Fensterbereich auf **Alle wiederherstellen**. HP Embedded Security for ProtectTools wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Ändern des Eigentümerkennworts

Administratoren können das Kennwort des Eigentümers ändern:

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

Erneutes Einrichten eines Benutzerkennworts

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

Migrieren von Schlüsseln mithilfe des Migrationsassistenten

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

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

11 Ausnahmen für lokalisierte Kennwörter

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

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

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

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

Bei manchen japanischen Installationen von Windows XP heißt der Standard-IME für Japanisch beispielsweise Microsoft IME Standard 2002. Dies entspricht dem Tastaturlayout E0010411. Hier handelt es sich jedoch um einen IME und nicht ein Tastaturlayout. (Das Tastaturlayout-Kodierungsschema wird von Microsoft nur für IMEs verwendet, die das Konzept eines Tastaturlayouts erweitern). Da es sich hier nicht um ein Tastaturlayout handelt, das in der Eingabeumgebung der Kennwort-Eingabeaufforderung für BIOS Pre-Boot Security oder HP Drive Encryption dargestellt werden kann, werden alle mit diesem IME eingegebenen Kennwörter von HP ProtectTools abgelehnt. Microsoft IME Standard 2002 für Japanisch unterscheidet sich auch von dem „gemeinsamen Namen“ in Microsoft Windows Vista®. Windows weist einige IMEs einem Tastaturlayout zu. In solchen Fällen unterstützt HP ProtectTools den IME, da die zugrunde liegende Tastaturlayoutdefinition (der Hexadezimalcode) verwendet wird.

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

- Microsoft IME für Japanisch
- Das japanische Tastaturlayout
- Office 2007 IME für Japanisch – Wenn Microsoft oder ein Dritter den Begriff IME oder Input Method Editor verwendet, handelt es sich bei der Eingabemethode nicht unbedingt um einen IME. Dies kann zu Verwirrung führen, aber die Software liest die Darstellung des Hexadezimalcodes. Aus diesem Grund kann HP ProtectTools die Konfiguration unterstützen, wenn ein IME einem unterstützten Tastaturlayout zugeordnet ist.

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

Ändern des Kennworts mit einem Tastaturlayout, das ebenfalls unterstützt wird

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



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

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

Behandeln von Sonderzeichen

- Chinesisch, Slowakisch, kanadisches Französisch und Tschechisch

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

- Koreanisch

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

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

Sprache	Windows	BIOS	Drive Encryption
Arabisch	Die Tasten ٱ, ٲ und ٳ erzeugen zwei Zeichen.	Die Tasten ٱ, ٲ und ٳ erzeugen ein Zeichen.	Die Tasten ٱ, ٲ und ٳ erzeugen ein Zeichen.
Französisch (Kanada)	ç, è, à und é mit Feststelltaste entsprechen Ç, Ê, Â und É in Windows.	ç, è, à und é mit Feststelltaste entsprechen ç, è, à und é in der BIOS Pre-Boot Security.	ç, è, à und é mit Feststelltaste entsprechen ç, è, à und é in HP Drive Encryption.
Spanisch	40a wird zwar nicht unterstützt, funktioniert aber trotzdem, da es von der Software zu c0a konvertiert wird. Aufgrund geringfügiger Unterschiede zwischen den Tastaturlayouts wird jedoch empfohlen, dass Spanisch sprechende Benutzer zum Tastaturlayout 1040a (spanische Variation) oder 080a (lateinamerikanisches Spanisch) wechseln.	N/V	N/V
US-International	<ul style="list-style-type: none"> ◦ Die Tasten j, ñ, ' , ' , ¥ und × in der oberen Reihe werden abgelehnt. ◦ Die Tasten â, @ und Þ in der zweiten Reihe werden abgelehnt. ◦ Die Tasten á, ð und ø in der dritten Reihe werden abgelehnt. ◦ Die Taste æ in der unteren Reihe wird abgelehnt. 	N/V	N/V

Sprache	Windows	BIOS	Drive Encryption
Tschechisch	<ul style="list-style-type: none"> ◦ Die Taste ě wird abgelehnt. ◦ Die Taste ě wird abgelehnt. ◦ Die Taste ů wird abgelehnt. ◦ Die Tasten é, í und ž werden abgelehnt. ◦ Die Tasten ě, ě, ě, ě und ř werden abgelehnt. 	N/V	N/V
Slowakisch	Die Taste ž wird abgelehnt.	<ul style="list-style-type: none"> ◦ Die Tasten š, š und š werden abgelehnt, wenn sie über die Tastatur eingegeben werden, jedoch bei Eingabe über die Bildschirmtastatur angenommen. ◦ Die unbelegte Taste ť erzeugt zwei Zeichen. 	N/V
Ungarisch	Die Taste ž wird abgelehnt.	Die Taste ť erzeugt zwei Zeichen.	N/V

Sprache	Windows	BIOS	Drive Encryption
Slowenisch	Die Taste žŽ wird in Windows abgelehnt, und die alt-Taste erzeugt im BIOS eine unbelegte Taste.	Die Tasten ú, Ú, ù, Û, š, Š, ś, Ś, š und Š werden im BIOS abgelehnt.	N/V
Japanisch	<p>Nur unter Windows XP wird das Standard-Tastaturlayout für Japanisch (411) voll unterstützt. Für einen IME, normalerweise unter Windows XP als Microsoft Standard IME 2002 dargestellt, wird normalerweise keine Unterstützung geboten. Empirische Tests haben jedoch gezeigt, dass dieser IME und das Tastaturlayout 411 fast identisch sind, wenn einfache Zeichen eingegeben werden. Aus diesem Grund wechselt die Software bei diesem IME zum Tastaturlayout 411, wenn lokalisierte japanische Kennwörter zur Sicherung vom BIOS und HP Drive Encryption verwendet werden.</p> <p>Wenn verfügbar, sollte Microsoft Office 2007 IME verwendet werden. Trotz des IME-Namens handelt es sich hier um das unterstützte Tastaturlayout 411.</p>	N/V	N/V

Vorgehensweise, wenn das Kennwort abgelehnt wird

Kennwörter können aus folgenden Gründen abgelehnt werden:

- Ein Benutzer verwendet einen nicht unterstützten IME. Dies kommt häufig bei Doppelbyte-Sprachen vor (Koreanisch, Japanisch, Chinesisch). So beheben Sie dieses Problem:
 1. Klicken Sie auf **Start**, auf **Systemsteuerung** und anschließend auf **Regions- und Sprachoptionen**.
 2. Klicken Sie auf die Registerkarte **Sprachen**.
 3. Klicken Sie auf die Schaltfläche **Details**.
 4. Klicken Sie auf der Registerkarte **Einstellungen** auf die Schaltfläche **Hinzufügen**, um eine unterstützte Tastatur hinzuzufügen (US-Tastaturen unter dem chinesischen Eingabegebietsschema hinzufügen).
 5. Legen Sie die unterstützte Tastatur als Standard-Eingabegebietsschema fest.
 6. Starten Sie HP ProtectTools neu, und geben Sie dann das Kennwort erneut ein.
- Ein Benutzer verwendet ein nicht unterstütztes Zeichen. So beheben Sie dieses Problem:
 1. Ändern Sie das Windows -Kennwort, sodass es nur unterstützte Zeichen enthält. Die nicht unterstützten Zeichen sind im Abschnitt [„Behandeln von Sonderzeichen“ auf Seite 119](#) aufgeführt.
 2. Führen Sie den Installations-Assistenten für Security Manager erneut aus, und geben Sie dann das neue Windows Kennwort ein.

Glossar

Administrator

Siehe *Windows Administrator*.

Aktivierung

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

Anmeldedaten

Ein Element innerhalb von Security Manager, das aus einem Benutzernamen und einem Kennwort besteht (und eventuell anderen ausgewählten Informationen), die zur Anmeldung bei Websites oder anderen Programmen verwendet werden können.

Anmeldeinformationen

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

ATM

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

Authentifizierung

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

Authentifizierung beim Systemstart

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

Automatisches Shreddern

Geplante Shred-Vorgänge, die der Benutzer in File Sanitizer 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.

Biometrisch

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

Dashboard

Eine zentrale Schnittstelle, über die Sie auf die Merkmale und Einstellungen von HP ProtectTools Security Manager zugreifen und sie verwalten können.

Datenbestand

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

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

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

Drive Encryption

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

Drive Encryption Anmeldebildschirm

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

DriveLock

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

Einfaches Löschen

Das Löschen des Windows Verweises zu einem Datenbestand. Der Inhalt des Datenbestands verbleibt auf der Festplatte, bis die Daten beim Überschreiben von freiem Speicherplatz überschrieben werden.

Einladung an vertrauenswürdige Kontakte

Eine E-Mail-Nachricht, die an eine Person gesendet wird, um sie zu bitten, ein vertrauenswürdiger Kontakt zu werden.

Empfänger einer Einladung an vertrauenswürdige Kontakte

Eine Person, die die Einladung erhält, einer vertrauenswürdiger Kontakt zu 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)

Ein System, das alle Dateien und Unterordner innerhalb des ausgewählten Ordners verschlüsselt.

Entschlüsselung

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

Fingerabdruck

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

Geräteklasse

Alle Geräte eines bestimmten Typs, beispielsweise Laufwerke.

Gerätezugriffsrichtlinie

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

Gruppe

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

Hintergrunddienst

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

HP SpareKey

Eine Wiederherstellungskopie des Drive Encryption-Schlüssels.

ID-Card

Windows Desktop-Minianwendung, mit der Ihr Desktop anhand Ihres Benutzernamens und eines ausgewählten Bildes visuell identifiziert werden kann. Klicken Sie auf die ID-Card, um HP ProtectTools Administrator-Konsole zu öffnen.

Identität

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

JITA

Just-In-Time-Authentifizierung.

Konsole

Eine zentrale Schnittstelle, über die Sie auf die Merkmale und Einstellungen von HP ProtectTools Administrator-Konsole zugreifen und sie verwalten können.

Kryptographie

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

Kryptographiediensteanbieter (Cryptographic Service Provider = CSP)

Ein Dienstanbieter oder eine Bibliothek von Verschlüsselungsalgorithmen, die in einer gut definierten Schnittstelle dazu benutzt werden können, bestimmte Verschlüsselungsfunktionen auszuüben.

Liste der vertrauenswürdigen Kontakte

Eine Liste der vertrauenswürdigen Kontakte.

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 vertrauenswürdigen Kontakten ermöglicht.

Netzwerkkonto

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

Neustart

Der Neustart des Computers.

Notfallwiederherstellungsarchiv

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

PIN

Persönliche Identifikationsnummer.

PKI

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

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

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

SATA-Gerätemodus

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

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 Schaltfläche, die auf der Symbolleiste der Microsoft Office-Anwendungen angezeigt wird. Durch Klicken auf die Schaltfläche können Sie ein Microsoft Office-Dokument signieren, verschlüsseln oder die Verschlüsselung von einem Microsoft Office-Dokument 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.

Sichern

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

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

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

SSO (Single Sign On)

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

Szene

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

Tastensequenz

Eine Kombination aus bestimmten Tasten, die gedrückt wird, um einen automatischen Shred-Vorgang auszulösen, z. B. [strg+alt+s](#).

Token

Siehe *Sicherheits-Anmeldemethode*.

TPM-Sicherheitschip (Trusted Platform Module)

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

TXT

Trusted Execution Technology.

Überschreiben von freiem Speicherplatz

Das sichere Überschreiben gelöschter Datenbestände mit willkürlichen Daten, um den Inhalt der gelöschten Datenbestände unwiderruflich zu vernichten.

USB-Token

Ein Sicherheitsgerät, das identifizierende Informationen über einen Benutzer speichert. Wie eine Smart Card oder ein biometrisches Lesegerät wird es zur Authentifizierung des Benutzers bei einem Computer verwendet.

Verschlüsselung

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

Versiegeln für vertrauenswürdige Kontakte

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 Nachricht

Eine Kommunikationssitzung, während der vertrauenswürdige Nachrichten von einem vertrauenswürdigen Absender an einen vertrauenswürdigen Kontakt gesendet werden.

Vertrauenswürdiger Absender

Ein vertrauenswürdiger Kontakt, der signierte und/oder verschlüsselte E-Mails und Microsoft Office Dokumente versendet.

Vertrauenswürdiger Kontakt

Eine Person, die eine Einladung an vertrauenswürdige Kontakte angenommen hat.

Virtuelles Token

Eine Sicherheitsfunktion, die ähnlich einer Smart Card und einem Lesegerät funktioniert. Das Token wird entweder auf der Festplatte des Computers oder in der Registrierungsdatenbank von Windows gespeichert. Wenn Sie sich mit einem virtuellen Token anmelden, werden Sie nach einer Benutzer-PIN gefragt, um die Authentifizierung abzuschließen.

Widerruf-Kennwort

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

Wiederherstellen

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

Windows Administrator

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

Windows Anmeldesicherheit

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

Windows Benutzerkonto

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

Zertifizierungsstelle (CA)

Ein Service, der Zertifikate ausstellt, die zum Betreiben einer öffentlichen Schlüsselinfrastruktur erforderlich sind.

Index

A

Abbrechen eines Shred- oder
Überschreibungsvorgangs 89

Administrator-Konsole

- Konfigurieren 20
- Verwenden 19

Aktivieren

- Drive Encryption für
selbstverschlüsselnde
Festplatten 52
- Drive Encryption für Standard-
Festplatten 52

Aktivieren des TPM-Chips 108

Aktivieren des Überschreibens von
freiem Speicherplatz 89

Ändern von Kennwörtern mit
verschiedenen Tastaturlayouts
118

Anfordern eines digitalen
Zertifikats 62

Anmeldedaten

- Bearbeiten 35
- Hinzufügen 34
- Kategorien 36
- Menü 36
- Verwalten 37

Anmeldeinformationen

- Festlegen 22

Anmelden am Computer 55

Anpassen

- Profil für einfaches Löschen
86
- Shred-Profil 84

Anwendungen konfigurieren 26

Anzeigen

- Signiertes Microsoft Office-
Dokument 76

- Verschlüsseltes Microsoft
Office-Dokument 76
- Versiegelte E-Mail-Nachricht
72

Anzeigen der Protokolldateien 89

Assistent, HP ProtectTools
Installation 14

Aufgaben, Sicherheit 8

Ausschließen von Datenbeständen
vom automatischen Löschen 86

Ausschließen von Datenbeständen
vom automatischen Shreddern
85

Auswählen

- Datenbestände für das
Shreddern 84
- Shred-Profil 84

Auswählen von Datenbeständen
für die Bestätigung

- Vor dem Löschen 86
- Vor dem Shreddern 85

Authentifizierung 20

B

Behandeln von Sonderzeichen
119

Benutzer

- Entfernen 97
- Zugriff erteilen 95
- Zugriff verweigern 95

Benutzer verwalten 21

C

Computrace 105

Credential Manager 40

D

Dashboard-Einstellungen 30

Daten

- Sichern 49
- Wiederherstellen 49
- Zugriff auf Daten
einschränken 8

Daten sichern 49

Daten wiederherstellen 49

Deaktivieren von Drive
Encryption 54

Device Access Manager for HP
ProtectTools 91

Diebstahl, Schutz 8

Digitales Zertifikat

- Anfordern 62
- Anzeigen von Details 64
- Einrichten 63
- Empfangen 63
- Erneuern 64
- Löschen 66
- Standard festlegen 66
- Widerrufen 67
- Wiederherstellen 66

Drive Encryption for HP
ProtectTools

- Aktivieren 52
- Anmelden, nachdem Drive
Encryption aktiviert wurde
52
- Deaktivieren 52
- Entschlüsseln einzelner
Laufwerke 57
- Sicherung und
Wiederherstellung 58
- Verschlüsseln einzelner
Laufwerke 57
- Verwalten von Drive
Encryption 57

- E**
- Eigentümerkennwort
 - Ändern 114
- Einfache Konfiguration 92
- Einfacher Benutzerschlüssel, Kennwort
 - ändern 112
 - Festlegen 110
- Einfaches Benutzerkonto 110
- Einschränken
 - Zugang zu Geräten 91
 - Zugriff auf sensible Daten 8
- Einstellungen
 - Allgemein, Registerkarte 26
 - Anwendungen 26, 30
 - Erweiterte
 - Benutzereinstellungen 46
 - Hinzufügen 26, 30
 - Symbol 38
- Einstellungen festlegen 48
- E-Mail-Nachricht
 - Anzeigen einer versiegelten Nachricht 72
 - Signieren 72
 - Versiegeln für vertrauenswürdigen Kontakt 72
- Embedded Security for HP ProtectTools
 - Aktivieren des TPM-Chips 108
 - Eigentümerkennwort ändern 114
 - Einfacher Benutzerschlüssel 110
 - Einfaches Benutzerkonto 110
 - Erneutes Einrichten eines Benutzerkennworts 114
 - Initialisieren des Chips 109
 - Kennwort des einfachen Benutzerschlüssels ändern 112
 - Migrieren von Schlüsseln 115
 - Persönliches sicheres Laufwerk 111
 - Setup-Verfahren 108
 - Sicherungsdatei erstellen 113
 - Verschlüsseln von Dateien und Ordnern 111
 - Verschlüsselte E-Mail 111
 - Zertifizierungsdaten wiederherstellen 113
- Empfohlener Signierer
 - Hinzufügen 74
 - Signaturzeile hinzufügen 74
- Entfernen des Zugriffs 97
- Entfernen einer Verschlüsselung von einem Microsoft Office-Dokument 75
- Entschlüsseln von Festplatten 58
- Entschlüsseln von Laufwerken 51
- Erstellen eines Shred-Profiles 84
- Erste Schritte 92
- Erweiterte Einstellungen 101
- Erweiterte Tasks, Embedded Security 113
- eSATA 102
- Excel, Signaturzeile hinzufügen 73
- F**
- Festlegen
 - Shred-Zeitplan 83
 - Zeitplan für das Überschreiben 83
- File Sanitizer for HP ProtectTools
 - Öffnen 82
 - Setup-Verfahren 83
- Fingerabdrücke
 - Einstellungen 23
- Fingerabdrücke registrieren 41
- Funktionen, HP ProtectTools 2
- G**
- Gerät, Zugriff für Benutzer erteilen 97
- Geräteeinstellungen
 - Fingerabdruck 23
 - Gesicht 24
 - SpareKey 22
- Geräteeinstellungen, Smart Card 24, 43
- Geräteklasse, Zugriff für Benutzer erteilen 96
- Geräteklassen, nicht verwaltet 102
- Geräteklassen-Konfiguration 93
- Gesicht
 - Einstellungen 24
- Grundlegende
 - Sicherheitsaufgaben 8
- Gruppe
 - Entfernen 97
 - Zugriff erteilen 95
 - Zugriff verweigern 95
- H**
- Hardwareverschlüsselung 52, 54
- Hintergrunddienst 93
- Hinzufügen
 - Empfohlener Signierer 74
 - Signaturzeile 73
 - Signaturzeile eines empfohlenen Signierers 74
- HP ProtectTools Administrator-Konsole 17
- HP ProtectTools Administrator-Konsole öffnen 18
- HP ProtectTools Funktionen 2
- HP ProtectTools Security Manager 28
- I**
- ID-Card 48
- Importieren, Zertifikat von einem anderen Anbieter 63
- Initialisieren des integrierten Sicherheitschips 109
- Installations-Assistent 14
- J**
- JITA
 - Erstellen einer verlängerbaren JITA für Benutzer oder Gruppe 99
 - Erstellen für Benutzer oder Gruppe 99
 - Für Benutzer oder Gruppe deaktivieren 99
- JITA-Konfiguration 98
- Just-In-Time-Authentifizierungskonfiguration 98
- K**
- Kennwort
 - Ändern 41
 - Ändern für Eigentümer 114

- Eigentümer 109
 - Einfacher Benutzerschlüssel 112
 - Erneut einrichten für Benutzer 114
 - HP ProtectTools 11
 - Notfallwiederherstellungs-Token 109
 - Richtlinien 10, 13
 - Sicher 13
 - Verwalten 11
 - Kennwort abgelehnt 122
 - Kennwortausnahmen 116
 - Kennwort des Eigentümers Festlegen 109
 - Kennwörter verwalten 26
 - Kennwort für Notfallwiederherstellungs-Token, festlegen 109
 - Kennwortsicherheit 38
 - Konfiguration
 - Einfache Konfiguration 92
 - Geräteklasse 93
 - Zurücksetzen 97
 - Konfigurieren
 - Administrator-Konsole 20
 - Anwendungen 26
 - Für ein Microsoft Office-Dokument 73
 - Für Microsoft Outlook 71
 - Zugriff auf Geräte 92
 - Konto, einfacher Benutzer 110
 - Kontrollieren des Gerätezugangs 91
- M**
- Management-Tools 27
 - Manuelles Shreddern
 - Alle ausgewählten Elemente 89
 - Ein bestimmter Datenbestand 88
 - Microsoft Excel, Signaturzeile hinzufügen 73
 - Microsoft Office-Dokument Signieren 73
 - Verschlüsseln 75
 - Verschlüsselt per E-Mail versenden 76
 - Verschlüsselung entfernen 75
- Microsoft Word, Signaturzeile hinzufügen 73
- N**
- Nachrichten 27
 - Nicht verwaltete Geräteklassen 102
 - Notfallwiederherstellung 109
- O**
- Öffnen
 - Device Access Manager for HP ProtectTools 91
 - File Sanitizer for HP ProtectTools 82
 - Öffnen von Drive Encryption 51
 - Öffnen von HP Device Access Manager for HP ProtectTools 91
 - Öffnen von HP ProtectTools Administrator-Konsole 18
 - Öffnen von Privacy Manager 61
 - Öffnen von Security Manager 29
- P**
- Password Manager 26, 33, 34
 - Persönliches sicheres Laufwerk (PSD) 111
 - Privacy Manager
 - Authentifizierungsmethoden 60
 - Mit einem Microsoft Office 2007 Dokument verwenden 72
 - Mit Microsoft Outlook verwenden 71
 - Öffnen 61
 - Sicherheits-Anmeldemethoden 60
 - Privacy Manager for HP ProtectTools
 - Migrieren von Privacy Manager Zertifikaten und vertrauenswürdigen Kontakten auf einen anderen Computer 77
 - Privacy Manager Zertifikate und vertrauenswürdige Kontakte auf einen anderen Computer migrieren 77
 - Setup-Verfahren 62
- Vertrauenswürdige Kontakte verwalten 67
- Verwalten von Privacy Manager Zertifikaten 62
- Privacy Manager-Zertifikat
 - Anfordern 62
 - Anzeigen von Details 64
 - Einrichten 63
 - Empfangen 63
 - Erneuern 64
 - Löschen 66
 - Standard festlegen 66
 - Widerrufen 67
 - Wiederherstellen 66
- Privacy Manager-Zertifikate
 - Sichern 77
 - Wiederherstellen 77
- Profil für einfaches Löschen anpassen 86
- Protokolldateien anzeigen 89
- R**
- Registerkarte Allgemein, Einstellungen 26
 - Registerkarte Anwendungen, Einstellungen 26
 - Registrieren
 - Fingerabdrücke 41
 - Szenen 44
- S**
- Security Manager, öffnen 29
 - Shreddern
 - Abbrechen 89
 - Automatisch 87
 - Manuell 88, 89
 - Tastensequenz 87
 - Shred-Profil
 - Anpassen 84
 - Auswählen 84
 - Erstellen 84
 - Shred-Zeitplan festlegen 83
 - Shred-Zyklus 85
 - Sicherheit
 - Grundlegende Aufgaben 8
 - Rollen 11
 - Übersicht 32
 - Sicherheitseinstellungen festlegen 21
 - Sicherheitsrollen 11

- Sichern und Wiederherstellen
 - Embedded Security 113
 - Zertifizierungs-informationen 113
 - Sichern von HP ProtectTools
 - Anmeldedaten 13
 - Sichern von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten 77
 - Sichern von
 - Verschlüsselungsschlüsseln 58
 - Sicherungs- und Wiederherstellungskennwort für HP ProtectTools Security Manager 11
 - Signieren
 - E-Mail-Nachricht 72
 - Microsoft Office-Dokument 73
 - Smart Card
 - Initialisieren 42
 - Konfigurieren 24, 43
 - Registrieren 43
 - Smart Card-PIN 12
 - Softwareverschlüsselung 52, 53, 54, 58
 - SpareKey, Einstellungen 22
 - SpareKey einrichten 41
 - Status der
 - Sicherheitsanwendungen 32
 - Symbol verwenden 88
 - Szenen registrieren 44
- T**
- Tastenfolge 87
 - TPM-Chip
 - Aktivieren 108
 - Initialisieren 109
- U**
- Überschreiben
 - Abbrechen 89
 - Aktivieren 89
 - Manuell 89
 - Zeitplan 83
 - Überschreiben von freiem Speicherplatz 83
 - Unbefugten Zugriff verhindern 8
 - Updates 27
- V**
- VeriSign Identity Protection (VIP) 39
 - Verschlüsseln von Dateien und Ordern 111
 - Verschlüsseln von Festplatten 56, 58
 - Verschlüsseln von Laufwerken 51
 - Verschlüsselte Dokumente per E-Mail versenden 76
 - Verschlüsselung
 - Entfernen 75
 - Hardware 52, 54
 - Software 52, 54, 58
 - Verschlüsselungsschlüssel
 - Sichern 58
 - Wiederherstellung 59
 - Verschlüsselungsstatus anzeigen 56
 - Versenden eines verschlüsselten Microsoft Office-Dokuments per E-Mail 76
 - Versiegeln 72
 - Vertrauenswürdige Kontakte
 - Anzeigen von Details 69
 - Hinzufügen 67
 - Sichern 77
 - Wiederherstellen 77
 - Vertrauenswürdiger Kontakt
 - Löschen 69
 - Widerruf-Status prüfen 69
 - Verwalten
 - Anmeldedaten 40
 - Kennwörter 33, 34
 - Laufwerke verschlüsseln oder entschlüsseln 58
 - Verweigern 95
 - Vorab zugewiesenes Zertifikat 63
 - Vordefiniertes Shred-Profil 84
- W**
- Widerherstellen von HP ProtectTools Anmeldedaten 13
 - Wiederbeschaffung gestohlener Geräte 105
 - Wiederherstellen eines Verschlüsselungsschlüssels 59
 - Wiederherstellen von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten 77
 - Windows Anmeldekennwort 11
 - Word, Signaturzeile hinzufügen 73
- Z**
- Zentrale Verwaltung 27, 78
 - Zertifikat, vorab zugewiesenes 63
 - Zertifikat von einem anderen Anbieter importieren 63
 - Zugang
 - Kontrollieren 91
 - Zugriff
 - Verhindern von unbefugtem Zugriff 8
 - Zugriff erteilen 95
 - Zurücksetzen 97

