HP Client Security

Einführung

Erste Ausgabe: August 2013

Dokumentennummer 735339-041

Inhaltsverzeichnis

1 Einführung in HP Client Security Manager 1

HP Client Security Funktionen 1

HP Client Security Produktbeschreibung und gängige Beispiele 3

Password Manager 3

HP Drive Encryption (bestimmte Modelle) 4

HP Device Access Manager (bestimmte Modelle) 4

Computrace (separat zu erwerben) 5

Die wichtigsten Sicherheitsziele 5

Schutz vor gezieltem Diebstahl 6

Beschränken des Zugriffs auf sensible Daten 6

Verhindern von nicht autorisiertem internen oder externen Zugriff 6

Erstellen von Richtlinien für starke Kennwörter 6

Zusätzliche Sicherheitselemente 7

Zuweisen von Sicherheitsrollen 7

Verwalten von HP Client Security Kennwörtern 7

Erstellen eines sicheren Kennworts 8

Sichern von Anmeldeinformationen und Einstellungen 8

2 Erste Schritte 9

Öffnen von HP Client Security 10

3 Small Business – Kurzanleitung zur Einrichtung 11

Erste Schritte 11

Password Manager 11

Anzeigen und Verwalten von gespeicherten Authentifizierungen in Password Manager .. 12

HP Device Access Manager 12

HP Drive Encryption 12

4 HP Client Security 13

Identitätsfunktionen, Anwendungen und Einstellungen 13

Fingerabdrücke 13

Fingerabdrücke – Verwaltungseinstellungen 14

Fingerabdrücke – Benutzereinstellungen 15

HP SpareKey – Kennwortwiederherstellung 15

HP SpareKey-Einstellungen 15

Windows Kennwort 16

Bluetooth-Geräte 16
Einstellungen für Bluetooth-Geräte 16
Karten 17
Einstellungen für Näherungskarten, kontaktlose Karten und Smart Cards 18
PIN 18
PIN-Einstellungen 19
RSA SecurID 19
Password Manager 19
Für Webseiten oder Programme, für die noch keine Anmeldeinformationen festgelegt wurden 20
Für Webseiten oder Programme, für die bereits Anmeldeinformationen festgelegt wurden 20
Hinzufügen von Anmeldeinformationen 21
Bearbeiten von Anmeldeinformationen 22
Verwenden des Password Manager-Menüs „Verknüpfungen“ 22
Organisieren von Anmeldeinformationen nach Kategorien 23
Verwalten der Anmeldeinformationen 23
Einschätzen der Kennwortsicherheit 24
Einstellungen für das Password Manager-Symbol 24
Importieren und Exportieren von Anmeldeinformationen 25
Einstellungen 26
Erweiterte Einstellungen 27
Administratorrichtlinien 27
Richtlinien für Standardbenutzer 28
Sicherheitsfunktionen 28
Benutzer 29
Meine Richtlinien 29
Sichern und Wiederherstellen Ihrer Daten 30

5 HP Drive Encryption (bestimmte Modelle) 32
Öffnen von Drive Encryption 32
Allgemeine Aufgaben 33
Aktivieren von Drive Encryption für Standard-Festplatten 33
Aktivieren von Drive Encryption für selbstverschlüsselnde Laufwerke 33
Deaktivieren von Drive Encryption 34
Anmelden, nachdem Drive Encryption aktiviert wurde 34
Verschlüsseln zusätzlicher Festplatten 35
Erweiterte Aufgaben 36
Verwalten von Drive Encryption (Administrator-Aufgabe) 36
Ver- und Entschlüsseln einzelner Laufwerkspartitionen (nur für Software-Verschlüsselung) 36

Festplattenverwaltung 36
Sichern und Wiederherstellen (Administratoraufgabe) 37
Sichern von Verschlüsselungsschlüsseln 37
Wiederherstellen des Zugriffs auf einen Computer, auf dem Drive Encryption aktiviert ist, mithilfe von Sicherungsschlüsseln 38
Durchführen einer HP SpareKey-Wiederherstellung 38

6 HP File Sanitizer (bestimmte Modelle) 39
Shreddern 39
Überschreiben von freiem Speicherplatz 39
Aufrufen von File Sanitizer 40
Setup-Verfahren 40
Festlegen eines Shred-Zeitplans 41
Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz 42
Schützen von Dateien vor dem Shreddern 42
Allgemeine Aufgaben 43
Verwenden des File Sanitizer-Symbols 43
Shreddern durch Rechtsklicken auf den Datenbestand 44
Manuelles Starten eines Shred-Vorgangs 44
Manuelles Starten des Überschreibens von freiem Speicherplatz 44
Anzeigen der Protokolldateien 45

7 HP Device Access Manager (bestimmte Modelle) 46
Aufrufen von Device Access Manager 46
Benutzeransicht 47
Systemansicht 47
JITA-Konfiguration 48
Erstellen einer JITA-Richtlinie für einen Benutzer oder eine Gruppe 49
Deaktivieren einer JITA-Richtlinie für einen Benutzer oder eine Gruppe 49
Einstellungen 49
Nicht verwaltete Geräteklassen 49

8 HP Trust Circles 51
Öffnen von Trust Circles 51
Einführung 51
Trust Circles 52
Hinzufügen von Ordnern zu einem Vertrauenskreis 52
Hinzufügen von Mitgliedern zu einem Vertrauenskreis 53
Hinzufügen von Dateien zu einem Vertrauenskreis 54

Verschlüsselte Ordner 54
Entfernen von Ordnern aus einem Vertrauenskreis 54
Entfernen einer Datei aus einem Vertrauenskreis 54
Entfernen von Mitgliedern aus einem Vertrauenskreis 54
Löschen eines Vertrauenskreises 55
Festlegen von Einstellungen 55

9 Theft recovery (select models only)Aero verwalten (bestimmte Modelle) 58

10 Ausnahmen für lokalisierte Kennwörter 59
Vorgehensweise, wenn ein Kennwort abgelehnt wird 59
Keine Unterstützung für Windows IMEs während der Authentifizierung beim Systemstart und der HP Drive Encryption-Authentifizierung 59
Ändern des Kennworts mit einem Tastaturlayout, das ebenfalls unterstützt wird 60
Behandeln von Sonderzeichen 60

Glossar 63

Index 67

1 Einführung in HP Client Security Manager

Mit HP Client Security können Sie Ihre Daten und Geräte und Ihre Identität schützen und auf diese Weise die Sicherheit Ihres Computers erhöhen.

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

Die HP Client Security 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 Sie die entsprechenden HP Client Security Softwaremodule bereits installiert haben.

HP Client Security Funktionen

In der folgenden Tabelle finden Sie nähere Informationen zu den Hauptfunktionen der HP Client Security Module.

Modul	Wichtige Funktionen
HP Client Security Manager	Administratoren können die folgenden Funktionen ausführen: • Den Zugriff auf Ihren Computer vor dem Starten von Windows® schützen • Den Zugriff auf Ihr Windows Konto durch starke Authentifizierung schützen • Anmeldenamen und Kennwörter für Websites und Anwendungen verwalten • Kennwörter für das Windows Betriebssystem schnell und einfach ändern • Fingerabdrücke für zusätzliche Sicherheit und Komfort verwenden • Eine Smartcard, kontaktlose Karte oder Näherungskarte als Identitätsnachweis für die Authentifizierung konfigurieren • Ein Bluetooth-Telefon als Mittel zur Identifizierung verwenden • Authentifizierungsoptionen durch Festlegen einer PIN erweitern • Anmelde- und Sitzungsrichtlinien konfigurieren • Programmdaten sichern und wiederherstellen • Weitere Anwendungen wie HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager und HP Computrace hinzufügen Allgemeine Benutzer können: • Einstellungen für den Verschlüsselungsstatus und Device Access Manager anzeigen • Computrace aktivieren • Voreinstellungen für Sicherungs- und Wiederherstellungsoptionen konfigurieren
Password Manager	Normale Benutzer können die folgenden Funktionen ausführen: • Benutzernamen und Kennwörter verwalten und einrichten. • Kennwörter mit hoher Sicherheit für verbesserte Sicherheit beim Zugriff auf E-Mail und Benutzerkonten im Internet erstellen. Die Eingabe und das Senden der Informationen wird von Password Manager automatisch erledigt. • Den Anmeldevorgang mit der Single Sign-On-Funktion beschleunigen, die Benutzeranmeldeinformationen automatisch speichert und anwendet. • Ein Konto als gefährdet kennzeichnen, so dass Sie bei anderen Konten mit ähnlichen Anmeldedaten entsprechend gewarnt werden • Anmeldeinformationen von einem unterstützten Browser importieren
HP Drive Encryption (bestimmte Modelle)	• Bietet eine komplette Verschlüsselung der gesamten Festplatte. • Erzwingt eine Authentifizierung vor dem Systemstart zum Entschlüsseln und Zugreifen auf Daten. • Bietet die Option zur Aktivierung selbstverschlüsselnder Laufwerke (bestimmte Modelle):

Modul	Wichtige Funktionen
HP Device Access Manager	• Ermöglicht IT-Managern die Zugriffssteuerung von Geräten auf Basis von Benutzerprofilen. • Verhindert, dass Daten von nicht autorisierten Benutzern auf externe Speichermedien kopiert werden und Viren über externe Medien in das System gelangen. • Ermöglicht Administratoren, den Zugriff auf Kommunikationsgeräte für bestimmte Personen oder Benutzergruppen zu sperren.
HP Trust Circles	• Bietet Datei- und Dokumentensicherheit. • Verschlüsselt Daten in von Benutzern festgelegten Ordnern und schützt sie innerhalb eines Vertrauenskreises. • Ermöglicht die gemeinsame Verwendung von Dateien exklusiv durch Mitglieder eines Vertrauenskreises.
Wiederbeschaffung gestohlener Geräte (Computrace, separat zu erwerben)	• Für die Aktivierung ist ein separates Tracking- and Tracing-Abonnement erforderlich. • Bietet sichere Bestandsverfolgung. • Überwacht Benutzeraktivität sowie Hardware- und Softwareänderungen. • Bleibt aktiv, auch wenn die Festplatte neu formatiert oder ersetzt wird.

HP Client Security Produktbeschreibung und gängige Beispiele

Die meisten HP Client Security Produkte verfügen sowohl über eine Benutzerauthentifizierung (in der Regel ein Kennwort) als auch über eine administrative Sicherung, um Zugriff erlange zu können, falls ein Kennwort verloren ging, nicht verfügbar ist oder vergessen wurde, oder falls die Unternehmenssicherheit einen Zugriff erfordert.

HINWEIS: Einige der HP Client Security Produkte sind dazu konzipiert, den Zugriff auf Daten einzuschränken. Die Daten sollten Verschlüsselt werden, wenn sie so wichtig sind, dass der Benutzer sie lieber verlieren als preisgeben würde. Es wird empfohlen, alle Daten an einem sicheren Ort zu sichern.

Password Manager

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

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

- Ein Konto als gefährdet kennzeichnen, so dass Sie bei anderen Konten mit ähnlichen Anmeldedaten entsprechend gewarnt werden
- Anmeldeinformationen von einem unterstützten Browser importieren

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

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

Beispiel 2: Ein hart arbeitender Mitarbeiter ist befördert worden und leitet nun die gesamte Buchhaltungsabteilung. Das Team muss auf eine große Anzahl von Kundenkonten im Internet zugreifen, von denen jedes andere Anmeldeinformationen verwendet. Die Anmeldeinformationen werden gemeinsam mit anderen Kollegen genutzt. Vertraulichkeit spielt daher eine wichtige Rolle. Der Mitarbeiter beschließt, alle Internetlinks, Namen und Kennwörter von Firmenbenutzern innerhalb von Password Manager zu verwalten. Nach dem Abschluss dieser Arbeit stellt der Mitarbeiter Password Manager für die Mitarbeiter bereit. Diese können sich jetzt ohne Kenntnis der verwendeten Anmeldeinformationen bei den Internetkonten anmelden.

HP Drive Encryption (bestimmte Modelle)

HP Drive Encryption wird dazu verwendet, den Zugriff auf die Daten auf der gesamten Festplatte des Computers oder einem sekundären Laufwerk einzuschränken. Drive Encryption kann auch selbstverschlüsselnde Laufwerke verwalten.

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

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.

HP Device Access Manager (bestimmte Modelle)

Mit HP Device Access Manager Administratoren den Zugriff auf die Hardware einschränken und verwalten. Device Access Manager kann dazu eingesetzt werden, unbefugten Zugriff auf USB-Flash-Laufwerk zu blockieren, auf die Daten kopiert werden könnten. Außerdem kann damit der Zugriff auf CD/DVD-Laufwerke, die Kontrolle über USB-Geräte, Netzwerkverbindungen usw. eingeschränkt werden. Ein Beispiel wäre eine Situation, in der Fremdanbieter Zugriff auf die Computer des Unternehmens benötigen, dabei aber nicht in der Lage sein sollten, Daten auf ein USB-Gerät zu kopieren.

Beispiel 1: Ein Manager eines Unternehmens für medizinische Versorgung arbeitet oft mit persönlichen medizinischen Daten zusammen mit seinen Firmendaten. Die Mitarbeiter brauchen Zugriff auf diese Daten, allerdings ist es äußerst wichtig, dass die Daten nicht über ein USB-Laufwerk oder andere externe Speichermedien vom Computer entfernt werden. Das Netzwerk ist zwar sicher, aber die Computer verfügen über CD-Brenner und USB-Anschlüsse, über die Daten kopiert oder gestohlen werden könnten. Der Manager setzt Device Access Manager ein, um die USB-Anschlüsse und CD-Brennern zu deaktivieren, sodass sie nicht verwendet werden können. Auch wenn die USB-Ports blockiert sind, funktionieren Maus und Tastatur weiterhin normal.

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

Computrace (separat zu erwerben)

Bei Computrace (separat zu erwerben) handelt es sich um einen Dienst, der den Standort eines gestohlenen Computers orten kann, wenn der Benutzer auf das Internet zugreift. Darüber hinaus kann Computrace helfen, Computer aus der Ferne zu verwalten und zu finden oder die Computernutzung und Anwendungen zu überwachen.

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

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

Die wichtigsten Sicherheitsziele

Die HP Client Security Module können zusammenarbeiten und bieten so Lösungen für eine Vielzahl von Sicherheitspolizei. Dazu gehören auch die folgenden Hauptziele der Sicherheit:

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

Schutz vor gezieltem Diebstahl

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

- Die Funktion zur Authentifizierung vor dem Systemstart verhindert den Zugriff auf das Betriebssystem.
  - HP Client Security – Siehe „HP Client Security“ auf Seite 13.
  - HP Drive Encryption – Siehe „HP Drive Encryption (bestimmte Modelle)“ auf Seite 32.
- Mithilfe der Verschlüsselung kann sichergestellt werden, dass auf Daten auch dann nicht zugegriffen werden kann, wenn die Festplatte entfernt und auf einem ungesichterten System installiert wird.
- Computrace kann die Position eines Computers nach einem Diebstahl feststellen.
  - Computrace – Siehe „Theft recovery (select models only)Aero verwalten (bestimmte Modelle)“ auf Seite 58.

Beschränken des Zugriffs auf sensible Daten

Angenommen, ein Wirtschaftsprüfer wird vor Ort eingesetzt. Ihm wird der Zugriff auf die Computer gewährleistet, um sensible Finanzdaten zu prüfen. Sie möchten allerdings nicht, dass er die Daten drucken oder auf einem beschreibbaren Medium wie einer CD speichern kann. Mit dem folgenden Merkmal können Sie den Zugriff auf Daten einschränken:

- HP Device Access Manager ermöglicht IT-Leitern, den Zugriff auf Kommunikationsmedien einzuschränken, damit keine sensiblen Daten von der Festplatte kopiert werden können. Siehe „Systemansicht“ auf Seite 47.

Verhindern von nicht autorisiertem internen oder externen Zugriff

Unautorisierter Zugriff auf einen Firmencomputer ist ein sehr reales Risiko für die Netzwerkressourcen eines Unternehmens wie z. B. die Informationen von Finanzdiensten, Führungskräften und dem Team für Forschung und Entwicklung, und private Informationen wie z. B. Patientenakten oder persönlichen Finanzdaten. Die folgende Funktion verhindert den unautorisierten Zugriff:

- Die Funktion zur Authentifizierung vor dem Systemstart verhindert, sofern aktiviert, den Zugriff auf das Betriebssystem. Siehe „HP Drive Encryption (bestimmte Modelle)“ auf Seite 32.
- HP Client Security hilft dabei sicherzustellen, dass ein nicht autorisierter Benutzer keinen Zugang zu Kennwörtern oder kennwortgeschützten Anwendungen erhält. Siehe „HP Client Security“ auf Seite 13.
- HP Device Access Manager ermöglicht IT-Leitern, den Zugriff auf beschreibbare Medien einzuschränken, damit keine sensiblen Daten von der Festplatte kopiert werden können. Siehe „HP Device Access Manager (bestimmte Modelle)“ auf Seite 46.

Erstellen von Richtlinien für starke Kennwörter

Für den Fall, dass eine Firmenrichtlinie wirksam wird, welche die Verwendung von Kennwörtern mit hoher Sicherheit für webbasierte Anwendungen und Datenbanken erfordert, bietet Password Manager ein geschützten Repository für Kennwörter und SSO-Komfort. Siehe „Password Manager“ auf Seite 19.

Zusätzliche Sicherheitselemente

Zuweisen von Sicherheitsrollen

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

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

Die Sicherheitsaufgaben und -rechte können bei HP Client Security auf die folgenden Rollen aufgeteilt werden.

- Sicherheitsbeauftragter - Diese Person definiert die Sicherheitsstufe für das Unternehmen oder das Netzwerk und legt die bereitzustellenden Sicherheitsfunktionen fest wie z. B. Drive Encryption.

  HINWEIS: Viele der Funktionen in HP Client Security können vom Sicherheitsbeauftragten zusammen mit HP individuell angepasst werden. Weitere Informationen finden Sie unter http://www.hp.com.

- IT-Administrator - Diese Person setzt die vom Sicherheitsbeauftragten definierten Maßnahmen um und verwaltet die Funktionen. Sie kann einige Merkmale aktivieren und deaktivieren. Wenn sich der Sicherheitsbeauftragte beispielsweise für den Einsatz von Smart Cards entschieden hat, kann der IT-Administrator das Kennwort und den Modus für die Smart Card aktivieren.

- Benutzer - Diese Person nutzt die Sicherheitsfunktionen. Wenn Sicherheitsbeauftragter und IT-Administrator beispielsweise Smart Cards für das System aktiviert haben, kann der Benutzer die Smart Card-PIN festlegen und die Smart Card zur Authentifizierung verwenden.

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

Nicht autorisierten Benutzern sollten keine administrativen Rechte gewährt werden.

Verwalten von HP Client Security Kennwörtern

Die meisten Funktionen in HP Client Security sind durch ein Kennwort geschützt. In der folgenden Tabelle werden häufig verwendete Kennwörter, das Softwaremodul, in dem das Kennwort festgelegt wird, und die Funktion des Kennworts beschrieben.

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

HP Client Security Kennwort	In folgendem Modul festgelegt	Funktion
Windows Anmeldekennwort	Windows Systemsteuerung oder HP Client Security	Zur manuellen Anmeldung oder Authentifizierung, um auf verschiedene HP Client Security-Funktionen zuzugreifen.

HP Client Security Kennwort	In folgendem Modul festgelegt	Funktion
HP Client Security-Kennwort für Sicherung und Wiederherstellung	HP Client Security, durch einzelnen Benutzer	Schützt den Zugriff auf die HP Client Security-Sicherungs- und Wiederherstellungsdatei.
Smart Card-PIN	Credential Manager	Kann zur Mehrfach-Authentifizierung verwendet werden. Kann zur Windows Authentifizierung verwendet werden. Authentifiziert Benutzer von Drive Encryption, wenn die Smart Card ausgewählt wird.

Erstellen eines sicheren Kennworts

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

- Verwenden Sie Kennwörter mit mehr als sechs Zeichen, idealerweise mit mehr als acht.
- Verwenden Sie Groß- und Kleinbuchstaben in Ihrem Kennwort.
- Wenn möglich, verwenden Sie eine Kombination aus alphanumerischen Zeichen, Sonderzeichen und Satzzeichen.
- Ersetzen Sie Buchstaben durch Zahlen oder Sonderzeichen. Verwenden Sie beispielsweise die Zahl 1 für die Buchstaben I oder L.
- Kombinieren Sie Wörter aus zwei oder mehreren Fremdsprachen.
- Teilen Sie ein Wort oder einen Ausdruck mit Zahlen oder Sonderzeichen in der Mitte auf, z. B. „Maria2-2Katze45“.
- Verwenden Sie kein Kennwort, das in derselben Form in einem Wörterbuch zu finden ist.
- Benutzen Sie für das Kennwort weder Ihren Namen noch andere persönliche Informationen wie Ihr Geburtsdatum, Namen von Haustieren, Mädchenname der Mutter usw., auch nicht rückwärts geschrieben.
- Ändern Sie Ihre Kennwörter regelmäßig. Dabei können Sie auch nur ein paar Zeichen ändern.
- Wenn Sie ein Kennwort aufschreiben, bewahren Sie die Notiz nicht an einem leicht einsehbaren Platz in der Nähe des Computers auf.
- Speichern Sie das Kennwort nicht in einer Datei (z. B. E-Mail) auf dem Computer.
- Teilen Sie Benutzerkonten nicht mit anderen Personen, und geben Sie Ihr Kennwort niemandem weiter.

Sichern von Anmeldeinformationen und Einstellungen

Sie können das Tool Sichern und Wiederherstellen in HP Client Security als zentralen Ausgangspunkt für die Sicherung und Wiederherstellung von Sicherheits-Anmeldeinformationen einiger der installierten HP Client Security-Module nutzen.

2 Erste Schritte

Um HP Client Security für die Verwendung mit Ihren Anmeldeinformationen zu konfigurieren, starten Sie HP Client Security auf eine der folgenden Weisen. Nachdem der Assistent durch einen Benutzer abgeschlossen wurde, kann er nicht erneut von diesem Benutzer gestartet werden.

1. Klicken oder tippen Sie auf dem Startbildschirm oder Apps-Bildschirm auf die App **HP Client Security** (Windows 8).

   – ODER –

   Klicken oder tippen Sie auf dem Windows Desktop auf das Gadget **HP Client Security** (Windows 7).

   – ODER –

   Doppelklicken oder doppeltippen Sie auf dem Windows Desktop auf das Symbol **HP Client Security** im Infobereich außen rechts in der Taskleiste.

   – ODER –

   Klicken oder tippen Sie auf dem Windows Desktop auf das Symbol **HP Client Security** im Infobereich, und wählen Sie **HP Client Security öffnen** aus.

2. Der Installationsassistent für HP Client Security wird gestartet und zeigt die Begrüßungsseite an.

3. Lesen Sie die Informationen auf der Begrüßungsseite, bestätigen Sie Ihre Identität durch Eingabe Ihres Windows Kennworts, und klicken oder tippen Sie auf **Weiter**.

   Wenn Sie noch kein Windows Kennwort eingerichtet haben, werden Sie zum Einrichten eines Kennworts aufgefordert. Ein Windows Kennwort ist erforderlich, um Ihr Windows Konto vor dem Zugriff unbefugter Personen zu schützen und die HP Client Security-Funktionen nutzen zu können.

4. Wählen Sie auf der Seite „HP SpareKey“ drei Sicherheitsfragen aus. Geben Sie zu jeder Frage eine Antwort, ein und klicken Sie dann auf **Weiter**. Es sind auch benutzerdefinierte Fragen möglich. Weitere Informationen finden Sie unter „HP SpareKey – Kennwortwiederherstellung“ auf Seite 15.

5. Registrieren Sie auf der Seite „Fingerabdrücke“ mindestens die minimal erforderliche Anzahl von Fingerabdrücken, und klicken oder tippen Sie dann auf **Weiter**. Weitere Informationen finden Sie unter „Fingerabdrücke“ auf Seite 13.

6. Aktivieren Sie auf der Seite „Drive Encryption“ die Verschlüsselung, sichern Sie den Verschlüsselungsschlüssel, und klicken oder tippen Sie dann auf **Weiter**. Weitere Informationen finden Sie in der Hilfe zur HP Drive Encryption-Software.

HINWEIS: Dies betrifft Szenarios, bei denen der Benutzer ein Administrator ist und der Installationsassistent für HP Client Security zuvor noch nicht von einem Administrator konfiguriert worden ist.

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

   Auf dieser Seite werden Statusinformationen zu Funktionen und Anmeldeinformationen bereitgestellt.

8. Der Installationsassistent für HP Client Security stellt sicher, dass die Just-In-Time-Authentifizierung und die File Sanitizer-Funktionen aktiviert werden. Weitere Informationen finden Sie in der Hilfe zur HP Device Access Manager-Software und der Hilfe zur HP File Sanitizer-Software.

HINWEIS: Dies betrifft Szenarios, bei denen der Benutzer ein Administrator ist und der Installationsassistent für HP Client Security zuvor noch nicht von einem Administrator konfiguriert worden ist.

Öffnen von HP Client Security

HP Client Security lässt sich auf folgende Arten öffnen:

HINWEIS: Bevor die Anwendung HP Client Security geöffnet werden kann, muss der Installationsassistent für HP Client Security vollständig ausgeführt worden sein.

- Klicken oder tippen Sie auf dem Startbildschirm oder Apps-Bildschirm auf die App **HP Client Security** (Windows 8).

  – ODER –

  Klicken oder tippen Sie auf dem Windows Desktop auf das Gadget **HP Client Security** (Windows 7).

  – ODER –

  Doppelklicken oder doppeltippen Sie auf dem Windows Desktop auf das Symbol **HP Client Security** im Infobereich außen rechts in der Taskleiste.

  – ODER –

  Klicken oder tippen Sie auf dem Windows Desktop auf das Symbol **HP Client Security** im Infobereich, und wählen Sie **HP Client Security öffnen** aus.

3 Small Business – Kurzanleitung zur Einrichtung

In diesem Kapitel werden die grundlegenden Schritte zum Aktivieren der gängigsten und nützlichsten Optionen in HP Client Security for Small Business vorgestellt. Mithilfe der zahlreichen Tools und Optionen in dieser Software können Sie Ihre Voreinstellungen optimieren und Ihre Zugriffssteuerung einrichten. Der Hauptzweck dieses Easy Setup Guide ist, jedes Modul mit möglichst geringem Arbeits- und Zeitaufwand einsatzbereit zu machen. Für weitere Informationen wählen Sie das gewünschte Modul aus und klicken dann in der oberen rechten Ecke auf die Schaltfläche **?** oder Hilfe. Dadurch werden automatisch Informationen angezeigt, die Ihnen bei dem aktuell angezeigten Fenster helfen.

Erste Schritte

1. Doppelklicken Sie auf dem Windows Desktop im Benachrichtigungsbereich (außen rechts in der Taskleiste) auf das Symbol **HP Client Security**, um die Anwendung zu öffnen.
2. Geben Sie Ihr Windows Kennwort ein, oder erstellen Sie ein Windows Kennwort.
3. Schließen Sie die HP Client Security Installation ab.

Wenn HP Client Security für die einmalige Authentifizierung während der Windows Anmeldung konfiguriert werden soll, lesen Sie bitte den Abschnitt unter „Sicherheitsfunktionen“ auf Seite 28.

Password Manager

Jede Person verfügt über eine ganze Reihe von Kennwörtern, besonders dann, wenn Sie regelmäßig Webseiten oder Anwendungen öffnen, bei denen eine Anmeldung erforderlich ist. Der normale Benutzer verwendet entweder dasselbe Kennwort für alle Anwendungen und Webseiten, oder er wird kreativ und vergisst dann schnell, welches Kennwort zu welcher Anwendung gehört.

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

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

So speichern Sie Websites, Benutzernamen und Kennwörter:

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

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

Anzeigen und Verwalten von gespeicherten Authentifizierungen in Password Manager

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

Öffnen Sie Password Manager unter Verwendung der Tastenkombination Ctrl+Windows Taste+h, und klicken Sie auf **Anmelden**, um den gespeicherten Link zu öffnen und die entsprechende Authentifizierung zu starten.

Die Option **Bearbeiten** in Password Manager die ermöglicht es Ihnen, den Namen und den Anmeldenamen anzuzeigen und zu ändern, und Sie können sogar das Kennwort anzeigen.

Mit HP Client Security for Small Business können alle Anmeldeinformationen und Einstellungen gesichert und/oder auf einen anderen Computer kopiert werden.

HP Device Access Manager

Device Access Manager kann verwendet werden, um die Nutzung verschiedener interner und externer Speichergeräte zu beschränken, sodass Ihre Daten sicher auf der Festplatte bleiben und Ihr Unternehmen nicht verlassen. Ein Beispiel wäre, einem Benutzer Zugriff auf Ihre Daten zu erlauben, dabei aber zu verhindern, dass diese Daten auf CD, persönliche Musikwiedergabegeräte oder USB-Speichergeräte kopiert werden können.

1. Öffnen Sie **Device Access Manager** (siehe „Aufrufen von Device Access Manager“ auf Seite 46.

   Der Zugriff für den aktuellen Benutzer wird angezeigt.
2. Zum Ändern des Zugriffs für Benutzer, Gruppen oder Geräte klicken oder tippen Sie auf **Ändern**. Weitere Informationen finden Sie unter „Systemansicht“ auf Seite 47.

HP Drive Encryption

HP Drive Encryption wird dazu verwendet, Ihre Daten durch Verschlüsselung der gesamten Festplatte zu schützen. Die Daten auf Ihrer Festplatte bleiben auch dann geschützt, wenn Ihre Ihr Computer gestohlen werden sollte oder die Festplatte aus dem ursprünglichen Computer entfernt und in einem anderen Computer eingesetzt wird.

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

Damit es für Sie einfacher wird, synchronisieren mehrere Softwaremodule die Kennwörter automatisch, darunter Windows Benutzerkonten, Domänen, HP Drive Encryption, Password Manager und HP Client Security.

Informationen zum Konfigurieren von HP Drive Encryption während der Ersteinrichtung mit dem Installationsassistenten für HP Client Security finden Sie unter „Erste Schritte“ auf Seite 9.

4 HP Client Security

Die Startseite von HP Client Security ist der zentrale Bereich für den problemlosen Zugriff auf die Funktionen, Anwendungen und Einstellungen von HP Client Security. Die Startseite ist in drei Abschnitte unterteilt:

- **DATEN** – Ermöglicht den Zugriff auf Anwendungen für die Verwaltung der Datensicherheit.
- **GERÄT** – Ermöglicht den Zugriff auf Anwendungen für die Verwaltung der Gerätesicherheit.
- **IDENTITÄT** – Ermöglicht Registrierung und Verwaltung von Anmeldeinformationen für die Authentifizierung.

Bewegen Sie den Zeiger über eine Anwendungskachel, um eine Beschreibung der Anwendung anzuzeigen.

Auf den Seiten von HP Client Security können im unteren Bereich Links zu Benutzer- und Verwaltungseinstellungen angezeigt werden. HP Client Security ermöglicht den Zugriff auf erweiterte Einstellungen und Funktionen durch Tippen oder Klicken auf das **Zahnrad**-Symbol (für Einstellungen).

Identitätsfunktionen, Anwendungen und Einstellungen

Die von HP Client Security bereitgestellten Identitätsfunktionen, Anwendungen und Einstellungen helfen Ihnen beim Verwalten verschiedener Aspekte Ihrer digitalen Identität. Klicken oder tippen Sie auf eine der folgenden Kacheln auf der Startseite von HP Client Security, und geben Sie dann Ihr Windows Kennwort ein:

- **Fingerabdrücke** – Registriert und verwaltet Ihre Fingerabdruckdaten für die Benutzeranmeldung.
- **SpareKey** – Konfiguriert und verwaltet Ihre HP SpareKey-Anmeldeinformationen, die Sie zur Anmeldung auf Ihrem Computer verwenden können, wenn andere Anmeldeinformationen verloren gingen oder nicht auffindbar sind. Sie ermöglichen es Ihnen auch, Ihr Kennwort zurückzusetzen, wenn Sie es vergessen haben.
- **Windows Kennwort** – Ermöglicht leichten Zugriff auf Ihre Windows Kennwort, um es zu ändern.
- **Bluetooth-Geräte** – Ermöglicht Ihnen das Registrieren und Verwalten von Bluetooth-Geräten.
- **Karten** – Ermöglicht Ihnen das Registrieren und Verwalten von Smart Cards, kontaktlosen Karten und Näherungskarten.
- **PIN** – Ermöglicht Ihnen das Registrieren Ihrer PIN-Anmeldeinformationen.
- **RSA SecurID** – Ermöglicht Ihnen das Registrieren und Verwalten Ihre RSA SecurID-Anmeldeinformationen (sofern entsprechend konfiguriert).
- **Password Manager** – Ermöglicht Ihnen das Verwalten von Kennwörtern für Websites und Anwendungen im Internet.

Fingerabdrücke

Der Installationsassistent für HP Client Security führt Sie durch den als „Registrierung“ bezeichneten Vorgang der Erfassung Ihrer Fingerabdrücke.

Sie können das Registrieren oder Löschen von Fingerabdrücken auch auf der Seite „Fingerabdrücke“ durchführen, auf die Sie zugreifen, indem Sie auf der Startseite von HP Client Security auf das Symbol **Fingerabdrücke** klicken oder tippen.

1. Streichen Sie bei geöffneter Seite „Fingerabdrücke“ mehrmals mit dem Finger über den Sensor des Fingerabdruck-Lesegeräts, bis der Fingerabdruck erfolgreich registriert ist.

   Die Anzahl der zu registrierenden Finger wird auf der Seite angezeigt. Zeige- und Mittelfinger sind dabei vorzuziehen.

2. Wenn Sie bereits registrierte Fingerabdrücke löschen möchten, klicken oder tippen Sie auf **Löschen**.

3. Zur Registrierung weitere Finger klicken oder tippen Sie auf **Zusätzlichen Fingerabdruck registrieren**.

4. Klicken oder tippen Sie auf **Speichern**, bevor Sie die Seite verlassen.

⚠ **ACHTUNG:** Bei der Registrierung der Fingerabdrücke über den Assistenten werden die Fingerabdruck-Informationen erst gespeichert, wenn Sie auf **Weiter** klicken. Sollten Sie den Computer für eine Weile inaktiv lassen oder das Programm beenden, werden die vorgenommenen Änderungen **nicht** gespeichert.

- ▲ Um auf die Seite „Fingerabdrücke – Verwaltungseinstellungen“ zuzugreifen, auf der Administratoren Einstellungen für die Registrierung, die Genauigkeit und andere Einstellungen konfigurieren können, klicken oder tippen Sie auf **Verwaltungseinstellungen** (erfordert Administratorberechtigungen).

- ▲ Um auf die Seite „Fingerabdrücke – Benutzereinstellungen“ zuzugreifen, auf der Sie Einstellungen bezüglich der Darstellung und des Verhaltens der Fingerabdruckerkennung konfigurieren können, klicken oder tippen Sie auf **Benutzereinstellungen**.

Fingerabdrücke – Verwaltungseinstellungen

Administratoren können die Registrierung, Genauigkeit der Erfassung und andere Einstellungen für ein Fingerabdruck-Lesegerät konfigurieren. Hierfür sind Administratorberechtigungen erforderlich.

- ▲ Um auf die Verwaltungseinstellungen für die Fingerabdruck-Anmeldeinformationen zuzugreifen, klicken oder tippen Sie auf der Seite „Fingerabdrücke“ auf **Verwaltungseinstellungen**.

- **Benutzerregistrierung** – Wählen Sie hier die minimal erforderliche und maximal zulässige Anzahl registrierter Fingerabdrücke für einen Benutzer aus.

- **Erkennung** – 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.

Fingerabdrücke – Benutzereinstellungen

Auf der Seite „Fingerabdrücke – Benutzereinstellungen“ können Sie Einstellungen bezüglich der Darstellung und des Verhaltens der Fingerabdruckerkennung konfigurieren.

▲ Um auf die Benutzereinstellungen für die Fingerabdruck-Anmeldeinformationen zuzugreifen, klicken oder tippen Sie auf der Seite „Fingerabdrücke“ auf **Benutzereinstellungen**.

- **Sound-Feedback aktivieren** – HP Client Security gibt akustische Signale aus, wenn ein Fingerabdruck durch Streichen über den Sensor registriert wurde, wobei für spezifische Programmereignisse verschiedene Signale verwendet werden. Sie können diesen Ereignissen auf der Registerkarte „Sounds“ in der Einstellung „Sound“ der Windows Systemsteuerung andere Töne zuweisen oder das Sound-Feedback ausschalten, indem Sie das Kontrollkästchen deaktivieren.
- **Feedback zur Scanqualität anzeigen** – Aktivieren Sie dieses Kontrollkästchen, wenn alle Scans unabhängig von ihrer Qualität angezeigt werden sollen. Um nur Fingerabdrücke guter Qualität anzuzeigen, deaktivieren Sie das Kontrollkästchen.

HP SpareKey – Kennwortwiederherstellung

Mit dem HP SpareKey können Sie auf Ihren Computer zugreifen, indem Sie drei Sicherheitsfragen beantworten. Diese Möglichkeit steht jedoch nur auf unterstützten Plattformen zur Verfügung.

Während der Erstinstallation werden Sie im Installationsassistenten für HP Client Security von HP Client Security aufgefordert, Ihren persönlichen HP SpareKey zu konfigurieren.

So konfigurieren Sie Ihren HP SpareKey:

1. Wählen Sie auf der Seite „HP SpareKey“ des Assistenten drei Sicherheitsfragen aus, und geben Sie dann zu jeder Frage eine Antwort ein.

   Sie können die Fragen aus einer vordefinierten Liste wählen oder Ihre eigenen Fragen formulieren.

2. Klicken oder tippen Sie auf **Registrieren**.

So löschen Sie Ihren HP SpareKey:

▲ Klicken oder tippen Sie auf **SpareKey löschen**.

Nach der Einrichtung können Sie mit dem SpareKey von einem beim Systemstart angezeigten Anmeldebildschirm für die Authentifizierung oder dem Windows Startbildschirm aus auf Ihren Computer zugreifen.

Auf der Seite „HP SpareKey“, auf die Sie über die Kachel „Kennwortwiederherstellung“ auf der Startseite von HP Client Security zugreifen, können Sie jederzeit andere Fragen auswählen oder Ihre Antworten ändern.

Um auf die Seite „HP SpareKey-Einstellungen“ zuzugreifen, auf der ein Administrator Einstellungen für die HP SpareKey-Anmeldeinformationen konfigurieren kann, klicken Sie auf **Einstellungen** (erfordert Administratorberechtigungen).

HP SpareKey-Einstellungen

Auf der Seite „HP SpareKey-Einstellungen“ können Sie Einstellungen bezüglich des Verhaltens und der Verwendung der HP SpareKey-Anmeldeinformationen konfigurieren.

▲ Um die Seite „HP SpareKey-Einstellungen“ zu öffnen, klicken oder tippen Sie auf der Seite „HP SpareKey“ auf **Einstellungen** (erfordert Administratorberechtigungen).

Administratoren können auf dieser Seite Folgendes konfigurieren:

- Fragen festlegen, die jedem Benutzer beim Einrichten des HP SpareKey präsentiert werden.
- Bis zu drei benutzerdefinierte Fragen zulassen, die zu der den Benutzern präsentierten Liste hinzugefügt werden können.
- Festlegen, ob es Benutzern möglich sein soll, ihre eigenen Sicherheitsfragen zu formulieren.
- Festlegen, welche Authentifizierungsumgebungen (Windows oder Systemstart) die Verwendung eines HP SpareKey für die Kennwortwiederherstellung zulassen sollen.

Windows Kennwort

Mit HP Client Security können Sie Ihr Windows Kennwort einfacher und schneller als mit der Windows Systemsteuerung ändern.

So ändern Sie Ihr Windows Kennwort:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf **Windows 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 diese Eingabe im Textfeld **Neues Kennwort bestätigen**.
4. Klicken Sie auf **Ändern**, um Ihr aktuelles Kennwort direkt durch das soeben eingegebene neue Kennwort zu ersetzen.

Bluetooth-Geräte

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

HINWEIS: Es werden nur Bluetooth-Telefone unterstützt.

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

Um auf die Seite „Einstellungen für Bluetooth-Geräte“ auf Seite 16 zuzugreifen, auf der ein Administrator Einstellungen für Bluetooth-Geräte konfigurieren kann, klicken Sie auf **Einstellungen** (erfordert Administratorberechtigungen).

Einstellungen für Bluetooth-Geräte

Administratoren können folgende Einstellungen bezüglich des Verhaltens und der Verwendung von Bluetooth-Geräten konfigurieren:

Unbeaufsichtigte Authentifizierung

- **Automatische Verwendung eines registrierten verbundenen Bluetooth-Geräts zur Identitätsüberprüfung zulassen** – Aktivieren Sie dieses Kontrollkästchen, um es Benutzern zu gestatten, Bluetooth-Geräte als Identitätsnachweis zur Authentifizierung zu verwenden, ohne

dass weitere Benutzerinteraktionen erforderlich sind, oder deaktivieren Sie es, um diese Option zu deaktivieren.

Bluetooth-Nähe

- **Computer sperren, wenn sich das registrierte Bluetooth-Geräte außerhalb der Reichweite Ihres Computers befindet** – Aktivieren Sie dieses Kontrollkästchen, um den Computer zu sperren, wenn ein während der Anmeldung verbundenes Bluetooth-Gerät den Bereich der Bluetooth-Reichweite verlässt, oder deaktivieren Sie es, um diese Option zu deaktivieren.

HINWEIS: Das Bluetooth-Modul Ihres Computers muss diese Fähigkeit unterstützen, damit diese Funktion genutzt werden kann.

Karten

HP Client Security kann verschiedene Arten von Identifizierungskarten unterstützen. Bei diesen Karten handelt es sich um kleine Plastikkarten mit integriertem Computerchip. Dazu zählen Smart Cards, kontaktlose Karten und Näherungskarten. Sofern das entsprechende Lesegerät mit dem Computer verbunden und eine Verbindung zwischen Karte und Lesegerät hergestellt ist, der Administrator den zugehörigen Treiber des Herstellers installiert und die Karte als Mittel der Authentifizierung aktiviert hat, können Sie diese Karte als Identitätsnachweis zur Authentifizierung verwenden.

Was Smart Cards betrifft, so sollten die Hersteller Tools zur Installation eines Sicherheitszertifikats und einer PIN-Verwaltung bereitstellen, die von HP Client Security für den Sicherheitsalgorithmus genutzt werden können. Anzahl und Art der für eine PIN verwendeten Zeichen können variieren. Ein Administrator muss die Smart Card initialisieren, bevor sie verwendet werden kann.

Folgende Smart Card-Formate werden von HP Client Security unterstützt:

- CSP
- PKCS11

Folgende Arten von kontaktlosen Karten werden von HP Client Security unterstützt:

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

Folgende Näherungskarten werden von HP Client Security unterstützt:

- HID-Näherungskarten

So registrieren Sie eine Smart Card:

1. Setzen Sie die Karte in ein angeschlossenes Smart Card-Lesegerät ein.
2. Sobald die Karte erkannt wird, geben Sie die PIN der Karte ein und klicken oder tippen Sie auf **Registrieren**.

So ändern Sie die PIN einer Smart Card:

1. Setzen Sie die Karte in ein angeschlossenes Smart Card-Lesegerät ein.
2. Sobald die Karte erkannt wird, geben Sie die PIN der Karte ein und klicken oder tippen Sie auf **Authentifizieren**.
3. Klicken oder tippen Sie auf **PIN ändern**, und geben Sie dann die neue PIN ein.

So registrieren Sie eine kontaktlose Karte oder eine Näherungskarte:

1. Platzieren Sie die Karte auf oder sehr nahe bei dem entsprechenden Lesegerät.
2. Sobald die Karte erkannt wird, klicken oder tippen Sie auf **Registrieren**.

So löschen Sie eine registrierte Karte:

1. Präsentieren Sie die Karte dem Lesegerät.
2. Nur bei Smart Cards: Geben Sie die der Karte zugewiesene PIN ein, und klicken oder tippen Sie auf **Authentifizieren**.
3. Klicken oder tippen Sie auf **Löschen**.

Sobald eine Karte registriert ist, werden Informationen zur Karte unter **Registrierte Karten** angezeigt. Wenn Sie eine Karte löschen, wird sie aus der Liste entfernt.

Um auf die Seite „Einstellungen für Näherungskarten, kontaktlose Karten und Smart Cards“ zuzugreifen, auf der ein Administrator Einstellungen für kartenbasierte Anmeldeinformationen konfigurieren kann, klicken Sie auf **Einstellungen** (erfordert Administratorberechtigungen).

Einstellungen für Näherungskarten, kontaktlose Karten und Smart Cards

Um auf die Einstellungen für eine Karte zuzugreifen, klicken oder tippen Sie zuerst auf die Karte in der Liste und dann auf den angezeigten Pfeil.

So ändern Sie die PIN einer Smart Card:

1. Präsentieren Sie die Karte dem Lesegerät.
2. Geben Sie die der Karte zugewiesene PIN ein, und klicken oder tippen Sie auf **Weiter**.
3. Geben Sie die neue PIN ein, bestätigen Sie diese und klicken oder tippen Sie auf **Weiter**.

So initialisieren Sie die PIN einer Smart Card:

1. Präsentieren Sie die Karte dem Lesegerät.
2. Geben Sie die der Karte zugewiesene PIN ein, und klicken oder tippen Sie auf **Weiter**.
3. Geben Sie die neue PIN ein, bestätigen Sie diese und klicken oder tippen Sie auf **Weiter**.
4. Klicken oder tippen Sie auf **Ja**, um die Initialisierung zu bestätigen.

So löschen Sie Kartendaten:

1. Präsentieren Sie die Karte dem Lesegerät.
2. Geben Sie die der Karte zugewiesene PIN ein (betrifft nur Smart Cards), und klicken oder tippen Sie auf **Weiter**.
3. Klicken oder tippen Sie auf **Ja**, um die Löschung zu bestätigen.

PIN

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

So richten Sie eine neue PIN ein:

- Geben Sie die PIN ein, bestätigen Sie diese durch erneute Eingabe, und klicken oder tippen Sie auf **Übernehmen**.

So löschen Sie eine PIN:

▲ Klicken oder tippen Sie auf **Löschen**, und klicken oder tippen Sie zur Bestätigung auf **Ja**.

Um auf die Seite „PIN-Einstellungen“ zuzugreifen, auf der ein Administrator Einstellungen für PIN-basierte Anmeldeinformationen konfigurieren kann, klicken Sie auf **Einstellungen** (erfordert Administratorberechtigungen).

PIN-Einstellungen

Auf der Seite „PIN-Einstellungen“ können Sie die minimal erforderliche und maximal zulässige Länge für die PIN-Anmeldeinformationen festlegen.

RSA SecurID

Wenn der Administrator RSA als Identitätsnachweis zur Authentifizierung aktiviert hat und die folgenden Bedingungen erfüllt sind, können Sie RSA SecurID-Anmeldeinformationen registrieren oder löschen.

HINWEIS: Hierfür sind entsprechende Einrichtungsvorgänge erforderlich.

- Für den Benutzer muss ein entsprechender Eintrag auf einem RSA-Server erstellt worden sein.
- Das dem Benutzer und dem Computer zugewiesene RSA SecurID-Token muss der RSA-Server-Domäne zugeordnet sein.
- Auf dem Computer ist SecurID-Software installiert.
- Es steht eine Verbindung zu dem ordnungsgemäß konfigurierten RSA-Server zur Verfügung.

So registrieren Sie RSA SecurID-Anmeldeinformationen:

▲ Geben Sie Ihren RSA SecurID-Benutzernamen und den Passcode (RSA SecurID-Tokencode oder PIN plus Tokencode, je nach Umgebung) ein, und klicken oder tippen Sie dann auf **Übernehmen**.

Nach erfolgreicher Registrierung wird die Meldung „Ihre RSA SecurID-Anmeldeinformationen wurden erfolgreich registriert“ angezeigt, und die Schaltfläche „Löschen“ ist verfügbar.

So löschen Sie RSA SecurID-Anmeldeinformationen:

▲ Klicken Sie auf **Löschen**. Ein Popup-Dialogfeld mit der Frage „Möchten Sie Ihre RSA SecurID-Anmeldeinformationen wirklich löschen?“ wird angezeigt. Klicken Sie auf **Ja**.

Password Manager

Die Anmeldung bei Websites und Anwendungen wird einfacher und sichererer, wenn Sie Password Manager verwenden. Sie können Kennwörter mit höherer Sicherheit erstellen, die Sie sich nicht notieren oder merken müssen, und sich dann schnell und problemlos unter Verwendung eines Fingerabdrucks, einer Smart Card, Näherungskarte oder kontaktlosen Karte, eines Bluetooth-Telefons, einer PIN, Ihrer RSA-Anmeldeinformationen oder Ihres Windows Kennworts anmelden.

HINWEIS: Aufgrund des sich ständig ändernden Aufbaus von Anmeldebildschirmen im Internet kann Password Manager möglicherweise nicht immer alle Websites unterstützen.

Password Manager bietet folgende Optionen:

Seite „Password Manager“

- Klicken oder tippen Sie auf ein Konto, um automatisch eine Webseite oder Anwendung zu öffnen und sich anzumelden.
- Organisieren Sie Ihre Konten nach Kategorien.

Kennwortsicherheit

- Auf einen Blick erkennen, ob eines Ihrer Kennwörter ein Sicherheitsrisiko birgt.
- Überprüfen Sie beim Hinzufügen von Anmeldeinformationen die Sicherheit einzelner Kennwörter, die für Websites und Anwendungen verwendet werden.
- Die Kennwortsicherheit wird mittels roter, gelber oder grüner Statusindikatoren dargestellt.

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

▲ Klicken oder tippen Sie auf das **Password Manager**-Symbol, um ein Kontextmenü mit folgenden Optionen zur Auswahl anzuzeigen:

- [Domänenname] zu Password Manager hinzufügen
- Password Manager öffnen
- Symboleinstellungen
- Hilfe

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

Folgende Optionen werden im Kontextmenü angezeigt:

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

Für Webseiten oder Programme, für die bereits Anmeldeinformationen festgelegt wurden

Folgende Optionen werden im Kontextmenü angezeigt:

- **Anmeldeinformationen eingeben** – Zeigt die Seite **Identität bestätigen** an. Wenn Sie sich erfolgreich authentifiziert haben, werden Ihre Anmeldeinformationen in die Anmeldefelder eingefügt und die Seite wird übermittelt (sofern die Übermittlung beim Erstellen oder bei der letzten Änderung der Anmeldeinformationen festgelegt wurde).
- **Anmeldeinformationen bearbeiten** – Hiermit können Sie Ihre Anmeldeinformationen für diese Website bearbeiten.
- **Anmeldeinformationen hinzufügen** – Hiermit können Sie ein Konto zu Password Manager hinzufügen.

- **Password Manager öffnen** – Startet Password Manager.
- **Hilfe** – Öffnet die Hilfe für HP Client Security.

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

Hinzufügen von Anmeldeinformationen

Sie können problemlos Anmeldeinformationen für eine Website oder ein Programm hinzufügen, indem Sie diese einmal eingeben. Ab diesem Zeitpunkt gibt Password Manager diese Informationen automatisch für Sie ein. Sie können diese Anmeldeinformationen anschließend benutzen, wenn Sie im Internet die Website besuchen oder das Programm aufrufen.

So fügen Sie Anmeldeinformationen hinzu:

1. Öffnen Sie den Anmeldebildschirm für eine Website oder ein Programm.
2. Klicken oder tippen Sie auf das **Password Manager**-Symbol, und klicken oder tippen Sie dann auf eine der folgenden Optionen, je nachdem, ob es sich um den Anmeldebildschirm einer Website oder eines Programms handelt.
   - Klicken oder tippen Sie im Falle einer Website auf **[Domänenname] zu Password Manager hinzufügen**.
   - Klicken oder tippen Sie im Falle eines Programms auf **Diesen Anmeldebildschirm zu Password Manager hinzufügen**.
3. Geben Sie Ihre Anmeldedaten ein. Anmeldefelder auf dem Bildschirm und die entsprechenden Felder im Dialogfeld sind mit einer fett formatierten orangefarbenen Umrandung gekennzeichnet.
   a. Um ein Anmeldefeld mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken oder tippen Sie auf die Pfeile rechts neben dem Feld.
   b. Um das Kennwort für diese Anmeldeinformationen anzuzeigen, klicken oder tippen Sie auf **Kennwort einblenden**.
   c. Um die Anmeldefelder automatisch auszufüllen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldeinformationen automatisch senden**.
   d. Klicken oder tippen Sie auf **OK**, um die gewünschte Authentifizierungsmethode (Fingerabdruck, Smart Card, Näherungskarte, kontaktlose Karte, Bluetooth-Telefon, PIN oder Kennwort) auszuwählen. Melden Sie sich dann mit dieser Methode an.

      Das Pluszeichen wird vom **Password Manager**-Symbol entfernt, um anzuzeigen, dass die Anmeldeinformationen erstellt wurden.
   e. Falls Password Manager die Anmeldefelder nicht erkennt, klicken oder tippen Sie auf **Weitere Felder**.
      - Aktivieren Sie das Kontrollkästchen für jedes Feld, das für die Anmeldung erforderlich ist, bzw. deaktivieren Sie das Kontrollkästchen für jedes Feld, das nicht für die Anmeldung erforderlich ist.
      - Klicken oder tippen Sie auf **Schließen**.

Ab jetzt wird bei jedem Zugriff auf die Website oder Öffnen des Programms das **Password Manager**-Symbol links oben auf dem Anmeldebildschirm der Website bzw. Anwendung angezeigt. Es weist darauf hin, dass Sie Ihre registrierten Anmeldeinformationen für die Anmeldung verwenden können.

Bearbeiten von Anmeldeinformationen

So bearbeiten Sie Anmeldeinformationen:

1. Öffnen Sie den Anmeldebildschirm für eine Website oder ein Programm.
2. Um ein Dialogfeld anzuzeigen, in dem Sie Ihre Anmeldedaten bearbeiten können, klicken oder tippen Sie auf den Pfeil auf dem **Password Manager**-Symbol und anschließend auf **Anmeldeinformationen bearbeiten**.

   Anmeldefelder auf dem Bildschirm und die entsprechenden Felder im Dialogfeld sind mit einer fett formatierten orangefarbenen Umrandung gekennzeichnet.

   Sie können auch Kontoinformationen von der Seite „Password Manager“ aus bearbeiten, indem Sie auf die Anmeldeinformationen klicken oder tippen, um die Bearbeitungsoptionen anzuzeigen, und dann **Bearbeiten** auswählen.
3. Bearbeiten Sie Ihre Anmeldeinformationen.
   - Um den Kontonamen zu bearbeiten, geben Sie einen neuen Namen in das Feld **Kontoname** ein.
   - Um den Namen einer **Kategorie** zu bearbeiten oder einen neuen Namen hinzuzufügen, ändern Sie den Namen im Feld **Kategorie** oder geben Sie den neuen Namen ein.
   - Um ein Anmeldefeld **Benutzername** mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken oder tippen Sie auf den Pfeil nach unten rechts neben dem Feld.

     Vorformatierte Auswahlmöglichkeiten sind nur dann verfügbar, wenn die Anmeldeinformationen unter Verwendung des Befehls „Bearbeiten“ im Kontextmenü des Password Manager-Symbols bearbeitet werden.
   - Um ein Anmeldefeld **Kennwort** mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken oder tippen Sie auf den Pfeil nach unten rechts neben dem Feld.

     Vorformatierte Auswahlmöglichkeiten sind nur dann verfügbar, wenn die Anmeldeinformationen unter Verwendung des Befehls „Bearbeiten“ im Kontextmenü des Password Manager-Symbols bearbeitet werden.
   - Um weitere Felder vom Bildschirm zu Ihren Anmeldeinformationen hinzuzufügen, klicken oder tippen Sie auf **Weitere Felder**.
   - Um das Kennwort für diese Anmeldeinformationen anzuzeigen, klicken oder tippen Sie auf das Symbol **Kennwort einblenden**.
   - Um die Anmeldefelder automatisch auszufüllen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldeinformationen automatisch senden**.
   - Um Anmeldeinformationen als mit einem kompromittierten Kennwort behaftet zu kennzeichnen, aktivieren Sie das Kontrollkästchen **Dieses Kennwort ist kompromittiert**.

     Nachdem alle Änderungen gespeichert sind, werden sämtliche anderen Anmeldeinformationen, die dasselbe Kennwort nutzen, ebenfalls als kompromittiert gekennzeichnet. Sie können dann jedes betroffene Konto besuchen und die Kennwörter nach Bedarf ändern.
4. Klicken oder tippen Sie auf **OK**.

Verwenden des Password Manager-Menüs „Verknüpfungen“

Password Manager ermöglicht es Ihnen, auf schnelle und einfache Weise Websites aufzurufen und Programme zu starten, für die Sie Anmeldeinformationen festgelegt haben. Doppelklicken oder

doppeltippen Sie einfach im Password Manager-Menü **Verknüpfungen** oder auf der Seite „Password Manager“ in HP Client Security auf ein Programm oder eine Website, um den Anmeldebildschirm zu öffnen, wo Sie dann Ihre Anmeldeinformationen eingeben.

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

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

- ▲ Drücken Sie die Tastenkombination für **Password Manager** (die Werkseinstellung lautet Ctrl +Windows Taste+h). Zum Ändern der Tastenkombination klicken oder tippen Sie auf der Startseite von HP Client Security auf **Password Manager** und anschließend auf **Einstellungen**.

Organisieren von Anmeldeinformationen nach Kategorien

Erstellen Sie zum Ordnen Ihrer Anmeldeinformationen eine oder mehrere Kategorien.

So ordnen Sie Anmeldeinformationen einer Kategorie zu:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf **Password Manager**.
2. Klicken oder tippen Sie auf einen Kontoeintrag und anschließend auf **Bearbeiten**.
3. Geben Sie in das Feld **Kategorie** den Namen einer Kategorie ein.
4. Klicken oder tippen Sie auf **Speichern**.

So entfernen Sie ein Konto aus einer Kategorie:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf **Password Manager**.
2. Klicken oder tippen Sie auf einen Kontoeintrag und anschließend auf **Bearbeiten**.
3. Löschen Sie im Feld **Kategorie** den Namen einer Kategorie.
4. Klicken oder tippen Sie auf **Speichern**.

So benennen Sie eine Kategorie um:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf **Password Manager**.
2. Klicken oder tippen Sie auf einen Kontoeintrag und anschließend auf **Bearbeiten**.
3. Ändern Sie im Feld **Kategorie** den Namen der Kategorie.
4. Klicken oder tippen Sie auf **Speichern**.

Verwalten der Anmeldeinformationen

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

Ihre Anmeldeinformationen werden auf der Seite „Password Manager“ aufgeführt.

So verwalten Sie Ihre Anmeldeinformationen:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf **Password Manager**.
2. Klicken oder tippen Sie auf vorhandene Anmeldeinformationen, wählen Sie eine der folgenden Optionen aus, und folgen Sie dann den Anweisungen auf dem Bildschirm:
   - **Bearbeiten** – Ermöglicht die Bearbeitung von Anmeldedaten. Weitere Informationen finden Sie unter „Bearbeiten von Anmeldeinformationen“ auf Seite 22.
   - **Anmelden** – Zum Anmelden beim ausgewählten Konto.
   - **Löschen** – Zum Löschen der Anmeldeinformationen für das ausgewählte Konto.

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

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

Beim Erstellen von Password Manager-Anmeldeinformationen für ein Konto wird während der Kennworteingabe unterhalb des Kennworts ein farbiger Balken eingeblendet, der den Sicherheitsgrad des Kennworts anzeigt. Die Farben signalisieren folgende Einstufungen:

- **Rot** – Niedrig
- **Gelb** – Ausreichend
- **Grün** – Hoch

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 Anmeldeinformationen erstellt

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

1. Klicken oder tippen Sie auf das Pfeilsymbol und anschließend auf **Symboleinstellungen**, um festzulegen, wie Password Manager mögliche Websites mit Anmeldung handhabt.

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

2. Verfahren Sie wie folgt, um Anmeldeinformationen für einen zuvor ausgeschlossenen Anmeldebildschirm hinzuzufügen:

   a. Melden Sie sich bei der bisher ausgeschlossenen Website an.

   b. Wenn sich Password Manager das Kennwort für diese Website merken soll, klicken oder tippen Sie im Popup-Dialogfeld auf **Merken**, um das Kennwort zu speichern und Anmeldeinformationen für den Anmeldebildschirm zu erstellen.

3. Um auf weitere Password Manager-Einstellungen zuzugreifen, klicken oder tippen Sie auf das Password Manager-Symbol, auf **Password Manager öffnen** und dann auf der Seite „Password Manager“ auf **Einstellungen**.

Importieren und Exportieren von Anmeldeinformationen

Auf der Seite „Import und Export“ von HP Password Manager können Sie Anmeldeinformationen importieren, die von Internetbrowsern auf Ihrem Computer gespeichert wurden. Außerdem können Sie Daten aus einer HP Client Security-Sicherungsdatei importieren sowie Daten in eine HP Client Security-Sicherungsdatei exportieren.

▲ Um die Seite „Import und Export“ zu öffnen, klicken oder tippen Sie auf der Seite „Password Manager“ auf **Import und Export**.

So importieren Sie Kennwörter von einem Browser:

1. Klicken oder tippen Sie auf den Browser, von dem Sie Kennwörter importieren möchten (es werden nur installierte Browser angezeigt).
2. Deaktivieren Sie das Kontrollkästchen für jedes Konto, für das Sie keine Kennwörter importieren möchten.
3. Klicken oder tippen Sie auf **Importieren**.

Das Importieren von Daten aus einer HP Client Security-Sicherungsdatei und das Exportieren von Daten in eine HP Client Security-Sicherungsdatei kann über die zugehörigen Links unter **Weitere Optionen** auf der Seite „Import und Export“ durchgeführt werden.

HINWEIS: Mit diesen Funktionen werden lediglich Password Manager-Daten importiert bzw. exportiert. Informationen zum Sichern und Wiederherstellen von weiteren HP Client Security-Daten finden Sie unter „Sichern und Wiederherstellen Ihrer Daten“ auf Seite 30.

So importieren Sie Daten aus einer HP Client Security-Sicherungsdatei:

1. Klicken oder tippen Sie auf der Seite „Import und Export“ von HP Password Manager auf **Daten aus einer HP Client Security-Sicherungsdatei importieren**.
2. Bestätigen Sie Ihre Identität.
3. Wählen Sie die zuvor erstellte Sicherungsdatei aus oder geben Sie den entsprechenden Pfad in das dafür bereitgestellte Feld ein, und klicken oder tippen Sie auf **Durchsuchen**.
4. Geben Sie das zum Schutz der Datei verwendete Kennwort ein, und klicken oder tippen Sie auf **Weiter**.
5. Klicken oder tippen Sie auf **Wiederherstellen**.

So exportieren Sie Daten in eine HP Client Security-Sicherungsdatei:

1. Klicken oder tippen Sie auf der Seite „Import und Export“ von HP Password Manager auf **Daten in eine HP Client Security-Sicherungsdatei exportieren**.
2. Bestätigen Sie Ihre Identität, und klicken oder tippen Sie auf **Weiter**.
3. Geben Sie einen Namen für die Sicherungsdatei ein. Die Datei wird standardmäßig im Ordner „Dokumente“ gespeichert. Um einen anderen Speicherort anzugeben, klicken oder tippen Sie auf **Durchsuchen**.
4. Geben Sie ein Kennwort zum Schutz der Datei ein, bestätigen Sie es und klicken oder tippen Sie auf **Speichern**.

Einstellungen

Sie können Einstellungen zur Personalisierung von Password Manager vornehmen:

- **Zum Hinzufügen von Anmeldeinformationen 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 Anmeldeinformationen für diesen Anmeldebildschirm im Menü **Anmeldeinformationen** hinterlegen können.

  Wenn diese Funktion nicht ausgeführt werden soll, deaktivieren Sie das Kontrollkästchen neben **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern**.

- **Password Manager mit Strg+Win+h öffnen** – Die Standardtastenkombination zum Öffnen des Menüs **Password Manager Verknüpfungen** lautet Strg+Windows-Taste+h.

  Zum Ändern der Tastenkombination klicken oder tippen 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.

  Für Windows oder Windows Anwendungen reservierte Tastenkombinationen können nicht verwendet werden.

- Um die Einstellungen auf die werksseitig eingestellten Standardwerte zurückzusetzen, klicken oder tippen Sie auf **Standardeinstellungen wiederherstellen**.

Erweiterte Einstellungen

Administratoren können auf die folgenden Optionen zugreifen, indem sie auf der Startseite von HP Client Security das **Zahnrad**-Symbol (für Einstellungen) auswählen.

- **Administratorrichtlinien** – Ermöglicht das Konfigurieren von Anmelde- und Sitzungsrichtlinien für Administratoren.
- **Standardbenutzer-Richtlinien** – Ermöglicht das Konfigurieren von Anmelde- und Sitzungsrichtlinien für Standardbenutzer.
- **Sicherheitsfunktionen** – Ermöglicht Ihnen, die Sicherheit Ihres Computers zu erhöhen, indem Sie Ihr Windows Konto durch starke Authentifizierung und/oder Authentifizierung vor dem Starten von Windows schützen.
- **Benutzer**- Ermöglicht die Verwaltung von Benutzern und ihren Anmeldedaten.
- **Meine Richtlinien** – Ermöglicht die Überprüfung Ihrer Authentifizierungsrichtlinien und Ihres Registrierungsstatus.
- **Sichern und Wiederherstellen** – Ermöglicht die Sicherung und Wiederherstellung von HP Client Security-Daten.
- **Info** – Zeigt Versionsinformationen zu HP Client Security an.

Administratorrichtlinien

Sie können Anmelde- und Sitzungsrichtlinien für Administratoren dieses Computers konfigurieren. Hier festgelegte Anmelderichtlinien regeln die Anmeldeinformationen, die ein lokaler Administrator für die Anmeldung bei Windows benötigt. Hier festgelegte Sitzungsrichtlinien regeln die Anmeldeinformationen, die ein lokaler Administrator für die Identitätsüberprüfung innerhalb einer Windows Sitzung benötigt.

Standardmäßig werden alle neuen oder geänderten Richtlinien direkt nach dem Tippen oder Klicken auf **Übernehmen** durchgesetzt.

So fügen Sie eine neue Richtlinie hinzu:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf das **Zahnrad**-Symbol.
2. Klicken oder tippen Sie auf der Seite „Erweiterte Einstellungen“ auf **Administratorrichtlinien**.
3. Klicken oder tippen Sie auf **Neue Richtlinie hinzufügen**.
4. Klicken Sie auf die Pfeile nach unten, um primäre und (optional) sekundäre Anmeldeinformationen für die neue Richtlinie auszuwählen, und klicken oder tippen Sie dann auf **Hinzufügen**.
5. Klicken Sie auf **Übernehmen**.

So verzögern Sie die Durchsetzung einer neuen oder geänderten Richtlinie:

1. Klicken oder tippen Sie auf **Diese Richtlinie sofort durchsetzen**.
2. Wählen Sie **Diese Richtlinie zum angegebenen Datum durchsetzen** aus.
3. Wählen Sie mithilfe des Popup-Kalenders ein Datum für die Durchsetzung dieser Richtlinie aus, oder geben Sie ein Datum dafür ein.
4. Wählen Sie ggf. aus, wann Benutzer an die neue Richtlinie erinnert werden sollen.
5. Klicken Sie auf **Übernehmen**.

Richtlinien für Standardbenutzer

Sie können Anmelde- und Sitzungsrichtlinien für Standardbenutzer dieses Computers konfigurieren. Hier festgelegte Anmelderichtlinien regeln die Anmeldeinformationen, die ein Standardbenutzer für die Anmeldung bei Windows benötigt. Hier festgelegte Sitzungsrichtlinien regeln die Anmeldeinformationen, die ein Standardbenutzer für die Identitätsüberprüfung innerhalb einer Windows Sitzung benötigt.

Standardmäßig werden alle neuen oder geänderten Richtlinien direkt nach dem Tippen oder Klicken auf **Übernehmen** durchgesetzt.

So fügen Sie eine neue Richtlinie hinzu:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf das **Zahnrad**-Symbol.
2. Klicken oder tippen Sie auf der Seite „Erweiterte Einstellungen“ auf **Richtlinien für Standardbenutzer**.
3. Klicken oder tippen Sie auf **Neue Richtlinie hinzufügen**.
4. Klicken Sie auf die Pfeile nach unten, um primäre und (optional) sekundäre Anmeldeinformationen für die neue Richtlinie auszuwählen, und klicken oder tippen Sie dann auf **Hinzufügen**.
5. Klicken Sie auf **Übernehmen**.

So verzögern Sie die Durchsetzung einer neuen oder geänderten Richtlinie:

1. Klicken oder tippen Sie auf **Diese Richtlinie sofort durchsetzen**.
2. Wählen Sie **Diese Richtlinie zum angegebenen Datum durchsetzen** aus.
3. Wählen Sie mithilfe des Popup-Kalenders ein Datum für die Durchsetzung dieser Richtlinie aus, oder geben Sie ein Datum dafür ein.
4. Wählen Sie ggf. aus, wann Benutzer an die neue Richtlinie erinnert werden sollen.
5. Klicken Sie auf **Übernehmen**.

Sicherheitsfunktionen

Mit HP Client Security stehen Ihnen Sicherheitsfunktionen zur Verfügung, die vor unberechtigtem Zugriff auf den Computer schützen.

So richten Sie Sicherheitsfunktionen ein:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf das **Zahnrad**-Symbol.
2. Klicken oder tippen Sie auf der Seite „Erweiterte Einstellungen“ auf **Sicherheitsfunktionen**.

3. Aktivieren Sie die Sicherheitsfunktionen durch Auswahl der entsprechenden Kontrollkästchen, und klicken Sie dann auf **Übernehmen**. Je mehr Funktionen Sie auswählen, desto sicherer ist Ihr Computer.

   Die hier vorgenommenen Einstellungen gelten für alle Benutzer.

   - **Windows Anmeldesicherheit** – Schützt Ihre Windows Konten, indem es dafür sorgt, dass der Zugriff nur mit Anmeldeinformationen von HP Client Security möglich ist.
   - **Systemstart-Sicherheit** (Authentifizierung beim Systemstart) – Schützt Ihren Computer vor dem Starten von Windows. Diese Option steht nur dann zur Verfügung, wenn sie vom BIOS unterstützt wird.
   - **One-Step-Anmeldung zulassen** – Diese Einstellung ermöglicht es, die Windows Anmeldung zu überspringen, wenn die Authentifizierung zuvor beim Systemstart oder über den Drive Encryption-Mechanismus erfolgt ist.

4. Klicken oder tippen Sie auf **Benutzer** und anschließend auf die Kachel des Benutzers.

Benutzer

Sie können die HP Client Security-Benutzer dieses Computers überwachen und verwalten.

So fügen Sie einen weiteren Windows Benutzer zu HP Client Security hinzu:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf das **Zahnrad**-Symbol.
2. Klicken oder tippen Sie auf der Seite „Erweiterte Einstellungen“ auf **Benutzer**.
3. Klicken oder tippen Sie auf **Weiteren Windows Benutzer zu HP Client Security hinzufügen**.
4. Geben Sie den Namen des Benutzers ein, der hinzugefügt werden soll, und klicken oder tippen Sie dann auf **OK**.
5. Geben Sie das Windows Kennwort des Benutzers ein.

   Auf der Seite „Benutzer“ wird eine Kachel für den hinzugefügten Benutzer angezeigt.

So löschen Sie einen Windows Benutzer in HP Client Security:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf das **Zahnrad**-Symbol.
2. Klicken oder tippen Sie auf der Seite „Erweiterte Einstellungen“ auf **Benutzer**.
3. Klicken oder tippen Sie auf den Namen des Benutzers, der gelöscht werden soll.
4. Klicken oder tippen Sie auf **Benutzer löschen**, und klicken oder tippen Sie zur Bestätigung auf **Ja**.

So zeigen Sie eine Zusammenfassung der für einen Benutzer durchgesetzten Anmelde- und Sitzungsrichtlinien an:

▲ Klicken oder tippen Sie auf **Benutzer** und anschließend auf die Kachel des Benutzers.

Meine Richtlinien

Sie können Ihre Authentifizierungsrichtlinien und Ihren Registrierungsstatus anzeigen. Auf der Seite „Meine Richtlinien“ finden sich außerdem Links zu den Seiten „Administratorrichtlinien“ und „Richtlinien für Standardbenutzer“.

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf das **Zahnrad**-Symbol.
2. Klicken oder tippen Sie auf der Seite „Erweiterte Einstellungen“ auf **Meine Richtlinien**.

   Die für den zurzeit angemeldeten Benutzer durchgesetzten Anmelde- und Sitzungsrichtlinien werden angezeigt.

Auf der Seite „Meine Richtlinien“ werden außerdem Links zu „Administratorrichtlinien“ auf Seite 27 und „Richtlinien für Standardbenutzer“ auf Seite 28 bereitgestellt.

Sichern und Wiederherstellen Ihrer Daten

Es wird empfohlen, regelmäßig eine Sicherungskopie der HP Client Security-Daten zu erstellen. Wie oft dies erforderlich ist, hängt davon ab, wie häufig sich die Daten ändern. Wenn Sie beispielsweise täglich neue Anmeldeinformationen 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 von Password Manager gesichert. Drive Encryption benutzt eine eigene Sicherungsmethode. Daten der Anwendung Device Access Manager sowei Daten für die Authentifizierung per Fingerabdruck werden nicht gesichert.

HP Client Security muss auf jedem Computer installiert sein, auf dem gesicherte Daten gespeichert werden sollen. Andernfalls können die Daten aus der Sicherungskopie nicht wiederhergestellt werden.

So sichern Sie Ihre Daten:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf das **Zahnrad**-Symbol.
2. Klicken oder tippen Sie auf der Seite „Erweiterte Einstellungen“ auf **Administratorrichtlinien**.
3. Klicken oder tippen Sie auf **Sichern und Wiederherstellen**.
4. Klicken oder tippen Sie auf **Sichern**, und bestätigen Sie anschließend Ihre Identität.
5. Wählen Sie das in die Sicherung einzuschließende Modul aus, und klicken oder tippen Sie dann auf **Weiter**.
6. Geben Sie einen Namen für die Speicherdatei ein. Die Datei wird standardmäßig im Ordner „Dokumente“ gespeichert. Um einen anderen Speicherort anzugeben, klicken oder tippen Sie auf **Durchsuchen**.
7. Geben Sie ein Kennwort zum Schützen der Datei ein.
8. Klicken oder tippen Sie auf **Speichern**.

So stellen Sie Ihre Daten wieder her:

1. Klicken oder tippen Sie auf der Startseite von HP Client Security auf das **Zahnrad**-Symbol.
2. Klicken oder tippen Sie auf der Seite „Erweiterte Einstellungen“ auf **Administratorrichtlinien**.
3. Klicken oder tippen Sie auf **Sichern und Wiederherstellen**.
4. Wählen Sie **Wiederherstellen** aus, und bestätigen Sie Ihre Identität.
5. Wählen Sie die zuvor erstellte Speicherdatei aus. Geben Sie den Pfad in das entsprechende Feld ein. Um einen anderen Speicherort anzugeben, klicken oder tippen Sie auf **Durchsuchen**.
6. Geben Sie das zum Schutz der Datei verwendete Kennwort ein, und klicken oder tippen Sie auf **Weiter**.

7. Wählen Sie die Module aus, deren Daten wiederhergestellt werden sollen.
8. Klicken oder tippen Sie auf **Wiederherstellen**.

5 HP Drive Encryption (bestimmte Modelle)

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

Über den Startbildschirm von HP Client Security können Windows Administratoren Drive Encryption aktivieren, den Verschlüsselungsschlüssel sichern sowie Festplatten oder Partitionen für die Verschlüsselung auswählen bzw. diese Auswahl aufheben. Weitere Informationen finden Sie in der Hilfe zur HP Client Security-Software.

Die folgenden Aufgaben können mit Drive Encryption durchgeführt werden:

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

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

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

Öffnen von Drive Encryption

Administratoren können durch Öffnen von HP Client Security auf Drive Encryption zugreifen:

1. Klicken oder tippen Sie im Startbildschirm auf die App **HP Client Security** (Windows 8).

   – oder –

   Doppelklicken oder doppeltippen Sie auf dem Windows Desktop auf das Symbol **HP Client Security** im Infobereich außen rechts in der Taskleiste.

2. Klicken oder tippen Sie auf das **Drive Encryption**-Symbol.

Allgemeine Aufgaben

Aktivieren von Drive Encryption für Standard-Festplatten

Standard-Festplatten werden mit Softwareverschlüsselung verschlüsselt. Gehen Sie wie folgt vor, um ein Laufwerk bzw. eine Laufwerkspartition zu verschlüsseln:

1. Starten Sie **Drive Encryption**. Weitere Informationen finden Sie unter „Öffnen von Drive Encryption“ auf Seite 32.
2. Aktivieren Sie das Kontrollkästchen für die zu verschlüsselnde Festplatte bzw. Partition, und klicken oder tippen Sie auf **Schlüssel sichern**.

HINWEIS: Aktivieren Sie zur Erhöhung der Sicherheit das Kontrollkästchen **Energiesparmodus für höhere Sicherheit deaktivieren**. Bei deaktiviertem Energiesparmodus gibt es absolut kein Risiko, dass die Anmeldeinformationen zum Entsperren des Laufwerks im Arbeitsspeicher gespeichert werden.

3. Wählen Sie eine oder mehrere Sicherheitsoptionen aus, und klicken oder tippen Sie auf **Sichern**. Weitere Informationen finden Sie unter „Sichern von Verschlüsselungsschlüsseln“ auf Seite 37.
4. Während der Sicherung des Verschlüsselungsschlüssels können Sie weiterarbeiten. Solange dieser Vorgang andauert, sollten Sie jedoch keinen Neustart Ihres Computers durchführen.

HINWEIS: Nach dem Abschluss des Vorgangs werden Sie dazu aufgefordert, den Computer neu zu starten. Während des Neustarts wird vor dem Hochfahren der Authentifizierungsbildschirm von Drive Encryption angezeigt, über den Sie sich vor dem Start von Windows authentifizieren müssen.

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

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

Aktivieren von Drive Encryption für selbstverschlüsselnde Laufwerke

Selbstverschlüsselnde Laufwerke nach den OPAL-Spezifikationen der Trusted Computing Group für die Verwaltung selbstverschlüsselnder Laufwerke lassen sich entweder mit Software- oder mit Hardware-Verschlüsselung verschlüsseln. Hardware-Verschlüsselung ist erheblich schneller als Software-Verschlüsselung. Dabei können Sie allerdings nicht auswählen, welche Laufwerkspartitionen Sie verschlüsseln möchten. Das gesamte Laufwerk und alle Partitionen werden verschlüsselt.

Zur Verschlüsselung ausgewählter Partitionen ist Software-Verschlüsselung erforderlich. Deaktivieren Sie daher unbedingt das Kontrollkästchen **Nur Hardware-Verschlüsselung für selbstverschlüsselnde Festplatten (SEDs) zulassen**.

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

1. Starten Sie **Drive Encryption**. Weitere Informationen finden Sie unter „Öffnen von Drive Encryption“ auf Seite 32.
2. Aktivieren Sie das Kontrollkästchen für die zu verschlüsselnde Festplatte, und klicken oder tippen Sie auf **Schlüssel sichern**.

HINWEIS: Aktivieren Sie zur Erhöhung der Sicherheit das Kontrollkästchen **Energiesparmodus für höhere Sicherheit deaktivieren**. Bei deaktiviertem Energiesparmodus gibt es absolut kein Risiko, dass die Anmeldeinformationen zum Entsperren des Laufwerks im Arbeitsspeicher gespeichert werden.

3. Wählen Sie eine oder mehrere Sicherheitsoptionen aus, und klicken oder tippen Sie auf **Sichern**. Weitere Informationen finden Sie unter „Sichern von Verschlüsselungsschlüsseln“ auf Seite 37.
4. Während der Sicherung des Verschlüsselungsschlüssels können Sie weiterarbeiten. Solange dieser Vorgang andauert, sollten Sie jedoch keinen Neustart Ihres Computers durchführen.

HINWEIS: Bei selbstverschlüsselnden Festplatten werden Sie aufgefordert, den Computer herunterzufahren.

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

Deaktivieren von Drive Encryption

1. Starten Sie **Drive Encryption**. Weitere Informationen finden Sie unter „Öffnen von Drive Encryption“ auf Seite 32.
2. Deaktivieren Sie bei allen verschlüsselten Festplatten das entsprechende Kontrollkästchen, und klicken Sie dann auf **Übernehmen**.

   Die Deaktivierung von Drive Encryption wird gestartet.

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

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

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

Anmelden, nachdem Drive Encryption aktiviert wurde

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

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

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

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

Anmeldung eines einzelnen Benutzers:

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

Anmeldung mehrerer Benutzer:

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

HINWEIS: Folgende Smart Cards werden unterstützt:

Unterstützte Smart Cards

- Gemalto Cyberflex Access 64k V2c

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

Verschlüsseln zusätzlicher Festplatten

Es wird empfohlen, HP Drive Encryption zu verwenden, um Daten durch Verschlüsselung der Festplatte zu schützen. Nach der Aktivierung können alle hinzugefügten Festplatten oder Partitionen folgendermaßen verschlüsselt werden:

1. Starten Sie **Drive Encryption**. Weitere Informationen finden Sie unter „Öffnen von Drive Encryption“ auf Seite 32.
2. Wählen Sie für Laufwerke mit Software-Verschlüsselung die zu verschlüsselnden Laufwerkspartitionen aus.

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

– oder –

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

Erweiterte Aufgaben

Verwalten von Drive Encryption (Administrator-Aufgabe)

Administratoren können mithilfe von Drive Encryption den Verschlüsselungsstatus (Verschlüsselt oder Nicht verschlüsselt) aller Festplatten des Computers anzeigen und ändern.

- Wenn der Status „Aktiviert“ lautet, wurde Drive Encryption aktiviert und konfiguriert. Das Laufwerk befindet sich in einem der folgenden Zustände:

Software-Verschlüsselung

- Nicht verschlüsselt
- verschlüsselt
- wird gerade verschlüsselt
- wird gerade entschlüsselt

Hardware-Verschlüsselung

- Verschlüsselt
- Nicht verschlüsselt (für zusätzliche Festplatten)

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

Administratoren können mithilfe von Drive Encryption eine oder mehrere Festplattenpartitionen auf dem Computer verschlüsseln oder bereits verschlüsselte Festplattenpartitionen entschlüsseln.

1. Starten Sie **Drive Encryption**. Weitere Informationen finden Sie unter „Öffnen von Drive Encryption“ auf Seite 32.
2. Aktivieren oder deaktivieren Sie unter **Laufwerkstatus** das Kontrollkästchen für jede Festplattenpartition, die ver- oder entschlüsselt werden soll, und klicken oder tippen Sie dann auf **Übernehmen**

HINWEIS: Während der Ver- oder Entschlüsselung einer Partition wird eine Fortschrittsanzeige angezeigt, auf der zu sehen ist, zu wie viel Prozent die Partition verschlüsselt ist.

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

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

Festplattenverwaltung

- **Spitzname** – Sie können Ihren Festplatten oder Partitionen zur leichteren Identifizierung einen Namen zuweisen.
- **Getrennte Laufwerke** – Drive Encryption kann Festplatten nachverfolgen, die aus dem Computer entfernt werden. Eine aus dem Computer entfernte Festplatte wird automatisch in die „Getrennt“-Liste verschoben. Sobald die Festplatte wieder im System installiert ist, wird es erneut in der „Verbunden“-Liste angezeigt.

- Wenn Sie die getrennte Festplatte nicht mehr nachverfolgen oder verwalten müssen, können Sie sie aus der „Getrennt“-Liste entfernen.
- Drive Encryption bleibt so lange aktiviert, bis die Kontrollkästchen für alle verbundenen Festplatten deaktiviert sind und die „Getrennt“-Liste leer ist.

Sichern und Wiederherstellen (Administratoraufgabe)

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

Sichern von Verschlüsselungsschlüsseln

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

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

1. Starten Sie **Drive Encryption**. Weitere Informationen finden Sie unter „Öffnen von Drive Encryption“ auf Seite 32.
2. Aktivieren Sie das Kontrollkästchen für eine Festplatte, und klicken oder tippen Sie auf **Schlüssel sichern**.
3. Wählen Sie unter **Wiederherstellungsschlüssel für HP Drive Encryption erstellen** eine oder mehrere der folgenden Optionen aus:
   - **Wechselmedien** – Aktivieren Sie das Kontrollkästchen, und wählen Sie das Speichergerät aus, auf dem der Verschlüsselungsschlüssel gespeichert werden soll.
   - **SkyDrive** – Aktivieren Sie das Kontrollkästchen. Dies erfordert eine Verbindung mit dem Internet. Melden Sie sich bei Microsoft SkyDrive an, und klicken oder tippen Sie auf **Ja**.

     HINWEIS: Um den auf SkyDrive gespeicherten HP Drive Encryption-Sicherungsschlüssel zu verwenden, müssen Sie ihn von SkyDrive auf ein Wechselmedium herunterladen und dieses in den Computer einführen.
   - **TPM** (nur bei bestimmten Modellen) – Ermöglicht Ihnen die Wiederherstellung Ihrer Daten unter Verwendung Ihres TPM-Kennworts.

     ACHTUNG: Wenn der TPM gelöscht wird oder der Computer beschädigt ist, können Sie nicht mehr auf die Sicherung zugreifen. Bei Auswahl dieser Methode sollte noch eine weitere Sicherungsmethode ausgewählt werden.
4. Klicken oder tippen Sie auf **Sichern**.

   Der Verschlüsselungsschlüssel wird auf dem von Ihnen ausgewählten Speichergerät gespeichert.

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

Administratoren können eine Wiederherstellung mithilfe des Drive Encryption-Schlüssels durchführen, der während der Aktivierung oder durch Auswahl der Option **Schlüssel sichern** in Drive Encryption auf einem Wechselmedium gesichert wurde.

1. Schließen Sie das Wechselmediengerät an, das Ihren Sicherungsschlüssel enthält.
2. Schalten Sie den Computer ein.
3. Klicken oder tippen Sie auf **Wiederherstellung**, sobald das Anmeldedialogfeld von HP Encryption geöffnet ist.
4. Geben Sie den Pfad oder Namen der Datei ein, die Ihren Sicherungsschlüssel enthält, und klicken oder tippen Sie anschließend auf **Wiederherstellung**.
5. Klicken oder tippen Sie im Bestätigungsdialogfeld auf **OK**.

   Der Anmeldebildschirm von Windows wird angezeigt.

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

Durchführen einer HP SpareKey-Wiederherstellung

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

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

1. Schalten Sie den Computer ein.
2. Wenn die Seite „HP Drive Encryption“ angezeigt wird, navigieren Sie zur Seite für die Benutzeranmeldung.
3. Klicken Sie auf **SpareKey**.

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

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

   Der Anmeldebildschirm von Windows wird angezeigt.

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

6 HP File Sanitizer (bestimmte Modelle)

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.

File Sanitizer kann nicht für die Bereinigung der folgenden Laufwerksarten verwendet werden:

- Solid-State-Laufwerke (SSD), einschließlich RAID-Volumes, die ein SSD-Gerät beinhalten
- Externe Laufwerke, die über eine USB-, Firewire- oder eSATA-Schnittstelle angeschlossen sind

Wenn versucht wird, die Daten auf einem SSD-Laufwerk zu shreddern oder zu überschreiben, wird eine Warnmeldung angezeigt und der Vorgang wird nicht ausgeführt.

Shreddern

Das Shreddern von Daten ist nicht mit einem Standard-Löschvorgang unter Windows® gleichzusetzen. 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.

Sie können für das Shreddern einen Zeitplan festlegen oder es direkt manuell aktivieren, indem Sie das Symbol **File Sanitizer** auf dem Startbildschirm von HP Client Security oder das Symbol **File Sanitizer** auf dem Windows Desktop auswählen. Weitere Informationen finden Sie unter „Festlegen eines Shred-Zeitplans“ auf Seite 41, „Shreddern durch Rechtsklicken auf den Datenbestand“ auf Seite 44 oder „Manuelles Starten eines Shred-Vorgangs“ auf Seite 44.

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

Überschreiben von freiem Speicherplatz

Beim Löschen eines Datenbestands unter Windows wird der Inhalt des Datenbestands nicht rückstandslos von der Festplatte entfernt. Windows löscht lediglich den Verweis auf den Datenbestand oder dessen Speicherort auf der Festplatte. Der Inhalt des Datenbestands bleibt weiterhin auf der Festplatte gespeichert, bis dieser Bereich der Festplatte durch neue Daten überschrieben wird.

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 bietet keine zusätzliche Sicherheit für geshredderte Datenbestände.

Sie können für das Überschreiben von freiem Speicherplatz einen Zeitplan festlegen oder das Überschreiben von zuvor geshredderten Datenbeständen direkt manuell aktivieren, indem Sie das Symbol **File Sanitizer** auf dem Startbildschirm von HP Client Security oder das Symbol **File Sanitizer** auf dem Windows Desktop auswählen. Weitere Informationen finden Sie unter „Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz“ auf Seite 42, „Manuelles Starten

des Überschreibens von freiem Speicherplatz“ auf Seite 44 oder „Verwenden des File Sanitizer-Symbols“ auf Seite 43.

Aufrufen von File Sanitizer

1. Klicken oder tippen Sie im Startbildschirm auf die App **HP Client Security** (Windows 8).

   – oder –

   Doppelklicken oder doppeltippen Sie auf dem Windows Desktop auf das Symbol **HP Client Security** im Infobereich außen rechts in der Taskleiste.

2. Klicken oder tippen Sie unter **Daten** auf **File Sanitizer**.

– oder –

▲ Doppelklicken oder doppeltippen Sie auf das Symbol **File Sanitizer** auf dem Windows Desktop.

– ODER –

▲ Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Windows Desktop oder tippen Sie auf das Symbol und halten Sie es. Wählen Sie anschließend **File Sanitizer öffnen** aus.

Setup-Verfahren

Shred-Vorgang – Beim Shred-Vorgang werden ausgewählte Kategorien von Datenbeständen durch File Sanitizer auf sichere Weise gelöscht oder überschrieben.

1. Wählen Sie unter **Shred-Vorgang** aus, welche Dateien geshreddert werden sollen oder nicht, indem Sie die Kontrollkästchen für die Dateitypen aktivieren bzw. deaktivieren.

   - **Papierkorb** – Shreddert alle Elemente im Papierkorb.
   - **Temporäre Systemdateien** – Shreddert alle Dateien im Ordner für temporäre Systemdateien. Dabei werden die folgenden Umgebungsvariablen in der genannten Reihenfolge durchsucht; der erste gefundene Pfad wird als Systemordner verwendet:
     - TMP
     - TEMP
   - **Temporäre Internetdateien** – Shreddert Kopien von Webseiten, Bildern und Medien, die von Webbrowsern gespeichert werden, um eine schnellere Anzeige zu ermöglichen.
   - **Cookies** – Shreddert alle Dateien, die von Websites auf dem Computer abgelegt werden, um Voreinstellungen zu speichern (z. B. Anmeldedaten).

2. Zum Starten des Shred-Vorgangs klicken oder tippen Sie auf **Shreddern**.

Überschreiben – Überschreibt freien Speicherplatz mit willkürlichen Daten und verhindert die Wiederherstellung von gelöschten Daten.

▲ Zum Starten des Überschreibungsvorgangs klicken oder tippen Sie auf **Überschreiben**.

File Sanitizer-Optionen – Die folgenden Optionen können durch Aktivierung bzw. Deaktivierung des entsprechenden Kontrollkästchens aktiviert bzw. deaktiviert werden:

- **Desktop-Symbol aktivieren** – Zeigt das File Sanitizer-Symbol auf dem Windows Desktop an.
- **Rechtsklicken aktivieren** – Ermöglicht es Ihnen, durch Rechtsklicken auf einen Datenbestand bzw. Tippen und Halten ein Kontextmenü zu öffnen und **HP File Sanitizer – Shreddern** auszuwählen.
- **Vor dem manuellen Shreddern Windows Kennwort abfragen** – Legt fest, dass vor dem manuellen Shreddern eines Elements eine Authentifizierung mit dem Windows Kennwort erfolgen soll.
- **Cookies und temporäre Internetdateien beim Schließen des Browsers shreddern** – Shreddert alle ausgewählten Datenbestände, die durch Browsernutzung angelegt wurden, sobald Sie einen Internetbrowser schließen.

Festlegen eines Shred-Zeitplans

Sie können einen Shred-Zeitplan für die automatische Durchführung des Shredderns festlegen. Es bleibt Ihnen jedoch unbenommen, jederzeit auch manuell Datenbestände zu shreddern. Weitere Informationen finden Sie unter „Setup-Verfahren“ auf Seite 40.

1. Öffnen Sie File Sanitizer, und klicken oder tippen Sie auf **Einstellungen**.
2. Wenn Sie für das Shreddern ausgewählter Datenbestände einen Zeitplan festlegen möchten, wählen Sie unter **Shred-Zeitplan** eine der Optionen **Niemals**, **Einmal**, **Täglich**, **Wöchentlich** oder **Monatlich** und anschließend einen Tag und eine Uhrzeit aus:
   a. Klicken oder tippen Sie auf die Felder "Stunde", "Minute" und "AM/PM".
   b. Führen Sie einen Bildlauf durch, bis der gewünschte Wert auf derselben Ebene wie die anderen Felder angezeigt wird.
   c. Klicken oder tippen Sie auf den Leerraum, der die Felder für die Zeiteinstellung umgibt.
   d. Wiederholen Sie den Vorgang für jedes Feld, bis der gewünschte Zeitplan ausgewählt ist.
3. Es stehen folgende Kategorien von Datenbeständen zur Auswahl:
   - **Papierkorb** – Shreddert alle Elemente im Papierkorb.
   - **Temporäre Systemdateien** – Shreddert alle Dateien im Ordner für temporäre Systemdateien. Dabei werden die folgenden Umgebungsvariablen in der genannten Reihenfolge durchsucht; der erste gefundene Pfad wird als Systemordner verwendet:
     - TMP
     - TEMP
   - **Temporäre Internetdateien** – Shreddert Kopien von Webseiten, Bildern und Medien, die von Webbrowsern gespeichert werden, um eine schnellere Anzeige zu ermöglichen.
   - **Cookies** – Shreddert alle Dateien, die von Websites auf dem Computer abgelegt werden, um Voreinstellungen zu speichern (z. B. Anmeldedaten).

Durch Aktivierung der Kontrollkästchen legen Sie fest, dass die entsprechenden Datenbestände zum geplanten Zeitpunkt geshreddert werden.

4. So wählen Sie zusätzliche benutzerdefinierte Datenbestände für das Shreddern aus:

   a. Klicken oder tippen Sie unter **Liste für geplanten Shred-Vorgang** auf **Ordner hinzufügen**, und navigieren Sie anschließend zu der Datei oder dem Ordner.

   b. Klicken oder tippen Sie auf **Öffnen** und dann auf **OK**.

   Um einen Datenbestand aus der Liste für den geplanten Shred-Vorgang zu entfernen, deaktivieren Sie das Kontrollkästchen für den Datenbestand.

Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz

Das Überschreiben von freiem Speicherplatz bietet keine zusätzliche Sicherheit für geshredderte Datenbestände.

1. Öffnen Sie File Sanitizer, und klicken oder tippen Sie auf **Einstellungen**.
2. Wenn Sie für das Überschreiben Ihres Festplattenlaufwerks einen Zeitplan festlegen möchten, wählen Sie unter **Zeitplan für das Überschreiben** eine der Optionen **Niemals**, **Einmal**, **Täglich**, **Wöchentlich** oder **Monatlich** und anschließend einen Tag und eine Uhrzeit aus:

   a. Klicken oder tippen Sie auf die Felder "Stunde", "Minute" und "AM/PM".

   b. Führen Sie einen Bildlauf durch, bis die gewünschte Uhrzeit auf derselben Ebene wie die anderen Felder angezeigt wird.

   c. Klicken oder tippen Sie auf den Leerraum, der die Felder für die Zeiteinstellung umgibt.

   d. Wiederholen Sie den Vorgang, bis der gewünschte Zeitplan ausgewählt ist.

HINWEIS: Das Überschreiben von freiem Speicherplatz kann einige Zeit in Anspruch nehmen. Stellen Sie sicher, dass der Computer an den Netzstrom angeschlossen ist. Obwohl der Vorgang im Hintergrund ausgeführt wird, kann die Computerleistung durch die zusätzliche Prozessorbelastung beeinträchtigt werden. Das Überschreiben von freiem Speicherplatz kann außerhalb der Arbeitszeit durchgeführt werden oder wenn der Computer nicht verwendet wird.

Schützen von Dateien vor dem Shreddern

So schützen Sie Dateien oder Ordner vor dem Shreddern:

1. Öffnen Sie File Sanitizer, und klicken oder tippen Sie auf **Einstellungen**.
2. Klicken oder tippen Sie unter **Ausschlussliste für das Shreddern** auf **Ordner hinzufügen**, und navigieren Sie anschließend zu der Datei oder dem Ordner.
3. Klicken oder tippen Sie auf **Öffnen** und dann auf **OK**.

HINWEIS: Dateien in dieser Liste sind geschützt, solange sie in dieser Liste bleiben.

Um einen Datenbestand aus der Ausschlussliste zu entfernen, deaktivieren Sie das Kontrollkästchen für den Datenbestand.

Allgemeine Aufgaben

Mit File Sanitizer können Sie die folgenden Aufgaben ausführen:

- **Verwenden des Symbols „File Sanitizer“, um den Shred-Vorgang einzuleiten** – Datei auf das Symbol **File Sanitizer** auf dem Windows-Desktop ziehen. Ausführliche Informationen zu diesem Thema finden Sie unter „Verwenden des File Sanitizer-Symbols“ auf Seite 43.
- **Manuelles Shreddern von bestimmten oder allen ausgewählten Datenbeständen** – Elemente zu einem beliebigen Zeitpunkt ohne Berücksichtigung des regulären Shred-Zeitplans shreddern. Ausführliche Informationen zu diesem Thema erhalten Sie unter „Shreddern durch Rechtsklicken auf den Datenbestand“ auf Seite 44 oder „Manuelles Starten eines Shred-Vorgangs“ auf Seite 44.
- **Manuelles Aktivieren des Überschreibens von freiem Speicherplatz** – Überschreiben von freiem Speicherplatz zu einem beliebigen Zeitpunkt aktivieren. Ausführliche Informationen zu diesem Thema finden Sie unter „Manuelles Starten des Überschreibens von freiem Speicherplatz“ auf Seite 44.
- **Anzeigen der Protokolle** – Protokolle zum Shred-Vorgang und zum Überschreiben von freiem Speicherplatz anzeigen. Diese Protokolle enthalten Angaben über Fehler, die beim letzten Shred- oder Überschreibungsvorgang aufgetreten sind. Ausführliche Informationen zu diesem Thema finden Sie unter „Anzeigen der Protokolldateien“ auf Seite 45.

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

Verwenden des File Sanitizer-Symbols

ACHTUNG: Geshredderte Daten können nicht wiederhergestellt werden. Prüfen Sie sorgfältig, welche Elemente Sie für manuelles Shreddern auswählen.

Wenn Sie einen Shred-Vorgang manuell starten, wird alles, was in der Standardliste für das Shreddern in der File Sanitizer-Ansicht ausgewählt ist, geshreddert (siehe „Setup-Verfahren“ auf Seite 40).

Sie können einen Shred-Vorgang wie folgt manuell starten:

1. Öffnen Sie File Sanitizer (siehe „Aufrufen von File Sanitizer“ auf Seite 40), und klicken oder tippen Sie auf **Shreddern**.
2. Wenn das Bestätigungsdialogfeld geöffnet wird, vergewissern Sie sich, dass die zu shreddernden Datenbestände ausgewählt sind, und klicken oder tippen Sie dann auf **OK**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Windows Desktop oder tippen Sie auf das Symbol und halten Sie es. Wählen Sie anschließend **Jetzt shreddern** aus.
2. Wenn das Bestätigungsdialogfeld geöffnet wird, vergewissern Sie sich, dass die zu shreddernden Datenbestände ausgewählt sind, und klicken oder tippen Sie dann auf **Shreddern**.

Shreddern durch Rechtsklicken auf den Datenbestand

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

Wenn in der File Sanitizer-Ansicht die Option **Rechtsklick-Shreddern aktivieren** ausgewählt wurde, können Sie einen Datenbestand wie folgt shreddern:

1. Navigieren Sie zu dem zu shreddernden Dokument oder Ordner.
2. Öffnen Sie das Kontextmenü für die Datei oder den Ordner, indem Sie mit der rechten Maustaste darauf klicken bzw. tippen und halten, und wählen Sie anschließend **HP File Sanitizer – Shreddern** aus.

Manuelles Starten eines Shred-Vorgangs

⚠ **ACHTUNG:** Geshredderte Daten können nicht wiederhergestellt werden. Prüfen Sie sorgfältig, welche Elemente Sie für manuelles Shreddern auswählen.

Wenn Sie einen Shred-Vorgang manuell starten, wird alles, was in der Standardliste für das Shreddern in der File Sanitizer-Ansicht ausgewählt ist, geshreddert (siehe „Setup-Verfahren“ auf Seite 40).

Sie können einen Shred-Vorgang wie folgt manuell starten:

1. Öffnen Sie File Sanitizer (siehe „Aufrufen von File Sanitizer“ auf Seite 40), und klicken oder tippen Sie auf **Shreddern**.
2. Wenn das Bestätigungsdialogfeld geöffnet wird, vergewissern Sie sich, dass die zu shreddernden Datenbestände ausgewählt sind, und klicken oder tippen Sie dann auf **OK**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Windows Desktop oder tippen Sie auf das Symbol und halten Sie es. Wählen Sie anschließend **Jetzt shreddern** aus.
2. Wenn das Bestätigungsdialogfeld geöffnet wird, vergewissern Sie sich, dass die zu shreddernden Datenbestände ausgewählt sind, und klicken oder tippen Sie dann auf **Shreddern**.

Manuelles Starten des Überschreibens von freiem Speicherplatz

Wenn Sie einen Überschreibungsvorgang manuell starten, wird alles, was in der Standardliste für das Shreddern in der File Sanitizer-Ansicht ausgewählt ist, überschrieben (siehe „Setup-Verfahren“ auf Seite 40).

Sie können einen Überschreibungsvorgang wie folgt manuell starten:

1. Öffnen Sie File Sanitizer (siehe „Aufrufen von File Sanitizer“ auf Seite 40), und klicken oder tippen Sie auf **Überschreiben**.
2. Klicken oder tippen Sie im Bestätigungsdialogfeld auf **OK**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Windows Desktop oder tippen Sie auf das Symbol und halten Sie es. Wählen Sie anschließend **Jetzt überschreiben** aus.
2. Klicken oder tippen Sie im Bestätigungsdialogfeld auf **Überschreiben**.

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 oder überschrieben wurden, werden in den Protokolldateien nicht aufgeführt.

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

- 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 Ordnern abgelegt:

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

7 HP Device Access Manager (bestimmte Modelle)

Mit HP 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 49.

Administratoren des Windows® Betriebssystems verwenden Device Access Manager, um den Zugriff auf die Geräte in einem System zu kontrollieren und unbefugte Zugriffe zu verhindern:

- Geräteprofile werden für jeden Benutzer erstellt, um festzulegen, auf welche Geräte die jeweiligen Benutzer zugreifen können.
- Mit der Just-In-Time-Authentifizierung (JITA) können vordefinierte Benutzer sich selbst authentifizieren, um auf Geräte zuzugreifen, für die der Zugriff ansonsten verweigert wird.
- Administratoren und vertrauenswürdige Benutzer können von den Einschränkungen für den Zugriff auf Geräte ausgenommen werden, die durch Device Access Manager auferlegt werden. Dazu werden diese Benutzer in die Gruppe der Geräte-Administratoren aufgenommen. Die Mitgliedschaft in dieser Gruppe wird über Erweiterten Einstellungen verwaltet.
- Der Zugriff auf Geräte kann in Abhängigkeit von der Gruppenmitgliedschaft gewährt oder verweigert werden.
- Für Geräteklassen wie CD-ROM- und DVD-Laufwerke können Lesezugriff und Schreibzugriff separat gewährt oder verweigert werden.

HP Device Access Manager wird während der Ausführung des Installationsassistenten von HP Client Security automatisch mit folgenden Einstellungen konfiguriert:

- Die Just-In-Time-Authentifizierung (JITA) für Wechselmedienlaufwerke ist für die Gruppen „Administratoren“ und „Benutzer“ aktiviert.
- Die Geräterichtlinie erteilt unbeschränkten Zugriff auf andere Geräte.

Aufrufen von Device Access Manager

1. Klicken oder tippen Sie im Startbildschirm auf die App **HP Client Security** (Windows 8).

   – oder –

   Doppelklicken oder doppeltippen Sie auf dem Windows Desktop auf das Symbol **HP Client Security** im Infobereich außen rechts in der Taskleiste.

2. Klicken oder tippen Sie unter **Gerät** auf **Geräteberechtigungen**.

   - Standardbenutzer können sich den aktuellen Stand ihrer Zugriffsberechtigungen für Geräte anzeigen lassen (siehe „Benutzeransicht“ auf Seite 47).
   - Administratoren können sich die aktuell für den Computer konfigurierten Einstellungen für den Gerätezugriff anzeigen lassen und diese ändern, indem sie auf **Ändern** klicken oder

tippen und anschließend das Administratorkennwort eingeben (siehe „Systemansicht“ auf Seite 47).

Benutzeransicht

Bei Auswahl von **Geräteberechtigungen** wird die Benutzeransicht angezeigt. Je nach Richtlinie können Standardbenutzer und Administratoren ihre eigenen Zugriffseinstellungen für Geräteklassen oder einzelne Geräte auf dem Computer anzeigen.

- **Aktueller Benutzer** – Hier wird der Name des zurzeit angemeldeten Benutzers angezeigt.
- **Geräteklasse** – Hier werden die Typen von Geräten angezeigt.
- **Zugriff** – Hier werden die zurzeit für den aktuellen Benutzer konfigurierten Zugriffsberechtigungen für Geräteklassen oder bestimmte Geräte angezeigt.
- **Dauer** – Hier wird das für den aktuellen Benutzer konfigurierte Zeitlimit für den Zugriff auf CD-ROM-/DVD-Laufwerke oder Wechselmedienlaufwerke angezeigt.
- **Einstellungen** – Hier können Administratoren die Auswahl der Laufwerke ändern, für die der Zugriff auf sie durch Device Access Manager gesteuert wird.

Systemansicht

In der Systemansicht können Administratoren den Zugriff auf Geräte dieses Computers für die Gruppen „Benutzer“ oder „Administratoren“ erteilen oder verweigern.

▲ Administratoren können auf die Systemansicht zugreifen, indem sie auf **Ändern** klicken oder tippen, ein Administratorkennwort eingeben und dann eine der folgenden Optionen auswählen:

- **Device Access Manager** – Um HP Device Access Manager mit Just-In-Time-Authentifizierung zu aktivieren oder zu deaktivieren, klicken oder tippen Sie auf **Ein** oder **Aus**.
- **Benutzer und Gruppen auf diesem PC** – Zeigt die Gruppe („Benutzer“ oder „Administratoren“) an, welcher der Zugriff auf die ausgewählten Geräteklassen erteilt oder verweigert wird.
- **Geräteklasse** – Zeigt die Geräteklassen und Geräte an, die im System installiert sind oder möglicherweise zuvor im System installiert waren. Um die Liste zu erweitern, klicken Sie auf das Symbol **+**. Es werden alle mit dem Computer verbundenen Geräte angezeigt, und die Darstellung der Gruppen „Benutzer“ und „Administratoren“ wird erweitert, um ihre Mitglieder anzuzeigen. Um die Anzeige der Geräteliste zu aktualisieren, klicken Sie auf das Rundpfeil-Symbol.
  - In der Regel erstreckt sich der Schutz auf eine Geräteklasse. Wenn für den Zugriff **Erlauben** festgelegt ist, kann der ausgewählter Benutzer bzw. die ausgewählte Gruppe auf alle Geräte der Geräteklasse zugreifen.
  - Es besteht außerdem die Möglichkeit, bestimmte Geräte zu schützen.
  - Durch Konfigurieren der Just-In-Time-Authentifizierung (JITA) können Sie ausgewählten Benutzern den Zugriff auf DVD-/CD-ROM-Laufwerke oder Wechselmedienlaufwerke erlauben, indem sie sich authentifizieren. Weitere Informationen finden Sie unter „JITA-Konfiguration“ auf Seite 48.
  - Sie können auch den Zugriff auf andere Geräteklassen erteilen oder verweigern, wie zum Beispiel Wechselmedienlaufwerke (z. B. USB-Flash-Laufwerke), serielle und parallele Anschlüsse, Bluetooth®-Geräte, Modemgeräte, PCMCIA/ExpressCard-Geräte, FireWire-Geräte, Fingerabdruck- und Smart Card-Lesegeräte. Wenn der Zugriff auf Fingerabdruck- und Smart Card-Lesegeräte verweigert wird, können diese zwar für

Authentifizierungszwecke, jedoch nicht auf der durch die Sitzungsrichtlinie gesteuerten Ebene genutzt werden.

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

- Bei Auswahl einer Einstellung auf Gruppen- oder Geräteklassenebene wird möglicherweise gefragt, ob Sie die Einstellung auf die untergeordneten Objekte anwenden möchten. In diesem Fall haben Sie folgende Optionen:

  Ja – Die Einstellung wird weitergereicht.

  Nein – Die Einstellung wird nicht weitergereicht.

- 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.

HINWEIS: Die Gruppe „Administratoren“ kann nicht zur „Benutzerliste“ hinzugefügt werden.

- **Zugriff** – Klicken oder tippen Sie auf den Pfeil nach unten, und wählen Sie anschließend eine der folgenden Zugriffsarten aus, für die der Zugriff erteilt oder verweigert werden soll:
  - **Erlauben – Uneingeschränkter Zugriff**
  - **Erlauben – Nur Lesen**
  - **Erlauben – JITA erforderlich** – Weitere Informationen finden Sie unter „JITA-Konfiguration“ auf Seite 48.

    Bei Auswahl dieser Zugriffsart klicken oder tippen Sie unter **Dauer** auf den Pfeil nach unten, um ein Zeitlimit auszuwählen.
  - **Verweigern**
- **Dauer** – Klicken oder tippen Sie auf den Pfeil nach unten, um ein Zeitlimit für den Zugriff auf CD-ROM-/DVD-Laufwerke oder Wechselmedienlaufwerke auszuwählen (siehe „JITA-Konfiguration“ auf Seite 48).

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.

Benutzer mit aktiviertem JITA-Zugriff können auf einige Geräte zugreifen, für die in der Ansicht **Geräteklassen-Konfiguration** erstellte Richtlinien beschränkt wurden.

Der JITA-Zeitraum kann für eine festgelegte Anzahl an Minuten oder unbegrenzt genehmigt sein. Benutzer mit unbegrenztem JITA-Zeitraum können ab dem Zeitpunkt der Authentifizierung bis zur Abmeldung vom System auf das Gerät zugreifen.

Wenn dem Benutzer ein begrenzter JITA-Zeitraum zugewiesen wurde, erfolgt eine Minute vor dem Ablauf die Abfrage, ob der Benutzer den Zeitraum verlängern möchte. Sobald sich der Benutzer vom System abmeldet oder ein andere Benutzer sich anmeldet, läuft der JITA-Zeitraum ab. Wenn der Benutzer sich das nächste Mal anmeldet und versucht, auf ein Gerät zuzugreifen, für das der JITA-Zugriff aktiviert ist, wird eine Aufforderung zur Eingabe der Anmeldeinformationen angezeigt.

JITA ist für die folgenden Geräteklassen verfügbar:

- DVD-/CD-ROM-Laufwerke
- Wechselmedienlaufwerke

Erstellen einer JITA-Richtlinie für einen Benutzer oder eine Gruppe

Administratoren können Benutzern oder Gruppen Zugriff auf Geräte unter Verwendung von Just-In-Time-Authentifizierung (JITA) erteilen.

1. Starten Sie **Device Access Manager**, und klicken oder tippen Sie auf **Ändern**.
2. Wählen Sie den Benutzer oder die Gruppe aus, klicken oder tippen Sie unter **Zugriff** wahlweise auf **Wechselmedienlaufwerke** oder **DVD-/CD-ROM-Laufwerke**, und wählen Sie anschließend **Erlauben – JITA erforderlich** aus.
3. Klicken oder tippen Sie unter **Dauer** auf den Pfeil nach unten, um einen Zeitraum für den JITA-Zugriff auszuwählen.

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

Deaktivieren einer JITA-Richtlinie für einen Benutzer oder eine Gruppe

Administratoren können den JITA-Zugriff von Benutzern oder Gruppen auf Geräte deaktivieren.

1. Starten Sie **Device Access Manager**, und klicken oder tippen Sie auf **Ändern**.
2. Wählen Sie den Benutzer oder die Gruppe aus, klicken oder tippen Sie unter **Zugriff** wahlweise auf **Wechselmedienlaufwerke** oder **DVD-/CD-ROM-Laufwerke**, und wählen Sie anschließend **Verweigern** aus.

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

Einstellungen

Über die Ansicht **Einstellungen** können Administratoren die Laufwerke anzeigen, für die der Zugriff auf sie durch Device Access Manager gesteuert wird.

HINWEIS: Device Access Manager muss aktiviert sein, wenn die Liste der Laufwerksbuchstaben konfiguriert wird (siehe „Systemansicht“ auf Seite 47).

Nicht verwaltete Geräteklassen

Folgende Geräteklassen werden von HP Device Access Manager NICHT verwaltet:

- Eingabe-/Ausgabegeräte
  - CD-ROM
  - Datenträgerlaufwerk
  - Disketten-Controller (FDC)
  - Festplatten-Controller (HDC)
  - Schnittstelle für die Benutzerinteraktion (HID)
  - Infrarot-Schnittstelle für die Benutzerinteraktion

- Maus
- Serieller Multi-Port
- Tastatur
- Plug-and-Play (PnP)-Drucker
- Drucker
- Drucker-Upgrade

- Energie
  - Support für erweiterte Energieverwaltung (APM)
  - Akku
- Sonstiges
  - Computer
  - Decoder
  - Display
  - Vereinheitlichter Display-Treiber von Intel®
  - Legacard
  - Medientreiber
  - Medienwechselgerät
  - Speichertechnologie
  - Monitor
  - Multifunktionsgerät
  - Netz-Client
  - Netzdienst
  - Netzübertragung
  - Prozessor
  - SCSI-Adapter
  - Sicherheitsbeschleuniger
  - Sicherheitsgerät
  - System
  - Unbekannt
  - Lautstärke
  - Volume-Schnappschuss

8 HP Trust Circles

HP Trust Circles ist eine Sicherheitsanwendung für den Schutz von Dateien und Dokumenten, die Verschlüsselung von Dateien auf Ordnerebene mit komfortablen Funktionen zur gemeinsamen Nutzung von Dokumenten auf der Basis von Vertrauenskreisen kombiniert. Die Anwendung verschlüsselt Daten in von Benutzern festgelegten Ordnern und schützt sie innerhalb eines Vertrauenskreises. Die derart geschützten Dateien können nur von Mitgliedern des Vertrauenskreises genutzt und geteilt werden. Wenn eine geschützte Datei von einem Nichtmitglied empfangen wird, bleibt die Datei verschlüsselt und das Nichtmitglied kann nicht auf deren Inhalt zugreifen.

Öffnen von Trust Circles

1. Klicken oder tippen Sie auf dem Startbildschirm auf die App **HP Client Security**.

   – ODER –

   Klicken Sie auf dem Windows-Desktop im Infobereich außen rechts in der Taskleiste auf das Symbol **HP Client Security**.

2. Klicken oder tippen Sie unter **Daten** auf **Trust Circles**.

Einführung

Es gibt zwei Arten, E-Mail-Einladungen zu versenden und auf sie zu antworten:

- **Mithilfe von Microsoft® Outlook** – Wenn Sie Trust Circles in Verbindung mit Microsoft Outlook verwenden, können Sie damit die Verarbeitung von Trust Circles-Einladungen und -Antworten von anderen Trust Circles-Benutzern automatisieren.
- **Mithilfe von Gmail, Yahoo, Outlook.com oder anderen E-Mail-Diensten (SMTP)** – Wenn Sie Ihren Namen, Ihre E-Mail-Adresse und Ihr Kennwort eingeben, benutzt Trust Circles Ihren E-Mail-Dienst zum Versenden von E-Mail-Einladungen an die Mitglieder, die für die Teilnahme an Ihrem Vertrauenskreis ausgewählt wurden.

So richten Sie Ihr Basisprofil ein:

1. Geben Sie Ihren Namen und Ihre E-Mail-Adresse ein, und klicken oder tippen Sie auf **Weiter**.

   Der Name ist für alle Mitglieder sichtbar, die zur Teilnahme an Ihrem Vertrauenskreis eingeladen werden. Die E-Mail-Adresse wird zum Versenden, Empfangen und Beantworten von Einladungen verwendet.

2. Geben Sie das Kennwort für das E-Mail-Konto ein, und klicken oder tippen Sie auf **Weiter**.

   Anschließend wird eine Test-E-Mail versendet, um sicherzustellen, dass die E-Mail-Einstellungen korrekt sind.

   HINWEIS: Der Computer muss mit einem Netzwerk verbunden sein.

3. Geben Sie in das Feld **Name des Vertrauenskreises** einen Namen für den Vertrauenskreis ein, und klicken oder tippen Sie auf **Weiter**.

4. Fügen Sie Mitglieder und Ordner hinzu, und klicken oder tippen Sie auf **Weiter**. Der Vertrauenskreis wird zusammen mit den ausgewählten Ordnern erstellt. Anschließend versendet

der Vertrauenskreis Einladungen an alle ausgewählten Mitglieder. Wenn eine Einladung nicht versendet werden kann, wird eine entsprechende Benachrichtigung angezeigt. Sie können jederzeit erneut Mitglieder einladen, indem Sie in der Vertrauenskreis-Ansicht auf **Meine Vertrauenskreise** klicken und dann auf den gewünschten Vertrauenskreis doppelklicken oder doppeltippen. Weitere Informationen finden Sie unter „Trust Circles“ auf Seite 52.

Trust Circles

Sie können einen Vertrauenskreis während der anfänglichen Einrichtung nach der Eingabe Ihrer E-Mail-Adresse oder danach über die Vertrauenskreis-Ansicht erstellen:

▲ Klicken oder tippen Sie in der Vertrauenskreis-Ansicht auf **Vertrauenskreis erstellen**, und geben Sie dann einen Namen für den Vertrauenskreis ein.

- Um Mitglieder zum Vertrauenskreis hinzuzufügen, klicken oder tippen Sie auf das Symbol **M+** neben **Mitglieder** und folgen Sie den Anweisungen auf dem Bildschirm.
- Um Ordner zum Vertrauenskreis hinzuzufügen, klicken oder tippen Sie auf das Symbol **+** neben **Ordner** und folgen Sie den Anweisungen auf dem Bildschirm.

Hinzufügen von Ordnern zu einem Vertrauenskreis

Hinzufügen von Ordnern zu einem neuen Vertrauenskreis:

- Sie können während der Erstellung eines Vertrauenskreises Ordner hinzufügen. Klicken oder tippen Sie dazu auf das Symbol **+** neben **Ordner**, und folgen Sie anschließend den Anweisungen auf dem Bildschirm.

  – ODER –

- Identifizieren Sie in Windows Explorer einen Ordner, der zurzeit nicht Teil eines Vertrauenskreises ist, klicken Sie mit der rechten Maustaste auf den Order bzw. tippen und halten Sie ihn, und wählen Sie dann **Vertrauenskreis** und **Vertrauenskreis von Ordner erstellen** aus.

TIPP: Sie können einen oder mehrere Ordner auswählen.

Hinzufügen von Ordnern zu einem vorhandenen Vertrauenskreis:

- Klicken oder tippen Sie in der Vertrauenskreis-Ansicht auf **Meine Vertrauenskreise**, doppelklicken oder doppeltippen Sie auf den vorhandenen Vertrauenskreis, um die aktuellen Ordner anzuzeigen, klicken oder tippen Sie auf das Symbol **+** neben **Ordner**, und folgen Sie den Anweisungen auf dem Bildschirm.

  – ODER –

- Identifizieren Sie in Windows Explorer einen Ordner, der zurzeit nicht Teil eines Vertrauenskreises ist, klicken Sie mit der rechten Maustaste auf den Order bzw. tippen und halten Sie ihn, und wählen Sie dann **Vertrauenskreis** und **Von Ordner zu vorhandenem Vertrauenskreis hinzufügen** aus.

TIPP: Sie können einen oder mehrere Ordner auswählen.

Nachdem ein Ordner zu einem Vertrauenskreis hinzugefügt wurde, werden der Ordner und dessen Inhalt automatisch von Trust Circles verschlüsselt. Sobald alle Dateien verschlüsselt sind, wird eine Benachrichtigung angezeigt. Außerdem wird über allen Symbolen verschlüsselter Dateien oder

Ordner ein grünes Schloss-Symbol eingeblendet, das angezeigt, dass es sich um vollständig geschützte Dateien bzw. Ordner handelt.

Hinzufügen von Mitgliedern zu einem Vertrauenskreis

Um Mitglieder zu einem Vertrauenskreis hinzuzufügen, sind drei Schritte erforderlich:

1. **Einladen** – Zuerst lädt der Eigentümer des Vertrauenskreises ein oder mehrere Mitglieder ein. Die Einladungs-E-Mail kann an mehrere Benutzer oder Verteilerlisten bzw. Gruppen gesendet werden.
2. **Akzeptieren** – Der Eingeladene empfängt die Einladung und entscheidet, ob er sie annimmt oder ablehnt. Wenn der Eingeladene die Einladung annimmt, wird per E-Mail eine Antwort an den Einladenden gesendet. Falls die Einladung an eine Gruppe gesendet wurde, empfängt jedes Gruppenmitglied eine Einladung und entscheidet über Annahme oder Ablehnung.
3. **Registrieren** – Dies ist die letzte Gelegenheit für den Einladenden, darüber zu befinden, ob das Mitglied zum Vertrauenskreis hinzugefügt werden soll. Wenn sich der Einladende dafür entscheidet, das Mitglied zu registrieren, wird eine E-Mail zur Bestätigung der Antwort an den Eingeladenen gesendet. Sowohl der Einladende als auch der Eingeladene können optional die Sicherheit des Einladungsprozesses überprüfen. In diesem Fall wird für den Eingeladenen ein Prüfcode angezeigt, den er dem Einladenden telefonisch mitteilen muss. Nachdem der Code auf diese Weise überprüft wurde, kann der Einladende die abschließende Registrierungs-E-Mail senden.

Hinzufügen von Mitgliedern zu einem neuen Vertrauenskreis:

- Sie können während der Erstellung eines Vertrauenskreises Mitglieder hinzufügen. Klicken oder tippen Sie dazu auf das Symbol **M+** neben **Mitglieder**, und folgen Sie anschließend den Anweisungen auf dem Bildschirm.
  - Sofern Sie Outlook verwenden, wählen Sie die Kontakte im Adressbuch von Outlook aus und klicken Sie anschließend auf **OK**
  - Wenn Sie einen anderen E-Mail-Dienst verwenden, können Sie entweder manuell neue E-Mail-Adressen zu Trust Circles hinzufügen oder aus den bei Trust Circles bereits registrierten E-Mail-Adressen abrufen.

Hinzufügen von Mitgliedern zu einem vorhandenen Vertrauenskreis:

- Klicken Sie in der Vertrauenskreis-Ansicht auf **Meine Vertrauenskreise**, doppelklicken oder doppeltippen Sie auf den vorhandenen Vertrauenskreis, um die aktuellen Mitglieder anzuzeigen, klicken oder tippen Sie auf das Symbol **M+** neben **Mitglieder**, und folgen Sie den Anweisungen auf dem Bildschirm.
  - Sofern Sie Outlook verwenden, wählen Sie die Kontakte im Adressbuch von Outlook aus und klicken Sie anschließend auf **OK**
  - Wenn Sie einen anderen E-Mail-Dienst verwenden, können Sie entweder manuell neue E-Mail-Adressen zu Trust Circles hinzufügen oder aus den bei Trust Circles bereits registrierten E-Mail-Adressen abrufen.

Hinzufügen von Dateien zu einem Vertrauenskreis

Dateien können wie folgt zu einem Vertrauenskreis hinzugefügt werden:

- Kopieren oder verschieben Sie die Datei in einen vorhandenen Ordner des Vertrauenskreises.

  – ODER –

- Identifizieren Sie in Windows Explorer eine Datei, die zurzeit nicht verschlüsselt ist, klicken Sie mit der rechten Maustaste auf die Datei bzw. tippen und halten Sie sie, und wählen Sie dann **Vertrauenskreis** und **Verschlüsseln** aus. Anschließend werden Sie aufgefordert, den Vertrauenskreis auszuwählen, zu dem die Datei hinzugefügt werden soll.

TIPP: Sie können eine oder mehrere Dateien auswählen.

Verschlüsselte Ordner

Jedes Mitglied eines Vertrauenskreises kann Dateien anzeigen und bearbeiten, die diesem Vertrauenskreis zugeordnet sind.

HINWEIS: Dateien eines Vertrauenskreises werden von Trust Circle Manager/Reader nicht zwischen Mitgliedern synchronisiert.

Die gemeinsame Nutzung von Dateien muss mit den vorhandenen Hilfsmitteln wie E-Mail, FTP oder Anbietern von Cloud-Speicher organisiert werden. Dateien, die in einen Ordner eines Vertrauenskreises kopiert oder verschoben oder in diesem erstellt werden, sind unmittelbar geschützt.

Entfernen von Ordnern aus einem Vertrauenskreis

Beim Entfernen eines Ordners aus einem Vertrauenskreis werden der Ordner und sein Inhalt entschlüsselt, und beide verlieren ihren Schutz.

- Klicken oder tippen Sie in der Vertrauenskreis-Ansicht auf **Meine Vertrauenskreise**, doppelklicken oder doppeltippen Sie auf den vorhandenen Vertrauenskreis, um die aktuellen Ordner anzuzeigen, und klicken oder tippen Sie auf das **Mülleimer**-Symbol neben dem Ordner.

  – ODER –

- Identifizieren Sie in Windows Explorer einen Ordner, der zurzeit Teil eines Vertrauenskreises ist, klicken Sie mit der rechten Maustaste auf den Order bzw. tippen und halten Sie ihn, und wählen Sie dann **Vertrauenskreis** und **Aus Vertrauenskreis entfernen** aus.

TIPP: Sie können einen oder mehrere Ordner auswählen.

Entfernen einer Datei aus einem Vertrauenskreis

Um eine Datei aus einem Vertrauenskreis zu entfernen, identifizieren Sie in Windows Explorer eine Datei, die zurzeit verschlüsselt ist, klicken Sie mit der rechten Maustaste auf die Datei bzw. tippen und halten Sie sie, und wählen Sie dann **Vertrauenskreis** und **Datei entschlüsseln** aus.

Entfernen von Mitgliedern aus einem Vertrauenskreis

Es ist nicht möglich, ein abschließend registriertes Mitglied aus einem Vertrauenskreis zu entfernen. Eine Alternative wäre, einen neuen Vertrauenskreis mit allen anderen Mitgliedern zu erstellen, alle Dateien und Ordner in den neuen Vertrauenskreis zu verschieben und dann den alten Vertrauenskreis zu löschen. Damit ist sichergestellt, dass alle neuen Dateien, die das

auszuschließende Mitglied empfängt, nicht zugänglich sind, hingegen alles, was zuvor gemeinsam genutzt wurde, für die anderen Mitglieder des alten Vertrauenskreises zugänglich bleibt.

Wenn ein Mitglied nicht abschließend registriert ist (weil es eine Einladung zur Teilnahme am Vertrauenskreis erhalten und entweder noch nicht beantwortet oder sie abgelehnt hat), können Sie das Mitglied auf eine der folgenden Weisen aus dem Vertrauenskreis entfernen:

- Klicken oder tippen Sie in der Vertrauenskreis-Ansicht auf **Meine Vertrauenskreise**, und doppelklicken oder doppeltippen Sie auf den Vertrauenskreis, um die Liste der aktuellen Mitglieder anzuzeigen. Klicken oder tippen Sie auf das **Mülleimer**-Symbol neben dem Namen des zu entfernenden Mitglieds.
- Klicken oder tippen Sie in der Vertrauenskreis-Ansicht auf **Mitglieder**, und doppelklicken oder doppeltippen Sie auf das Mitglied, um die Vertrauenskreise anzuzeigen, zu denen es gehört. Klicken oder tippen Sie auf das **Mülleimer**-Symbol neben dem Mitglied, das aus diesem Vertrauenskreis entfernt werden soll.

Löschen eines Vertrauenskreises

Ein Vertrauenskreis kann nur von dessen Eigentümer gelöscht werden.

▲ Klicken oder tippen Sie in der Vertrauenskreis-Ansicht auf **Meine Vertrauenskreise**, und klicken oder tippen Sie auf das **Mülleimer**-Symbol neben dem zu löschenden Vertrauenskreis.

Mit dieser Aktion wird der Vertrauenskreis gelöscht. Außerdem werden E-Mails an alle Mitglieder des Vertrauenskreises gesendet, in denen sie über das Löschen des Vertrauenskreises informiert werden. Alle zu diesem Vertrauenskreis gehörigen Dateien und Ordner werden entschlüsselt.

Festlegen von Einstellungen

Klicken oder tippen Sie in der Vertrauenskreis-Ansicht auf **Einstellungen**. Es werden drei Registerkarten angezeigt.

- **E-Mail-Einstellungen**

Option	Beschreibung
Benutzername	Hier wird der zurzeit verwendete Benutzername angezeigt. Um ihn zu ändern, geben Sie einen neuen Benutzernamen in das Textfeld ein. Änderungen werden automatisch gespeichert.
E-Mail-Adresse	Hier wird das zurzeit verwendete E-Mail-Konto angezeigt. Um es zu ändern, klicken oder tippen Sie auf **E-Mail-Einstellungen ändern**, und folgen Sie den Anweisungen auf dem Bildschirm.

Option	Beschreibung
Bestätigung neuer Mitglieder	Wählen Sie eine der folgenden Optionen aus: ◦ **Automatisch bestätigen** – Nachdem die Akzeptanznachricht des oder der Eingeladenen empfangen wurde, werden die Mitglieder ohne weitere manuelle Eingabe in den Vertrauenskreis übernommen und es wird eine Bestätigungs-E-Mail an den oder die Eingeladenen gesendet. ◦ **Manuell bestätigen** – Nachdem die Akzeptanznachricht des oder der Eingeladenen empfangen wurde, muss die Registrierung der neuen Mitglieder manuell bestätigt werden. Erst nach der manuellen Eingabe wird eine Bestätigungs-E-Mail an den oder die Eingeladenen gesendet. ◦ **Überprüfung erforderlich** – Nachdem die Akzeptanznachricht des oder der Eingeladenen empfangen wurde, muss zur abschließenden Registrierung des oder der Eingeladenen ein Prüfcode übermittelt werden. Der Eigentümer des Vertrauenskreises muss den oder die Eingeladenen kontaktieren und den Prüfcode von ihnen anfordern. Erst nach Eingabe des richtigen Codes werden die Bestätigungs-E-Mails gesendet.
Regelmäßige Authentifizierung	Bei regelmäßiger Authentifizierung muss der Benutzer nach Ablauf des in Minuten angegebenen Zeitlimits bzw. während der Durchführung kritischer Aktionen das Windows Kennwort eingeben. Mit dieser Einstellung können Benutzer die Authentifizierung aktivieren oder deaktivieren.
Zeitlimit für Authentifizierung	Wählen Sie hier das Zeitlimit in Minuten aus, nach dessen Überschreitung eine Authentifizierung erforderlich ist.
Keine Bestätigungsmeldung anzeigen	Aktivieren oder deaktivieren Sie dieses Kontrollkästchen, um die Anzeige von Bestätigungsmeldungen zu aktivieren bzw. zu deaktivieren.
Ich möchte durch anonyme Nutzungsnachverfolgung zur Verbesserung von HP Trust Circles beitragen	Aktivieren oder deaktivieren Sie dieses Kontrollkästchen, je nachdem, ob Sie partizipieren möchten oder nicht.

- **Sichern/Wiederherstellen**

Option	Beschreibung
Sicherung	Kopiert Ihre Trust Circle Manager/Reader-Anwendungsdaten (Einstellungen und Vertrauenskreise) in eine Sicherungsdatei. Bei einem Absturz oder Systemfehler können Sie mithilfe dieser Datei für Ihre neue Installation von Trust Circles den in der Datei gespeicherten Zustand der Anwendungsdaten wiederherstellen. **HINWEIS:** Beim Sichern werden lediglich Ihre Trust Circles-Anwendungsdaten gespeichert, also Vertrauenskreise, Einstellungen und Mitglieder. Die Dateien in den Vertrauenskreis-Ordnern werden nicht gesichert. Diese Dateien sollten getrennt gesichert werden. So sichern Sie Einstellungen und Benutzerdaten von Trust Circles: **1.** Klicken oder tippen Sie auf **Sichern**. **2.** Wählen Sie einen Dateinamen und ein Verzeichnis für die Sicherungsdatei aus, und klicken oder tippen Sie anschließend auf **Speichern**. **3.** Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken oder tippen Sie auf **OK**. Dieses Kennwort ist für die Wiederherstellung der Datei erforderlich.
Wiederherstellen	Stellt Einstellungen und Vertrauenskreise von einer Sicherheitsdatei wieder her, gewöhnlich nach einem Systemabsturz oder einer Migration auf einen anderen Computer. So stellen Sie Einstellungen und Benutzerdaten von Trust Circles wieder her: **1.** Klicken oder tippen Sie auf **Wiederherstellen**. **2.** Navigieren Sie zu dem Verzeichnis und der gewünschten Sicherungsdatei, und klicken oder tippen Sie auf **Öffnen**. **3.** Geben Sie das Kennwort ein, das beim Erstellen der Sicherungsdatei eingerichtet wurde.

- **Info** – Durch Auswahl dieser Option wird die Version der Trust Circle Manager/Reader-Software angezeigt. Außerdem werden Links angezeigt, über die Sie einen Upgrade von Trust Circle Manager auf die Pro-Version durchführen oder die Datenschutzerklärung von HP anzeigen können.

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

Mit Computrace (separat zu erwerben) können Sie Ihren Computer aus der Ferne überwachen, verwalten und nachverfolgen.

Nach der Aktivierung wird Computrace über das Absolute Software Customer Center konfiguriert. Über das Customer Center kann der Administrator Computrace für die Überwachung oder Verwaltung des Computers konfigurieren. Falls das System verlegt oder gestohlen wird, kann das Customer Center den örtlichen Behörden helfen, den Computer zu orten und wiederzubeschaffen. Bei entsprechender Konfiguration funktioniert Computrace selbst dann weiter, wenn die Festplatte gelöscht oder ersetzt wird.

So aktivieren Sie Computrace:

1. Stellen Sie eine Verbindung zum Internet her.
2. Öffnen Sie HP Client Security. Weitere Informationen finden Sie unter „Öffnen von HP Client Security“ auf Seite 10.
3. Klicken Sie auf **Wiederbeschaffung gestohlener Geräte**.
4. Zum Starten des Computrace Aktivierungsassistenten klicken Sie auf **Los geht's**.
5. Geben Sie Ihre Kontakt- und Kreditkarteninformationen oder einen bereits gekauften Produktschlüssel ein.

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

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

So melden Sie sich beim Kundencenter an:

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

Im Kundencenter können Sie:

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

▲ Klicken Sie auf **Weitere Informationen**, um mehr über Computrace zu erfahren.

10 Ausnahmen für lokalisierte Kennwörter

Die Kennwortlokalisierung wird auf der Ebene der Systemstart-Authentifizierung und der Authentifizierung durch HP Drive Encryption nur eingeschränkt unterstützt. Weitere Informationen finden Sie unter „Keine Unterstützung für Windows IMEs während der Authentifizierung beim Systemstart und der HP Drive Encryption-Authentifizierung“ auf Seite 59.

Vorgehensweise, wenn ein Kennwort abgelehnt wird

Kennwörter können aus folgenden Gründen abgelehnt werden:

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

  1. Fügen Sie über die **Systemsteuerung** ein unterstütztes Tastaturlayout hinzu (zum Beispiel ein US-Tastaturlayout, wenn Chinesisch als Eingabesprache festgelegt ist).
  2. Legen Sie die unterstützte Tastatur als Standardeingabetastatur fest.
  3. Starten Sie HP Client Security, und geben Sie das Windows Kennwort ein.

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

  1. Ändern Sie das Windows Kennwort so, dass es nur unterstützte Zeichen enthält. Weitere Informationen zu nicht unterstützten Zeichen finden Sie unter „Behandeln von Sonderzeichen“ auf Seite 60.
  2. Starten Sie HP Client Security, und geben Sie das Windows Kennwort ein.

Keine Unterstützung für Windows IMEs während der Authentifizierung beim Systemstart und der HP Drive Encryption-Authentifizierung

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.

Die Verwendung von IMEs während der Authentifizierung beim Systemstart und der HP Drive Encryption-Authentifizierung wird nicht unterstützt. Ein IME kann nicht dazu verwendet werden, ein Windows Kennwort im Anmeldebildschirm der Authentifizierung beim Systemstart oder im HP Drive Encryption-Anmeldebildschirm einzugeben. Die Eingabe über einen IME kann zu einer Sperrung führen. In manchen Fällen zeigt Microsoft® Windows den IME nicht an, wenn der Benutzer das Kennwort eingibt.

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

- Microsoft IME für Japanisch
- Das japanische Tastaturlayout
- Office 2007 IME für Japanisch – Auch wenn Microsoft oder ein Dritter den Begriff IME oder Input Method Editor verwendet, handelt es sich bei der Eingabemethode nicht unbedingt um einen

IME. Dies kann zu Verwirrung führen, aber die Software liest die Hexadezimaldarstellung des Codes. Aus diesem Grund kann HP Client Security die Konfiguration unterstützen, wenn ein IME einem unterstützten Tastaturlayout zugeordnet ist.

VORSICHT! Wenn HP Client Security bereitgestellt wurde, werden mit einem Windows IME eingegebene Kennwörter abgelehnt.

Ändern des Kennworts mit einem Tastaturlayout, das ebenfalls unterstützt wird

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

HINWEIS: Administratoren können dieses Problem lösen, indem sie die Seite „Benutzer“ von HP Client Security (erreichbar über das **Zahnrad**-Symbol auf der Startseite) verwenden, das gewünschte Tastaturlayout im Betriebssystem auswählen und anschließend den Installationsassistenten für HP Client Security für denselben 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, welche 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 während der Authentifizierung beim Systemstart und der HP Drive Encryption-Authentifizierung dasselbe Kennwort eingegeben werden, wobei die Umschalttaste für Kleinschreibung bzw. die Umschalttaste und die Feststelltaste für Großschreibung gedrückt werden müssen. Bei der Eingabe von numerischen Kennwörtern muss der Ziffernblock verwendet werden.

- Koreanisch

  Wenn ein Benutzer ein unterstütztes koreanisches Tastaturlayout auswählt und dann ein Kennwort eingibt, muss während der Authentifizierung beim Systemstart und der HP Drive Encryption-Authentifizierung dasselbe Kennwort eingegeben werden, wobei die rechte Alt-Taste für Kleinschreibung und die rechte Alt-Taste und die Feststelltaste für Großschreibung gedrückt werden müssen.

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

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

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

Glossar

Administrator
Siehe *Windows Administrator*.

Aktivierung
Bezeichnet einen Vorgang, der abgeschlossen sein muss, bevor die Drive Encryption-Funktionen verfügbar sind. Administratoren können Drive Encryption über den Installationsassistenten von HP Client Security oder die Anwendung HP Client Security aktivieren. Der Aktivierungsprozess umfasst das Aktivieren der Software, die Verschlüsselung des Laufwerks und Erstellung einer ersten Sicherung des Verschlüsselungsschlüssels auf einem Wechselmedium.

Angeschlossenes Gerät
Ein Hardwaregerät, das mit einem Anschluss am Computer verbunden ist.

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

Anmeldeinformationen
Spezielle Informationen oder ein Hardware-Gerät zur Authentifizierung eines einzelnen Benutzers.

Authentifizierung
Der Prozess, der bestätigt, dass Sie die Person sind, für die Sie sich ausgeben. Verwendet werden hierfür Anmeldeinformationen, wie Ihr Windows Kennwort, Ihr Fingerabdruck, eine Smart Card, eine kontaktlose Karte oder eine Näherungskarte.

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
In File Sanitizer eingeplante Shred-Vorgänge.

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.

Bluetooth
Funktechnologie, mit der Bluetooth-fähige Computer, Drucker, Computermäuse, Mobiltelefone und andere Geräte über kurze Entfernungen drahtlos miteinander kommunizieren können.

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

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

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

Drive Encryption Anmeldebildschirm
Siehe „Drive Encryption-Systemstart-Authentifizierung“.

Drive Encryption-Systemstart-Authentifizierung
Ein Anmeldebildschirm, der angezeigt wird, bevor Windows startet. Benutzer müssen ihren Windows Benutzernamen und das Kennwort oder Ihre Smart Card-PIN eingeben oder mit einem registrierten Finger über den Sensor streichen. Wurde One-Step Logon ausgewählt, kann mit der Eingabe der richtigen Informationen am Drive Encryption-Anmeldebildschirm direkt auf Windows zugegriffen werden, ohne dass eine erneute Anmeldung am Windows Anmeldebildschirm erforderlich ist.

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

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

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

Fingerabdruck
Durch digitales Extrahieren Ihres Fingerabdruck-Bildes gewonnene Daten. Das tatsächliche Fingerabdruck-Bild wird nie von HP Client Security gespeichert.

Geräteklasse
Alle Geräte eines bestimmten Typs, beispielsweise Laufwerke.

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

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

Hardwareverschlüsselung
Die Verwendung von selbstverschlüsselnden Laufwerken, die den OPAL-Spezifikationen der Trusted Computing Group für die Verwaltung von selbstverschlüsselnden Laufwerken entsprechen, um eine sofortige Verschlüsselung zu erzielen. Die Hardware-Verschlüsselung erfolgt unmittelbar und dauert nur einige Minuten, wohingegen die Software-Verschlüsselung einige Stunden in Anspruch nehmen kann.

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

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

Identität
Eine Gruppe von Anmeldeinformationen und Einstellungen in HP Client Security, die wie ein Konto oder Profil eines bestimmten Benutzers behandelt werden.

Just-in-Time-Authentifizierung (JITA)
Eine Erläuterung hierzu finden Sie in der Hilfe für die Software HP Device Access Manager.

Kontaktlose Karte
Eine Plastikkarte mit integriertem Computerchip, die zur Authentifizierung verwendet werden kann.

Manuelles Shreddern
Sofortiges Shreddern eines Datenbestands oder ausgewählter Datenbestände unter Umgehung des planmäßigen Shredderns.

Näherungskarte
Eine Plastikkarte mit integriertem Computerchip, die Sie zur Authentifizierung in Verbindung mit weiteren Anmeldeinformationen für zusätzliche Sicherheit verwenden können.

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
Eine persönliche Identifikationsnummer für einen registrierten Benutzer, die zur Anmeldeauthentifizierung verwendet wird.

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

Shreddern
Die Ausführung eines Algorithmus, mit dem ein Datenbestand durch bedeutungslose Daten überschrieben wird.

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

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

Smart Card
Ein Hardwaregerät, das zur Authentifizierung unter Verwendung einer PIN verwendet werden kann.

Software-Verschlüsselung
Die Verwendung von Software, um die Festplatte Sektor für Sektor zu verschlüsseln. Dieser Vorgang ist wesentlich langsamer als die Hardware-Verschlüsselung.

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

Startseite
Ein zentraler Bereich, in dem Sie auf die Funktionen und Einstellungen von HP Client Security zugreifen und diese verwalten können.

TPM-Sicherheitschip (Trusted Platform Module)
Ein TPM authentifiziert einen Computer anstatt eines Benutzers. Dazu werden spezifische Informationen über das Host-System gespeichert, wie beispielsweise Verschlüsselungsschlüssel, digitale Zertifikate und Kennwörter. Durch ein TPM wird das Risiko minimiert, dass Informationen auf dem Computer durch physischen Diebstahl oder einen Angriff durch einen externen Hacker gefährdet werden.

Trust Circle Manager/Reader
Trust Circle Reader-Benutzer können lediglich Einladungen akzeptieren, die von Trust Circle Manager-Benutzern versendet werden. Trust Circle Manager-Benutzer hingegen können Vertrauenskreise erstellen. Zu den verfügbaren Funktionen gehören das Einladen per E-Mail zur Teilnahme an einem Vertrauenskreis und das

Akzeptieren der entsprechenden Einladungen von anderen. Sobald ein Vertrauenskreis eingerichtet ist, können durch diesen Vertrauenskreis geschützte Daten auf sichere Weise gemeinsam genutzt werden.

Überschreiben von freiem Speicherplatz
Das Überschreiben von gelöschten Datenbeständen und ungenutztem Speicherplatz mit willkürlichen Daten. Der gelöschte Datenbestand wird durch Überschreiben weitgehend unkenntlich gemacht, so dass das Wiederherstellen des Originaldatenbestands erschwert wird.

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

Vertrauenskreis
Ermöglicht eine bessere Kontrolle von Daten, indem diese an eine bestimmte Gruppe vertrauenswürdiger Benutzer gebunden werden. Dies verhindert, dass Daten zufällig oder absichtlich in falsche Hände geraten. Die Daten werden unter Verwendung der Zero Overhead Key Management-Technologie von CryptoMill geschützt und kryptografisch an einen Vertrauenskreis gebunden. Diese Bindung verhindert eine Entschlüsselung von Dokumenten oder anderer kritischer Informationen außerhalb des Vertrauenskreises.

Vertrauenskreis-Ordner
Jeder Ordner, der durch einen Vertrauenskreis geschützt ist.

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
Ein Benutzer mit der Berechtigung, sich in einem Netzwerk oder an einem bestimmten Computer anzumelden.

Index

A

aero verwalten 58
Aktivieren
  Drive Encryption für selbstverschlüsselnde Laufwerke 33
  Drive Encryption für Standard-Festplatten 33
Ändern von Kennwörtern mit verschiedenen Tastaturlayouts 60
Anmeldeinformationen
  Bearbeiten 22
  Hinzufügen 21
  Importieren und Exportieren 25
  Kategorien 23
  Verwalten 23
Anmelden am Computer 34
Anzeigen der Protokolldateien 45

B

Behandeln von Sonderzeichen 60
Benutzeransicht 47
Beschränken
  Zugriff auf sensible Daten 6
Bluetooth-Geräte 16

C

Computrace 58

D

Daten
  Zugriff beschränken auf 6
Deaktivieren von Drive Encryption 34
Diebstahl, Schutz vor 6

E

Einführung 51
Einschränken
  Zugriff auf Geräte 46
Einstellungen 15, 55
  Bluetooth-Geräte 16
  HP SpareKey 15
  Password Manager 26
  PIN 19
  Symbol 24
Entfernen von Dateien 54
Entfernen von Mitgliedern 54
Entfernen von Ordnern 54
Entschlüsseln
  Laufwerke 32
Erste Schritte 11
Erweiterte Einstellungen 49
Erweiterte Einstellungen für HP Client Security 27

F

Festlegen
  Shred-Zeitplan 41
  Zeitplan für das Überschreiben 42
Festplattenverwaltung 36
File Sanitizer 43
  Öffnen 40
  Setup-Verfahren 40
Fingerabdrücke
  Benutzereinstellungen 15
  Verwaltungseinstellungen 14
Fingerabdrücke registrieren 13
FSA SecurID 19
Funktionen, HP Client Security 1

G

Geräteklassen, nicht verwaltet 49

H

Hardware-Verschlüsselung 33, 34
Hinzufügen von Dateien 54
Hinzufügen von Mitgliedern 53
Hinzufügen von Ordnern 52
HP Client Security 13
HP Client Security Funktionen 1
HP Client Security Installation 9
HP Client Security öffnen 10
HP Device Access Manager 46
  Einfaches Setup 12
  Öffnen 46
HP Drive Encryption 32, 36
  Aktivieren 33
  Anmelden nach Aktivierung der Laufwerkverschlüsselung 33
  Deaktivieren 33
  Einfaches Setup 12
  Entschlüsseln einzelner Laufwerke 36
  Sichern und Wiederherstellen 37
  Verschlüsseln einzelner Laufwerke 36
  Verwalten von Drive Encryption 36
HP File Sanitizer 39
HP SpareKey 15
HP SpareKey-Wiederherstellung 38
HP Trust Circles 51

J

JITA-Konfiguration 48
JITA-Richtlinie
  Erstellen für Benutzer oder Gruppe 49
  Für Benutzer oder Gruppe deaktivieren 49

K

Karten 17
Kennwort
  Hinweise 8
  HP Client Security 7
  Richtlinien 6
  Sicher 8
  Verwalten 7
Kennwort abgelehnt 59
Kennwortausnahmen 59
Kennwortsicherheit 24
Kennwortwiederherstellung 15
Konfiguration
  Geräteklasse 47

Konfiguration der Just-In-Time-Authentifizierung 48

L
Laufwerkspartitionen entschlüsseln 36
Laufwerkspartitionen verschlüsseln 36
Löschen von Vertrauenskreisen 55

M
Manuelles Starten eines Shred-Vorgangs 44
Meine Richtlinien 29

N
Näherungskarten, kontaktlose Karten und Smart Cards, Einstellungen 18
Nicht autorisierten Zugriff verhindern 6
Nicht verwaltete Geräteklassen 49

O
Öffnen
File Sanitizer 40
HP Device Access Manager 46
Öffnen von Drive Encryption 32
Öffnen von Trust Circles 51

P
Password Manager 19, 20
Anzeigen und Verwalten von gespeicherten Authentifizierungen 12
Kurzanleitung 11
PIN 18
Protokolldateien anzeigen 45

R
Registrieren
Fingerabdrücke 13
Richtlinie
Administratorkennwort 27
Standardbenutzer 28

S
Schützen von Datenbeständen vor dem Shreddern 42
Shreddern
Manuell 44
Mit der rechten Maustaste klicken 44
Shreddern durch Rechtsklicken auf den Datenbestand 44
Shred-Profil 41
Shred-Zeitplan festlegen 41
Sicherheit 7
Rollen 7
Sicherheitsziele 5
Sicherheitsfunktionen 28
Sicherheitsziele 5
Sichern
HP Client Security Anmeldeinformationen 8
Sichern des Verschlüsselungsschlüssels 37
Small Business – Kurzanleitung zur Einrichtung 11
Smart Card
PIN 8
Software-Verschlüsselung 33, 34, 36
Starten des Überschreibens von freiem Speicherplatz 44
Steuern des Zugriffs auf Geräte 46
Symbol verwenden 43
Systemansicht 47

T
Trust Circles
Öffnen 51

U
Überschreiben
Manuell 44
Start 44
Zeitplan 42
Überschreiben von freiem Speicherplatz 42

V
Verknüpfungen
Kontextmenü-Taste 22
Verschlüsseln
Laufwerke 32
Verschlüsseln von Festplatten 35
Verschlüsselte Ordner 54
Verschlüsselung
Hardware 33, 34
Software 33, 34, 36
Verschlüsselungsschlüssel
Sichern 37
Verwalten
Kennwörter 19, 20
Laufwerkspartitionen verschlüsseln oder entschlüsseln 36
Verwaltungseinstellungen
Fingerabdrücke 14, 15
Verwenden von HP Client Security
Kennwort für Sicherung und Wiederherstellung 8

W
Wiederherstellen
HP Client Security Anmeldeinformationen 8
Wiederherstellen des Zugriffs mithilfe von Sicherungsschlüsseln 38
Windows Anmeldekennwort 7
Windows Kennwort ändern 16

Z
Ziele, Sicherheit 5
Zugriff
Nicht autorisierten Zugriff verhindern 6
Steuern von 46