

Dell Data Security Console – Benutzerhandbuch

Encryption Status/Authentication Enrollment v8.17



Anmerkungen, Vorsichtshinweise und Warnungen

- ⓘ ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.
- ⚠ VORSICHT:** Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.
- ⚠ WARNUNG:** Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

© 2017 Dell Inc. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

In den Dokumenten zu Dell Encryption, Endpoint Security Suite Pro, Endpoint Security Suite Enterprise und Data Guardian verwendete eingetragene Marken und Marken: Dell™ und das Logo von Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® und KACE™ sind Marken von Dell Inc. Cylance®, CylancePROTECT und das Cylance Logo sind eingetragene Marken von Cylance, Inc. in den USA und anderen Ländern. McAfee® und das McAfee-Logo sind Marken oder eingetragene Marken von McAfee, Inc. in den USA und anderen Ländern. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, und Xeon® sind eingetragene Marken der Intel Corporation in den USA und anderen Ländern. Adobe®, Acrobat® und Flash® sind eingetragene Marken von Adobe Systems Incorporated. Authen Tec® und Eikon® sind eingetragene Marken von Authen Tec. AMD® ist eine eingetragene Marke von Advanced Micro Devices, Inc. Microsoft®, Windows® und Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, und Visual C++® sind entweder Marken oder eingetragene Marken von Microsoft Corporation in den USA und/oder anderen Ländern. VMware® ist eine eingetragene Marke oder eine Marke von VMware, Inc. in den USA oder anderen Ländern. Box® ist eine eingetragene Marke von Box. DropboxSM ist eine Dienstleistungsmarke von Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® und Google™ Play sind entweder Marken oder eingetragene Marken von Google Inc. in den Vereinigten Staaten oder anderen Ländern. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® und Siri® sind entweder Dienstleistungsmarken, Marken oder eingetragene Marken von Apple, Inc. in den Vereinigten Staaten oder anderen Ländern. GO ID®, RSA® und SecurID® sind eingetragene Marken von Dell EMC. EnCase™ und Guidance Software® sind entweder Marken oder eingetragene Marken von Guidance Software. Entrust® ist eine eingetragene Marke von Entrust®, Inc. in den USA und anderen Ländern. InstallShield® ist eine eingetragene Marke von Flexera Software in den USA, China, der EU, Hong Kong, Japan, Taiwan und Großbritannien. Micron® und RealSSD® sind eingetragene Marken von Micron Technology, Inc. in den USA und anderen Ländern. Mozilla® Firefox® ist eine eingetragene Marke von Mozilla Foundation in den USA und/oder anderen Ländern. iOS® ist eine Marke oder eingetragene Marke von Cisco Systems, Inc. in den USA und bestimmten anderen Ländern und wird in Lizenz verwendet. Oracle® und Java® sind eingetragene Marken von Oracle und/oder seinen Tochtergesellschaften. Andere Namen können Marken ihrer jeweiligen Inhaber sein. SAMSUNG™ ist eine Marke von SAMSUNG in den USA oder anderen Ländern. Seagate® ist eine eingetragene Marke von Seagate Technology LLC in den USA und/oder anderen Ländern. Travelstar® ist eine eingetragene Marke von HGST, Inc. in den USA und anderen Ländern. UNIX® ist eine eingetragene Marke von The Open Group. VALIDITY™ ist eine Marke von Validity Sensors, Inc. in den USA und anderen Ländern. VeriSign® und andere zugehörige Marken sind Marken oder eingetragene Marken von VeriSign, Inc. oder seinen Tochtergesellschaften und verbundenen Unternehmen in den USA und anderen Ländern und werden von der Symantec Corporation in Lizenz verwendet. KVM on IP® ist eine eingetragene Marke von Video Products. Yahoo!® ist eine eingetragene Marke von Yahoo! Inc. Dieses Produkt verwendet Teile des Programms 7-Zip. Der Quellcode ist unter 7-zip.org verfügbar. Die Lizenzierung erfolgt gemäß der GNU LGPL-Lizenz und den unRAR-Beschränkungen (7-zip.org/license.txt).

Dell Data Security Console – Benutzerhandbuch

2018 - 01

Rev. A01

1 Dell Data Security Console – Einführung.....	4
Kontaktaufnahme mit dem Dell ProSupport.....	4
2 Data Security Console.....	5
Navigation.....	5
3 Verschlüsselungsstatus.....	8
4 Registrierungen.....	9
Erstmaliges Eintragen von Anmeldeinformationen.....	9
Hinzufügen, Ändern oder Anzeigen von Registrierungen.....	9
Passwort.....	10
Wiederherstellungsfragen.....	10
Wiederherstellungsfragen bereits eingetragen.....	10
Fingerabdrücke.....	11
Smart Cards.....	11
5 Glossar.....	12

Dell Data Security Console – Einführung

Dell Advanced Authentication bietet einfach zu verwendende und intuitive Werkzeuge zur Erhöhung der Sicherheit auf Ihrem Computer.

Die folgenden Funktionen sind über die Data Security Console auf dem Betriebssystem einer Workstation verfügbar:

- Registrieren von Anmeldeinformationen für die Verwendung mit Advanced Authentication
- Nutzen der Vorteile von mehrstufigen Anmeldeinformationen, einschließlich Passwörter, Fingerabdrücke und Smartcards
- Wiederherstellen des Zugangs zu Ihrem Computer ohne Helpdesk-Anrufe oder Administratorunterstützung, wenn Sie Ihr Passwort vergessen haben
- Sicherung und Wiederherstellung Ihrer Programmdateien
- Einfache und leichte Änderung Ihres Windows-Passworts
- Festlegen persönlicher Einstellungen
- Anzeigen des Verschlüsselungsstatus (auf Computern mit [selbstverschlüsselnden Laufwerken](#))

Data Security Console

Die Data Security Console ist die Oberfläche, über die Sie sich registrieren, Ihre Anmeldeinformationen verwalten und Wiederherstellungsfragen konfigurieren können.

Sie haben Zugriff auf die folgenden Anwendungen:

- Das Verschlüsselungstool ermöglicht Ihnen, den Verschlüsselungsstatus der Computerlaufwerke anzuzeigen.
- Mit dem Eintragungstool können Sie Anmeldeinformationen einrichten und verwalten, Wiederherstellungsfragen konfigurieren und den Status Ihrer Anmeldeinformationseintragung anzeigen. Ob Sie die Möglichkeit zur Registrierung von allen Anmeldeinformationstypen haben, wird durch den Administrator festgelegt.

Diese Anleitung beschreibt, wie jede dieser Anwendungen verwendet wird.

Stellen Sie sicher, dass Sie in regelmäßigen Abständen dell.com/support nach aktualisierten Dokumenten überprüfen.

Kontaktaufnahme mit dem Dell ProSupport

Telefonischen Support rund um die Uhr für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell Produkte unter dell.com/support zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Halten Sie bei Ihrem Anruf Ihre Service-Tag-Nummer oder Ihren Express-Servicecode bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter [Dell ProSupport – Internationale Telefonnummern](#).

Data Security Console

Die Data Security Console bietet Zugriff auf Anwendungen, die die Sicherheit für alle Benutzer des Computers gewährleisten, um den Verschlüsselungsstatus der Laufwerke und Partitionen des Computers anzuzeigen und zu verwalten und, basierend auf vom Administrator festgelegten Richtlinien, ihre Anmeldungen bei Websites, Programmen und Netzwerkressourcen zu verwalten und ihre Anmeldeinformationen zur Authentifizierung auf einfache Weise zu registrieren.

Zum Öffnen der Data Security Console doppelklicken Sie vom *Desktop* aus auf das Symbol **Dell Data Security Console**.

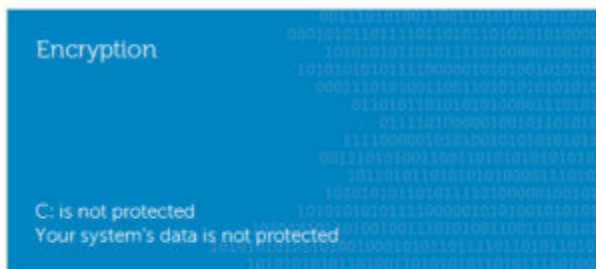


Wenn die Data Security Console startet, werden auf der Startseite die Anwendungen Advanced Authentication angezeigt:

- [Verschlüsselungsstatus](#)
- [Registrierungen](#)
- Um Anmeldeinformationen erstmalig einzurichten, wählen Sie den Link **Erste Schritte** auf der Kachel „Registrierungen“ aus. Ein Assistent leitet Sie durch den kurzen Registrierungsvorgang. Weitere Informationen finden Sie unter [Erstmaliges Eintragen von Anmeldeinformationen](#).

Navigation

Klicken Sie zum Öffnen einer Anwendung auf die entsprechende Kachel.



Dell Encryption Enterprise v5.16.0

Titelleiste

Um innerhalb einer Anwendung zur Startseite zurückzukehren, klicken Sie in der linken Ecke der Titelleiste auf den Rückwärtspfeil, der sich neben dem Namen der aktiven Anwendung befindet.

Um direkt zu einer anderen Anwendung zu navigieren, klicken Sie den Pfeil nach unten neben dem Namen der aktiven Anwendung, und wählen Sie eine andere Anwendung aus.

Um die Data Security Console zu minimieren, zu maximieren oder zu schließen, klicken Sie auf das entsprechende Symbol in der rechten Ecke der Titelleiste.



Um die Data Security Console nach dem Minimieren wiederherzustellen, doppelklicken Sie auf das Taskleistensymbol.

Um die Hilfe zu öffnen, klicken Sie auf das ? in der Titelleiste.



Data Security Console – Details

Um Informationen zur Data Security Console, zu den Richtlinien, Ausführungsdiensten und Protokollen anzuzeigen, klicken Sie auf das Zahnradsymbol auf der linken Seite der Titelleiste. Diese Informationen können beispielsweise vom Administrator im Rahmen des technischen Supports benötigt werden.



Wählen Sie ein Element im Menü aus.

Menüelement	Zweck
Info	Enthält Versions- und Copyright-Informationen.
Info anzeigen	Enthält die folgenden Informationen: <ul style="list-style-type: none"> · Produktversion und Datumsinformationen · ob die Data Security Console auf diesem Computer durch einen Unternehmens- oder einen lokalen Administrator verwaltet wird · Versionsnummern für Betriebssystem, BIOS, Hauptplatine und TPM (Trusted Platform Module).
MS Info	Führt das Dienstprogramm für Microsoft Windows-Systeminformationen aus, um detaillierte Informationen zur Hardware, zu den Komponenten und der Softwareumgebung anzuzeigen.
Info kopieren	Kopiert alle Systeminformationen in die Zwischenablage, um sie in eine E-Mail an Ihren Administrator oder den Dell ProSupport einzufügen.
Feedback	Zeigt ein Formular an, mit dem Sie Dell Feedback zu diesem Produkt geben können. (Auf Nicht-Domänencomputern ist diese Option jederzeit verfügbar. Auf Domänencomputern richtet sich diese Option der Unternehmensrichtlinie.)
Richtlinien	Zeigt eine Hierarchie der Richtlinien an, die auf diesem Computer gelten.
Services	Zeigt Details zu den ausgeführten Diensten an.
Support	Stellt eine Verbindung zur Dell ProSupport-Website her.
Protokolle	Zeigt eine detaillierte Liste der protokollierten Ereignisse für Fehlerbehebungszwecke an.
Start Ablaufverfolgung	Hiermit können Sie die Aufzeichnung der Anmeldeaktivitäten zur Fehlerbehebung starten und anhalten.



Verschlüsselungsstatus

Auf der Seite „Verschlüsselung“ wird der Verschlüsselungsstatus des Computers angezeigt. Ist eine Festplatte, ein Laufwerk oder eine Partition nicht verschlüsselt, wird der Status als *Schutz aufgehoben* angezeigt. Ein Laufwerk oder eine Partition, das bzw. die verschlüsselt ist, wird mit dem Status als *Geschützt* angezeigt.

Um den Verschlüsselungsstatus zu aktualisieren, klicken Sie mit der rechten Maustaste auf die jeweilige Festplatte, das Laufwerk oder die Partition und dann auf **Aktualisieren**.

Registrierungen

Mit dem Registrierungstool können Sie basierend auf den vom Administrator festgelegten Richtlinien Registrierungen und Änderungen vornehmen sowie den Registrierungsstatus überprüfen.

Wenn Sie Ihre Anmeldeinformationen zum ersten Mal bei der Data Security Console eintragen, führt Sie ein Assistent durch den Eintragungsprozess für Passwortänderung, Wiederherstellungsfragen, Fingerabdrücke und Smart Card. Je nach Richtlinie können Sie die einzelnen Anmeldeinformationen registrieren oder übergehen. Nach der erstmaligen Registrierung können Sie auf die Kachel „Registrierungen“ klicken, um Anmeldeinformationen hinzuzufügen oder zu ändern.

ANMERKUNG: Die Kachel "Anmeldungen" wird nur angezeigt, wenn die PBA aktiv ist.

Erstmaliges Eintragen von Anmeldeinformationen

Gehen Sie wie folgt vor, um Anmeldeinformationen erstmals einzutragen:

- 1 Klicken Sie auf der Data Security Console-Startseite auf den Link **Erste Schritte** auf der Registrierungsschaltfläche.
- 2 Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.
- 3 Melden Sie sich auf dem Dialogfeld „Authentifizierung erforderlich“ mit Ihrem Windows-Kennwort an und klicken Sie auf **OK**.
- 4 Um Ihr Windows-Kennwort zu ändern, geben Sie auf der Seite „Kennwort“ ein neues Passwort ein, bestätigen es und klicken dann auf **Weiter**.
Um den Schritt der Kennwort-Änderung zu überspringen, klicken Sie auf **Überspringen**. Der Assistent bietet Ihnen die Möglichkeit, eine Anmeldeinformation zu überspringen, falls Sie diese nicht eintragen möchten. Um zu einer vorherigen Seite zurückzukehren, klicken Sie auf **Zurück**.
- 5 Folgen Sie den jeweiligen Bildschirmanweisungen, und klicken Sie nach Bedarf auf die folgenden Schaltflächen: **Weiter**, **Überspringen** und **Zurück**.
- 6 Bestätigen Sie auf der Zusammenfassungsseite die eingetragenen Anmeldeinformationen, und klicken Sie anschließend auf **Übernehmen**.
Um zu einer Seite für die Eintragung von Anmeldeinformationen zurückzukehren und dort Änderungen durchzuführen, klicken Sie solange auf **Zurück**, bis Sie auf der Seite angekommen sind, die Sie ändern möchten.

Detailliertere Informationen über die Registrierung von Anmeldeinformationen oder die Änderung von Anmeldeinformationen finden Sie unter [Hinzufügen, Ändern oder Anzeigen von Registrierungen](#).

Hinzufügen, Ändern oder Anzeigen von Registrierungen

Klicken Sie zum Hinzufügen, Ändern oder Anzeigen von Registrierungen auf die Kachel **Registrierungen**.

Register im linken Fenster zeigen verfügbare Eintragungen an. Sie variieren je nach Plattform und Hardware.

Die Seite „Status“ zeigt die unterstützten Anmeldeinformationen, die zugehörigen Richtlinieneinstellungen („Erforderlich“ oder „–“) sowie den Eintragungsstatus an. Über diese Seite können Benutzer ihre Registrierungen auf Basis der durch den Administrator definierten Richtlinie verwalten.

- Um eine Anmeldeinformation zum ersten Mal einzutragen, klicken Sie in der Zeile der Anmeldeinformation auf **Registrieren**.



- Um eine bereits eingetragene Anmeldeinformation zu löschen, klicken Sie auf **Löschen**.
- Wenn die Richtlinie nicht zulässt, dass Benutzer ihre eigenen Anmeldeinformationen registrieren oder ändern, sind die Links **Registrieren** und **Löschen** auf der Statusseite deaktiviert.
- Um eine vorhandene Registrierung zu ändern, klicken Sie auf die entsprechende Registerkarte im linken Bereich.

Wenn Richtlinie keine Registrierung oder Änderung von Anmeldeinformationen zulässt, wird die Meldung „Änderung der Anmeldeinformationen laut Richtlinie unzulässig“ auf der Seite für die Eintragung von Anmeldeinformationen angezeigt.

Passwort

So ändern Sie Ihr Windows-Passwort:

- 1 Klicken Sie auf die Registerkarte **Kennwort**.
- 2 Geben Sie Ihr derzeitiges Windows-Passwort ein.
- 3 Geben Sie das neue Passwort ein, wiederholen Sie es zur Bestätigung und klicken Sie anschließend auf **Ändern**.
Kennwortänderungen sind sofort gültig.
- 4 Klicken Sie im Eintragungsdialog auf **OK**.

ANMERKUNG:

Sie sollten Ihr Windows-Passwort nur in der Data Security Console und nicht in Windows ändern. Falls das Windows-Passwort außerhalb der Data Security Console geändert wird, stimmen die Passwörter nicht mehr überein. In diesem Fall muss eine Wiederherstellung durchgeführt werden.

Wiederherstellungsfragen

Auf der Seite „Wiederherstellungsfragen“ können Sie Ihre Wiederherstellungsfragen und -antworten erstellen, löschen oder ändern. Wiederherstellungsfragen ermöglichen es Ihnen, über ein Frage-Antwort-Verfahren auf Ihr Windows-Konto zuzugreifen, wenn Sie beispielsweise Ihr Passwort vergessen haben oder dieses abgelaufen ist.

ANMERKUNG:

Wiederherstellungsfragen werden nur dazu verwendet, den Zugriff auf einen Computer wiederherstellen. Die Fragen und Antworten können nicht für die Anmeldung verwendet werden.

Gehen Sie folgendermaßen vor, falls Sie noch keine Wiederherstellungsfragen eingetragen haben:

- 1 Klicken Sie auf die Registerkarte **Wiederherstellungsfragen**.
- 2 Wählen Sie in einer Liste vordefinierter Fragen aus, geben Sie dann Ihre Antworten ein, und bestätigen Sie diese.
- 3 Klicken Sie auf **Registrieren**.

ANMERKUNG:

Klicken Sie auf die Schaltfläche **Wiederherstellen**, um die Auswahl auf dieser Seite zu löschen und erneut zu beginnen.

Wiederherstellungsfragen bereits eingetragen

Wenn bereits Wiederherstellungsfragen eingetragen wurden, können Sie diese entweder löschen oder erneut eintragen.

- 1 Klicken Sie auf die Registerkarte **Wiederherstellungsfragen**.
- 2 Klicken Sie auf die entsprechende Schaltfläche:
 - Um die Wiederherstellungsfragen vollständig zu löschen, klicken Sie auf **Löschen**.

- Um die Wiederherstellungsfragen und die zugehörigen Antworten neu zu definieren, klicken Sie auf **Erneut registrieren**.

Fingerabdrücke

① ANMERKUNG:

Um diese Funktion nutzen zu können, muss Ihr Computer über einen Fingerabdruckleser verfügen.

Gehen Sie folgendermaßen vor, um Fingerabdrücke einzutragen:

- 1 Klicken Sie auf die Registerkarte **Fingerabdrücke**.
- 2 Klicken Sie auf der Seite „Fingerabdrücke“ auf den Finger, den Sie eintragen möchten.
- 3 Folgen Sie den Anweisungen im Bildschirm, um Ihren Fingerabdruck einzutragen.

① ANMERKUNG:

Der jeweilige Finger muss vier Mal erfolgreich gescannt werden, um als eingetragen zu gelten. Die Anzahl der zur Fingerabdruckeintragung erforderlichen Scans richtet sich nach der Qualität der einzelnen Fingerabdruckscans. Mindest- und Maximalanzahl der Fingerabdrücke wurden vom Administrator festgelegt.

- 4 Klicken Sie auf den jeweils nächsten zu scannenden Finger, bis Sie die gemäß Richtlinie erforderliche Mindestanzahl von Fingerabdrücken eingetragen haben.
Falls Sie nicht die Mindestanzahl an Fingerabdrücken eingetragen haben, werden Sie anhand eines Dialogfelds darüber informiert. Klicken Sie zum Fortfahren auf **OK**.
- 5 Schließen Sie den Scanvorgang für die erforderliche Anzahl an Fingerabdrücken ab und klicken Sie dann auf **Speichern**.
Um einen gescannten Fingerabdruck zu löschen, klicken Sie auf der Seite für die Fingerabdruckeintragung auf einen markierten Fingerabdruck, um die Eintragung für diesen Abdruck aufzuheben. Klicken Sie dann zum Bestätigen des Löschvorgangs auf **Ja** und anschließend auf **Speichern**.

Smart Cards

① ANMERKUNG:

Um diese Funktion nutzen zu können, muss Ihr Computer über einen Smart-Card-Leser verfügen.

Führen Sie für das Eintragen von Smart Cards die folgenden Schritte aus:

- 1 Klicken Sie auf die Registerkarte **Smart Card**.
- 2 Tragen Sie die Smart Card je nach Kartentyp ein:
 - Legen Sie die Smart Card in den Kartenleser ein.
 - Bei einer kontaktlosen Karte genügt es, diese auf dem Lesegerät zu platzieren oder sie in dessen Nähe zu halten.
- 3 Wird die Karte erkannt, wird ein grünes Kontrollkästchen und die Aufforderung *Die Karte anmelden* angezeigt. Wählen Sie **Karte registrieren** aus.
- 4 Klicken Sie im Eintragsdialog auf **OK**.

Um die Eintragung aller mit dem Benutzer verknüpften Smart Cards aufzuheben, wählen Sie auf der Seite für die Smart Card-Eintragung **Registrierte Karten von Ihrem Konto entfernen** aus.



Glossar

Anmeldeinformationen – Über Anmeldeinformationen, wie beispielsweise einen Fingerabdruck oder das Windows-Passwort wird die Identität einer Person nachgewiesen.

Preboot-Authentifizierung (PBA) – Die Preboot-Authentifizierung dient als Erweiterung des BIOS oder der Systemstart-Firmware und schafft eine sichere, manipulationsgeschützte Umgebung außerhalb des Betriebssystems als vertrauenswürdige Authentifizierungsebene. Die PBA unterbindet den Zugriff auf die Festplatte und somit auch auf das Betriebssystem, bis der Benutzer die richtigen Anmeldeinformationen eingibt.

Geschützt – Bei selbstverschlüsselnden SED-Laufwerken ist der Computer geschützt, wenn das SED aktiviert wurde und die PBA (Pre-Boot-Authentifizierung) eingesetzt wird.

Selbstverschlüsselnde Laufwerke (SEDs) - Eine Festplatte mit einem eingebauten Verschlüsselungsmechanismus, der automatisch alle Daten verschlüsselt, die auf dem Medium gespeichert werden und alle Daten entschlüsselt, die das Medium verlassen. Dieser Typ der Verschlüsselung ist für den Benutzer völlig transparent.

Single Sign-on (SSO): Die einstufige Anmeldung vereinfacht den Anmeldevorgang, wenn die mehrstufige Authentifizierung sowohl vor dem Neustart als auch bei der Windows-Anmeldung aktiviert ist. Wenn aktiviert, ist eine Authentifizierung nur vor dem Neustart erforderlich, und Benutzer werden automatisch bei Windows angemeldet. Wenn nicht aktiviert, ist die Authentifizierung möglicherweise mehrfach erforderlich.

Trusted Platform Module (TPM) – Das TPM ist ein Sicherheits-Chip mit drei Hauptfunktionen: sicherer Speicher, Messung und Bestätigung. Beim Encryption-Client wird das TPM für den sicheren Speicher genutzt. Das TPM kann auch verschlüsselte Container für das Software-Vault bereitstellen.