Dell Data Protection | Access – Startseite

Die Startseite von **Dell Data Protection | Access** stellt den zentralen Ausgangspunkt dar, um auf die Funktionen dieser Anwendung zuzugreifen. In diesem Fenster können Sie folgende Funktionen aufrufen:

System Access Wizard
Zugriffsoptionen
Self-Encrypting Drive
Erweiterte Optionen

Unten rechts im Fenster befindet sich die Verknüpfung **Erweitert**, auf die Sie klicken können, um erweiterte Optionen aufzurufen.

Im Fenster Erweiterte Optionen können Sie unten rechts auf die Verknüpfung **Startseite** klicken, um zur Startseite zurückzukehren.

System Access Wizard

Der System Access Wizard wird automatisch beim ersten Start der Anwendung **Dell Data Protection | Access** gestartet. Der Assistent führt Sie durch die Einrichtung aller Sicherheitsaspekte auf Ihrem System, unter anderem wie Sie sich am System anmelden (z. B. nur mit Kennwort oder mit Fingerabdruck und Kennwort) und wann (beim Windows-Start, vor dem Windows-Start oder zu beiden Zeitpunkten). Wenn Ihr System über ein Self-Encrypting Drive verfügt, können Sie dieses mit diesem Assistenten konfigurieren.

Administratorfunktionen

Benutzer, die auf dem System mit Windows-Administratorrechten eingerichtet wurden, verfügen über die Berechtigung, in **Dell Data Access | Protection** die folgenden Funktionen auszuführen, die Standardbenutzer nicht ausführen können:

- Systemkennwort (Pre-Windows) festlegen/ändern
- Festplattenkennwort festlegen/ändern
- Administratorkennwort festlegen/ändern
- TPM-Besitzerkennwort festlegen/ändern
- ControlVault-Administratorkennwort festlegen/ändern
- System zurücksetzen
- Anmeldedaten archivieren und wiederherstellen
- Administrator-PIN für Smartcard festlegen/ändern
- Smartcard löschen/zurücksetzen
- Dell Secure-Anmeldung für Windows aktivieren/deaktivieren
- Windows-Anmelderichtlinie festlegen
- Self-Encrypting Drives verwalten, z. B.:
    - Sperre für Self-Encrypting Drive aktivieren/deaktivieren
    - Windows-Kennwortsynchronisierung (WPS) aktivieren/deaktivieren
    - Single Sign-On (SSO) aktivieren/deaktivieren
    - Kryptografische Löschung ausführen

Fernverwaltung

Ihre Organisation kann eine Umgebung einrichten, in der die Sicherheitsfunktionen der Anwendung **Dell Data Protection | Access** auf mehreren Plattformen zentral verwaltet werden (mit der sogenannten Fernverwaltung). In diesem Fall kann die Windows-Sicherheitsinfrastruktur, z. B. Active Directory, zum sicheren Verwalten spezifischer Funktionen von **Dell Data Protection | Access** verwendet werden.

Wenn ein Computer fernverwaltet wird (z. B. wenn der Fernadministrator der "Besitzer" ist), wird die lokale Verwaltung der Funktionen von **Dell Data Protection | Access** deaktiviert. Es kann dann nicht mehr lokal auf die Verwaltungsfenster der Anwendung zugegriffen werden. Die Fernverwaltung kann für folgende Funktionen verwendet werden:

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows-Anmeldung
- System zurücksetzen
- BIOS-Kennwörter
- Windows-Anmelderichtlinie
- Self-Encrypting Drives
- Registrierung von Fingerabdrücken und Smartcards

Um weitere Informationen zur Verwendung von EMBASSY® Remote Administration Server (ERAS) von Wave Systems für die Fernverwaltung anzufordern, wenden Sie sich bitte an Ihren Dell-Vertreter, oder informieren Sie sich auf dell.com.

Zugriffsoptionen

Im Fenster Zugriffsoptionen können Sie einstellen, wie Sie auf Ihr System zugreifen.

Wenn Sie Optionen von **Dell Data Protection | Access** eingerichtet haben, werden diese mit den verfügbaren Optionen (z. B. Kennwort für Pre-Windows-Anmeldung ändern) auf der Startseite angezeigt. Bei den verfügbaren Optionen handelt es sich um Verknüpfungen, mit denen Sie per Mausklick zum entsprechenden Fenster gelangen, um eine bestimmte Aufgabe auszuführen (z. B. Ändern Ihres Pre-Windows-Kennworts oder Registrierung eines weiteren Fingerabdrucks).

Allgemein
Zunächst können Sie angeben, wann (Windows, Pre-Windows oder beides) und wie (z. B. per Fingerabdruck und Kennwort) die Anmeldung erfolgen soll. Sie können eine oder zwei Optionen dafür auswählen, wie die Anmeldung erfolgen soll; dazu zählen Kombinationen aus Fingerabdruck, Smartcard und Kennwort. Die aufgeführten Optionen sind von den Anmelderichtlinien abhängig, die in Ihrer Umgebung gelten, und davon, was auf der Plattform unterstützt wird.

Fingerabdruck
Wenn Ihr System über einen Fingerabdruckscanner verfügt, können Sie Fingerabdrücke registrieren oder aktualisieren, die Sie zum Anmelden am System verwenden. Nachdem Sie die Fingerabdrücke registriert haben, können Sie die registrierten Finger beim Windows-Start, vor dem Windows-Start oder zu beiden Zeitpunkten (je nachdem, was Sie in den allgemeinen Zugriffsoptionen angegeben haben) über den Fingerabdruckscanner des Systems ziehen, um auf Ihr System zuzugreifen. Weitere Informationen finden Sie unter Registrieren von Fingerabdrücken.

Pre-Windows-Anmeldung
Wenn Sie festgelegt haben, dass sich die Benutzer vor dem Windows-Start anmelden, müssen Sie ein Systemkennwort (manchmal Pre-Windows-Kennwort genannt) für den Zugriff vor dem Windows-Start einrichten. Sobald dieses eingerichtet wurde, kann der Administrator das Kennwort jederzeit ändern.

Sie können die Pre-Windows-Anmeldung in diesem Fenster auch deaktivieren. Dazu müssen Sie Ihr aktuelles Systemkennwort eingeben, das Kennwort bestätigen und dann auf die Schaltfläche **Deaktivieren** klicken.

Smartcard
Wenn Sie festgelegt haben, dass die Benutzer sich mit einer Smartcard anmelden, müssen Sie mindestens eine herkömmliche (auch als "Contacted" bezeichnet) oder Contactless Smartcard registrieren. Klicken Sie auf die Verknüpfung **Eine weitere Smartcard registrieren**, um den Assistenten zur Smartcard-Registrierung zu starten. Bei der Registrierung wird Ihre Smartcard für die Anmeldung eingerichtet.

Nachdem Sie eine Smartcard registriert haben, können Sie über die Verknüpfung **Meine Smartcard-PIN ändern oder einrichten** eine PIN für diese Karte ändern oder einrichten.

Pre-Windows-Anmeldung

Wenn die Pre-Windows-Anmeldung eingerichtet ist, müssen Sie sich beim Systemstart authentifizieren (mit Kennwort, Fingerabdruck oder Smartcard), bevor Windows geladen wird. Die Pre-Windows-Anmeldefunktion bietet zusätzliche Sicherheit für das System, indem nicht berechtigte Benutzer davon abgehalten werden, Windows zu beeinträchtigen oder auf den Computer zuzugreifen (z. B. wenn er gestohlen wurde).

Im Fenster "Pre-Windows-Anmeldung" können Administratoren die Pre-Windows-Anmeldung einrichten oder ein Pre-Windows-Kennwort (Systemkennwort) erstellen oder ändern. Wenn dieses Kennwort bereits festgelegt wurde, können Sie die Pre-Windows-Anmeldung in diesem Fenster deaktivieren. Beim Einrichten der Pre-Windows-Anmeldung wird ein Assistent gestartet, der folgende Schritte ausführt:

- Systemkennwort: Systemkennwort (auch Pre-Windows-Kennwort genannt) für den Zugriff vor dem Windows-Start einrichten. Dieses Kennwort wird auch als Sicherung verwendet, falls ein Benutzer über zusätzliche Authentifizierungsfaktoren verfügt (z. B. um sich am System anzumelden, wenn es Probleme mit dem Fingerabdruckscanner gibt).
- Fingerabdruck oder Smartcard: Fingerabdruck oder Smartcard für die Pre-Windows-Anmeldung einrichten und festlegen, ob dieser Authentifizierungsfaktor anstelle von oder zusätzlich zum Pre-Windows-Kennwort verwendet wird.
- Single Sign-On: Standardmäßig wird Ihre Pre-Windows-Authentifizierung (Kennwort, Fingerabdruck oder Smartcard) automatisch auch für die Windows-Anmeldung verwendet (diese Einmalanmeldung wird als "Single Sign-On" bezeichnet). Wenn Sie diese Funktion deaktivieren möchten, aktivieren Sie das Kontrollkästchen "Ich möchte mich beim Windows-Start erneut anmelden".
- Wenn zusätzlich zu einem Pre-Windows-Kennwort ein BIOS-Festplattenkennwort festgelegt wurde, haben Sie auch die Möglichkeit, das Festplattenkennwort zu ändern oder zu deaktivieren.

HINWEIS: Nicht alle Fingerabdruckscanner können für die Pre-Windows-Authentifizierung verwendet werden. Wenn Ihr Scanner nicht kompatibel ist, können Sie lediglich Fingerabdrücke für die Windows-Anmeldung registrieren. Um herauszufinden, ob ein bestimmter Fingerabdruck-Scanner kompatibel ist, wenden Sie sich an Ihren Systemadministrator, oder lesen Sie die Liste der unterstützten Fingerabdruck-Scanner auf support.dell.com.

Pre-Windows-Anmeldung deaktivieren
Sie können die Pre-Windows-Anmeldung in diesem Fenster auch deaktivieren. Dazu müssen Sie Ihr aktuelles Pre-Windows-Kennwort (Systemkennwort) eingeben, das Kennwort bestätigen und dann auf die Schaltfläche **Deaktivieren** klicken. Beachten Sie, dass bei der Deaktivierung der Pre-Windows-Anmeldung sämtliche registrierte Fingerabdrücke oder Smartcards weiterhin registriert bleiben.

Registrieren/Entfernen von Fingerabdrücken

Die Benutzer können Fingerabdrücke registrieren oder aktualisieren, mit denen sie sich entweder vor dem Windows-Start oder bei der Windows-Anmeldung authentifizieren können. Auf der Registerkarte "Fingerabdruck" wird mithilfe von Handabbildungen angezeigt, welche Finger ggf. registriert wurden. Durch Klicken auf die Verknüpfung **Einen weiteren registrieren** wird der Fingerabdruck-Anmeldungsassistent gestartet, der Sie durch den Registrierungsvorgang führt. Bei der Registrierung wird ein Fingerabdruck für die Anmeldung gespeichert. Sie müssen über einen funktionierenden, ordnungsgemäß installierten und konfigurierten Fingerabdruckscanner verfügen, um Fingerabdrücke zu registrieren.

HINWEIS: Nicht alle Fingerabdruckscanner können für die Pre-Windows-Anmeldung verwendet werden. Wenn Sie versuchen, sich mit einem inkompatiblen Scanner vor dem Windows-Start anzumelden, wird eine Fehlermeldung angezeigt. Um herauszufinden, ob das Gerät kompatibel ist, wenden Sie sich an Ihren Systemadministrator, oder lesen Sie die Liste der unterstützten Fingerabdruckscanner auf support.dell.com.

Wenn Sie Fingerabdrücke registrieren, werden Sie aufgefordert, Ihr Windows-Kennwort einzugeben, damit Ihre Identität überprüft werden kann. Wenn Ihre Richtlinie dies verlangt, werden Sie zudem aufgefordert, auch Ihr Pre-Windows-Kennwort (Systemkennwort) einzugeben. Mit dem Pre-Windows-Kennwort können Sie auf das System zugreifen, wenn es ein Problem mit dem Fingerabdruckscanner gibt.

HINWEISE:

- Es empfiehlt sich, während des Registrierungsvorgangs mindestens zwei Fingerabdrücke zu registrieren.
- Sie müssen sicherstellen, dass die Fingerabdrücke ordnungsgemäß registriert sind, bevor Sie die Fingerabdruck-Authentifizierungsfunktion aktivieren.
- Wenn Sie den Fingerabdruckscanner in einem System auswechseln, müssen Sie die Fingerabdrücke mit dem neuen Scanner erneut registrieren. Die abwechselnde Verwendung zweier unterschiedlicher Fingerabdruckscanner wird nicht empfohlen.
- Falls beim Registrieren von Fingerabdrücken wiederholt Meldungen angezeigt werden, dass der Sensorfokus verloren ist, könnte dies bedeuten, dass der Computer den Fingerabdruckscanner nicht erkennt. Wenn es sich um einen externen Fingerabdruckscanner handelt, kann dieses Problem häufig gelöst werden, indem der Fingerabdruckscanner vom Computer getrennt und wieder angeschlossen wird.

Löschen von registrierten Fingerabdrücken
Sie können registrierte Fingerabdrücke entfernen, indem Sie auf die Verknüpfung **Einen Fingerabdruck entfernen** klicken oder im Fingerabdruck-Anmeldungsassistenten auf einen registrierten Finger klicken (um ihn zu deaktivieren).

Um einen spezifischen Benutzer zu entfernen, der Fingerabdrücke für die Pre-Windows-Authentifizierung registriert hat, kann der Administrator alle für diesen Benutzer registrierten Fingerabdrücke deaktivieren.

HINWEIS: Falls während des Fingerabdruck-Registrierungsvorgangs Fehler auftreten, schlagen Sie weitere Informationen auf wave.com/support/Dell nach.

Registrieren von Smartcards

Dell Data Protection | Access bietet Ihnen die Möglichkeit, eine herkömmliche (auch als "Contacted" bezeichnet) oder Contactless Smartcard für die Anmeldung bei Windows oder die Authentifizierung vor dem Start von Windows zu verwenden. Klicken Sie auf der Registerkarte "Smartcard" auf die Verknüpfung **Eine weitere Smartcard registrieren**, um den Assistenten zur Smartcard-Registrierung zu starten, der Sie durch den Registrierungsvorgang führt. Bei der Registrierung wird Ihre Smartcard für die Anmeldung eingerichtet.

Sie müssen über ein funktionierendes, ordnungsgemäß installiertes und konfiguriertes Smartcard-Authentifizierungsgerät verfügen, um die Registrierung auszuführen.

HINWEIS: Um herauszufinden, ob ein bestimmtes Gerät kompatibel ist, wenden Sie sich an Ihren Systemadministrator, oder lesen Sie die Liste der unterstützten Smartcards auf support.dell.com.

Registrierung
Wenn Sie eine Smartcard registrieren, werden Sie aufgefordert, Ihr Windows-Kennwort einzugeben, damit Ihre Identität überprüft werden kann. Wenn Ihre Richtlinie dies verlangt, werden Sie zudem aufgefordert, auch Ihr Pre-Windows-Kennwort (Systemkennwort) einzugeben. Mit dem Pre-Windows-Kennwort können Sie auf das System zugreifen, wenn es ein Problem mit dem Smartcard-Leser gibt.

Bei der Registrierung werden Sie nach der Smartcard-PIN gefragt, falls eine festgelegt wurde. Wenn Ihre Richtlinie eine PIN verlangt und keine festgelegt wurde, werden Sie aufgefordert, eine zu erstellen.

HINWEISE:

- Sobald ein Benutzer für die Verwendung einer Smartcard vor dem Start von Windows registriert wurde, kann dieser nicht mehr entfernt werden.
- Standardbenutzer können die Benutzer-PIN für eine Smartcard ändern, und der Administrator kann sowohl die Administrator-PIN als auch die Benutzer-PIN ändern.
- Der Administrator kann eine Smartcard auch zurücksetzen. Nach dem Zurücksetzen kann die Smartcard erst wieder für die Authentifizierung bei der Windows-Anmeldung oder vor dem Start von Windows verwendet werden, nachdem sie erneut registriert wurde.

HINWEIS: Für die Authentifizierung mit TPM-Zertifikaten können Administratoren TPM-Zertifikate im Rahmen des Smartcard-Registrierungsvorgangs von Microsoft Windows anmelden. Aus Gründen der Kompatibilität muss dabei anstelle eines Smartcard-CSP der Wave TCG-Enabled CSP als Cryptographic Service Provider ausgewählt werden. Außerdem muss die Dell Secure-Anmeldung mit dem entsprechenden Typ der Authentifizierungsrichtlinie für den Client aktiviert werden.

HINWEIS: Wenn Sie die Fehlermeldung erhalten, dass der Smartcard-Dienst nicht ausgeführt wird, können Sie diesen Dienst folgendermaßen starten bzw. neu starten:

- Navigieren Sie in der Systemsteuerung zum Fenster "Verwaltung", wählen Sie "Dienste", klicken Sie dann mit der rechten Maustaste auf "Smartcard", und wählen Sie "Starten" oder "Neu starten".
- Weitere Informationen zu spezifischen Fehlermeldungen finden Sie auf wave.com/support/Dell.

Self-Encrypting Drive – Übersicht

Dell Data Protection | Access verwaltet die hardwarebasierten Sicherheitsfunktionen von Self-Encrypting Drives, in deren Hardware Datenverschlüsselung integriert ist. Mithilfe dieser Funktion wird sichergestellt, dass nur berechtigte Benutzer auf verschlüsselte Daten zugreifen können (wenn die Laufwerkssperre aktiviert ist).

Das Fenster "Self-Encrypting Drive" wird durch Klicken auf die Registerkarte **Self-Encrypting Drive** unten geöffnet. Diese Registerkarte wird nur dann angezeigt, wenn auf Ihrem System ein oder mehrere Self-Encrypting Drives (SED) vorhanden sind.

Klicken Sie auf die Verknüpfung **Einrichten**, um den Einrichtungsassistenten für das Self-Encrypting Drive zu starten. In diesem Assistenten erstellen Sie ein Kennwort für den Laufwerksadministrator, sichern dieses Kennwort und übernehmen Ihre Verschlüsselungseinstellungen für das Laufwerk. Ausschließlich Systemadministratoren können den Einrichtungsassistenten für das Self-Encrypting Drive aufrufen.

Wichtig! Sobald das Laufwerk eingerichtet wurde, sind der Datenschutz und die Laufwerkssperre "aktiviert". Wenn ein Laufwerk gesperrt ist, verhält es sich folgendermaßen:

- Das Laufwerk wechselt in den *Sperrmodus*, sobald das Laufwerk ausgeschaltet wird.
- Das Laufwerk startet erst, nachdem der Benutzer den korrekten Benutzernamen und das korrekte Kennwort (oder Fingerabdruck) auf dem Pre-Windows-Authentifizierungsbildschirm eingegeben hat. Bevor die Laufwerkssperre aktiviert ist, können die Daten auf dem Laufwerk von jedem Benutzer am Computer abgerufen werden.
- Das Laufwerk ist auch dann gesichert, wenn es als sekundäres Laufwerk an einen anderen Computer angeschlossen wird. Um auf die Daten auf dem Laufwerk zuzugreifen ist eine Authentifizierung erforderlich.

Sobald das Laufwerk eingerichtet wurde, werden im Fenster Self-Encrypting Drive das Laufwerk (oder die Laufwerke) angezeigt sowie eine Verknüpfung, mit der die Benutzer ihr Kennwort für das Laufwerk ändern können. Wenn Sie Laufwerksadministrator sind, können Sie in diesem Fenster zudem Laufwerksbenutzer hinzufügen oder entfernen. Wenn ein externes Laufwerk eingerichtet wurde, wird es in diesem Fenster angezeigt und kann entsperrt werden.

HINWEIS: Zum Sperren eines sekundären, externen Laufwerks muss das Laufwerk unabhängig vom Computer abgeschaltet werden.

Der Laufwerksadministrator kann die Einstellungen für das Laufwerk in **Erweitert>Geräte** verwalten. Weitere Informationen finden Sie unter Geräteverwaltung – Self-Encrypting Drives.

Laufwerkseinrichtung

Der Einrichtungsassistent für das Self-Encrypting Drive führt Sie durch die Einrichtung Ihres Laufwerks. Die folgenden Begriffe sind während der Ausführung dieses Vorgangs wichtig:

Laufwerksadministrator
Der erste Benutzer mit Administratorrechten für das System, der den Zugriff auf das Laufwerk einrichtet (und das Kennwort für den Laufwerksadministrator festlegt), wird zum Laufwerksadministrator. Nur dieser Benutzer hat die Berechtigung, Änderungen am Laufwerkszugriff vorzunehmen. Damit sichergestellt ist, dass der erste Benutzer absichtlich als Laufwerksadministrator eingerichtet wird, müssen Sie das Kontrollkästchen "Ich habe dies verstanden" aktivieren, um mit diesem Schritt fortzufahren.

Kennwort für den Laufwerksadministrator
Der Assistent fordert Sie auf, ein Kennwort für den Laufwerksadministrator zu erstellen und das Kennwort zur Bestätigung erneut einzugeben. Sie müssen Ihr Windows-Kennwort eingeben, um Ihre Identität zu bestätigen, bevor Sie das Kennwort für den Laufwerksadministrator erstellen können. Der aktuelle Windows-Benutzer muss über Administratorrechte verfügen, um dieses Kennwort zu erstellen.

Sicherung der Anmeldedaten des Laufwerksadministrators
Geben Sie einen Speicherort ein, oder klicken Sie auf die Schaltfläche **Durchsuchen**, um einen Speicherort auszuwählen, an dem Sie eine Sicherungskopie Ihrer Anmeldedaten als Laufwerksadministrator speichern.

WICHTIG**!**

- Es wird dringend empfohlen, dass Sie eine Sicherung dieser Anmeldedaten durchführen, und zwar auf einem anderen Laufwerk als Ihrer primären Festplatte (z. B. auf einem Wechseldatenträger). Andernfalls können Sie nicht auf die Sicherung zugreifen, falls Sie keinen Zugriff zu Ihrem Laufwerk haben.
- Sobald Sie die Einrichtung des Laufwerks abgeschlossen haben, müssen alleBenutzer vor dem Windows-Start den korrekten Benutzernamen und das korrekte Kennwort (oder Fingerabdruck) eingeben, um sich beim nächsten Systemstart am System anmelden zu können.

Laufwerksbenutzer hinzufügen
Der Laufwerksadministrator kann aktuelle Windows-Benutzer als weitere Benutzer für das Laufwerk hinzufügen. Beim Hinzufügen von Benutzern für das Laufwerk kann der Administrator verlangen, dass die Benutzer ihr Kennwort bei der ersten Anmeldung zurücksetzen. Die Benutzer müssen ihr Kennwort auf dem Pre-Windows-Authentifizierungsbildschirm zurücksetzen, bevor das Laufwerk entsperrt wird.

Erweiterte Einstellungen

- *Single Sign-On*: Standardmäßig wird Ihr Kennwort für das Self-Encrypting Drive, das Sie vor dem Windows-Start zur Authentifizierung für das Laufwerk eingeben, automatisch auch für die Windows-Anmeldung verwendet (diese Einmalanmeldung wird als "Single Sign-On" bezeichnet). Wenn Sie diese Funktion deaktivieren möchten, aktivieren Sie beim Konfigurieren Ihrer Laufwerkseinstellungen das Kontrollkästchen "Ich möchte mich beim Windows-Start erneut anmelden".
- *Fingerabdruck-Anmeldung*: Auf unterstützten Plattformen können Sie angeben, dass Sie sich beim Self-Encrypting Drive anhand eines Fingerabdrucks anstelle eines Kennworts authentifizieren möchten.
- *Unterstützung für Energiesparmodus/Standbymodus (S3)* (falls auf der Plattform unterstützt): Wenn dies aktiviert ist, kann Ihr Self-Encrypting Drive sicher in den Energiesparmodus/Standbymodus (auch S3-Modus genannt) versetzt werden. Beim Hochfahren aus dem Energiesparmodus/Standbymodus ist die Pre-Windows-Authentifizierung erforderlich.

HINWEISE:

- Wenn die S3-Unterstützung aktiviert ist, unterliegen auch Verschlüsselungskennwörter für das Laufwerk den vorhandenen BIOS-Kennwortbeschränkungen. Wenden Sie sich an den Hardware-Hersteller, um weitere Informationen über mögliche BIOS-spezifische Kennwortbeschränkungen für den Computer zu erhalten.
- Nicht alle Self-Encrypting Drives unterstützen den S3-Modus. Während der Einrichtung des Laufwerks werden Sie darüber benachrichtigt, ob das Laufwerk den Energiesparmodus/Standbymodus unterstützt. Bei Laufwerken, die diesen Modus nicht unterstützen, werden Anforderungen, in den Windows-S3-Modus zu wechseln, automatisch in Anforderungen umgewandelt, in den Windows-Ruhezustand zu wechseln,

sofern dieser aktiviert ist. (Es wird dringend empfohlen, den auf dem Computer zu aktivieren.)

- Bei der ersten Anmeldung, nachdem die Option "Single Sign-On (SSO)" aktiviert wurde, wird der Vorgang bei der Windows-Anmeldung unterbrochen. Sie müssen Ihre Windows-Authentifizierung eingeben, die für zukünftige Windows-Anmeldevorgänge sicher gespeichert wird. Beim nächsten Systemstart meldet SSO Sie automatisch bei Windows an. Derselbe Vorgang ist auch erforderlich, wenn sich die Windows-Authentifizierung eines Benutzers (Kennwort, Fingerabdruck, Smartcard-PIN) ändert. Wenn sich der Computer in einer Domäne befindet und die Domänenrichtlinie fordert, dass Ctrl-Alt-Delete für die Windows-Anmeldung gedrückt werden müssen, wird diese Richtlinie eingehalten.

ACHTUNG! Wenn Sie die Anwendung **Dell Data Protection | Access** deinstallieren, müssen Sie zuerst den Datenschutz des Self-Encrypting Drive deaktivieren und das Laufwerk entsperren.

Self-Encrypting Drive – Benutzerfunktionen

Administratoren für Self-Encrypting Drives führen sämtliche Verwaltungsvorgänge für die Sicherheit und Benutzer des Laufwerks durch. Benutzer des Laufwerks, die nicht Administrator des Laufwerks sind, können lediglich die folgenden Aufgaben ausführen:

- Ihre eigenen Kennwörter für das Laufwerk ändern
- Ein Laufwerk entsperren

Diese Aufgaben können in **Dell Data Protection | Access** auf der Registerkarte **Self-Encrypting Drive** ausgeführt werden.

Kennwort ändern
Ermöglicht es registrierten Benutzern, ein neues Authentifizierungskennwort für das Laufwerk zu erstellen. Sie müssen Ihr aktuelles Kennwort für das Self-Encrypting Drive angeben, bevor das Laufwerkkennwort geändert wird.

HINWEISE:

- Die Anwendung wendet die Windows-Richtlinien zu Länge und Komplexität von Kennwörtern an, sofern diese aktiviert wurden. Falls jedoch keine Windows-Kennwortrichtlinien aktiviert sind, beträgt die Höchstlänge für ein Self-Encrypting Drive-Kennwort 32 Zeichen. Beachten Sie, dass die Höchstlänge 127 Zeichen beträgt, wenn S3 (Energiesparmodus/Standbymodus) nicht aktiviert ist.
- Das Kennwort eines Benutzers für das Self-Encrypting Drive ist ein anderes als sein Windows-Kennwort. Wenn das Windows-Kennwort eines Benutzers geändert oder zurückgesetzt wird, hat dies keine Auswirkungen auf das Laufwerkkennwort des Benutzers, es sei denn, die Windows-Kennwortsynchronisierung ist aktiviert. Weitere Informationen finden Sie unter Geräte: Self-Encrypting Drives.
- Bei einigen nicht-englischen Tastaturen gibt es unzulässige Zeichen, die nicht im Kennwort für das Self-Encrypting Drive verwendet werden dürfen. Wenn das Windows-Kennwort eines der unzulässigen Zeichen enthält und die Windows-Kennwortsynchronisierung aktiviert ist, schlägt die Synchronisierung fehl, und eine Fehlermeldung wird ausgegeben.

Laufwerk entsperren
Mit der Funktion "Laufwerk entsperren" kann ein angemeldeter Laufwerkbenutzer ein gesperrtes Laufwerk entsperren. Wenn die Laufwerksperre aktiviert ist, wechselt das Laufwerk in einen gesperrten Zustand, sobald der Computer abgeschaltet wird. Wenn das System wieder gestartet wird, müssen Sie sich für das Laufwerk authentifizieren, indem Sie Ihr Kennwort auf dem Pre-Windows-Authentifizierungsbildschirm eingeben.

HINWEISE:

- Wenn auf dem Computer mehrere Benutzerkonten für das Self-Encrypting Drive gleichzeitig aktiv sind, kann dies dazu führen, dass der Computer nicht in den Energiesparmodus (Standbymodus oder Ruhezustand) wechseln kann.
- In den folgenden Sprachversionen der Anwendung werden statt der Namen der Laufwerkbenutzer auf dem Pre-Windows-Authentifizierungsbildschirm die Einträge "User 1", "User 2", "User 3" und "User 4" aufgeführt: Chinesisch, Japanisch, Koreanisch und Russisch.

Erweiterte Optionen

Mit den erweiterten Optionen in **Dell Data Protection | Access** können Benutzer mit Administratorrechten die folgenden Aspekte der Anwendung verwalten:

Wartung
Kennwörter
Geräte

HINWEIS: Ausschließlich Benutzer mit Administratorrechten können Änderungen in den erweiterten Optionen vornehmen; Standardbenutzer können diese Einstellungen anzeigen, aber nicht ändern.

Wartung – Übersicht

Im Fenster "Wartung" können Administratoren Einstellungen für die Windows-Anmeldung festlegen, ein System zurücksetzen, um es für einen neuen Zweck zu verwenden, oder die Anmeldedaten von Benutzern, die auf der Sicherheitshardware des Systems gespeichert sind, archivieren oder wiederherstellen. Einzelheiten finden Sie in den folgenden Themen:

Zugriffseinstellungen
System zurücksetzen
Anmeldedaten archivieren und wiederherstellen

Zugriffseinstellungen

Im Fenster "Zugriffseinstellungen" können Administratoren Einstellungen für die Windows-Anmeldung für alle Benutzer des Systems festlegen.

Aktivieren der Dell Secure-Anmeldung
Mit der Option, das Windows-Standardfenster (Ctrl-Alt-Delete) zu ersetzen, können Sie anstatt des Windows-Kennworts (oder zusätzlich dazu) verschiedene Authentifizierungsfaktoren für den Zugriff auf Windows verwenden. Sie können einen Fingerabdruck als zweiten Authentifizierungsfaktor hinzufügen, um die Sicherheit des Windows-Anmeldevorgangs zu erhöhen. Zudem können weitere Authentifizierungsfaktoren für die Windows-Anmeldung hinzugefügt werden, beispielsweise eine Smartcard oder ein TPM-Zertifikat.

HINWEISE:

- Von der Aktivierung der Dell Secure-Anmeldung sind alle Benutzer im System betroffen.
- Es empfiehlt sich, diese Option zu aktivieren, NACHDEM die Benutzer ihre Fingerabdrücke oder Smartcard registriert haben.
- Bei der ersten Anmeldung nach dem Einrichten dieser Option werden Sie aufgefordert, sich gemäß Ihrer Standardrichtlinie bei Windows zu authentifizieren. Beim nächsten Start müssen Sie dann die neuen Authentifizierungsfaktoren verwenden.

Dell Secure-Anmeldung deaktivieren
Mit dieser Option werden alle Funktionen von **Dell Data Protection | Access** für die Windows-Anmeldung deaktiviert. Durch Auswählen dieser Option kehren Sie zur Standard-Anmelderichtlinie von Windows zurück.

HINWEISE:

- Wenn Sie bei der Anmeldung eine Fehlermeldung zur sicheren Windows-Anmeldung bekommen, deaktivieren Sie die Option für die Dell Secure-Anmeldung, und aktivieren Sie sie anschließend wieder.
- Weitere Informationen zu spezifischen Fehlermeldungen finden Sie auf wave.com/support/Dell.

System zurücksetzen

Mit der Funktion "System zurücksetzen" können alle Benutzerdaten von der Sicherheitshardware auf der Plattform gelöscht werden. Diese Funktion wird beispielsweise verwendet, wenn ein Computer für einen neuen Zweck eingesetzt werden soll. Mit dieser Option werden außer den Windows-Benutzerkennwörtern alle Kennwörter auf dem System sowie alle Daten in den Hardwaregeräten (ControlVault, TPM und Fingerabdruckscanner) gelöscht. Bei Self-Encrypting Drives deaktiviert diese Funktion außerdem den Schutz der Daten, sodass auf die Daten auf dem Laufwerk zugegriffen werden kann.

Sie müssen bestätigen, dass Ihnen bewusst ist, dass Sie das System zurücksetzen. Klicken Sie dann auf **Weiter**. Um das System zurückzusetzen, müssen Sie die Kennwörter für alle Sicherheitsgeräte eingeben, falls welche festgelegt wurden:

- TPM-Besitzer
- ControlVault-Administrator
- BIOS-Administrator
- BIOS-System (Pre-Windows)
- Festplatte (BIOS)
- Administrator für Self-Encrypting Drive

HINWEIS: Bei Self-Encrypting Drives ist lediglich das Kennwort des Laufwerksadministrators erforderlich, nicht alle Kennwörter der Laufwerksbenutzer.

Wichtig! Die einzige Möglichkeit, die beim Zurücksetzen des Systems gelöschten Daten wiederherzustellen, besteht darin, sie wieder aus einem zuvor gespeicherten Archiv zu laden. Wenn Sie über kein Archiv verfügen, können diese Daten nicht wiederhergestellt werden. Bei einem Self-Encrypting Drive werden nur die Einrichtungsdaten gelöscht; es werden keine persönlichen Daten auf dem Laufwerk gelöscht.

Anmeldedaten archivieren und wiederherstellen

Mit der Funktion "Anmeldedaten archivieren und wiederherstellen" werden alle Benutzeranmeldedaten (Anmelde- und Verschlüsselungsinformationen), die im ControlVault und Trusted Platform Module (TPM) gespeichert sind, gesichert und wiederhergestellt. Eine Sicherung dieser Daten ist wichtig, wenn ein Computer umgenutzt wird oder um Daten im Fall eines Hardwarefehlers wiederherzustellen. In diesem Fall können Sie Ihre gesamten Anmeldedaten einfach aus einer gespeicherten Archivdatei auf Ihrem neuen Computer wiederherstellen.

Sie können die Anmeldedaten für einen einzelnen Benutzer oder für alle Benutzer im System archivieren oder wiederherstellen.

Die Anmeldedaten der Benutzer bestehen aus Daten, die vor dem Windows-Start verwendet werden, z. B. registrierten Fingerabdrücken und Smartcard-Daten, sowie aus Schlüsseln, die im TPM gespeichert sind. Das TPM erstellt Schlüssel auf Anforderung von sicheren Anwendungen; so werden beim Generieren eines digitalen Zertifikats beispielsweise Schlüssel im TPM erstellt.

HINWEIS: Informationen darüber, ob die TPM-Schlüssel von **Dell Data Protection | Access** archiviert werden können, finden Sie in der Dokumentation zur sicheren Anwendung. Im Allgemeinen werden Anwendungen unterstützt, die zur Erstellung von Schlüsseln den Wave TCG-Enabled CSP verwenden.

Archivieren von Anmeldedaten
Gehen Sie zum Archivieren von Anmeldedaten folgendermaßen vor:

- Geben Sie an, ob Sie Anmeldedaten für sich selbst oder für alle Benutzer im System archivieren.
- Authentifizieren Sie sich bei der Sicherheitshardware, indem Sie das Systemkennwort (Pre-Windows-Kennwort), das ControlVault-Administratorkennwort und das TPM-Besitzerkennwort eingeben.
- Erstellen Sie ein Kennwort für die Sicherung der Anmeldedaten.
- Geben Sie mithilfe der Schaltfläche **Durchsuchen** einen Archivspeicherort an. Das Archiv sollte auf einem Wechseldatenträger gespeichert werden, z. B. auf einem USB-Flash-Laufwerk oder einem Netzlaufwerk, damit die Daten im Fall eines Festplattenfehlers geschützt sind.

Wichtige Hinweise:

- Notieren Sie sich den Archivspeicherort, da der Benutzer diese Informationen zum Wiederherstellen der Anmeldedaten benötigt.
- Notieren Sie sich das Kennwort für die Sicherung der Anmeldedaten, um sicherzustellen, dass die Daten wiederhergestellt werden können. Dies ist wichtig, da das Kennwort nicht wiederhergestellt werden kann.
- Wenn Sie das TPM-Besitzerkennwort nicht kennen, wenden Sie sich an den Systemadministrator oder schlagen in der Anleitung zur Einrichtung des TPM nach.

Wiederherstellen von Anmeldedaten
Gehen Sie zum Wiederherstellen von Anmeldedaten folgendermaßen vor:

- Geben Sie an, ob Sie Anmeldedaten für sich selbst oder für alle Benutzer im System wiederherstellen.
- Navigieren Sie zum Archivspeicherort, und wählen Sie die Archivdatei aus.
- Geben Sie das Kennwort für die Sicherung der Anmeldedaten ein, das erstellt wurde, als Sie das Archiv eingerichtet haben.

- Authentifizieren Sie sich für die Sicherheitshardware, indem Sie das Systemkennwort (Pre-Windows-Kennwort), das ControlVault-Administratorkennwort und das TPM-Besitzerkennwort eingeben.

HINWEISE:

- Wenn Sie nach mehreren Versuchen immer wieder die Fehlermeldung erhalten, dass die Wiederherstellung der Anmeldedaten fehlgeschlagen ist, versuchen Sie, eine andere Archivdatei wiederherzustellen. Wenn dies nicht funktioniert, erstellen Sie ein weiteres Archiv mit den Anmeldedaten, und versuchen Sie, die Daten aus dem neuen Archiv wiederherzustellen.
- Wenn Sie die Fehlermeldung erhalten, dass die TPM-Schlüssel nicht wiederhergestellt werden konnten, erstellen Sie ein Archiv mit den Anmeldedaten, und löschen Sie das TPM im BIOS. Zum Löschen des TPM starten Sie den Computer neu, drücken Sie beim Start die **F2**-Taste, um auf die BIOS-Einstellungen zuzugreifen, und navigieren Sie dann zu "Security>TPM Security". Legen Sie anschließend den Besitzer des TPM erneut fest, und versuchen Sie noch einmal, die Anmeldedaten wiederherzustellen.
- Weitere Informationen zu spezifischen Fehlermeldungen finden Sie auf wave.com/support/Dell.

Kennwortverwaltung

Im Fenster "Kennwortverwaltung" kann ein Administrator alle Sicherheitskennwörter auf Ihrem System erstellen oder ändern:

- System (auch Pre-Windows genannt)*
- Administrator*
- Festplatte*
- ControlVault
- TPM-Besitzer
- TPM-Master
- TPM-Kennworttresor
- Self-Encrypting Drive

HINWEISE:

- Es werden nur die Kennwörter angezeigt, die für die aktuelle Plattformkonfiguration relevant sind; daher ändert sich dieses Fenster je nach Systemkonfiguration und -status.
- Bei den oben aufgeführten Kennwörtern mit einem Sternchen (*) handelt es sich um BIOS-Kennwörter, die auch über das System-BIOS geändert werden können.
- Die Kennwörter auf BIOS-Ebene können nicht erstellt oder geändert werden, wenn der BIOS-Administrator keine Kennwortänderungen gestattet hat.
- Durch Klicken auf die Verknüpfung **Einrichten** für ein Self-Encrypting Drive wird der Einrichtungsassistent für das Self-Encrypting Drive gestartet. Durch Klicken auf **Verwalten** können die Benutzer ein oder mehrere Self-Encrypting Drive-Kennwörter ändern.
- Durch Klicken auf die Verknüpfung **Verwalten** für den TPM-Kennworttresor wird ein Fenster angezeigt, in dem Sie die Kennwörter anzeigen oder ändern können, die Ihre TPM-Schlüssel schützen. Wenn ein TPM-Schlüssel erstellt wird, der ein Kennwort erfordert, wird das Kennwort zufällig generiert und im Tresor abgelegt. Sie können den TPM-Kennworttresor erst verwalten, nachdem Sie ein TPM-Master-Kennwort erstellt haben.

Komplexitätsregeln für Windows-Kennwörter

Mit **Dell Data Protection | Access** wird sichergestellt, dass das folgende Kennwort mit den Komplexitätsregeln für Windows-Kennwörter des Computers kompatibel ist:

- TPM-Besitzerkennwort

Zum Bestimmen der Richtlinie für die Komplexität von Windows-Kennwörtern auf einem Computer führen Sie die folgenden Schritte aus:

1. Rufen Sie die Systemsteuerung auf.
2. Doppelklicken Sie auf "Verwaltung".
3. Doppelklicken Sie auf "Lokale Sicherheitsrichtlinie".
4. Erweitern Sie "Kontorichtlinien", und wählen Sie "Kennwortrichtlinien" aus.

Geräte – Übersicht

Im Fenster "Geräte" können Administratoren alle Sicherheitsgeräte verwalten, die auf ihrem System installiert sind. Für jedes Gerät können Sie den Status und weitere detaillierte Informationen anzeigen, z. B. die Firmware-Version. Klicken Sie auf **Einblenden**, um die Informationen für die jeweiligen Geräte anzuzeigen, oder auf **Ausblenden**, um diesen Abschnitt zu verbergen. Die folgenden Geräte können verwaltet werden, sofern sie auf Ihrer Plattform installiert sind:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Informationen zum Authentifizierungsgerät

Trusted Platform Module (TPM)

Der TPM-Sicherheitschip muss aktiviert sein, und der Besitzer des TPM muss festgelegt sein, um die erweiterten Sicherheitsfunktionen zu verwenden, die **Dell Data Protection | Access** und das TPM bereitstellen.

Das Fenster "Trusted Platform Module" in der **Geräteverwaltung** wird nur dann angezeigt, wenn ein TPM auf Ihrem System erkannt wurde.

TPM-Verwaltung
Diese Funktionen ermöglichen dem Systemadministrator die Verwaltung des TPM.

Status
Zeigt den Status *Aktiv* oder *Inaktiv* für das TPM an. Der Status "Aktiv" bedeutet, dass das TPM im BIOS aktiviert wurde und zum Einrichten bereit ist (d. h., der Besitzer kann festgelegt werden). Das TPM kann nicht verwaltet werden, und auf seine Sicherheitsfunktionen kann nicht zugegriffen werden, wenn das TPM nicht aktiviert wurde.

Wenn das TPM auf dem System erkannt wird, dieses aber nicht aktiviert wurde, können Sie es aktivieren, indem Sie in diesem Fenster auf die Verknüpfung **Aktivieren** klicken, ohne das System-BIOS aufzurufen. Nach der Aktivierung des TPM mit dieser Funktion muss der Computer neu gestartet werden. Während des Neustarts wird in einigen Fällen ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob die Änderungen übernommen werden sollen.

HINWEIS: Die Möglichkeit, das TPM über diese Anwendung zu aktivieren, wird u. U. nicht auf allen Plattformen unterstützt. Falls dies nicht unterstützt wird, müssen Sie das TPM im System-BIOS aktivieren. Starten Sie dazu das System neu, drücken Sie vor dem Windows-Start die **F2**-Taste, um auf das BIOS zuzugreifen, navigieren Sie dann zu Security>TPM Security, und aktivieren Sie das TPM.

Sie können das TPM an dieser Stelle auch *deaktivieren*, indem Sie auf die Verknüpfung **Deaktivieren** klicken. Nachdem das TPM deaktiviert wurde, ist es für die erweiterten Sicherheitsfunktionen nicht mehr verfügbar. Durch die Deaktivierung werden jedoch weder TPM-Einstellungen geändert noch werden im TPM gespeicherte Informationen oder Schlüssel gelöscht oder geändert.

Besitzer liegt vor
Zeigt den Besitzerstatus an und gibt Ihnen die Möglichkeit, den TPM-Besitzer festzulegen oder zu ändern. Der TPM-Besitzer muss festgelegt werden, damit die Sicherheitsfunktionen des TPM zur Verfügung stehen. Bevor der Besitzer festgelegt werden kann, muss das TPM aktiviert werden.

Der Prozess zur Festlegung des Besitzers besteht darin, dass der Benutzer (mit Administratorrechten) ein TPM-Besitzerkennwort erstellt. Nach dem Festlegen dieses Kennworts ist das TPM in Besitz genommen und einsatzbereit.

HINWEIS: Das TPM-Besitzerkennwort muss den Komplexitätsregeln für Windows-Kennwörter in Ihrem System entsprechen.

Wichtig! Sie dürfen das TPM-Besitzerkennwort auf keinen Fall verlieren oder vergessen, da es für den Zugriff auf die erweiterten Sicherheitsfunktionen für das TPM in **Dell Data Protection | Access** erforderlich ist.

Gesperrt
Zeigt den Status *Gesperrt* oder *Entsperrt* für das TPM an. Die "Sperre" ist eine Sicherheitsfunktion des TPM. Das TPM wechselt in den gesperrten Status, nachdem das TPM-

Besitzerkennwort eine festgelegte Anzahl von Malen falsch eingegeben wurde. Der TPM-Besitzer kann das TPM hier entsperren; dazu ist die Eingabe des TPM-Besitzerkennworts erforderlich.

HINWEISE:

- Wenn Sie die Fehlermeldung erhalten, dass der Besitzer für das TPM nicht festgelegt werden konnte, löschen Sie im System-BIOS die Daten aus dem TPM, und versuchen Sie erneut, den Besitzer festzulegen. Zum Löschen des TPM starten Sie den Computer neu, drücken Sie beim Start die **F2**-Taste, um auf die BIOS-Einstellungen zuzugreifen, und navigieren Sie dann zu "Security>TPM Security".
- Wenn Sie die Fehlermeldung erhalten, dass das TPM-Besitzerkennwort nicht geändert werden konnte, archivieren Sie die TPM-Daten (Anmeldedaten archivieren), löschen Sie das TPM im BIOS, legen Sie den Besitzer des TPM erneut fest, und stellen Sie die TPM-Daten wieder her (Anmeldedaten wiederherstellen).
- Weitere Informationen zu spezifischen Fehlermeldungen finden Sie auf wave.com/support/Dell.

Dell ControlVault®

Bei Dell ControlVault® (CV) handelt es sich um einen sicheren Hardwarespeicher für die Benutzeranmeldedaten, die bei der Pre-Windows-Anmeldung verwendet werden (z. B. Benutzerkennwörter oder Daten zu registrierten Fingerabdrücken). Das Fenster "ControlVault" in der **Geräteverwaltung** wird nur dann angezeigt, wenn ein ControlVault auf Ihrem System erkannt wurde.

ControlVault-Verwaltung

Diese Funktionen ermöglichen dem Systemadministrator die Verwaltung des ControlVault auf dem System.

Status
Zeigt den Status *Aktiv* oder *Inaktiv* für den ControlVault an. Der Status "Inaktiv" bedeutet, dass der ControlVault auf Ihrem System nicht zum Speichern verfügbar ist. Lesen Sie in der Dell-Systemdokumentation nach, ob das System einen ControlVault enthält.

Kennwort
Gibt an, ob das ControlVault-Administratorkennwort festgelegt wurde, und lässt Sie ein Kennwort festlegen oder dieses ändern (wenn bereits ein Kennwort festgelegt wurde). Ausschließlich Systemadministratoren können dieses Kennwort festlegen oder ändern. Für folgende Aufgaben muss ein ControlVault-Administratorkennwort festgelegt werden:

- Anmeldedaten archivieren und wiederherstellen.
- Benutzerdaten löschen (für alle Benutzer).

HINWEIS: Wenn versucht wird, Daten zu archivieren oder wiederherzustellen, ohne dass ein ControlVault-Administratorkennwort festgelegt wurde, wird der Benutzer aufgefordert, eines zu erstellen (wenn es sich um einen Administrator handelt).

Registrierte Benutzer
Gibt an, ob Benutzer Anmeldedaten (z. B. Kennwörter, Daten zu Fingerabdrücken oder Smartcards) registriert haben, die derzeit im ControlVault gespeichert werden.

Benutzerdaten löschen
Die Daten im ControlVault müssen u. U. zu einem bestimmten Zeitpunkt gelöscht werden, z. B. wenn die Benutzer Probleme beim Verwenden oder Registrieren der Pre-Windows-Anmeldedaten für die Authentifizierung haben. Alle im ControlVault gespeicherten Daten können in diesem Fenster gelöscht werden, sowohl für einzelne als auch für alle Benutzer.

Das ControlVault-Administratorkennwort muss eingegeben werden, um alle Benutzerdaten von der Plattform zu löschen. Sie werden auch aufgefordert, dass System-Kennwort (Pre-Windows-Kennwort) einzugeben, wenn Pre-Windows-Anmeldedaten registriert sind. Wenn Sie alle Benutzerdaten löschen, werden das ControlVault-Administratorkennwort und das Systemkennwort zurückgesetzt. Beachten Sie, dass dies die einzige Möglichkeit ist, das ControlVault-Administratorkennwort zu löschen.

HINWEIS: Sobald Sie alle Benutzerdaten gelöscht haben, werden Sie aufgefordert, den Computer neu zu starten. Für das ordnungsgemäße Funktionieren des Systems ist es wichtig, dass Sie einen Neustart durchführen.

Das ControlVault-Administratorkennwort muss nicht festgelegt werden, um die Anmeldedaten eines einzelnen Benutzers zu löschen. Wenn Sie auf **Benutzerdaten löschen** klicken, werden Sie aufgefordert, den Benutzer auszuwählen, dessen ControlVault-Anmeldedaten Sie löschen

möchten. Sobald Sie einen Benutzer ausgewählt haben, werden Sie zur Eingabe des Systemkennworts aufgefordert (nur wenn Pre-Windows-Anmeldedaten registriert sind).

HINWEISE:

- Wenn Sie die Fehlermeldung erhalten, dass das ControlVault-Administratorkennwort nicht erstellt werden kann, sollten Sie Ihre Anmeldedaten archivieren, sämtliche Daten aus dem ControlVault löschen, den Computer neu starten und erneut versuchen, das Kennwort zu erstellen.
- Wenn Sie die Fehlermeldung erhalten, dass Anmeldedaten für einen einzelnen Benutzer nicht aus dem ControlVault gelöscht werden konnten, sollten Sie Ihre Anmeldedaten archivieren und versuchen, alle Benutzerdaten zu löschen. Versuchen Sie anschließend erneut, die Daten für den einzelnen Benutzer zu löschen.
- Wenn Sie die Fehlermeldung erhalten, dass die Anmeldedaten für alle Benutzer nicht aus dem ControlVault gelöscht werden konnten, sollten Sie in Erwägung ziehen, das System zurückzusetzen. **Wichtig!** Lesen Sie das Hilfethema "System zurücksetzen", bevor Sie diesen Schritt ausführen, da dabei ALLE Sicherungsdaten für Benutzer gelöscht werden.
- Wenn Sie die Fehlermeldung erhalten, dass die ControlVault- und TPM-Daten nicht gesichert werden konnten, deaktivieren Sie das TPM im System-BIOS. Starten Sie dazu den Computer neu, drücken Sie beim Start die **F2**-Taste, um auf die BIOS-Einstellungen zuzugreifen, und navigieren Sie dann zu "Security>TPM Security". Aktivieren Sie anschließend das TPM wieder, und versuchen Sie erneut, Ihre ControlVault-Daten zu archivieren.
- Weitere Informationen zu spezifischen Fehlermeldungen finden Sie auf wave.com/support/Dell.

Self-Encrypting Drives: Erweitert

Dell Data Protection | Accessverwaltet die hardwarebasierten Sicherheitsfunktionen von Self-Encrypting Drives, in deren Hardware Datenverschlüsselung integriert ist. Dadurch wird sichergestellt, dass nur berechtigte Benutzer auf verschlüsselte Daten zugreifen können, wenn die Laufwerkssperre aktiviert ist.

In der **Geräteverwaltung** wird das Fenster "Self-Encrypting Drive" nur dann angezeigt, wenn auf Ihrem System ein oder mehrere Self-Encrypting Drives (SED) vorhanden sind.

Wichtig! Sobald das Laufwerk eingerichtet wurde, sind der Datenschutz des Self-Encrypting Drive und die Laufwerkssperre "aktiviert".

Laufwerksverwaltung
Diese Funktionen ermöglichen dem Laufwerksadministrator die Verwaltung von Sicherheitseinstellungen für das Laufwerk. Änderungen an den Sicherheitseinstellungen für das Laufwerk werden wirksam, nachdem das Laufwerk ausgeschaltet wurde.

Datenschutz
Zeigt den Status *Aktiviert* oder *Deaktiviert* für den Datenschutz des Self-Encrypting Drive an. Der Status "Aktiviert" bedeutet, dass die Laufwerkssicherheit eingerichtet wurde. Die Benutzer müssen sich jedoch erst dann bei der Pre-Windows-Anmeldung authentifizieren, wenn die *Sperre* des Laufwerks aktiviert wurde.

Hier können Sie den Datenschutz für das Self-Encrypting Drive deaktivieren. Wenn er deaktiviert ist, werden alle erweiterten Sicherheitsfunktionen des Self-Encrypting Drive ausgeschaltet, und das Laufwerk verhält sich wie ein Standardlaufwerk. Beim Deaktivieren des Datenschutzes werden auch alle Sicherheitseinstellungen gelöscht, darunter die Anmeldedaten des Laufwerksadministrators und der Laufwerkbenutzer. Diese Funktion ändert oder entfernt jedoch keine Benutzerdaten auf dem Laufwerk.

Sperren
Zeigt den Status *Aktiviert* oder *Deaktiviert* für die Self-Encrypting Drives an. Weitere Informationen zum Verhalten von gesperrten Laufwerken finden Sie in Self-Encrypting Drive.

Gegebenenfalls ist es erforderlich, die Laufwerkssperre vorübergehend zu deaktivieren. Diese Einstellung können Sie hier vornehmen. Die Deaktivierung der Laufwerkssperre wird nicht empfohlen, da dann keine Anmeldedaten mehr erforderlich sind, um auf das Laufwerk zuzugreifen, sodass ein beliebiger Plattformbenutzer die Daten auf dem Laufwerk abrufen kann. Beim Deaktivieren der Laufwerkssperre werden keine Sicherheitseinstellungen gelöscht, weder die Anmeldedaten des Laufwerksadministrators und der Laufwerksbenutzer noch irgendwelche anderen Benutzerdaten auf dem Laufwerk.

ACHTUNG! Wenn Sie die Anwendung **Dell Data Protection | Access** deinstallieren, müssen Sie zuerst den Datenschutz des Self-Encrypting Drive deaktivieren und das Laufwerk entsperren.

Laufwerksadministrator

Zeigt den aktuellen Laufwerksadministrator an. Der Laufwerksadministrator kann hier ändern, welcher Benutzer Laufwerksadministrator ist. Bei dem neuen Administrator muss es sich um einen gültigen Windows-Benutzer auf dem System mit Administratorrechten handeln. Es kann nur einen Laufwerksadministrator im System geben.

Laufwerksbenutzer

Zeigt die registrierten Laufwerksbenutzer und die Anzahl der gegenwärtig registrierten Benutzer an. Die maximal unterstützte Benutzeranzahl hängt vom Self-Encrypting Drive ab (zurzeit 4 Benutzer für Laufwerke von Seagate und 24 für Laufwerke von Samsung).

Windows-Kennwortsynchronisierung

Die Windows-Kennwortsynchronisierung (WPS) legt automatisch das Windows-Kennwort der Benutzer als ihr Kennwort für das Self-Encrypting Drive fest. Diese Funktion wird für den Laufwerksadministrator nicht erzwungen; sie wird nur auf die Laufwerksbenutzer angewendet. Die WPS-Funktion kann in Unternehmensumgebungen verwendet werden, in denen Kennwörter regelmäßig geändert werden müssen (z. B. alle 90 Tage). Wenn diese Option aktiviert ist, werden alle Benutzerkennwörter für das Self-Encrypting Drive automatisch aktualisiert, sobald diese Windows-Kennwörter geändert werden.

HINWEIS: Wenn die Windows-Kennwortsynchronisierung (WPS) aktiviert ist, kann das Benutzerkennwort für das Self-Encrypting Drive nicht geändert werden. Ihr Windows-Kennwort muss geändert werden, um das Kennwort für das Laufwerk automatisch zu aktualisieren.

Letzten Benutzernamen merken

Wenn diese Option aktiviert ist, wird der letzte eingegebene Benutzername standardmäßig im Feld **Benutzername** auf dem Pre-Windows-Authentifizierungsbildschirm angezeigt.

Einen Benutzer auswählen

Wenn diese Option aktiviert ist, können die Benutzer standardmäßig alle Benutzernamen für das Laufwerk im Feld **Benutzername** auf dem Pre-Windows-Authentifizierungsbildschirm anzeigen.

Kryptografische Löschung

Mit dieser Option können alle Daten auf dem Self-Encrypting Drive "gelöscht" werden. Dabei werden die Daten nicht tatsächlich gelöscht, sondern die Schlüssel, mit denen die Daten verschlüsselt werden, wodurch die Daten unbrauchbar werden. Nach einer kryptografischen Löschung gibt es keine Möglichkeit, die Daten des Laufwerks wiederherzustellen. Zudem wird der Datenschutz des Self-Encrypting Drive deaktiviert, und das Laufwerk ist bereit für eine anderweitige Nutzung.

HINWEISE:

- Wenn Fehler im Zusammenhang mit den Verwaltungsfunktionen des Self-Encrypting Drive auftreten, schalten Sie den Computer vollständig aus (kein Neustart), und starten Sie ihn dann neu.
- Weitere Informationen zu spezifischen Fehlermeldungen finden Sie auf wave.com/support/Dell.

Informationen zum Authentifizierungsgerät

In der **Geräteverwaltung** werden im Fenster "Informationen zum Authentifizierungsgerät" Informationen zu allen angeschlossenen Authentifizierungsgeräten (Fingerabdruckscanner, Leser für herkömmliche oder Contactless Smartcards) im System sowie deren Status angezeigt.

Technischer Kundendienst

Den technischen Kundendienst für die Software **Dell Data Protection | Access** finden Sie auf http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Der Wave Systems Trusted Computing Group (TCG)-Enabled Cryptographic Service Provider (CSP) ist in der Anwendung **Dell Data Protection | Access** enthalten und kann immer dann eingesetzt werden, wenn ein CSP erforderlich ist. Er kann entweder direkt über eine Anwendung aufgerufen oder aus einer Liste installierter CSPs ausgewählt werden. Wählen Sie wenn möglich "Wave TCG-Enabled CSP" aus, um sicherzustellen, dass das TPM die Schlüssel generiert und dass die Schlüssel und die zugehörigen Kennwörter von **Dell Data Protection | Access** verwaltet werden.

Der Wave Systems TCG-Enabled CSP ermöglicht Anwendungen die Nutzung von auf TCG-kompatiblen Plattformen verfügbaren Funktionen direkt über MSCAPI. Der TCG-Enabled CSP ist ein TCG-fähiges MSCAPI-CSP-Modul, das im TPM asymmetrische Schlüsselfunktionen bereitstellt und die erweiterten Sicherheitsfunktionen des TPM-Moduls nutzt, unabhängig von lieferantenspezifischen Anforderungen hinsichtlich des TSS-Anbieters (Trusted Software Stack).

HINWEIS: Wenn für die vom Wave TCG-Enabled CSP generierten TPM-Schlüssel ein Kennwort erforderlich ist und der Benutzer ein TPM-Master-Kennwort erstellt hat, werden die einzelnen Schlüsselkennwörter zufällig generiert und im TPM-Kennworttresor gespeichert.