Dell Data Protection | Personal Edition

Installationshandbuch v8.13

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.

Personal Edition-Installationshandbuch

2017 - 04

Rev. A01

Inhaltsverzeichnis

1

Personal Edition-Übersicht

Dieses Handbuch nimmt an, dass Security Tools mit Personal Edition installiert wird.

Personal Edition

Der Zweck von Personal Edition ist, die Daten auf Ihrem Computer zu schützen, auch wenn der Computer verloren ging oder gestohlen wurde.

Um die Sicherheit Ihrer vertraulichen Daten zu gewährleisten, verschlüsselt Personal Edition die Daten auf Ihrem Windows-Computer. Sie können immer auf die Daten zugreifen, wenn Sie am Computer angemeldet sind, nicht autorisierte Benutzer haben jedoch keinen Zugriff auf diese geschützten Daten. Daten bleiben auf dem Laufwerk immer verschlüsselt, aber da die Verschlüsselung transparent ist, brauchen Sie Ihre Arbeitsweise mit Anwendungen und Daten nicht zu ändern.

Normalerweise entschlüsselt der Encryption Client die Daten, während Sie mit ihnen arbeiten. Gelegentlich versucht eine Softwareanwendung, auf eine Datei zuzugreifen, während diese gerade durch den Encryption Client verschlüsselt oder entschlüsselt wird. In diesem Fall zeigt der Encryption Client nach ein bis zwei Sekunden ein Dialogfeld an, über das Sie wählen können, ob Sie warten oder die Verschlüsselung bzw. Entschlüsselung abbrechen möchten. Falls Sie sich entscheiden zu warten, gibt der Encryption Client die Datei frei, sobald die Verarbeitung beendet ist (im Allgemeinen innerhalb weniger Sekunden).

Security Tools

Die Security Tools sind dazu gedacht, eine End-to-End-Sicherheitslösung zur Unterstützung von Advanced Authentication bereitzustellen.

Die Security Tools bieten eine umfassende Unterstützung für die Windows-Authentifizierung mit Passwörtern, Fingerabdrucklesern und Smart Cards (kontaktlose und mit Kontakt) und ermöglichen außerdem die Selbsteintragung, Einmalpasswörter (OTP) und die einstufige Anmeldung (Single Sign-On [SSO]).

Die Security Console ist die Security Tools-Oberfläche, die den Benutzer durch den Konfigurationsvorgang für Anmeldeinformationen und die Selbstwiederherstellungsfragen führt, je nachdem, welche Richtlinie der lokale Administrator festgelegt hat.

Das Tool „Administratoreinstellungen“ steht Benutzern mit Administratorrechten zur Verfügung und wird zur Einrichtung von Authentifizierungsrichtlinien und Wiederherstellungsoptionen, zur Verwaltung von Benutzern und zur Konfiguration erweiterter Einstellungen sowie von Einstellungen verwendet, die sich auf bestimmte unterstützte Anmeldeinformationen für die Windows-Anmeldung beziehen.

Unter Security Tools-Administratoreinstellungen konfigurieren im *Dell Console-Benutzerhandbuch* erfahren Sie, wie die Funktionen der Security Tools verwendet werden.

Kontaktaufnahme mit dem Dell ProSupport

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

Zusätzlich steht Ihnen unser Online-Support für Dell Data Protection-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 Ihren Service Code 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.

2

Personal Edition-Anforderungen

Diese Anforderungen beschreiben im Detail, was zur Installation der Personal Edition erforderlich ist.

Encryption-Client

- Für eine erfolgreiche Installation der Personal Edition ist eine Berechtigung erforderlich. Sie erhalten diese Berechtigung beim Erwerb von Personal Edition. Je nachdem, wie Sie Personal Edition kaufen, müssen Sie die Befugnis manuell installieren. Wenn dies der Fall ist, befolgen Sie die einfachen Anweisungen, die die Befugnis begleiten. Falls Personal Edition mit Dell Digital Delivery installiert wird, kümmert sich der Dell Digital Delivery-Dienst um die Installation der Befugnis. (Für Enterprise Edition und Personal Edition werden die gleichen Binärdateien verwendet. Durch die Berechtigung weiß das Installationsprogramm, welche Version installiert werden muss).
- Es wird von Dell nachdrücklich empfohlen, ein Windows-Passwort einzurichten (sofern noch nicht vorhanden), um den Zugriff auf Ihre verschlüsselten Daten zu beschränken. Wenn Sie den Computer durch ein Kennwort schützen, können sich andere nicht ohne dieses Kennwort bei Ihrem Benutzerkonto anmelden.
  a Rufen Sie die Windows-Systemsteuerung auf (**Start** > **Systemsteuerung**).
  b Klicken Sie auf das Symbol für **Benutzerkonto**.
  c Klicken Sie auf **Kennwort für das eigene Konto erstellen**.
  d Geben Sie ein neues Kennwort ein und bestätigen Sie es.
  e Sie können auch einen Kennworthinweis eingeben.
  f Klicken Sie auf **Kennwort erstellen**.
  g Starten Sie den Computer neu.
- Bei der Implementierung sind die bewährten IT-Verfahren zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Benutzer.
- Die Installation/Aktualisierung/Deinstallation kann nur von einem lokalen Benutzer oder einem Domänenadministrator durchgeführt werden, der über ein Implementierungstool wie Microsoft SMS oder KACE vorübergehend zugewiesen werden kann. Benutzer ohne Administratorstatus, aber mit höheren Rechten, werden nicht unterstützt.
- Sichern Sie vor Beginn der Installation/Deinstallation/Aktualisierung alle wichtigen Daten.
- Nehmen Sie während der Installation/Deinstallation/Aktualisierung keine Änderungen am Computer vor, dazu gehört auch das Einsetzen oder Entfernen von externen (USB-)Laufwerken.
- Entfernen Sie mithilfe des Windows-Desktopbereinigungs-Assistenten temporäre Dateien und andere unnötige Daten, um den Zeitaufwand für die anfängliche Verschlüsselung (wie auch den Zeitaufwand für die Entschlüsselung bei einer Deinstallation) zu verringern.
- Schalten Sie den Energiesparmodus bei der ersten Verschlüsselungssuche aus, um zu verhindern, dass ein unbeaufsichtigter Computer in diesen Modus umschaltet. Im Energiesparmodus kann keine Verschlüsselung (oder Entschlüsselung) erfolgen.
- Der Encryption-Client unterstützt keine Dual-Boot-Konfigurationen, da es hierdurch zur Verschlüsselung von Systemdateien des anderen Betriebssystems kommen kann, was den Betrieb stören würde.
- Das Master-Installationsprogramm unterstützt keine Aktualisierungen von Komponenten vor Version 8.0. Extrahieren Sie untergeordnete Installationsprogramme aus dem Master-Installationsprogramm und aktualisieren Sie einzeln die Komponente. Falls Sie Fragen oder Bedenken haben, wenden Sie sich an den Dell ProSupport.
- Der Encryption-Client unterstützt jetzt den Audit-Modus. Der Audit-Modus ermöglicht Administratoren die Bereitstellung des Encryption-Clients als Teil des Unternehmens-Image, anstatt das SCCM eines Drittanbieters oder ähnliche Lösungen zur Bereitstellung des Encryption-Clients zu verwenden. Anleitungen zur Installation der Verschlüsselungs-Client in einem Unternehmens-Image finden Sie unter http://www.dell.com/support/article/us/en/19/SLN304039.
- Das TPM wird zum Versiegeln des GPK-Schlüssels verwendet. Falls Sie den Encryption-Client ausführen, löschen Sie daher das TPM im BIOS, bevor Sie ein neues Betriebssystem auf dem Client-Computer installieren.
- Der Encryption-Client wurde getestet und ist kompatibel mit McAfee, dem Symantec-Client, Kaspersky und MalwareBytes. Für diese Anbieter von Virenschutzsoftware wurden hartkodierte Ausschlüsse implementiert, um Inkompatibilitäten zwischen Virenschutzprüfung

und Verschlüsselung zu verhindern. Der Encryption-Client wurde außerdem mit dem Microsoft Enhanced Mitigation Experience Toolkit getestet.

Falls Ihr Unternehmen Virenschutzsoftware von einem hier nicht aufgeführten Anbieter verwendet, lesen Sie den KB-Artikel SLN298707 oder Dell ProSupport kontaktieren, um Hilfe zu erhalten.

- Eine direkte Aktualisierung des Betriebssystems wird nicht unterstützt, wenn der Encryption-Client installiert ist. Deinstallieren Sie den Encryption-Client, führen Sie eine Entschlüsselung durch, aktualisieren Sie das Betriebssystem auf die neue Version, und führen Sie anschließend eine Neuinstallation von Encryption-Client durch.

  Die Neuinstallation des Betriebssystems wird ebenfalls nicht unterstützt. Zur Neuinstallation des Betriebssystems sichern Sie den Zielcomputer, setzen Sie den Computer zurück, installieren Sie das Betriebssystem, und stellen Sie anschließend die verschlüsselten Daten gemäß den üblichen Wiederherstellungsverfahren wieder her.
- Überprüfen Sie regelmäßig die Website www.dell.com/support, um stets über die neueste Dokumentation und die neuesten technischen Ratgeber zu verfügen.

Encryption-Client-Anforderungen

- Microsoft .Net Framework 4.5.2 (oder später) ist für den Master-Installations-Client sowie den untergeordneten Installations-Client erforderlich.

  Auf allen von Dell werksseitig ausgelieferten Computern ist Microsoft .Net Framework 4.5.2 (oder später) bereits vorinstalliert. Wenn Sie jedoch keine Dell Hardware verwenden oder den Client auf älterer Dell Hardware aktualisieren, sollten Sie überprüfen, welche Version von Microsoft .Net installiert ist und diese gegebenenfalls aktualisieren, **bevor Sie den Client installieren,** um Fehler bei der Installation/Aktualisierung zu vermeiden. Um die installierte Version von Microsoft .Net zu überprüfen, folgen Sie auf dem Computer, auf dem die Installation vollzogen werden soll, den folgenden Anweisungen: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Gehen Sie zu https://www.microsoft.com/en-us/download/details.aspx?id=42643, um Microsoft .Net Framework 4.5.2 zu installieren.
- Das Master-Installationsprogramm installiert Microsoft Visual C++ 2012 Update 4, falls diese Komponente noch nicht auf dem Computer vorhanden ist. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponente installieren, bevor Sie den Encryption-Client installieren.

Voraussetzungen

- Visual C++ 2012 Update 4 oder höheres Redistributable Package (x86 und x64)
- Microsoft SQL Server Compact 3.5 SP2 (x86 und x64)

Encryption-Client-Hardware

- Die folgende Tabelle enthält Informationen zur unterstützten Computer-Hardware.

Hardware

- Die Mindestanforderungen für die Hardware müssen den Mindestspezifikationen des Betriebssystems entsprechen.

- Die folgende Tabelle enthält Informationen zur unterstützten optionalen Computer-Hardware.

Optionale integrierte Hardware

- TPM 1.2 oder 2.0

Encryption-Client-Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

Windows-Betriebssysteme (32-Bit und 64-Bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 mit Application Compatibility-Vorlage (Hardwareverschlüsselung wird nicht unterstützt)
- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (Hardwareverschlüsselung wird nicht unterstützt)
- Windows 10: Education, Enterprise, Pro
- VMWare Workstation 5.5 und höher

> **ANMERKUNG: Der UEFI-Modus wird auf Windows 7, Windows Embedded Standard 7 und Windows Embedded 8.1 Industry Enterprise nicht unterstützt.**

Betriebssysteme für External Media Shield (EMS)

- Die folgende Tabelle enthält Informationen zu den unterstützten Betriebssystemen für den Zugriff auf Medien, die von EMS geschützt werden.

> **ANMERKUNG: Zur Verwendung von EMS müssen ungefähr 55 MB auf dem externen Speichermedium frei sein sowie weiterer freier Speicherplatz, in der Größe der umfangreichsten zu verschlüsselnden Datei, verfügbar sein.**

> **ANMERKUNG:**
> Windows XP wird nur bei Verwendung von EMS Explorer unterstützt.

Unterstützte Windows-Betriebssysteme für den Zugriff auf EMS-geschützte Medien (32-Bit und 64-Bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Unterstützte Mac-Betriebssysteme für den Zugriff auf EMS-geschützte Medien (64-Bit-Kernel)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- Mac OS Sierra 10.12.0

Encryption-Client-Sprachunterstützung

- Der Encryption-Client ist MUI-konform und unterstützt die folgenden Sprachen.

Sprachunterstützung

- EN: Englisch
- ES: Spanisch
- JA: Japanisch
- KO: Koreanisch

Sprachunterstützung

- FR: Französisch
- IT: Italienisch
- DE: Deutsch
- PT-BR: Portugiesisch, Brasilien
- PT-PT: Portugiesisch, Portugal

Advanced Authentication-Client

- Bei Verwendung von Advanced Authentication sichern Benutzer den Zugriff auf den Computer durch erweiterte Anmeldeinformationen, die mit Security Tools verwaltet und eingetragen werden. Security Tools ist damit das primäre Programm zur Verwaltung der Authentifizierungsinformationen für die Windows-Anmeldung, einschließlich Windows-Passwort, Fingerabdrücke und Smart Cards. Über das Microsoft-Betriebssystem eingetragene Authentifizierungsinformationen für die Anmeldung per Bildcode, PIN und Fingerabdruck werden bei der Windows-Anmeldung nicht erkannt.

  Wenn Sie Ihre Anmeldeinformationen weiterhin mit dem Microsoft-Betriebssystem verwalten möchten, installieren Sie Security Tools nicht, bzw. deinstallieren Sie das Programm.
- Für die Einmalpasswort (OTP)-Funktion in Security Tools muss ein TPM vorhanden, aktiviert und zugewiesen sein. OTP wird nicht mit TPM 2.0 unterstützt. Weitere Informationen zum Löschen und Definieren der TMP-Zuweisung finden Sie unter https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Advanced Authentication-Client-Hardware

- Die folgende Tabelle enthält detaillierte Informationen über die unterstützte Authentifizierungs-Hardware.

Fingerabdruck- und Smart Card-Leser

- Validity VFS495 im sicheren Modus
- Dell ControlVault Swipe Reader
- UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
- Authentec Eikon und Eikon To Go USB-Lesegeräte

Kontaktlose Karte

- Kontaktlose Karten nutzen die entsprechenden Lesegeräte, die auf bestimmten Dell Laptops installiert sind

Smart Card

- PKCS #11 Smart Cards verwenden den ActivIdentity-Client.

  ANMERKUNG: Der ActivIdentity-Client ist nicht vorinstalliert und muss daher separat installiert werden.
- CSP Cards
- Common Access Cards (CACs)
- Net-Karten der B/SIPR-Klasse

- Treiber und Firmware für Dell ControlVault, Fingerabdruckleser und Smart Cards (siehe unten) sind nicht im Master-Installationsprogramm oder in den untergeordneten ausführbaren Installationsdateien enthalten. Treiber und Firmware müssen jederzeit auf dem aktuellen Stand sein und können nach Auswahl des jeweiligen Computermodells von der Website http://www.dell.com/support heruntergeladen werden. Laden Sie die jeweiligen Treiber und die Firmware basierend auf Ihrer Authentifizierungshardware herunter.

  - Dell ControlVault
  - NEXT Biometrics Fingerprint-Treiber
  - Validity Fingerprint Reader 495-Treiber
  - O2Micro Smart Card-Treiber

Falls Sie Hardware installieren möchten, die nicht von Dell stammt, müssen Sie die aktualisierten Treiber und die Firmware von der Website des jeweiligen Herstellers herunterladen. Installationsanweisungen für Dell ControlVault-Treiber finden Sie unter Dell ControlVault Drivers.

- In der folgenden Tabelle werden die Dell-Computermodelle mit Unterstützung von Netzkarten der Klasse SIPR aufgelistet.

Dell-Computermodelle – Class B/SIPR Net Card-Unterstützung

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Advanced Authentication Client - Betriebssysteme

Windows-Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

Windows-Betriebssysteme (32-Bit und 64-Bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

ⓘ | **ANMERKUNG: Der UEFI-Modus wird auf Windows 7 nicht unterstützt.**

Betriebssysteme für Mobilgeräte

- Die folgenden mobilen Betriebssystem werden von der Einmal-Passwort-Funktion von Security Tools unterstützt.

Android-Betriebssysteme

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

iOS-Betriebssysteme

- iOS 7.x
- iOS 8.x

Windows Phone-Betriebssysteme

- Windows Phone 8.1
- Windows 10 Mobile

Advanced Authentication Client - Sprachunterstützung

- Der Advanced Authentication-Client ist MUI-konform und unterstützt die folgenden Sprachen. Der UEFI-Modus sowie die Preboot-Authentifizierung werden auf Russisch sowie auf traditionellem und vereinfachtem Chinesisch nicht unterstützt.

Sprachunterstützung

- EN: Englisch
- FR: Französisch
- IT: Italienisch
- DE: Deutsch
- ES: Spanisch
- JA: Japanisch
- KO: Koreanisch
- ZH-CN: Chinesisch, vereinfacht
- ZH-TW: Chinesisch, traditionell/Taiwan
- PT-BR: Portugiesisch, Brasilien
- PT-PT: Portugiesisch, Portugal
- RU: Russisch

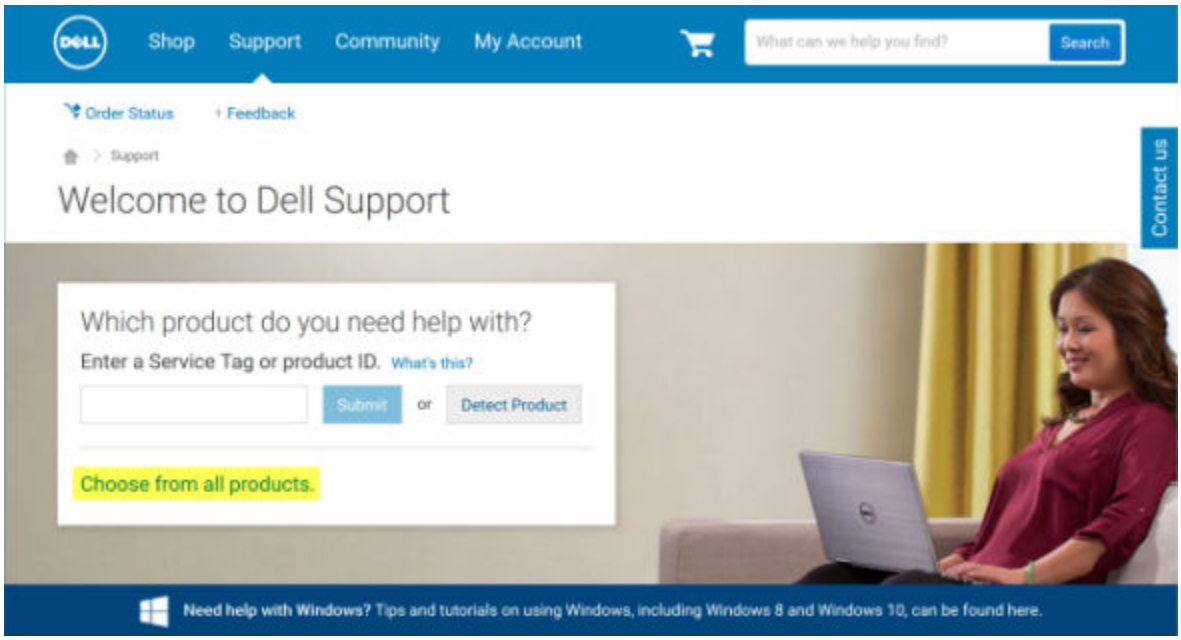
Fahren Sie mit Software abrufen fort.

Herunterladen der Software

Dieser Abschnitt erläutert den Bezug der Software unter dell.com/support. Wenn Sie die Software bereits haben, können Sie diesen Abschnitt überspringen.

Rufen Sie dell.com/support auf, um zu beginnen.

1 Wählen Sie auf der Dell Support-Webseite **Aus allen Produkten auswählen** aus.



2 Wählen Sie **Software und Sicherheit** aus der Produktliste aus.

3 Wählen Sie im Abschnitt *Software und Sicherheit* **Endpoint Security Solutions** aus.
Wenn diese Auswahl einmal vorgenommen wurde, wird sie von der Website gespeichert.

4 Wählen Sie die Dell Data Protection Produkt.
Beispiele:

Dell Verschlüsselung

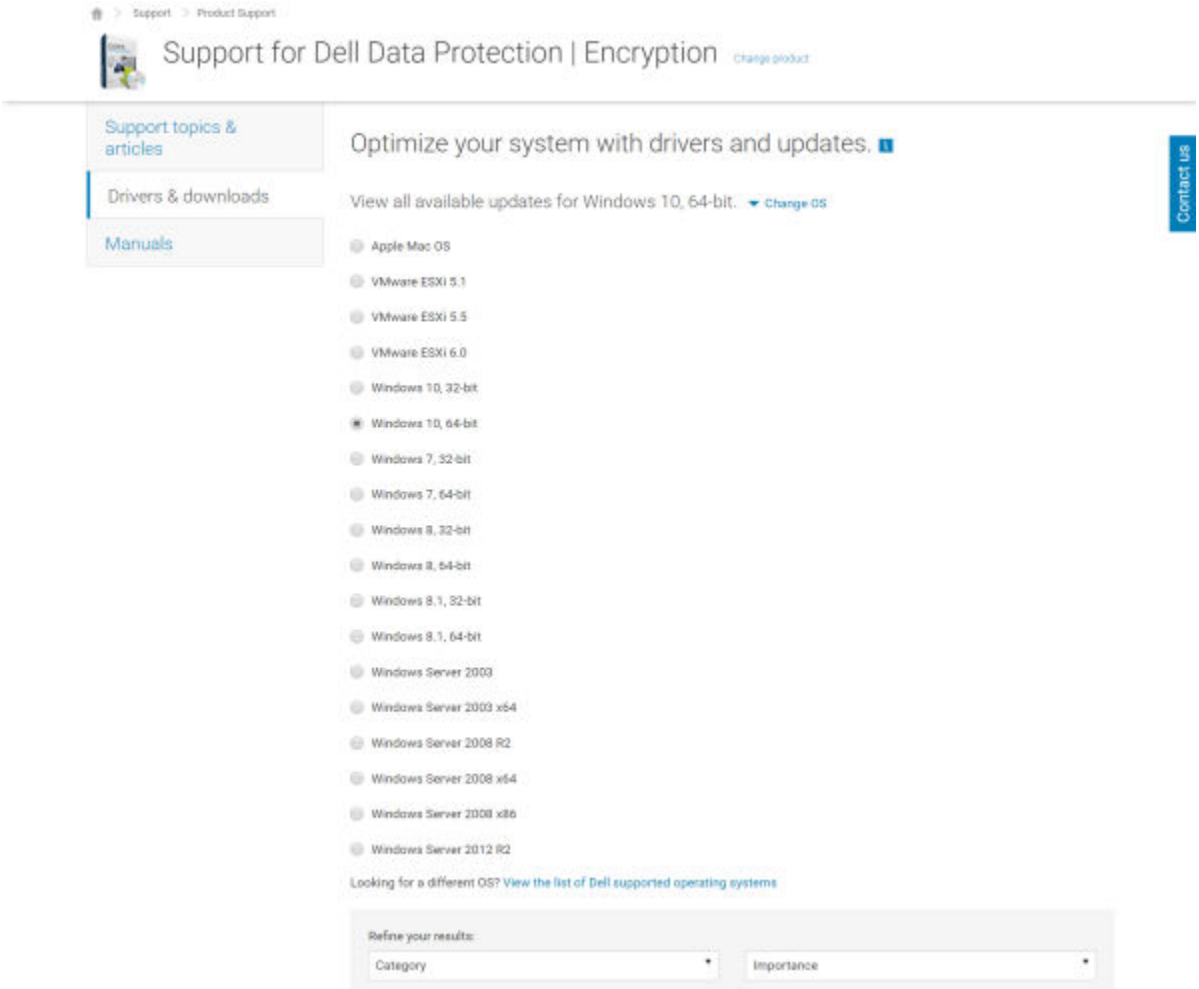
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 Wählen Sie **Treiber und Downloads** aus.

6 Wählen Sie den gewünschten Client-Betriebssystemtyp aus.

7 Wählen Sie aus den Ergebnissen **Dell Data Protection (4 Dateien)** aus. Da es sich hierbei nur um ein Beispiel handelt, wird es sich wahrscheinlich ein wenig anders darstellen. Beispielsweise stehen möglicherweise keine 4 Dateien zur Auswahl.



8 Wählen Sie **Datei herunterladen** oder **Zu meiner Downloadliste #XX hinzufügen** aus.
Fahren Sie mit Personal Edition installieren fort.

4

Personal Edition installieren

Sie können Personal Edition mit dem Master-Installationsprogramm (empfohlen) oder einzeln installieren, indem Sie die untergeordneten Installationsprogramme aus dem Master-Installationsprogramm extrahieren. In jedem Fall kann Personal Edition mit beliebigen Benutzerschnittstellen, Befehlszeilen oder Skripts und mit jeder verfügbaren Push-Technologie in Ihrer Organisation installiert werden.

Benutzer sollten die folgenden Hilfedateien lesen, um Unterstützung für die Anwendung zu erhalten:

- Informationen zur Verwendung der Funktionen von Encryption-Client finden Sie im Hilfedokument *Dell Encrypt Help*. Hier können Sie auf die Hilfe zugreifen: **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
- Informationen zur Verwendung der Funktionen von External Media Shield finden Sie im Hilfedokument *EMS Help*. Hier können Sie auf die Hilfe zugreifen: **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
- In der *Hilfe zu Security Tools* erfahren Sie, wie Sie die Funktionen von Advanced Authentication verwenden. Hier können Sie auf die Hilfe zugreifen: **<Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**.

Installationsverfahren auswählen

Es gibt zwei Methoden, um den Client zu installieren. Entscheiden Sie sich für **eine** davon:

- Personal Edition mit dem Master-Installationsprogramm installieren - EMPFOHLEN
- Individuelle Personal Edition-Installation unter Verwendung der untergeordneten Installationsprogramme

Personal Edition mit dem Master-Installationsprogramm installieren - EMPFOHLEN

Zur Installation von Personal Edition muss das Installationsprogramm die entsprechende Berechtigung auf dem Computer vorfinden. Wenn die entsprechende Berechtigung nicht gefunden wird, kann Personal Edition nicht installiert werden.

Der Dell Data Protection Installer wird auch als Master Installer bezeichnet, weil damit mehrere Clients installiert werden. Handelt es sich um Personal Edition, installiert dieses den Encryption Client und den Advanced Authentication Client.

Falls Sie die Benutzerschnittstelle des Master-Installationsprogramms zur Installation verwenden, kann Personal Edition auf einen Computer nach dem anderen installiert werden.

Die Protokolldateien des Master-Installationsprogramms befinden sich unter **C:\ProgramData\Dell\Dell Data Protection\Installer.**

Wählen Sie eine Methode aus:

Installation mithilfe der Benutzerschnittstelle

Installation unter Verwendung der Befehlszeile

Installation mithilfe der Benutzerschnittstelle

Falls nötig, installieren Sie die Befugnis auf dem Zielcomputer.

Kopieren Sie DDPSetup.exe auf den lokalen Computer.

Doppelklicken Sie auf DDPSetup.exe, um das Installationsprogramm aufzurufen.

Es wird ein Dialogfeld angezeigt, das Sie auf den Installationsstatus der Voraussetzungen aufmerksam macht. Dieser Vorgang kann einige Minuten dauern.

Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.

Lesen Sie die Lizenzvereinbarung, stimmen Sie den Bedingungen zu, und klicken Sie auf **Weiter**.

Klicken Sie auf **Weiter**, um Personal Edition am Standardort **C:\Program Files\Dell\Dell Data Protection\.** zu installieren.

Security Tools wird standardmäßig installiert und kann nicht deaktiviert werden. Im Installer sind sie unter Security Framework aufgeführt.

Advanced Authentication wird standardmäßig installiert und kann nicht deaktiviert werden.

Klicken Sie auf **Weiter**.

Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Ein Statusfenster wird angezeigt. Dieser Vorgang kann mehrere Minuten dauern.

Wählen Sie **Ja, ich möchte meinen Computer jetzt neu starten** aus, und klicken Sie dann auf **Fertigstellen**.

Wenn der Computer neu gestartet wird, authentifizieren Sie sich bei Windows.

Die Installation von Personal Edition + Security Tools ist abgeschlossen.

Personal Edition Setup-Assistent und Konfiguration werden separat beschrieben.

Starten Sie die Security Tools Administrator Console nach Abschluss des Personal Edition Setup-Assistenten und Fertigstellung der Konfiguration.

Im Rest des Abschnitts werden weitere Installationsaufgaben beschrieben, die Sie überspringen können. Fahren Sie mit Security Tools und Personal Edition Setup-Assistenten fort.

Installation unter Verwendung der Befehlszeile

Falls nötig, installieren Sie die Befugnis auf dem Zielcomputer.

Schalter:

Für eine Installation über die Befehlszeile müssen zunächst die Befehlszeilenschalter festgelegt werden. Die folgende Tabelle umfasst die für die Installation verfügbaren Schalter.

Schalter	Erläuterung
-y -gm2	Daten an den Selbstextraktor geben
/S	Im Hintergrund
/z	Daten an die InstallScript-Systemvariable CMDLINE geben

Parameter:

Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

Parameter
InstallPath=Pfad zum alternativen Installationsspeicherort.
FEATURE=PE

Beispiel einer Installation über die Befehlszeile

Obwohl der Neustart in diesen Beispielen unterdrückt wird, ist ein Neustart irgendwann einmal erforderlich. Die Verschlüsselung kann erst nach dem Neustart des Computers beginnen.

Stellen Sie sicher, dass ein Wert eingegeben wird, der eines oder mehrere Sonderzeichen, z. B. eine Leerstelle, zwischen in Escape-Zeichen gesetzten Anführungszeichen enthält.

Bei den Befehlszeilen ist die Groß- und Kleinschreibung zu beachten.

Im folgenden Beispiel wird Personal Edition und Security Tools installiert (Installation im Hintergrund, kein Neustart, Installation im Standardverzeichnis **C:\Program Files\Dell\Dell Data Protection**).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE\""
```

Im folgenden Beispiel wird Personal Edition und Security Tools installiert (Installation im Hintergrund, kein Neustart, Installation an einem alternativen Standort **C:\Program Files\Dell\My_New_Folder**).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
```

Melden Sie sich nach dem Neustart des Computers bei Windows an.

Die Installation von Personal Edition + Security Tools ist abgeschlossen.

Personal Edition Setup-Assistent und Konfiguration werden separat beschrieben.

Starten Sie die Security Tools Administrator Console nach Abschluss des Personal Edition Setup-Assistenten und Fertigstellung der Konfiguration.

Im Rest des Abschnitts werden weitere Installationsaufgaben beschrieben, die Sie überspringen können. Fahren Sie mit Security Tools und Personal Edition Setup-Assistenten fort.

Individuelle Personal Edition-Installation unter Verwendung der untergeordneten Installationsprogramme

Um Personal Edition mit den untergeordneten Installationsprogrammen zu installieren, müssen die untergeordneten ausführbaren Dateien zuerst vom Master-Installationsprogramm extrahiert werden. Weitere Informationen finden Sie unter Untergeordnete Installer aus dem Master Installer extrahieren. Kehren Sie nach Abschluss zu diesem Abschnitt zurück.

Installation über die Befehlszeile

Bei den Befehlszeilenschaltern und -parametern ist die Groß- und Kleinschreibung zu beachten.

Stellen Sie sicher, dass Werte, die ein oder mehrere Sonderzeichen enthalten, z. B. eine Leerstelle in der Befehlszeile, zwischen in Escape-Zeichen gesetzte Anführungszeichen gesetzt werden.

Verwenden Sie diese Installationsprogramme zur Installation der Clients. Nutzen Sie dazu eine skriptgesteuerte Installation, Batchdateien oder eine andere verfügbare Push-Technologie.

Der Neustart wurde in den Befehlszeilenbeispielen unterdrückt. Es ist jedoch ein abschließender Neustart erforderlich. Die Verschlüsselung kann erst nach dem Neustart des Computers beginnen.

Protokolldateien: Windows erstellt für den angemeldeten Benutzer eindeutige Installationsprotokolldateien des untergeordneten Installationsprogramms im Verzeichnis %temp%, unter **C:\Users\<UserName>\AppData\Local\Temp.**

Falls Sie sich dafür entscheiden, beim Ausführen des Installationsprogramms eine separate Protokolldatei hinzuzufügen, stellen Sie sicher, dass die Protokolldatei einen eindeutigen Namen hat, da Protokolldateien des untergeordneten Installationsprogramms keine Anhänge zulassen. Mit dem standardmäßigen .msi-Befehl kann eine Protokolldatei unter Verwendung von **/l*v C:\<any directory>\<any log file name>.log** erstellt werden.

Für Installationen über die Befehlszeile verwenden alle untergeordneten Installationsprogramme, soweit nicht anders angegeben, die gleichen grundlegenden .msi-Schalter und Anzeigeoptionen. Die Schalter müssen zuerst angegeben werden. Der /v-Schalter ist erforderlich und benötigt ein Argument. Andere Parameter gehen in ein Argument ein, das an den /v-Schalter weitergegeben wird.

Anzeigeoptionen können am Ende des Arguments angegeben werden, das an den /v-Schalter weitergegeben wird, um das erwartete Verhalten zu erzielen. Verwenden Sie /q und /qn nicht in derselben Befehlszeile. Verwenden Sie ! und - nur nach /qb.

Schalter	Erläuterung
/v	Gibt Variablen an die .msi-Datei innerhalb der *.exe-Datei weiter.
/s	Im Hintergrund
/i	Installationsmodus

Option	Erläuterung
/q	Kein Fortschrittsdialogfeld, führt nach Abschluss der Installation selbstständig einen Neustart durch
/qb	Fortschrittsdialogfeld mit der Schaltfläche **Abbrechen,** fordert zum Neustart auf
/qb-	Fortschrittsdialogfeld mit der Schaltfläche **Abbrechen**, führt nach Abschluss des Vorgangs selbstständig einen Neustart durch
/qb!	Fortschrittsdialogfeld ohne die Schaltfläche **Abbrechen**, fordert zum Neustart auf
/qb!-	Fortschrittsdialogfeld ohne die Schaltfläche **Abbrechen**, führt nach Abschluss des Vorgangs selbstständig einen Neustart durch
/qn	Keine Benutzeroberfläche

Treiber installieren

Treiber und Firmware für Dell ControlVault, Fingerabdruckleser und Smart Cards sind **nicht** im Master-Installationsprogramm oder in den untergeordneten ausführbaren Installationsdateien enthalten. Treiber und Firmware müssen jederzeit auf dem aktuellen Stand sein und können nach Auswahl des jeweiligen Computermodells von der Website http://www.dell.com/support heruntergeladen werden. Laden Sie die jeweiligen Treiber und die Firmware basierend auf Ihrer Authentifizierungshardware herunter.

Dell ControlVault

NEXT Biometrics Fingerprint-Treiber

Validity Fingerprint Reader 495-Treiber

O2Micro Smart Card-Treiber

Falls Sie Hardware installieren möchten, die nicht von Dell stammt, müssen Sie die aktualisierten Treiber und die Firmware von der Website des jeweiligen Herstellers herunterladen.

Dann:

Installieren der Advanced Authentication Clients

Benutzer melden sich mit ihren Windows-Anmeldeinformationen an der PBA an.

Machen Sie die Datei unter **C:\extracted\Security Tools** und **C:\extracted\Security Tools\Authentication. ausfindig.**

Beispiel einer Installation über die Befehlszeile

\Security Tools

Im folgenden Beispiel wird das Security Framework installiert (Installation im Hintergrund, kein Neustart, und wird am Standard-Standort C:\Program Files\Dell\Dell Data Protection installiert).

```
EMAgent_XXbit_setup.exe /s /v"/norestart /qn"
```

:

Dieser Client ist für Advanced Authentication in Version v8.x erforderlich.

Dann:

\Security Tools\Authentication

Im folgenden Beispiel werden die Security Tools installiert (Installation im Hintergrund, kein Neustart, Installation im Standardverzeichnis **C:\Program Files\Dell\Dell Data Protection**).

```
setup.exe /s /v"/norestart /qn"
```

Dann:

Encryption-Client installieren

Überprüfen Sie die Encryption-Client-Anforderungen, falls Ihre Organisation ein von einer Stammstelle signiertes Zertifikat verwendet, wie EnTrust oder Verisign. Zur Aktivierung der Zertifikatsprüfung muss eine Registrierungseinstellung auf dem Client-Computer geändert werden.

Machen Sie die Datei unter **C:\extracted\Encryption ausfindig.**

Beispiel einer Installation über die Befehlszeile

Im folgenden Beispiel werden Personal Edition, Encrypt for Sharing installiert, die Overlay-Symbole werden ausgeblendet, es gibt keinen Dialog, keine Statusanzeige und keinen Neustart.

```
DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

Melden Sie sich nach dem Neustart des Computers bei Windows an.

Die Installation von Personal Edition + Security Tools ist abgeschlossen. Personal Edition Setup-Assistent und Konfiguration werden separat beschrieben.

Fahren Sie mit Security Tools und Personal Edition Setup-Assistenten fort.

Security Tools und Personal Edition Setup-Assistenten

Melden Sie sich mit Ihrem Windows-Benutzernamen und Kennwort an. Sie werden nahtlos an Windows weitergeleitet. Die Oberfläche sieht möglicherweise anders aus, als sie es gewohnt sind.

1 Möglicherweise werden Sie durch die UAC (Benutzerkontensteuerung) zum Ausführen der Anwendung aufgefordert. Ist dies der Fall, dann klicken Sie auf „Ja“.

2 Nach dem ersten Neustart während der Installation wird der Security Tools Aktivierungsassistent angezeigt. Klicken Sie auf **Weiter**.

3 Geben Sie ein neues Administrator-Passwort für die Verschlüsselung (Encryption Administrator Password, EAP) ein und geben Sie es noch einmal ein. Klicken Sie auf **Weiter**.

4 Geben Sie zum Speichern der Wiederherstellungsinformationen einen auf einem Netzwerk oder einem Wechseldatenträger gelegenen Speicherpfad ein und klicken Sie auf **Weiter**.

5 Klicken Sie auf **Anwenden**, um mit der ST-Aktivierung zu beginnen.

6 Starten Sie nach Abschluss des Security Tools-Aktivierungsassistenten den Personal Edition Setup-Assistenten über das DDP-Symbol in der Taskleiste (möglicherweise startet er auch selbständig).

Der Installationsassistent hilft Ihnen dabei, die Daten auf dem Computer durch Verschlüsselung zu schützen. Wenn dieser Assistent nicht abgeschlossen wird, kann die Verschlüsselung nicht gestartet werden.

Lesen Sie die Informationen im Begrüßungsbildschirm, und klicken Sie auf **Weiter**.

7 Wählen Sie eine Richtlinienvorlage aus. Die Richtlinienvorlage legt die Standardrichtlinieneinstellungen für die Verschlüsselung fest.

Sie können ganz einfach eine andere Richtlinienvorlage anwenden oder in der lokalen Management Console eine ausgewählte Vorlage anpassen, sobald die ursprüngliche Konfiguration abgeschlossen wurde.

Klicken Sie auf **Weiter**.

8 Lesen und bestätigen Sie die Warnung zum Windows-Passwort. Falls Sie ein Windows-Passwort einrichten möchten, gehen Sie zu Anforderungen.

9 Richten Sie ein Administratorpasswort für die Verschlüsselung (EAP) ein, das aus 9 bis 32 Zeichen besteht, und bestätigen Sie es. Das Passwort sollte Buchstaben, Zahlen und Sonderzeichen enthalten. Dieses Passwort kann das gleiche sein wie das EAP, das Sie für Security Tools einrichten, es steht jedoch in keiner Beziehung dazu. **Notieren Sie sich das Passwort, und bewahren Sie es an einem sicheren Ort auf.** Klicken Sie auf **Weiter**.

10 Klicken Sie auf **Durchsuchen**, um ein Netzlaufwerk oder Wechselspeichermedium zur Sicherung Ihrer Verschlüsselungsschlüssel auszuwählen. (Die Schlüssel sind in einer Anwendung namens LSARecovery_[hostname].exe enthalten).

Bei bestimmten Systemausfällen werden diese Schlüssel zur Wiederherstellung der Daten verwendet.

Auch bei künftigen Richtlinienänderungen ist es manchmal notwendig, die Verschlüsselungsschlüssel erneut zu sichern. Ist das Netzwerklaufwerk oder das Wechselspeichermedium gerade angeschlossen, erfolgt die Sicherung der Verschlüsselungsschlüssel im Hintergrund. Steht dieser Speicherpfad jedoch nicht zur Verfügung (zum Beispiel wenn das Wechselspeichermedium nicht an den Computer angeschlossen ist), treten Richtlinienänderungen so lange nicht in Kraft, bis die Verschlüsselungsschlüssel manuell gesichert wurden.

> **ANMERKUNG: Um zu erfahren, wie Sie Verschlüsselungsschlüssel manuell sichern können, klicken Sie auf "? > Hilfe</1>" oben rechts in der lokalen Management Console oder durch Klicken auf Start > Alle Programme > Dell > Dell Data Protection > Verschlüsselung > Verschlüsselungshilfe.**

Klicken Sie auf **Weiter**.

11 Auf dem Bildschirm „Verschlüsselungseinstellungen bestätigen“ wird eine Liste der Verschlüsselungseinstellungen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf **Bestätigen**.

Die Konfiguration des Computers wird durchgeführt. Eine Statusleiste zeigt den Fortschritt der Konfiguration an.

12 Klicken Sie zum Abschluss der Konfiguration auf **Fertig stellen**.

13 Nach der Konfiguration des Computers für die Verschlüsselung ist ein Neustart erforderlich. Klicken Sie auf **Jetzt neustarten**. Sie können den Neustart auch 5 mal um jeweils 20 Minuten verzögern.

14 Öffnen Sie nach dem Neustart des Computers vom Startmenü aus die Local Management Console, um den Status der Verschlüsselung zu sehen.

Die Verschlüsselung findet im Hintergrund statt. Die Local Management Console kann hierbei geöffnet oder geschlossen sein. In beiden Fällen wird die Verschlüsselung der Dateien fortgesetzt. Sie können während der Verschlüsselung den Computer wie gewohnt verwenden.

15 Nach Abschluss der Suche startet der Computer noch einmal neu.

Nachdem alle Verschlüsselungssuchen und Neustarts abgeschlossen wurden, können Sie den Konformitätsstatus überprüfen, indem Sie die Local Management Console starten. Das Laufwerk wird als „In Compliance“ (konform) bezeichnet.

Fahren Sie mit Security Tools-Administratoreinstellungen konfigurieren fort.

Konfigurieren der Security Tools-Administrator-Einstellungen

Die Security Tools Standardeinstellung sieht vor, dass Administratoren und Benutzer Security Tools sofort nach der Installation und Aktivierung ohne zusätzliche Konfiguration nutzen können. Benutzer werden automatisch als Security Tools-Benutzer hinzugefügt, wenn sie sich mit ihrem Windows-Passwort beim Computer anmelden. Standardmäßig ist die mehrstufige Windows-Authentifizierung jedoch deaktiviert.

Um Security Tools-Funktionen zu konfigurieren, müssen Sie auf dem Computer Administratorrechte besitzen.

Administrator-Passwort und Sicherungsverzeichnis ändern

Nach der Security Tools-Aktivierung können das Administratorpasswort und der Speicherort der Sicherungsdatei bei Bedarf geändert werden.

1 Als Administrator starten Sie Security Tools über die Desktop-Verknüpfung.
2 Klicken Sie auf die Kachel **Administratoreinstellungen**.
3 Geben Sie im Dialogfeld „Authentifizierung“ das Administrator-Passwort ein, das bei der Aktivierung eingerichtet wurde, und bestätigen Sie es mit **OK.**
4 Klicken Sie auf die Registerkarte **Administratoreinstellungen**.
5 Wenn Sie das Passwort ändern möchten, geben Sie auf der Administratorpasswort-Seite ein neues Passwort mit 8-32 Zeichen ein, darunter mindestens ein Buchstabe, eine Zahl und ein Sonderzeichen.
6 Geben Sie das Passwort zur Bestätigung ein zweites Mal ein und klicken Sie dann auf **Übernehmen**.
7 Um den Speicherort des Wiederherstellungsschlüssels zu ändern, wählen Sie im linken Fensterbereich **Speicherort der Sicherungsdatei ändern** aus.
8 Wählen Sie einen neuen Speicherort für die Sicherung aus, und klicken Sie dann auf **Übernehmen**.

   Der Speicherort der Sicherungsdatei muss ein Netzlaufwerk oder ein Wechseldatenträger sein. Die Sicherungsdatei enthält die Schlüssel, die zur Wiederherstellung von Daten auf diesem Computer erforderlich sind. Dell ProSupport muss auf diese Datei zugreifen können, um Sie bei der Wiederherstellung zu unterstützen.

   Wiederherstellungsdaten werden automatisch am angegebenen Speicherort gesichert. Falls der Speicherort nicht verfügbar ist (wenn beispielsweise das USB-Sicherungs-Laufwerk nicht angeschlossen ist), fordert Security Tools zur Eingabe eines Speicherorts für die Sicherung der Daten auf. Damit die Verschlüsselung starten kann, ist der Zugriff auf die Wiederherstellungsdaten erforderlich.

Authentifizierungsoptionen konfigurieren

Mithilfe der Steuerungen der Registerkarte „Authentifizierung“ in den Administratoreinstellungen können Sie Anmeldeoptionen für Benutzer festlegen und die einzelnen Einstellungen anpassen.

ANMERKUNG: Die Einmalpasswort-Funktion wird unter den Wiederherstellungsoptionen nicht angezeigt, wenn TPM nicht vorhanden ist bzw. nicht zugewiesen oder aktiviert wurde.

Anmeldeoptionen konfigurieren

Auf der Seite „Anmeldeoptionen“ können Sie Anmeldungsrichtlinien konfigurieren. Standardmäßig sind alle unterstützten Anmeldeinformationen unter „Verfügbare Optionen“ aufgelistet.

Um die Anmeldeoptionen zu konfigurieren:

Wählen Sie im linken Bildschirmbereich unter Authentifizierung **Anmeldeoptionen** aus.

Um eine Rolle auszuwählen, die Sie einrichten möchten, wählen Sie die Rolle in der Liste **Anmeldeoptionen anwenden auf** aus: **Benutzer** oder **Administratoren**. Alle Änderungen, die Sie auf dieser Seite vornehmen, beziehen sich nur auf die von Ihnen ausgewählte Rolle.

Legen Sie die verfügbaren Optionen für die Authentifizierung fest.

Standardmäßig ist jede Authentifizierungsmethode so konfiguriert, dass sie individuell, also nicht in Kombination mit anderen Authentifizierungsmethoden, verwendet wird. Sie können die Standardeinstellungen folgendermaßen ändern:

Um eine Kombination von Authentifizierungsoptionen einzurichten, klicken Sie unter „Verfügbare Optionen“ auf , um die erste Authentifizierungsmethode auszuwählen. Wählen Sie im Dialogfeld „Verfügbare Optionen“ die zweite Authentifizierungsmethode aus, und klicken Sie anschließend auf **OK**.

Sie können beispielsweise als Anmeldeinformationen sowohl einen Fingerabdruck, als auch ein Passwort verlangen. Wählen Sie im Dialogfeld die zweite Authentifizierungsmethode aus, die zusammen mit der Authentifizierung durch Fingerabdruck verwendet werden soll.

Um jede Authentifizierungsmethode einzeln verwenden zu können, lassen Sie im Dialogfeld „Verfügbare Optionen“ die Einstellung für die zweite Authentifizierungsmethode auf **Ohne** eingestellt und klicken Sie dann auf **OK**.

Um eine Anmeldeoption zu entfernen, klicken Sie unter „Verfügbare Optionen“ auf der Seite „Anmeldeoption“ auf das **X**, um das Verfahren zu entfernen.

Um eine neue Kombination an Authentifizierungsmethoden hinzuzufügen, klicken Sie auf **Eine Option hinzufügen**.

Legen Sie Wiederherstellungsoptionen für Benutzer fest, die ihre Zugangsdaten nach der Abmeldung wiederherstellen möchten.

Um Benutzern die Festlegung von Wiederherstellungsfragen zur Wiederherstellung Ihrer Anmeldedaten zu ermöglichen, wählen Sie **Wiederherstellungsfragen** aus.

Entfernen Sie die Markierung, wenn Sie das Einrichten von Wiederherstellungsfragen verhindern möchten.

Um Benutzern die Wiederherstellung ihrer Anmeldedaten über ein mobiles Gerät zu ermöglichen, wählen Sie **Einmalpasswort** aus. Wenn die Option „Einmalpasswort“ (OTP) als das Wiederherstellungsverfahren ausgewählt ist, ist sie als Anmeldeoption auf dem Anmeldebildschirm von Windows nicht verfügbar.

Um die OTP-Funktion zur Anmeldung zu verwenden, deaktivieren Sie diese Methode unter Wiederherstellungsoptionen. Wenn OTP als Wiederherstellungsoption deaktiviert wird, erscheint die OTP-Option auf der Windows-Anmeldeseite, sofern sich mindestens ein Benutzer für OTP eingetragen hat.

: Als Administrator kontrollieren Sie, wie das Einmalpasswort verwendet werden kann – entweder zur Authentifizierung oder zur Wiederherstellung. Die OTP-Funktion kann zur Authentifizierung oder zur Wiederherstellung verwendet werden, aber nicht für beides. Die Konfiguration betrifft entweder alle Benutzer des Computers oder alle Administratoren, basierend auf der Auswahl im Anmeldeoptionen-Feld Anmeldeoptionen übernehmen für.

Wird die Einmalpasswort-Option in den Wiederherstellungsoptionen nicht angezeigt wird, wird diese Option auf der Konfiguration Ihres Computers nicht unterstützt. Weitere Informationen finden Sie unter Anforderungen.

Wenn Sie möchten, dass der Benutzer bei Verlust oder Vergessen der Anmeldeinformationen Kontakt mit dem Help Desk aufnimmt, deaktivieren Sie die Kontrollkästchen unter „Wiederherstellungsoptionen“: Wiederherstellungsfragen und Einmalpasswort.

Wählen Sie **Toleranzzeitraum** aus, um einen Zeitraum festzulegen, in dem Benutzer ihre Anmeldeinformationen für die Authentifizierung eintragen können.

Sie können mit der Funktion „Toleranzzeitraum“ ein Datum angeben, ab dem eine konfigurierte Anmeldeoption durchgesetzt wird. Sie können also eine Anmeldeoption vor dem Datum ihrer Durchsetzung konfigurieren und eine Zeitspanne festlegen, in der Benutzer ihre Daten eintragen können. Standardmäßig wird die Richtlinie sofort durchgesetzt.

Um den Zeitpunkt für die Durchsetzung der Anmeldeoption im Dialogfeld „Toleranzzeitraum“ von *Sofort* in ein anderes Datum zu ändern, wählen Sie im Dropdown-Menü die Option **Bestimmtes Datum** aus. Klicken Sie rechts neben dem Datumsfeld auf den Pfeil nach unten, um einen Kalender aufzurufen, in dem Sie das Datum auswählen können. Die Durchsetzung der Richtlinie beginnt in der Regel um 00:01 Uhr am ausgewählten Datum.

Benutzer können bei ihrer nächsten Windows-Anmeldung an die Eintragung der erforderlichen Anmeldeinformationen erinnert werden (Standardeinstellung), oder aber Sie richten regelmäßige Erinnerungen ein. Wählen Sie das Erinnerungsintervall in der Dropdown-Liste *Benutzer erinnern* aus.

:

Wie die Erinnerung dem Benutzer dann angezeigt wird, richtet sich danach, ob der Benutzer beim Auslösen der Erinnerungsmeldung den Windows-Anmeldebildschirm geöffnet hat oder bereits in einer Windows-Sitzung arbeitet. Erinnerungen werden nicht auf Anmeldebildschirmen für die Preboot-Authentifizierung angezeigt.

Funktionsumfang während des Toleranzzeitraums

Während des angegebenen Toleranzzeitraums erhalten Benutzer bei jeder Anmeldung die Benachrichtigung „Zusätzliche Anmeldeinformationen“, wenn sie die für die neue Anmeldeoption erforderlichen Anmeldeinformationen noch nicht eingetragen haben. Die Benachrichtigung lautet: *Zusätzliche Anmeldeinformationen für die Registrierung verfügbar.*

Wenn zusätzliche Anmeldeinformationen verfügbar, aber nicht erforderlich sind, wird die Benachrichtigung nach der Änderung der Richtlinie nur ein Mal angezeigt.

Je nach Kontext geschieht Folgendes, wenn ein Benutzer auf die Benachrichtigung klickt:

Falls noch keine Anmeldeinformationen eingetragen sind, wird der Einrichtungsassistent geöffnet. Damit können administrative Benutzer computerspezifische Einstellungen ändern, und Benutzer können die üblichen Anmeldeinformationen eintragen.

Nach der ersten Registrierung von Anmeldeinformationen wird per Klick auf die Benachrichtigung der Einrichtungsassistent der DPP Security Console geöffnet.

Funktionsumfang nach Ablauf des Toleranzzeitraums

Nach Ablauf des Toleranzzeitraums können Benutzer sich nur anmelden, wenn sie die gemäß Anmeldeoption erforderlichen Anmeldeinformationen eingetragen haben. Bei Anmeldeversuchen mit einer Anmeldeinformation oder einer Kombination aus Anmeldeinformationen, die nicht der Anmeldeoption entsprechen, wird oben im Windows-Anmeldebildschirm der Einrichtungsassistent angezeigt.

Wenn der Benutzer die erforderlichen Anmeldeinformationen registriert, wird die Anmeldung bei Windows durchgeführt.

Wenn der Benutzer die erforderlichen Anmeldeinformationen nicht registriert oder den Assistenten abbricht, gelangt er automatisch zurück zum Windows-Anmeldebildschirm.

Klicken Sie zum Speichern der Einstellungen für die ausgewählte Rolle auf **Übernehmen**.

Password-Manager-Authentifizierung konfigurieren

Auf der Seite „Password-Manager“ können Sie konfigurieren, wie sich Benutzer bei Password-Manager authentifizieren.

So konfigurieren Sie die Password-Manager-Authentifizierung:

Wählen Sie im linken Fensterbereich, unter Authentifizierung, **Password-Manager** aus.

Um eine Rolle auszuwählen, die Sie einrichten möchten, wählen Sie die Rolle in der Liste **Anmeldeoptionen anwenden auf** aus: **Benutzer** oder **Administratoren**. Alle Änderungen, die Sie auf dieser Seite vornehmen, beziehen sich nur auf die von Ihnen ausgewählte Rolle.

Aktivieren Sie optional das Kontrollkästchen **Keine Authentifizierung erforderlich**, um zuzulassen, dass die ausgewählte Benutzerrolle automatisch bei allen Softwareanwendungen und Internetseiten mit den Password Manager gespeicherten Anmeldeinformationen angemeldet wird.

Legen Sie die verfügbaren Optionen für die Authentifizierung fest.

Standardmäßig ist jede Authentifizierungsmethode so konfiguriert, dass sie individuell, also nicht in Kombination mit anderen Authentifizierungsmethoden, verwendet wird. Sie können die Standardeinstellungen folgendermaßen ändern:

Um eine Kombination von Authentifizierungsoptionen einzurichten, klicken Sie unter „Verfügbare Optionen“ auf , um die erste Authentifizierungsmethode auszuwählen. Wählen Sie im Dialogfeld „Verfügbare Optionen“ die zweite Authentifizierungsmethode aus, und klicken Sie anschließend auf **OK**.

Sie können beispielsweise als Anmeldeinformationen sowohl einen Fingerabdruck, als auch ein Passwort verlangen. Wählen Sie im Dialogfeld die zweite Authentifizierungsmethode aus, die zusammen mit der Authentifizierung durch Fingerabdruck verwendet werden soll.

Um jede Authentifizierungsmethode einzeln verwenden zu können, lassen Sie im Dialogfeld „Verfügbare Optionen“ die Einstellung für die zweite Authentifizierungsmethode auf **Ohne** eingestellt und klicken Sie dann auf **OK**.

Um eine Anmeldeoption zu entfernen, klicken Sie unter „Verfügbare Optionen“ auf der Seite „Anmeldeoption“ auf das **X**, um das Verfahren zu entfernen.

Um eine neue Kombination an Authentifizierungsmethoden hinzuzufügen, klicken Sie auf **Eine Option hinzufügen**.

Um die Einstellungen für die ausgewählte Rolle zu speichern, klicken Sie auf **Übernehmen.**

: Klicken Sie auf die Standardeinstellungen-Schaltfläche, um die Standardeinstellungen wiederherzustellen.

Wiederherstellungsfragen konfigurieren

Auf der Seite „Wiederherstellungsfragen“ können Sie die Fragen auswählen, die den Benutzern präsentiert werden, wenn diese persönliche Wiederherstellungsfragen festlegen. Wiederherstellungsfragen ermöglichen es den Benutzern, Zugriff auf Ihren Computer zu erhalten, wenn sie ihr Passwort vergessen haben oder das Passwort abgelaufen ist.

Um Wiederherstellungsfragen zu konfigurieren:

Wählen Sie im linken Fensterbereich, unter Authentifizierung, **Wiederherstellungsfragen** aus.

Wählen Sie auf der Seite „Wiederherstellungsfragen“ mindestens drei vordefinierte Wiederherstellungsfragen aus.

Optional können Sie bis zu drei eigene Fragen zur Auswahlliste hinzufügen.

Klicken Sie zum Speichern der Wiederherstellungsfragen auf **Anwenden**.

Authentifizierung über Fingerabdrücke konfigurieren

So konfigurieren Sie die Authentifizierung über Fingerabdrücke:

Wählen Sie im linken Fensterbereich unter „Authentifizierung“ den Eintrag **Fingerabdrücke** aus.

Legen Sie bei „Eintragungen“ die minimale und die maximale Anzahl der Finger fest, die ein Benutzer eintragen kann.

Stellen Sie die Empfindlichkeit des Scanvorgangs für die Fingerabdrücke ein.

Durch eine geringere Empfindlichkeit wird die Abweichungstoleranz und damit die Akzeptanz eines falschen Fingerabdrucks erhöht. Bei der höchsten Einstellung besteht die Gefahr, dass legitime Fingerabdrücke abgelehnt werden. Mit der Empfindlichkeitseinstellung „Mehr“ können Sie die Quote einer fälschlichen Akzeptanz auf 1 pro 10.000 Scanvorgänge reduzieren.

Klicken Sie zum Entfernen aller Fingerabdruckscans und Registrierungen von Anmeldeinformation aus dem Speicher des Fingerabdrucklesers auf **Fingerabdruckleser löschen**. Dadurch werden nur die Daten entfernt, die Sie gerade hinzufügen. Zuvor gespeicherte Scans und Eintragungen werden nicht gelöscht.

Um die Einstellungen zu speichern, klicken Sie auf **Übernehmen**.

Einmalpasswort-Authentifizierung konfigurieren

: Für die Funktion für das Einmalpasswort (OTP) muss das TPM vorhanden, aktiviert und zugewiesen sein. Anleitungen zum Einrichten des TPM finden Sie unter Pre-Installationskonfiguration für Einmalpasswort.

Zur Verwendung der Einmalpasswort-Funktion muss der Benutzer mithilfe der Security Tools | Mobile-App auf seinem Mobilgerät ein Einmalpasswort generieren und dieses dann auf dem Computer eingeben. Das Passwort kann nur einmal verwendet werden und läuft nach einer bestimmten Gültigkeitsdauer ab.

Um die Sicherheit zusätzlich zu erhöhen, kann der Administrator die Mobilanwendung sichern, indem er die Eingabe eines Passworts konfiguriert.

Auf der Seite „Mobilgeräte“ können Sie Einstellungen zur weiteren Erhöhung der Sicherheit des Mobilgeräts und des Einmalpassworts konfigurieren.

Um die Einmalpasswort-Authentifizierung zu konfigurieren:

Wählen Sie im linken Fensterbereich unter Authentifizierung **Mobilgerät** aus.

Um beim Zugriff auf die Security Tools Mobile-App auf dem Mobilgerät ein Passwort abzufragen, wählen Sie **Password erforderlich** aus.

: Das Aktivieren der Richtlinie *Passwort erforderlich* nach der Anmeldung von mobilen Geräten auf einem Computer führt dazu, dass alle mobilen Geräten abgemeldet werden. Benutzer müssen ihre mobilen Geräte erneut eintragen, nachdem diese Richtlinie aktiviert wurde.

Wenn das Kontrollkästchen **Kennwort erforderlich** aktiviert ist, müssen Benutzer ihre mobilen Geräte für den Zugriff auf die Security Tools Mobile-App entsperren. Ist auf dem mobilen Gerät keine Gerätesperre vorhanden ist, ist die Eingabe eines Passworts erforderlich.

Um die Länge des Einmalpassworts (OTP) auszuwählen, wählen Sie für **Länge des Einmalpassworts** die Anzahl der erforderlichen Passwortzeichen aus.

Um die Anzahl der Versuche auszuwählen, die einem Benutzer zur Verfügung stehen, um das Einmalpasswort korrekt einzugeben, wählen Sie für **Anzahl der Anmeldeversuche** eine Zahl zwischen **5** und **30** aus.

Ist die Maximalzahl erreicht, wird die OTP-Funktion deaktiviert bis der Benutzer sein Mobilgerät erneut registriert hat.

: Dell empfiehlt, zusätzlich zum Einmalpasswort mindestens eine weitere Authentifizierungsmethode zu verwenden.

Smart Card-Eintragung konfigurieren

DDP|Security Tools unterstützt zwei Arten von Smart Cards: Kontakt-Karten und kontaktlose Karten.

Kontaktkarten erfordern einen Smart Card-Leser, in den die Karte eingeschoben wird. Kontaktkarten sind nur mit Domänen-Computern kompatibel. CAC- und SIPRNet-Karten sind Kontaktkarten. Aufgrund der erweiterten Funktionalität dieser Karten muss der Benutzer nach dem Einschieben der Karte ein Zertifikat auswählen.

Kontaktlose Karten werden von Nicht-Domänen-Computern und von Computern mit Domänen-Spezifikationen unterstützt.

Benutzer können als Smart Card pro Benutzerkonto eine Kontaktkarte oder mehrere kontaktlose Karten eintragen.

Smart Cards werden von der Preboot-Authentifizierung nicht unterstützt.

: Wird eine Smart Card von einem Konto entfernt, bei dem mehrere Karten eingetragen wurden, werden alle Karten gleichzeitig ausgetragen.

Um die Smart Card-Eintragung zu konfigurieren:

Wählen Sie auf der Registerkarte „Authentifizierung“ des Tools für die Administratoreinstellungen die Option **Smartcard** aus.

Erweiterte Berechtigungen konfigurieren

Zum Anpassen erweiterter Endbenutzeroptionen klicken Sie auf **Erweitert**. Unter *Erweitert* können Sie Benutzern optional die Möglichkeit geben, Anmeldeinformationen selbst einzutragen. Optional können Sie Benutzern auch die Möglichkeit geben, ihre eingetragenen Anmeldeinformationen zu ändern und die Anmeldung in einen Schritt zu aktivieren.

Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:

Eintragung von Anmeldeinformationen durch Benutzer zulassen – Dieses Kontrollkästchen ist standardmäßig aktiviert. Benutzer können ihre Anmeldeinformationen ohne Eingriff durch einen Administrator eintragen. Wenn Sie die Aktivierung des Kontrollkästchens aufheben, müssen die Anmeldeinformationen durch einen Administrator eingetragen werden.

Änderung eingetragener Anmeldeinformationen durch Benutzer zulassen – Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn diese Option markiert ist, können Benutzer ihre eingetragenen Anmeldeinformationen ohne Eingriff durch einen Administrator ändern oder löschen. Wenn Sie die Markierung des Kontrollkästchens aufheben, müssen die Anmeldeinformationen durch einen Administrator geändert oder gelöscht werden.

: Gehen Sie für das Eintragen von Anmeldeinformationen auf die Seite *Benutzer* des Tools „Administratoreinstellungen“, wählen Sie einen Benutzer aus und klicken Sie auf Eintragen.

Einstufige Anmeldung zulassen – Die einstufige Anmeldung entspricht dem Single Sign-on (SSO). Das Kontrollkästchen ist standardmäßig aktiviert. Wenn diese Funktion aktiviert ist, müssen Benutzer ihre Anmeldeinformationen nur auf dem Preboot-Authentifizierungs-Bildschirm eingeben. Die Benutzer werden automatisch bei Windows angemeldet. Wenn Sie diese Markierung entfernen, müssen sich Benutzer möglicherweise wiederholt anmelden.

: Diese Option ist nur verfügbar, wenn auch die Einstellung Benutzern die Eintragung ihrer Anmeldeinformationen erlauben ausgewählt wurde.

Klicken Sie nach Abschluss auf **Übernehmen**.

Benutzerauthentifizierung verwalten

Mithilfe der Steuerungen der Registerkarte „Authentifizierung“ in den Administratoreinstellungen können Sie Anmeldeoptionen für Benutzer festlegen und die jeweiligen Einstellungen anpassen.

Um die Benutzerauthentifizierung zu verwalten:

1 Klicken Sie als Administrator auf die Schaltfläche **Administratoreinstellungen**.

2 Klicken Sie auf **Benutzer**, um Benutzer zu verwalten und deren Eintragungsstatus anzuzeigen. Über diese Registerkarte können Sie außerdem Folgendes tun:

- Neue Benutzer eintragen
- Anmeldeinformationen hinzufügen oder ändern
- Anmeldeinformationen eines Benutzers entfernen

ANMERKUNG:
Unter **Anmeldung** und **Sitzung** werden der Eintragungsstatus eines Benutzers angezeigt.

Lautet der Status bei **Anmeldung** auf **OK**, wurden alle Eintragungen vorgenommen, die der Benutzer zum Durchführen von Anmeldungen benötigt. Lautet der Status bei **Sitzung** auf **OK**, wurden alle Eintragungen vorgenommen, die der Benutzer zum Verwenden von Password-Manager benötigt.

Lauten beide **Stati** auf **Nein**, muss der Benutzer zusätzliche Eintragungen durchführen. Um herauszufinden, welche Eintragungen noch ausstehen, wählen Sie das Tool **Administratoreinstellungen** aus, und öffnen Sie die Registerkarte **Benutzer**. Grau hinterlegte Kontrollkästchen stellen unvollständige Eintragungen dar. Kicken Sie alternativ auf die Kachel **Eintragungen**, und überprüfen Sie in der Registerkarte **Status** die Spalte **Richtlinie**, in der die erforderlichen Eintragungen aufgeführt sind.

Neue Benutzer hinzufügen

: Neue Windows-Benutzer werden automatisch hinzugefügt, wenn sie sich bei Windows anmelden oder Anmeldeinformationen registrieren.

Klicken Sie auf **Benutzer hinzufügen**, um den Eintragungsprozess für einen bereits bestehenden Windows-Benutzer zu starten.

Wählen Sie im Dialogfeld *Benutzer auswählen* die Option **Objekttypen** aus.

Geben Sie in das Textfeld den Objektnamen eines Benutzers ein, und klicken Sie auf **Namen überprüfen**.

Klicken Sie anschließend auf **OK**.

Der Eintragungsassistent wird gestartet.

Fahren Sie mit Anmelden oder Ändern der Benutzeranmeldeinformationen für weitere Anweisungen fort.

Anmelden oder Ändern der Benutzeranmeldeinformationen

Der Administrator kann zwar die Anmeldeinformationen für den Benutzer eintragen oder ändern, einige Eintragungsaktivitäten erfordern jedoch die Anwesenheit des Benutzers, z. B. die Beantwortung der Wiederherstellungsfragen oder das Scannen der Fingerabdrücke des Benutzers.

So können Sie Anmeldeinformationen von Benutzern eintragen oder ändern:

Klicken Sie in den Administratoreinstellungen auf die Registerkarte **Benutzer**.

Klicken Sie auf der Benutzer-Seite auf **Eintragen**.

Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.

Melden Sie sich im Dialogfeld „Authentifizierung erforderlich“ mit dem Windows-Passwort des Benutzers an, und klicken Sie auf **OK**.

Um das Windows-Passwort des Benutzers zu ändern, geben Sie auf der Seite „Passwort“ ein neues Passwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.

Um den Schritt der Passwort-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**.

Folgen Sie den jeweiligen Bildschirmanweisungen, und klicken Sie nach Bedarf auf die folgenden Schaltflächen: **Weiter**, **Überspringen** und **Zurück**.

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.

Weitere Informationen über das Registrieren von Anmeldeinformation oder das Ändern von Anmeldeinformationen finden Sie im *Dell Data Protection / Konsolen-Benutzerhandbuch*.

Eingetragene Anmeldeinformation entfernen

Klicken Sie auf die Kachel **Administratoreinstellungen**.

Klicken Sie auf die Registerkarte **Benutzer**, und machen Sie den Benutzer ausfindig, dessen Anmeldeinformation Sie entfernen möchten.

Fahren Sie mit der Maus über das grüne Häkchen der Anmeldeinformation, die Sie entfernen möchten. Das Symbol ändert sich in .

Klicken Sie auf das -Symbol, und klicken Sie anschließend auf **Ja**, um den Löschvorgang zu bestätigen.

: Eine Anmeldeinformation kann nicht auf diese Weise entfernt werden, wenn es sich um die einzige eingetragene Anmeldeinformation des Benutzers handelt. Auch das Passwort kann nicht mit dieser Methode entfernt werden. Verwenden Sie den Entfernen-Befehl, um den Computerzugang eines Benutzers vollständig zu entfernen.

Alle eingetragenen Eintragungen eines Benutzers entfernen

Klicken Sie auf die Kachel **Administratoreinstellungen**.

Klicken Sie auf die Registerkarte **Benutzer**, und machen Sie den Benutzer ausfindig, den Sie entfernen möchten.

Klicken Sie auf **Entfernen**. (Der Befehl „Entfernen“ wird im unteren Bereich der Benutzereinstellungen in Rot angezeigt.)

Nach dem er entfernt wurde, kann sich der Benutzer erst wieder am Computer anmelden, wenn er erneut Anmeldedaten eingetragen hat.

Deinstallation unter Verwendung des Master-Installationsprogramms

- Jede Komponente muss einzeln deinstalliert werden, gefolgt von der Deinstallation des Master-Installationsprogramms. Die Clients **müssen in einer bestimmten Reihenfolge deinstalliert werden**, um Fehler bei der Deinstallation zu vermeiden.
- Folgen Sie den Anweisungen unter Untergeordnete Installationsprogramme aus dem Master-Installationsprogramm extrahieren zum Abrufen von untergeordneten Installationsprogrammen.
- Stellen Sie sicher, dass Sie für die Deinstallation dieselbe Version des Master-Installationsprogramms (und damit der Clients) verwenden, wie bei der Installation.
- Dieses Kapitel verweist auf ein weiteres Kapitel, das *ausführliche* Informationen zum Deinstallieren der untergeordneten Installationsprogramme enthält. In diesem Kapitel wird **nur der letzte Schritt** beschrieben, die Deinstallation des Master-Installationsprogramms.

Deinstallieren Sie die Clients in der folgenden Reihenfolge.

1 Encryption-Client deinstallieren.
2 DDP | Client-Sicherheitsrahmenwerk deinstallieren.
3 Deinstallation der Erweiterten Authentifizierung (Advanced Authentication).

Das Treiberpaket muss nicht deinstalliert werden.

Fahren Sie mit Deinstallationsverfahren auswählen fort.

Deinstallationsverfahren auswählen

Es gibt zwei Methoden, um das Master-Installationsprogramm zu deinstallieren. Entscheiden Sie sich für **eine** davon:

- Über „Programme Hinzufügen/Entfernen“ deinstallieren
- Deinstallation von der Befehlszeile aus

Über „Programme Hinzufügen/Entfernen“ deinstallieren

Rufen Sie in der Windows-Systemsteuerung die Option „Programm deinstallieren“ auf. (**Start** > **Systemteuerung** > **Programme und Funktionen** > **Programm deinstallieren.**).

Markieren Sie **Dell Data Protection-Installationsprogramm**, und klicken Sie mit der linken Maustaste auf **Ändern**, um den Installationsassistenten zu starten.

Lesen Sie die Informationen im Begrüßungsbildschirm, und klicken Sie auf **Weiter**.

Folgen Sie den Eingabeaufforderungen zur Deinstallation, und klicken Sie dann auf **Fertigstellen**.

Starten Sie den Computer neu und melden Sie sich bei Windows an.

Das Master-Installationsprogramm wird deinstalliert.

Deinstallation von der Befehlszeile aus

Im folgenden Beispiel wird das Master-Installationsprogramm im Hintergrund deinstalliert.

```
"DDPSetup.exe" -y -gm2 /S /x
```

Führen Sie einen Neustart des Computers durch, wenn Sie fertig sind.

Das Master-Installationsprogramm wird deinstalliert.

Fahren Sie mit Deinstallation unter Verwendung der untergeordneten Installationsprogramme fort.

8

Deinstallation unter Verwendung der untergeordneten Installationsprogramme

- Der Benutzer, der die Entschlüsselung und Deinstallation ausführt, muss ein lokaler Administrator oder Domänenadministrator sein. Für eine Deinstallation unter Verwendung der Befehlszeile werden Domänenadministrator-Anmeldeinformationen benötigt.
- Wenn Sie die Personal Edition mit dem Master-Installationsprogramm installiert haben, müssen vor der Deinstallation zuerst die untergeordneten ausführbaren Dateien aus dem Master-Installationsprogramm extrahiert werden, wie unter Untergeordnete Installationsprogramme aus dem Master-Installationsprogramm extrahieren beschrieben.
- Stellen Sie sicher, dass Sie für die Deinstallation dieselben Client-Versionen verwenden, wie bei der Installation.
- Führen Sie die Entschlüsselung nach Möglichkeit über Nacht durch.
- Schalten Sie den Energiesparmodus aus, um zu verhindern, dass ein unbeaufsichtigter Computer in diesen Modus umschaltet. Im Energiesparmodus kann keine Entschlüsselung erfolgen.
- Schließen Sie alle Prozesse und Anwendungen, um Fehler aufgrund gesperrter Dateien zu vermeiden.

Encryption-Client deinstallieren

- **Vor der Deinstallation** finden Sie weitere Informationen unter (Optional) Encryption Removal Agent-Protokolldatei anlegen. Diese Protokolldatei erleichtert das Beheben von Fehlern, die unter Umständen beim Deinstallieren/Entschlüsseln auftreten. Falls Sie Dateien während der Deinstallation nicht entschlüsseln möchten, müssen Sie keine Encryption Removal Agent-Protokolldatei anlegen.
- Führen nach Abschluss der Deinstallation aber vor dem Neustart des Computers WSScan aus, um sicherzustellen, dass alle Daten entschlüsselt wurden. Siehe WSScan verwenden, um Anweisungen zu erhalten.
- Führen Sie gelegentlich Überprüfen des Encryption-Removal-Agent-Status durch. Die Datenentschlüsselung läuft noch, falls der Encryption Removal Agent-Dienst weiterhin im Dialogfeld „Dienste“ angezeigt wird.

Deinstallationsverfahren auswählen

Es gibt zwei Methoden, um den Encryption Client zu deinstallieren. Entscheiden Sie sich für **eine** davon:

Deinstallation mithilfe der Benutzerschnittstelle

Deinstallation von der Befehlszeile aus

Deinstallation mithilfe der Benutzerschnittstelle

Rufen Sie in der Windows-Systemsteuerung die Option „Programm deinstallieren“ auf. (**Start** > **Systemteuerung** > **Programme und Funktionen** > **Programm deinstallieren.**).

Markieren Sie **Verschlüsselung**, und klicken Sie mit der linken Maustaste auf **Ändern**, um den Installationsassistenten für Personal Edition zu starten.

Lesen Sie die Informationen im Begrüßungsbildschirm, und klicken Sie auf **Weiter**.

Wählen Sie auf dem Bildschirm „Installation von Encryption Removal Agent“ eine der beiden folgenden Optionen aus:

: Die zweite Option ist standardmäßig aktiviert. Wenn Sie Dateien entschlüsseln möchten, müssen Sie unbedingt die erste Option auswählen.

Encryption Removal Agent – Schlüssel aus Datei importieren

Bei SDE-, Benutzer- oder allgemeiner Verschlüsselung werden mit dieser Option verschlüsselte Dateien entschlüsselt, und der Encryption Client wird deinstalliert. **Dies ist die empfohlene Auswahl.**

Encryption Removal Agent nicht installieren

Mit dieser Option wird der Encryption Client deinstalliert, aber *verschlüsselte Dateien werden nicht entschlüsselt*. Diese Option sollte **nur** auf Anraten des Dell ProSupports zur Fehlerbehebung ausgewählt werden.

Klicken Sie auf **Weiter**.

Geben Sie in das Textfeld *Sicherungsdatei* den Pfad zum Netzwerklaufwerk oder Wechselspeichermedium ein, auf dem sich die Sicherungsdatei befindet, oder klicken Sie auf **...**, um zum gewünschten Speicherort zu gelangen. Die Datei hat das Format LSARecovery_[Hostname].exe.

Geben Sie Ihr Verschlüsselungs-Administratorpasswort in das Textfeld „Passwort“ ein. Hierbei handelt es sich um das während der Installation der Software im Setup-Assistenten eingerichtete Passwort.

Klicken Sie auf **Weiter**.

Im Bildschirm *Dell Decryption Agent-Dienstanmeldung* stehen zwei Optionen zur Auswahl. Wählen Sie **Lokales Systemkonto** aus. Klicken Sie auf **Fertigstellen**.

Klicken Sie auf dem Bildschirm „Programm entfernen“ auf **Entfernen**.

Klicken Sie auf dem Bildschirm „Konfiguration abgeschlossen“ auf **Fertigstellen**.

Starten Sie den Computer neu und melden Sie sich bei Windows an.

Die Entschlüsselung wird nun durchgeführt.

Die Entschlüsselung kann je nach Anzahl der verschlüsselten Laufwerke und der darauf befindlichen Daten mehrere Stunden in Anspruch nehmen. Informationen zum Überprüfen des Entschlüsselungsprozesses finden Sie unter Überprüfen des Encryption-Removal-Agent-Status.

Deinstallation von der Befehlszeile aus

Bei den Befehlszeilenschaltern und -parametern ist die Groß- und Kleinschreibung zu beachten.

Stellen Sie sicher, dass Werte, die ein oder mehrere Sonderzeichen enthalten, z. B. eine Leerstelle in der Befehlszeile, zwischen in Escape-Zeichen gesetzte Anführungszeichen gesetzt werden. Bei den Befehlszeilenparametern ist die Groß- und Kleinschreibung zu beachten.

Verwenden Sie diese Installationsprogramme zur Deinstallation der Clients. Nutzen Sie dazu eine skriptgesteuerte Installation, Batchdateien oder eine andere verfügbare Push-Technologie.

Protokolldateien

Windows erstellt für den angemeldeten Benutzer eindeutige Deinstallationsprotokolldateien des untergeordneten Installationsprogramms im Verzeichnis %temp%, unter **C:\Benutzer\<Benutzername>\AppData\Local\Temp.**

Falls Sie sich dafür entscheiden, beim Ausführen des Installationsprogramms eine separate Protokolldatei hinzuzufügen, stellen Sie sicher, dass die Protokolldatei einen eindeutigen Namen hat, da Protokolldateien des untergeordneten Installationsprogramms keine Anhänge zulassen. Mit dem standardmäßigen .msi-Befehl kann eine Protokolldatei unter Verwendung von /l **C:\<beliebiges Verzeichnis>\<beliebiger Name der Protokolldatei>.log** erstellt werden. Der Benutzername und das Passwort werden in der Protokolldatei aufgezeichnet, daher rät Dell von der Verwendung von "/l*v" (ausführliche Protokollierung) bei der Deinstallation über die Befehlszeile ab.

Für Deinstallationen über die Befehlszeile verwenden alle untergeordneten Installationsprogramme, soweit nicht anders angegeben, die gleichen grundlegenden .msi-Schalter und Anzeigeoptionen. Die Schalter müssen zuerst angegeben werden. Der /v-Schalter ist erforderlich und benötigt ein Argument. Andere Parameter gehen in ein Argument ein, das an den /v-Schalter weitergegeben wird.

Anzeigeoptionen können am Ende des Arguments angegeben werden, das an den /v-Schalter weitergegeben wird, um das erwartete Verhalten zu erzielen. Verwenden Sie /q und /qn nicht in derselben Befehlszeile. Verwenden Sie ! und - nur nach /qb.

Schalter	Erläuterung
/v	Gibt Variablen an die .msi-Datei innerhalb der setup.exe-Datei weiter
/s	Im Hintergrund
/x	Deinstallationsmodus

Option	Erläuterung
/q	Kein Fortschrittsdialogfeld, führt nach Abschluss der Installation selbstständig einen Neustart durch
/qb	Fortschrittsdialogfeld mit der Schaltfläche **Abbrechen,** fordert zum Neustart auf
/qb-	Fortschrittsdialogfeld mit der Schaltfläche **Abbrechen**, führt nach Abschluss des Vorgangs selbstständig einen Neustart durch
/qb!	Fortschrittsdialogfeld ohne die Schaltfläche **Abbrechen**, fordert zum Neustart auf
/qb!-	Fortschrittsdialogfeld ohne die Schaltfläche **Abbrechen**, führt nach Abschluss des Vorgangs selbständig einen Neustart durch
/qn	Keine Benutzeroberfläche

Nach der Extraktion aus dem Master-Installationsprogramm befindet sich das Encryption-Client-Installationsprogramm unter **C:\extracted\Encryption\DDPE_XXbit_setup.exe**.

Die folgende Tabelle umfasst die für die Deinstallation verfügbaren Parameter.

Parameter	Auswahl
CMG_DECRYPT	Eigenschaft zur Auswahl des Installationstyps des Encryption Removal Agent 2 - Schlüssel unter Verwendung eines forensischen Schlüsselpakets beziehen 0 – Encryption Removal Agent nicht installieren
CMGSILENTMODE	Eigenschaft für Deinstallation im Hintergrund: 1 – Im Hintergrund 0 – Nicht im Hintergrund
DA_KM_PW	Das Passwort für das Konto „Domänenadministrator“.
DA_KM_PATH	Pfad zum Schlüsselmaterialpaket.

Im folgenden Beispiel wird der Verschlüsselungs-Client deinstalliert, ohne dass zuvor der Encryption Removal Agent installiert wurde.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1 DA_KM_PATH=C:\FullPathToLSA.exe
DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

Im folgenden Beispiel wird der Verschlüsselungs-Client unter Verwendung eines forensischen Schlüsselpakets deinstalliert. Kopieren Sie das forensische Schlüsselpaket auf den lokalen Datenträger und führen Sie anschließend diesen Befehl aus.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1 DA_KM_PATH=C:
\FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

Führen Sie einen Neustart des Computers durch, wenn Sie fertig sind.

Die Entschlüsselung kann je nach Anzahl der verschlüsselten Laufwerke und der darauf befindlichen Daten mehrere Stunden in Anspruch nehmen. Informationen zum Überprüfen des Entschlüsselungsprozesses finden Sie unter Überprüfen des Encryption-Removal-Agent-Status.

Deinstallation der Erweiterten Authentifizierung (Advanced Authentication)

Deinstallationsverfahren auswählen

Es gibt zwei Methoden, um den Encryption Client zu deinstallieren. Entscheiden Sie sich für **eine** davon:

Deinstallation mithilfe der Benutzerschnittstelle

Deinstallation von der Befehlszeile aus

Deinstallation mithilfe der Benutzerschnittstelle

1. Rufen Sie in der Windows-Systemsteuerung die Option „Programm deinstallieren“ auf. (**Start** > **Systemteuerung** > **Programme und Funktionen** > **Programm deinstallieren.**).
2. Markieren Sie **Security Tools-Authentifizierung** und klicken Sie mit der linken Maustaste auf **Ändern**, um den Installationsassistenten zu starten.
3. Lesen Sie die Informationen im Begrüßungsbildschirm, und klicken Sie auf **Weiter**.
4. Geben Sie das Administrator-Kennwort ein.
5. Folgen Sie den Eingabeaufforderungen zur Deinstallation, und klicken Sie dann auf **Fertigstellen**.
6. Starten Sie den Computer neu und melden Sie sich bei Windows an.

Security Tools-Authentifizierung ist deinstalliert.

Deinstallation von der Befehlszeile aus

1. Nach der Extraktion aus dem Master-Installationsprogramm befindet sich das Advanced Authentication-Client-Installationsprogramm unter C:\extracted\Security Tools\Authentication\<x64/x86>\setup.exe.
2. Im folgenden Beispiel wird der Advanced Authentication-Client im Hintergrund deinstalliert.

```
setup.exe /x /s /v" /qn"
```

3. Wenn Sie fertig sind, fahren Sie den Computer herunter und starten Sie ihn neu.

Fahren Sie mit Beschreibungen von Richtlinien und Vorlagen fort.

Deinstallieren des Client Security Framework

Deinstallationsverfahren auswählen

Es gibt zwei Methoden, um den Encryption Client zu deinstallieren. Entscheiden Sie sich für **eine** davon:

Deinstallation mithilfe der Benutzerschnittstelle

Deinstallation von der Befehlszeile aus

Deinstallation mithilfe der Benutzerschnittstelle

1. Rufen Sie in der Windows-Systemsteuerung die Option „Programm deinstallieren“ auf. (**Start** > **Systemteuerung** > **Programme und Funktionen** > **Programm deinstallieren.**).
2. Markieren Sie **Client Security Framework** und klicken Sie mit der linken Maustaste auf **Ändern**, um den Installationsassistenten zu starten.

Lesen Sie die Informationen im Begrüßungsbildschirm, und klicken Sie auf **Weiter**.

Folgen Sie den Eingabeaufforderungen zur Deinstallation, und klicken Sie dann auf **Fertigstellen**.

Starten Sie den Computer neu und melden Sie sich bei Windows an.

Client-Sicherheits-Framework wurde deinstalliert.

Deinstallation von der Befehlszeile aus

Nach der Extraktion aus dem Master-Installationsprogramm befindet sich das Client-Sicherheits-Framework-Client-Installationsprogramm unter C:\extracted\Security Tools\EMAgent_.

Im folgenden Beispiel wird der SED-Client im Hintergrund deinstalliert.

```
EMAgent_XXbit_setup.exe /x /s /v" /qn"
```

Wenn Sie fertig sind, fahren Sie den Computer herunter und starten Sie ihn neu.

Beschreibungen von Richtlinien und Vorlagen

Die QuickInfos werden angezeigt, wenn Sie in der Local Management Console die Maus über einer Richtlinie ruhen lassen.

Richtlinien

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
Richtlinien für Festspeicher										
SDE-Verschlüsselung aktiviert	Wahr								Falsch	Diese Richtlinie ist die „Master-Richtlinie“ für alle weiteren System Data Encryption (SDE)-Richtlinien. Wenn für diese Richtlinie „Falsch“ ausgewählt wurde, erfolgt keine SDE-Verschlüsselung, unabhängig von anderen Richtlinienwerten. Der Wert „Wahr“ bedeutet, dass alle Daten, die nicht durch andere intelligente Verschlüsselungsrichtlinien verschlüsselt sind, über die SDE-Verschlüsselungsregeln verschlüsselt werden. Wird der Wert dieser Richtlinie geändert, muss ein Neustart durchgeführt werden.
SDE-Verschlüsselungsalgorithmus	AES256									AES 256, AES 128, 3DES
SDE-Verschlüsselungsregeln										Verschlüsselungsregeln, die bei der Verschlüsselung bzw. beim Ausschluss der Verschlüsselung bestimmter

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										Laufwerke, Verzeichnisse und Ordner verwendet werden. Wenden Sie sich an den Dell ProSupport, wenn Sie nicht sicher sind, ob Sie die Standardwerte ändern können.
Richtlinien für allgemeine Einstellungen										
Verschlüsselung aktiviert	Wahr							Falsch		Diese Richtlinie ist die „Master-Richtlinie“ für alle Richtlinien für allgemeine Einstellungen. Wenn der Wert „Falsch“ eingestellt wurde, erfolgt keine Verschlüsselung, unabhängig von anderen Richtlinienwerten. Wenn „Wahr“ ausgewählt wurde, sind alle Verschlüsselungsrichtlinien aktiviert. Bei einer Änderung dieses Richtlinienwerts wird ein neuer Suchvorgang nach zu ver-/entschlüsselnden Dateien durchgeführt.
Allgemein verschlüsselte Ordner										Zeichen: maximal 100 Einträge mit je 500 Zeichen (bis zu maximal 2048 Zeichen) Eine Liste von Ordnern auf Endpunktlaufwerken, die verschlüsselt oder von der Verschlüsselung ausgeschlossen werden sollen und dann für alle verwalteten Benutzer zugänglich sind, die Zugriff auf den Endpunkt haben. Die verfügbaren Laufwerksbuchstaben heißen: #: bezieht sich auf alle Laufwerke f#: Bezieht sich auf alle Festplattenlaufwerke

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										#: bezieht sich auf alle Wechseldatenträger Wichtiger Hinweis: Die Aufhebung des Verzeichnisschutzes kann dazu führen, dass Ihr Computer möglicherweise nicht mehr gestartet werden kann und/oder Laufwerke neu formatiert werden müssen. Wenn für ein und denselben Ordner diese Richtlinie und die Richtlinie „Benutzerverschlüsselte Ordner“ festgelegt ist, hat diese Richtlinie Vorrang.
Allgemeiner Verschlüsselungsalgorithmus	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES Systemauslagerungsdateien werden mit AES 128 verschlüsselt.
Anwendungsdaten-Verschlüsselungsliste	winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe notepad.exe wordpad.exe winzip.exe winrar.exe									Zeichen: maximal 100 Einträge mit je 500 Zeichen Dell rät davon ab, explorer.exe oder iexplorer.exe zur ADE-Liste hinzuzufügen, da dies zu unerwarteten oder unbeabsichtigten Ergebnissen führen kann. Allerdings kann mit explorer.exe über das Kontextmenü auf dem Desktop eine neue Editor-Datei erstellt werden. Wird die Verschlüsselung anhand der Dateierweiterung anstelle der ADE-Liste festgelegt, erhält man eine umfassendere Abdeckung. Listet Prozessnamen von Anwendungen auf (ohne Pfade), deren neue Daten Sie verschlüsseln möchten, getrennt durch Wagenrückläufe. Verwenden Sie keine Platzhalter.

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
	onenote.exe onenotem.exe									Dell empfiehlt, keine Anwendungen oder Installationsprogramme aufzuführen, die systemkritische Dateien schreiben. da es andernfalls zur Verschlüsselung von wichtigen Systemdateien kommen würde. Möglicherweise könnte der Computer dann nicht mehr gestartet werden. Gängige Prozessnamen: outlook.exe, winword.exe, frontpg.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe Folgende fest codierte Namen von System- und Installationsprozessen werden ignoriert, falls sie in dieser Richtlinie festgelegt sind: hotfix.exe, update.exe, setup.exe, msiexec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe
Anwendungsdaten-Verschlüsselungsschlüssel	Allgemein									Gemeinsam oder Benutzer Wählen Sie einen Schlüssel aus, um anzugeben, wer wo Zugriff auf Dateien haben soll, die durch die Anwendungsdaten-Verschlüsselungsliste verschlüsselt sind. „Allgemein“, falls diese Dateien für alle verwalteten Benutzer auf dem Endpunkt, auf dem sie erstellt wurden, zugänglich sein (gleiche Zugriffsstufe wie allgemein verschlüsselte Ordner) und mit dem allgemeinen Verschlüsselungsalgorithmus verschlüsselt werden sollen.

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										„Benutzer“, falls diese Dateien nur für den Benutzer, der sie erstellt hat, auf dem Endpunkt, auf dem sie erstellt wurden, zugänglich sein (gleiche Zugriffsstufe wie benutzerverschlüsselte Ordner) und mit dem Benutzerverschlüsselungsalgorithmus verschlüsselt werden sollen. Änderungen an dieser Richtlinie betreffen keine Dateien, die bereits aufgrund dieser Richtlinie verschlüsselt sind.
Persönliche Outlook-Ordner verschlüsseln	Wahr							Falsch		Mit „Wahr“ werden persönliche Outlook-Ordner verschlüsselt.
Temporäre Dateien verschlüsseln	Wahr							Falsch		Mit „Wahr“ werden die Pfade in den Umgebungsvariablen TEMP und TMP mit dem Benutzerdaten-Verschlüsselungsschlüssel verschlüsselt.
temporäre Internetdateien verschlüsseln	Wahr	Falsch								Mit „Wahr“ werden die Pfade in der Umgebungsvariablen CSIDL_INTERNET_CACHE mit dem Benutzerdaten-Verschlüsselungsschlüssel verschlüsselt. Zur Beschleunigung der Verschlüsselungssuche löscht der Client den Inhalt von CSIDL_INTERNET_CACHE für die erste Verschlüsselung sowie für Aktualisierungen dieser Richtlinie. Diese Richtlinie ist nur dann gültig, wenn der Microsoft Internet Explorer verwendet wird.

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
Benutzerprofildokumente verschlüsseln	Wahr								Falsch	Mit „Wahr“ wird Folgendes verschlüsselt: · Das Benutzerprofil (**C:\Users\jsmith**) mit dem Benutzerdaten-Verschlüsselungsschlüssel · \Users\Public mit dem allgemeinen Verschlüsselungsschlüssel
Windows-Auslagerungsdatei verschlüsseln	Wahr								Falsch	Mit „Wahr“ wird die Windows-Auslagerungsdatei verschlüsselt. Nach Änderung dieser Richtlinie ist ein Neustart erforderlich.
Verwaltete Dienste										Zeichen: maximal 100 Einträge mit je 500 Zeichen (bis zu maximal 2048 Zeichen) Wird ein Dienst durch diese Richtlinie verwaltet, wird der Dienst erst gestartet, nachdem der Benutzer angemeldet und der Client entsperrt ist. Diese Richtlinie stellt außerdem sicher, dass der durch diese Richtlinie verwaltete Dienst beendet wird, bevor der Client bei der Abmeldung gesperrt wird. Diese Richtlinie kann auch die Abmeldung eines Benutzers verhindern, wenn ein Dienst nicht antwortet. Die Syntax verlangt einen Dienstnamen pro Zeile. Leerstellen im Dienstnamen werden unterstützt. Platzhalter werden nicht unterstützt. Verwaltete Dienste werden nicht gestartet, wenn sich ein nicht verwalteter Benutzer anmeldet.

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
Sichere Bereinigung nach Verschlüsselung	Dreifaches Überschreiben	Einfaches Überschreiben							Kein Überschreiben	Kein Überschreiben, Einfaches Überschreiben, Dreifaches Überschreiben, Siebenfaches Überschreiben Sobald Ordner, die mit anderen Richtlinien in dieser Kategorie festgelegt wurden, verschlüsselt sind, bestimmt diese Richtlinie, was mit den restlichen unverschlüsselten Dateien geschieht: · Mit „Kein Überschreiben“ werden sie gelöscht. Dieser Wert bietet die schnellste Verschlüsselung. · Mit „Einfaches Überschreiben“ werden sie mit Zufallsdaten überschrieben. · Mit „Dreifaches Überschreiben“ werden sie mit einem Standardmuster aus 1 und 0 überschrieben, anschließend mit dem genauen Gegenstück und schließlich mit einer Folge von Zufallsdaten. · Mit „Siebenfaches Überschreiben“ werden sie mit einem Standardmuster aus 1 und 0 überschrieben, anschließend mit dem genauen Gegenstück und schließlich fünfmal mit einer Folge von Zufallsdaten. Mit diesem Wert ist es am schwierigsten, die Originaldateien aus dem Speicher wiederherzustellen. Dies ist also die sicherste Verschlüsselung.
Sichere Windows-Ruhezustand-Datei	Wahr					Falsch		Wahr	Falsch	Bei Aktivierung wird die Ruhezustandsdatei nur verschlüsselt, wenn der Computer in den Ruhezustand schaltet. Der Client setzt den Schutz aus, wenn der Computer den Ruhezustand

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										verlässt. So ergibt sich ein Schutz ohne Beeinträchtigung von Benutzern oder Anwendungen, solange der Computer genutzt wird.
Ungeschützten Ruhezustand unterbinden	Wahr					Falsch		Wahr	Falsch	Wenn dies aktiviert ist, erlaubt der Client dem Computer nicht, in den Ruhezustand zu wechseln, wenn der Client die Ruhezustandsdaten nicht verschlüsseln kann.
Workstation-Suchpriorität	Hoch	Normal								Höchste, Hoch, Normal, Niedrig, Niedrigste Legt die relative Windows-Priorität beim Durchsuchen von verschlüsselten Ordnern fest.
Benutzerverschlüsselte Ordner										Zeichen: maximal 100 Einträge mit je 500 Zeichen (bis zu maximal 2048 Zeichen) Eine Liste der Ordner auf der Endpunktfestplatte, die mit dem Benutzerdaten-Verschlüsselungsschlüssel verschlüsselt oder von der Verschlüsselung ausgeschlossen werden sollen. Diese Richtlinie gilt für alle Laufwerke, die von Windows als Festplattenlaufwerke eingeordnet werden. Sie können diese Richtlinie nicht zur Verschlüsselung von Laufwerken oder externen Medien verwenden, die als „Wechseldatenträger“ deklariert sind. Verwenden Sie dafür stattdessen „EMS-Verschlüsselung externer Medien“.
Benutzer-Verschlüsselungsalgorithmus	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES Verschlüsselungsalgorithmus, der für die Verschlüsselung

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										von Daten auf der Ebene des einzelnen Benutzers verwendet wird. Sie können gleichzeitig verschiedene Werte für verschiedene Benutzer desselben Endpunkts festlegen.
Benutzerdaten-Verschlüsselungsschlüssel	Benutzer	Allgemein		Benutzer	Allgemein				Benutzer	Gemeinsam oder Benutzer Wählen Sie einen Schlüssel aus, um anzugeben, wer wo Zugriff auf Dateien haben soll, die durch die folgenden Richtlinien verschlüsselt sind: · Benutzerverschlüsselte Ordner · Persönliche Outlook-Ordner verschlüsseln · Temporäre Dateien verschlüsseln (nur \Dokumente und Einstellungen \Benutzername\Lokale Einstellungen\Temp) · Temporäre Internetdateien verschlüsseln · Benutzerprofildokumente verschlüsseln Wählen Sie: · „Allgemein“, falls benutzerverschlüsselte Dateien/Ordner für alle verwalteten Benutzer auf dem Endpunkt, auf dem sie erstellt wurden, zugänglich sein (gleiche Zugriffsstufe wie allgemein verschlüsselte Ordner) und mit dem allgemeinen Verschlüsselungsalgorithmus verschlüsselt werden sollen. · „Benutzer“, falls diese Dateien nur für den Benutzer, der sie erstellt hat, auf dem Endpunkt, auf dem sie erstellt

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										wurden, zugänglich sein (gleiche Zugriffsstufe wie benutzerverschlüsselte Ordner) und mit dem Benutzerverschlüsselungsalgorithmus verschlüsselt werden sollen. Wenn Sie sich für die Aufnahme einer Verschlüsselungsrichtlinie entscheiden, die ganze Festplattenpartitionen verschlüsselt, wird empfohlen, dass Sie anstelle von „Allgemein“ oder „Benutzer“ die Standard-SDE-Verschlüsselungsrichtlinie verwenden. Dadurch wird sichergestellt, dass alle verschlüsselten Betriebssystemdateien auch dann zugänglich sind, wenn der verwaltete Benutzer nicht angemeldet ist.
Hardware Crypto Accelerator (Unterstützung nur für Clients mit Verschlüsselung Ver. 8.3 bis Ver. 8.9.1)										
Hardware Crypto Accelerator (HCA)	Falsch									Diese „Master-Richtlinie“ gilt für alle Hardware Crypto Accelerator (HCA)-Richtlinien. Wenn für diese Richtlinie „Falsch“ ausgewählt wurde, erfolgt keine HCA-Verschlüsselung, unabhängig von anderen Richtlinienwerten. HCA-Richtlinien können nur auf Computern mit Hardware Crypto Accelerator verwendet werden.
Zur Verschlüsselung vorgesehene Datenträger	Alle Festplatten									Alle Festplatten oder nur Systemdatenträger Geben Sie an, welche(n) Datenträger Sie verschlüsseln möchten.
Forensische Metadaten verfügbar	Falsch									Wahr oder Falsch

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
auf mit HCA verschlüsseltem Laufwerk										Wenn „Wahr“ eingestellt ist, werden auf dem Laufwerk forensische Metadaten mit einbezogen, um die Forensik zu vereinfachen. Dazu zählen die folgenden Metadaten: • Geräte-ID (MCID) des aktuellen Computers • Geräte-ID (DCID/SCID) der aktuellen Shield-Installation Wenn „Falsch“ eingestellt ist, werden auf dem Laufwerk keine forensischen Metadaten mit einbezogen. Beim Umschalten von „Falsch“ auf „Wahr“ wird die Suche nach forensischen Daten auf Grundlage der HCA-Richtlinien zum Hinzufügen forensischer Daten wiederholt.
Benutzergenehmigung der Verschlüsselung sekundärer Laufwerke zulassen	Falsch									Bei „Wahr“ kann der Benutzer entscheiden, ob zusätzliche Laufwerke verschlüsselt werden.
Verschlüsselungsalgorithmus	AES256									AES 256 oder AES 128
Richtlinien für Port Control										
Port Control System	Deaktiviert									Alle Richtlinien für Port Control System aktivieren oder deaktivieren. Wenn diese Richtlinie auf Deaktivieren eingestellt ist, werden unabhängig von anderen Richtlinien für das Port Control System keine Richtlinien für das Port Control System angewendet.

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										Anmerkung: Für PCS-Richtlinien ist ein Neustart erforderlich, damit die entsprechende Richtlinie wirksam wird.
Port: Express-Card-Steckplatz	Aktiviert									Aktivieren, deaktivieren oder umgehen Sie die über den Express-Card-Steckplatz zugänglichen Ports.
Port: eSATA	Aktiviert									Aktivieren, deaktivieren oder umgehen Sie den Portzugriff auf externe SATA-Ports.
Port: PCMCIA	Aktiviert									Aktivieren, deaktivieren oder umgehen Sie den Portzugriff auf externe PCMCIA-Ports.
Port: Firewire (1394)	Aktiviert									Aktivieren, deaktivieren oder umgehen Sie den Portzugriff auf externe Firewire-Ports (1394).
Port: SD	Aktiviert									Aktivieren, deaktivieren oder umgehen Sie den Portzugriff auf SD-Karten-Ports.
Unterklasse Speicher: Steuerung externer Laufwerke	Gesperrt	Schreibgeschützt			Vollständiger Zugriff			Schreibgeschützt	Vollständiger Zugriff	UNTERGEORDNETES ELEMENT von Klasse: Speicher. Klasse: Speicher muss aktiviert sein, damit diese Richtlinie verwendet werden kann. Diese Richtlinie interagiert mit PCS. Siehe EMS und PCS Interaktionen. Vollständiger Zugriff: Der Port des externen Laufwerks ist weder lese- noch schreibgeschützt. Schreibgeschützt: Gewährt Lesezugriff. Die Daten sind schreibgeschützt Gesperrt: Der Lese- und Schreibzugriff auf den Port ist gesperrt

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										Diese Richtlinie ist endpunktbasiert und kann durch die Benutzerrichtlinie nicht außer Kraft gesetzt werden.
Port: Memory Transfer Device (MTD)	Aktiviert									Aktivieren, deaktivieren oder umgehen Sie den Zugriff auf MTD-Ports (Memory Transfer Device).
Klasse: Speicher	Aktiviert									ÜBERGEORDNETES ELEMENT für die nächsten drei Richtlinien. Stellen Sie diese Richtlinie auf „Aktiviert“ ein, um die nächsten drei Unterklassenrichtlinien für Speicher zu verwenden. Wenn diese Richtlinie auf „Deaktiviert“ eingestellt ist, werden alle drei Unterklassenrichtlinien für Speicher – unabhängig von ihrem Wert – ebenfalls deaktiviert.
Unterklasse Speicher: Steuerung optischer Laufwerke	Schreibgeschützt	Nur UDF				Vollständiger Zugriff		Nur UDF	Vollständiger Zugriff	UNTERGEORDNETES ELEMENT von Klasse: Speicher. Klasse: Speicher muss aktiviert sein, damit diese Richtlinie verwendet werden kann. Vollständiger Zugriff: Der Port des optischen Laufwerks ist weder lese- noch schreibgeschützt. Nur UDF: Schreibvorgänge, die nicht im UDF-Format erfolgen (Brennen von CD/DVD, Brennen im ISO-Format), werden gesperrt. Der Lesezugriff ist aktiviert. Schreibgeschützt: Gewährt Lesezugriff. Die Daten sind schreibgeschützt

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										Gesperrt: Der Lese- und Schreibzugriff auf den Port ist gesperrt Diese Richtlinie ist endpunktbasiert und kann durch die Benutzerrichtlinie nicht außer Kraft gesetzt werden. Universal Disk Format (UDF) ist eine Implementierung von ISO/IEC 13346 und ECMA-167 und ein offenes, anbieterunabhängiges Dateisystem zum Speichern von Computerdaten auf einer Vielzahl von Medien. Diese Richtlinie interagiert mit PCS. Siehe EMS und PCS Interaktionen.
Unterklasse Speicher: Steuerung von Diskettenlaufwerken	Gesperrt	Schreibgeschützt				Vollständiger Zugriff		Schreibgeschützt	Vollständiger Zugriff	UNTERGEORDNETES ELEMENT von Klasse: Speicher. Klasse: Speicher muss aktiviert sein, damit diese Richtlinie verwendet werden kann. Vollständiger Zugriff: Der Port des Diskettenlaufwerks ist weder lese- noch schreibgeschützt. Schreibgeschützt: Gewährt Lesezugriff. Die Daten sind schreibgeschützt Gesperrt: Der Lese- und Schreibzugriff auf den Port ist gesperrt Diese Richtlinie ist endpunktbasiert und kann durch die Benutzerrichtlinie nicht außer Kraft gesetzt werden.
Klasse: Tragbares Windows-	Aktiviert									ÜBERGEORDNETES ELEMENT für die nächste Richtlinie. Stellen Sie diese

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
Gerät (Windows Portable Device, WPD)										Richtlinie auf „Aktiviert“ ein, um die Unterklassenrichtlinie „Tragbares Windows-Gerät (Windows Portable Device, WPD): Speicher“ zu verwenden. Wenn diese Richtlinie auf „Deaktiviert“ eingestellt ist, wird die Unterklassenrichtlinie „Tragbares Windows-Gerät (Windows Portable Device, WPD): Speicher“ – unabhängig von ihrem Wert – ebenfalls deaktiviert. Steuern Sie den Zugriff auf alle tragbaren Windows-Geräte.
Unterklasse: Tragbares Windows-Gerät (Windows Portable Device, WPD): Speicher	Aktiviert									UNTERGEORDNETES ELEMENT von Klasse: Tragbares Windows-Gerät (Windows Portable Device, WPD). Klasse: Tragbares Windows-Gerät (Windows Portable Device, WPD) muss auf „Aktiviert“ eingestellt sein, um diese Richtlinie verwenden zu können. Vollständiger Zugriff: Der Port ist weder lese- noch schreibgeschützt. Schreibgeschützt: Gewährt Lesezugriff. Die Daten sind schreibgeschützt Gesperrt: Der Lese- und Schreibzugriff auf den Port ist gesperrt
Klasse: Eingabegerät (Human Interface Device, HID)	Aktiviert									Steuern Sie den Zugriff auf alle Eingabegeräte (Tastaturen, Mäuse). **Anmerkung**: Die Sperrung von USB-Ports und auf HID-Klassenebene wird nur dann beibehalten, wenn der Computer anhand seines

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										Gehäuses als Laptop/ Notebook erkannt wurde. Zur Identifizierung des Gehäuses wird auf das BIOS des Computers zurückgegriffen.
Klasse: Sonstige	Aktiviert									Steuern Sie den Zugriff auf alle Geräte, die keiner anderen Klasse zugeordnet sind.
Richtlinien für Wechselspeichermedien										
EMS-Verschlüsselung externer Medien	Wahr					Falsch		Wahr	Falsch	Diese Richtlinie ist die „Master-Richtlinie“ für alle Richtlinien für Wechselspeichermedien. Wenn der Wert „Falsch“ ausgewählt wurde, erfolgt keine Verschlüsselung von Wechselspeichermedien, unabhängig von anderen Richtlinienwerten. Wenn der Wert „Wahr“ ausgewählt wurde, sind alle Verschlüsselungsrichtlinien für Wechselspeichermedien aktiviert. Diese Richtlinie interagiert mit PCS. Siehe EMS und PCS Interaktionen.
EMS CD/ DVD-Verschlüsselung ausschließen	Falsch								Wahr	Mit „Falsch“ werden CD/DVD-Geräte verschlüsselt. Diese Richtlinie interagiert mit PCS. Siehe EMS und PCS Interaktionen.
EMS-Zugriff auf nicht durch Shield geschützte Medien	Blockieren	Schreibgeschützt				Vollständiger Zugriff		Schreibgeschützt	Vollständiger Zugriff	Sperren, Schreibgeschützt, Vollständiger Zugriff Diese Richtlinie interagiert mit PCS. Siehe EMS und PCS Interaktionen. Wenn diese Richtlinie so eingestellt ist, dass der Zugriff gesperrt wird, haben Sie nur dann Zugriff auf

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										Wechselspeichermedien, wenn sie verschlüsselt sind. Wenn Sie entweder „Schreibgeschützt“ oder „Vollständiger Zugriff“ auswählen, können Sie entscheiden, welche Wechselspeichermedien verschlüsselt werden sollen. Wenn Sie Wechselspeichermedien nicht verschlüsseln möchten und diese Richtlinie auf „Voller Zugriff“ eingestellt ist, erhalten Sie vollen Lese-/Schreibzugriff auf Wechselspeichermedien. Wenn Sie Wechselspeicher nicht verschlüsseln lassen und diese Richtlinie auf „Schreibgeschützt“ eingestellt ist, können Sie vorhandene Dateien auf dem unverschlüsselten Wechselspeicher nicht lesen oder löschen. Der Client verhindert, dass Dateien auf dem Wechselspeicher bearbeitet oder hinzugefügt werden, wenn dieser nicht verschlüsselt ist.
EMS-Verschlüsselungsalgorithmus	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES
EMS-Suchvorgang für externe Medien	Wahr	Falsch								Mit „Wahr“ werden EMS-Wechselspeichermedien bei jeder Nutzung durchsucht. Wenn diese Richtlinie auf „Falsch“ und die Richtlinie „EMS-Verschlüsselung externer Medien“ auf „Wahr“ eingestellt ist, verschlüsselt EMS nur neue und geänderte Dateien.

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										Ein Suchvorgang findet bei jedem Anschluss statt, so dass EMS alle Dateien erkennt, die ohne Authentifizierung zum Wechselspeicherdatenträger hinzugefügt wurden. Wenn Sie die Authentifizierung ablehnen, können Sie Dateien zum Wechselspeichermedium hinzufügen, aber nicht auf verschlüsselte Daten zugreifen. Die hinzugefügten Dateien werden in diesem Fall nicht verschlüsselt. Wenn Sie sich das nächste Mal beim Wechselspeichermedium für die Arbeit mit verschlüsselten Daten authentifizieren, durchsucht EMS das Medium und verschlüsselt alle Dateien, die ohne Verschlüsselung hinzugefügt wurden.
EMS-Zugriff auf einem nicht durch Shield geschützten Gerät	Wahr									„Wahr“ ermöglicht dem Benutzer den Zugriff auf verschlüsselte Daten auf Wechselspeichermedien, unabhängig davon, ob der Endpunkt durch Shield geschützt ist.
EMS-Gerät – Positivliste										Diese Richtlinie ermöglicht die Angabe von externen Mediengeräten, die von der EMS-Verschlüsselung ausgeschlossen werden sollen. Externe Datenträger, die nicht auf der Liste stehen, werden geschützt. Maximal 150 Geräte mit maximal 500 Zeichen pro PNPDeviceID. Maximal 2048 Zeichen insgesamt. So finden Sie die PNP-Gerätekennung für Wechselspeichermedien: 1 Setzen Sie das Wechselspeichergerät in einen Shield-geschützten Computer ein.

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung

2 Öffnen Sie das EMSService.log in C:\Programdata\Dell\Dell Data Protection\Encryption\EMS.

3 So finden Sie "PNPDeviceID="

Zum Beispiel: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0

Geben Sie Folgendes in der Richtlinie für EMS-Gerät – Positivliste an:

VEN=Vendor (z. B.: USBSTOR\DISK&VEN_SEAGATE)

PROD=Produkt-/Modellname (z. B.: &PROD_USB); Von der EMS-Verschlüsselung werden außerdem alle USB-Laufwerke von Seagate ausgeschlossen; ein VEN-Wert (z. B.: USBSTOR\DISK&VEN_SEAGATE) muss diesem Wert vorangehen

Rev=Firmware-Version (Bsp: &REV_0409); das verwendete Modell wird außerdem ausgeschlossen; VEN- und PROD-Werte müssen diesem Wert vorangehen

Seriennummer (z. B.: \ 2HC015KJ& 0); schließt nur dieses Gerät aus; VEN-, PROD- und REV-Werte müssen diesem Wert vorangehen

Zulässige Begrenzungszeichen: Tabulator, Komma, Semikolon, hexadezimales Zeichen 0x1E (Datensatztrennzeichen)

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
Alphabetische Zeichen im EMS-Passwort erforderlich	Wahr									Mit Wahr muss das Passwort mindestens einen Buchstaben enthalten.
Gemischte Groß-/Kleinbuchstaben im EMS-Passwort erforderlich	Wahr	Falsch								Mit „Wahr“ muss das Passwort mindestens einen Groß- und einen Kleinbuchstaben enthalten.
Erforderliche Anzahl Zeichen im EMS-Passwort	8					6		8		1-40 Zeichen Mindestzahl der im Passwort erforderlichen Zeichen.
Numerische Zeichen im EMS-Passwort erforderlich	Wahr	Falsch								Mit Wahr muss das Passwort mindestens ein numerisches Zeichen enthalten.
Zulässige EMS-Passwortversuche	2	3				4		3		1-10 Anzahl der Versuche, die ein Benutzer für die Eingabe des richtigen Passworts hat.
Sonderzeichen im EMS-Passwort erforderlich	Wahr	Falsch							Wahr	Mit „Wahr“ muss das Passwort mindestens ein Sonderzeichen enthalten.
EMS-Cooldown – Zeitverzögerung	30									0–5000 Sekunden Anzahl der Sekunden, die der Benutzer zwischen der ersten und zweiten Runde an Versuchen zur Eingabe des Zugriffscodes warten muss.
EMS-Cooldown-Verzögerung	30	20				10	30	10		0–5000 Sekunden Zusätzliche Zeit, die nach jeder fehlgeschlagenen Runde von Eintragsversuchen für den

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										Zugriffscode zur vorherigen Cooldown-Zeit addiert wird.
EMS-Verschlüsselungsregeln										Verschlüsselungsregeln für die Verschlüsselung bzw. den Ausschluss der Verschlüsselung von bestimmten Laufwerken, Verzeichnissen und Ordnern. Insgesamt sind 2.048 Zeichen zulässig. Für das Hinzufügen von Leerzeilen verwendete Leerzeichen und Eingabezeichen werden bei der Zeichenanzahl mitgezählt. Alles, was über die 2.048 Zeichen hinausgeht, wird ignoriert. Bei Speichergeräten, die mehrere Schnittstellen anbieten, z. B. Firewire, USB, eSATA usw., kann es zur Verschlüsselung des Geräts notwendig sein, sowohl EMS als auch Verschlüsselungsregeln anzuwenden. Das liegt daran, dass das Betriebssystem Windows Speichergeräte ausgehend von deren Schnittstellentyp unterschiedlich behandelt. Siehe Vorgehensweise bei der EMS-Verschlüsselung eines iPods.
EMS-Zugriff auf nicht durch Shield geschützte Medien sperren	Wahr								Falsch	Sperrt den Zugriff auf alle Wechselspeichermedien, die weniger als 17 MB Speicher und damit nicht genügend Kapazität für Wechselspeichermedien-Shield bieten (z. B. eine Diskette mit 1,44 MB). Der gesamte Zugriff wird gesperrt, wenn die Richtlinie „Externe Medien verschlüsseln“ und diese Richtlinie beide auf „Wahr“

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
										eingestellt sind. Ist die Richtlinie „Externe Medien verschlüsseln“ auf „Wahr“, diese Richtlinie jedoch auf „Falsch“ eingestellt, können Daten von nicht verschlüsselbaren Wechselspeichermedien zwar gelesen werden, doch der Schreibzugriff auf das Medium ist gesperrt. Ist die Richtlinie „Externe Medien verschlüsseln“ auf „Falsch“ eingestellt, hat diese Richtlinie keine Auswirkungen, und der Zugriff auf nicht verschlüsselbare Wechselspeichermedien ist nicht beeinträchtigt.
Richtlinien zur Steuerung der Benutzerfreundlichkeit										
Neustart bei Aktualisierung erzwingen	Wahr								Falsch	Wird der Wert auf Wahr gestellt, erfolgt sofort ein Neustart des Computers, um die Bearbeitung der Verschlüsselung oder Aktualisierungen im Zusammenhang mit der gerätebezogenen Richtlinie, z. B. Systemdatenverschlüsselung, zuzulassen.
Länge der Verzögerung beim Neustart	5	10				20		15		Die Anzahl der Minuten für die Verzögerung, wenn der Benutzer den Neustart für gerätebezogene Richtlinien verzögert.
Anzahl der zulässigen Verzögerungen beim Neustart	1					5		3		Die Anzahl der Vorgänge, die ein Benutzer beim Neustart für gerätebezogene Richtlinien hat.
Benachrichtigung bei fragwürdige	Falsch									Diese Richtlinie regelt, ob ein Benutzer Benachrichtigungs-Popup-Meldungen sieht, wenn eine Anwendung versucht, auf

Richtlinien	Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten	PCI-Vorschriften	Datenschutzvorschriften	HIPAA-Vorschriften	Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)	Einfacher Schutz für alle Festplattenlaufwerke	Einfacher Schutz nur für das Systemlaufwerk	Einfacher Schutz für externe Festplatten	Verschlüsselung deaktiviert	Beschreibung
r Datei unterbinden										eine Datei zuzugreifen, während sie vom Client verarbeitet wird.
Lokale Verschlüsselungssteuerung anzeigen	Falsch		Wahr					Falsch		Bei der Auswahl von „Wahr“ sieht der Benutzer eine Menüoption in dem Taskleistensymbol, mit der er die Ver- bzw. Entschlüsselung (je nach ausgeführtem Shield-Vorgang) anhalten und wieder aufnehmen kann. **ANMERKUNG: Wichtiger Hinweis: Wenn Sie die Unterbrechung der Verschlüsselung durch Benutzer zulassen, kann dies gemäß der Richtlinie die vollständige Ver- oder Entschlüsselung von Daten durch Shield beeinträchtigen.**
Verschlüsselungsverarbeitung nur bei gesperrtem Bildschirm zulassen	Falsch		Benutzer optional					Falsch		Wahr, Falsch, Benutzer optional Mit „Wahr“ werden Daten nicht ver- oder entschlüsselt, während der Benutzer aktiv arbeitet. Der Client verarbeitet nur dann Daten, wenn der Bildschirm gesperrt ist. „Benutzer optional“ fügt eine Option in der Taskleiste hinzu, mit der der Benutzer diese Funktion aktivieren oder deaktivieren kann. Mit „Falsch“ wird die Verschlüsselung jederzeit durchgeführt, auch während der Benutzer arbeitet. Bei einer Aktivierung dieser Option verlängert sich die Dauer der Ver- oder Entschlüsselung erheblich.

Vorlagenbeschreibungen

Massiver Schutz für alle Festplattenlaufwerke und externen Festplatten

Diese Richtlinienvorlage wurde auf Organisationen zugeschnitten, deren Hauptziel in der Durchsetzung von Sicherheitsvorgaben und der Risikovermeidung besteht. Sie kommt dann am besten zur Anwendung, wenn Sicherheit die Benutzerfreundlichkeit überwiegt und nur ein minimaler Bedarf an Richtlinienausnahmen mit niedrigerer Sicherheitsstufe für bestimmte Benutzer, Gruppen oder Geräte besteht.

Diese Richtlinienvorlage:

- bietet durch eine extrem eingeschränkte Konfiguration erhöhten Schutz
- schützt das Systemlaufwerk sowie alle Festplattenlaufwerke
- verschlüsselt alle Daten auf Wechselspeichermedien und verhindert die Verwendung unverschlüsselter Wechselspeichermedien
- ermöglicht die Steuerung schreibgeschützter optischer Laufwerke

Schutz nach PCI-Vorschriften

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein Sicherheitsstandard der Kreditkartenbranche, der Anforderungen für die Sicherheitsverwaltung, für Richtlinien, Verfahren, Netzwerkarchitektur, Softwaredesign und andere wichtige Schutzmaßnahmen einschließt. Der umfassende Standard soll Unternehmen als verbindliche Richtlinie zum Schutz ihrer Kundendaten dienen.

Diese Richtlinienvorlage:

- schützt das Systemlaufwerk sowie alle Festplattenlaufwerke
- fordert Benutzer zur Verschlüsselung von Wechselspeichermedien auf
- ermöglicht ausschließlich das Schreiben von UDF-CD/DVDs Port Control-Einstellungen lassen schreibgeschützten Zugriff auf alle optischen Laufwerke zu.

Schutz nach Datenschutzvorschriften

Der Sarbanes-Oxley Act schreibt ausreichende Kontrollen für Finanzdaten vor. Da ein großer Teil dieser Daten im elektronischen Format vorliegt, bietet die Verschlüsselung eine wichtige Kontrolle bei der Datenspeicherung oder -übertragung. Richtlinien gemäß dem US-amerikanischen Gramm-Leach-Bliley Act (GLB, auch als Modernisierungsgesetz für Finanzdienstleistungen bekannt) erfordern keine Verschlüsselung. Die US-Kontrollinstanz für Finanzinstitute, der Federal Financial Institutions Examination Council (FFIEC), empfiehlt jedoch: „Finanzinstitute sollten Verschlüsselung einsetzen, um das Risiko der Offenlegung oder Änderung vertraulicher Daten im Speicher oder bei der Übertragung zu verhindern.“ Das kalifornische Gesetz California Senate Bill 1386 zur Bekanntgabe von Sicherheitsvorfällen bei Datenbanken soll die Einwohner Kaliforniens vor Identitätsdiebstahl schützen, indem Organisationen, deren Computersicherheit kompromittiert wurde, alle betroffenen Personen benachrichtigen. Organisationen können diese Benachrichtigung ihrer Kunden nur dann vermeiden, wenn sie nachweisen können, dass alle persönlichen Daten vor der Sicherheitsverletzung verschlüsselt waren.

Diese Richtlinienvorlage:

- schützt das Systemlaufwerk sowie alle Festplattenlaufwerke
- fordert Benutzer zur Verschlüsselung von Wechselspeichermedien auf
- ermöglicht ausschließlich das Schreiben von UDF-CD/DVDs Port Control-Einstellungen lassen schreibgeschützten Zugriff auf alle optischen Laufwerke zu.

Schutz nach HIPAA-Vorschriften

Der US-amerikanische Health Insurance Portability and Accountability Act (HIPAA) schreibt vor, dass Organisationen im Gesundheitssektor verschiedene technische Maßnahmen ergreifen müssen, um den Schutz und die Integrität aller personenbezogenen Patientendaten zu gewährleisten.

Diese Richtlinienvorlage:

schützt das Systemlaufwerk sowie alle Festplattenlaufwerke

fordert Benutzer zur Verschlüsselung von Wechselspeichermedien auf

ermöglicht ausschließlich das Schreiben von UDF-CD/DVDs Port Control-Einstellungen lassen schreibgeschützten Zugriff auf alle optischen Laufwerke zu.

Einfacher Schutz für alle Festplattenlaufwerke und externen Festplatten (Standard)

Diese Richtlinienvorlage stellt die empfohlene Konfiguration bereit, die einen hohen Schutz bietet, ohne die Benutzerfreundlichkeit des Systems zu beeinträchtigen.

Diese Richtlinienvorlage:

schützt das Systemlaufwerk sowie alle Festplattenlaufwerke

fordert Benutzer zur Verschlüsselung von Wechselspeichermedien auf

ermöglicht ausschließlich das Schreiben von UDF-CD/DVDs Port Control-Einstellungen lassen schreibgeschützten Zugriff auf alle optischen Laufwerke zu.

Einfacher Schutz für alle Festplattenlaufwerke

Diese Richtlinienvorlage:

schützt das Systemlaufwerk sowie alle Festplattenlaufwerke

ermöglicht das Schreiben von CD/DVDs in beliebigen unterstützten Formaten Port Control-Einstellungen lassen schreibgeschützten Zugriff auf alle optischen Laufwerke zu.

Von dieser Richtlinienvorlage nicht abgedeckt:

Verschlüsselung für Wechselspeichermedien

Einfacher Schutz nur für das Systemlaufwerk

Diese Richtlinienvorlage:

schützt das Systemlaufwerk, in der Regel Laufwerk C:, auf dem sich das Betriebssystem befindet

ermöglicht das Schreiben von CD/DVDs in beliebigen unterstützten Formaten Port Control-Einstellungen lassen schreibgeschützten Zugriff auf alle optischen Laufwerke zu.

Von dieser Richtlinienvorlage nicht abgedeckt:

Verschlüsselung für Wechselspeichermedien

Einfacher Schutz für externe Festplatten

Diese Richtlinienvorlage:

bietet Schutz von Wechselspeichermedien

ermöglicht ausschließlich das Schreiben von UDF-CD/DVDs Port Control-Einstellungen lassen schreibgeschützten Zugriff auf alle optischen Laufwerke zu.

Von dieser Richtlinienvorlage nicht abgedeckt:

Schutz des Systemlaufwerks (in der Regel Laufwerk C:, auf dem sich das Betriebssystem befindet) oder anderer Festplattenlaufwerke

Verschlüsselung deaktiviert

Diese Richtlinienvorlage bietet keinen Verschlüsselungsschutz. Wenn Sie diese Vorlage verwenden, sollten Sie zusätzliche Maßnahmen zum Schutz bei Verlust und Diebstahl ergreifen.

Diese Richtlinie eignet sich für Organisationen, die die Umstellung auf höhere Sicherheitsstandards ohne aktive Verschlüsselung beginnen möchten. Ist das Unternehmen einmal mit dem Umgang mit Richtlinien vertraut, lässt sich nach und nach die Möglichkeit der Verschlüsselung hinzufügen, indem einzelne Richtlinien oder übergeordnete Vorlagen für das Unternehmen bzw. Bereiche des Unternehmens angewendet werden.

Fahren Sie mit Vorinstallationskonfiguration für Einmalpasswort fort.

Vorinstallationskonfiguration für Einmalpasswort

Diese Funktionen der Personal Edition müssen bereits **vor** der Installation konfiguriert werden.

TPM initialisieren

- Für diesen Vorgang müssen Sie Mitglied der lokalen Administratorgruppe oder dergleichen sein.
- Der Computer muss mit einem kompatiblen BIOS und TPM ausgestattet sein.

Diese Aufgabe ist bei der Verwendung von Einmalpasswort erforderlich.

- Folgen Sie den Anweisungen unter http://technet.microsoft.com/en-us/library/cc753140.aspx.

Untergeordnete Installer aus dem Master Installer extrahieren

- Zur Einzelinstallation der Clients müssen zunächst die untergeordneten ausführbaren Dateien aus dem Installationsprogramm extrahiert werden.
- Falls das Master-Installationsprogramm für die Installation verwendet wurde, müssen die Clients einzeln deinstalliert werden. Verwenden Sie dieses Verfahren zum Extrahieren der Clients aus dem Master-Installationsprogramm, sodass sie für die Deinstallation verwendet werden können.

1 Kopieren Sie die Datei `DDPSetup.exe` vom Dell Installationsmedium auf den lokalen Computer.

2 Öffnen Sie am Speicherort der Datei `DDPSetup.exe` eine Eingabeaufforderung und geben Sie Folgendes ein:

```
DDPSetup.exe /z"\"EXTRACT_INSTALLERS=C:\extracted\""
```

Der Extraktionspfad darf maximal 63 Zeichen enthalten.

Stellen Sie vor Beginn des Installationsvorgangs sicher, dass alle Voraussetzungen erfüllt sind und die gesamte erforderliche Software installiert wurde, und zwar für jedes untergeordnete Installationsprogramm, das Sie installieren möchten. Einzelheiten erhalten Sie im Abschnitt Anforderungen.

Die extrahierten untergeordneten Installer befinden sich unter **C:\extracted\.**

Fahren Sie mit Fehlerbehebung fort.

Fehlerbehebung

Upgrade auf Windows 10 Anniversary Update

Für Computer, auf denen Encryption installiert ist, muss ein speziell konfiguriertes Upgrade-Paket verwendet werden, um eine Aktualisierung auf das Windows 10 Anniversary Update durchzuführen. Diese konfigurierte Version des Upgrade-Pakets sorgt dafür, dass Dell Data Protection den Zugriff auf Ihre verschlüsselten Dateien verwalten kann, um sie während des Aktualisierungsvorgangs zu schützen.

Um ein Upgrade auf die Windows 10 Anniversary-Version durchzuführen, befolgen Sie die Anleitungen in folgendem Artikel:

http://www.dell.com/support/article/us/en/19/SLN298382

Fehlerbehebung für den Client für Verschlüsselung

Upgrade auf die Windows 10 Anniversary-Aktualisierung

Um ein Upgrade auf die Windows 10 Anniversary-Aktualisierungsversion auszuführen, folgen Sie den Anweisungen im folgenden Artikel: http://www.dell.com/support/article/us/en/19/SLN298382.

Erstellen einer Encryption Removal Agent-Protokolldatei (optional)

- Vor der Deinstallation können Sie optional eine Encryption Removal Agent-Protokolldatei anlegen. Diese Protokolldatei erleichtert das Beheben von Fehlern, die unter Umständen beim Deinstallieren/Entschlüsseln auftreten. Falls Sie während der Deinstallation keine Dateien entschlüsseln möchten, müssen Sie diese Protokolldatei nicht anlegen.
- Die Encryption Removal Agent-Protokolldatei wird nach dem Start des Encryption Removal Agent-Service – also erst nach dem Neustart des Computers – erstellt. Nach Abschluss der Deinstallation und Entschlüsselung des Computers wird die Protokolldatei gelöscht.
- Der Pfad der Protokolldatei ist **C:\ProgramData\Dell\Dell Data Protection\Encryption.**.
- Erstellen Sie auf dem für die Entschlüsselung vorgesehenen Computer den folgenden Registrierungseintrag.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: Keine Protokollierung

  1: Protokolliert Fehler, die den Betrieb des Dienstes verhindern

  2: Protokolliert Fehler, die eine vollständige Datenentschlüsselung verhindern (empfohlene Protokollebene)

  3: Protokolliert Informationen über alle zu entschlüsselnden Datenträger und Dateien

  5: Protokolliert Informationen zum Debuggen

TSS-Version suchen

- TSS ist eine Komponente, die als Schnittstelle zu TPM fungiert. Zur Ermittlung der TSS-Version wechseln Sie zu **C:\Program Files\Dell \Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe** (Standardspeicherort). Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Eigenschaften** aus. Überprüfen Sie die Dateiversion auf der Registerkarte **Details**.

EMS und PCS Interaktionen

Um sicherzugehen, dass Medien nicht schreibgeschützt sind und der Port nicht blockiert ist

Die Richtlinie „EMS-Zugriff auf nicht durch Shield geschützte Medien“ interagiert mit „Port Control System – Speicherklasse: Richtlinie zur Steuerung externer Laufwerke “ Wenn Sie beabsichtigen, die Richtlinie „EMS-Zugriff auf nicht durch Shield geschützte Medien“ auf *vollen Zugriff*, zu setzen, stellen Sie sicher, dass die Speicherklasse: Richtlinie zur Steuerung externer Laufwerke auch auf *uneingeschränkten Zugang* setzen, um sicherzustellen, dass der Datenträger nicht auf schreibgeschützt gesetzt wird und die Schnittstelle nicht blockiert ist.

So verschlüsseln Sie Daten, die auf CD/DVD geschrieben werden:

- Stellen Sie „EMS-Verschlüsselung externer Medien“ auf „Wahr“ ein.
- Stellen Sie „EMS CD/DVD-Verschlüsselung ausschließen“ auf „Falsch“ ein.
- Unterklasse Speicher: Steuerung optischer Laufwerke = nur UFD.

WSScan verwenden

- WSScan ermöglicht Ihnen, sicherzugehen, dass bei der Deinstallation des Clients für die Verschlüsselung alle Daten entschlüsselt werden. Es zeigt Ihnen außerdem den Verschlüsselungsstatus und erkennt unverschlüsselte Dateien, die verschlüsselt sein sollten.
- Zur Ausführung dieses Dienstprogramms sind Administratorberechtigungen erforderlich.

Ausführen von WSScan

1 Kopieren Sie „WSScan.exe“ von den Dell Installationsmedien auf den Windows-Computer.

2 Öffnen Sie am obigen Speicherort eine Befehlszeile, und geben Sie an der Eingabeaufforderung **wsscan.exe** ein. WSScan wird gestartet.

3 Klicken Sie auf **Erweitert**.

4 Wählen Sie den Typ des zu prüfendenden Laufwerks aus dem Drop-Down-Menü aus: *Alle Laufwerke, Feste Laufwerke*, *Wechsellaufwerke* oder *CD-ROMs/DVDROMs*.

5 Wählen Sie den gewünschten Berichtstyp für die Verschlüsselung aus dem Drop-Down-Menü aus: *Verschlüsselte Dateien*, *Unverschlüsselte Dateien*, *Alle Dateien* oder *Unverschlüsselte Dateien verletzt*:

   - *Verschlüsselte Dateien* – Um sicherzustellen, dass alle Daten bei der Deinstallation des Clients für die Verschlüsselung entschlüsselt werden. Befolgen Sie das übliche Verfahren für die Entschlüsselung von Daten, z. B. die Ausgabe einer Richtlinienaktualisierung für die Entschlüsselung. Nach der Entschlüsselung der Daten und vor dem Neustart zur Vorbereitung der Deinstallation führen Sie bitte den WSScan aus, um zu gewährleisten, dass alle Daten entschlüsselt sind.
   - *Unverschlüsselte Dateien* – Um Dateien zu identifizieren, die nicht verschlüsselt sind, einschließlich einem Hinweis, ob sie verschlüsselt sein sollten (J/N).
   - *Alle Dateien* – Zum Auflisten aller verschlüsselten und unverschlüsselten Dateien einschließlich einem Hinweis, ob sie verschlüsselt sein sollten (J/N).
   - *Unverschlüsselte Dateien verletzt* – Um nicht verschlüsselte Dateien zu erkennen, die verschlüsselt sein sollten.

6 Klicken Sie auf **Suchen**.

ODER

1 Klicken Sie auf **Erweitert,** um zur Ansicht **Einfach** zu wechseln und einen bestimmten Ordner zu durchsuchen.

2 Wechseln Sie zu „Sucheinstellungen“, und geben Sie im Feld ***Suchpfad*** den Ordnerpfad ein. Wenn Sie dieses Feld verwenden, wird die Auswahl im Drop-Down-Feld ignoriert.

3 Falls die Ausgabe des Suchdienstprogramms „WSScan“ nicht in einer Datei gespeichert werden soll, deaktivieren Sie das Kontrollkästchen **Ausgabe in Datei**.

4 Ändern Sie unter *Pfad* ggf. den Standardpfad und den Standarddateinamen.

5 Wählen Sie **Zu vorhandener Datei hinzufügen** aus, wenn Sie bereits bestehende WSScan-Ausgabedateien nicht überschreiben möchten.

6 Wählen Sie das Ausgabeformat aus:

- Wählen Sie Berichtsformat, um eine Liste der Berichtsstile für das Suchergebnis zu erhalten. Das ist das Standardformat.
- Wählen Sie Datei mit Wertbegrenzung für eine Ausgabe, die in eine Tabellenkalkulation importiert werden kann. Das Standardtrennzeichen ist „|“, doch können auch bis zu 9 alphanumerische Zeichen, Leerzeichen oder Zeichensetzungszeichen der Tastatur verwendet werden.
- Wählen Sie die Option Werte in Anführungszeichen, damit jeder Wert in doppelte Anführungszeichen gesetzt wird.
- Wählen Sie „Datei mit fester Breite“ für eine Ausgabe ohne Trennzeichen aus, die eine durchgängige Zeile von Informationen fester Breite über jede verschlüsselte Datei enthält.

7 Klicken Sie auf **Suchen**.

Klicken Sie auf **Suche stoppen**, um die Suche zu beenden. Klicken Sie auf **Löschen**, um die angezeigten Meldungen zu löschen.

WSScan-Ausgabe

Die WSScan-Daten über verschlüsselte Dateien enthalten die folgenden Informationen.

Beispiel der Ausgabe:

[2015-07-28 07:52:33] SysData.07vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" ist noch AES256 verschlüsselt

Ausgabe	Erläuterung
Zeitstempel	Das Datum und die Uhrzeit der Durchsuchung der Datei.
Verschlüsselungstyp	Die Art der Verschlüsselung für die Datei. **SysData**: SDE-Verschlüsselungscode. **Benutzer:** Benutzer-Verschlüsselungscode. **Allgemein:** Allgemeiner Verschlüsselungscode. WSScan meldet keine Dateien, die mittels „Für Freigabe verschlüsseln“ verschlüsselt wurden.
KCID	Die ID des Schlüssel-Computers. Im Beispiel oben „**7vdlxrsb**“ Wenn Sie ein zugeordnetes Netzwerklaufwerk durchsuchen, gibt der Abfragebericht keine KCID aus.
UCID	Die Benutzer-ID. Im Beispiel oben „**_SDENCR_**“ Die UCID ist für alle Benutzer des Computers gleich.
Datei	Der Pfad der verschlüsselten Datei. Wie im Beispiel oben angezeigt, „**c:\temp\Dell - test.log**“
Algorithmus	Im Folgenden finden Sie den für die Verschlüsselung der Datei verwendeten Verschlüsselungsalgorithmus. Im Beispiel oben „**is still AES256 encrypted**“

Ausgabe	Erläuterung
	Rijndael 128
	Rijndael 256
	AES 128
	AES 256
	3DES

Überprüfen des Encryption-Removal-Agent-Status

Der Status des Encryption Removal Agent wird im Beschreibungsbereich des Dialogfelds „Dienste“ (Start > Ausführen... > services.msc > OK) wie folgt angezeigt: Aktualisieren Sie in regelmäßigen Abständen den Service-Status (markieren Sie den Service > rechte Maustaste > Aktualisieren).

- **Warten auf SDE-Deaktivierung** – Der Encryption-Client ist noch installiert und/oder konfiguriert. Die Entschlüsselung beginnt erst nach der Deinstallation des Encryption-Clients.
- **Erste Suche** – Dieser Dienst führt eine erste Suche durch und berechnet die Anzahl verschlüsselter Dateien und Bytes. Die erste Suche wird nur einmal durchgeführt.
- **Entschlüsselungssuche** – Dieser Dienst entschlüsselt Dateien und stellt möglicherweise eine Anfrage zur Entschlüsselung gesperrter Dateien.
- **Entschlüsselung bei Neustart (teilweise)** – Die Entschlüsselungssuche ist abgeschlossen, und einige gesperrte Dateien (aber nicht alle) werden beim nächsten Neustart entschlüsselt.
- **Entschlüsselung bei Neustart** – Die Entschlüsselungssuche ist abgeschlossen, und alle gesperrten Dateien werden beim nächsten Neustart entschlüsselt.
- **Nicht alle Dateien konnten entschlüsselt werden** – Die Entschlüsselungssuche ist abgeschlossen, aber es konnten nicht alle Dateien entschlüsselt werden. Dieser Status kann folgende Gründe haben:
  - Die gesperrten Dateien wurden nicht für die Entschlüsselung vorgesehen, weil sie entweder zu groß sind oder ein Fehler bei der Anfrage nach ihrer Freigabe auftrat.
  - Während der Entschlüsselung der Dateien trat ein Eingabe-/Ausgabefehler auf.
  - Die Dateien konnten nicht richtliniengemäß entschlüsselt werden.
  - Die Dateien waren zur Verschlüsselung markiert.
  - Während der Entschlüsselungssuche trat ein Fehler auf.
  - In sämtlichen Fällen wird eine Protokolldatei erstellt, sofern mindestens LogVerbosity=2 eingestellt ist (und die Protokollierung aktiviert wurde). Zur Fehlerbehebung sollten Sie die Ausführlichkeitsstufe auf 2 einstellen (LogVerbosity=2) und den Encryption Removal Agent-Dienst neu starten, um eine weitere Entschlüsselungssuche zu erzwingen.
- **Vollständig** – Die Entschlüsselungssuche wurde abgeschlossen. Der Service, die ausführbare Datei, der Treiber und die ausführbare Treiberdatei werden beim nächsten Neustart des Computers gelöscht.

Vorgehensweise bei der EMS-Verschlüsselung eines iPods

Diese Regeln schalten die Verschlüsselung für diese Ordner und Dateitypen für alle Wechselspeichermedien, nicht nur für einen iPod aus bzw. ein. Gehen Sie bei der Definition von Richtlinien vorsichtig vor.

- Von der Verwendung mit iPod Shuffle wird abgeraten, da dies zu Fehlfunktionen führen kann.
- Wenn iPods geändert werden, könnten sich auch diese Informationen ändern. Gehen Sie daher bei Verwendung eines iPods an Computern mit aktiviertem EMS vorsichtig vor.
- Da die Ordnernamen auf iPods vom jeweiligen iPod-Modell abhängen, empfehlen wir die Erstellung einer ausschließenden Richtlinie, die die Ordnernamen aller iPod-Modelle berücksichtigt.

- Um sicherzustellen, dass ein iPod auch nach der Verschlüsselung mittels EMS genutzt werden kann, geben Sie in der Richtlinie „EMS-Verschlüsselungsrichtlinien“ die folgenden Richtlinien ein:

  -R#:\Calendars

  -R#:\Contacts

  -R#:\iPod_Control

  -R#:\Notes

  -R#:\Photos
- Sie können in den oben angegebenen Verzeichnissen auch die Verschlüsselung bestimmter Dateitypen erzwingen. Durch Hinzufügen der folgenden Richtlinien werden Dateien mit den Erweiterungen ppt, pptx, doc, docx, xls und xlsx in den durch die obigen Richtlinien von der Verschlüsselung *ausgeschlossenen* Verzeichnissen verschlüsselt:

  ^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx
- Werden diese fünf Regeln durch die folgende Regel ersetzt, wird die Verschlüsselung von Dateien mit den Erweiterungen ppt, pptx, doc, docx, xls und xlsx in allen Verzeichnissen des iPod erzwungen, auch in Calendars, Contacts, iPod_Control, Notes und Photos:

  ^R#:\;ppt.doc.xls.pptx.docx.xlsx
- Diese Richtlinien wurden an den folgenden iPods getestet:

  iPod Video, 30 GB, fünfte Generation

  iPod Nano, 2 GB, zweite Generation

  iPod Mini, 4 GB, zweite Generation

Dell ControlVault-Treiber

Aktualisieren von Treibern und Firmware für Dell ControlVault

Die auf Dell-Computern werkseitig installierte(n) Treiber und Firmware für Dell ControlVault sind nicht mehr aktuell und müssen anhand des folgenden Verfahrens in der angegebenen Reihenfolge aktualisiert werden.

Wenn Sie während der Client-Installation aufgefordert werden, das Installationsprogramm zu schließen, um die Dell ControlVault-Treiber zu installieren, können Sie diese Meldung ignorieren und die Client-Installation fortsetzen. Die Dell ControlVault-Treiber (und die zugehörige Firmware) können nach dem erfolgreichen Abschluss der Client-Installation aktualisiert werden.

Herunterladen der aktuellen Treiber

1 Gehen Sie zu support.dell.com.
2 Wählen Sie Ihr Computermodell aus.
3 Wählen Sie **Treiber & Downloads**.
4 Wählen Sie das auf dem Zielcomputer ausgeführte **Betriebssystem** aus.
5 Erweitern Sie die Kategorie **Sicherheit**.
6 Laden Sie die Dell ControlVault-Treiber herunter, und speichern Sie sie.

7 Laden Sie die Dell ControlVault-Firmware herunter, und speichern Sie sie.

8 Kopieren Sie die Treiber und die Firmware bei Bedarf auf die Zielcomputer.

Installieren des Dell ControlVault-Treibers

Gehen Sie zu dem Ordner, in den Sie die Treiberinstallationsdatei abgelegt haben.

Doppelklicken Sie auf den Dell ControlVault-Treiber, um die selbstextrahierende EXE-Datei aufzurufen.

:

Achten Sie darauf, als Erstes den Treiber zu installieren. Der Dateiname des Treibers *zum Zeitpunkt der Erstellung dieses Dokuments* lautet „ControlVault_Setup_2MYJC_A37_ZPE.exe“.

Klicken Sie zum Fortsetzen des Vorgangs auf **Weiter**.

Klicken Sie auf **OK**, um die Treiberdateien in den Standardordner **C:\Dell\Drivers\<New Folder>** zu entpacken.

Klicken Sie auf **Ja**, um die Erstellung eines neuen Ordners zu genehmigen.

Klicken Sie auf **OK**, wenn die Nachricht angezeigt wird, dass die Dateien erfolgreich entpackt wurden.

Nach dem Entpacken wird der Ordner angezeigt, der die entpackten Dateien enthält. Ist dies nicht der Fall, gehen Sie zu dem Ordner, in den Sie die Dateien entpackt haben. Der Ordner ist als **JW22F** bezeichnet

Doppelklicken Sie auf die Datei **CVHCI64.MSI**, um das Treiberinstallationsprogramm zu starten. [Die Datei **CVHCI64.MSI** in diesem Beispiel bezieht sich auf ein 64-Bit-System. Bei einem 32-Bit-System wählen Sie die Datei **CVHCI32.MSI** aus].

Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.

Klicken Sie auf **Weiter**, um die Treiber in den Standardordner unter **C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.** zu installieren.

Wählen Sie die Option **Abschließen** aus, und klicken Sie auf **Weiter**.

Klicken Sie auf **Installieren**, um mit der Installation der Treiber zu beginnen.

Aktivieren Sie optional das Kontrollkästchen, um die Protokolldatei für das Installationsprogramm anzuzeigen. Klicken Sie zum Beenden des Assistenten auf **Fertig stellen**.

Überprüfen der Treiberinstallation

Der Gerätemanager zeigt je nach Betriebssystem und Hardwarekonfiguration ein Dell ControlVault-Gerät (sowie weitere Geräte) an.

Installieren der Dell ControlVault-Firmware

1 Gehen Sie zu dem Ordner, in den Sie die Firmware-Installationsdatei abgelegt haben.

2 Doppelklicken Sie auf die Dell ControlVault-Firmware, um die selbstextrahierende EXE-Datei aufzurufen.

3 Klicken Sie zum Fortsetzen des Vorgangs auf **Weiter**.

4 Klicken Sie auf **OK**, um die Treiberdateien in den Standardordner **C:\Dell\Drivers\<New Folder>** zu entpacken.

5 Klicken Sie auf **Ja**, um die Erstellung eines neuen Ordners zu genehmigen.

6 Klicken Sie auf **OK**, wenn die Nachricht angezeigt wird, dass die Dateien erfolgreich entpackt wurden.

7 Nach dem Entpacken wird der Ordner angezeigt, der die entpackten Dateien enthält. Ist dies nicht der Fall, gehen Sie zu dem Ordner, in den Sie die Dateien entpackt haben. Wählen Sie den Ordner **Firmware** aus.

8 Doppelklicken Sie auf die Datei **ushupgrade.exe**, um das Firmware-Installationsprogramm zu starten.

9 Klicken Sie zum Starten der Firmware auf **Start**.

:

Sie werden möglicherweise dazu aufgefordert, das Administratorkennwort einzugeben, wenn Sie ein Upgrade von einer älteren Firmware-Version durchführen. Geben Sie **`Broadcom`** als Kennwort ein, und klicken Sie auf **Eingabe**, wenn diese Option im Dialogfeld angezeigt wird.

Es werden nun verschiedene Statusmeldungen angezeigt.

10 Klicken Sie auf **Neu starten**, um das Firmware-Upgrade abzuschließen.

Die Aktualisierung der Treiber und der Firmware für Dell ControlVault ist damit abgeschlossen.

Registrierungseinstellungen

Dieser Abschnitt führt alle durch den Dell ProSupport genehmigten Registrierungseinstellungen für lokale Client-Computer im Detail auf.

Encryption-Client

Erstellen einer Encryption Removal Agent-Protokolldatei (optional)

Vor der Deinstallation können Sie optional eine Encryption Removal Agent-Protokolldatei anlegen. Diese Protokolldatei erleichtert das Beheben von Fehlern, die unter Umständen beim Deinstallieren/Entschlüsseln auftreten. Falls Sie während der Deinstallation keine Dateien entschlüsseln möchten, müssen Sie diese Protokolldatei nicht anlegen.

Die Encryption Removal Agent-Protokolldatei wird nach dem Start des Encryption Removal Agent-Service – also erst nach dem Neustart des Computers – erstellt. Nach Abschluss der Deinstallation und Entschlüsselung des Computers wird die Protokolldatei gelöscht.

Der Pfad der Protokolldatei ist **C:\ProgramData\Dell\Dell Data Protection\Encryption.**.

Erstellen Sie auf dem für die Entschlüsselung vorgesehenen Computer den folgenden Registrierungseintrag.

[HKLM\Software\Credant\DecryptionAgent]

„LogVerbosity“=dword:2

0: Keine Protokollierung

1: Protokolliert Fehler, die den Betrieb des Dienstes verhindern

2: Protokolliert Fehler, die eine vollständige Datenentschlüsselung verhindern (empfohlene Protokollebene)

3: Protokolliert Informationen über alle zu entschlüsselnden Datenträger und Dateien

5: Protokolliert Informationen zum Debuggen

Verwenden von Smart Cards mit Windows-Anmeldung

Um Smart Cards mit der Windows-Authentifizierung zu verwenden, muss der folgende Registrierungswert auf dem Client-Computer eingestellt sein.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

Beibehalten von temporären Dateien während der Installation

Standardmäßig werden alle temporären Dateien im Verzeichnis C:\Windows\Temp während der Installation automatisch gelöscht. Durch das Löschen der temporären Dateien vor der ersten Verschlüsselungssuche wird die Verschlüsselungsdauer verkürzt.

Wenn Ihre Organisation jedoch eine Drittanbieter-Anwendung einsetzt, die auf die Dateistruktur im Verzeichnis \Temp angewiesen ist, sollten Sie das Löschen verhindern.

Durch die Erstellung oder Änderung des folgenden Registrierungseintrags können Sie das Löschen temporärer Dateien verhindern:

[HKLM\SOFTWARE\CREDANT\CMGShield]

"DeleteTempFiles"=REG_DWORD:0

Werden temporäre Dateien nicht gelöscht, verlängert sich die Verschlüsselungsdauer.

Ändern des Standardverhaltens der Benutzer-Eingabeaufforderung für Start oder Verzögerung der Verschlüsselung

Der Encryption-Client zeigt die Eingabeaufforderung `Verzögerung der einzelnen Richtlinienaktualisierungen` jeweils fünf Minuten lang an. Reagiert der Benutzer nicht auf die Aufforderung, beginnt die nächste Verzögerung. Die endgültige Verzögerungsaufforderung enthält einen Countdown und einen Fortschrittsbalken und wird angezeigt, bis der Benutzer reagiert oder die endgültige Verzögerung abläuft und die verlangte Abmeldung bzw. der verlangte Neustart durchgeführt wird.

Sie können das Verhalten der Benutzeraufforderung dahingehend ändern, dass die Verschlüsselung begonnen oder verzögert wird, damit keine Verschlüsselung durchgeführt wird, wenn der Benutzer nicht auf die Aufforderung reagiert. Legen Sie dazu den folgenden Registrierungswert fest:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"SnoozeBeforeSweep"=DWORD:1

Jeder Wert ungleich Null ändert das Standardverhalten auf Schlummern. Ohne Benutzerinteraktion wird die Verschlüsselung bis zur maximal konfigurierbaren Anzahl von Verzögerungen verzögert. Die Verarbeitung der Verschlüsselung beginnt, nachdem die letzte Verzögerung abgelaufen ist.

Berechnen Sie die maximal mögliche Verzögerung wie folgt (eine maximale Verzögerung bedeutet, dass der Benutzer auf keine der Verzögerungsaufforderungen reagiert, die jeweils 5 Minuten lang angezeigt werden):

(ANZAHL DER ZULÄSSIGEN VERZÖGERUNGEN BEI AKTUALISIERUNG DER RICHTLINIE LÄNGE DER VERZÖGERUNG BEI AKTUALISIERUNG DER RICHTLINIE) + (5 MINUTEN x [ANZAHL DER ZULÄSSIGEN VERZÖGERUNGEN BEI AKTUALISIERUNG DER RICHTLINIE - 1])

Standardmäßige Verwendung des SDUser-Schlüssels ändern

Die Systemdatenverschlüsselung (System Data Encryption, SDE) wird auf Basis des Richtlinienwerts für SDE-Verschlüsselungsregeln durchgesetzt. Zusätzliche Verzeichnisse werden standardmäßig geschützt, wenn die Richtlinie „SDE-Verschlüsselung – Aktiviert“ markiert ist. Weitere Informationen finden Sie unter dem Stichwort „SDE-Verschlüsselungsregeln“ in der Adminhilfe. Wenn der Encryption-Client eine Richtlinienaktualisierung mit einer aktiven SDE-Richtlinie verarbeitet, wird das aktuelle Benutzerprofilverzeichnis standardmäßig mit dem Benutzerschlüssel SDUser verschlüsselt, und nicht mit dem Geräteschlüssel SDE. Der SDUser-Schlüssel wird außerdem zur Verschlüsselung von Dateien oder Ordnern verwendet, die in ein Benutzerverzeichnis kopiert (nicht verschoben) werden, das nicht mit SDE verschlüsselt ist.

Erstellen Sie den folgenden Registrierungseintrag auf dem Computer, um den SDUser-Schlüssel zu deaktivieren und stattdessen den SDE-Schlüssel für die Verschlüsselung dieser Benutzerverzeichnisse zu verwenden:

[HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

„EnableSDUserKeyUsage“=dword:00000000

Wenn dieser Registrierungsschlüssel nicht vorhanden ist oder einen anderen Wert aufweist als 0, wird der SDUser-Schlüssel für die Verschlüsselung dieser Benutzerverzeichnisse verwendet.

Advanced Authentication-Client

Deaktivieren der Smart Card und biometrischen Dienste (optional)

Wenn Sie nicht möchten, dass Security Tools die Dienste in Verbindung mit Smart Cards und biometrischen Geräten in den Starttyp „Automatisch“ ändert, können Sie die Funktion zum Starten von Diensten deaktivieren.

Ist diese Funktion deaktiviert, unternimmt Security Tools für folgende drei Dienste keinen Startversuch:

SCardSvr – Verwaltet den Zugang zu den von einem Computer gelesenen Smartcards. Wird dieser Dienst gestoppt, kann der Computer keine Smartcards lesen. Wird dieser Dienst deaktiviert, können alle direkt davon abhängigen Dienste nicht gestartet werden.

SCPolicySvc – Ermöglicht es, das System so zu konfigurieren, dass der Benutzer-Desktop bei Entfernen der Smartcard gesperrt wird.

WbioSrvc – Der Biometrie-Dienst von Windows ermöglicht es Client-Anwendungen, biometrische Daten ohne direkten Zugriff auf Biometrie-Hardware oder -Proben zu erfassen, zu vergleichen, zu ändern und zu speichern. Der Dienst wird in einem bevorzugten SVCHOST-Prozess gehostet.

Das Deaktivieren der Funktion bewirkt auch, dass keine Warnmeldungen in Verbindung zu den nicht ausgeführten Diensten angezeigt werden.

Falls der Registrierungsschlüssel nicht existiert oder auf 0 gesetzt ist, ist diese Funktion standardmäßig aktiviert.

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

Legen Sie den Wert 0 fest, um die Funktion zu aktivieren.

Legen Sie den Wert 1 fest, um die Funktion zu deaktivieren.

Verwenden von Smart Cards mit Windows-Anmeldung

Um Smart Cards mit der Windows-Authentifizierung zu verwenden, muss der folgende Registrierungswert auf dem Client-Computer eingestellt sein.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

Fahren Sie mit Glossar fort.

13

Glossar

Advanced Authentication – Das Produkt Advanced Authentication bietet Optionen für vollständig integrierte Fingerabdrücke, Smart Card und kontaktlose Smart Card-Leser. Advanced Authentication vereinfacht die Verwaltung all dieser Hardware-Authentifizierungsmethoden, unterstützt die Anmeldung bei selbstverschlüsselnden Laufwerken, SSO und verwaltet Benutzeranmeldeinformationen und Passwörter. Darüber hinaus kann Advanced Authentication nicht nur für den Zugriff auf PCs verwendet werden, sondern auch für den Zugriff auf beliebige Websites, SaaS oder Anwendungen. Nachdem der Benutzer seine Anmeldeinformationen eingetragen hat, ermöglicht Advanced Authentication deren Verwendung für die Anmeldung am Gerät und die Ersetzung des Passworts.

Administrator-Passwort für die Verschlüsselung (Encryption Administrator Password, EAP) – Das EAP ist ein computerspezifisches Administrator-Passwort. Für die meisten Konfigurationsänderungen in der lokalen Management Console ist die Eingabe dieses Passworts erforderlich. Das Passwort wird auch benötigt, falls Sie über die Datei „LSARecovery_[Hostname].exe“ Ihre Daten wiederherstellen müssen. Notieren Sie sich das Passwort und bewahren Sie es an einem sicheren Ort auf.

Encryption-Client – Der Encryption-Client ist die geräteinterne Komponente, die Sicherheitsrichtlinien durchsetzt, egal ob ein Endpunkt mit dem Netzwerk verbunden oder vom Netzwerk getrennt ist, verloren gegangen ist oder gestohlen wurde. Der Encryption-Client erzeugt eine vertrauenswürdige Computerumgebung für Endpunkte, indem er als Layer über dem Betriebssystem des Geräts fungiert und Authentifizierung, Verschlüsselung und Autorisierung lückenlos anwendet, um den Schutz vertraulicher Informationen zu maximieren.

Encryption Keys – In den meisten Fällen verwendet der Encryption-Client den Benutzerschlüssel plus zwei weitere Verschlüsselungsschlüssel. Es gibt allerdings auch Ausnahmen: Alle SDE-Richtlinien und die Richtlinie „Windows-Anmeldeinformationen schützen“ verwenden den SDE-Schlüssel. Die Richtlinien „Windows-Auslagerungsdatei verschlüsseln“ und „Sichere Windows-Ruhezustand-Datei“ verwenden einen eigenen Schlüssel, den General Purpose Key (GPK). Der „allgemeine“ Schlüssel macht Dateien allen verwalteten Benutzern auf dem Gerät zugänglich, auf dem sie erstellt wurden. Der „Benutzer“-Schlüssel macht Dateien nur dem Benutzer zugänglich, der sie erstellt hat, und zwar nur auf dem Gerät, auf dem sie erstellt wurden. Der „Benutzer-Roaming“-Schlüssel macht Dateien nur dem Benutzer zugänglich, der sie erstellt hat, und zwar auf jedem mit Shield geschützten Windows- oder Mac-Gerät.

Verschlüsselungssuche – Bei einer Verschlüsselungssuche werden die zu verschlüsselnden Ordner auf einem mit einem Shield geschützten Endpunkt durchsucht, um sicherzustellen, dass die enthaltenen Dateien den richtigen Verschlüsselungsstatus haben. Einfache Operationen zur Erstellung und Umbenennung von Dateien lösen keine Verschlüsselungssuche aus. Es ist wichtig zu verstehen, wann eine Verschlüsselungssuche stattfindet und wodurch die Dauer der Suche beeinflusst wird: Eine Verschlüsselungssuche erfolgt sofort nach Eingang einer Richtlinie mit aktivierter Verschlüsselung. Das kann unmittelbar nach der Aktivierung sein, wenn für Ihre Richtlinie die Verschlüsselung aktiviert ist. - Wenn die Richtlinie „Workstation bei Anmeldung durchsuchen“ aktiviert ist, werden die zur Verschlüsselung angegebenen Ordner bei jeder Benutzeranmeldung durchsucht. - Eine Suche kann unter bestimmten nachfolgenden Richtlinienänderungen erneut ausgelöst werden. Jeder Richtlinienänderung, die sich auf die Definition der Verschlüsselungsordner, der Verschlüsselungsalgorithmen oder der Verwendung der Verschlüsselungsschlüssel („Allgemein“ oder „Benutzer“) bezieht, löst eine Suche aus. Auch beim Umschalten zwischen aktivierter und deaktivierter Verschlüsselung wird eine Verschlüsselungssuche ausgelöst.

Einmalpasswort (OTP) – Ein Einmalpasswort ist ein Passwort mit begrenzter Gültigkeit, das nur einmal verwendet werden kann. Für die OTP-Funktion muss ein TPM vorhanden, aktiviert und zugewiesen sein. Für die Aktivierung der OTP-Funktion muss ein Mobilgerät mit dem Computer über die Security Console und die Security Tools Mobile-App gekoppelt werden. Die Security Tools | Mobile-App generiert das Passwort auf dem Mobilgerät, mit dem die Anmeldung auf dem Computer über den Windows-Anmeldebildschirm erfolgt. Je nach Richtlinie kann die OTP-Funktion verwendet werden, um den Zugriff auf den Computer wiederherzustellen, falls das Passwort abgelaufen ist oder vergessen wurde, vorausgesetzt, das OTP wurde nicht bereits für die Anmeldung am Computer verwendet. Die OTP-Funktion kann zur Authentifizierung oder zur Wiederherstellung verwendet werden, aber nicht für beides. OTP ist sicherer als einige andere Authentifizierungsmethoden, weil das generierte Passwort nur einmal verwendet werden kann und nach kurzer Zeit abläuft.

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.

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.

System Data Encryption (SDE) – Mit SDE werden das Betriebssystem und die Programmdateien verschlüsselt. Dazu muss SDE in der Lage sein, den Schlüssel beim Start des Betriebssystems zu öffnen. SDE dient zum Schutz des Betriebssystems vor unbefugten Änderungen oder Offline-Angriffen SDE is not intended for user data. Zum Schutz vertraulicher Benutzerdaten empfiehlt sich die allgemeine Verschlüsselung oder die Benutzerverschlüsselung, bei denen zum Entsperren der Verschlüsselungsschlüssel ein Benutzerpasswort erforderlich ist. SDE-Richtlinien verschlüsseln keine Dateien, die das Betriebssystem zum Start des Boot-Vorgangs benötigt. SDE-Richtlinien erfordern keine Authentifizierung vor dem Neustart und haben auch keinerlei Auswirkungen auf den Master Boot Record. Beim Computerstart stehen die verschlüsselten Dateien lange vor der Anmeldung eines Benutzers zur Verfügung (damit Patchmanagement, SMS, Sicherungs- und Wiederherstellungstools funktionieren). Durch die Deaktivierung der SDE-Verschlüsselung werden alle relevanten Dateien und Verzeichnisse mit SDE-Verschlüsselung automatisch entschlüsselt, unabhängig von anderen SDE-Richtlinien wie beispielsweise SDE-Verschlüsselungsregeln.

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. Das TPM ist auch für die Verwendung der Einmalpasswort-Funktion erforderlich.