Dell Encryption Personal

Installation Guide v11.9

January 2024
Rev. A01

DELL Technologies

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

Contents

1

Übersicht

Die folgenden Anweisungen setzen voraus, dass Advanced Authentication zusammen mit Encryption Personal installiert wird.

Encryption Personal

Der Zweck von Encryption Personal ist, die Daten auf Ihrem Computer zu schützen, auch wenn der Computer verloren geht oder gestohlen wird.

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

Advanced Authentication

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

Unter Advanced Authentication-Administratoreinstellungen konfigurieren im *Dell Data Security Console User Guide* (*Dell Data Security Console-Benutzerhandbuch*) erfahren Sie, wie die erweiterte Authentifizierung verwendet wird.

Dell ProSupport for Software kontaktieren

Telefonischen Support 24x7 für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

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

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

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter Dell ProSupport for Software – Internationale Telefonnummern.

2

Anforderungen

Diese Anforderungen beschreiben im Detail, was zur Installation von Encryption Personal erforderlich ist.

Verschlüsselung

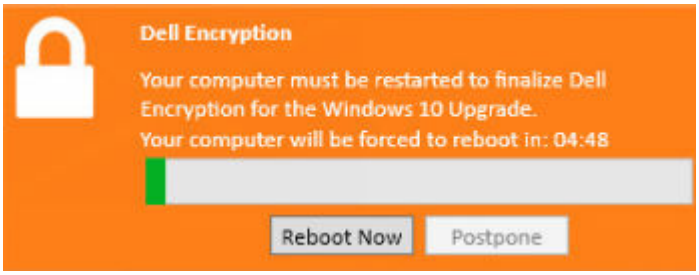
- Für eine erfolgreiche Installation von Encryption Personal ist eine Berechtigung erforderlich. Sie erhalten diese Berechtigung beim Erwerb von Encryption Personal. Je nachdem, wie Sie Encryption Personal erwerben, können Sie die Berechtigung manuell installieren, indem Sie die beigefügten einfachen Anweisungen befolgen. Sie können außerdem die Berechtigung über die Befehlszeile eingeben. Falls Encryption Personal mit Dell Digital Delivery installiert wird, kümmert sich der Dell Digital Delivery-Dienst um die Installation der Berechtigung. (Die gleichen Binärdateien werden für Encryption Enterprise und Encryption Personal verwendet. Durch die Berechtigung weiß das Installationsprogramm, welche Version installiert werden muss).
- Microsoft- und Office 365-Konten werden beim Ausführen von Encryption Personal v11.0 oder höher auf Windows 10 unterstützt.
- Zum Aktivieren eines Microsoft Live-Kontos mit Encryption Personal siehe KB-Artikel 124722.
- Ein Windows-Kennwort ist erforderlich (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 Nutzerkonto anmelden. Encryption Personal kann nicht aktiviert werden, wenn kein Kennwort erstellt wurde.
- Dell Encryption kann nicht auf v10.7.0 von Versionen vor v8.16.0 aktualisiert werden. Endpunkte, auf denen Versionen vor v8.16.0 ausgeführt werden, müssen auf v 8.16.0 aktualisiert werden. Anschließend wird ein Upgrade auf v 10.7.0 durchgeführt.
- Dell Encryption nutzt Verschlüsselungsbefehlssätze von Intel, Integrated Performance Primitives (IPP). Weitere Informationen finden Sie im KB-Artikel 126015.

1. Rufen Sie die Windows-Systemsteuerung auf (**Start** > **Systemsteuerung**).
2. Klicken Sie auf das Symbol für **Nutzerkonto**.
3. Klicken Sie auf **Kennwort für das eigene Konto erstellen**.
4. Geben Sie ein neues Kennwort ein und bestätigen Sie es.
5. Sie können auch einen Kennworthinweis eingeben.
6. Klicken Sie auf **Kennwort erstellen**.
7. Starten Sie den Computer neu.

- Bei der Bereitstellung sind die bewährten IT-Verfahren zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Nutzer.
- Die Installation/Aktualisierung/Deinstallation kann nur von einem lokalen Nutzer oder einem Domänenadministrator durchgeführt werden, der über ein Implementierungstool wie Microsoft SMS vorübergehend zugewiesen werden kann. Nutzer 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-Datenträgerbereinigungs-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 des Encryption Client in einem Unternehmens-Image finden Sie im KB-Artikel 129990.

- Das TPM wird zum Versiegeln des Allzweckschlüssels (General Purpose Key) verwendet. Falls Sie den Encryption-Client ausführen, löschen Sie daher das TPM im BIOS, bevor Sie ein neues Betriebssystem auf dem Zielcomputer installieren.
- Der Encryption-Client wurde getestet und ist mit mehreren gängigen signaturbasierten Antivirenprogrammen und KI-basierten Virenschutzlösungen kompatibel, einschließlich McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense und einige andere. Standardmäßig sind hartkodierte Ausschlüsse für viele Virenschutzanbieter vorhanden, um Inkompatibilitäten zwischen Virenüberprüfung und Verschlüsselung zu vermeiden.

  Wenn Ihr Unternehmen einen nicht aufgelisteten Virenschutzanbieter verwendet oder Kompatibilitätsprobleme auftreten, lesen Sie den KB-Artikel 126046 oder wenden Sie sich an Dell ProSupport, um unterstützende Informationen zur Validierung der Konfiguration für die Interoperabilität zwischen ihren Softwarelösungen und Dell Data Security Lösungen zu erhalten.
- Die Neuinstallation des Betriebssystems wird 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 dell.com/support, um stets über die neueste Dokumentation und die neuesten technischen Ratgeber zu verfügen.
- Nach dem Windows 10-Upgrade ist ein Neustart **erforderlich**, um Dell Encryption abzuschließen. Die folgende Meldung wird im Infobereich nach Windows 10-Funktions-Upgrades angezeigt:



Voraussetzungen

- Microsoft .NET Framework 4.5.2 (oder höher) ist für das Master-Installationsprogramm sowie untergeordnete Installationsprogramme erforderlich. Das Installationsprogramm installiert nicht die Komponente Microsoft .NET Framework.

  ANMERKUNG: .NET Framework 4.6 (oder höher) ist bei Ausführung im FIPS-Modus erforderlich.

- Das Master-Installationsprogramm installiert die folgenden benötigten Komponenten, falls sie auf Ihrem Computer nicht bereits installiert sind. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponente installieren, bevor Sie Encryption installieren.

Voraussetzungen
○ Visual C++ 2012 Update 4 oder höheres Redistributable Package (x86 oder x64) ○ Visual C++ 2017 Update 3 oder höheres Redistributable Package (x86 oder x64) ○ Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt.

Hardware

- Die folgende Tabelle enthält Informationen zu den Mindestanforderungen unterstützter Computer-Hardware.

Hardware
○ Intel Pentium- oder AMD-Prozessor ○ 110 MB verfügbarer Speicherplatz ○ 512 MB RAM

Hardware
ANMERKUNG: Zum Verschlüsseln der Dateien am Endpunkt ist zusätzlicher freier Speicherplatz erforderlich. Diese Größe variiert auf Grundlage von Richtlinien und der Kapazität der Festplatte.

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

Optionale integrierte Hardware
○ TPM 1.2 oder 2.0

Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

Windows-Betriebssysteme (32-Bit und 64-Bit)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (November 2019 Update/19H2 – November 2022 Update/ 22H2) **Hinweis:** OEMs und ODMs liefern Windows 10 v2004 (Mai 2020 Update/20H1 und höher) nicht mit 32-Bit-Architektur. Weitere Informationen finden Sie unter https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Betriebssysteme – Encryption External Media

- Zur Verwendung von Encryption External Media müssen ungefähr 55 MB auf dem Wechseldatenträger frei sein. Des Weiteren muss die Größe des freien Speicherplatzes der Größe der umfangreichsten zu verschlüsselnden Datei entsprechen.
- Im Folgenden ist aufgelistet, welche Betriebssysteme beim Zugriff auf Dell-geschützte Medien unterstützt werden.

Unterstützte Windows-Betriebssysteme für den Zugriff auf verschlüsselte Medien (32-Bit und 64-Bit)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (November 2019 Update/19H2 – November 2022 Update/ 22H2) **Hinweis:** OEMs und ODMs liefern Windows 10 v2004 (Mai 2020 Update/20H1 und höher) nicht mit 32-Bit-Architektur. Weitere Informationen finden Sie unter https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Unterstützte Mac-Betriebssysteme für den Zugriff auf verschlüsselte Medien (64-Bit-Kernel)
○ macOS High Sierra 10.13.5 – 10.13.6 ○ macOS Mojave 10.14.0–10.14.4 ○ macOS Catalina 10.15.5 – 10.15.6

Lokalisierung

- Encryption ist MUI-konform und in den folgenden Sprachen lokalisiert.

Sprachunterstützung	
○ EN: Englisch	○ JA: Japanisch
○ ES: Spanisch	○ KO: Koreanisch
○ FR: Französisch	○ PT-BR: Portugiesisch, Brasilien
○ IT: Italienisch	○ PT-PT: Portugiesisch, Portugal
○ DE: Deutsch	

SED Manager

- IPv6 wird nicht unterstützt.
- Nach der Übernahme von Richtlinien, die nun angewendet werden sollen, müssen Sie den Computer u. U. herunterfahren und neu starten.
- Computer, die mit selbstverschlüsselnden Laufwerken ausgerüstet sind, können nicht mit HCA-Karten verwendet werden. Sie sind nicht kompatibel, was die Bereitstellung der HCA verhindert. Dell verkauft keine Computer mit selbstverschlüsselnden Laufwerken, die das HCA-Modul unterstützen. Eine solche Konfiguration wäre nur als After-Market-Konfiguration möglich.
- Wenn der zu verschlüsselnde Computer über eine selbstverschlüsselnde Festplatte verfügt, muss in Active Directory die Option *Nutzer muss das Kennwort bei der nächsten Anmeldung ändern* deaktiviert sein. Die Preboot-Authentifizierung bietet keine Unterstützung für diese Active Directory-Option.
- Der SED Manager wird nicht mit Konfigurationen mit mehreren Laufwerken unterstützt.
- **ANMERKUNG:**

  Aufgrund der Struktur von RAID und SEDs wird RAID vom SED Manager nicht unterstützt. Das Problem bei *RAID=On* mit SEDs besteht darin, dass zum Lesen und Schreiben der RAID-Daten Zugriff auf einen höheren Sektor erforderlich ist. Dieser Sektor ist auf einem gesperrten SED beim Start nicht verfügbar, und RAID benötigt diese Daten bereits vor der Nutzeranmeldung. Sie können das Problem umgehen, indem Sie im BIOS für SATA statt *AHCI* den Eintrag *RAID=On* auswählen. Wenn die Treiber für den AHCI-Controller im Betriebssystem nicht bereits vorinstalliert sind, führt der Wechsel von *RAID=On* zu *AHCI* allerdings zum Betriebssystemabsturz.

- Das Master-Installationsprogramm installiert die folgenden benötigten Komponenten, falls sie auf Ihrem Computer nicht bereits installiert sind. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponente installieren, bevor Sie die SED Manager installieren.

Voraussetzungen
○ Visual C++ 2017 Update 3 oder höheres Redistributable Package (x86 oder x64)
○ Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt.

- Die Konfiguration von selbstverschlüsselnden Laufwerken für SED Manager weicht bei NVMe- und Nicht-NVMe-Laufwerken (SATA) folgendermaßen ab:
  - NVMe-Laufwerke, die für PBA genutzt werden:
    - Wenn das Dell Gerät 2018 oder später hergestellt wurde: Entweder „RAID EIN“ oder „AHCI“ können mit NVMe-Laufwerken genutzt werden.
    - Der BIOS-Startmodus muss auf „Unified Extensible Firmware Interface (UEFI)“ eingestellt werden. Legacy-Vorgangs-ROMs müssen deaktiviert sein.
  - Nicht-NVMe-Laufwerke, die für PBA genutzt werden:
    - Der BIOS-SATA-Betrieb kann entweder auf AHCI oder RAID ON eingestellt werden.
    - Das Betriebssystem stürzt ab, wenn es von RAID EIN auf AHCI umgeschaltet wird, wenn den AHCI-Controller-Treiber nicht vorinstalliert wurde. Eine Anleitung zum Umschalten von RAID auf AHCI (oder umgekehrt) finden Sie im KB-Artikel 124714.

Unterstützte Opal-konforme SEDs erfordern aktualisierte Intel Rapid Storage Technology-Treiber, die unter www.dell.com/support verfügbar sind. Dell empfiehlt den neuesten Intel Rapid Storage Technology-Treiber mit NVMe-Laufwerken.

ANMERKUNG: Die Intel Rapid Storage Technology-Treiber sind plattformabhängig. Sie können Ihren Systemtreiber basierend auf Ihrem Computermodell unter dem Link oben finden.

- Verschlüsselungskonfigurationen für mehrere Festplatten mit SED Manager setzen Folgendes voraus:
  - Alle Festplatten im Zielsystem müssen SEDS sein.
  - Alle Festplatten im Zielsystem müssen im gleichen Startmodus konfiguriert werden.
  - Im UEFI-Startmodus kann das Betriebssystem auf jeder Zielfestplatte installiert werden.
  - Im Legacy-Startmodus muss das Betriebssystem auf der ersten Festplatte installiert werden (Festplattenr. 0). Wenn das Betriebssystem nicht auf der ersten Festplatte installiert ist, ist die Verschlüsselung mehrerer Festplatten deaktiviert.
- Einige BIOS-Versionen können blockbasierte SID standardmäßig aktivieren, wodurch SED Manager blockiert werden kann. Weitere Informationen finden Sie im KB-Artikel 126083.
- Direkte Funktionsupdates von Windows 10 v1607 (Anniversary Update/Redstone 1) auf Windows 10 v1903 (May 2019 Update/19H1) werden von Dell Encryption nicht unterstützt. Dell empfiehlt beim Update auf Windows 10 v1903 das Betriebssystem auf ein neueres Funktionsupdate zu aktualisieren. Beim Versuch, direkt von Windows 10 v1607 auf v1903 zu aktualisieren, wird eine Fehlermeldung angezeigt und das Update wird verhindert.
- **ANMERKUNG:** Bei der Preboot-Authentifizierung ist ein Kennwort erforderlich. Dell empfiehlt, ein Kennwort mit mindestens 9 Zeichen festzulegen.

- **ANMERKUNG:** Ein Kennwort ist für alle im Bereich *Nutzer hinzufügen* hinzugefügten Nutzer erforderlich. Nutzer von Kennwörter mit einer Länge von null werden nach der Aktivierung aus dem Computer ausgesperrt.
- **ANMERKUNG:** Durch SED Manager geschützte Computer müssen auf Windows 10 v1703 (Creators Update/Redstone 2) aktualisiert werden, bevor eine Aktualisierung auf Windows 10 v1903 (May 2019 Update/19H1) oder höher durchgeführt werden kann. Beim Versuch, ein direktes Betriebssystem-Update durchzuführen, wird eine Fehlermeldung angezeigt.
- Für SED Manager müssen Windows-Kennwortänderungen und Datenverschlüsselungsschlüssel mit dem nutzerdefinierten Dell Zugangsdatenanbieter synchronisiert werden. Wenn Sie Anwendungen von Drittanbietern verwenden möchten, die nutzerdefinierte Zugangsdatenanbieter verwenden, die auf von SED Manager geschützten Computern ausgeführt werden, müssen Sie Windows-Kennwortänderungen über die Data Security Console initiieren. Weitere Informationen zum Ändern Ihres Kennworts in der Data Security Console finden Sie im Kapitel *Kennwort* im Benutzerhandbuch für die Data Security Console.

Hardware

- Für die aktuellste Liste Opal-kompatibler SEDs, die mit SED Manager unterstützt werden, lesen Sie KB-Artikel: 126855.
- Für die aktuellste Liste von Plattformen, die mit SED Manager unterstützt werden, lesen Sie KB-Artikel: 126855.
- Eine Liste der Docking-Stationen und Adapter, die von SED Manager unterstützt werden, finden Sie im KB-Artikel 124241.

Internationale Tastaturen

Die folgende Tabelle listet unterstützte internationale Tastaturen mit Preboot-Authentifizierung auf UEFI- und Nicht-UEFI-Computern.

International Keyboard Support - UEFI	
DE-FR – (Französisch – Schweiz)	EN-GB – Englisch (Britisches Englisch)
DE-CH – (Deutsch – Schweiz)	EN-CA – Englisch (Kanadisches Englisch)
EN-US – Englisch (Amerikanisches Englisch)	

Internationale Tastatur-Unterstützung – Nicht-UEFI	
AR – Arabisch (mit lateinischen Buchstaben)	EN-US – Englisch (Amerikanisches Englisch)
DE-FR – (Französisch – Schweiz)	EN-GB – Englisch (Britisches Englisch)
DE-CH – (Deutsch – Schweiz)	EN-CA – Englisch (Kanadisches Englisch)

Betriebssysteme

- Die folgende Tabelle enthält Informationen zu den unterstützten Betriebssystemen.

Windows-Betriebssysteme (32-Bit und 64-Bit)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (November 2019 Update/19H2 – November 2022 Update/ 22H2) **Hinweis:** OEMs und ODMs liefern Windows 10 v2004 (Mai 2020 Update/20H1 und höher) nicht mit 32-Bit-Architektur. Weitere Informationen finden Sie unter https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Authentication-Funktionen stehen nur dann zur Verfügung, wenn die Preboot-Authentifizierung aktiviert ist.

Lokalisierung

SED Manager ist MUI-konform und in den folgenden Sprachen lokalisiert. UEFI-Modus und Preboot-Authentifizierung werden in den folgenden Sprachen unterstützt:

Sprachunterstützung	
● EN: Englisch	● JA: Japanisch
● FR: Französisch	● KO: Koreanisch
● IT: Italienisch	● PT-BR: Portugiesisch, Brasilien
● DE: Deutsch	● PT-PT: Portugiesisch, Portugal
● ES: Spanisch	

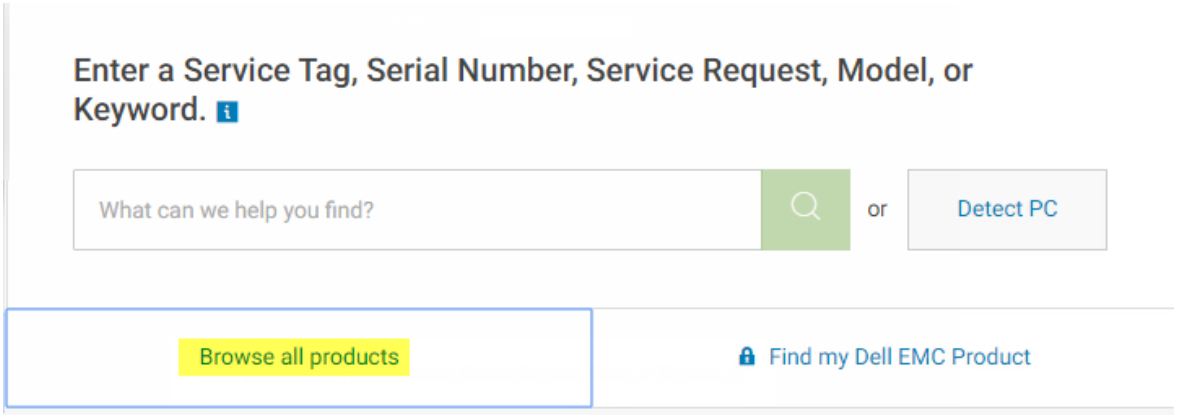
3

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 **Alle Produkte durchsuchen** aus.



2. Wählen Sie **Sicherheit** aus der Produktliste aus.
3. Wählen Sie **Dell Data Security** aus.

   Wenn diese Auswahl einmal vorgenommen wurde, wird sie von der Website gespeichert.
4. Wählen Sie das Dell Produkt.

   Beispiele:

   Dell Encryption Enterprise

   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 Übereinstimmungen **Dell Encryption** aus. Da es sich hierbei nur um ein Beispiel handelt, wird es sich wahrscheinlich ein wenig anders darstellen. Beispielsweise stehen möglicherweise keine vier Dateien zur Auswahl.
8. Klicken Sie auf **Herunterladen**.

   Fahren Sie mit Encryption Personal installieren fort.

4

Damit ist die Installation

Sie können Encryption Personal mit dem Master-Installationsprogramm (empfohlen) oder einzeln installieren, indem Sie die untergeordneten Installationsprogramme aus dem Master-Installationsprogramm extrahieren. In jedem Fall kann Encryption Personal 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:

ANMERKUNG: Wenn die richtlinienbasierte Verschlüsselung vor dem Encryption Management Agent installiert wird, kann es zu einem Computerabsturz kommen. Dieses Problem wird durch einen Fehler beim Laden des Verschlüsselungs-Standby-Treibers verursacht, der die PBA-Umgebung verwaltet. Um dieses Problem zu umgehen, verwenden Sie das Master-Installationsprogramm oder stellen Sie sicher, dass die richtlinienbasierte Verschlüsselung nach dem Encryption Management Agent installiert ist.

- Informationen zur Verwendung der Funktionen von Encryption finden Sie in der *Dell Encrypt Hilfe*. Greifen Sie auf die Hilfe über `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help` zu.
- In der *Encryption External Media Hilfe* finden Sie die Funktionen von Encryption External Media. Greifen Sie auf die Hilfe über `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption` zu.
- In der Encryption Personal erfahren Sie, wie Sie die Funktionen von Advanced Authentication verwenden. Greifen Sie auf die Hilfe über `<Install dir>\Program Files\Dell\Dell Data Protection\Security Tools\Help` zu.

Berechtigung importieren

Die Installation von Encryption Personal erfordert einen Registrierungsschlüssel auf dem Zielcomputer. Dieser Registrierungsschlüssel wird über die Befehlszeilenschnittstelle während der Installation oder über die GUI vor der Installation hinzugefügt.

Informationen zum Hinzufügen des Registrierungsschlüssels über die Befehlszeilenschnittstelle finden Sie unter Installieren mithilfe der Befehlszeile.

So fügen Sie den Registrierungsschlüssel über die GUI hinzu:

1. Öffnen Sie einen Texteditor.
2. Fügen Sie den folgenden Text hinzu.

   ```
   [HKEY_LOCAL_MACHINE\Software\Dell\Dell Data Protection\Entitlement]

   "SaEntitlement"="1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-
   XXXXXXXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX="
   ```

3. Speichern Sie die Textdatei mit der Erweiterung `.reg`.
4. Doppelklicken Sie auf die gespeicherte Registrierungsdatei, um die Berechtigung Encryption Personal zu importieren.

Installationsverfahren auswählen

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

- Interaktiv installieren – empfohlen
- Installation über die Befehlszeile

Interaktive Installation

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

- Das Master-Installationsprogramm installiert mehrere Clients. Im Fall von Encryption Personal installiert es Encryption und die SED-Verwaltung.
- Die Protokolldateien des Master-Installationsprogramms befinden sich unter `C:\ProgramData\Dell\Dell Data Protection\Installer`.

1. Falls nötig, installieren Sie die Befugnis auf dem Zielcomputer. Anweisungen zum Hinzufügen der Befugnis auf dem Computer sind in der E-Mail mit Lizenzinformationen enthalten.
2. Kopieren Sie DDSSetup.exe auf den lokalen Computer.
3. Doppelklicken Sie auf DDSSetup.exe, um das Installationsprogramm aufzurufen.
4. Es wird ein Dialogfeld angezeigt, das Sie auf den Installationsstatus von Voraussetzungen aufmerksam macht. Dieser Vorgang kann einige Minuten dauern.
5. Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.
6. Lesen Sie die Lizenzvereinbarung, stimmen Sie den Bedingungen zu, und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Weiter** für die Installation von Encryption Personal im Standardverzeichnis von `C:\Program Files\Dell\Dell Data Protection\`.
8. Authentication wird standardmäßig installiert und kann nicht deaktiviert werden. Im Installer sind sie unter Security Framework aufgeführt.

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

   Ein Statusfenster wird angezeigt. Dieser Vorgang kann mehrere Minuten dauern.
10. Wählen Sie **Ja, ich möchte meinen Computer jetzt neu starten** aus, und klicken Sie dann auf **Fertigstellen**.
11. Wenn der Computer neu gestartet wird, authentifizieren Sie sich bei Windows.

Die Installation von Encryption Personal und Advanced Authentication ist abgeschlossen.

Der Encryption Personal Setup-Assistent und die Konfiguration werden separat beschrieben.

Starten Sie die Encryption Personal-Administratorkonsole nachdem der Encryption Personal-Installationsassistent und die Konfiguration abgeschlossen wurde.

Im Rest des Abschnitts werden weitere Installationsaufgaben beschrieben, die Sie überspringen können. Fahren Sie mit dem Advanced Authentication- und Encryption Personal-Installationsassistenten fort.

Installation über die Befehlszeile

Um Encryption Personal 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.

- Falls nötig, installieren Sie die Befugnis auf dem Zielcomputer.
- **ANMERKUNG:** Dell Encryption-Protokolle geben nicht an, ob eine Installation aufgrund unzureichenden Speicherplatzes fehlschlägt.
- 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
/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
ENTITLEMENT=1:PE:{hier Berechtigungsschlüssel für Encryption Personal} **ANMERKUNG:** Dieser Parameter kann **nur** mit Encryption Personal verwendet werden

- Beispiel einer Installation über die Befehlszeile

  Der Neustart wurde in den Befehlszeilenbeispielen unterdrückt. Es ist jedoch ein abschließender Neustart erforderlich.

  Die richtlinienbasierte 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 Encryption client installiert (automatische Installation, kein Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`), wobei der Berechtigungsschlüssel direkt an das Installationsprogramm weitergegeben wird.

  DDPE_XXbit_setup.exe /s /v"ENTITLEMENT=1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-XXXXX-XXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX= /l*v c:\Shieldinstall.log /qn /norestart"

- Im folgenden Beispiel werden Encryption Personal und Advanced Authentication installiert (automatische Installation, kein Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE\""
  ```

- Im folgenden Beispiel wird Encryption Personal und Advanced Authentication installiert (automatische Installation, kein Neustart, Installation an einem alternativen Speicherort `C:\Program Files\Dell\My_New_Folder`).

  ```
  DDSSetup.exe /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 Encryption Personal und Advanced Authentication ist abgeschlossen.

  Der Encryption Personal Setup-Assistent und die Konfiguration werden separat beschrieben.

  Starten Sie die Encryption Personal-Administratorkonsole nachdem der Encryption Personal-Installationsassistent und die Konfiguration abgeschlossen wurde.

  Im Rest des Abschnitts werden weitere Installationsaufgaben beschrieben, die Sie überspringen können. Fahren Sie mit dem Advanced Authentication- und Personal Edition-Installationsassistenten fort.

5

Advanced Authentication- und Encryption Personal-Installationsassistenten

Melden Sie sich mit Ihrem Windows-Nutzernamen 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 Advanced Authentication 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**.

   Hinweis: Das Administrator-Kennwort für die Verschlüsselung muss mindestens acht Zeichen lang sein und darf 127 Zeichen nicht überschreiten.
4. Geben Sie zum Speichern der Wiederherstellungsinformationen einen auf einem Netzwerk oder Wechselmedien gelegenen Speicherpfad ein und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Anwenden**, um mit der Aktivierung von Advanced Authentication zu beginnen.

   Nachdem der Aktivierungsassistent von Advanced Authentication abgeschlossen wurde, fahren Sie mit dem nächsten Schritt fort.
6. Starten Sie den Installationsassistenten für Encryption Personal über das Dell Encryption-Symbol im Infobereich (kann auch selbständig starten).

   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 Local 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 8 bis 127 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 Advanced Authentication 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**.

   Hinweis: Das Administrator-Kennwort für die Verschlüsselung muss mindestens acht Zeichen lang sein und darf 127 Zeichen nicht überschreiten.
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**" oben rechts in der lokalen Managementkonsole oder auf **Start > Dell > 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 „Konform“ bezeichnet.

6

Konfigurieren der Konsoleneinstellungen

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

Um Funktionen der erweiterten Authentifizierung zu konfigurieren, müssen Sie auf dem Computer Administratorrechte besitzen.

Administrator-Passwort und Sicherungsverzeichnis ändern

Nach der Aktivierung der erweiterten Authentifizierung können das Administratorpasswort und der Speicherort der Sicherungsdatei bei Bedarf geändert werden.

1. Starten Sie als Administrator die Dell Data Security Console 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-Sicherungslaufwerk nicht angeschlossen ist), fordert Advanced Authentication zur Eingabe eines Speicherorts für die Sicherung der Daten auf. Damit die Verschlüsselung starten kann, ist der Zugriff auf die Wiederherstellungsdaten erforderlich.

Pre-Boot-Authentifizierung konfigurieren

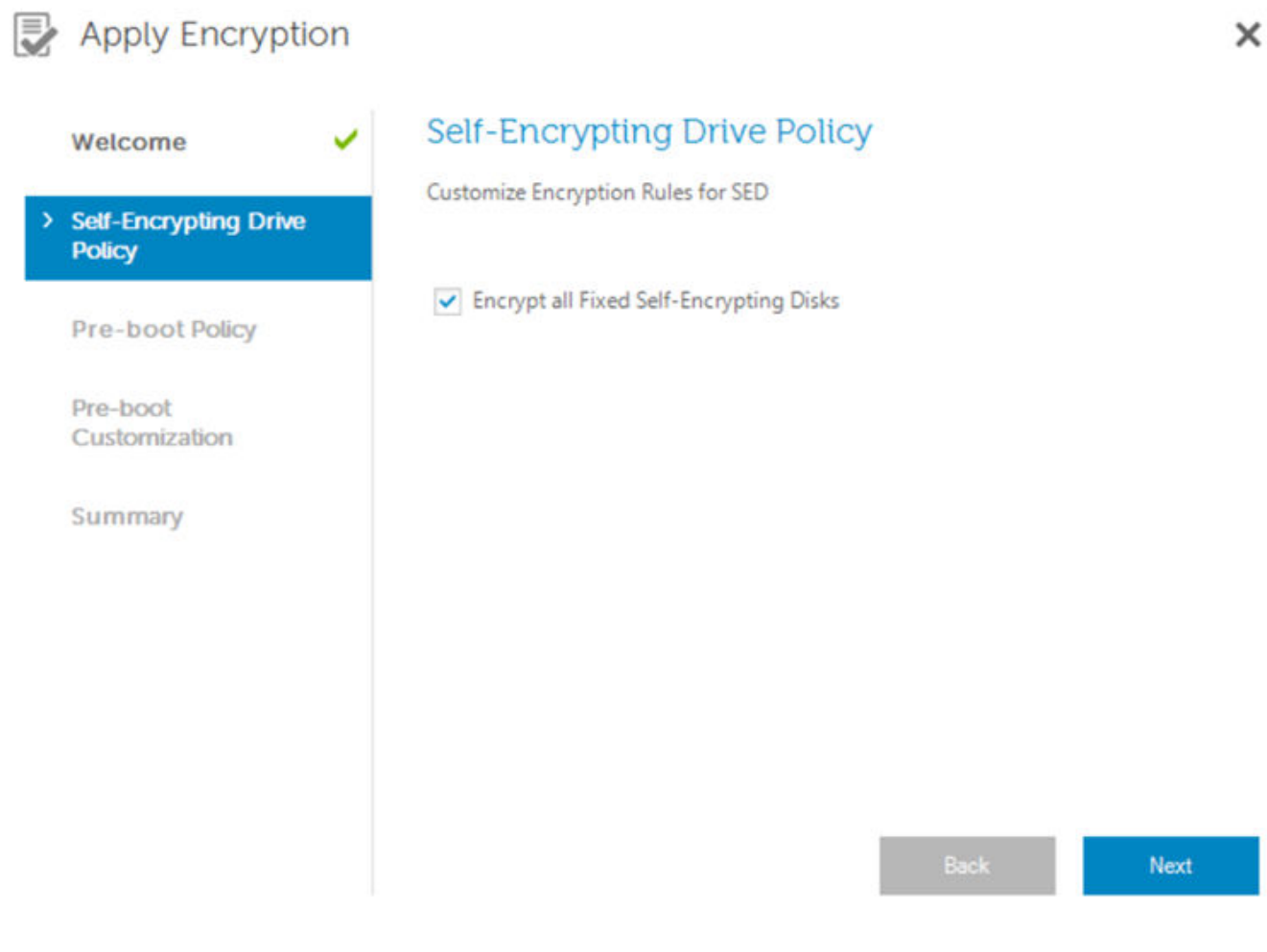
PBA ist verfügbar, wenn Ihr Computer mit einem SED ausgestattet ist. PBA wird über die Encryption-Registerkarte konfiguriert. Wenn SED Manager Ownership von SED übernimmt, wird PBA aktiviert.

SED Management aktivieren:

1. Klicken Sie in der Data Security Console auf die Schaltfläche **Administratoreinstellungen**.
2. Stellen Sie sicher, dass der Speicherort der Sicherungsdatei auf Ihrem Computer zugänglich ist.

   Wird *Speicherort nicht gefunden* angezeigt und ist der Speicherort ein USB-Laufwerk, ist entweder Ihr USB-Laufwerk nicht angeschlossen oder mit einem anderen als dem Steckplatz verbunden, den Sie beim Sichern verwendet haben. Wird die Meldung angezeigt, obwohl sich der Speicherort auf einem Netzwerklaufwerk befindet, ist das Netzwerklaufwerk von dem Computer aus nicht zugänglich. Der Speicherort der Sicherungsdatei muss über die Registerkarte **Administratoreinstellungen** geändert werden, indem Sie auf **Speicherort der Sicherungsdatei ändern** klicken und als Speicherort den aktuellen Steckplatz oder ein zugängliches Laufwerk auswählen. Wenige Sekunden nach der Neuzuweisung des Speicherorts kann die Verschlüsselung fortgesetzt werden.

3. Klicken Sie auf die Registerkarte **Verschlüsselung** und dann auf **Verschlüsseln**.
4. Auf der Willkommensseite klicken Sie auf **Weiter**.
5. Wählen Sie **Alle feststehenden selbstverschlüsselnden Festplatten verschlüsseln** aus, um die Multi-Disk-Verschlüsselung zu aktivieren.



6. Ändern oder bestätigen Sie auf der Seite „Preboot-Richtlinien“ die folgenden Werte und klicken Sie dann auf **Weiter**.

Versuche mit nicht gespeicherter Nutzeranmeldung	Höchstzahl der Anmeldeversuche durch einen unbekannten Nutzer (damit ist ein Nutzer gemeint, der sich bisher noch nicht beim Computer angemeldet hat [für den noch keine Anmeldedaten gespeichert sind]).
Versuche mit gespeicherter Nutzeranmeldung	Höchstzahl der Anmeldeversuche durch einen bekannten Nutzer.
Versuche beim Beantworten von Wiederherstellungsfragen	Anzahl der Versuche, die ein Nutzer für die Eingabe der richtigen Antwort hat.
Crypto Erase-Passwort aktivieren	Markieren Sie die Option, um sie zu aktivieren.
Crypto Erase-Passwort eingeben	Ein Wort oder Code mit bis zu 100 Zeichen als ausfallsichere Sicherheitsmaßnahme. Die Eingabe dieses Wortes oder Codes in das Nutzer- oder Kennwortfeld während der Preboot-Authentifizierung löst eine Crypto-Erase-Aktion aus, die die Schlüssel aus dem sicheren Speicher entfernt. Nachdem dieser Prozess aufgerufen wird, ist das Laufwerk nicht mehr wiederherstellbar. Lassen Sie dieses Feld leer, wenn Sie für den Notfall kein Crypto Erase-Passwort verfügbar haben wollen.

	Lassen Sie dieses Feld leer, wenn Sie für den Notfall kein Crypto Erase-Passwort verfügbar haben wollen.
Angemeldet bleiben	Aktiviert oder deaktiviert die Funktion für Nutzer, mit der Sie auf dem Anmeldebildschirm von PBA die Anmeldedaten speichern können.

7. Geben Sie auf der Seite „Preboot-Anpassungen“ den nutzerdefinierten Text ein, der auf dem Preboot-Authentifizierungsbildschirm (PBA) angezeigt werden soll, und klicken Sie dann auf **Weiter**.

Preboot-Titeltext	Dieser Text erscheint oben auf dem PBA-Bildschirm. Wenn Sie dieses Feld leer lassen, wird kein Titel angezeigt. Der Text wird nicht umgebrochen und kann daher bei Eingabe von mehr als 17 Zeichen abgeschnitten werden.
Text für Support-Informationen	Text, der auf dem Bildschirm mit den Informationen zum PBA-Support angezeigt wird. Geben Sie in der Meldung spezifische Anweisungen an, wie der Nutzer sich an einen Helpdesk oder Sicherheitsadministrator wenden kann. Wenn in diesem Feld kein Text eingegeben wird, stehen dem Nutzer keine Kontaktangaben für den Support zur Verfügung. Textumbruch erfolgt auf Wortebene, nicht auf Zeichenebene. Wenn ein einzelnes Wort mit etwa 50 Zeichen vorliegt, wird es nicht umgebrochen und es wird keine Bildlaufleiste angezeigt. Der Text wird also abgeschnitten.
Text des Rechtshinweises	Dieser Text wird angezeigt, bevor sich der Nutzer bei dem Gerät anmelden darf. Beispiel: „Durch Klicken auf OK verpflichten Sie sich, die Richtlinie für eine angemessene Nutzung des Computers einzuhalten.“ Wenn in diesem Feld kein Text eingegeben wird, werden kein Text und keine OK/Abbrechen-Schaltfläche angezeigt. Textumbruch erfolgt auf Wortebene, nicht auf Zeichenebene. Wenn z. B. ein einzelnes Wort mit mehr als etwa 50 Zeichen vorliegt, wird es nicht umgebrochen, und es wird keine Bildlaufleiste angezeigt. Der Text wird also abgeschnitten.

8. Klicken Sie auf der Zusammenfassungsseite auf **Übernehmen**.
9. Klicken Sie auf **Herunterfahren**, wenn Sie dazu aufgefordert werden.

   Um mit der Verschlüsselung zu beginnen, muss der Computer vollständig heruntergefahren werden.

10. Starten Sie den Computer dann erneut.

    Die Authentifizierung wird jetzt vom Encryption Management Agent verwaltet. Nutzer müssen sich auf dem PBA-Bildschirm mit ihrem Windows-Passwort anmelden.

Ändern der Einstellungen für SED-Verwaltung und PBA

Nachdem Sie die Verschlüsselung zum ersten Mal aktiviert und die Preboot-Richtlinie und -Anpassung konfiguriert haben, stehen Ihnen auf der Registerkarte „Encryption“ folgende Optionen zur Verfügung:

- Preboot-Richtlinie oder -Anpassung ändern – Klicken Sie auf die Registerkarte **Encryption** und dann auf **Ändern**.
- Die SED-Verwaltung deaktivieren, beispielsweise zur Deinstallation: Klicken Sie auf **Entschlüsseln**.

Nachdem Sie die SED-Verwaltung zum ersten Mal aktiviert und die Preboot-Richtlinie und -Anpassung konfiguriert haben, stehen Ihnen auf der Registerkarte „Preboot-Einstellungen“ folgende Optionen zur Verfügung:

- Preboot-Policy oder -Anpassung ändern – Klicken Sie auf die Registerkarte **Preboot-Einstellungen** und wählen Sie **Policy zu selbstverschlüsselnden Festplatten**, **Preboot-Einstellungen** oder **Preboot-Anpassungen** aus.

Benutzer und Benutzerauthentifizierung verwalten

Hinzufügen eines Benutzers

Windows-Benutzer werden automatisch zu Encryption Personal-Benutzern, wenn sie sich entweder bei Windows anmelden oder eine Anmeldeinformation eintragen.

Der Computer muss mit der Domain verbunden sein, damit ein Domainbenutzer in der Data Security Console über die Registerkarte „Benutzer hinzufügen“ hinzugefügt werden kann.

1. Wählen Sie im linken Bereich des Administratoreinstellungstools **Benutzer** aus.
2. Klicken Sie rechts oben in der Seite „Benutzer“ auf **Benutzer hinzufügen**, um den Registrierungsvorgang für einen vorhandenen Windows-Benutzer zu starten.
3. Wählen Sie im Dialogfeld „Benutzer auswählen“ die Option **Objekttypen** aus.
4. Geben Sie in das Textfeld den Objektnamen eines Benutzers ein und klicken Sie auf **Namen überprüfen**.
5. Klicken Sie anschließend auf **OK**.

Benutzer löschen

1. Wählen Sie im linken Bereich des Administratoreinstellungstools **Benutzer** aus.
2. Um einen Benutzer zu löschen, wählen Sie die Spalte des Benutzers aus und klicken Sie auf **Entfernen**. (Scrollen Sie ans Ende der Benutzer-Spalte, um die Löschoptionen zu sehen.)

Alle eingetragenen Eintragungen eines Benutzers entfernen

1. Klicken Sie auf die Kachel **Administrator-Einstellungen** und authentifizieren Sie sich mit Ihrem Kennwort.
2. Klicken Sie auf die Registerkarte **Benutzer**, und machen Sie den Benutzer ausfindig, den Sie entfernen möchten.
3. 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.

7

Deinstallation 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. Encryption Management Agent deinstallieren.

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

Interaktiv deinstallieren

1. Gehen Sie auf *Programm deinstallieren* in der Windows-Systemsteuerung (geben Sie in das Suchfeld der Taskleiste **Systemsteuerung** ein, wählen Sie dann „Systemsteuerung“ aus den Ergebnissen).
2. Markieren Sie **Dell Installationsprogramm** 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. Folgen Sie den Eingabeaufforderungen zur Deinstallation, und klicken Sie dann auf **Fertigstellen**.
5. 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.

  ```
  "DDSSetup.exe" /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

- Dell empfiehlt die Verwendung des Data Security Deinstallationsprogramms zum Entfernen von Encryption Personal.
- 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 Encryption Personal 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 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.

  ANMERKUNG: Stellen Sie vor der Deinstallation sicher, dass alle Richtlinienvorlagen auf „Deaktiviert“ gesetzt sind und setzen Sie zur ordnungsgemäßen Entschlüsselung alle verschlüsselten externen Datenträger ein.

  In diesem Video wird erläutert, wie Sie Richtlinienvorlagen in der lokalen Verwaltungskonsole ändern können.
- 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:

- Interaktiv deinstallieren
- Deinstallation von der Befehlszeile aus

Interaktiv deinstallieren

1. Gehen Sie auf *Programm deinstallieren* in der Windows-Systemsteuerung (geben Sie in das Suchfeld der Taskleiste **Systemsteuerung** ein und wählen Sie dann **Systemsteuerung** aus den Ergebnissen).
2. Markieren Sie **Dell Encryption XX-bit** und klicken Sie mit der linken Maustaste auf **Ändern**, um den Installationsassistenten für Encryption Personal zu starten.
3. Lesen Sie die Informationen im Begrüßungsbildschirm, und klicken Sie auf **Weiter**.
4. Wählen Sie auf dem Bildschirm „Installation von Encryption Removal Agent“ eine der beiden folgenden Optionen aus:

ANMERKUNG: 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**.

5. Geben Sie in *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 Administrator-Kennwort für die Verschlüsselung ein. Dies ist das Kennwort vom Installationsassistenten bei der Installation der Software.

   Klicken Sie auf **Weiter**.

6. Wählen Sie unter *Dell Decryption Agent-Dienstanmeldung* **Lokales Systemkonto** und klicken Sie auf **Fertigstellen**.
7. Klicken Sie auf dem Bildschirm „Programm entfernen“ auf **Entfernen**.
8. Klicken Sie auf dem Bildschirm „Konfiguration abgeschlossen“ auf **Fertigstellen**.
9. 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:\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 `C:\<any directory>\<any log file name>.log`. 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 nur ! und - nach /qb.

Schalter	Erläuterung
/v	Gibt Variablen an die .msi-Datei innerhalb der setup.exe-Datei weiter

Schalter	Erläuterung
/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 – Leise: erforderlich bei msiexec-Variablen, die /q oder /qn enthalten. 0 – nicht leise: nur möglich, wenn msiexec-Variablen mit /q nicht in der Befehlszeilensyntax vorhanden sind
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.

Encryption Management Agent deinstallieren

Deinstallationsverfahren auswählen

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

- Interaktiv deinstallieren
- Deinstallation von der Befehlszeile aus

Interaktiv deinstallieren

1. Gehen Sie auf *Programm deinstallieren* in der Windows-Systemsteuerung (geben Sie in das Suchfeld der Taskleiste **Systemsteuerung** ein und wählen Sie dann **Systemsteuerung** aus den Ergebnissen).
2. Markieren Sie **Dell Encryption Management Agent** 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. Folgen Sie den Eingabeaufforderungen zur Deinstallation, und klicken Sie dann auf **Fertigstellen**.
5. 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 Encryption Management Agent-Installationsprogramm unter `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- Im folgenden Beispiel wird die SED-Verwaltung 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.

9

Data Security-Deinstallationsprogramm

Deinstallieren von Encryption Personal

Dell liefert das Deinstallationsprogramm von Data Security als Master-Deinstallationsprogramm. Dieses Dienstprogramm sammelt die derzeit installierten Produkte und entfernt diese in der entsprechenden Reihenfolge.

Dieses Deinstallationsprogramm für die Datensicherheit ist verfügbar in: `C:\Program Files (x86)\Dell\Dell Data Protection`

Für weitere Informationen oder für die Verwendung der Befehlszeilenoberfläche (CLI) siehe KB-Artikel 125052.

Protokolle werden in `C:\ProgramData\Dell\Dell Data Protection\` für alle Komponenten erzeugt, die entfernt werden.

Um das Dienstprogramm auszuführen, öffnen Sie den Ordner, in dem es enthalten ist, klicken mit der rechten Maustaste auf **DataSecurityUninstaller.exe** und wählen **Als Administrator ausführen**.

Klicken Sie auf **Weiter**.

Optional löschen Sie eine beliebige Anwendung vom Entfernen und klicken auf **Weiter**.

Erforderliche Abhängigkeiten werden automatisch ausgewählt oder gelöscht.

Um Anwendungen ohne vorherige Installation des Encryption Removal Agent zu entfernen, wählen Sie **Encryption Removal Agent nicht installieren** und anschließend **Weiter**.

Wählen Sie **Encryption Removal Agent – Schlüssel aus einer Datei importieren** und anschließend **Weiter**.

Navigieren Sie zum Speicherort der Wiederherstellungsschlüssel und geben Sie dann die Passphrase für die Datei ein, bevor Sie auf **Weiter** klicken.

Wählen Sie **Entfernen,** um den Deinstallationsvorgang zu starten.

Klicken Sie auf **Fertigstellen**, um das Entfernen abzuschließen, und starten Sie den Computer neu. **Rechner nach dem Klicken auf Fertig stellen neu starten** ist standardmäßig ausgewählt.

Deinstallation und Entfernen sind abgeschlossen.

Beschreibungen von Richtlinien und Vorlagen

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

Richtlinien

Richtlinie	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 richtlinienbasierte 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

Richtlinie	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
SDE-Verschlüsselungsregeln										Verschlüsselungsregeln, die bei der Verschlüsselung bzw. beim Ausschluss der Verschlüsselung bestimmter 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.

Richtlinie	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
										Die verfügbaren Laufwerksbuchstaben heißen: #: bezieht sich auf alle Laufwerke f#: Bezieht sich auf alle Festplattenlaufwerke #: 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 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									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

Richtlinie	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
	wordpad.exe winzip.exe winrar.exe onenote.exe onenotem.exe									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. 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, 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

Richtlinie	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
Anwendungsdaten-Verschlüsselungsschlüssel	Allgemein									Gemeinsam oder Benutzer Wählen Sie einen Schlüssel aus, um anzugeben, wer wo auf Dateien zugreifen kann, die durch die Anwendungsdaten-Verschlüsselungsliste verschlüsselt sind. „Allgemein“, damit diese Dateien für alle verwalteten Benutzer auf dem Endpunkt, auf dem sie erstellt wurden, zugänglich sind (gleiche Zugriffsstufe wie allgemein verschlüsselte Ordner) und mit dem allgemeinen Verschlüsselungsalgorithmus verschlüsselt werden. „Benutzer“, damit diese Dateien nur für den Benutzer, der sie erstellt hat, auf dem Endpunkt, auf dem sie erstellt wurden, zugänglich sind (gleiche Zugriffsstufe wie benutzerverschlüsselte Ordner) und mit dem Benutzerverschlüsselungsalgorithmus verschlüsselt werden. 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	Wahr							Falsch		Mit „Wahr“ werden die Pfade in den Umgebungsvariablen

Richtlinie	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
verschlüsseln										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.
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

Richtlinie	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
										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.
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

Richtlinie	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
										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-Ruhezustanddatei	Wahr					Falsch	Wahr		Falsch	Bei Markierung wird die Ruhezustandsdatei nur verschlüsselt, wenn der Computer in den Ruhezustand schaltet. Der Client setzt den Schutz aus, wenn der Computer den Ruhezustand verlässt. So ergibt sich ein Schutz ohne Beeinträchtigung von Benutzern oder Anwendungen, solange der Computer genutzt wird.
Ungeschützten	Wahr					Falsch	Wahr		Falsch	Wenn dies aktiviert ist, erlaubt der Client dem

Richtlinie	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
Ruhezustand unterbinden										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 Wechselmedien 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 Verschlüsselungsalgorithmus, der für die Verschlüsselung von Daten auf der Ebene des

Richtlinie	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
										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, um anzugeben, wer wo auf Dateien zugreifen darf, die von den folgenden Richtlinien verschlüsselt werden: · 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“, damit benutzerverschlüsselte Dateien/Ordner für alle verwalteten Benutzer auf dem Endpunkt, auf dem sie erstellt wurden, zugänglich sind (gleiche Zugriffsstufe wie allgemein verschlüsselte Ordner) und mit dem allgemeinen Verschlüsselungsalgorithmus verschlüsselt werden.

Richtlinie	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“, damit diese Dateien nur für den Benutzer, der sie erstellt hat, auf dem Endpunkt, auf dem sie erstellt wurden, zugänglich sind (gleiche Zugriffsstufe wie benutzerverschlüsselte Ordner) und mit dem Benutzerverschlüsselungsalgorithmus verschlüsselt werden. 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)										
Der Hardware Crypto Accelerator (HCA, Hardware-Crypto-Beschleuniger)	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

Richtlinie	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
										Accelerator verwendet werden.
Zur Verschlüsselung vorgesehene Datenträger	Alle Festplatten									Alle Festplatten oder nur Systemdatenträger Geben Sie an, welche(s) Volume(s) Sie verschlüsseln möchten.
Forensische Metadaten verfügbar auf mit HCA verschlüsseltem Laufwerk	Falsch									Wahr oder Falsch 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 Encryption client-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 Richtlinien zum Hinzufügen forensischer Daten wiederholt.
Benutzergenehmigung der Verschlüsselung sekundärer	Falsch									Bei „Wahr“ kann der Benutzer entscheiden, ob zusätzliche Laufwerke verschlüsselt werden.

Richtlinie	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 zulassen										
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 Werten anderer Richtlinien für das Port Control System keine Richtlinien für das Port Control System angewendet. Für PCS-Richtlinien ist ein Neustart erforderlich, damit die entsprechende Richtlinie wirksam wird. **ANMERKUNG:** Das Blockieren von Gerätevorgängen führt dazu, dass Gerätenamen leer angezeigt werden.
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.

Richtlinie	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
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 Encryption External Media 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 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

Richtlinie	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
										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 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

Richtlinie	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
										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 Encryption External Media 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-Gerät (Windows Portable Device, WPD)	Aktiviert									ÜBERGEORDNETES ELEMENT für die nächste Richtlinie. Stellen Sie diese Richtlinie auf „Aktiviert“ ein, um die Unterklassenrichtlinie „Tragbares Windows-Gerät (Windows Portable Device,

Richtlinie	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
										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

Richtlinie	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
										seines 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 Encryption External Media und PCS Interaktionen.
EMS CD/DVD-Verschlüsselung ausschließen	Falsch								Wahr	Mit „Falsch“ werden CD/DVD-Geräte verschlüsselt. Diese Richtlinie interagiert mit PCS. Siehe Encryption External Media und PCS Interaktionen.
EMS-Zugriff auf nicht durch Shield	Blockieren	Schreibgeschützt				Vollständiger Zugriff		Schreibgeschützt	Vollständiger Zugriff	Sperren, Schreibgeschützt, Vollständiger Zugriff Diese Richtlinie interagiert mit PCS. Siehe Encryption

Richtlinie	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
geschützte Medien										External Media und PCS Interaktionen. Wenn diese Richtlinie so eingestellt ist, dass der Zugriff gesperrt wird, haben Sie nur dann Zugriff auf 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-Verschlüs	AES256									AES-256, Rijndael 256, AES-128, Rijndael 128

Richtlinie	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
selungsalgorithmus										
EMS-Suchvorgang für externe Medien	Wahr	Falsch								„Wahr“ ermöglicht, dass Wechseldatenträger jedes Mal untersucht werden, wenn sie eingesetzt werden. Wenn diese Richtlinie „Falsch“ ist und die Richtlinie „EMS-Verschlüsselung externer Medien“ „Wahr“ ist, werden nur neue und geänderte Dateien verschlüsselt. Ein Scan tritt bei jedem Einsetzen auf, sodass alle Dateien, die ohne Authentifizierung zum Wechselmedium hinzugefügt wurden, erkannt werden. Dateien können zum Medium hinzugefügt werden, wenn die Authentifizierung abgelehnt wird, es ist aber kein Zugriff auf verschlüsselte Daten möglich. Die hinzugefügten Dateien werden in diesem Fall nicht verschlüsselt. Bei der nächsten Authentifizierung des Wechselspeichermediums (für die Arbeit mit verschlüsselten Daten), werden alle hinzugefügten Dateien gescannt und verschlüsselt.
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.

Richtlinie	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
EMS-Gerät – Positivliste										Diese Richtlinie ermöglicht die Angabe von Wechselmedien, die von der Verschlüsselung ausgeschlossen werden sollen. Wechselmedien, 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 verschlüsselten Computer ein. 2. Öffnen Sie die Datei 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

Richtlinie	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
										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)
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	8					6		8		1-40 Zeichen

Richtlinie	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
im EMS-Passwort										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 Zugriffscode zur vorherigen Cooldown-Zeit addiert wird.
EMS-Verschlüsselungsregeln										Verschlüsselungsregeln für die Verschlüsselung bzw. den Ausschluss der Verschlüsselung von bestimmten Laufwerken,

Richtlinie	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
										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 notwendig sein, zur Verschlüsselung des Geräts sowohl Encryption External Media als auch Verschlüsselungsregeln anzuwenden. Das liegt daran, dass das Betriebssystem Windows Speichergeräte ausgehend von deren Schnittstellentyp unterschiedlich behandelt. Siehe Vorgehensweise bei der Encryption External Media-Verschlüsselung eines iPods.
EMS-Zugriff auf nicht durch Shield geschützte Medien sperren	Wahr								Falsch	Sperrt den Zugriff auf alle Wechselmedien, die weniger als 55 MB Speicher und damit nicht genügend Kapazität für Encryption External Media bieten (z. B. eine Diskette mit 1,44 MB). Der gesamte Zugriff wird gesperrt, wenn die Richtlinie EMS und diese Richtlinie beide auf „Wahr“ eingestellt sind. Ist „EMS Encrypt External

Richtlinie	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
										Media“ auf „Wahr“, diese Richtlinie jedoch auf „Falsch“ eingestellt, können Daten von nicht verschlüsselbaren Medien zwar gelesen werden, doch der Schreibzugriff auf das Medium ist gesperrt. Ist „EMS Encrypt External Media“ auf „Falsch“ eingestellt, hat diese Richtlinie keine Auswirkungen und der Zugriff auf nicht verschlüsselbare Medien 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 fragwürdi	Falsch									Diese Richtlinie regelt, ob ein Benutzer Benachrichtigungs-Popup-Meldungen sieht, wenn

Richtlinie	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
ger Datei unterbinden										eine Anwendung versucht, auf eine Datei zuzugreifen, während sie vom Client verarbeitet wird.
Lokale Verschlüsselungssteuerung anzeigen	Falsch		Wahr					Falsch		Bei der Auswahl von „Wahr“ sieht der Benutzer in dem Infobereichssymbol eine Menüoption, mit der er die Ver- bzw. Entschlüsselung (je nach ausgeführtem Encryption-Vorgang) anhalten und wieder aufnehmen kann. Wichtiger Hinweis: Wenn Sie die Unterbrechung der Verschlüsselung durch Benutzer zulassen, kann dies gemäß der Richtlinie die vollständige Ver- oder Entschlüsselung von Daten durch den Encryption client 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 im Infobereichsymbol 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

Richtlinie	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
										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 Wechselspeichergeräten und verhindert die Verwendung unverschlüsselter Wechselspeichergeräte
- 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 Wechselspeichergeräten 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 Wechselspeichergeräten 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 Wechselspeichergeräten 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 Wechselspeichergeräten 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 Wechselspeichergeräte

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 Wechselspeichergeräte

Einfacher Schutz für externe Festplatten

Diese Richtlinienvorlage:

- bietet Schutz von Wechselspeichergeräten
- 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.

11

Untergeordnete Installationsprogramme 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 `DDSSetup.exe` vom Dell Installationsmedium auf den lokalen Computer.
2. Öffnen Sie am Speicherort der Datei `DDSSetup.exe` eine Eingabeaufforderung und geben Sie Folgendes ein:

   ```
   DDSSetup.exe /s /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.

12

Troubleshooting

Aktualisieren mit Windows 10 oder Windows 11 Funktionsupdates

Um ein Upgrade auf das Windows 10 oder Windows 11 Funktionsupdate durchzuführen, folgen Sie den Anweisungen im folgenden KB-Artikel: 125419.

Dell Encryption – Fehlerbehebung

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**.

Encryption External Media 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 – Klasse: Speicher > Unterklasse Speicher: 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 Unterklasse Speicher: 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 „Windows Media Encryption“ auf „An“ ein.
- Stellen Sie „EMS CD/DVD-Verschlüsselung ausschließen“ auf „nicht ausgewählt“ ein.
- Unterklasse Speicher: Steuerung optischer Laufwerke = nur UFD.

WSScan verwenden

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

ANMERKUNG: WSScan muss im Systemmodus mit dem Tool PsExec ausgeführt werden, wenn sich eine Zieldatei im Besitz des Systemkontos befindet.

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: *Alle Laufwerke, Feste Laufwerke*, *Wechsellaufwerke* oder *CD-ROMs/DVDROMs*.
5. Wählen Sie den Berichtstyp für die Verschlüsselung aus: *Verschlüsselte Dateien*, *Unverschlüsselte Dateien*, *Alle Dateien* oder *Unverschlüsselte Dateien verletzt*:
   - *Verschlüsselte Dateien* – Um sicherzustellen, dass alle Daten bei der Deinstallation von Encryption 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 Menü 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-Schlüssel. **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**“ 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 Dienst-Status (markieren Sie den Dienst > rechte Maustaste > Aktualisieren).

- **Warten auf SDE-Deaktivierung** – Encryption ist noch installiert und/oder konfiguriert. Die Entschlüsselung beginnt erst nach der Deinstallation von Encryption.
- **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 Dienst, die ausführbare Datei, der Treiber und die ausführbare Treiberdatei werden beim nächsten Neustart des Computers gelöscht.

Anleitung zum Verschlüsseln eines iPod mit Encryption External Media

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.

- Dell rät von der Verwendung mitiPod Shuffle ab, 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 Encryption External Media vorsichtig vor.
- Da die Ordnernamen auf iPods vom jeweiligen iPod-Modell abhängen, empfiehlt Dell die Erstellung einer ausschließenden Richtlinie, die die Ordnernamen aller iPod-Modelle berücksichtigt.
- Um sicherzustellen, dass ein iPod auch nach der Verschlüsselung mittels Encryption External Media genutzt werden kann, geben Sie in der Richtlinie „Encryption External Media-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 dell.com/support.
2. Wählen Sie Ihr Computermodell aus.
3. Wählen Sie **Treiber & Downloads**.
4. Wählen Sie das auf dem Zielcomputer ausgeführte **Betriebssystem** aus.
5. Wählen 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

1. Gehen Sie zu dem Ordner, in den Sie die Treiberinstallationsdatei abgelegt haben.
2. Doppelklicken Sie auf den Dell ControlVault-Treiber, um die selbstextrahierende ausführbare Datei aufzurufen.

   ANMERKUNG:

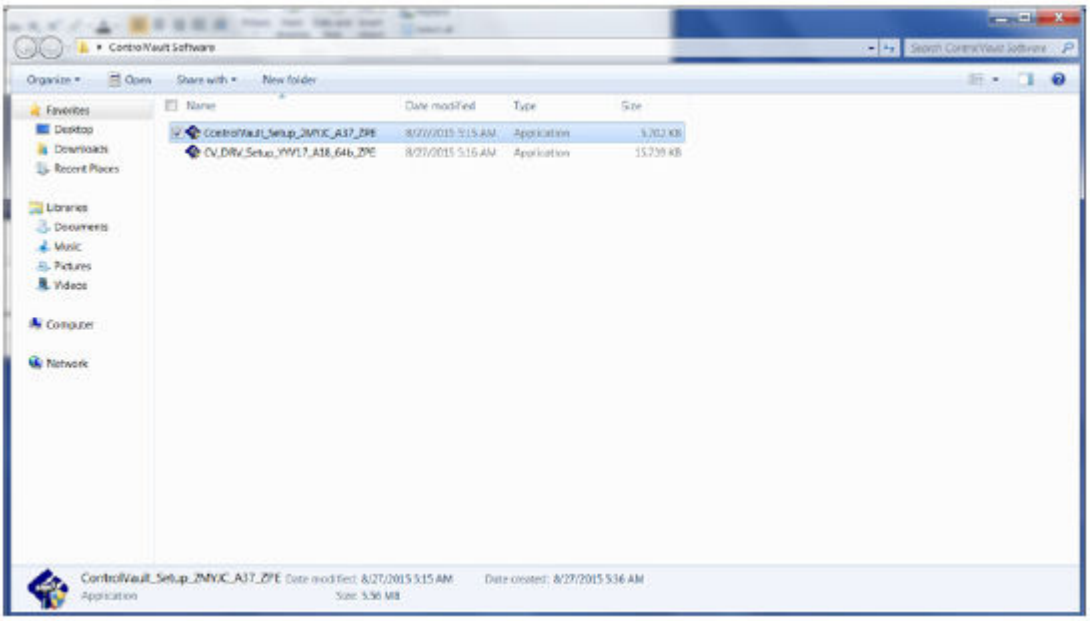
   Achten Sie darauf, als Erstes den Treiber zu installieren. Der Dateiname des Treibers *zum Zeitpunkt der Erstellung dieses Dokuments* lautet „ControlVault_Setup_2MYJC_A37_ZPE.exe“.
3. Klicken Sie zum Fortsetzen des Vorgangs auf **Weiter**.
4. Klicken Sie auf **OK**, um die Treiberdateien in den Standardordner `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. Der Ordner ist als **JW22F** bezeichnet
8. 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].
9. Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.
10. Klicken Sie auf **Weiter** für die Installation im Standardverzeichnis von `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. Wählen Sie die Option **Abschließen** aus, und klicken Sie auf **Weiter**.
12. Klicken Sie auf **Installieren**, um mit der Installation der Treiber zu beginnen.
13. Aktivieren Sie optional das Kontrollkästchen, um die Protokolldatei für das Installationsprogramm anzuzeigen. Klicken Sie zum Beenden des Assistenten auf **Fertig stellen**.

Überprüfen der Treiberinstallation

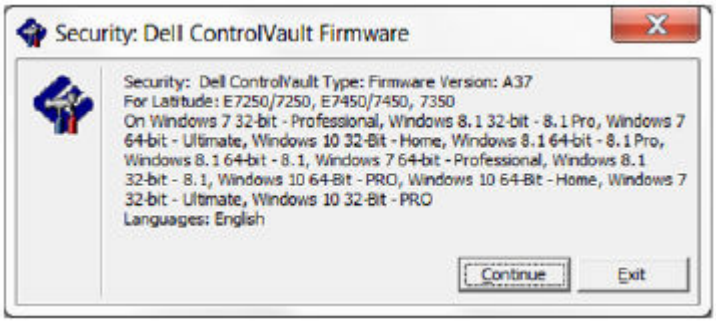
- Der Device Manager zeigt je nach Betriebssystem und Hardwarekonfiguration ein Dell ControlVault-Gerät (sowie weitere Geräte) an.

Installieren der Dell ControlVault-Firmware

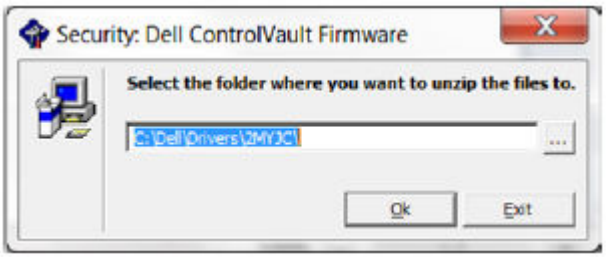
1. Gehen Sie zu dem Ordner, in den Sie die Firmware-Installationsdatei abgelegt haben.



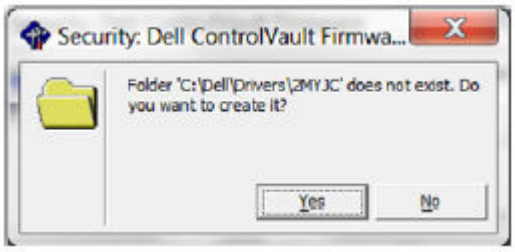
2. Doppelklicken Sie auf die Dell ControlVault-Firmware, um die selbstextrahierende ausführbare Datei aufzurufen.
3. Klicken Sie zum Fortsetzen des Vorgangs auf **Weiter**.



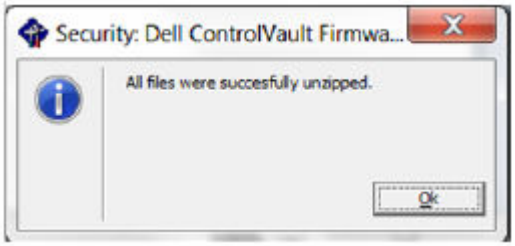
4. Klicken Sie auf **OK**, um die Treiberdateien in den Standardordner `C:\Dell\Drivers\<New Folder>` zu entpacken.



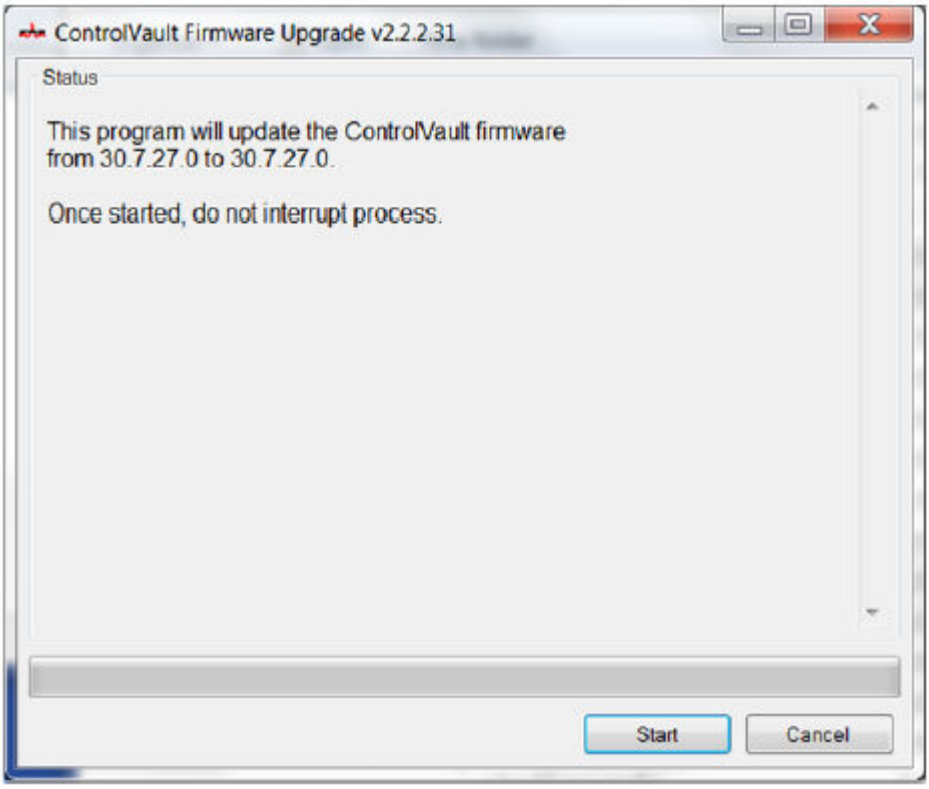
5. Klicken Sie auf **Ja**, um die Erstellung eines neuen Ordners zu genehmigen.



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**.



ANMERKUNG:

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 verschiedene Statusmeldungen angezeigt.

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

    Das Update 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.

Verschlüsselung

Erstellen einer Encryption Removal Agent-Protokolldatei (optional)

- Vor der Deinstallation können Sie optional eine Encryption Removal Agent-Protokolldatei anlegen. Diese Protokolldatei erleichtert das Troubleshooting, 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 Smartcards mit Windows-Anmeldung

- Um festzustellen, ob eine Smartcard vorhanden und aktiv ist, stellen Sie sicher, dass der folgende Wert eingestellt ist:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Wenn SmartcardEnabled fehlt oder einen Wert von Null hat, zeigt der Anmeldeinformationsanbieter nur das Kennwort zur Authentifizierung an.

  Wenn SmartcardEnabled einen Wert ungleich Null hat, zeigt der Anmeldeinformationsanbieter Optionen für Kennwort und Smartcard-Authentifizierung an.

- Der folgende Registrierungswert gibt an, ob Winlogon eine Benachrichtigung für Anmeldeereignisse von Smartcards erzeugen soll.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0 = Deaktiviert

  1 = Aktiviert

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 Nutzer-Eingabeaufforderung für Start oder Verzögerung der Verschlüsselung

- Der Encryption-Client zeigt die Aufforderung *`length of each policy update delay`* zum Neustart jedes Mal fünf Minuten lang an. Reagiert der Nutzer nicht auf die Aufforderung, beginnt die nächste Verzögerung. Die endgültige Verzögerungsaufforderung enthält einen Countdown und einen Fortschrittsbalken und wird angezeigt, bis der Nutzer

reagiert oder die endgültige Verzögerung abläuft und die verlangte Abmeldung bzw. der verlangte Neustart durchgeführt wird.

Sie können das Verhalten der Nutzeraufforderung dahingehend ändern, dass die Verschlüsselung begonnen oder verzögert wird, damit keine Verschlüsselung durchgeführt wird, wenn der Nutzer 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 Nutzerinteraktion 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 Nutzer 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 Encryption eine Richtlinienaktualisierung mit einer aktiven SDE-Richtlinie verarbeitet, wird das aktuelle Nutzerprofilverzeichnis standardmäßig mit dem Nutzerschlüssel SDUser verschlüsselt, und nicht mit dem Geräteschlüssel SDE. Der SDUser-Schlüssel wird außerdem zur Verschlüsselung von Dateien oder Ordnern verwendet, die in ein Nutzerverzeichnis 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 Nutzerverzeichnisse 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 Nutzerverzeichnisse verwendet.

Deaktivieren/Aktivieren von Encrypt for Sharing im Rechtsklick-Kontextmenü

- Um die Option *Encrypt for Sharing* im Kontextmenü zu deaktivieren oder zu aktivieren, verwenden Sie den folgenden Registrierungsschlüssel.

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

  0 = Deaktivieren der Option „Encrypt for Sharing“ im Rechtsklick-Kontextmenü.

  1 = Aktivieren der Option „Encrypt for Sharing“ im Rechtsklick-Kontextmenü.

Deaktivieren/Aktivieren der Benachrichtigung für die Aktivierung von Encryption Personal

- HKCU\Software\Dell\Dell Data Protection\Encryption

  "HidePasswordPrompt"=DWORD

  1 = deaktiviert die Kennwort-Eingabeaufforderung für die Encryption Personal Aktivierung

  0 = aktiviert die Passwort-Eingabeaufforderung für Encryption Personal Aktivierung

Die Aufforderung zum Neustart deaktivieren/aktivieren, nachdem der Encryption Removal Agent die abschließende Phase der Entschlüsselung abgeschlossen hat

- Um zu deaktivieren, dass der Nutzer aufgefordert wird, den Computer neu zu starten, nachdem der Encryption Removal Agent seinen endgültigen Status im Entschlüsselungsvorgang abgeschlossen hat, ändern Sie den folgenden Registrierungswert.

  HKLM\Software\Dell\Dell Data Protection

  "ShowDecryptAgentRebootPrompt"=DWORD

  Standard = aktiviert

1 = aktiviert (zeigt Eingabeaufforderung an)

0 = deaktiviert (Aufforderung zum Ausblenden)

Advanced Authentication

Deaktivieren der Smartcard und biometrischen Dienste (optional)

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

Ist diese Funktion deaktiviert, unternimmt Authentication für diese 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. Ist dieser Dienst deaktiviert, können alle direkt davon abhängigen Dienste nicht gestartet werden.
- SCPolicySvc – Ermöglicht es, das System so zu konfigurieren, dass der Nutzer-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 Smartcards mit Windows-Anmeldung

- Um festzustellen, ob die PBA aktiviert ist, stellen Sie sicher, dass der folgende Wert festgelegt ist:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]

  "PBAIsActivated"=DWORD (32-bit):1

  Der Wert „1“ bedeutet, dass die PBA aktiviert ist. Der Wert „0“ bedeutet, dass die PBA nicht aktiviert ist.

  ANMERKUNG: Das manuelle Löschen dieser Schlüssel kann unerwünschte Ergebnisse für Nutzer nach sich ziehen, die sich mit der PBA synchronisieren. Unter Umständen ergibt sich die Notwendigkeit einer manuellen Wiederherstellung.

- Um festzustellen, ob eine Smartcard vorhanden und aktiv ist, stellen Sie sicher, dass der folgende Wert eingestellt ist:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Wenn SmartcardEnabled fehlt oder einen Wert von Null hat, zeigt der Anmeldeinformationsanbieter nur das Kennwort zur Authentifizierung an.

  Wenn SmartcardEnabled einen Wert ungleich Null hat, zeigt der Anmeldeinformationsanbieter Optionen für Kennwort und Smartcard-Authentifizierung an.

- Der folgende Registrierungswert gibt an, ob Winlogon eine Benachrichtigung für Anmeldeereignisse von Smartcards erzeugen soll.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0 = Deaktiviert

  1 = Aktiviert

  Fahren Sie mit Glossar fort.

- Erstellen Sie den folgenden Registrierungsschlüssel, um zu verhindern, dass die SED-Verwaltung Drittanbieter von Anmeldeinformationen deaktiviert:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 = Deaktiviert (Standardeinstellung)

  1 = Aktiviert

- Der Encryption Management Agent gibt standardmäßig keine Richtlinien mehr aus. Erstellen Sie den folgenden Registrierungsschlüssel, um zukünftig verbrauchte Richtlinien auszugeben:

  HKLM\Software\Dell\Dell Data Protection\

  DWORD: DumpPolicies

  Wert=1

  Anmerkung: Es ist ein Neustart erforderlich, damit die Änderungen wirksam werden.

- Zur Unterdrückung aller Toaster-Benachrichtigungen vom Encryption Management Agent muss der folgende Registrierungswert auf dem Client-Computer gesetzt werden.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = Aktiviert (Standard)

  1 = Deaktiviert

13

Glossar

Advanced Authentication: Das Advanced Authentication-Produkt bietet Optionen für Smart Card-Leser. Advanced Authentication vereinfacht die Verwaltung all dieser Authentifizierungsmethoden, unterstützt die Anmeldung bei selbstverschlüsselnden Laufwerken, SSO und verwaltet Benutzeranmeldeinformationen und Passwörter.

Administrator-Passwort für die Verschlüsselung (Encryption Administrator Password, EAP) – Das EAP ist ein computerspezifisches Administrator-Passwort. Für die meisten Konfigurationsänderungen in der lokalen Verwaltungskonsole ist die Eingabe dieses Passworts erforderlich. Dasselbe Passwort wird auch benötigt, falls Sie die Datei „LSARecovery_[Hostname].exe“ verwenden, um Daten wiederherzustellen. 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.

Verschlüsselungsschlüssel – In den meisten Fällen verwendet Encryption 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“ Verschlüsselungsschlüssel macht Dateien allen verwalteten Benutzern auf dem Gerät zugänglich, auf dem sie erstellt wurden. Der „Benutzer“-Verschlüsselungsschlüssel macht Dateien nur dem Benutzer zugänglich, der sie erstellt hat, und zwar nur auf dem Gerät, auf dem sie erstellt wurden. Der „Benutzer-Roaming“-Verschlüsselungsschlüssel macht Dateien nur dem Benutzer zugänglich, der sie erstellt hat, und zwar auf jedem verschlüsselten Windows- oder Mac-Gerät.

Verschlüsselungssuche – Bei dem Vorgang werden zu verschlüsselnde Ordner 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.

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 von SDE werden alle relevanten Dateien und Verzeichnisse mit SDE-Verschlüsselung automatisch entschlüsselt, unabhängig von anderen SDE-Richtlinienwerten 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.