

# Dell Data Protection | Encryption

Enterprise Edition - Einfaches Installationshandbuch  
v8.13



## Anmerkungen, Vorsichtshinweise und Warnungen

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

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

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

### Enterprise Edition - Einfaches Installationshandbuch

2017 - 04

Rev. A01

<b>1 Einleitung</b>	<b>5</b>
Vor der Installation	5
Verwendung des Handbuchs	5
Kontaktaufnahme mit dem Dell ProSupport	5
<b>2 Anforderungen</b>	<b>7</b>
Alle Clients	7
Alle Clients - Voraussetzungen	7
Alle Clients - Hardware	8
Alle Clients - Sprachunterstützung	8
Encryption-Client	8
Encryption-Client-Anforderungen	9
Encryption-Client-Betriebssysteme	9
Externes Medien-Shield (EMS)-Betriebssysteme	9
SED-Client	10
SED-Client-Anforderungen	10
SED-Client-Hardware	11
SED-Client-Betriebssysteme	11
Advanced Authentication-Client	11
Advanced Authentication-Client-Hardware	12
Advanced Authentication Client - Betriebssysteme	12
BitLocker Manager-Client	13
Voraussetzungen für den BitLocker Manager-Client	13
BitLocker Manager Client-Betriebssysteme	13
<b>3 Installation unter Verwendung des -Master-Installationsprogramms</b>	<b>14</b>
Interaktive Installation unter Verwendung des -Master Installationsprogramms	14
Installation durch Befehlszeile mit dem -Master Installationsprogramm	15
<b>4 Deinstallation unter Verwendung des -Master-Installationsprogramms</b>	<b>18</b>
-Master-Installationsprogramm deinstallieren	18
Deinstallation über die Befehlszeile	18
<b>5 Deinstallation unter Verwendung der untergeordneten Installationsprogramme</b>	<b>19</b>
Client für Verschlüsselung und Serververschlüsselung deinstallieren	20
Verfahren	20
Deinstallation über die Befehlszeile	20
External Media Edition deinstallieren	22
Deinstallation der SED- und Advanced Authentication-Clients	22
Verfahren	22
PBA deaktivieren	23
Deinstallieren des SED-Clients und der Advanced Authentication-Clients	23
Deinstallation des BitLocker Manager-Clients	24

Deinstallation über die Befehlszeile.....	24
<b>6 Herunterladen der Software.....</b>	<b>25</b>
<b>7 Untergeordnete Installationsprogramme aus dem -Master-Installationsprogramm extrahieren.....</b>	<b>27</b>
<b>8 Konfiguration des Key Servers für die Deinstallation des auf einem EE-Server aktivierten Encryption-Clients.....</b>	<b>28</b>
Dialogfeld „Dienste“ - Domänenbenutzerkonto hinzufügen.....	28
Schlüsselserver-Konfigurationsdatei - Fügen Sie Benutzer für EE-Server-Kommunikation hinzu.....	28
Dialogfeld „Dienste“ - Key Server-Dienst neu starten.....	29
Remote Management-Konsole - Hinzufügen eines forensischen Administrators.....	29
<b>9 Verwenden Sie das administrative Dienstprogramm zum Herunterladen (CMGAd).....</b>	<b>30</b>
Verwenden des Administrator-Download-Dienstprogramms im forensischen Modus.....	30
Verwenden des Administrator-Download-Dienstprogramms im Admin-Modus.....	31
<b>10 Fehlerbehebung.....</b>	<b>32</b>
Alle Clients – Fehlerbehebung.....	32
Fehlerbehebung für den Client für Verschlüsselung und Serververschlüsselung .....	32
Upgrade auf die Windows 10 Anniversary-Aktualisierung.....	32
Aktivierung auf einem Serverbetriebssystem.....	32
EMS und PCS Interaktionen.....	35
WSScan verwenden.....	35
Überprüfen des Encryption-Removal-Agent-Status.....	37
Dell ControlVault-Treiber.....	38
Aktualisieren von Treibern und Firmware für Dell ControlVault.....	38
<b>11 Glossar.....</b>	<b>40</b>



# Einleitung

In diesem Handbuch wird die Installation und Konfiguration der Anwendung unter Verwendung des -Master-Installationsprogramms beschrieben. Das Handbuch bietet eine grundlegende Hilfestellung bei der Installation. Ziehen Sie das *erweiterte Installationshandbuch* heran, wenn Sie Informationen zum Installieren der untergeordneten Installationsprogramme oder zum Konfigurieren von EE-Server/VE-Server benötigen, oder weitere Informationen, die über die grundlegende Hilfestellung durch das -Master-Installationsprogramm hinausgehen.

Alle Richtlinieninformationen und deren Beschreibungen finden Sie in der AdminHelp.

## Vor der Installation

1 Installieren Sie den EE-Server/VE-Server, bevor Sie die Clients bereitstellen. Machen Sie das richtige Handbuch ausfindig (siehe unten), folgen Sie den Anweisungen, und kehren Sie anschließend zu diesem Handbuch zurück.

- *Installations- und Migrationshandbuch für DDP Enterprise Server*
- *Schnellanleitung und Installationshandbuch für DDP Enterprise Server – Virtual Edition*

Stellen Sie sicher, dass die Richtlinien wie gewünscht eingestellt sind. Durchsuchen Sie die AdminHilfe, die Sie über das **?** ganz rechts im Bildschirm aufrufen können. Die AdminHilfe ist eine seitenbezogene Hilfe, die eigens dafür entwickelt wurde, Sie bei der Einstellung und Änderung von Richtlinien zu unterstützen und mit den Optionen Ihres EE-Servers/VE-Servers vertraut zu machen.

- 2 Lesen Sie sich das Kapitel [Anforderungen](#) in diesem Dokument genau durch.
- 3 Stellen Sie Clients für die Endbenutzer bereit.

## Verwendung des Handbuchs

Wenden Sie das Handbuch in der folgenden Reihenfolge an.

- Machen Sie unter [Anforderungen](#) die Client-Voraussetzungen ausfindig.
  - Führen Sie eine der folgenden Maßnahmen durch:
    - [Interaktive Installation unter Verwendung des -Master-Installationsprogramms](#)
- oder
- [Installation durch Befehlszeile mit dem -Master Installationsprogramm](#)

## Kontaktaufnahme mit dem Dell ProSupport

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

Zusätzlich steht Ihnen unser Online-Support für Dell Data Protection-Produkte unter [dell.com/support](http://dell.com/support) zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Halten Sie bei Ihrem Anruf Ihren Service Code bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.



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



# Anforderungen

## Alle Clients

- Bei der Implementierung sind die bewährten IT-Verfahren zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Benutzer.
- Die Installation/Aktualisierung/Deinstallation kann nur von einem lokalen Benutzer oder einem Domänenadministrator durchgeführt werden, der über ein Implementierungstool wie Microsoft SMS oder KACE vorübergehend zugewiesen werden kann. Benutzer ohne Administratorstatus, aber mit höheren Rechten, werden nicht unterstützt.
- Sichern Sie vor der Installation/Deinstallation alle wichtigen Daten.
- Nehmen Sie während der Installation oder Deinstallation keine Änderungen am Computer vor, dazu gehört auch das Einsetzen oder Entfernen von externen (USB-)Laufwerken.
- Stellen Sie sicher, dass der ausgehende Port 443 für die Datenübertragung zum EE-Server/VE-Server zur Verfügung steht, falls die Clients des -Master-Installationsprogramms für die Verwendung von Dell Digital Delivery (DDD) berechtigt werden sollen. Die Berechtigung kann nicht eingerichtet werden, wenn Port 443 blockiert ist. DDD wird nicht verwendet, wenn die Installation über die untergeordneten Installationsprogramme erfolgt.
- Überprüfen Sie regelmäßig die Website [www.dell.com/support](http://www.dell.com/support), um stets über die neueste Dokumentation und die neuesten technischen Ratgeber zu verfügen.

## Alle Clients - Voraussetzungen

- Microsoft .Net Framework 4.5.2 (oder höher) ist für das -Master-Installationsprogramm und die untergeordneten Installationsprogramm-Clients erforderlich. Das Installationsprogramm installiert die Microsoft .Net Framework-Komponente *nicht*.

Auf allen von Dell werksseitig ausgelieferten Computern ist Microsoft .Net Framework 4.5.2 (oder höher) in der Vollversion vorinstalliert. Wenn Sie jedoch keine Dell Hardware verwenden oder den Client auf älterer Dell Hardware aktualisieren, sollten Sie überprüfen, welche Version von Microsoft .Net installiert ist und diese gegebenenfalls aktualisieren, **bevor Sie den Client installieren**, um Fehler bei der Installation/Aktualisierung zu vermeiden. Um die installierte Version von Microsoft .Net zu überprüfen, folgen Sie auf dem Computer, auf dem die Installation vollzogen werden soll, den folgenden Anweisungen: [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx). Zum Installieren von Microsoft .Net Framework 4.5.2 rufen Sie <https://www.microsoft.com/en-us/download/details.aspx?id=42643> auf.

- Treiber und Firmware für ControlVault, Fingerabdruckleser und Smartcards (siehe unten) sind nicht im -Master-Installationsprogramm oder in den untergeordneten ausführbaren Dateien enthalten. Treiber und Firmware müssen jederzeit auf dem aktuellen Stand sein und können nach Auswahl des jeweiligen Computermodells von der Website <http://www.dell.com/support> heruntergeladen werden. Laden Sie die jeweiligen Treiber und die Firmware basierend auf Ihrer Authentifizierungshardware herunter.
  - ControlVault
  - NEXT Biometrics Fingerprint-Treiber
  - Validity Fingerprint Reader 495-Treiber
  - O2Micro Smart Card-Treiber

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



## Alle Clients - Hardware

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

### Hardware

---

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

## Alle Clients - Sprachunterstützung

- Die Encryption-, und BitLocker Manager-Clients sind Multilingual User Interface (MUI)-konform und unterstützen die folgenden Sprachen.

### Sprachunterstützung

---

- EN: Englisch
  - ES: Spanisch
  - FR: Französisch
  - IT: Italienisch
  - DE: Deutsch
  - JA: Japanisch
  - KO: Koreanisch
  - PT-BR: Portugiesisch, Brasilien
  - PT-PT: Portugiesisch, Portugal
- Der SED-Client und der Advanced Authentication-Client sind MUI-kompatibel (Multilingual User Interface) und unterstützen folgende Sprachen. Der UEFI-Modus sowie die Preboot-Authentifizierung werden auf Russisch sowie auf traditionellem und vereinfachtem Chinesisch nicht unterstützt.

### Sprachunterstützung

---

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

## Encryption-Client

- Der Client-Computer muss über Netzwerkkonnektivität verfügen.
- 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.
- Der Encryption-Client wurde getestet und ist kompatibel mit McAfee, dem Symantec-Client, Kaspersky und MalwareBytes. Für diese Anbieter von Virenschutzsoftware wurden hartkodierte Ausschlüsse implementiert, um Inkompatibilitäten zwischen Virenschutzprüfung und Verschlüsselung zu verhindern. Der Encryption-Client wurde außerdem mit dem Microsoft Enhanced Mitigation Experience Toolkit getestet.

Falls Ihr Unternehmen Virenschutzsoftware von einem hier nicht aufgeführten Anbieter verwendet, lesen Sie unter <http://www.dell.com/support/Article/us/en/19/SLN298707> nach oder [kontaktieren Sie Dell ProSupport](#), um Hilfe zu erhalten.

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

Die Neuinstallation des Betriebssystems wird ebenfalls nicht unterstützt. Zur Neuinstallation des Betriebssystems sichern Sie den Zielcomputer, setzen Sie den Computer zurück, installieren Sie das Betriebssystem, und stellen Sie anschließend die verschlüsselten Daten gemäß den üblichen Wiederherstellungsverfahren wieder her.

## Encryption-Client-Anforderungen

- Das -Master-Installationsprogramm installiert Microsoft Visual C++ 2012 Update 4, falls diese Komponente noch nicht auf dem Computer vorhanden ist.

### Voraussetzungen

---

- Visual C++ 2012 Update 4 oder höheres Redistributable Package (x86 und x64)

## Encryption-Client-Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

---

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

**ANMERKUNG:**

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

## Externes Medien-Shield (EMS)-Betriebssysteme

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

**ANMERKUNG:**

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

**ANMERKUNG:**

Windows XP wird nur bei Verwendung von EMS Explorer unterstützt.



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

---

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

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

---

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

# SED-Client

- Der Computer muss über Netzwerkkonnektivität verfügen, damit SED Management erfolgreich installiert werden kann.
- 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 ein selbstverschlüsselndes Laufwerk verfügt, muss in Active Directory die Option *Benutzer muss das Kennwort bei der nächsten Anmeldung ändern* deaktiviert sein. Die Preboot-Authentifizierung bietet keine Unterstützung für diese Active Directory-Option.
- Dell empfiehlt, die Authentifizierungsmethode nicht mehr zu ändern, nachdem die PBA aktiviert worden ist. Wenn Sie zu einer anderen Authentifizierungsmethode wechseln müssen, gibt es zwei Möglichkeiten:
  - Entfernen Sie alle Benutzer aus der PBA.

oder

- Deaktivieren Sie die PBA, ändern Sie die Authentifizierungsmethode, und aktivieren Sie die PBA erneut.

### WICHTIG:

Aufgrund der Struktur von RAID und SEDs wird RAID von der SED-Verwaltung 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 Benutzeranmeldung. 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 („Bluescreen“).

- SED-Management wird mit Server Encryption nicht unterstützt.

# SED-Client-Anforderungen

- Das -Master-Installationsprogramm installiert Microsoft Visual C++2010 SP1 **und** Microsoft Visual C++ 2012 Update 4, falls diese Komponenten noch nicht auf dem Computer vorhanden sind.

## Voraussetzungen

---

- Visual C++ Redistributable Package ab Version 2010 SP1 (x86 und x64)
- Visual C++ 2012 Update 4 oder höheres Redistributable Package (x86 und x64)

# SED-Client-Hardware

## Internationale Tastaturen

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

### International Keyboard Support - UEFI

---

- DE-CH: Deutsch
- DE-FR: Französisch

### Internationale Tastatur-Unterstützung – Nicht-UEFI

---

- AR – Arabisch (mit lateinischen Buchstaben)
- DE-CH: Deutsch
- DE-FR: Französisch

# SED-Client-Betriebssysteme

- Die folgende Tabelle enthält Informationen zu den unterstützten Betriebssystemen.

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

---

- Windows 7 SP0-SP1: Enterprise, Professional (unterstützt mit Legacy Boot-Modus aber nicht UEFI)



#### ANMERKUNG:

Legacy Boot-Modus wird auf Windows 7 unterstützt. UEFI wird auf Windows 7 nicht unterstützt.

- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

# Advanced Authentication-Client

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

Wenn Sie Ihre Anmeldeinformationen weiterhin mit dem Microsoft-Betriebssystem verwalten möchten, installieren Sie Security Tools nicht, bzw. deinstallieren Sie das Programm.

- Für die Einmalpasswort (OTP)-Funktion in Security Tools muss ein TPM vorhanden, aktiviert und zugewiesen sein. OTP wird nicht mit TPM 2.0 unterstützt. Weitere Informationen zum Löschen und Definieren der TMP-Zuweisung finden Sie unter <https://technet.microsoft.com>.



# Advanced Authentication-Client-Hardware

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

## Fingerabdruck- und Smart Card-Leser

---

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

## Kontaktlose Karte

---

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

## Smart Cards

---

- PKCS #11 Smart Cards verwenden den [ActivIdentity](#)-Client.

### ① ANMERKUNG:

Der ActivIdentity-Client ist nicht vorinstalliert und muss daher separat installiert werden.

- CSP Cards
- Common Access Cards (CACs)
- Net-Karten der B/SIPR-Klasse

# Advanced Authentication Client - Betriebssysteme

## Windows-Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

---

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

### ① ANMERKUNG: Der UEFI-Modus wird auf Windows 7 nicht unterstützt.

## Betriebssysteme für Mobilgeräte

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

### Android-Betriebssysteme

---

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

## iOS-Betriebssysteme

---

- iOS 7.x
- iOS 8.x

## Windows Phone-Betriebssysteme

---

- Windows Phone 8.1
- Windows 10 Mobile

# BitLocker Manager-Client

- Lesen Sie den Abschnitt [Microsoft BitLocker-Anforderungen](#), falls BitLocker in Ihrer Umgebung bislang noch nicht bereitgestellt wurde.
- Überprüfen Sie, ob die PBA-Partition bereits eingerichtet worden ist. Wenn BitLocker Manager vor Einrichtung der PBA-Partition installiert wird, kann BitLocker nicht aktiviert werden, und BitLocker Manager funktioniert nicht.
- Tastatur, Maus und Videokomponenten müssen direkt an den Computer angeschlossen sein. Setzen Sie keinen KVM-Schalter zur Verwaltung der Peripherie ein, da dies die ordnungsgemäße Erfassung der Hardware durch den Computer behindern kann.
- Aktivieren Sie das TPM. BitLocker Manager übernimmt automatisch die Zuweisung des TPM und erfordert keinen Neustart. Wenn das TPM bereits zugewiesen ist, leitet BitLocker Manager den Einrichtungsvorgang für die Verschlüsselung ein (kein Neustart erforderlich). Wichtig ist, dass das TPM „zugewiesen“ und aktiviert ist.
- BitLocker Manager wird mit Server Encryption nicht unterstützt.

## Voraussetzungen für den BitLocker Manager-Client

- Das -Master-Installationsprogramm installiert Microsoft Visual C++2010 SP1 **und** Microsoft Visual C++ 2012 Update 4, falls diese Komponenten noch nicht auf dem Computer vorhanden sind.

### Voraussetzungen

---

- Visual C++ Redistributable Package ab Version 2010 SP1 (x86 und x64)
- Visual C++ 2012 Update 4 oder höheres Redistributable Package (x86 und x64)

## BitLocker Manager Client-Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

### Windows-Betriebssysteme

---

- Windows 7 SP0-SP1: Enterprise, Ultimate (32- und 64-Bit)
- Windows 8: Enterprise (64-Bit)
- Windows 8.1: Enterprise Edition, Pro Edition (64-Bit)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64-Bit)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64-Bit)
- Windows Server 2016



# Installation unter Verwendung des -Master-Installationsprogramms

- Bei den Befehlszeilenschaltern und -parametern ist die Groß- und Kleinschreibung zu beachten.
  - Um die Installation unter Verwendung nicht standardmäßiger Ports durchzuführen, verwenden Sie untergeordnete Installationsprogramme anstelle des -Master-Installationsprogramms.
  - Die Protokolldateien des Master-Installationsprogramms befinden sich unter **C:\ProgramData\Dell\Dell Data Protection\Installer**.
  - Weisen Sie die Benutzer an, sich mit dem folgenden Dokument und den Hilfedateien vertraut zu machen, um Unterstützung bei der Anwendung zu erhalten:
    - Informationen zur Verwendung der Funktionen von Encryption-Client finden Sie im Hilfedokument *Dell Encrypt Help*. Hier können Sie auf die Hilfe zugreifen: **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
    - Informationen zur Verwendung der Funktionen von External Media Shield finden Sie im Hilfedokument *EMS Help*. Hier können Sie auf die Hilfe zugreifen: **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
    - Weitere Informationen zur Verwendung der Funktionen Advanced Authentication und finden Sie in der *Security Tools-Hilfe*. Greifen Sie auf die Hilfe über **<Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help** auf.
  - Nach Abschluss der Installation sollten Endbenutzer die Richtlinien aktualisieren, indem sie in der Taskleiste mit der rechten Maustaste auf das Symbol für „Dell Data Protection“ klicken und die Option **Nach Richtlinienaktualisierungen suchen** auswählen.
  - Das -Master-Installationsprogramm installiert die gesamte Suite von Produkten. Es gibt zwei Methoden zur Installation unter Verwendung des -Master-Installationsprogramms. Wählen Sie eine der folgenden Optionen aus:
    - [Interaktive Installation unter Verwendung des -Master-Installationsprogramms](#)
- oder
- [Installation durch Befehlszeile mit dem -Master Installationsprogramm](#)

## Interaktive Installation unter Verwendung des -Master Installationsprogramms

- Das -Master-Installationsprogramm finden Sie hier:
  - **Über die Website [support.dell.com](http://support.dell.com)** – Erhalten Sie ggf. die Software von [support.dell.com](http://support.dell.com), und extrahieren Sie dann die untergeordneten Installationsprogramme aus dem -Master-Installationsprogramm.
  - **Über Ihr Dell FTP-Konto** – Suchen Sie das Installationspaket unter DDP-Enterprise-Edition-8.x.x.xxx.zip
- Verwenden Sie diese Anweisungen für die interaktive Installation von Dell Enterprise Edition über das -Master-Installationsprogramm. Sie können dieses Verfahren anwenden, um die gesamte Produkt-Suite gleichzeitig auf einem Computer zu installieren.
  - 1 Suchen Sie die Datei **DDPSetup.exe** auf dem Dell-Installationsmedium. Kopieren Sie sie auf den lokalen Computer.
  - 2 Doppelklicken Sie auf , um das Installationsprogramm zu starten. Dieser Vorgang kann mehrere Minuten dauern.
  - 3 Klicken Sie im Dialogfeld „Willkommen“ auf **Weiter**.
  - 4 Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen, und klicken Sie auf **Weiter**.
  - 5 Wählen Sie **Enterprise Edition** und klicken Sie auf **Weiter**.  
Wählen Sie die External Media Edition nur aus, wenn Sie nur die External Media Edition installieren möchten.
  - 6 Geben Sie im Feld **Name des Enterprise Servers** den vollständigen Hostnamen des EE-Servers/VE-Servers ein, mit dem der Zielbenutzer verwaltet werden soll, z. B. server.organisation.de.

Geben Sie im Feld **URL des Device Servers** die URL des Device Servers (Security Servers) ein, mit dem der Client kommunizieren soll.

Wenn Sie einen EE-Server vor Version 7.7 verwenden, lautet das Format wie folgt: `https://server.organisation.de:8081/xapi`.

Wenn Sie über einen EE-Server ab Version 7.7 verfügen, lautet das Format wie folgt: `https://server.organization.com:8443/xapi/` (einschließlich des nachfolgenden Schrägstrichs).

Klicken Sie auf **Weiter**.

- 7 Klicken Sie auf **Weiter**, um die Produkte im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\` zu speichern. **Dell recommends installing in the default location only**, da bei der Installation an anderen Speicherorten Probleme auftreten könnten.
- 8 Wählen Sie die zu installierenden Komponenten aus.  
*Security Framework* installiert das unterliegende Sicherheitsrahmenwerk und Security Tools, den erweiterten Authentifizierungs-Client, der mehrere Authentifizierungsmethoden verwaltet, darunter PBA und Anmeldeinformationen wie Fingerabdrücke und Passwörter.

*Advanced Authentication* installiert die Dateien und die erforderlichen Services für Advanced Authentication. .

*Encryption* installiert den Encryption-Client, die Komponente, die Sicherheitsrichtlinien durchsetzt, egal ob ein Computer mit dem Netzwerk verbunden oder vom Netzwerk getrennt ist, verloren gegangen ist oder gestohlen wurde.

*BitLocker Manager* installiert den BitLocker Manager-Client, der speziell auf die Verbesserung der Sicherheit von BitLocker-Bereitstellungen ausgelegt ist. Er sorgt für Vereinfachung und senkt gleichzeitig die Betriebskosten durch eine zentralisierte Verwaltung der BitLocker- Verschlüsselungsrichtlinien.

Klicken Sie auf **Weiter**, wenn Ihre Auswahl abgeschlossen sind.

- 9 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen. Die Installation kann mehrere Minuten dauern.
- 10 Wählen Sie **Ja, ich möchte meinen Computer jetzt neu starten** aus, und klicken Sie auf **Fertig stellen**.  
Damit ist die Installation abgeschlossen.

## Installation durch Befehlszeile mit dem -Master Installationsprogramm

- Bei einer Installation über die Befehlszeile müssen die Schalter zuerst angegeben werden. Andere Parameter gehen in ein Argument ein, das an den /v-Schalter weitergegeben wird.

### Schalter

- In der folgenden Tabelle werden die Schalter beschrieben, die mit dem -Master-Installationsprogramm verwendet werden können.

Schalter	Beschreibung
-y -gm2	Vorab-Extrahierung des -Master Installationsprogramms. Die Schalter -y und -gm2 müssen zusammen verwendet werden.  Trennen Sie sie bitte nicht.
/S	Installation im Hintergrund
/z	Gibt Variablen an die MSI-Datei innerhalb der DDPSetup.exe-Datei weiter.

### Parameter

- In der folgenden Tabelle werden die Parameter beschrieben, die mit dem -Master-Installationsprogramm verwendet werden können.



Parameter	Beschreibung
SUPPRESSREBOOT	Unterbindet nach Abschluss der Installation den automatischen Neustart. Kann im HINTERGRUND-Modus verwendet werden.
SERVER	Gibt die URL des EE-Servers/VE-Servers an.
InstallPath	Gibt den Pfad für die Installation an. Kann im HINTERGRUND-Modus verwendet werden.
FUNKTIONEN	Gibt die Komponenten an, die im HINTERGRUND-Modus installiert werden können.  DE = Drive Encryption (Laufwerksverschlüsselung) (Encryption-Client)  EME = Nur External Media Edition  BLM = BitLocker Manager  SED = Self-encrypting Drive management (Verwaltung eines selbstverschlüsselnde Laufwerks) (EMAgent/Manager, PBA/GPE-Treiber)
BLM_ONLY=1	Muss verwendet werden, wenn FEATURES=BLM in der Befehlszeile verwendet wird, um das SED Management-Plugin auszuschließen.

### Beispiel für eine Befehlszeile

- Bei den Befehlszeilenparametern ist die Groß- und Kleinschreibung zu beachten.
- In diesem Beispiel wird lediglich ESSE Manager unter Verwendung des -Master-Installationsprogramms auf Standardports, im Hintergrund und am Standardspeicherort **C:\Program Files\Dell\Dell Data Protection\** installiert und für die Verwendung des angegebenen EE-Servers/VE-Servers konfiguriert.  
  

```
"DDPSetup.exe" -y -gm2 /S /z "\"SERVER=server.organization.com\""
```
- In diesem Beispiel wird lediglich SED Management unter Verwendung des Master-Installationsprogramms auf Standardports, im Hintergrund und am Standardspeicherort **C:\Program Files\Dell\Dell Data Protection\** mit einem unterdrückten Neustart installiert und für die Verwendung des angegebenen EE-Servers/VE-Servers konfiguriert.  
  

```
"DDPSetup.exe" -y -gm2 /S /z "\"SERVER=server.organization.com, FEATURES=EME-SED, SUPPRESSREBOOT=1\""
```
- In diesem Beispiel wird lediglich SED Management unter Verwendung des Master-Installationsprogramms auf Standardports, im Hintergrund und am Standardspeicherort **C:\Program Files\Dell\Dell Data Protection\** mit einem unterdrückten Neustart installiert und für die Verwendung des angegebenen EE-Servers/VE-Servers konfiguriert.  
  

```
"DDPSetup.exe" -y -gm2 /S /z "\"SERVER=server.organization.com, FEATURES=SED, SUPPRESSREBOOT=1\""
```
- In diesem Beispiel wird lediglich SED Management unter Verwendung des Master-Installationsprogramms auf Standardports, im Hintergrund und am Standardspeicherort **C:\Program Files\Dell\Dell Data Protection\** installiert und für die Verwendung des angegebenen EE-Servers/VE-Servers konfiguriert.  
  

```
"DDPSetup.exe" -y -gm2 /S /z "\"SERVER=server.organization.com, FEATURES=SED\""
```
- In diesem Beispiel werden der Encryption-Client und BitLocker Manager (ohne das SED Management-Plugin) unter Verwendung des Master-Installationsprogramms auf Standardports, im Hintergrund und am Standardspeicherort **C:\Program Files\Dell\Dell Data Protection\** installiert und für die Verwendung des angegebenen EE-Servers/VE-Servers konfiguriert.  
  

```
"DDPSetup.exe" -y -gm2 /S /z "\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
```
- In diesem Beispiel wird BitLocker Manager (mit dem SED-Management-Plugin) und die External Media Edition mit dem Master-Installationsprogramm auf Standard-Ports, im Hintergrund und mit unterdrücktem Neustart auf dem Standardspeicherort **C:\Program Files\Dell\Dell Data Protection\** installiert und für die Verwendung des angegebenen EE-Servers/VE-Servers konfiguriert.  
  

```
"DDPSetup.exe" -y -gm2 /S /z "\"SERVER=server.organization.com, FEATURES=BLM-EME, SUPPRESSREBOOT=1\""
```



- In diesem Beispiel wird BitLocker Manager (ohne das SED Management-Plugin) und die External Media Edition mit dem Master-Installationsprogramm auf Standardports, im Hintergrund und unterdrücktem Neustart auf dem Standardspeicherort **C:\Program Files\Dell\Dell Data Protection\** installiert und für die Verwendung des angegebenen EE-Servers/VE-Servers konfiguriert.

```
"DDPSetup.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1, SUPPRESSREBOOT=1\""
```



# Deinstallation unter Verwendung des -Master-Installationsprogramms

- Jede Komponente muss einzeln deinstalliert werden, gefolgt von der Deinstallation des -Master-Installationsprogramms. Die Clients **müssen in einer bestimmten Reihenfolge deinstalliert werden**, um Fehler bei der Deinstallation zu vermeiden.
- Folgen Sie den Anweisungen unter [Untergeordnete Installationsprogramme aus dem -Master-Installationsprogramm](#) 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 weitere Kapitel, die *ausführliche* Informationen zum Deinstallieren der untergeordneten Installationsprogramme enthalten. In diesem Kapitel wird **nur** der letzte Schritt beschrieben, die Deinstallation des -Master-Installationsprogramms.
- Deinstallieren Sie die Clients in der folgenden Reihenfolge.
  - a [Encryption-Client deinstallieren](#).
  - b [SED- und Advanced Authentication-Clients deinstallieren](#).
  - c [BitLocker Manager-Client deinstallieren](#).
- Fahren Sie mit dem Schritt [-Master-Installationsprogramm deinstallieren](#) fort.

## -Master-Installationsprogramm deinstallieren

Nach der Deinstallation der einzelnen Clients kann nun auch das -Master Installationsprogramm deinstalliert werden.

## Deinstallation über die Befehlszeile

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

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

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

# Deinstallation unter Verwendung der untergeordneten Installationsprogramme

- Um jeden Client einzeln zu deinstallieren, müssen die untergeordneten ausführbaren Dateien zuerst aus dem -Master-Installationsprogramm extrahiert werden, wie unter [Extrahieren der untergeordneten Installationsprogramme aus dem -Master-Installationsprogramm](#) angezeigt. Führen Sie alternativ dazu eine administrative Installation zum Extrahieren der .msi aus.
- Stellen Sie sicher, dass Sie für die Deinstallation dieselben Client-Versionen verwenden wie bei der Installation.
- 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 eindeutige Deinstallationsprotokolldateien des untergeordneten Installationsprogramms für den angemeldeten Benutzer 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 **/I C:\<any directory>\<any log file name>.log** erstellt werden. Der Benutzername und das Passwort werden in der Protokolldatei aufgezeichnet, daher rät Dell von der Verwendung von **"/I\*v"** (ausführliche Protokollierung) bei der Deinstallation über die Befehlszeile ab.

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

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

Schalter	Erläuterung
/v	Gibt Variablen an die .msi-Datei innerhalb der setup.exe-Datei weiter. Der Inhalt muss immer von Anführungszeichen in Klartext umrahmt sein.
/s	Im Hintergrund
/x	Deinstallationsmodus
/a	Administrative Installation (mit Kopieren aller Dateien in der .msi)

## ANMERKUNG:

Mit /v stehen die Microsoft Standardoptionen zur Verfügung. Eine Liste der Optionen finden Sie unter [https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx) .



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

## Client für Verschlüsselung und Serververschlüsselung deinstallieren

- Entfernen Sie mithilfe des Windows Festplattenbereinigungs-Assistenten temporäre Dateien und andere nicht benötigte Daten, um den Zeitaufwand für die Entschlüsselung zu verringern.
- 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 Entschlüsselungsfehler aufgrund gesperrter Dateien zu vermeiden.
- Sobald die Deinstallation abgeschlossen ist und die Entschlüsselung läuft, deaktivieren Sie die gesamte Netzwerkkonnektivität. Andernfalls werden womöglich neue Richtlinien erfasst, mit denen die Verschlüsselung wieder aktiviert wird.
- Befolgen Sie das übliche Verfahren für die Verschlüsselung von Daten, z. B. die Ausgabe einer Richtlinienaktualisierung.
- Zu Beginn einer Shield-Deinstallation aktualisieren Windows und EME Shields den EE-Server/VE-Server, um den Status in *Ungeschützt* zu ändern. Wenn der Client jedoch keine Verbindung zum EE-Server/VE-Server herstellen kann, ist keine Statusaktualisierung möglich. In diesem Fall müssen Sie ein manuelles Entfernen des Endpunkts in der Remote-Verwaltungskonsolle durchführen. Falls Ihr Unternehmen diese Vorgehensweise im Rahmen der Compliance einsetzt, empfiehlt Dell, zu überprüfen, ob in der Remote-Verwaltungskonsolle oder in Compliance Reporter erwartungsgemäß der Status *Ungeschützt* erscheint.

## Verfahren

- Der Key Server (und EE-Server) müssen vor der Deinstallation konfiguriert werden, falls Sie die Option **Encryption Removal Agent lädt Schlüssel von Server herunter** verwenden möchten. Weitere Informationen finden Sie unter [Key Server für die Deinstallation von auf EE-Server aktiviertem Encryption-Client konfigurieren](#). Falls der zu deaktivierende Client auf einem VE-Server aktiviert ist, sind keine weiteren Maßnahmen erforderlich, da der VE-Server den Key Server nicht verwendet.
- Sie müssen vor dem Starten des Encryption Removal Agent das Dell Administrator-Download-Dienstprogramm (CMGAd) verwenden, falls Sie die Option **Encryption Removal Agent importiert Schlüssel aus Datei** verwenden möchten. Über dieses Dienstprogramm erhalten Sie das Verschlüsselungsschlüsselpaket. Weitere Informationen finden Sie unter [Administrator-Download-Dienstprogramms verwenden \(CMGAd\)](#). Das Dienstprogramm ist auf dem Dell Installationsmedium enthalten.

## Deinstallation über die Befehlszeile

- Nach der Extraktion aus dem -Master-Installationsprogramm befindet sich das Installationsprogramm für den Client für die Verschlüsselung 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  3 – LSARecovery-Paket verwenden  2 – Zuvor heruntergeladenes Material für forensischen Schlüssel verwenden  1 – Schlüssel vom Dell Server herunterladen  0 – Encryption Removal Agent nicht installieren
CMGSILENTMODE	Eigenschaft für Deinstallation im Hintergrund:  1 – Im Hintergrund  0 – Nicht im Hintergrund

### Erforderliche Eigenschaften

DA_SERVER	Vollständig qualifizierter Hostname (FGHN) für den EE-Server, auf dem die Vermittlungssitzung gehostet wird.
DA_PORT	EE-Server-Port für die Anfrage (die Standardeinstellung ist 8050).
SVCPN	Benutzername im UPN-Format, unter dem der Key Server-Dienst beim EE-Server angemeldet ist.
DA_RUNAS	Benutzername im mit SAM kompatiblen Format, unter dem die Anfrage zum Schlüsselabruf erfolgt. Dieser Benutzer muss in der Key Server-Liste des EE-Servers enthalten sein.
DA_RUNASPWD	Passwort für den RUNAS-Benutzer.
FORENSIC_ADMIN	Das forensische Administratorkonto auf dem Dell Server, das für forensische Anfragen für Deinstallationen oder Schlüssel verwendet werden kann.
FORENSIC_ADMIN_PWD	Das Passwort für das Konto „Forensischer Administrator“.

### Optionale Eigenschaften

SVCLOGONUN	Benutzername im UPN-Format zur Anmeldung beim Encryption Removal Agent-Dienst als Parameter.
SVCLOGONPWD	Passwort für die Anmeldung als Benutzer.

- Im folgenden Beispiel werden im Hintergrund der Encryption-Client deinstalliert und die Verschlüsselungsschlüssel vom EE-Server heruntergeladen.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1 DA_SERVER=server.organization.com
DA_PORT=8050 SVCPN=administrator@organization.com DA_RUNAS=domain\username
DA_RUNASPWD=password /qn"
```

MSI-Befehl:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050"
SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
```

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



- Im folgenden Beispiel werden im Hintergrund der Encryption-Client deinstalliert und die Verschlüsselungsschlüssel über ein Konto vom Typ „Forensischer Administrator“ heruntergeladen.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
```

MSI-Befehl:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn CMG_DECRYPT=1 CMGSILENTMODE=1
FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit
REBOOT=REALLYSUPPRESS
```

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

### ❗ WICHTIG:

Dell empfiehlt die folgenden Aktionen bei Verwendung eines forensischen Administratorkennworts in der Befehlszeile:

- 1 Erstellen Sie in der Remote Management Console ein Konto vom Typ „Forensischer Administrator“ zum Durchführen der Deinstallation im Hintergrund.
- 2 Verwenden Sie für dieses Konto ein temporäres und befristetes Passwort.
- 3 Nach Abschluss der Deinstallation im Hintergrund entfernen Sie das temporäre Konto dann aus der Liste der Administratoren oder ändern das entsprechende Passwort.

### ❗ ANMERKUNG:

Einige ältere Clients erfordern unter Umständen Escape-Zeichen \" um die Werte von Parametern. Beispiel:

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=
\"server.organization.com\" DA_PORT=\"8050\" SVCPN=\"administrator@organization.com\"
DA_RUNAS=\"domain\username\" DA_RUNASPWD=\"password\" /qn"
```

## External Media Edition deinstallieren

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

### Deinstallation über die Befehlszeile

Führen Sie einen Befehl nach folgendem Schema aus:

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

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

## Deinstallation der SED- und Advanced Authentication-Clients

- Zur PBA-Deaktivierung muss eine Netzwerkverbindung zum EE-Server/VE-Server bestehen.

## Verfahren

- Deaktivieren Sie die PBA; dabei werden alle PBA-Daten vom Computer entfernt und die SED-Schlüssel entsperrt.
- Deinstallieren Sie den SED-Client.
- Deinstallieren Sie den Advanced Authentication-Client.

## PBA deaktivieren

- 1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.
- 2 Klicken Sie im linken Bereich auf **Schutz und Verwaltung > Endpunkte**.
- 3 Wählen Sie den entsprechenden Endpunkttyp aus.
- 4 Wählen Sie Anzeigen > *Sichtbar, Ausgeblendet* oder *Alle* aus.
- 5 Wenn der Hostname des Computers bekannt ist, geben Sie ihn im Feld „Hostname“ ein (Platzhalter werden unterstützt). Sie können das Feld leer lassen, um alle Computer anzuzeigen. Klicken Sie auf **Suchen**.

Wenn Sie den Hostnamen nicht kennen, machen Sie den Computer in der Liste ausfindig.

Je nach Suchfilter wird ein Computer oder eine Liste von Computern angezeigt.

- 6 Klicken Sie auf das Symbol **Details** des gewünschten Computers.
- 7 Klicken Sie im Hauptmenü auf **Sicherheitsrichtlinien**.
- 8 Wählen Sie **Selbstverschlüsselnde Laufwerke** aus dem Drop-down-Menü **Richtlinienkategorie** aus.
- 9 Erweitern Sie den Bereich **SED-Verwaltung**, und ändern Sie die Richtlinien **SED-Verwaltung aktivieren** und **PBA aktivieren** von *True* in **False**.
- 10 Klicken Sie auf **Speichern**.
- 11 Klicken Sie im linken Bereich auf **Aktionen > Richtlinien bestätigen**.
- 12 Klicken Sie auf **Änderungen anwenden**.

Warten Sie, während die Richtlinie vom EE-Server/VE-Server auf den für die Deaktivierung vorgesehenen Computer übertragen wird.

Deinstallieren Sie nach der Deaktivierung von PBA den SED- und die Authentication-Clients.

## Deinstallieren des SED-Clients und der Advanced Authentication-Clients

### Deinstallation über die Befehlszeile

- Nach der Extrahierung aus dem -Master-Installationsprogramm befindet sich das SED-Client-Installationsprogramm unter **C:\extracted\Security Tools\EMAgent\_XXbit\_setup.exe**.
- Nach der Extrahierung aus dem -Master-Installationsprogramm befindet sich das SED-Client-Installationsprogramm unter **C:\extracted\Security Tools\Authentication\<x64/x86>\setup.exe**.
- Im folgenden Beispiel wird der SED-Client im Hintergrund deinstalliert.

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

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

Dann:

- Im folgenden Beispiel wird der Advanced Authentication-Client im Hintergrund deinstalliert.

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

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



# Deinstallation des BitLocker Manager-Clients

## Deinstallation über die Befehlszeile

- Nach der Extraktion aus dem -Master-Installationsprogramm befindet sich das BitLocker-Installationsprogramm unter **C:\extracted\Security Tools\EMAgent\_XXbit\_setup.exe**.
- Im folgenden Beispiel wird der BitLocker Manager-Client im Hintergrund deinstalliert.

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

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

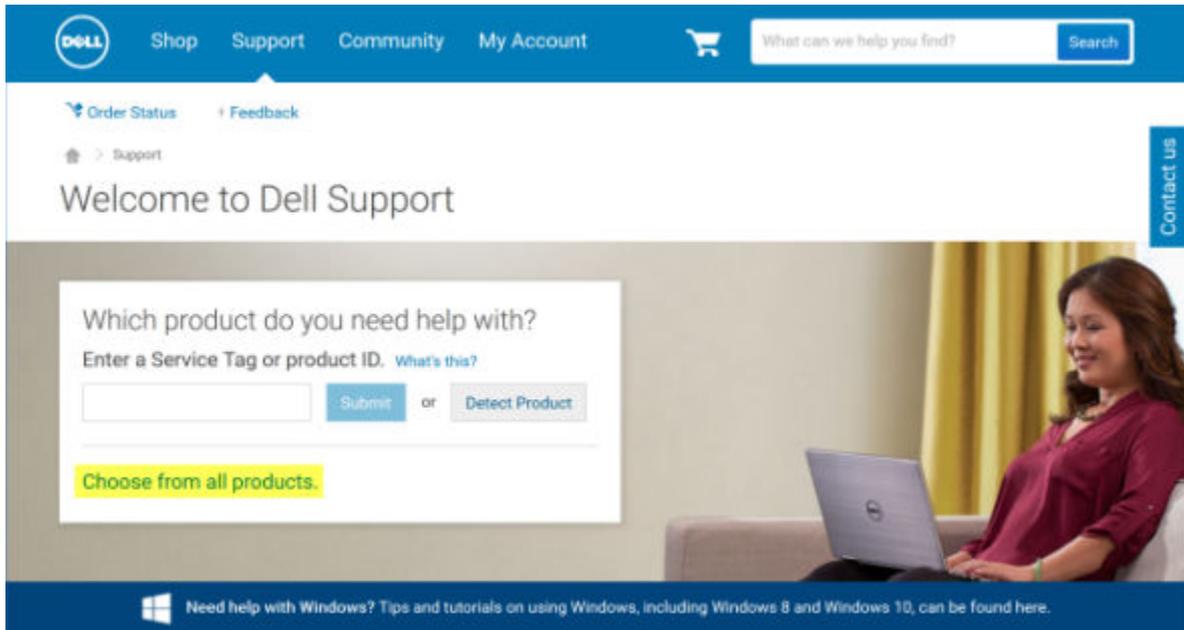


# Herunterladen der Software

Dieser Abschnitt erläutert den Bezug der Software unter [dell.com/support](https://dell.com/support). Wenn Sie die Software bereits haben, können Sie diesen Abschnitt überspringen.

Rufen Sie [dell.com/support](https://dell.com/support) auf, um zu beginnen.

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



- 2 Wählen Sie **Software und Sicherheit** aus der Produktliste aus.
- 3 Wählen Sie im Abschnitt *Software und Sicherheit* **Endpoint Security Solutions** aus.  
Wenn diese Auswahl einmal vorgenommen wurde, wird sie von der Website gespeichert.
- 4 Wählen Sie die Dell Data Protection Produkt.  
Beispiele:

## Dell Verschlüsselung

### Dell Endpoint Security Suite

### Dell Endpoint Security Suite Enterprise

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





Support topics & articles

Drivers & downloads

Manuals

## Optimize your system with drivers and updates. [1](#)

View all available updates for Windows 10, 64-bit. [Change OS](#)

- Apple Mac OS
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- Windows 10, 32-bit
- Windows 10, 64-bit
- Windows 7, 32-bit
- Windows 7, 64-bit
- Windows 8, 32-bit
- Windows 8, 64-bit
- Windows 8.1, 32-bit
- Windows 8.1, 64-bit
- Windows Server 2003
- Windows Server 2003 x64
- Windows Server 2008 R2
- Windows Server 2008 x64
- Windows Server 2008 x86
- Windows Server 2012 R2

Looking for a different OS? [View the list of Dell supported operating systems](#)

Refine your results:

Category

Importance

Contact us

8 Wählen Sie **Datei herunterladen** oder **Zu meiner Downloadliste #XX hinzufügen** aus.



# Untergeordnete Installationsprogramme aus dem -Master-Installationsprogramm extrahieren

- Das -Master-Installationsprogramm ist kein *Master-Deinstallationsprogramm*. Jeder Client muss einzeln deinstalliert werden, gefolgt von der Deinstallation des -Master-Installationsprogramms. Verwenden Sie dieses Verfahren zum Extrahieren der Clients aus dem -Master-Installationsprogramm, sodass sie für die Deinstallation verwendet werden können.

- 1 Kopieren Sie vom Dell-Installationsmedium die Datei **DDPSetup.exe** auf den lokalen Computer.
- 2 Öffnen Sie am gleichen Speicherort wie die Datei **DDPSetup.exe** eine Eingabeaufforderung, und geben Sie Folgendes ein:

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

Der Extraktionspfad darf maximal 63 Zeichen enthalten.

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



# Konfiguration des Key Servers für die Deinstallation des auf einem EE-Server aktivierten Encryption-Clients

- In diesem Abschnitt wird beschrieben, wie Komponenten für die Verwendung mit der Kerberos-Authentifizierung/-Autorisierung bei Verwendung eines EE-Servers konfiguriert werden. Der VE-Server verwendet den Key Server nicht.
- Wenn die Kerberos-Authentifizierung/-Autorisierung verwendet werden soll, muss der Server, der die Key Server-Komponente enthält, zur betroffenen Domäne gehören.
- Da der VE-Server den Key Server nicht verwendet, ist die typische Deinstallation beeinträchtigt. Wenn ein Encryption-Client deinstalliert wird, der auf einem VE-Server aktiviert ist, wird anstelle der Kerberos-Methode des Key Servers der standardmäßige, forensische Schlüsselabruf über den Security Server genutzt. Weitere Informationen finden Sie unter [Befehlszeilen-Deinstallation](#).

## Dialogfeld „Dienste“ - Domänenbenutzerkonto hinzufügen

- 1 Navigieren Sie auf dem EE-Server zum Dialogfeld „Dienste“ (Start > Ausführen... > services.msc > OK)
- 2 Klicken Sie mit der rechten Maustaste auf „Dell Key Server“ und wählen Sie **Eigenschaften** aus.
- 3 Rufen Sie die Registerkarte „Anmelden“ auf, und wählen Sie die Option **Dieses Konto:** aus.

Geben Sie in das Feld *Dieses Konto:* den gewünschten Domänenbenutzer ein. Dieser Domänenbenutzer muss mindestens über lokale Administratorrechte für den Key Server-Ordner verfügen (er muss Schreibzugriff für die Key Server-Konfigurationsdatei und die Datei „log.txt“ besitzen).

Geben Sie das Passwort für den Domänenbenutzer ein, und wiederholen Sie es.

Klicken Sie auf **OK**

- 4 Starten Sie den Key Server-Dienst neu (lassen Sie das Dialogfeld „Dienste“ für weitere Arbeitsschritte geöffnet).
- 5 Navigieren Sie zu „<Key Server-Installationsverzeichnis> log.txt“, um zu überprüfen, ob der Dienst korrekt gestartet wurde.

## Schlüsselserver-Konfigurationsdatei - Fügen Sie Benutzer für EE-Server-Kommunikation hinzu

- 1 Navigieren Sie zu <Key Server-Installationsverzeichnis>.
- 2 Öffnen Sie **Credant.KeyServer.exe.config** mit einem Texteditor.
- 3 Gehen Sie zu <add key="user" value="superadmin" /> und ändern Sie den Wert „superadmin“ in den Namen des entsprechenden Benutzers (Sie können auch „superadmin“ stehen lassen).
- 4 Gehen Sie zu <add key="epw" value="<verschlüsselter Wert des Passworts>" /> und ändern Sie „epw“ in „password“. Ändern Sie dann „<verschlüsselter Wert des Passworts>“ in das Passwort des Benutzers aus Schritt 3. Beim Neustart des EE-Servers wird dieses Passwort neu verschlüsselt.

Wenn Sie in Schritt 3 „superadmin“ verwendet haben und das Superadmin-Passwort nicht „changeit“ lautet, muss es hier geändert werden. Speichern und schließen Sie die Datei.

# Dialogfeld „Dienste“ - Key Server-Dienst neu starten

- 1 Gehen Sie zurück zum Dialogfeld „Dienste“ (Start > Ausführen... > services.msc > OK).
- 2 Führen Sie einen Neustart des Key Server-Dienstes durch.
- 3 Navigieren Sie zu „<Key Server-Installationsverzeichnis> log.txt“, um zu überprüfen, ob der Dienst korrekt gestartet wurde.
- 4 Schließen Sie das Dialogfeld „Dienste“.

# Remote Management-Konsole - Hinzufügen eines forensischen Administrators

- 1 Melden Sie sich gegebenenfalls bei der Remote Management Console an.
- 2 Klicken Sie auf **Bestückung > Domänen**.
- 3 Wählen Sie die gewünschte Domäne aus.
- 4 Klicken Sie auf die Registerkarte **Key Server**.
- 5 Fügen Sie im Feld „Konto“ den Benutzer hinzu, der die Administratortasks ausführt. Das Format lautet: DOMÄNE\Benutzername. Klicken Sie auf **Konto hinzufügen**.
- 6 Klicken Sie im linken Menü auf **Benutzer**. Geben Sie in das Suchfeld den in Schritt 5 hinzugefügten Benutzernamen ein. Klicken Sie auf **Suchen**.
- 7 Sobald der korrekte Benutzer gefunden wurde, klicken Sie auf die Registerkarte **Admin**.
- 8 Wählen Sie **Forensischer Administrator** und klicken Sie auf **Aktualisieren**.  
Die Komponenten sind nun für die Kerberos-Authentifizierung/-Autorisierung konfiguriert.



# Verwenden Sie das administrative Dienstprogramm zum Herunterladen (CMGAd)

- Mit diesem Dienstprogramm können Sie Schlüsseldatenpakete zur Verwendung auf einem Computer herunterladen, der nicht mit einem EE-Server/VE-Server verbunden ist.
- Je nachdem, welche Befehlszeilenparameter an die Anwendung übergeben werden, verwendet das Dienstprogramm eine der folgenden Methoden zum Herunterladen von Schlüsselpaketen:
  - Forensischer Modus – wird bei Ausführung des Befehlszeilenparameters -f verwendet, oder wenn kein Befehlszeilenparameter verwendet wird.
  - Admin-Modus – wird bei Ausführung des Befehlszeilenparameters -a verwendet.

Die Protokolldateien befinden sich unter `C:\ProgramData\CmgAdmin.log`

## Verwenden des Administrator-Download-Dienstprogramms im forensischen Modus

- 1 Doppelklicken Sie auf **cmgad.exe** beim Start des Dienstprogramms oder öffnen Sie eine Eingabeaufforderung, wo sich CMGAd befindet, und geben Sie **cmgad.exe -f** (oder **cmgad.exe**) ein.
- 2 Geben Sie die folgenden Informationen ein (einige Felder sind möglicherweise bereits ausgefüllt).  
 URL des Device Servers: Vollständig qualifizierte URL für den Security Server (Device Server). Das Format lautet: `https://securityserver.domain.com:8443/xapi/`. Bei älteren Versionen als EE Server v7.7 gilt das Format `https://deviceserver.domain.com:8081/xapi` (andere Port-Nummer, ohne den nachfolgenden Schrägstrich).  
  
 Dell Admin: Name des Administrators mit forensischen Zugriffsrechten (aktiviert in der Remote-Verwaltungskonsole), z. B. „hschmidt“  
  
 Passwort: Forensisches Administrator-Passwort  
  
 MCID: Geräte-ID, z. B. `machinelD.domain.com`  
  
 DCID: die ersten acht Stellen der 16-stelligen Shield-ID

### ① TIPP:

In der Regel genügt es, entweder die MCID *oder* die DCID anzugeben. Wenn jedoch beide Werte bekannt sind, empfiehlt es sich, beide einzugeben. Jeder Parameter enthält unterschiedliche Informationen zum Client und Client-Computer.

Klicken Sie auf **Weiter**.

- 3 Geben Sie in das Feld „Passphrase:“ eine Passphrase ein, um die heruntergeladene Datei zu schützen. Die Passphrase muss mindestens acht Zeichen enthalten, darunter mindestens einen Buchstaben und eine Ziffer. Bestätigen Sie die Passphrase. Akzeptieren Sie entweder die Standardwerte für Dateinamen und Speicherort, oder klicken Sie auf ..., um einen anderen Speicherort auszuwählen.

Klicken Sie auf **Weiter**.

Eine Meldung zeigt an, dass die Schlüsseldaten erfolgreich entsperrt wurden. Die Dateien sind jetzt frei zugänglich.

- 4 Klicken Sie anschließend auf **Fertig stellen**.

# Verwenden des Administrator-Download-Dienstprogramms im Admin-Modus

Der VE-Server verwendet den Key Server nicht, d. h. im Admin-Modus kann kein Schlüsselpaket über den VE-Server abgerufen werden. Verwenden Sie den forensischen Modus, um das Schlüsselpaket zu erhalten, wenn der Client auf einem VE-Server aktiviert ist.

- 1 Öffnen Sie am Speicherort von CMGAd eine Befehlseingabe, und geben Sie **cmgad.exe -a** ein.
- 2 Geben Sie die folgenden Informationen ein (einige Felder sind möglicherweise bereits ausgefüllt).

Server: Vollständiger Hostname des Key Server, z. B. keyserver.domain.com

Portnummer: der Standardport ist 8050

Server-Konto: der Domänenbenutzer, unter dem der Key Server ausgeführt wird. Das Format lautet „Domäne\Benutzername“. Der Domänenbenutzer, der das Dienstprogramm ausführt, muss über die Berechtigung zum Download vom Key Server verfügen.

MCID: Geräte-ID, z. B. machinelD.domain.com

DCID: die ersten acht Stellen der 16-stelligen Shield-ID

## TIPP:

In der Regel genügt es, entweder die MCID *oder* die DCID anzugeben. Wenn jedoch beide Werte bekannt sind, empfiehlt es sich, beide einzugeben. Jeder Parameter enthält unterschiedliche Informationen zum Client und Client-Computer.

Klicken Sie auf **Weiter**.

- 3 Geben Sie in das Feld „Passphrase:“ eine Passphrase ein, um die heruntergeladene Datei zu schützen. Die Passphrase muss mindestens acht Zeichen enthalten, darunter mindestens einen Buchstaben und eine Ziffer.  
Bestätigen Sie die Passphrase.

Akzeptieren Sie entweder die Standardwerte für Dateinamen und Speicherort, oder klicken Sie auf ..., um einen anderen Speicherort auszuwählen.

Klicken Sie auf **Weiter**.

Eine Meldung zeigt an, dass die Schlüsseldaten erfolgreich entsperrt wurden. Die Dateien sind jetzt frei zugänglich.

- 4 Klicken Sie anschließend auf **Fertig stellen**.



# Fehlerbehebung

## Alle Clients – Fehlerbehebung

- Die Protokolldateien des **-Master-Installationsprogramms** befinden sich unter `C:\ProgramData\Dell\Dell Data Protection\Installer`.
- Windows erstellt für den angemeldeten Benutzer eindeutige Installationsprotokolldateien des untergeordneten Installationsprogramms im Verzeichnis „%temp%“ unter `C:\Users\\AppData\Local\Temp`.
- Windows erstellt Protokolldateien für Client-Voraussetzungen, z. B. Visual C++, für den angemeldeten Benutzer im Verzeichnis „%Temp%“ unter `C:\Users\\AppData\Local\Temp`. For example, `C:\Users\\AppData\Local\Temp\dd_vcredist_amd64_20160109003943.log`
- Befolgen Sie die Anleitungen unter <http://msdn.microsoft.com>, um die Version von Microsoft .Net zu überprüfen, die auf dem Computer installiert ist, auf dem die Installation erfolgen soll.

Gehen Sie zu <https://www.microsoft.com/en-us/download/details.aspx?id=30653>, um die vollständige Version von Microsoft .Net Framework 4.5 herunterzuladen.

- Siehe *Dell Data Protection | Security Tools Compatibility*, wenn auf dem Computer, der für die Installation vorgesehen ist (oder in der Vergangenheit war) "Dell Access" installiert ist. DDP|A ist nicht kompatibel mit dieser Suite von Produkten.

## Fehlerbehebung für den Client für Verschlüsselung und Serververschlüsselung

## Upgrade auf die Windows 10 Anniversary-Aktualisierung

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

## Aktivierung auf einem Serverbetriebssystem

Wenn die Verschlüsselung auf einem Serverbetriebssystem installiert ist, erfordert die Aktivierung zwei Phasen: erstmalige Aktivierung und Geräteaktivierung.

### Fehlerbehebung bei der erstmaligen Aktivierung

Die erstmalige Aktivierung schlägt fehl, wenn:

- Mithilfe der bereitgestellten Anmeldeinformationen kein gültiger UPN erstellt werden kann.
- Die Anmeldeinformationen in der Enterprise Vault nicht gefunden werden.
- Die zur Aktivierung verwendeten Anmeldeinformationen nicht die des Domänenadministrators sind.

### Fehlermeldung: Unbekannter Benutzername oder ungültiges Passwort

Der Benutzername oder das Passwort stimmen nicht überein.

Mögliche Lösung: Versuchen Sie, sich erneut anzumelden, und achten Sie genau auf die korrekte Eingabe von Benutzernamen und Passwort.

**Fehlermeldung: Die Aktivierung ist fehlgeschlagen, weil das Benutzerkonto nicht über Domänenadministrator-Rechte verfügt.**

Die für die Aktivierung verwendeten Anmeldeinformationen haben keine Domänenadministrator-Rechte, oder der Administrator-Benutzername lag nicht im UPN-Format vor.

Mögliche Lösung: Geben Sie im Aktivierungsdialog die Anmeldeinformationen eines Domänenadministrators ein und stellen Sie sicher, dass diese das UPN-Format haben.

#### **Fehlermeldung: Es konnte keine Verbindung zum Server aufgebaut werden.**

oder

The operation timed out.

Serververschlüsselung konnte an Port 8449 nicht über https mit dem DDP Security Server kommunizieren.

#### **Mögliche Lösungen**

- Verbinden Sie sich direkt mit dem Netzwerk und versuchen Sie die Aktivierung erneut.
- Wenn Sie über VPN verbunden sind, dann versuchen Sie, sich direkt mit dem Netzwerk zu verbinden und versuchen Sie die Aktivierung erneut.
- Überprüfen Sie die DDP-Server-URL um sicherzustellen, dass diese mit der durch den Administrator bereitgestellten URL übereinstimmt. Die URL und andere vom Benutzer im Installationsprogramm eingegebene Daten werden in der Registrierungsdatenbank gespeichert. Überprüfen Sie die Richtigkeit der Daten unter [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] und [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].
- Trennen Sie den Server vom Netzwerk. Starten Sie den Server neu und verbinden Sie ihn wieder mit dem Netzwerk.

#### **Fehlermeldung: Die Aktivierung ist fehlgeschlagen, weil der Server diese Anfrage nicht unterstützt.**

#### **Mögliche Lösungen**

- Die Serververschlüsselung kann nicht mit einem Legacy-Server aktiviert werden; die DDP Serverversion muss 9.1 oder höher sein. Aktualisieren Sie Ihren DDP-Server bei Bedarf auf Version 9.1 oder höher.
- Überprüfen Sie die DDP-Server-URL um sicherzustellen, dass diese mit der durch den Administrator bereitgestellten URL übereinstimmt. Die URL und andere vom Benutzer im Installationsprogramm eingegebene Daten werden in der Registrierungsdatenbank gespeichert.
- Überprüfen Sie die Richtigkeit der Daten unter [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] und [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].

#### **Ablauf der erstmaligen Aktivierung**

Das folgende Diagramm zeigt eine erfolgreiche erstmalige Aktivierung.

Bei der erstmaligen Aktivierung der Serververschlüsselung muss ein echter Benutzer auf den Server zugreifen. Der Benutzer kann beliebig sein: zur Domäne gehörig oder nicht, verbunden per Remote-Desktop oder interaktiv, aber er muss in jedem Fall Zugriff auf die Anmeldeinformationen des Domänenadministrators haben.

Das Dialogfeld zur Aktivierung wird angezeigt, wenn eins der beiden folgenden Ereignisse eintritt:

- Ein neuer (nicht verwalteter) Benutzer meldet sich am Computer an.
- Ein neuer Benutzer klickt mit der rechten Maustaste im Systembereich auf das Symbol des Clients für die Verschlüsselung und aktiviert Dell Encryption.

Der Ablauf für die erstmalige Aktivierung ist wie folgt:

- 1 Der Benutzer meldet sich an.
- 2 Bei der Erkennung eines neuen (nicht verwalteten) Benutzers wird das Dialogfenster für die Aktivierung angezeigt. Der Benutzer klickt auf **Abbrechen**.
- 3 Der Benutzer öffnet das Feld „Info“ der Serververschlüsselung, um zu bestätigen, dass sie im Servermodus ausgeführt wird.
- 4 Der Benutzer klickt mit der rechten Maustaste im Systembereich auf das Symbol des Clients für die Verschlüsselung und wählt **Dell Encryption aktivieren**.
- 5 Der Benutzer gibt die Anmeldeinformationen des Domänenadministrators im Dialogfenster für die Aktivierung ein.



### ANMERKUNG:

Die Anforderung der Anmeldeinformationen des Domänenadministrators ist eine Sicherheitsmaßnahme, die verhindert, dass die Serververschlüsselung auf Serverumgebungen eingeführt wird, die sie nicht unterstützen. So deaktivieren Sie die Anforderung der Anmeldeinformationen des Domänenadministrators: [Bevor Sie beginnen](#).

- 6 Der DDP Server gleicht die Anmeldeinformationen in der Enterprise Vault (Active Directory oder gleichwertig) ab, um zu überprüfen, ob es sich um Anmeldeinformationen des Domänenadministrators handelt.
- 7 Mit den Anmeldeinformationen wird ein UPN erstellt.
- 8 Mit dem UPN erstellt der DDP Server ein neues Benutzerkonto für den virtuellen Serverbenutzer und speichert die Anmeldeinformationen in der Vault des DDP Servers.

Das **virtuelle Serverbenutzerkonto** gilt ausschließlich für die Verwendung des Clients für die Verschlüsselung. Er wird zur Authentifizierung am Server, zum Umgang mit gängigen Verschlüsselungsschlüsseln und zum Empfang von Richtlinien-Updates verwendet.

### ANMERKUNG:

Passwort und DPAPI-Authentifizierung sind für dieses Konto deaktiviert, sodass *nur* der virtuelle Serverbenutzer auf dem Computer auf Verschlüsselungsschlüssel zugreifen kann. Dieses Konto ist unabhängig von allen anderen Benutzerkonten auf dem Computer oder in der Domäne.

- 9 Nach erfolgreicher Aktivierung startet der Benutzer den Computer neu, wodurch der zweite Teil der Aktivierung eingeleitet wird: die Authentifizierung und Geräteaktivierung.

## Fehlerbehebung bei Authentifizierung und Geräteaktivierung

Die Geräteaktivierung schlägt fehl, wenn:

- Die erstmalige Aktivierung fehlgeschlagen ist.
- Keine Verbindung zum Server aufgebaut werden konnte.
- Das Vertrauenszertifikat nicht überprüft werden konnte.

Nach der Aktivierung, wenn der Computer neu gestartet wird, meldet sich die Serververschlüsselung automatisch als virtueller Serverbenutzer an und fordert den Computerschlüssel vom DDP Enterprise Server an. Dies findet bereits statt, bevor sich sonst ein Benutzer anmelden kann.

- Öffnen Sie das Dialogfeld „Info“, um zu bestätigen, dass die Serververschlüsselung authentifiziert und im Servermodus ist.
- Wenn die Shield ID rot ist, wurde die Verschlüsselung noch nicht aktiviert.
- In der Remote Management Console wird die Version eines Servers mit installierter Serververschlüsselung aufgeführt als *Shield für Server*.
- Wenn der Abruf des Computerschlüssels aufgrund eines Netzwerkfehlers fehlschlägt, meldet die Serververschlüsselung sich für Netzwerkbenachrichtigungen im Betriebssystem an.
- Wenn der Abruf des Computerschlüssels fehlschlägt:
  - Die virtuelle Serverbenutzeranmeldung ist nach wie vor erfolgreich.
  - Richten Sie die Richtlinie *Intervall für Neuversuch nach Netzwerkfehler* ein, um Schlüsselabrufversuche in festen Zeitabständen durchzuführen.

Weitere Einzelheiten zur Richtlinie *Intervall für Neuversuch nach Netzwerkfehler* erhalten Sie unter AdminHelp in der Remote Management Console.

## Ablauf der Authentifizierung und Geräteaktivierung

Das folgende Diagramm stellt eine erfolgreiche Authentifizierung und Geräteaktivierung dar.

- 1 Nach dem Neustart nach einer erfolgreichen erstmaligen Aktivierung wird ein Computer mit Serververschlüsselung automatisch für die Verwendung des virtuellen Serverbenutzerkontos authentifiziert und führt den Client für die Verschlüsselung im Servermodus aus.

- 2 Der Computer gleicht den Status seiner Geräteaktivierung am DDP Server ab:
  - Wenn für den Computer bisher keine Geräteaktivierung erfolgt ist, weist der DDP Server ihm eine MCID, eine DCID und ein Vertrauenszertifikat zu und speichert alle Informationen im Vault des DDP Server.
  - Wenn für den Computer bereits eine Geräteaktivierung erfolgt ist, überprüft der DDP Server das Vertrauenszertifikat.
- 3 Nachdem der DDP Server dem Server das Vertrauenszertifikat zugewiesen hat, kann er auf dessen Verschlüsselungsschlüssel zugreifen.
- 4 Die Geräteaktivierung ist erfolgreich.

**ANMERKUNG:**

Um bei der Ausführung im Servermodus Zugang zu den Verschlüsselungsschlüsseln zu erhalten, muss der Client für die Verschlüsselung auf dasselbe Zertifikat zugreifen, das zur Geräteaktivierung verwendet wurde.

## EMS und PCS Interaktionen

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

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

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

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

## WSScan verwenden

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

### Ausführen von WSScan

- 1 Kopieren Sie „WSScan.exe“ von den Dell Installationsmedien auf den Windows-Computer.
- 2 Öffnen Sie am obigen Speicherort eine Befehlszeile, und geben Sie an der Eingabeaufforderung **wsscan.exe** ein. WSScan wird gestartet.
- 3 Klicken Sie auf **Erweitert**.
- 4 Wählen Sie den Typ des zu prüfenden Laufwerks aus dem Drop-Down-Menü aus: *Alle Laufwerke*, *Feste Laufwerke*, *Wechsellaufwerke* oder *CD-ROMs/DVDROMs*.
- 5 Wählen Sie den gewünschten Berichtstyp für die Verschlüsselung aus dem Drop-Down-Menü aus: *Verschlüsselte Dateien*, *Unverschlüsselte Dateien*, *Alle Dateien* oder *Unverschlüsselte Dateien verletzt*:
  - *Verschlüsselte Dateien* – Um sicherzustellen, dass alle Daten bei der Deinstallation des Clients für die Verschlüsselung entschlüsselt werden. Befolgen Sie das übliche Verfahren für die Entschlüsselung von Daten, z. B. die Ausgabe einer Richtlinienaktualisierung für die Entschlüsselung. Nach der Entschlüsselung der Daten und vor dem Neustart zur Vorbereitung der Deinstallation führen Sie bitte den WSScan aus, um zu gewährleisten, dass alle Daten entschlüsselt sind.
  - *Unverschlüsselte Dateien* – Um Dateien zu identifizieren, die nicht verschlüsselt sind, einschließlich einem Hinweis, ob sie verschlüsselt sein sollten (J/N).
  - *Alle Dateien* – Zum Auflisten aller verschlüsselten und unverschlüsselten Dateien einschließlich einem Hinweis, ob sie verschlüsselt sein sollten (J/N).
  - *Unverschlüsselte Dateien verletzt* – Um nicht verschlüsselte Dateien zu erkennen, die verschlüsselt sein sollten.



6 Klicken Sie auf **Suchen**.

ODER

- 1 Klicken Sie auf **Erweitert**, um zur Ansicht **Einfach** zu wechseln und einen bestimmten Ordner zu durchsuchen.
- 2 Wechseln Sie zu „Sucheinstellungen“, und geben Sie im Feld **Suchpfad** den Ordnerpfad ein. Wenn Sie dieses Feld verwenden, wird die Auswahl im Drop-Down-Feld ignoriert.
- 3 Falls die Ausgabe des Suchdienstprogramms „WSScan“ nicht in einer Datei gespeichert werden soll, deaktivieren Sie das Kontrollkästchen **Ausgabe in Datei**.
- 4 Ändern Sie unter *Pfad* ggf. den Standardpfad und den Standarddateinamen.
- 5 Wählen Sie **Zu vorhandener Datei hinzufügen** aus, wenn Sie bereits bestehende WSScan-Ausgabedateien nicht überschreiben möchten.
- 6 Wählen Sie das Ausgabeformat aus:
  - Wählen Sie Berichtsformat, um eine Liste der Berichtsstile für das Suchergebnis zu erhalten. Das ist das Standardformat.
  - Wählen Sie Datei mit Wertbegrenzung für eine Ausgabe, die in eine Tabellenkalkulation importiert werden kann. Das Standardtrennzeichen ist „|“, doch können auch bis zu 9 alphanumerische Zeichen, Leerzeichen oder Zeichensetzungszeichen der Tastatur verwendet werden.
  - Wählen Sie die Option Werte in Anführungszeichen, damit jeder Wert in doppelte Anführungszeichen gesetzt wird.
  - Wählen Sie „Datei mit fester Breite“ für eine Ausgabe ohne Trennzeichen aus, die eine durchgängige Zeile von Informationen fester Breite über jede verschlüsselte Datei enthält.
- 7 Klicken Sie auf **Suchen**.

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

## WSScan-Ausgabe

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

Beispiel der Ausgabe:

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

Ausgabe	Erläuterung
Zeitstempel	Das Datum und die Uhrzeit der Durchsuchung der Datei.
Verschlüsselungstyp	Die Art der Verschlüsselung für die Datei. <b>SysData:</b> SDE-Verschlüsselungscode. <b>Benutzer:</b> Benutzer-Verschlüsselungscode. <b>Allgemein:</b> Allgemeiner Verschlüsselungscode. WSScan meldet keine Dateien, die mittels „Für Freigabe verschlüsseln“ verschlüsselt wurden.
KCID	Die ID des Schlüssel-Computers. Im Beispiel oben „ <b>7vdlxrsb</b> “ Wenn Sie ein zugeordnetes Netzwerklaufwerk durchsuchen, gibt der Abfragebericht keine KCID aus.
UCID	Die Benutzer-ID. Im Beispiel oben „ <b>_SDENCR_</b> “ Die UCID ist für alle Benutzer des Computers gleich.

Ausgabe	Erläuterung
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 „ <b>is still AES256 encrypted</b> “  Rijndael 128  Rijndael 256  AES 128  AES 256  3DES

## Überprüfen des Encryption-Removal-Agent-Status

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

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



# Dell ControlVault-Treiber

## Aktualisieren von Treibern und Firmware für Dell ControlVault

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

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

### Herunterladen der aktuellen Treiber

- 1 Gehen Sie zu [support.dell.com](http://support.dell.com).
- 2 Wählen Sie Ihr Computermodell aus.
- 3 Wählen Sie **Treiber & Downloads**.
- 4 Wählen Sie das auf dem Zielcomputer ausgeführte **Betriebssystem** aus.
- 5 Erweitern Sie die Kategorie **Sicherheit**.
- 6 Laden Sie die Dell ControlVault-Treiber herunter, und speichern Sie sie.
- 7 Laden Sie die Dell ControlVault-Firmware herunter, und speichern Sie sie.
- 8 Kopieren Sie die Treiber und die Firmware bei Bedarf auf die Zielcomputer.

### Installieren des Dell ControlVault-Treibers

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

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



Achten Sie darauf, als Erstes den Treiber zu installieren. Der Dateiname des Treibers *zum Zeitpunkt der Erstellung dieses Dokuments* lautet „ControlVault\_Setup\_2MYJC\_A37\_ZPE.exe“.

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

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

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

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

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

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

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

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

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

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

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

### Überprüfen der Treiberinstallation

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

## Installieren der Dell ControlVault-Firmware

- 1 Gehen Sie zu dem Ordner, in den Sie die Firmware-Installationsdatei abgelegt haben.
- 2 Doppelklicken Sie auf die Dell ControlVault-Firmware, um die selbstextrahierende EXE-Datei aufzurufen.
- 3 Klicken Sie zum Fortsetzen des Vorgangs auf **Weiter**.
- 4 Klicken Sie auf **OK**, um die Treiberdateien in den Standardordner **C:\Dell\Drivers\ zu entpacken.**
- 5 Klicken Sie auf **Ja**, um die Erstellung eines neuen Ordners zu genehmigen.
- 6 Klicken Sie auf **OK**, wenn die Nachricht angezeigt wird, dass die Dateien erfolgreich entpackt wurden.
- 7 Nach dem Entpacken wird der Ordner angezeigt, der die entpackten Dateien enthält. Ist dies nicht der Fall, gehen Sie zu dem Ordner, in den Sie die Dateien entpackt haben. Wählen Sie den Ordner **Firmware** aus.
- 8 Doppelklicken Sie auf die Datei **ushupgrade.exe**, um das Firmware-Installationsprogramm zu starten.
- 9 Klicken Sie zum Starten der Firmware auf **Start**.



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

Es werden nun verschiedene Statusmeldungen angezeigt.

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

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

## Glossar

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

**BitLocker Manager** – Windows BitLocker schützt Windows-Computer durch die Verschlüsselung von Daten- und Betriebssystemdateien. Um die Sicherheit von BitLocker-Implementierungen zu erhöhen und Betriebskosten zu vereinfachen sowie zu verringern, bietet Dell eine einzige, zentrale Management Console. Diese Console nimmt sich zahlreicher Sicherheitsbedenken an und bietet einen integrierten Ansatz für die Verwaltung verschlüsselter Daten auf Plattformen, die nicht zu BitLocker gehören, seien sie physisch, virtuell oder cloudbasiert. BitLocker Manager unterstützt BitLocker-Verschlüsselung für Betriebssysteme, Festplattenlaufwerke und BitLocker To Go. Mit BitLocker Manager können Sie BitLocker nahtlos in Ihre bestehende Verschlüsselung integrieren und mit minimalem Verwaltungsaufwand sowohl die Sicherheit als auch die Compliance optimieren. BitLocker Manager bietet eine integrierte Verwaltung für die Wiederherstellung von Schlüsseln, Richtlinienverwaltung und -durchsetzung, automatisierte TPM-Verwaltung, FIPS-Compliance und Compliance Reporting.

**Deaktivieren** – Die Deaktivierung erfolgt, wenn SED Management in der Remote-Verwaltungskonsole auf OFF gesetzt wird. Nach der Deaktivierung des Computers wird die PBA -Datenbank gelöscht, und es gibt keine Aufzeichnung der im Cache gespeicherten Benutzer mehr.

**EMS (External Media Shield)** - externe Medienabschirmung - Dieses Service innerhalb des Dell Encryption Client wendet Richtlinien auf Wechseldatenträger und externe Speichergeräte an.

**EMS-Zugriffscodes** - Dieses Service innerhalb des Dell Enterprise Server/VE ermöglicht die Wiederherstellung von EMS-geschützten Geräten, wenn der Benutzer sein Kennwort vergessen hat und sich nicht mehr anmelden kann. Nach Abschluss dieses Vorgangs kann der Benutzer das auf dem Wechseldatenträger oder einem externen Speichergerät festgelegte Kennwort zurücksetzen.

**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.

**Endpunkt** – ein Computer oder eine mobile Hardwarekomponente, der/die von Dell Enterprise Server/VE verwaltet wird.

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

**Computerschlüssel** – Wenn die Verschlüsselung auf einem Serverbetriebssystem installiert ist, schützt der Computerschlüssel die Dateiverschlüsselung und der Richtlinien eines Servers. Der Computerschlüssel wird auf dem Dell Enterprise Server/VE gespeichert. Der

neue Server tauscht während der Aktivierung Zertifikate mit dem DDP-Server aus und verwendet das Zertifikat für die folgenden Authentifizierungsereignisse.

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

**SED Management** – SED Management ist eine Plattform für die sichere Verwaltung selbstverschlüsselnder Laufwerke. Selbstverschlüsselnde Laufwerke haben zwar eine eigene Verschlüsselungsfunktion, ihnen fehlt aber eine Plattform für die Verwaltung ihrer Verschlüsselung mit den verfügbaren Richtlinien. SED Management ist eine zentrale, skalierbare Verwaltungskomponente, mit der Sie Daten wirksamer schützen. SED Management beschleunigt und vereinfacht die Administration von Unternehmensdaten.

**Serverbenutzer** – Ein virtuelles Benutzerkonto, das durch Dell Server Encryption erstellt wird und für die Verarbeitung von Verschlüsselungsschlüsseln und Richtlinienaktualisierungen bestimmt ist. Dieses virtuelle DDP-Serverbenutzerkonto ist unabhängig von allen anderen Benutzerkonten auf dem Computer oder in der Domäne, und es hat keinen Benutzernamen und kein Passwort, das physisch verwendet werden kann. Dem Konto wird in der Dell Enterprise Server/VE Remote Management Console ein eindeutiger UCID-Wert zugewiesen.

