Encryption Enterprise

Grundlegendes Installationshandbuch v10.1

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.

2018 - 11

Rev. A01

Inhaltsverzeichnis

1

Einleitung

Dieses Handbuch beschreibt die Installation und Konfiguration der Anwendung unter Verwendung des -Master-Installationsprogramms. Das Handbuch bietet eine grundlegende Hilfestellung bei der Installation. Im *Erweiterten Installationshandbuch* finden Sie weitere Informationen zum Installieren von untergeordneten Installationsprogrammen, zur Konfiguration von Security Management Server/Security Management Server Virtual oder Informationen, die über die grundlegende Hilfe des -Master-Installationsprogramms hinausgehen.

Für die Einhaltung und Überwachung von Gerätedetails, Shield-Details und Audit-Ereignissen, siehe Berichterstellung > Verwalten von Berichten.

Vor der Installation

1 Installieren Sie den Dell Server vor der Bereitstellung von Clients. Machen Sie das richtige Handbuch ausfindig (siehe unten), folgen Sie den Anweisungen, und kehren Sie anschließend zu diesem Handbuch zurück.

   - *Security Management Server Installation and Migration Guide* (Security Management Server Installations- und Migrationshandbuch)
   - *Security Management Server Virtual Quick Start Guide and Installation Guide* (Security Management Server Virtual Schnellanleitung und Installationshandbuch)
   - 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 unterstützten und mit den Optionen Ihres Dell Server vertraut zu machen.

2 Lesen Sie sich das Kapitel Anforderungen in diesem Dokument genau durch.

3 Stellen Sie Clients für die Benutzer 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:
  - Aktive Installation unter Verwendung des Master-Installationsprogramms

    oder
  - Installation über die Befehlszeile mit dem Master-Installationsprogramm

Kontaktaufnahme mit dem Dell ProSupport

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

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

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

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

2

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 SCCM oder Quest 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.
- Administratoren sollten sicherstellen, dass alle benötigten Ports verfügbar sind.
- Überprüfen Sie regelmäßig die Website www.dell.com/support, um stets über die neueste Dokumentation und die neuesten technischen Ratgeber zu verfügen.
- **ANMERKUNG: Das Produktangebot von Dell Data Security unterstützt keine Versionen von Windows Insider Preview.**

Alle Clients - Voraussetzungen

- Das Master-Installationsprogramm installiert die folgenden benötigten Komponenten, falls sie auf Ihrem Computer nicht bereits installiert sind.

Voraussetzungen
– Visual C++ 2012 Update 4 oder höheres Redistributable Package (x86 und x64)
– Visual C++ 2015 Update 3 oder höheres Redistributable Package (x86 und x64)

Visual C++ 2015 erfordert Windows Update KB2999226 bei Installation auf Windows 7.

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

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. Zum Installieren von Microsoft .Net Framework 4.5.2 gehen Sie zu https://www.microsoft.com/de-de/download/details.aspx?id=42643.

Alle Clients - Hardware

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

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

Hardware

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

Alle Clients – Lokalisierung

- Die Encryption-, und BitLocker Manager-Clients sind Multilingual User Interface (MUI)-konform und unterstützen die folgenden Sprachen. Die vollständige Datenträgerverschlüsselung wird nur auf englischen Betriebssystemen unterstützt.

Sprachunterstützung

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

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 wird hinsichtlich branchenführender Antivirus-Anbieter überprüft. 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/SLN288353/ nach oder kontaktieren Sie den Dell ProSupport, um Hilfe zu erhalten.
- Die Neuinstallation zur direkten Aktualisierung des Betriebssystems wird nicht unterstützt. Zur Neuinstallation des Betriebssystems sichern Sie den Zielcomputer, setzen Sie den Computer zurück, installieren Sie das Betriebssystem, und stellen Sie anschließend die verschlüsselten Daten gemäß den üblichen Wiederherstellungsverfahren wieder her.

Encryption-Client-Anforderungen

Encryption-Client-Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 mit Anwendungskompatibilitätsvorlage
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro

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

- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) bis Version 1803 (April 2018 Update/ Redstone 4)
- VMWare Workstation 12.5 und höher

ANMERKUNG:
Bei der Verwendung des UEFI-Modus wird die Richtlinie „Sicherer Ruhezustand“ nicht unterstützt.

Encryption-Client-Betriebssysteme mit verzögerter Aktivierung

- Die verzögerte Aktivierung dient dazu, dass das Active Directory-Benutzerkonto, das im Rahmen der Aktivierung verwendet wird, unabhängig von dem Konto sein kann, das zur Anmeldung beim Endpunkt verwendet wird. Statt dass der Netzwerkanbieter die Authentifizierungsinformationen erfasst, gibt der Benutzer das Active Directory-basierte Konto an, wenn er dazu aufgefordert wird. Sobald die Anmeldeinformationen eingegeben wurden, werden die Authentifizierungsinformationen sicher an den Dell Server gesendet, der diese anhand der konfigurierten Active Directory-Domänen validiert. Weitere Informationen finden Sie unter http://www.dell.com/support/article/us/en/19/sln306341.
- In der folgenden Tabelle sind die unterstützten Betriebssysteme mit verzögerter Aktivierung aufgeführt.

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

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 mit Anwendungskompatibilitätsvorlage
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) bis Version 1803 (April 2018 Update/ Redstone 4)

Encryption External Media-Betriebssysteme

- Die folgende Tabelle enthält Informationen zu den unterstützten Betriebssystemen, wenn auf Medien zugegriffen wird, die von Encryption External Media geschützt werden.

ANMERKUNG:
Zur Verwendung von Encryption External Media müssen ungefähr 55 MB auf dem Wechseldatenträger frei sein. Des Weiteren muss die Größe des freien Speicherplatzes der Größe der umfangreichsten zu verschlüsselnden Datei entsprechen.

Unterstützte Windows-Betriebssysteme für den Zugriff auf mit Encryption External Media geschützte Medien (32-Bit und 64-Bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 mit Anwendungskompatibilitätsvorlage
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) bis Version 1803 (April 2018 Update/ Redstone 4)

Unterstützte Mac-Betriebssysteme für den Zugriff auf mit Encryption External Media geschützte Medien (64-Bit-Kernel)

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14

Vollständige Datenträgerverschlüsselung

Die vollständige Datenträgerverschlüsselung kann **nur** über die Befehlszeilenschnittstelle (CLI) installiert werden. Falls Sie die vollständige Datenträgerverschlüsselung installieren möchten, laden Sie das erweiterte Installationshandbuch für Encryption Enterprise herunter und lesen die darin enthaltenen Anweisungen.

- Die vollständige Datenträgerverschlüsselung erfordert die Aktivierung anhand eines Dell Servers mit V 9.8.2 oder höher.
- Vollständige Datenträgerverschlüsselung wird zurzeit nicht auf virtualisierten Host-Computer unterstützt.
- Vollständige Datenträgerverschlüsselungen von Konfigurationen mit mehreren Laufwerken werden nicht unterstützt.
- Anmeldedaten von Drittanbietern funktionieren nicht mit installierten FDE-Funktionen. Alle Anmeldedaten von Drittanbietern werden deaktiviert, wenn PBA aktiviert ist.
- Der Client-Computer muss für die Aktivierung über Netzwerkkonnektivität oder einen Zugangscode verfügen.
- Der Computer muss über eine verkabelte Netzwerkverbindung verfügen, damit sich ein Smartcard-Benutzer zum ersten Mal über die Preboot-Authentifizierung anmelden kann.
- Funktionsaktualisierungen des Betriebssystems werden mit vollständiger Festplattenverschlüsselung nicht unterstützt.
- Für die Kommunikation der PBA mit dem Dell Server ist eine kabelgebundene Verbindung erforderlich.
- Es darf kein SED am Zielcomputer vorhanden sein.
- Die vollständige Datenträgerverschlüsselung wird nicht von BitLocker oder BitLocker Manager unterstützt. Installieren Sie die vollständige Datenträgerverschlüsselung nicht auf einem Computer, auf dem BitLocker oder BitLocker Manager installiert ist.
- NVMe-Laufwerke, die als PBA genutzt werden – Der SATA-Betrieb im BIOS muss auf „RAID EIN“ eingestellt sein, da die PBA-Verwaltung von Dell keine Unterstützung für AHCI auf NVMe-Laufwerken bietet.
- NVMe-Laufwerke, die als PBA genutzt werden – Der Startmodus des BIOS muss UEFI sein und Legacy-Option-ROMs müssen deaktiviert sein.
- Nicht-NVMe-Laufwerke, die als PBA genutzt werden – Der SATA-Betrieb im BIOS muss auf „AHCI“ eingestellt sein, da die PBA-Verwaltung von Dell keine Unterstützung für RAID auf Nicht-NVMe-Laufwerken bietet.
  - RAID EIN wird nicht unterstützt, da der Lese- und Schreibzugriff auf RAID-bezogene Daten (in einem Sektor, der auf einem gesperrten nicht-NVME-Laufwerk nicht verfügbar ist) beim Start nicht verfügbar ist und mit dem Lesen dieser Daten nicht gewartet werden kann, bis der Benutzer angemeldet ist.
  - Das Betriebssystem stürzt ab, wenn es von RAID EIN auf AHCI umgeschaltet wird, wenn den AHCI-Controller-Treiber nicht vorinstalliert wurde. Eine Anleitung zum Umschalten von RAID auf AHCI (oder umgekehrt) finden Sie unter http://www.dell.com/support/article/us/en/19/SLN306460.

    Dell empfiehlt Intel Rapid Storage Technology-Treiberversion 15.2.0.0 oder höher für NVMe-Laufwerke.
- 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 Client für vollständige Datenträgerverschlüsselung unterstützt keine Dual-Boot-Konfigurationen, da es hierdurch zur Verschlüsselung von Systemdateien des anderen Betriebssystems kommen kann, was den Betrieb stören würde.
- Die Neuinstallation zur direkten Aktualisierung des Betriebssystems wird nicht unterstützt. Zur Neuinstallation des Betriebssystems sichern Sie den Zielcomputer, setzen Sie den Computer zurück, installieren Sie das Betriebssystem, und stellen Sie anschließend die verschlüsselten Daten gemäß den üblichen Wiederherstellungsverfahren wieder her.
- **ANMERKUNG: Bei der Preboot-Authentifizierung ist ein Passwort erforderlich. Dell empfiehlt Mindestvorgaben für das Passwort, die den internen Sicherheitsrichtlinien entsprechen.**

ANMERKUNG: Die vollständige Datenträgerverschlüsselung muss so konfiguriert werden, dass die Verschlüsselungsalgorithmen auf AES 256 und der Verschlüsselungsmodus auf CBC eingestellt sind.

Client-Voraussetzungen für vollständige Datenträgerverschlüsselung

- Microsoft .Net Framework 4.5.2 (oder später) ist für den Master-Installations-Client sowie den untergeordneten Installations-Client erforderlich. Das Installationsprogramm installiert die Microsoft .Net Framework-Komponente *nicht*.

  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. Zum Installieren von Microsoft .Net Framework 4.5.2 gehen Sie zu https://www.microsoft.com/de-de/download/details.aspx?id=42643.

Client-Hardware für vollständige Datenträgerverschlüsselung

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

Optionale integrierte Hardware
– TPM 1.2 oder 2.0

Client-Betriebssysteme für vollständige Datenträgerverschlüsselung

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

Windows-Betriebssysteme (64-Bit)
– Windows 7 SP1: Enterprise, Professional, Ultimate (Legacy-Startmodus erforderlich)
– Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) bis Version 1803 (April 2018 Update/ Redstone 4) (UEFI-Startmodus erforderlich)

SED-Client

- Der Computer muss über Netzwerkkonnektivität verfügen, damit SED Management erfolgreich installiert werden kann.
- Der Computer muss über eine verkabelte Netzwerkverbindung verfügen, damit sich ein Smartcard-Benutzer zum ersten Mal über die Preboot-Authentifizierung anmelden kann.
- Anmeldedaten von Drittanbietern funktionieren nicht mit installierter SED-Verwaltung und alle Anmeldedaten von Drittanbietern werden deaktiviert, wenn die PBA aktiviert ist.
- IPv6 wird nicht unterstützt.
- Der SED-Manager wird nicht mit Konfigurationen mit mehreren Laufwerken unterstützt.
- SED-Manager wird zurzeit nicht auf virtualisierten Host-Computern 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* zum Betriebssystemabsturz.

- Die Konfiguration von selbstverschlüsselnden Laufwerken für die SED-Verwaltung von Dell weicht bei NVMe- und nicht-NVMe-Laufwerken (SATA) folgendermaßen ab:
  - NVMe-Laufwerke, die als SED genutzt werden – Der SATA-Betrieb im BIOS muss auf „RAID EIN“ eingestellt sein, da die SED-Verwaltung von Dell keine Unterstützung für AHCI auf NVMe-Laufwerken bietet.
  - NVMe-Laufwerke, die als SED genutzt werden – Der Startmodus des BIOS muss UEFI sein und Legacy-Option-ROMs müssen deaktiviert sein.
  - Nicht-NVMe-Laufwerke, die als SED genutzt werden – Der SATA-Betrieb im BIOS muss auf „AHCI“ eingestellt sein, da die SED-Verwaltung von Dell keine Unterstützung für RAID auf Nicht-NVMe-Laufwerken bietet.
    - RAID EIN wird nicht unterstützt, da der Lese- und Schreibzugriff auf RAID-bezogene Daten (in einem Sektor, der auf einem gesperrten nicht-NVME-Laufwerk nicht verfügbar ist) beim Start nicht verfügbar ist und mit dem Lesen dieser Daten nicht gewartet werden kann, bis der Benutzer angemeldet ist.
    - Das Betriebssystem stürzt ab, wenn es von RAID EIN auf AHCI umgeschaltet wird, wenn den AHCI-Controller-Treiber nicht vorinstalliert wurde. Eine Anleitung zum Umschalten von RAID auf AHCI (oder umgekehrt) finden Sie unter http://www.dell.com/support/article/us/en/19/SLN306460.

  Unterstützte Opal-konforme SEDs erfordern aktualisierte Intel Rapid Storage Technology-Treiber, die unter http://www.dell.com/support verfügbar sind. Dell empfiehlt Intel Rapid Storage Technology-Treiberversion 15.2.0.0 oder höher für NVMe-Laufwerke.

ANMERKUNG: Die Intel Rapid Storage Technology-Treiber sind abhängig von der spezifischen Plattform. Sie finden die Treiber Ihres Systems unter dem oben genannten Link basierend auf dem Modell Ihres Computers.

- SED-Management wird mit der Serververschlüsselung nicht unterstützt.
- **ANMERKUNG: Bei der Preboot-Authentifizierung ist ein Passwort erforderlich. Dell empfiehlt Mindestvorgaben für das Kennwort, die den internen Sicherheitsrichtlinien entsprechen.**

SED-Client-Hardware

SED-Client – 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-FR – (Französisch – Schweiz)
- DE-CH – (Deutsch – Schweiz)
- EN-US – Englisch (Amerikanisches Englisch)
- EN-GB – Englisch (Britisches Englisch)
- EN-CA – Englisch (Kanadisches Englisch)

Internationale Tastatur-Unterstützung – Nicht-UEFI

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

SED-Client –Lokalisierung

Der SED-Client ist Multilingual User Interface (MUI)-konform und unterstützt die folgenden Sprachen. Der UEFI-Modus sowie die Preboot-Authentifizierung werden in den folgenden Sprachen unterstützt, **mit Ausnahme von** Russisch sowie traditionellem und vereinfachtem Chinesisch.

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

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, Ultimate (unterstützt mit Legacy Boot-Modus aber nicht UEFI)

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

ANMERKUNG:
Selbstverschlüsselnde NVMe-Laufwerke werden nicht unter Windows 7 unterstützt.

- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) bis Version 1803 (April 2018 Update/Redstone 4)

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.
- Ein Dell Server ist erforderlich, um BitLocker Manager zu verwenden.
- Stellen Sie sicher, dass ein Signaturzertifikat in der Datenbank zur Verfügung steht. Weitere Informationen finden Sie unter http://www.dell.com/support/article/us/en/19/sln307028.
- 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.

Hardware für den BitLocker Manager-Client

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

Optionale integrierte Hardware

- TPM 1.2 oder 2.0

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: Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) bis Version 1803 (April 2018 Update/Redstone 4)
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64-Bit)
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64-Bit)
- Windows Server 2016

Die Windows-Updates KB3133977 und KB3125574 **dürfen nicht** installiert sein, wenn BitLocker Manager auf Systemen mit Windows 7 installiert wird.

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.
- Master-Installationsprogramm-Protokolldateien 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 in der *Dell Encrypt Help* (Hilfe zu Dell Encrypt). Hier können Sie auf die Hilfe zugreifen: **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - In der *Encryption External Media Help* (Hilfe zu Encryption External Media) finden Sie die Funktionen von Encryption External Media. Hier können Sie auf die Hilfe zugreifen: **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Siehe *Encryption Enterprise-Hilfe* für weitere Informationen zur Verwendung der Funktionen von . Hier können Sie auf die Hilfe zugreifen: **<Install dir>:\Program Files\Dell\Dell Data Protection\Client Security Framework\Help**.
- Nach Abschluss der Installation sollten Benutzer die Richtlinien aktualisieren, indem sie im Infobereich mit der rechten Maustaste auf das Symbol für „Dell Encryption“ 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:
  - Aktive Installation unter Verwendung des Master-Installationsprogramms

  oder

  - Installation durch Befehlszeile mit dem Master Installationsprogramm

Aktive Installation unter Verwendung des Master-Installationsprogramms

- Das Master-Installationsprogramm befindet sich unter:
  - **Über die Website support.dell.com** – Beziehen Sie ggf. die Software von support.dell.com, und extrahieren Sie dann die untergeordneten Installationsprogramme aus dem Master-Installationsprogramm.
  - **Über Ihr Dell FTP-Konto** – Suchen Sie das Installationspaket unter Dell-Encryption-8.x.x.xxx.zip
- Verwenden Sie diese Anweisungen zur interaktiven Installation und Aktualisierung von Dell Encryption Enterprise mithilfe des Master-Installationsprogramms. Sie können dieses Verfahren anwenden, um die gesamte Produkt-Suite gleichzeitig auf einem Computer zu installieren.

1. Suchen Sie die Datei **DDSSetup.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 **Encryption Enterprise** und klicken Sie auf **Weiter.**

   Wählen Sie das Kontrollkästchen „Nur Encryption External Media“, wenn Sie nur Encryption External Media installieren wollen
6. Geben Sie in *Dell Management Server-Name vor Ort* den vollständigen qualifizierten Hostnamen des Dell Server zur Verwaltung des Zielbenutzers ein, wie z. B. server.organization.com.

Geben Sie im Feld *URL des Dell Device Servers* die URL des Dell Server ein, mit dem der Client kommunizieren soll.

Wenn Sie einen Dell Server vor Version 7.7 verwenden, lautet das Format https://server.organization.com:**8081**/xapi.

Wenn Sie einen Dell Server der Version 7.7 oder höher verwenden Format 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 zugrunde liegende Sicherheits-Framework.

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 Switches zuerst angegeben werden. Andere Parameter gehen in ein Argument ein, das an den /v-Schalter weitergegeben wird.

Schalter

- Die folgende Tabelle beschreibt die Switches, die mit dem Master-Installationsprogramm verwendet werden können.

ANMERKUNG: Wenn Ihre Organisation die Verwendung von Anmeldedaten von Drittanbietern erfordert, muss der Verschlüsselungsverwaltungsagent mit dem Parameter FEATURE = BLM oder FEATURE = BASIC installiert oder aktualisiert werden.

Schalter	Beschreibung
-y -gm2	Vor dem Extrahieren 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 Datei DDSSetup.exe weiter.

Parameter

- Die folgende Tabelle beschreibt die Parameter, 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 Dell Server 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 = nur Laufwerk Encryption Client EME = Encryption External Media allein BLM = BitLocker Manager SED = SED-Verwaltung (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 werden alle Komponenten 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 Dell Server konfiguriert.

```
"DDSSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com\""
```

- In diesem Beispiel wird SED Management und Encryption External Media 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 Dell Server konfiguriert.

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

- In diesem Beispiel wird 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 Dell Server konfiguriert.

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

- In diesem Beispiel wird 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 Dell Server konfiguriert.

```
"DDSSetup.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 Dell Server konfiguriert.

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

- In diesem Beispiel werden BitLocker Manager (mit dem SED-Management-Plugin) und Encryption External Media 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 Dell Server konfiguriert.

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

- In diesem Beispiel werden BitLocker Manager (ohne das SED Management-Plugin) und Encryption External Media 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 Dell Server konfiguriert.

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

Deinstallation des Master-Installationsprogramms

- Dell empfiehlt die Verwendung des Data Security-Deinstallationsprogramm, um die Data Security-Suite zu entfernen.
- Jede Komponente muss separat deinstalliert werden, gefolgt von der Deinstallation des -Master-Installationsprogramms. Die Clients **müssen in einer bestimmten Reihenfolge deinstalliert werden**, um Fehler bei der Deinstallation zu vermeiden.
- Folgen Sie den Anweisungen unter Untergeordnete Installationsprogramme aus dem Master-Installationsprogramm extrahieren zum Abrufen von untergeordneten Installationsprogrammen.
- Stellen Sie sicher, dass die gleiche Version des -Master-Installationsprogramms (und damit der Clients) zur Deinstallation und Installation verwendet wird.
- 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-Client deinstallieren.

  c BitLocker Manager-Client deinstallieren.
- Fahren Sie mit dem Schritt Master-Installationsprogramm deinstallieren fort.

Deinstallieren des -Master-Installationsprogramms

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.

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

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

5

Deinstallation unter Verwendung der untergeordneten Installationsprogramme

- Dell empfiehlt die Verwendung des Data Security-Deinstallationsprogramm, um die Data Security-Suite zu entfernen.
- 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 erläutert. 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 /l **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 "/l*v" (ausführliche Protokollierung) bei der Deinstallation über die Befehlszeile ab.
- Für Deinstallationen über die Befehlszeile verwenden alle untergeordneten Installationsprogramme, soweit nicht anders angegeben, die gleichen grundlegenden .msi-Schalter und Anzeigeoptionen. Die Schalter müssen zuerst angegeben werden. Der /v-Schalter ist erforderlich und benötigt ein Argument. Andere Parameter gehen in ein Argument ein, das an den /v-Schalter weitergegeben wird.

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

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

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

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.
- Dell Encryption und Encryption External Media aktualisieren den Dell Server durch Ändern des Status zu *Ungeschützt* zu Beginn eines Encryption-Client-Deinstallationsvorgangs. Wenn der Client keine Verbindung zum Dell Server herstellen kann, ist keine Statusaktualisierung möglich. In diesem Fall müssen Sie ein manuelles *Entfernen des Endpunkts* in der Verwaltungskonsole durchführen. Falls Ihr Unternehmen diese Vorgehensweise im Rahmen der Compliance einsetzt, empfiehlt Dell, zu überprüfen, ob in der Verwaltungskonsole oder in Compliance Reporter erwartungsgemäß der Status *Ungeschützt* erscheint.

Verfahren

- Der Key Server (und Security Management 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 Security Management Server aktiviertem Encryption-Client konfigurieren. Falls der zu deaktivierende Client auf einem Security Management Server Virtual aktiviert ist, sind keine weiteren Maßnahmen erforderlich, da der Security Management Server Virtual 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

- Sobald es aus dem -Master-Installationsprogramm extrahiert wurde, befindet sich das Encryption-Client-Installationsprogramm unter **C:\extracted\Encryption\DDPE_XXbit_setup.exe**.
- Die folgende Tabelle umfasst die für die Deinstallation verfügbaren Parameter.

Parameter	Auswahl
CMG_DECRYPT	Eigenschaft zur Auswahl des Installationstyps des Encryption Removal Agent 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	Vollständiger Hostname für den Security Management Server, auf dem die Vermittlungssitzung gehostet wird
DA_PORT	Security Management Server-Port für die Anfrage (die Standardeinstellung ist 8050).
SVCPN	Benutzername im UPN-Format, unter dem der Key Server-Dienst beim Security Management 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 Security Management Server 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 des Typs „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 Security Management 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 Verwaltungskonsole 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"
```

Encryption External Media 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.

SED-Client deinstallieren

- Zur PBA-Deaktivierung muss eine Netzwerkverbindung zum Dell 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.

PBA deaktivieren

1 Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.
2 Klicken Sie im linken Fensterbereich auf **Bestückungen** > **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 den Hostnamen des gewünschten Computers.
7 Klicken Sie im Hauptmenü auf **Sicherheitsrichtlinien**.
8 Wählen Sie **Selbstverschlüsselnde Laufwerke** auf der Seite **Richtlinienkategorie** aus.
9 Ändern Sie die Richtlinie der **Selbstverschlüsselnden Laufwerke (SED)** von `On` zu ***`Off`***.
10 Klicken Sie auf **Speichern**.
11 Klicken Sie im linken Bereich auf das Banner **Richtlinien festlegen**.
12 Klicken Sie auf **Richtlinien bestätigen**.

   Warten Sie, während die Richtlinie vom Dell Server an den Zielcomputer der Deaktivierung übertragen wird.

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

SED-Client deinstallieren

Deinstallation über die Befehlszeile

- Nach der Extraktion aus dem Master-Installationsprogramm befindet sich das SED-Client-Installationsprogramm unter C:\extracted\Encryption Management Agent\EMAgent_XXbit_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.

Deinstallation des BitLocker Manager-Clients

Deinstallation über die Befehlszeile

- Sobald es aus dem -Master-Installationsprogramm extrahiert wurde, befindet sich das BitLocker-Client-Installationsprogramm unter C:\extracted\Encryption Management Agent\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.

6

Data Security Deinstallationsprogramm

Deinstallieren von

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

Das Deinstallationsprogramm von Data Security gibt es am folgenden Speicherort: C:\Program Files (x86)\Dell\Dell Data Protection

Für weitere Informationen oder für die Verwendung der Befehlszeilenoberfläche (CLI) siehe KB-Artikel SLN307791.

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

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

Klicken Sie auf **Weiter**.

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

ANMERKUNG: Erforderliche Abhängigkeiten werden automatisch ausgewählt oder gelöscht.

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

Wählen Sie **Encryption Removal Agent – Schlüssel von Server herunterladen**.

Geben Sie die vollständig qualifizierten Anmeldeinformationen für einen forensischen Administrator ein und wählen Sie **Weiter**.

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

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

Deinstallation und Entfernen sind abgeschlossen.

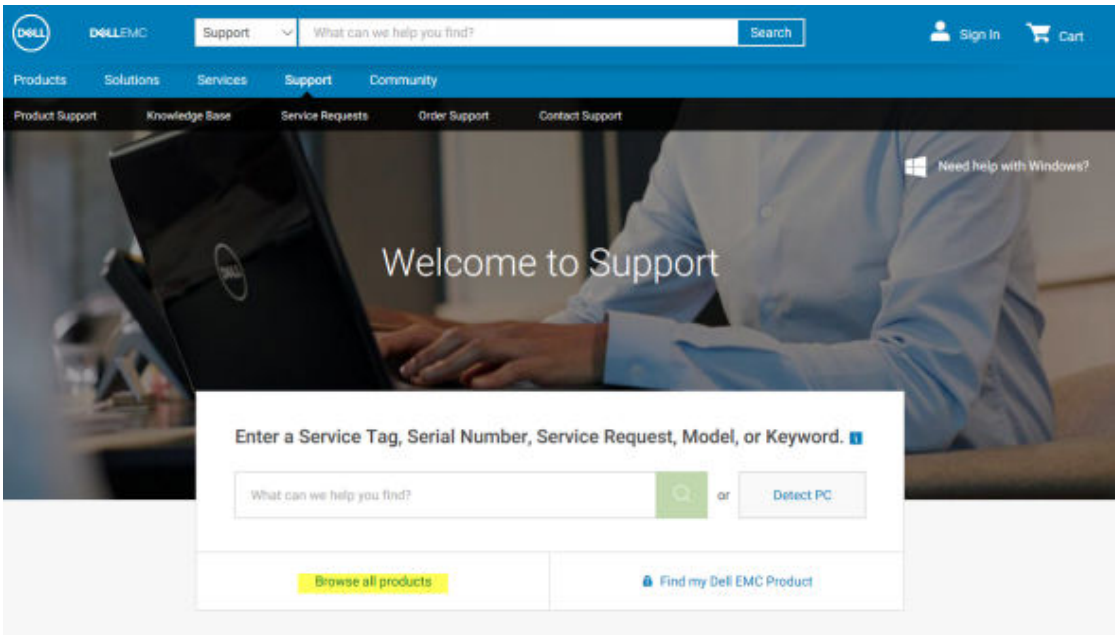
7

Herunterladen der Software

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

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

1 Wählen Sie auf der Dell Support-Webseite **Alle Produkte durchsuchen** aus.



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

3 Wählen Sie **Dell Data Security** aus.
Wenn diese Auswahl einmal vorgenommen wurde, wird sie von der Website gespeichert.

4 Wählen Sie das Dell Produkt.
Beispiele:

Dell Encryption Enterprise

Dell Endpoint Security Suite Enterprise

Dell Data Guardian

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

6 Wählen Sie den gewünschten Client-Betriebssystemtyp aus.

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

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

8

Extrahieren Sie die untergeordneten Installationsprogrammen

- Das Master-Installationsprogramm ist kein Master-*Deinstallationsprogramm*. Jede Komponente 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 **DDSSetup.exe** auf den lokalen Computer.

2 Öffnen Sie am gleichen Speicherort wie dem der Datei **DDSSetup.exe** eine Eingabeaufforderung und geben Sie Folgendes ein:

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

Der Extraktionspfad darf maximal 63 Zeichen enthalten.

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

9

Konfigurieren von Key Server

- In diesem Abschnitt wird beschrieben, wie Komponenten für die Verwendung mit der Kerberos-Authentifizierung/-Autorisierung bei Verwendung eines Security Management Server konfiguriert werden. Der Security Management Server Virtual 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 Security Management Server Virtual den Key Server nicht verwendet, ist die typische Deinstallation beeinträchtigt. Wenn ein Encryption-Client deinstalliert wird, der auf einem Security Management Server Virtual aktiviert ist, wird anstelle der Kerberos-Methode des Key-Servers der standardmäßige forensische Schlüsselabruf über den Security Server genutzt. Unter Deinstallation über die Befehlszeile finden Sie weitere Informationen.

Dialogfeld „Dienste" - Domänenbenutzerkonto hinzufügen

1 Navigieren Sie auf dem Security Management Server zum Bereich „Dienste“ (Start > Ausführen ... > services.msc > OK).

2 Klicken Sie mit der rechten Maustaste auf „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 install dir> log.txt“, um zu überprüfen, ob der Dienst korrekt gestartet wurde.

Key-Server-Konfigurationsdatei – Fügen Sie Benutzer für Security Management Server-Kommunikation hinzu

1 Navigieren Sie zu <Key Server install dir>.

2 Öffnen Sie die Datei ***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="<encrypted value of the password>" /> und ändern Sie „epw“ in „password“. Ändern Sie dann „<encrypted value of the password>“ in das Passwort des Benutzers aus Schritt 3. Beim Neustart des Security Management Server wird dieses Kennwort 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.

Services (Dialogfeld) – 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 install dir> log.txt“, um zu überprüfen, ob der Dienst korrekt gestartet wurde.
4 Schließen Sie das Dialogfeld „Dienste“.

Verwaltungskonsole - forensischen Administrator hinzufügen

1 Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.
2 Klicken Sie auf **Bestückungen** > **Domänen**.
3 Wählen Sie die gewünschte Domäne aus.
4 Klicken Sie auf die Registerkarte **Key Server**.
5 Fügen Sie in *Konto* den Benutzer hinzu, um die Administratoraktionen auszuführen. 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** aus, und klicken Sie dann 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 Security Management Server/Security Management Server Virtual 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 Security Management Server Version 7.7 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. machineID.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**.

Verwenden des Administrator-Download-Dienstprogramms im Admin-Modus

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

- **Master-Installationsprogramm-Protokolldateien** befinden sich unter **C: \Programme\Dell\Dell Data Protection\Installer.**
- Windows erstellt für den angemeldeten Benutzer eindeutige Installationsprotokolldateien des untergeordneten Installationsprogramms im Verzeichnis „%temp%“ unter **C:\Users\<Benutzername>\AppData\Local\Temp.**
- Windows erstellt Protokolldateien für Client-Voraussetzungen, z. B. Visual C++, für den angemeldeten Benutzer im Verzeichnis „%Temp %“ unter **C:\Users\<Benutzername>\AppData\Local\Temp. For example, C:\Users\<Benutzername>\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 4.5.2 oder höher herunterzuladen.
- Siehe *dieses Dokument*, wenn auf dem Computer, der für die Installation vorgesehen ist, „Dell Access“ installiert ist (oder in der Vergangenheit war). DDP|A ist nicht kompatibel mit dieser Suite von Produkten.

Alle Clients – Schutzstatus

Eine neue Methode zur Feststellung des Schutzstatus eines Geräts wurde im Dell Security Management Server Version 9.8.2 implementiert. Zuvor wurde im Statusbereich „Endpoint Protection“ im Dashboard der Verwaltungskonsole nur der Verschlüsselungsstatus des Geräts angezeigt.

Der Status „Geschützt“ wird jetzt angezeigt, wenn eines der folgenden Kriterien erfüllt ist:

- Advanced Threat Prevention ist installiert und aktiviert.
- Web Protection oder Client Firewall ist installiert und entweder die Richtlinie für Web Protection oder Client Firewall ist aktiviert.
- Dell Data Guardian ist installiert und aktiviert.
- Self-Encrypting Drive Management ist installiert sowie aktiviert und die Pre-Boot-Authentifizierung (PBA) ist aktiviert.
- BitLocker Manager ist installiert sowie aktiviert und die Verschlüsselung wurde abgeschlossen.
- Dell Encryption (Mac) ist installiert sowie aktiviert und die richtlinienbasierte Verschlüsselung wurde umgesetzt.
- Dell Encryption (Windows) ist installiert und aktiviert, die richtlinienbasierte Verschlüsselung wurde für den Endpunkt eingerichtet und die Gerätesuchläufe sind abgeschlossen.

Fehlerbehebung für den Client für Verschlüsselung und Serververschlüsselung

Aktualisierung auf das Windows 10 Creators Update

Um ein Upgrade auf die Version Windows 10 October 2018 durchzuführen, 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 Anmeldeinformationen im UPN-Format für einen Domänenadministrator an.

Fehlermeldung: Es konnte keine Verbindung zum Server aufgebaut werden.

oder

```
The operation timed out.
```

Serververschlüsselung konnte an Port 8449 nicht über HTTPS mit dem Dell 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 Dell 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 Dell Server-Version muss 9.1 oder höher sein. Aktualisieren Sie Ihren Dell Server bei Bedarf auf Version 9.1 oder höher.
- Überprüfen Sie die Dell 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 Infobereich 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: Vor der Installation.
6. Der Dell 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 Dell Server ein neues Benutzerkonto für den Benutzer des virtuellen Servers und speichert die Anmeldeinformationen in der Vault des Dell Server.

   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 die zweite Phase 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 Server Encryption automatisch als virtueller Serverbenutzer an und fordert den Computerschlüssel vom Dell 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 Encryption-Client-ID rot ist, wurde die Verschlüsselung noch nicht aktiviert.
- In der 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 Management Console.

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 unter Verwendung des virtuellen Serverbenutzerkontos authentifiziert und führt den Client für die Verschlüsselung im Servermodus aus.

2 Der Computer gleicht den Status seiner Geräteaktivierung am Dell Server ab:

- Wenn für den Computer bisher keine Geräteaktivierung erfolgt ist, weist der Dell Server ihm eine MCID, eine DCID und ein Vertrauenszertifikat zu und speichert alle Informationen im Vault des Dell Server.
- Wenn für den Computer bereits eine Geräteaktivierung erfolgt ist, überprüft der Dell Server das Vertrauenszertifikat.

3 Nachdem der Dell 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.

Encryption External Media und PCS Interaktionen

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

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

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

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

WSScan verwenden

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

Ausführen von WSScan

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

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

3 Klicken Sie auf **Erweitert**.

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

5 Wählen Sie den Berichtstyp für die Verschlüsselung aus: *Verschlüsselte Dateien*, *Unverschlüsselte Dateien*, *Alle Dateien* oder *Unverschlüsselte Dateien verletzt*:

- *Verschlüsselte Dateien* – Um sicherzustellen, dass alle Daten bei der Deinstallation 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 Menü ignoriert.

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

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

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

6 Wählen Sie das Ausgabeformat aus:

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

7 Klicken Sie auf **Suchen**<2></2>.

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.

Ausgabe	Erläuterung
	SysData: SDE-Schlüssel. **Benutzer:** Benutzer-Verschlüsselungscode. **Allgemein:** Allgemeiner Verschlüsselungscode. WSScan meldet keine Dateien, die mittels „Für Freigabe verschlüsseln“ verschlüsselt wurden.
KCID	Die ID des Schlüssel-Computers. Im Beispiel oben „**7vdlxrsb**“ Wenn Sie ein zugeordnetes Netzwerklaufwerk durchsuchen, gibt der Abfragebericht keine KCID aus.
UCID	Die Benutzer-ID. Im Beispiel oben „**_SDENCR_**“ Die UCID ist für alle Benutzer des Computers gleich.
Datei	Der Pfad der verschlüsselten Datei. Wie im Beispiel oben angezeigt, „**c:\temp\Dell - test.log**“
Algorithmus	Im Folgenden finden Sie den für die Verschlüsselung der Datei verwendeten Verschlüsselungsalgorithmus. Im Beispiel oben „**is still AES256 encrypted**“ Rijndael 128 Rijndael 256 AES-128 AES-256 3DES

Überprüfen des Encryption-Removal-Agent-Status

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

- **Warten auf SDE-Deaktivierung** – 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 Dienst, 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.
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\<Neuer Ordner>** 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\<Neuer Ordner>** zu entpacken.
5. Klicken Sie auf **Ja**, um die Erstellung eines neuen Ordners zu genehmigen.
6. Klicken Sie auf **OK**, wenn die Nachricht angezeigt wird, dass die Dateien erfolgreich entpackt wurden.
7. Nach dem Entpacken wird der Ordner angezeigt, der die entpackten Dateien enthält. Ist dies nicht der Fall, gehen Sie zu dem Ordner, in den Sie die Dateien entpackt haben. Wählen Sie den Ordner **Firmware** aus.
8. Doppelklicken Sie auf die Datei **ushupgrade.exe**, um das Firmware-Installationsprogramm zu starten.
9. Klicken Sie zum Starten der Firmware auf **Start**.

:

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

Es werden nun verschiedene Statusmeldungen angezeigt.

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

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

Glossar

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 Verwaltungskonsole auf AUS gesetzt wird. Nach der Deaktivierung des Computers wird die PBA -Datenbank gelöscht, und es gibt keine Aufzeichnung der im Cache gespeicherten Benutzer mehr.

Encryption External Media – Dieser Service innerhalb des Dell Encryption Client wendet Richtlinien auf Wechseldatenträger und externe Speichergeräte an.

Encryption External Media-Zugriffscode - Dieser Dienst von Dell Server ermöglicht die Wiederherstellung von mit Encryption External Media geschützten Geräten, bei denen der Benutzer das Kennwort vergessen hat und sich nicht mehr anmelden kann. Nach Abschluss dieses Vorgangs kann der Benutzer das auf dem Medium 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, der von Dell Server 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. Jede 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 Security Management Server/Security Management Server Virtual gespeichert. Der neue Server tauscht während der Aktivierung Zertifikate mit dem Dell Server aus und verwendet das Zertifikat für die folgenden Authentifizierungsereignisse.

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 Benutzerkonto ist unabhängig von allen anderen

Benutzerkonten auf dem Computer oder in der Domäne und es hat keinen Benutzernamen und kein Kennwort, das physisch verwendet werden kann. Dem Konto wird in der Verwaltungskonsole ein eindeutiger UCID-Wert zugewiesen.