Encryption

Systemanforderungen 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 Dokument enthält die Anforderungen für Dell Encryption.

Um auf die gesamte Dell Encryption-Dokumentation zuzugreifen, gehen Sie zu www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.

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

Diese Anforderungen gelten für alle Clients. Anforderungen, die in anderen Abschnitten aufgeführt sind, gelten für bestimmte 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 Security Management Server/Security Management Server Virtual 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, 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 erforderlich für das Master Installationsprogramm und die untergeordneten Installationsprogramm-Clients. 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. Zur Installation von Microsoft .Net Framework 4.5.2 gehen Sie zu https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- 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

Alle Clients - Hardware

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

Hardware

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

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.

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.
- Entfernen Sie mithilfe des Windows-Desktopbereinigungs-Assistenten temporäre Dateien und andere unnötige Daten, um den Zeitaufwand für die anfängliche Verschlüsselung zu verringern.
- Schalten Sie den Energiesparmodus bei der ersten Verschlüsselungssuche aus, um zu verhindern, dass ein unbeaufsichtigter Computer in diesen Modus umschaltet. Im Energiesparmodus kann keine Verschlüsselung (oder Entschlüsselung) erfolgen.
- Der Encryption-Client unterstützt keine Dual-Boot-Konfigurationen, da es hierdurch zur Verschlüsselung von Systemdateien des anderen Betriebssystems kommen kann, was den Betrieb stören würde.
- Das Master-Installationsprogramm unterstützt keine Aktualisierungen von Komponenten vor Version 8.0. Extrahieren Sie untergeordnete Installationsprogramme aus dem Master-Installationsprogramm und aktualisieren Sie einzeln die Komponente.
- Der Encryption-Client unterstützt jetzt den Audit-Modus. Der Audit-Modus ermöglicht Administratoren die Bereitstellung des Encryption-Clients als Teil des Unternehmens-Image, anstatt das SCCM eines Drittanbieters oder ähnliche Lösungen zur Bereitstellung des Encryption-Clients zu verwenden. Eine Anleitung zur Installation des Encryption-Clients in einem Image des Unternehmens finden Sie unter http://www.dell.com/support/article/us/en/19/SLN304039.
- 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/SLN288353 nach oder kontaktieren Sie den Dell ProSupport, um Hilfe zu erhalten.
- Das TPM wird zum Versiegeln des GPK-Schlüssels verwendet. Falls Sie den Encryption-Client ausführen, löschen Sie daher das TPM im BIOS, bevor Sie ein neues Betriebssystem auf dem Client-Computer installieren.
- 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. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponente installieren, bevor Sie den Encryption-Client installieren.

Voraussetzungen

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

Encryption-Client-Hardware

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

Optionale integrierte Hardware

- TPM 1.2 oder 2.0

Encryption-Client-Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

- Windows 7 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 Version 1607 (Anniversary Update/Redstone 1) bis Version 1803 (April 2018 Update/Redstone 4)
- VMWare Workstation 12.5 und höher

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

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 8: Enterprise, Pro, Consumer
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- 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)

- Mac OS Sierra 10.12.4 und 10.12.5
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14

Serververschlüsselungs-Client

Die Serververschlüsselung ist für die Verwendung auf Computern gedacht, die im Servermodus ausgeführt werden, insbesondere Dateiserver.

- Die Serververschlüsselung ist nur mit Encryption Enterprise und Endpoint Security Suite Enterprise kompatibel.
- Die Serververschlüsselung bietet Folgendes:
  - Software-Verschlüsselung wird
  - Verschlüsselung von Wechselmedien
  - Portsteuerung

    ANMERKUNG:
    Der Server muss Portsteuerungen unterstützen.

    Die Server-Portsteuerungssystem-Richtlinien wirken sich auf die auf geschützten Servern befindlichen Wechselmedien aus, indem z. B. der Zugriff und die Nutzung der USB-Ports des Servers durch USB-Geräte gesteuert wird. Die USB-Port-Richtlinie gilt für externe USB-Ports. Die interne USB-Port-Funktionalität wird durch die USB-Port-Richtlinie nicht beeinflusst. Bei deaktivierter USB-Port-Richtlinie funktionieren USB-Tastatur und Maus des Clients nicht und der Benutzer kann den Computer nicht verwenden, wenn vor Anwenden der Richtlinie keine Remote Desktop-Verbindung eingerichtet wurde.

Die Serververschlüsselung wird angewendet auf:

- Dateiserver mit lokalen Laufwerken
- Virtual Machine (VM)-Gäste, die ein Server-Betriebssystem oder Nicht-Server-Betriebssystem als einfachen Dateiserver ausführen
- Unterstützte Konfigurationen:
  - Mit RAID 5- oder 10-Laufwerken ausgestattete Server; RAID 0 (Striping) und RAID 1 (Mirroring) werden unabhängig voneinander unterstützt.
  - Mit Multi TB RAID-Laufwerken ausgestattete Server
  - Server, die mit Laufwerken ausgestattet sind, die ohne Herunterfahren des Computers ausgetauscht werden können.
  - Die Serververschlüsselung wird hinsichtlich branchenführender Antivirus-Anbieter überprüft. Für diese Antivirus-Anbieter wurden hart kodierte Ausnahmen eingerichtet, um Inkompatibilitäten zwischen Antivirus-Überprüfungen und Verschlüsselung zu verhindern. Falls Ihr Unternehmen Virenschutzsoftware von einem hier nicht aufgeführten Anbieter verwendet, lesen Sie den KB-Artikel SLN298707 oder kontaktieren Sie Dell ProSupport, um Hilfe zu erhalten.

Nicht unterstützt

Die Serververschlüsselung wird nicht angewendet auf:

- Security Management Servers/Security Management Server Virtuals oder Server, die Datenbanken für Security Management Servers/ Security Management Server Virtual ausführen.
- Serververschlüsselung ist nicht kompatibel mit Encryption Personal.
- Serververschlüsselung wird nicht unterstützt mit SED-Management oder BitLocker Manager-Client.
- Server Encryption wird nicht auf Servern unterstützt, die Teil von verteilten Dateisystemen (DFS) sind.
- Migration zu oder von der Serververschlüsselung wird nicht unterstützt. Upgrades von Encryption External Media auf Server Encryption erfordern, dass das vorherige Produkt oder die vorherigen Produkte vor der Installation von Server Encryption vollständig deinstalliert werden.
- VM-Hosts (ein VM-Host enthält typischerweise mehrere VM-Gäste.)
- Domain-Controller
- Exchange-Server
- Server, die Datenbanken hosten (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange, etc.)
- Server, die eine der folgenden Technologien verwenden:
  - Robuste Dateisysteme (ReFS)
  - Fluid-Dateisysteme
  - Microsoft-Speicherplätze
  - SAN/NAS-Netzwerkspeicherlösungen
  - Über iSCSI verbundene Geräte
  - Deduplizierungssoftware
  - Hardware-Deduplizierung
  - Aufgeteilte RAIDs (mehrere Volumes über ein einzelnes RAID)
  - SED-Laufwerke (RAIDs und NICHT-RAID)
  - Auto-Anmeldung (Windows 7, 8/8.1) für Kiosk-Systeme
  - Microsoft Storage Server 2012
- Die Serververschlüsselung 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 mit folgenden Wiederherstellungsverfahren wieder her. Weitere Informationen zur Wiederherstellung von verschlüsselten Daten finden Sie in der *Recovery Guide* (Wiederherstellungsanleitung).

Serververschlüsselungs-Client – Hardware

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

Serververschlüsselungs-Client – Betriebssysteme

In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

Betriebssystem (32- und 64-Bit)
• Windows 7 SP1: Enterprise, Professional, Ultimate • Windows 8.0: 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)

Unterstützte Server-Betriebssysteme

- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition, Enterprise Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Datacenter Edition (Server Core wird nicht unterstützt)
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition (Server Core wird nicht unterstützt)
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition (Server Core wird nicht unterstützt)

Betriebssysteme, die vom UEFI-Modus unterstützt werden

- 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)

ANMERKUNG:

Auf einem unterstützten UEFI-Computer startet der Computer neu, nachdem Sie die Option **Neustart** im Hauptmenü ausgewählt haben, und zeigt einen von zwei möglichen Anmeldebildschirmen an. Der angezeigte Anmeldebildschirm richtet sich nach der jeweiligen Architektur der Computer-Plattform.

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

Unterstützte Server-Betriebssysteme

- Windows Server 2012 R2

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