Dell Endpoint Security Suite Enterprise

Advanced Installation Guide v3.9

January 2024
Rev. A01

DELL Technologies

Anmerkungen, Vorsichtshinweise und Warnungen

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

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

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

Contents

1

Einleitung

Dieses Handbuch beschreibt die Installation und Konfiguration von Advanced Threat Prevention, Encryption, SED-Verwaltung, Full Disk Encryption, Web Protection und Client Firewall und BitLocker Manager.

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 (Installations- und Migrationshandbuch für Security Management Server)*
   - *Security Management Server Virtual Quick Start Guide and Installation Guide (Schnellanleitung und Installationshandbuch für Security Management Server Virtual)*
   - Stellen Sie sicher, dass die Richtlinien wie gewünscht eingestellt sind. Durchsuchen Sie die AdminHilfe, die Sie über das **?** ganz rechts im Bildschirm aufrufen können. Die AdminHilfe ist eine seitenbezogene Hilfe, die eigens dafür entwickelt wurde, Sie bei der Einstellung und Änderung von Richtlinien zu unterstützen und mit den Optionen Ihres Dell Server vertraut zu machen.
2. Bereitstellung eines Mandanten für Advanced Threat Prevention Ein Tenant muss im Dell Server bereitgestellt werden, bevor die Durchsetzung von Advanced Threat Prevention-Richtlinien aktiv wird.
3. Lesen Sie sich das Kapitel Anforderungen in diesem Dokument genau durch.
4. Stellen Sie Clients für die Benutzer bereit.

Verwendung des Handbuchs

Wenden Sie das Handbuch in der folgenden Reihenfolge an.

- Unter Anforderungen finden Sie Informationen über Client-Voraussetzungen, Computer-Hardware und -Software, Einschränkungen und spezielle Registrierungsänderungen, die für bestimmte Funktionen erforderlich sind.
- Lesen Sie bei Bedarf die Abschnitte Vorinstallationskonfiguration für SED UEFI und BitLocker.
- Wenn Ihren Clients über Dell Digital Delivery Rechte zugewiesen werden sollen, lesen Sie GPO auf Domänen-Controller zur Aktivierung von Rechten einstellen.
- Zur Installation von Clients unter Verwendung des Endpoint Security Suite Enterprise Master-Installationsprogramms finden Sie Informationen unter:
  - Aktive Installation unter Verwendung des Master-Installationsprogramms

    oder auf
  - Installation durch Befehlszeile mit dem Master Installationsprogramm
- Falls Sie Clients unter Verwendung der untergeordneten Installationsprogramme installieren möchten, müssen Sie die untergeordneten ausführbaren Dateien zuerst aus dem Master-Installationsprogramm extrahieren. Lesen Sie den Abschnitt Extrahieren der untergeordneten Installationsprogramme aus dem Master-Installationsprogramm und kehren Sie anschließend hierher zurück.
  - Installation der untergeordneten Installationsprogramme über die Befehlszeile:
    - Encryption installieren – Verwenden Sie diese Anweisungen zum Installieren von Encryption, der Komponente, die Sicherheitsrichtlinien durchsetzt, egal ob ein Computer mit dem Netzwerk verbunden oder vom Netzwerk getrennt ist, verloren gegangen ist oder gestohlen wurde.
    - Installieren des Clients für Full Disk Encryption – Verwenden Sie diese Anweisungen zum Installieren von Full Disk Encryption, der Komponente, die Sicherheitsrichtlinien durchsetzt, egal ob ein Computer mit dem Netzwerk verbunden oder vom Netzwerk getrennt ist, verloren gegangen ist oder gestohlen wurde.

- Advanced Threat Prevention installieren – Verwenden Sie diese Anweisungen zur Installation von Advanced Threat Prevention, des Virenschutzes der nächsten Generation, der algorithmische Wissenschaft und maschinelles Lernen einsetzt, um bekannte sowie unbekannte Cyber-Bedrohungen zu identifizieren, zu klassifizieren und von der Ausführung bzw. der Beschädigung von Endpunkten abzuhalten.
- Web Protection und Firewall installieren – Verwenden Sie diese Anweisungen zur Installation der *optionalen* Komponenten Web Protection und Firewall. Die Client-Firewall ist eine statusbehaftete Firewall, die den gesamten ein- und ausgehenden Verkehr gegen eine Liste mit Regeln vergleicht. Der Web-Schutz überwacht das Browsen im Web und das Herunterladen von Dateien aus dem Internet, um Bedrohungen zu identifizieren und basierend auf der Bewertung der aufgerufenen Website eine in der Richtlinie festgelegte Maßnahme durchzuführen, wenn eine Bedrohung erfasst wird.
- SED Manager installieren – Verwenden Sie diese Anweisungen zur Installation der Verschlüsselungssoftware für SEDs. Selbstverschlüsselnde Laufwerke haben zwar eine eigene Verschlüsselungsfunktion, ihnen fehlt aber eine Plattform für die Verwaltung ihrer Verschlüsselung und Richtlinien. Bei Verwendung von SED Manager sind sämtliche Richtlinien, Speicher und der Abruf von Verschlüsselungsschlüsseln über eine einzige Konsole verfügbar. Dadurch verringert sich das Risiko, dass Computer bei Verlust oder unberechtigtem Zugriff ungeschützt sind.
- BitLocker Manager installieren – Folgen Sie diesen Anweisungen, um BitLocker Manager zu installieren. Dieser wurde speziell dafür entwickelt, die Sicherheit von BitLocker-Implementierungen zu erhöhen und zu vereinfachen sowie Betriebskosten zu senken.

  ANMERKUNG:

  Die *meisten* untergeordneten Installationsprogramme können interaktiv installiert werden. Dies ist jedoch nicht Gegenstand dieses Handbuchs. Die untergeordneten Installationsprogramme Advanced Threat Prevention und Full Disk Encryption können jedoch nur über die Befehlszeile installiert werden.

- Unter Üblicherweise verwendete Szenarien finden Sie Skripte von unseren gängigsten Szenarien.

Dell ProSupport for Software kontaktieren

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

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

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

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

2

Anforderungen

Alle Clients

Diese Anforderungen gelten für alle Clients. Anforderungen, die in anderen Abschnitten aufgeführt sind, gelten für bestimmte Clients.

- Bei der Bereitstellung sind die bewährten IT-Verfahren zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Benutzer.
- Die Installation/Aktualisierung/Deinstallation kann nur von einem lokalen Benutzer oder einem Domänenadministrator durchgeführt werden, der über ein Implementierungstool wie Microsoft SCCM 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 dell.com/support, um stets über die neueste Dokumentation und die neuesten technischen Ratgeber zu verfügen.
- Das Produktangebot von Dell Data Security unterstützt keine Versionen von Windows Insider Preview.

Voraussetzungen

- Microsoft .Net Framework 4.5.2 (oder höher) ist erforderlich für das Endpoint Security Suite Enterprise Master-Installationsprogramm und die Clients der untergeordneten Installationsprogramme. Das Installationsprogramm installiert die Microsoft .Net Framework-Komponenten *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: Lesen Sie diese Anweisungen zur Installation von Microsoft .Net Framework 4.5.2.
- Zum Installieren von Encryption im FIPS-Modus ist Microsoft .Net Framework 4.6 erforderlich.

Hardware

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

Hardware
○ Intel Pentium- oder AMD-Prozessor ○ 500 MB verfügbarer Speicherplatz ○ 2 GB RAM **ANMERKUNG:** Zum Verschlüsseln von Dateien am Endpunkt ist zusätzlicher freier Speicherplatz erforderlich. Die Größe variiert je nach aktivierten Richtlinien und Laufwerkskapazität.

Lokalisierung

- Dell Encryption, SED Manager, PBA Advanced Authentication, Advanced Threat Prevention und BitLocker Manager sind MUI-konform und in den folgenden Sprachen lokalisiert. Auf der Managementkonsole angezeigte Advanced Threat Prevention-Daten sind nur in der englischen Sprache verfügbar.

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

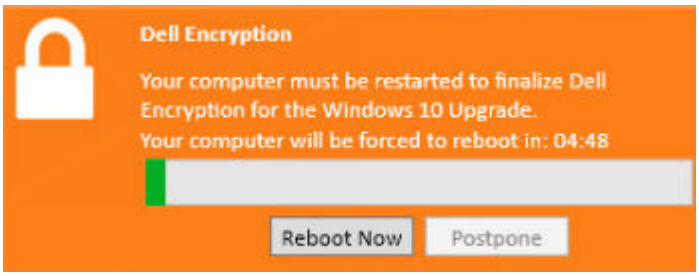
Verschlüsselung

- Der Client-Computer muss über Netzwerkverbindung verfügen.
- Entfernen Sie mithilfe des Windows-Datenträgerbereinigungs-Assistenten temporäre Dateien und andere unnötige Daten, um den Zeitaufwand für die anfängliche Verschlüsselung zu verringern.
- Für die Unterstützung von Windows Hello for Business-Support wird Endpoint Security Suite Enterprise v3.0 oder höher benötigt, auf denen Windows 10 ausgeführt wird.
- Für die Unterstützung von Windows Hello for Business ist die Aktivierung anhand eines Dell Servers mit v11.0 oder höher erforderlich.
- 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.
- Encryption unterstützt keine Dual-Boot-Konfigurationen, da es hierdurch zur Verschlüsselung von Systemdateien des anderen Betriebssystems kommen kann, was den Betrieb stören würde.
- Dell Encryption kann nicht auf v2.7 von Versionen vor v1.6.0 aktualisiert werden. Endpunkte, auf denen Versionen vor v 1.6.0 ausgeführt werden, müssen auf v1.6.0 aktualisiert werden. Anschließend wird ein Upgrade auf v 2.7 durchgeführt.
- Encryption unterstützt jetzt den Audit-Modus. Der Audit-Modus ermöglicht Administratoren die Bereitstellung von Encryption als Teil des Unternehmens-Image, anstatt das SCCM eines Drittanbieters oder ähnliche Lösungen zu verwenden. Anleitungen zur Installation von Encryption in einem Unternehmens-Image finden Sie im KB-Artikel 129990.
- Der Encryption-Client wurde getestet und ist mit mehreren gängigen signaturbasierten Antivirenprogrammen und KI-basierten Virenschutzlösungen kompatibel, einschließlich McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense und einige andere. Standardmäßig sind hartkodierte Ausschlüsse für viele Virenschutzanbieter vorhanden, um Inkompatibilitäten zwischen Virenüberprüfung und Verschlüsselung zu vermeiden.

  Wenn Ihr Unternehmen einen nicht aufgelisteten Virenschutzanbieter verwendet oder Kompatibilitätsprobleme auftreten, lesen Sie den KB-Artikel 126046 oder wenden Sie sich an Dell ProSupport, um unterstützende Informationen zur Validierung der Konfiguration für die Interoperabilität zwischen ihren Softwarelösungen und Dell Data Security Lösungen zu erhalten.
- Dell Encryption nutzt Verschlüsselungsbefehlssätze von Intel, Integrated Performance Primitives (IPP). Weitere Informationen finden Sie im KB-Artikel 126015.
- Das TPM wird zum Versiegeln des Allzweckschlüssels (General Purpose Key) verwendet. Falls Sie Encryption ausführen, löschen Sie daher das TPM im BIOS, bevor Sie ein neues Betriebssystem auf dem Zielcomputer installieren.
- 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.
- Das Master-Installationsprogramm installiert diese Komponenten, wenn sie nicht bereits auf dem Zielcomputer installiert sind. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponenten installieren, bevor Sie die Clients installieren.

Voraussetzungen
○ Visual C++ 2012 Update 4 oder höheres Redistributable Package (x86 oder x64) ○ Visual C++ 2017 oder höheres Redistributable Package (x86 oder x64) ○ Ab Januar 2020 sind SHA1-Signaturzertifikate nicht mehr gültig und können nicht verlängert werden. Auf Geräten, auf denen Windows Server 2008 R2 ausgeführt wird, müssen Microsoft KBs https://support.Microsoft.com/help/4474419 und https://support.Microsoft.com/help/4490628 installiert werden, um die SHA256-Signierung von Zertifikaten auf Anwendungen und Installationspaketen zu validieren. Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt.

- Die Richtlinien *Sichere Windows-Ruhezustand-Datei* und *Ungeschützten Ruhezustand unterbinden* werden im UEFI-Modus nicht unterstützt.
- Die verzögerte Aktivierung dient dazu, dass das Active Directory-Nutzerkonto, 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 Nutzer das Active Directory-basierte Konto an, wenn er dazu aufgefordert wird. Sobald die Zugangsdaten eingegeben wurden, werden die Authentifizierungsinformationen sicher an den Dell Server gesendet, der diese anhand der konfigurierten Active Directory-Domänen validiert. Weitere Informationen finden Sie im KB-Artikel 124736.
- Nach dem Windows 10-Upgrade ist ein Neustart **erforderlich**, um Dell Encryption abzuschließen. Die folgende Meldung wird im Infobereich nach Windows 10-Funktions-Upgrades angezeigt:



Hardware

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

Optionale integrierte Hardware
○ TPM 1.2 oder 2.0

Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

Encryption External Media

Betriebssysteme

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

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

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

Vollständige Datenträgerverschlüsselung

- Die vollständige Datenträgerverschlüsselung erfordert die Aktivierung anhand eines Dell Servers mit v9.8.2 oder höher.
- Vollständige Datenträgerverschlüsselung wird zurzeit nicht auf virtualisierten Host-Computer unterstützt.
- Für die vollständige Datenträgerverschlüsselung ist ein separates Hardware-TPM erforderlich. PTT- und Firmware-basierte TPMs werden aktuell 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 Netzwerkverbindung oder einen Zugangscode verfügen.
- Der Computer muss über eine verkabelte Netzwerkverbindung verfügen, damit sich ein Smartcard-Nutzer 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.
- Dell empfiehlt den neuesten Intel Rapid Storage Technology-Treiber mit NVMe-Laufwerken.
- NVMe-Laufwerke, die für PBA genutzt werden:
  - Wenn das Dell Gerät 2018 oder später hergestellt wurde: Entweder „RAID EIN“ oder „AHCI“ können mit NVMe-Laufwerken genutzt werden.
  - Der BIOS-Startmodus muss auf „Unified Extensible Firmware Interface (UEFI)“ eingestellt werden. Legacy-Vorgangs-ROMs müssen deaktiviert sein.
- Nicht-NVMe-Laufwerke, die für PBA genutzt werden:
  - Der BIOS-SATA-Betrieb kann entweder auf AHCI oder RAID ON eingestellt werden.
  - Das Betriebssystem stürzt ab, wenn es von RAID EIN auf AHCI umgeschaltet wird, wenn den AHCI-Controller-Treiber nicht vorinstalliert wurde. Eine Anleitung zum Umschalten von RAID auf AHCI (oder umgekehrt) finden Sie im KB-Artikel 124714.
- Das Managen 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.
- Direkte Funktionsupdates von Windows 10 v1607 (Anniversary Update/Redstone 1) auf Windows 10 v1903 (May 2019 Update/19H1) werden von FDE nicht unterstützt. Dell empfiehlt beim Update auf Windows 10 v1903 das Betriebssystem auf ein neueres Funktionsupdate zu aktualisieren. Beim Versuch, direkt von Windows 10 v1607 auf v1903 zu aktualisieren, wird eine Fehlermeldung angezeigt und das Update wird verhindert.

- Alle Festplatten müssen initialisiert und formatiert werden, bevor die vollständige Datenträgerverschlüsselung aktiviert wird.
- Für Verschlüsselungskonfigurationen für mehrere Festplatten mit vollständiger Datenträgerverschlüsselung ist Folgendes erforderlich:
  - Alle Festplatten im Zielsystem müssen über die folgende Konfiguration verfügen:
    - Nicht-SED-Laufwerke
    - Konfiguriert im selben Startmodus
    - Initialisiert als GUID-Partitionstabelle (GPT)
    - Festplatten müssen primäre Partitionen sein
    - Festplatten müssen über einen zugewiesenen Laufwerksbuchstaben verfügen
  - Ein Neustart ist erforderlich, um neue Festplatten nach der Erstkonfiguration zu verschlüsseln.
  - Es können maximal 16 Festplatten verschlüsselt werden.
  - Im UEFI-Startmodus kann das Betriebssystem auf jeder Zielfestplatte installiert werden.
  - Im Legacy-Startmodus muss das Betriebssystem auf der ersten Festplatte installiert werden (Festplattenr. 0). Wenn das Betriebssystem nicht auf der ersten Festplatte installiert ist, ist die Verschlüsselung mehrerer Festplatten deaktiviert.

    Aktivieren Sie die Multi-Disk-Verschlüsselung in der Managementkonsole. Rufen Sie die Registrierungseinstellungen auf, um die Windows-Registrierungswerte für Verschlüsselung mit mehreren Laufwerken und Multi-Sweep anzuzeigen.

  - Für die vollständige Festplattenverschlüsselung müssen Windows-Kennwortänderungen und Datenverschlüsselungsschlüssel mit dem nutzerdefinierten Dell Zugangsdatenanbieter synchronisiert werden. Wenn Sie Anwendungen von Drittanbietern verwenden möchten, die nutzerdefinierte Zugangsdatenanbieter verwenden, die auf durch vollständige Festplattenverschlüsselung geschützten Computern ausgeführt werden, müssen Sie Windows-Kennwortänderungen über die Data Security Console initiieren. Weitere Informationen zum Ändern Ihres Kennworts in der Data Security Console finden Sie im Kapitel *Kennwort* im Benutzerhandbuch für die Data Security Console.
- Das Master-Installationsprogramm installiert diese Komponenten, wenn sie nicht bereits auf dem Zielcomputer installiert sind. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponenten installieren, bevor Sie die Clients installieren.

Voraussetzungen
○ Visual C++ 2017 oder höheres Redistributable Package (x86 oder x64) ○ Ab Januar 2020 sind SHA1-Signaturzertifikate nicht mehr gültig und können nicht verlängert werden. Auf Geräten, auf denen Windows Server 2008 R2 ausgeführt wird, müssen Microsoft KBs https://support.microsoft.com/help/4474419 und https://support.microsoft.com/help/4490628 installiert werden, um die SHA256-Signierung von Zertifikaten auf Anwendungen und Installationspaketen zu validieren. Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt.

- **ANMERKUNG:** Bei der Preboot-Authentifizierung ist ein Kennwort erforderlich. Dell empfiehlt Mindestvorgaben für das Kennwort, die den internen Sicherheitsrichtlinien entsprechen.
- **ANMERKUNG:** Wenn PBA verwendet wird, sollte die Richtlinie „Alle Nutzer synchronisieren“ aktiviert werden, wenn ein Computer über mehrere Nutzer verfügt. Darüber hinaus müssen alle Nutzer über Kennwörter verfügen. Nutzer von Kennwörter mit einer Länge von null werden nach der Aktivierung aus dem Computer ausgesperrt.
- **ANMERKUNG:** Durch Full Disk Encryption geschützte Computer müssen auf Windows 10 v1703 (Creators Update/ Redstone 2) aktualisiert werden, bevor eine Aktualisierung auf Windows 10 v1903 (May 2019 Update/19H1) oder höher durchgeführt werden kann. Beim Versuch, ein direktes Betriebssystem-Update durchzuführen, wird eine Fehlermeldung angezeigt.

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

Hardware

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

Optionale integrierte Hardware
○ TPM 1.2 oder 2.0

Authentifizierungsoptionen mit Full Disk Encryption-Client

- Es wird eine spezifische Hardware zum Verwenden von Smartcards und zum Authentifizieren bei UEFI-Computern benötigt. Eine Konfiguration ist erforderlich, um Smartcards mit Preboot-Authentifizierung zu verwenden. In den folgenden Tabellen werden die verfügbaren Authentifizierungsoptionen nach Betriebssystem angezeigt, wenn die Hardware- und Konfigurationsanforderungen erfüllt sind.

UEFI				
	PBA – auf unterstützten Dell Computern			
	Kennwort	Fingerabdruck	Kontakt-Smartcard	SIPR-Karte
Windows 10	X[1]		X[1]	
Windows 11	X[1]		X[1]	
1. Verfügbar auf unterstützten UEFI-Computern.				

Dell Computermodelle mit UEFI-Startmodus-Unterstützung

- Eine aktuelle Liste der mit der vollständigen Datenträgerverschlüsselung unterstützten Plattformen finden Sie im KB-Artikel 126855.
- Eine Liste der Docking-Stationen und Adapter, die von der vollständigen Datenträgerverschlüsselung unterstützt werden, finden Sie unter KB-Artikel 124241.

Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

Encryption auf Serverbetriebssystemen

Encryption auf Serverbetriebssystemen ist für die Verwendung auf Computern gedacht, die im Servermodus ausgeführt werden, insbesondere Dateiserver.

- Encryption auf Serverbetriebssystemen ist nur mit Encryption Enterprise und Endpoint Security Suite Enterprise kompatibel.
- Encryption auf Serverbetriebssystemen bietet:
  - Software-Verschlüsselung

- Verschlüsselung von Wechselmedien
- Portsteuerung

  ANMERKUNG:

  Der Server muss Portsteuerungen unterstützen.

  Die 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 Nutzer kann den Computer nicht verwenden, wenn vor Anwenden der Richtlinie keine Remote Desktop-Verbindung eingerichtet wurde.

- Das Master-Installationsprogramm installiert diese Komponenten, wenn sie nicht bereits auf dem Zielcomputer installiert sind. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponenten installieren, bevor Sie die Clients installieren.

Voraussetzungen
○ Visual C++ 2012 Update 4 oder höheres Redistributable Package (x86 oder x64) ○ Visual C++ 2017 oder höheres Redistributable Package (x86 oder x64) ○ Ab Januar 2020 sind SHA1-Signaturzertifikate nicht mehr gültig und können nicht verlängert werden. Auf Geräten, auf denen Windows Server 2008 R2 ausgeführt wird, müssen Microsoft KBs https://support.Microsoft.com/help/4474419 und https://support.Microsoft.com/help/4490628 installiert werden, um die SHA256-Signierung von Zertifikaten auf Anwendungen und Installationspaketen zu validieren. Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt.

Encryption auf Serverbetriebssystemen ist für die Verwendung mit Folgendem gedacht:

- Dateiserver mit lokalen Laufwerken
- Virtual Machine (VM)-Gäste, die ein Serverbetriebssystem oder Nicht-Serverbetriebssystem 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 Virenschutz-Anbieter wurden hart kodierte Ausnahmen eingerichtet, um Inkompatibilitäten zwischen Virenüberprüfung und Verschlüsselung zu verhindern. Falls Ihr Unternehmen Virenschutzsoftware von einem hier nicht aufgeführten Anbieter verwendet, lesen Sie den KB-Artikel 126046 oder kontaktieren Sie den Dell ProSupport, um Hilfe zu erhalten.

Encryption auf Serverbetriebssystemen ist nicht für die Verwendung mit Folgendem gedacht:

- Security Management Servers/Security Management Server Virtuals oder Server, die Datenbanken für Security Management Servers/Security Management Server Virtual ausführen.
- Encryption Personal.
- SED Manager, erweiterte PBA-Authentifizierung oder BitLocker Manager.
- Server, die Teil von verteilten Dateisystemen (DFS) sind.
- Migration zu oder von Encryption auf einem Serverbetriebssystem. Für ein Upgrade von der External Media Edition auf Encryption für Serverbetriebssysteme ist es erforderlich, das vorhergehende Produkt vollständig zu deinstallieren, bevor Encryption auf Serverbetriebssystemen installiert wird.
- 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-Netzwerk-Storage-Lösungen
- Über iSCSI verbundene Geräte
- Deduplizierungssoftware
- Hardware-Deduplizierung
- Aufgeteilte RAIDs (mehrere Volumes über ein einzelnes RAID)
- SEDs (RAIDs und NICHT-RAID)
- Microsoft Storage Server 2012

- Encryption auf einem Serverbetriebssystem 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 *Wiederherstellungsanleitung*.

Betriebssysteme

In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

Unterstützte Serverbetriebssysteme
• 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) • Windows Server 2019: Standard Edition, Datacenter Edition • Windows Server 2022: Standard Edition, Datacenter Edition

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

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

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

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

Unterstützte Serverbetriebssysteme
• Windows Server 2012 R2

Unterstützte Mac-Betriebssysteme für den Zugriff auf verschlüsselte Medien (64-Bit-Kernel)
• macOS High Sierra 10.13.5 – 10.13.6 • macOS Mojave 10.14.0–10.14.4 • macOS Catalina 10.15.1 – 10.15.4

Advanced Threat Prevention

- Zur kompletten Installation von Advanced Threat Prevention muss der Computer Netzwerkverbindung aufweisen, wenn der Dell Server, der den Client gemanagt, im Verbindungsmodus (Standardeinstellung) ausgeführt wird. Jedoch ist eine Netzwerkverbindung ***nicht*** für die Installation von Advanced Threat Prevention erforderlich, wenn der gemanagte Dell Server im getrennten Modus ausgeführt wird.
- Für die Bereitstellung eines Mandanten für Advanced Threat Prevention muss der Dell Server über eine Internetverbindung verfügen.
- Die optionalen Funktionen Client Firewall und Web Protection sollten ***nicht*** auf Client-Computern installiert sein, die von einem im getrennten Modus ausgeführten Dell Server gemanagt werden.
- Antivirus-, Antimalware- und Antispyware-Anwendungen von anderen Anbietern können zu Störungen des Advanced Threat Prevention-Clients führen. Falls möglich, deinstallieren Sie diese Anwendungen. Windows Defender ist keine Konflikte verursachende Software. Firewall-Anwendungen sind zulässig.

  Wenn das Deinstallieren anderer Antivirus-, Antimalware- und Antispyware-Anwendungen nicht möglich ist, müssen Sie der Advanced Threat Prevention im Dell Server wie auch den anderen Anwendungen Ausnahmen hinzufügen. Anweisungen zum Hinzufügen von Ausnahmen zu Advanced Threat Prevention im Dell Server finden Sie im KB-Artikel 126745. Eine Liste der Erweiterungen, die zu den anderen Antiviren-Anwendungen hinzugefügt werden können, finden Sie im KB-Artikel 126118.

Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

Windows-Betriebssysteme (32-Bit und 64-Bit)
○ Ab Januar 2020 sind SHA1-Signaturzertifikate nicht mehr gültig und können nicht verlängert werden. Auf Geräten, auf denen Windows Server 2008 R2 ausgeführt wird, müssen Microsoft KBs https://support.Microsoft.com/help/4474419 und https://support.Microsoft.com/help/4490628 installiert werden, um die SHA256-Signierung von Zertifikaten auf Anwendungen und Installationspaketen zu validieren. Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt. ○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (November 2019 Update/19H2 – November 2022 Update/ 22H2) **Hinweis:** OEMs und ODMs liefern Windows 10 v2004 (Mai 2020 Update/20H1 und höher) nicht mit 32-Bit-Architektur. Weitere Informationen finden Sie unter https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2 ○ Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition, Enterprise Edition, Webserver Edition ○ Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition ○ Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition ○ Windows Server 2019: Standard Edition, Datacenter Edition

Ports

- Die Advanced Threat Prevention-Agenten werden von der SaaS-Plattform der Managementkonsole gemanagt und erstatten Bericht an diese. Port 443 (https) wird für die Kommunikation verwendet und muss auf der Firewall geöffnet sein, damit die Agenten mit der Konsole kommunizieren können. Die Konsole wird von Amazon Web Services gehostet und verfügt über keine festen IP-Adressen. Sollte Port 443 gesperrt sein, können keine Aktualisierungen heruntergeladen werden. In diesem Fall ist ein ordnungsgemäßer Schutz der Computer nicht gewährleistet. Stellen Sie sicher, dass die Client-Computer wie folgt auf die URLs zugreifen können.

Über die Option	Anwendungsprotokoll	Transportprotokoll	Portnummer	Ziel	Richtung
Gesamte Kommunikation	HTTPS	TCP	443	Lassen Sie den gesamten https-Datenverkehr an *.cylance.com zu.	Ausgehend

Ausführliche Informationen bezüglich der verwendeten URLs finden Sie im KB-Artikel 127053.

Integritätsüberprüfung des BIOS-Abbildes

Wenn die Richtlinie *BIOS-Gewährleistung aktivieren* in der Managementkonsole ausgewählt ist, validiert der Cylance-Mandant einen BIOS-Hash auf Endpunktsystemen, um sicherzustellen, dass das BIOS nicht von der werkseitigen Dell Version verändert wurde, was einen möglichen Angriffspunkt darstellen würde. Wenn eine Gefahr erkannt wird, wird eine Benachrichtigung an den Dell Server gesendet und der IT-Administrator wird in der Managementkonsole über diesen Vorfall benachrichtigt. Eine Übersicht über den Prozess finden Sie unter Prozess für die Integritätsüberprüfung des BIOS-Abbildes.

ANMERKUNG: Ein nutzerdefiniertes Originalabbild kann mit dieser Funktion nicht verwendet werden, da das BIOS verändert wurde.

Dell Computermodelle, auf denen die Integritätsüberprüfung des BIOS-Abbildes unterstützt wird	
• Latitude 3470 • Latitude 3570 • Latitude 7275 • Latitude 7370	• OptiPlex 5040 • OptiPlex 7040 • OptiPlex 7440 • Precision Mobile Workstation 3510

Dell Computermodelle, auf denen die Integritätsüberprüfung des BIOS-Abbildes unterstützt wird		
• Latitude E5270 • Latitude E5470 • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extreme • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240	• Precision Mobile Workstation 5510 • Precision Workstation 3620 • Precision Workstation 7510 • Precision Workstation 7710 • Precision Workstation T3420 • Venue 10 Pro 5056 • Venue Pro 5855 • Venue XPS 12 9250 • XPS 13 9350 • XPS 9550	

Kompatibilität

Die folgende Tabelle zeigt die Kompatibilität mit Windows, Mac und Linux.

Nicht verfügbar – Die Technologie gilt nicht für diese Plattform.

Leeres Feld – Die Richtlinie wird nicht mit Endpoint Security Suite Enterprise unterstützt.

Funktionen	Richtlinien	Zu Beginn einer Shield-Deinstallation aktualisieren Windows	macOS	Linux
Dateimaßnahmen				
	Automatische Quarantäne (Unsicher)	x	x	x
	Automatische Quarantäne (Anormal)	x	x	x
	Automatisch hochladen	x	x	x
	Richtlinie „Sichere Liste“	x	x	x
Speichermaßnahmen				
	Speicherschutz	x	x	x
Ausnutzung				
	Stapeldrehung	x	x	x
	Stapelschutz	x	x	x
	Code überschreiben	x	k. A.	
	RAM-Scraping	x	k. A.	
	Schädliche Nutzlast	x		
Vorgangsinjektion				
	Remote-Zuweisung von Speicher	x	x	k. A.
	Remote-Zuordnung von Speicher	x	x	k. A.
	Remote Schreiben in Speicher	x	x	k. A.
	Remote Schreiben von PE in Speicher	x	k. A.	k. A.
	Code remote überschreiben	x	k. A.	

Funktionen	Richtlinien	Zu Beginn einer Shield-Deinstallation aktualisieren Windows	macOS	Linux
	Zuordnung von Speicher remote aufheben	x	k. A.	
	Remote-Thread-Erstellung	x	x	
	Remote-APC geplant	x	k. A.	k. A.
	DYLD-Injektion		x	x
Eskalation				
	LSASS lesen	x	k. A.	k. A.
	Null-Zuweisung	x	x	
Schutzeinstellungen				
	Ausführungssteuerung	x	x	x
	Herunterfahren des Dienstes vom Gerät verhindern	x	x	
	Unsichere Prozesse und ihre Unterprozesse, die gerade ausgeführt werden, beenden	x	x	x
	Entdeckung einer Hintergrundsbedrohung	x	x	x
	Nach neuen Dateien Ausschau halten	x	x	x
	Maximale Größe der zu scannenden Archivdatei	x	x	x
	Bestimmte Ordner ausschließen	x	x	x
	Dateimuster kopieren	x		
Anwendungssteuerung				
	Fenster ändern	x		x
	Ordnerausschlüsse	x		
Agenten-Einstellungen				
	Automatisches Hochladen von Protokolldateien aktivieren	x	x	x
	Desktop-Benachrichtigungen aktivieren	x		
Skriptsteuerung				
	Aktives Skript	x		
	Powershell	x		
	Office-Makros	x		k. A.
	Powershell-Konsolennutzung blockieren	x		
	Skripte in diesen Ordnern (und Unterordnern) genehmigen	x		
	Protokolliergrad	x		
	Selbstschutzebene	x		

Funktionen	Richtlinien	Zu Beginn einer Shield-Deinstallation aktualisieren Windows	macOS	Linux
	Automatische Aktualisierung	x		
	Erkennung durchführen (von Agent-UI)	x		
	In Quarantäne löschen (Agent-UI und Konsolen-UI)	x		
	Getrennter Modus	x		x
	Detaillierte Bedrohungsdaten	x		
	Zertifizierte sichere Liste	x	x	k. A.
	Malware-Muster kopieren	x	x	x
	Proxy-Einstellungen	x	x	x
	Manuelle Richtlinienüberprüfung (Agent-UI)	x	x	

Client Firewall und Web Protection

- Für die erfolgreiche Installation von Client Firewall und Web Protection muss der Computer mit dem Netzwerk verbunden sein.
- Deinstallieren Sie die Viren-, Malware- und Spyware-Schutzprogramme sowie die Firewall-Anwendungen anderer Hersteller, bevor Sie die Client Firewall- und Web Protection-Clients installieren, um Fehler bei der Installation zu vermeiden. Windows Defender und Endpoint Security Suite Enterprise zählen nicht zu den Softwareprodukten, die Konflikte verursachen.
- Das Master-Installationsprogramm installiert diese Komponenten, wenn sie nicht bereits auf dem Zielcomputer installiert sind. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponenten installieren, bevor Sie Client Firewall und Web Protection installieren.

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

- Die Web Protection-Funktion wird nur von den folgenden Browsern unterstützt:

Browser	Web Protection-Unterstützung	Version
Google Chrome	Ja	Alle modernen Versionen
Microsoft Edge	Ja	Microsoft Edge wird mit Endpoint Security Suite Enterprise v10.1 und höher unterstützt.
Microsoft Internet Explorer 11	Ja	Alle modernen Versionen
Mozilla Firefox	Ja	○ Firefox 56 und höher wird mit Endpoint Security Suite Enterprise v10.0 und höher unterstützt. ○ Firefox 51 wird mit Endpoint Security Suite Enterprise v1.8 und höher unterstützt.

Ports

- Um zu gewährleisten, dass die Client Firewall- und Web Protection mit den aktuellsten Client Firewall- und Web Protection-Aktualisierungen versorgt werden, müssen die Ports 443 und 80 auf dem Client verfügbar sein, damit er

mit den verschiedenen Zielservern kommunizieren kann. Sollten die Ports gesperrt sein, können Updates der Virenschutz-Definitionen (DAT-Dateien) nicht heruntergeladen werden. In diesem Fall ist ein ordnungsgemäßer Schutz der Computer nicht gewährleistet. Stellen Sie sicher, dass die Client-Computer wie folgt auf die URLs zugreifen können.

Über die Option	Anwendungsprotokoll	Transportprotokoll	Portnummer	Ziel	Richtung
Reputation Service	SSL	TCP	443	tunnel.web.trustedsource.org	Ausgehend
Reputation Service Feedback	SSL	TCP	443	gtifeedback.trustedsource.org	Ausgehend
Update der URL-Reputation-Datenbank	HTTP	TCP	80	list.smartfilter.com	Ausgehend
URL Reputation Lookup	SSL	TCP	443	tunnel.web.trustedsource.org	Ausgehend

Betriebssysteme

- In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

Windows-Betriebssysteme (32-Bit und 64-Bit)
○ Ab Januar 2020 sind SHA1-Signaturzertifikate nicht mehr gültig und können nicht verlängert werden. Auf Geräten, auf denen Windows Server 2008 R2 ausgeführt wird, müssen Microsoft KBs https://support.Microsoft.com/help/4474419 und https://support.Microsoft.com/help/4490628 installiert werden, um die SHA256-Signierung von Zertifikaten auf Anwendungen und Installationspaketen zu validieren. Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt.
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (November 2019 Update/19H2 – November 2022 Update/ 22H2) **Hinweis:** OEMs und ODMs liefern Windows 10 v2004 (Mai 2020 Update/20H1 und höher) nicht mit 32-Bit-Architektur. Weitere Informationen finden Sie unter https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC
○ Windows 11: Enterprise, Pro v21H2 - 22H2

SED Manager

- Der Computer muss über Netzwerkverbindung verfügen, damit SED Manager erfolgreich installiert werden kann.
- Der Computer muss über eine verkabelte Netzwerkverbindung verfügen, damit sich ein Smartcard-Nutzer zum ersten Mal über die Preboot-Authentifizierung anmelden kann.
- Anmeldedaten von Drittanbietern funktionieren nicht mit installiertem SED Manager und alle Anmeldedaten von Drittanbietern werden deaktiviert, wenn die PBA aktiviert ist.
- IPv6 wird nicht 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 eine selbstverschlüsselnde Festplatte verfügt, muss in Active Directory die Option *Nutzer muss das Kennwort bei der nächsten Anmeldung ändern* deaktiviert sein. Diese Option von Active Directory wird durch die Preboot-Authentifizierung nicht unterstützt.
- 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 Nutzer aus der PBA.

    oder auf

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

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

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

- Für SED Manager müssen Windows-Kennwortänderungen und Datenverschlüsselungsschlüssel mit dem nutzerdefinierten Dell Zugangsdatenanbieter synchronisiert werden. Wenn Sie Anwendungen von Drittanbietern verwenden möchten, die nutzerdefinierte Zugangsdatenanbieter verwenden, die auf von SED Manager geschützten Computern ausgeführt werden, müssen Sie Windows-Kennwortänderungen über die Data Security Console initiieren. Weitere Informationen zum Ändern Ihres Kennworts in der Data Security Console finden Sie im Kapitel *Kennwort* im Benutzerhandbuch für die Data Security Console.
- Das Master-Installationsprogramm installiert diese Komponenten, wenn sie nicht bereits auf dem Zielcomputer installiert sind. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponenten installieren, bevor Sie die Clients installieren.

Voraussetzungen
○ Visual C++ 2017 oder höheres Redistributable Package (x86 oder x64) ○ Ab Januar 2020 sind SHA1-Signaturzertifikate nicht mehr gültig und können nicht verlängert werden. Auf Geräten, auf denen Windows Server 2008 R2 ausgeführt wird, müssen Microsoft KBs https://support.Microsoft.com/help/4474419 und https://support.Microsoft.com/help/4490628 installiert werden, um die SHA256-Signierung von Zertifikaten auf Anwendungen und Installationspaketen zu validieren. Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt.

- SED Manager wird mit Encryption auf Serverbetriebssystemen oder Advanced Threat Prevention auf einem Serverbetriebssystem nicht unterstützt.
- Verschlüsselungskonfigurationen für mehrere Festplatten mit SED Manager setzen Folgendes voraus:
  - Alle Festplatten im Zielsystem müssen über die folgende Konfiguration verfügen:
    - SED-Laufwerke
    - Festplatten müssen über einen zugewiesenen Laufwerksbuchstaben verfügen
  - Im UEFI-Startmodus kann das Betriebssystem auf jeder Zielfestplatte installiert werden.

- Im Legacy-Startmodus muss das Betriebssystem auf der ersten Festplatte installiert werden (Festplattenr. 0). Wenn das Betriebssystem nicht auf der ersten Festplatte installiert ist, ist die Verschlüsselung mehrerer Festplatten deaktiviert.

  Aktivieren Sie die Multi-Disk-Verschlüsselung in der Managementkonsole. Rufen Sie die Registrierungseinstellungen auf, um die Windows-Registrierungswerte für Verschlüsselung mit mehreren Laufwerken und Multi-Sweep anzuzeigen.

- **ANMERKUNG:** Bei der Preboot-Authentifizierung ist ein Kennwort erforderlich. Dell empfiehlt Mindestvorgaben für das Kennwort, die den internen Sicherheitsrichtlinien entsprechen.

- **ANMERKUNG:** Wenn PBA verwendet wird, sollte die Richtlinie „Alle Nutzer synchronisieren“ aktiviert werden, wenn ein Computer über mehrere Nutzer verfügt. Darüber hinaus müssen alle Nutzer über Kennwörter verfügen. Nutzer von Kennwörter mit einer Länge von null werden nach der Aktivierung aus dem Computer ausgesperrt.
- **ANMERKUNG:** Durch SED Manager geschützte Computer müssen auf Windows 10 v1703 (Creators Update/Redstone 2) aktualisiert werden, bevor eine Aktualisierung auf Windows 10 v1903 (May 2019 Update/19H1) oder höher durchgeführt werden kann. Beim Versuch, ein direktes Betriebssystem-Update durchzuführen, wird eine Fehlermeldung angezeigt.
-

Hardware

OPAL-kompatible SEDs

- Für die auf dem neuesten Stand Liste der Opal kompatible SEDs unterstützt, wenn das SED Management, beziehen sich auf dieses KB-Artikel: 126855.
- Für die aktuellste Liste von Plattformen, die mit SED Manager unterstützt werden, lesen Sie KB-Artikel: 126855.
- Eine Liste der Docking-Stationen und Adapter, die von SED Manager unterstützt werden, finden Sie im KB-Artikel 124241.

Preboot-Authentifizierungsoptionen mit SED Manager

- Es wird eine spezifische Hardware zum Verwenden von Smartcards und zum Authentifizieren bei UEFI-Computern benötigt. Eine Konfiguration ist erforderlich, um Smartcards mit Preboot-Authentifizierung zu verwenden. In den folgenden Tabellen werden die verfügbaren Authentifizierungsoptionen nach Betriebssystem angezeigt, wenn die Hardware- und Konfigurationsanforderungen erfüllt sind.

Ohne UEFI				
	PBA			
	Kennwort	**Fingerabdruck**	**Kontakt-Smartcard**	**SIPR-Karte**
Windows 10	X[1]		X[1 2]	
Windows 11	X[1]		X[1 2]	
1. Verfügbar, wenn die Authentifizierungstreiber von dell.com/support heruntergeladen wurden 2. Verfügbar auf einem unterstützten OPAL-SED				

UEFI				
	PBA – auf unterstützten Dell Computern			
	Kennwort	**Fingerabdruck**	**Kontakt-Smartcard**	**SIPR-Karte**
Windows 10	X[1]		X[1]	

UEFI				
	PBA – auf unterstützten Dell Computern			
	Kennwort	Fingerabdruck	Kontakt-Smartcard	SIPR-Karte
Windows 11	X[1]		X[1]	
1. Verfügbar mit einem unterstützten OPAL-SED auf unterstützten UEFI-Computern				

Internationale Tastaturen

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

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

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

Betriebssysteme

- Die folgende Tabelle enthält Informationen zu den unterstützten Betriebssystemen.

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

Lokalisierung

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

Sprachunterstützung	
EN: Englisch	JA: Japanisch

Sprachunterstützung	
FR: Französisch	KO: Koreanisch
IT: Italienisch	PT-BR: Portugiesisch, Brasilien
DE: Deutsch	PT-PT: Portugiesisch, Portugal
ES: Spanisch	

BitLocker Manager

- 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. Lesen Sie Vorinstallationskonfiguration zum Einrichten einer BitLocker PBA-Partition.
- 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 im KB-Artikel 124931.
- Tastatur, Maus und Videokomponenten müssen direkt an den Computer angeschlossen sein. Setzen Sie keinen KVM-Schalter zum Verwalten 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 verwendet die zulässigen von AES FIPS validierten Algorithmen, falls der FIPS-Modus für die GPO-Sicherheitseinstellung „System-Kryptographie: FIPS-konforme Algorithmen für Verschlüsselung, Hashing und Signatur verwenden“ auf dem Gerät aktiviert ist und Sie dieses Gerät über unser Produkt managen. BitLocker Manager erzwingt diesen Modus nicht als Standardeinstellung für BitLocker-verschlüsselte Clients, da Microsoft seinen Kunden mittlerweile empfiehlt, die FIPS-validierte Verschlüsselung nicht zu verwenden, da vermehrt Probleme mit der Anwendungskompatibilität, Wiederherstellung und Medienverschlüsselung aufgetreten sind: http://blogs.technet.com.
- BitLocker Manager wird nicht mit Encryption auf Serverbetriebssystemen oder Advanced Threat Prevention auf einem Serverbetriebssystem unterstützt.
- Bei Verwendung einer Remote-Desktopverbindung mit einem Endpunkt, der BitLocker Manager nutzt, empfiehlt Dell das Ausführen einer beliebigen Remote-Desktopsitzung im Konsolenmodus, um etwaige UI-Interaktionsprobleme bei der vorhandenen Nutzersitzung mit dem folgenden Befehl zu vermeiden:

  ```
  mstsc /admin /v:<target_ip_address>
  ```

- Das Master-Installationsprogramm installiert diese Komponenten, wenn sie nicht bereits auf dem Zielcomputer installiert sind. **Wenn Sie das untergeordnete Installationsprogramm verwenden**, müssen Sie diese Komponenten installieren, bevor Sie die Clients installieren.

Voraussetzungen
○ Visual C++ 2017 oder höheres Redistributable Package (x86 oder x64) ○ Ab Januar 2020 sind SHA1-Signaturzertifikate nicht mehr gültig und können nicht verlängert werden. Auf Geräten, auf denen Windows Server 2008 R2 ausgeführt wird, müssen Microsoft KBs https://support.Microsoft.com/help/4474419 und https://support.Microsoft.com/help/4490628 installiert werden, um die SHA256-Signierung von Zertifikaten auf Anwendungen und Installationspaketen zu validieren. Anwendungen und Installationspakete, die mit SHA1-Zertifikaten signiert sind, funktionieren, aber wenn diese Aktualisierungen nicht installiert sind, wird während der Installation oder Ausführung der Anwendung auf dem Endpunkt ein Fehler angezeigt.

- **ANMERKUNG:** Durch SED Manager geschützte Computer müssen auf Windows 10 v1703 (Creators Update/Redstone 2) aktualisiert werden, bevor eine Aktualisierung auf Windows 10 v1903 (May 2019 Update/19H1) oder höher durchgeführt werden kann. Beim Versuch, ein direktes Betriebssystem-Update durchzuführen, wird eine Fehlermeldung angezeigt.

- **ANMERKUNG:** Direkte Betriebssystemupgrades auf eine neuere Version – wie z. B. Windows 10 – auf Windows 11 werden nicht unterstützt.

Hardware

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

Optionale integrierte Hardware
○ TPM 1.2 oder 2.0

Betriebssysteme

- In den folgenden Tabellen sind die unterstützten Betriebssysteme aufgeführt.

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

Windows Server Betriebssysteme
○ Windows Server 2008 R2: Standard Edition, Enterprise Edition (64-Bit) ○ Windows Server 2012 R2: Standard Edition, Enterprise Edition (64-Bit) ○ Windows Server 2016: Standard Edition, Datacenter Edition (64-Bit) ○ Windows Server 2019: Standard Edition, Datacenter Edition (64-Bit) ○ Windows Server 2022: Standard Edition, Datacenter Edition

3

Registrierungseinstellungen

- In diesem Abschnitt werden alle vom Dell ProSupport genehmigten Registrierungseinstellungen für lokale **Client**-Computer beschrieben, unabhängig vom Grund für Registrierungseinstellung. Falls eine Registrierungseinstellung für zwei Produkte gilt, wird sie in beiden Kategorien aufgeführt.
- Diese Registrierungsänderungen sollten nur von Administratoren ausgeführt werden und sind möglicherweise nicht für alle Szenarios geeignet oder funktionieren nicht in allen Szenarios.

Verschlüsselung

- Wenn ein selbstsigniertes Zertifikat auf dem Dell Server verwendet wird. Bei Windows muss die Zertifikatvertrauensüberprüfung auf dem Clientcomputer deaktiviert bleiben (Vertrauensüberprüfung ist standardmäßig *deaktiviert* bei Dell Server). Vor dem *Aktivieren* der Vertrauensprüfung auf dem Client-Computer müssen die folgenden Voraussetzungen erfüllt sein:
  - Ein von einer Stammzertifizierungsstelle wie EnTrust oder Verisign signiertes Zertifikat muss in den Dell Server importiert werden.
  - Die vollständige Vertrauenskette des Zertifikats muss im Microsoft Keystore des Client-Computers gespeichert werden.
  - Um die Vertrauensüberprüfung für Encryption zu *aktivieren*, ändern Sie den Wert des folgenden Registrierungseintrags auf dem Zielcomputer in 0.

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

    "IgnoreCertErrors"=DWORD:00000000

    0 = bei Zertifikatsfehler fehlschlagen

    1= Fehler ignorieren

- Um eine Encryption Removal Agent-Protokolldatei anzulegen, erstellen Sie auf dem für die Entschlüsselung vorgesehenen Computer den folgenden Registrierungseintrag. Weitere Informationen finden Sie unter (Optional) Encryption Removal Agent-Protokolldatei.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=DWORD:2

  0: Keine Protokollierung

  1: Protokolliert Fehler, die den Betrieb des Dienstes verhindern

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

  3: Protokolliert Informationen über alle zu entschlüsselnden Datenträger und Dateien

  5: Protokolliert Informationen zum Debuggen

- Ändern Sie den folgenden Registrierungswert oder ändern Sie in der die Richtlinie *Neustart nach Aktualisierung erzwingen*, um den Benutzer zu deaktivieren, um den Computer neu zu starten.

  [HKLM\Software\Dell\Dell Data Protection]

  "ShowDecryptAgentRebootPrompt"=DWORD

  1 = aktiviert (zeigt Eingabeaufforderung an)

  0 = deaktiviert (Aufforderung zum Ausblenden)

- Standardmäßig wird das Infobereichssymbol während der Installation angezeigt. Verwenden Sie die folgenden Registrierungseinstellungen, um das Infobereichssymbol für alle verwalteten Benutzer nach der ursprünglichen Installation auf einem Computer auszublenden. So erstellen oder ändern Sie die Registrierungseinstellungen:

  [HKLM\Software\CREDANT\CMGShield]

  "HIDESYSTRAYICON"=DWORD:1

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

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

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

  [HKLM\SOFTWARE\CREDANT\CMGShield]

  "DeleteTempFiles"=REG_DWORD:0

  Werden temporäre Dateien nicht gelöscht, verlängert sich die Verschlüsselungsdauer.

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

  Sie können das Verhalten der Benutzeraufforderung dahingehend ändern, dass die Verschlüsselung begonnen oder verzögert wird, damit keine Verschlüsselung durchgeführt wird, wenn der Benutzer nicht auf die Aufforderung reagiert. Legen Sie zu diesem Zweck den Wert wie folgt fest:

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

  "SnoozeBeforeSweep"=DWORD:1

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

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

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

- Über die Registrierungseinstellung wird Encryption veranlasst, beim Dell Server eine durchgesetzte Richtlinienaktualisierung abzufragen. So erstellen oder ändern Sie die Registrierungseinstellungen:

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  Nach erfolgter Änderung werden die Registrierungseinstellungen automatisch geschlossen.

- Verwenden Sie die Registrierungseinstellungen, um Encryption zu erlauben, optimierte, vollständige (aktivierte und nicht aktivierte Benutzer) oder vollständige (nur aktivierte Benutzer) Bestandsinformationen an den Dell Server zu senden.
  - Senden optimierter Bestandsinformationen an den Dell Server:

    So erstellen oder ändern Sie die Registrierungseinstellungen:

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

    "OnlySendInvChanges"=REG_DWORD:1

    Wenn kein Eintrag vorhanden ist, werden optimierte Bestandsinformationen an den Dell Server gesendet.
  - Senden vollständiger Bestandsinformationen an den Dell Server:

    So erstellen oder ändern Sie die Registrierungseinstellungen:

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

    "OnlySendInvChanges"=REG_DWORD:0

    Wenn kein Eintrag vorhanden ist, werden optimierte Bestandsinformationen an den Dell Server gesendet.
  - Senden vollständiger Bestandsinformationen für alle aktivierten Benutzer

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

    "RefreshInventory"=REG_DWORD:1

Dieser Eintrag wird nach der Verarbeitung aus der Registrierung gelöscht, der Wert wird jedoch gespeichert. Dadurch ist Encryption in der Lage, die Anfrage beim nächsten Upload zu erfüllen, selbst wenn der Computer neu gestartet wird, bevor die Bestandsinformationen hochgeladen wurden.

Dieser Eintrag ersetzt den Registrierungswert für OnlySendInvChanges.

- Die Aktivierung mit Zeitfenster ist eine Funktion, mit der Sie Aktivierungen von Clients über einen vorgegebenen Zeitraum verteilen können, um während einer Massenimplementierung eine Überlastung des Dell Server zu vermeiden. Aktivierungen werden basierend auf Zeitfenstern verzögert, die durch Algorithmen generiert werden, um eine gleichmäßige Verteilung der Aktivierungszeiten zu erreichen.

  Für Benutzer, die eine Aktivierung durch VPN benötigen, kann eine Aktivierungskonfiguration mit Zeitfenster erforderlich sein, damit die anfängliche Aktivierung lange genug verzögert wird, um dem VPN-Client den Aufbau einer Netzwerkverbindung zu erlauben.

  Die folgenden Änderungen an der Registrierung treten erst nach einem Neustart des Computers in Kraft.

  - **Gestaffelte Aktivierung**

    Um diese Funktion zu aktivieren bzw. zu deaktivieren, erstellen Sie einen DWORD mit dem Namen **SlottedActivation** unter dem übergeordneten Schlüssel:

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

  - **Aktiverungszeitfenster**

    Um diese Funktion zu aktivieren bzw. zu deaktivieren, erstellen Sie einen Sekundärschlüssel mit dem Namen **ActivationSlot** unter dem übergeordneten Schlüssel:

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

    Aktivierungszeitfenster – eine Zeichenkette zum Festlegen des Zeitfensters, in dem Encryption versucht, sich beim Dell Server zu aktivieren. Diese Werte werden in Sekunden angegeben und die Syntax wird durch <lowervalue>,<uppervalue> definiert. Ein Beispiel wäre 120,300. Dies bedeutet, dass Encryption einen Aktivierungsversuch zu einem zufällig bestimmten Zeitpunkt zwischen 2 Minuten und 5 Minuten nach der Benutzeranmeldung unternimmt.

    - **Kalenderwiederholung**

      Um diese Funktion zu aktivieren bzw. zu deaktivieren, erstellen Sie einen Sekundärschlüssel mit dem Namen **CalRepeat** unter dem übergeordneten Schlüssel:

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

      CalRepeat – Ein DWORD, das den Zeitraum in Sekunden angibt, in dem das Aktivierungszeitintervall liegt. Mit dieser Einstellung überschreiben Sie den Zeitraum in Sekunden, in dem das Aktivierungszeitintervall auftritt. 25.200 Sekunden stehen zur Verfügung, um Aktivierungen während eines Zeitraums von sieben Stunden einzuplanen. Die Standardeinstellung ist 86400 Sekunden, was einer täglichen Wiederholung entspricht. Der vorgeschlagene Dezimalwert ist 600, also 10 Minuten.

    - **Zeitintervall**

      Um diese Funktion zu aktivieren bzw. zu deaktivieren, erstellen Sie einen Sekundärschlüssel mit dem Namen **SlotInterval** unter dem übergeordneten Schlüssel:

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

      Zeitintervall – Eine Zeichenfolge, die die Intervalle zwischen Aktivierungen mit Zeitfenster definiert. Die empfohlene Einstellung ist 45,120. Dies bedeutet, dass die Aktivierungszeit zwischen 45 und 120 Sekunden liegt und zufällig bestimmt wird.

    - **Verfehlter Schwellenwert**

      Um diese Funktion zu aktivieren bzw. zu deaktivieren, erstellen Sie einen Sekundärschlüssel mit dem Namen **MissThreshold** unter dem übergeordneten Schlüssel:

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

      MissThreshold – eine DWORD-Wert, der eine positive Ganzzahl enthält, die angibt, wie viele Aktivierungsversuche unternommen werden, bevor eine Abmeldung erforderlich ist. Wenn der Wert von MissThreshold erreicht ist, werden keine Aktivierungsversuche mehr unternommen bis zur nächsten Anmeldung des nicht aktivierten Benutzers. Der Zählwert von MissThreshold wird beim Abmelden immer zurückgesetzt.

      In den Registrierungsschlüsseln werden die Nutzerdaten der Aktivierung mit Zeitfenster gesammelt:

      [HKCU/Software/CREDANT/ActivationSlot] (Daten pro Benutzer)

Verzögerungszeit bis zum Versuch der Aktivierung mit Zeitfenster, die eingestellt wird, wenn sich der Benutzer zum ersten Mal beim Netzwerk anmeldet, nachdem die Aktivierung mit Zeitfenster aktiviert wurde. Das Aktivierungszeitfenster wird für jeden Aktivierungsversuch neu berechnet.

[HKCU/Software/CREDANT/SlotAttemptCount] (Daten pro Benutzer)

Anzahl der fehlgeschlagenen oder verpassten Versuche, wenn das Zeitfenster beginnt und ein Aktivierungsversuch gestartet wird, aber fehlschlägt. Wenn diese Anzahl den in ACTIVATION_SLOT_MISSTHRESHOLD festgelegten Wert erreicht, versucht der Computer bei der Verbindung mit dem Netzwerk noch eine einzige Aktivierung.

- Um nicht verwaltete Benutzer auf dem Client-Computer zu ermitteln, stellen Sie den Registrierungswert auf dem Client-Computer ein:

  [HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]

  "UnmanagedUserDetected"=DWORD value:1

  Nicht verwaltete Benutzer auf diesem Computer ermitteln = 1

  Nicht verwaltete Benutzer nicht auf diesem Computer ermitteln = 0

- Um die automatische Reaktivierung im Hintergrund zu aktivieren, für den seltenen Fall, dass ein Benutzer deaktiviert wird, muss der Registrierungseintrag auf dem Client-Computer festgelegt werden.

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=DWORD:00000001

  0 = Deaktiviert (Standardeinstellung)

  1 = Aktiviert

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

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=DWORD:00000000

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

  Weitere Informationen über SDUser finden Sie im KB-Artikel 131035.

- Stellen Sie den Registrierungseintrag EnableNGMetadata ein, wenn Probleme im Zusammenhang mit Microsoft-Updates auf Computern mit gemeinsamen mittels Schlüssel verschlüsselten Daten oder mit der Verschlüsselung, der Entschlüsselung oder dem Entpacken einer großen Anzahl von Dateien in einem Ordner auftreten.

  Stellen Sie den Registrierungseintrag EnableNGMetadata an folgendem Pfad ein:

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

  "EnableNGMetadata" = DWORD:1

  0 = Deaktiviert (Standardeinstellung)

  1 = Aktiviert

- Wenn Sie die Funktion zur Nicht-Domänen-Aktivierung aktivieren möchten, wenden Sie sich bitte an den Dell ProSupport, um die entsprechenden Anweisungen zu erhalten.
- Der Encryption Management Agent gibt standardmäßig keine Richtlinien mehr aus. Erstellen Sie den folgenden Registrierungsschlüssel, um zukünftig verbrauchte Richtlinien auszugeben:

  HKLM\Software\Dell\Dell Data Protection\

  " DumpPolicies" = DWORD

  Wert=1

  Hinweis: Protokolle werden in C:\ProgramData\Dell\Dell Data Protection\Policy geschrieben.

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

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

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

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

Vollständige Datenträgerverschlüsselung

- In diesem Abschnitt werden alle vom Dell ProSupport genehmigten Registrierungseinstellungen für lokale Computer beschrieben, unabhängig vom Grund für die Registrierungseinstellung. Falls eine Registrierungeinstellung für zwei Produkte gilt, wird sie in beiden Kategorien aufgeführt.
- Diese Registrierungsänderungen sollten nur von Administratoren ausgeführt werden und sind möglicherweise nicht für alle Szenarios geeignet oder funktionieren nicht in allen Szenarios.
- Fügen Sie den folgenden Registrierungswert hinzu, um das Wiederholungsintervall festzulegen, wenn der Dell Server nicht mit Full Disk Encryption kommunizieren kann.

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD:300

  Dieser Wert steht für die Anzahl der Sekunden, die Full Disk Encryption abwartet, bis es erneut versucht, den Dell Server zu kontaktieren, wenn dieser nicht mit Full Disk Encryption kommunizieren kann. Der Standardwert lautet 300 Sekunden (5 Minuten).

- Falls auf dem Dell Server ein selbstsigniertes Zertifikat für Full Disk Encryption verwendet wird, muss die SSL/TLS-Vertrauensprüfung auf dem Client-Computer deaktiviert bleiben (die SSL/TLS-Vertrauensprüfung ist standardmäßig bei Full Disk Encryption *deaktiviert*). Vor dem *Aktivieren* der SSL/TLS-Vertrauensprüfung auf dem Client-Computer müssen die folgenden Voraussetzungen erfüllt sein.
  - Ein von einer Stammzertifizierungsstelle wie EnTrust oder Verisign signiertes Zertifikat muss in den Dell Server importiert werden.
  - Die vollständige Vertrauenskette des Zertifikats muss im Microsoft Keystore des Client-Computers gespeichert werden.
  - Um die SSL/TLS-Vertrauensprüfung für Dell Encryption Management zu *aktivieren*, ändern Sie den Wert des folgenden Registrierungseintrags auf dem Client-Computer in 0.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    „DisableSSLCertTrust“=DWORD:0

    0 = Aktiviert

    1 = Deaktiviert

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

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

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

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

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

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

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

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

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

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

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

  "SmartCardLogonNotify"=DWORD:1

  0 = Deaktiviert

  1 = Aktiviert

- Bei der Erstinstallation wird der Standort des Security Server-Hosts festgelegt. Diesen können Sie bei Bedarf ändern. Die Hostinformationen werden bei jeder Richtlinienänderung durch den Client-Computer gelesen. Ändern Sie den folgenden Registrierungswert auf dem Client-Computer:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com

- Bei der Erstinstallation wird der Standort des Security Server-Ports festgelegt. Diesen können Sie bei Bedarf ändern. Dieser Wert wird bei jeder Richtlinienänderung durch den Clientcomputer gelesen. Ändern Sie den folgenden Registrierungswert auf dem Client-Computer:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888

- (Nur mit Preboot-Authentifizierung) Wenn Sie **nicht** möchten, dass die erweiterte PBA-Authentifizierung die Dienste in Verbindung mit Smartcards und biometrischen Geräten in den Starttyp „Automatisch“ ändert, deaktivieren Sie die Funktion zum Starten von Diensten. Das Deaktivieren der Funktion bewirkt auch, dass keine Warnmeldungen in Verbindung zu den nicht ausgeführten Diensten angezeigt werden.

  Ist diese Funktion **deaktiviert**, unternimmt die erweiterte PBA-Authentifizierung für folgende Dienste keinen Startversuch:

  - SCardSvr – Verwaltet den Zugang zu den von einem Computer gelesenen Smartcards. Wird dieser Dienst gestoppt, kann der Computer keine Smartcards lesen. Ist dieser Dienst deaktiviert, können alle direkt davon abhängigen Dienste nicht gestartet werden.
  - SCPolicySvc – Ermöglicht es, das System so zu konfigurieren, dass der Benutzer-Desktop bei Entfernen der Smartcard gesperrt wird.
  - WbioSrvc – Der Biometrie-Dienst von Windows ermöglicht es Client-Anwendungen, biometrische Daten ohne direkten Zugriff auf Biometrie-Hardware oder -Proben zu erfassen, zu vergleichen, zu ändern und zu speichern. Der Dienst wird in einem bevorzugten SVCHOST-Prozess gehostet.

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Aktiviert

    1 = Deaktiviert

- Um zu verhindern, dass Full Disk Encryption Drittanbieter von Anmeldeinformation deaktiviert, erstellen Sie den folgenden Registrierungsschlüssel:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 = Deaktiviert (Standardeinstellung)

  1 = Aktiviert

  Hinweis: Dieser Wert kann anfänglich verhindern, dass der Dell-Anmeldeinformationsanbieter die Anmeldeinformationen korrekt synchronisiert, da die Anmeldeinformationen von Drittanbietern deaktiviert sind. Stellen Sie sicher, dass die Geräte, die diesen Registrierungsschlüssel verwenden, ordnungsgemäß mit dem Dell-Server kommunizieren können.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = Aktiviert (Standard)

  1 = Deaktiviert

- Um die Installation der vollen Datenträgerverschlüsselung mit richtlinienbasierter Verschlüsselung zuzulassen, muss der folgende Registrierungswert auf dem Client-Computer eingestellt sein.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  " EnableFDE" = DWORD: 1

  0 = Deaktiviert (Standardeinstellung)

  1 = Aktiviert

Advanced Threat Prevention

- Damit das Advanced Threat Prevention-Plugin „HKLM\SOFTWARE\Dell\Dell Data Protection“ Änderungen des Werts „LogVerbosity“ überwacht und die Client-Protokollierungsebene entsprechend aktualisiert, legen Sie den folgenden Wert fest.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=DWORD:<see below>

  Dump: 0

  Schwerwiegender Fehler: 1

  Fehler 3

  Warnung 5

  Info 10

  Ausführlich 12

  Verfolgen 14

  Debuggen 15

  Der Registrierungswert ist aktiviert, wenn der Advanced Threat Prevention-Dienst startet oder immer dann, wenn der Wert sich ändert. Wenn der Registrierungswert nicht vorhanden ist, gibt es keine Änderung auf der Protokollierungsebene.

  Verwenden Sie diese Registrierungseinstellung nur für Prüfungs-/Debugging-Aktivitäten, da sie die Ausführlichkeitsstufe für andere Komponenten steuert, einschließlich Encryption und Encryption Management Agent.

- Mit dem Kompatibilitätsmodus können Anwendungen auf dem Client-Computer ausgeführt werden, während die Richtlinien Speicherschutz oder Speicherschutz und Skriptsteuerung aktiviert sind. Das Aktivieren des Kompatibilitätsmodus macht das Hinzufügen eines Registrierungswerts auf dem Clientcomputer notwendig.

  Führen Sie zur Aktivierung des Kompatiblitätsmodus die folgenden Schritte aus:

  1. Deaktivieren Sie in der Verwaltungskonsole die Richtlinie *Speicherschutz aktiviert*. Wenn die *Skriptsteuerung*srichtlinie aktiviert ist, deaktivieren Sie sie.
  2. Fügen Sie die Registrierungswert CompatibilityMode hinzu.
     a. Gehen Sie mithilfe des Registrierungs-Editors auf dem Client-Computer zu `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`.
     b. Klicken Sie mit der rechten Maustaste auf **Desktop**, klicken Sie auf **Berechtigungen**, übernehmen Sie dann den Besitz und gewähren Sie sich selbst Vollzugriff.
     c. Klicken Sie mit der rechten Maustaste auf **Desktop**, wählen Sie dann **Neu Binarwert** aus.
     d. Geben Sie für den Namen `CompatibilityMode` ein.
     e. Öffnen Sie die Einstellung der Registrierungsdatei und ändern Sie den Wert in `01`.
     f. Klicken Sie auf **OK**, und schließen Sie dann den Registrierungs-Editor.

     Zum Hinzufügen des Registrierungswerts durch einen Befehl können Sie eine der folgenden Befehlszeilenoptionen zur Ausführung auf dem Clientcomputer verwenden:

     - (Für einen einzigen Computer) Psexec:

       ```
       psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v
       CompatibilityMode /t REG_BINARY /d 01
       ```

     - (Für mehrere Computer) Invoke-Command cmdlet:

       ```
       $servers = "testComp1","testComp2","textComp3"
       ```

```
$credential = Get-Credential -Credential {UserName}\administrator

Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item
-Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value
01}
```

3. Aktivieren Sie in der Verwaltungskonsole die Richtlinie *Speicherschutz aktiviert* erneut. Wenn die *Skriptsteuerung*srichtlinie zuvor aktiviert war, aktivieren Sie sie erneut.

SED Manager

- Fügen Sie den folgenden Registrierungswert hinzu, um das Wiederholungsintervall festzulegen, wenn der Dell Server nicht mit dem SED Manager kommunizieren kann.

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD:300

  Dieser Wert steht für die Anzahl der Sekunden, die SED Manager abwartet, bis sie erneut versucht, den Dell Server zu kontaktieren, wenn dieser nicht kommunizieren kann. Der Standardwert lautet 300 Sekunden (5 Minuten).

- Falls auf dem Dell Server für SED Manager ein selbstsigniertes Zertifikat verwendet wird, muss die SSL/TLS-Vertrauensprüfung auf dem Client-Computer deaktiviert bleiben (die SSL/TLS-Vertrauensprüfung ist bei SED Manager standardmäßig *deaktiviert*). Vor dem *Aktivieren* der SSL/TLS-Vertrauensprüfung auf dem Client-Computer müssen die folgenden Voraussetzungen erfüllt sein.
  - Ein von einer Stammzertifizierungsstelle wie EnTrust oder Verisign signiertes Zertifikat muss in den Dell Server importiert werden.
  - Die vollständige Vertrauenskette des Zertifikats muss im Microsoft Keystore des Client-Computers gespeichert werden.
  - Um die SSL/TLS-Vertrauensprüfung für SED Manager zu *aktivieren*, ändern Sie den Wert des folgenden Registrierungseintrags auf dem Client-Computer in 0.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    „DisableSSLCertTrust“=DWORD:0

    0 = Aktiviert

    1 = Deaktiviert

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

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

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

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

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

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

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

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

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

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

  "SmartCardLogonNotify"=DWORD:1

  0 = Deaktiviert

  1 = Aktiviert

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

  HKLM\SOFTWARE\Dell\Dell Data Protection\

"AllowOtherCredProviders" = DWORD:1

0 = Deaktiviert (Standardeinstellung)

1 = Aktiviert

Hinweis: Dieser Wert kann anfänglich verhindern, dass der Dell-Anmeldeinformationsanbieter die Anmeldeinformationen korrekt synchronisiert, da die Anmeldeinformationen von Drittanbietern deaktiviert sind. Stellen Sie sicher, dass die Geräte, die diesen Registrierungsschlüssel verwenden, ordnungsgemäß mit dem Dell-Server kommunizieren können.

- Um das Intervall festzulegen, in dem SED Manager versucht, den Dell Server anzusprechen, wenn dieser nicht in der Lage ist zu kommunizieren, definieren Sie den folgenden Wert auf dem Zielcomputer:

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD Value:300

  Dieser Wert steht für die Anzahl der Sekunden, die SED Manager abwartet, bis sie erneut versucht, den Dell Server zu kontaktieren, wenn dieser nicht kommunizieren kann. Der Standardwert lautet 300 Sekunden (5 Minuten).

- Bei der Erstinstallation wird der Standort des Security Server-Hosts festgelegt. Diesen können Sie bei Bedarf ändern. Die Hostinformationen werden bei jeder Richtlinienänderung gelesen. Ändern Sie den folgenden Registrierungswert auf dem Client-Computer:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com

- Bei der Erstinstallation wird der Standort des Security Server-Ports festgelegt. Diesen können Sie bei Bedarf ändern. Dieser Wert wird bei jeder Richtlinienänderung gelesen. Ändern Sie den folgenden Registrierungswert auf dem Client-Computer:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888

- Bei der Erstinstallation wird die URL des Security Server-Ports festgelegt. Diese können Sie bei Bedarf ändern. Dieser Wert wird bei jeder Richtlinienänderung durch den Clientcomputer gelesen. Ändern Sie den folgenden Registrierungswert auf dem Client-Computer:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent

- (Nur mit Preboot-Authentifizierung) Wenn Sie **nicht** möchten, dass die erweiterte PBA-Authentifizierung die Dienste in Verbindung mit Smartcards und biometrischen Geräten in den Starttyp „Automatisch“ ändert, deaktivieren Sie die Funktion zum Starten von Diensten. Das Deaktivieren der Funktion bewirkt auch, dass keine Warnmeldungen in Verbindung zu den nicht ausgeführten Diensten angezeigt werden.

  Ist diese Funktion **deaktiviert**, unternimmt die erweiterte PBA-Authentifizierung für folgende Dienste keinen Startversuch:

  - SCardSvr – Verwaltet den Zugang zu den von einem Computer gelesenen Smartcards. Wird dieser Dienst gestoppt, kann der Computer keine Smartcards lesen. Ist dieser Dienst deaktiviert, können alle direkt davon abhängigen Dienste nicht gestartet werden.
  - SCPolicySvc – Ermöglicht es, das System so zu konfigurieren, dass der Benutzer-Desktop bei Entfernen der Smartcard gesperrt wird.
  - WbioSrvc – Der Biometrie-Dienst von Windows ermöglicht es Client-Anwendungen, biometrische Daten ohne direkten Zugriff auf Biometrie-Hardware oder -Proben zu erfassen, zu vergleichen, zu ändern und zu speichern. Der Dienst wird in einem bevorzugten SVCHOST-Prozess gehostet.

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Aktiviert

    1 = Deaktiviert

- Um Smartcards mit der SED-PBA-Authentifizierung zu verwenden, muss der folgende Registrierungswert auf dem mit SED ausgestatteten Client-Computer eingestellt sein.

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

  "MSSmartcardSupport"=DWORD:1

Setzen Sie in der Managementkonsole die Richtlinie für die Authentifizierungsmethode auf Smartcard und bestätigen Sie die Änderung.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = Aktiviert (Standard)

  1 = Deaktiviert

BitLocker Manager

- Falls auf dem Dell Server für BitLocker Manager ein selbstsigniertes Zertifikat verwendet wird, muss die SSL/TLS-Vertrauensprüfung auf dem Client-Computer deaktiviert bleiben (die SSL/TLS-Vertrauensprüfung ist standardmäßig *deaktiviert* bei BitLocker Manager). Vor dem *Aktivieren* der SSL/TLS-Vertrauensprüfung auf dem Client-Computer müssen die folgenden Voraussetzungen erfüllt sein.
  - Ein von einer Stammzertifizierungsstelle wie EnTrust oder Verisign signiertes Zertifikat muss in den Dell Server importiert werden.
  - Die vollständige Vertrauenskette des Zertifikats muss im Microsoft Keystore des Client-Computers gespeichert werden.
  - Um die SSL/TLS-Vertrauensprüfung für BitLocker Manager zu *aktivieren*, ändern Sie den Wert des folgenden Registrierungseintrags auf dem Client-Computer in 0.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    „DisableSSLCertTrust“=DWORD:0

    0 = Aktiviert

    1 = Deaktiviert

  - Um zu verhindern, dass BitLocker Manager Wechseldatenträger als Festplatten erkennt, fügen Sie den folgenden Registrierungsschlüssel hinzu:

    HKLM\Software\Dell\Dell Data Protection\

    "UseEncryptableVolumeType" = DWORD:1

    0 = Deaktiviert (Standardeinstellung)

    1 = Aktiviert

4

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.
- Endpoint Security Suite Enterprise master-Installationsprogramm-Protokolldateien befinden sich unter `C:\ProgramData\Dell\Dell Data Protection\Installer`.

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

- 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 finden Sie in der *Dell Encrypt Hilfe*. Greifen Sie auf die Hilfe über `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help` zu.
  - In der *Encryption External Media Hilfe* finden Sie die Funktionen von Encryption External Media. Greifen Sie auf die Hilfe über `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS` zu.
  - Siehe *Endpoint Security Suite Enterprise-Hilfe* für weitere Informationen zur Verwendung der Funktionen von Advanced Threat Prevention. Greifen Sie auf die Hilfe über `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help` zu.
- 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 auf
  - Installation durch Befehlszeile mit dem Master Installationsprogramm

Aktive Installation unter Verwendung des Master-Installationsprogramms

- Das Endpoint Security Suite EnterpriseMaster-Installationsprogramm befindet sich unter:
  - **Über Ihr Dell FTP-Konto** – Suchen Sie das Installationspaket unter Endpoint-Security-Suite-Ent-1.x.x.xxx.zip.
- Verwenden Sie diese Anweisungen zur interaktiven Installation und Aktualisierung von Dell Endpoint Security Suite Enterprise mithilfe des Endpoint Security Suite EnterpriseMaster-Installationsprogramms. Sie können dieses Verfahren anwenden, um die gesamte Produkt-Suite gleichzeitig auf einem Computer zu installieren.

1. Suchen Sie die Datei **DDSSuite.exe** auf dem Dell-Installationsmedium. Kopieren Sie sie auf den lokalen Computer.
2. Doppelklicken Sie auf **DDSSuite.exe**, 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. Geben Sie in *Dell Management Server-Name vor Ort* den vollständigen qualifizierten Hostnamen des Dell Servers zur Verwaltung des Zielbenutzers ein.

   Geben Sie die Portwerte in die Ports für den *Core-Server* und den *Security-Server* ein, wenn Ihr Unternehmen nicht standardmäßige Ports verwendet.

   Klicken Sie auf **Weiter.**

6. Klicken Sie auf **Weiter**, um das Produkt am standardmäßigen Speicherort `C:\Program Files\Dell\Dell Data Protection\. Dell recommends installing in the default location only` zu speichern, da es zu Problemen kommen kann, falls dieser an anderen Speicherorten installiert wird.
7. Wählen Sie die zu installierenden Komponenten aus.

   Security Framework installiert das zugrunde liegende Sicherheits-Framework.

   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.

   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.

   Advanced Threat Prevention installiert den Advanced Threat Prevention-Client, den Virenschutz der nächsten Generation, der algorithmische Wissenschaft und maschinelles Lernen einsetzt, um bekannte sowie unbekannte Cyber-Bedrohungen zu identifizieren, zu klassifizieren und von der Ausführung bzw. der Beschädigung von Endpunkten abzuhalten.

   Web Protection und Firewall installiert die optionalen Funktionen Web Protection und Firewall. Die Client-Firewall vergleicht den gesamten ein- und ausgehenden Verkehr anhand einer Liste mit Regeln. Der Web-Schutz überwacht das Browsen im Web und das Herunterladen von Dateien aus dem Internet, um Bedrohungen zu identifizieren und basierend auf der Bewertung der aufgerufenen Website eine in der Richtlinie festgelegte Maßnahme durchzuführen, wenn eine Bedrohung erfasst wird.

   Encryption External Media installiert nur die Komponente, die Encryption External Media erzwingt.

   Bei der *vollständigen Datenträgerverschlüsselung* wird die Komponente installiert, die die vollständige Datenträgerverschlüsselung erzwingt.

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

8. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen. Die Installation kann mehrere Minuten dauern.
9. 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 Endpoint Security Suite EnterpriseMaster-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
/s	Automatische Installation
/z	Gibt Variablen an die MSI-Datei innerhalb der Datei DDSSuite.exe weiter.

Parameter

- Die folgende Tabelle beschreibt die Parameter, die mit dem Endpoint Security Suite EnterpriseMaster-Installationsprogramm verwendet werden können. Das Endpoint Security Suite Enterprise-Master-Installationsprogramm kann keine einzelnen Komponenten ausschließen, aber Befehle empfangen, die angeben, welche Komponenten installiert werden sollen.

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. ATP = *nur* Advanced Threat Prevention DE-ATP = Advanced Threat Prevention und Encryption. Dies ist die standardmäßige Installation, wenn der Parameter FUNKTIONEN nicht festgelegt ist. DE = nur Laufwerk Encryption Client BLM = BitLocker Manager SED = SED Manager (Encryption Management Agent/Manager, PBA/GPE Drivers)(Nur verfügbar, wenn auf einem Workstation-Betriebssystem installiert) ATP-WEBFIREWALL = Advanced Threat Prevention mit Client Firewall und Web Protection DE-ATP-WEBFIREWALL = Encryption und Advanced Threat Prevention mit Client Firewall und Web Protection **ANMERKUNG:** Bei Upgrades von Encryption Enterprise oder Endpoint Security Suite Enterprise vor Version 1.4 ***muss*** ATP-WEBFIREWALL oder DE-ATP-WEBFIREWALL angegeben werden, um Client Firewall und Web Protection zu installieren. Geben Sie nicht ATP-WEBFIREWALL bzw. DE-ATP-WEBFIREWALL an, wenn Sie einen Client installieren, der von Dell Server im getrennten Modus ausgeführt wird.
BLM_ONLY=1	Muss verwendet werden, wenn FEATURES=BLM in der Befehlszeile verwendet wird, um das Plugin SED Manager auszuschließen.

Beispiel für eine Befehlszeile

- Bei den Befehlszeilenparametern ist die Groß- und Kleinschreibung zu beachten.
- (Auf einem Workstation-Betriebssystem) In diesem Beispiel werden alle Komponenten unter Verwendung des Endpoint Security Suite EnterpriseMaster-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.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com\""
  ```
- (Auf einem Arbeitsplatz-Betriebssystem) In diesem Beispiel werden ***nur*** Advanced Threat Prevention und Encryption unter Verwendung des Endpoint Security Suite Enterprise-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.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
  ```
- (Auf einem Workstation-Betriebssystem) In diesem Beispiel werden Advanced Threat Prevention, Encryption und SED Manager unter Verwendung des Master-Installationsprogramms für Endpoint Security Suite Enterprise 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.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=ATP-SED,
  SUPPRESSREBOOT=1\""
  ```
- (Auf einem Arbeitsplatz-Betriebssystem) In diesem Beispiel werden Advanced Threat Prevention, Encryption, Web Protection und Client-Firewall unter Verwendung des Endpoint Security Suite Enterprise-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.

```
"DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=ATP-WEBFIREWALL\""
```

- (Auf einem Serverbetriebssystem) In diesem Beispiel werden ***nur*** Advanced Threat Prevention und Encryption unter Verwendung des Endpoint Security Suite Enterprise-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.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
  ```

- (Auf einem Serverbetriebssystem) In diesem Beispiel werden Advanced Threat Prevention, Encryption, Web Protection und Client-Firewall unter Verwendung des Endpoint Security Suite Enterprise-Master-Installationsprogramms auf Standardports, im Hintergrund und am Standardspeicherort installiert: `C:\Program Files\Dell\Dell Data Protection\`

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-ATP-WEBFIREWALL\""
  ```

- (Auf einem Serverbetriebssystem) In diesem Beispiel wird ***nur*** Advanced Threat Prevention unter Verwendung des Endpoint Security Suite Enterprise-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.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=ATP\""
  ```

- (Auf einem Workstation-Betriebssystem) In diesem Beispiel werden Advanced Threat Prevention, BitLocker Manager und Web Protection unter Verwendung des Master-Installationsprogramms für Endpoint Security Suite Enterprise 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.

  ```
  "DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.domain.com, FEATURES=BLM-ATP-WEBFIREWALL,
  SUPPRESSREBOOT=1, BLM_ONLY=1\""
  ```

- (Auf einem Serverbetriebssystem) In diesem Beispiel wird ***nur*** Encryption unter Verwendung des Endpoint Security Suite Enterprise-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.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE\""
  ```

5

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 Endpoint Security Suite EnterpriseMaster-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 Endpoint Security Suite EnterpriseMaster-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.
  1. Encryption deinstallieren
  2. Advanced Threat Prevention deinstallieren.
  3. Full Disk Encryption deinstallieren (Hiermit wird der Dell Encryption Management Agent deinstalliert, der erst nach der Deinstallation von Advanced Threat Prevention deinstalliert werden kann).
  4. SED Manager deinstallieren (Hiermit wird der Dell Encryption Management Agent deinstalliert, der erst nach der Deinstallation von Advanced Threat Prevention deinstalliert werden kann).
  5. BitLocker Manager deinstallieren
- Fahren Sie mit dem Schritt Master-Installationsprogramm deinstallieren fort.

Deinstallieren des Master-Installationsprogramms für Endpoint Security Suite Enterprise

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 für Endpoint Security Suite Enterprise im Hintergrund deinstalliert.

  ```
  "DDSSuite.exe" /s /x
  ```

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

6

Installation unter Verwendung der untergeordneten Installationsprogramme

- Um jeden Client einzeln zu installieren oder zu erweitern, müssen die untergeordneten ausführbaren Dateien zuerst aus dem Endpoint Security Suite EnterpriseMaster-Installationsprogramm extrahiert werden, wie unter Extrahieren der untergeordneten Installationsprogramme aus dem Master-Installationsprogramm erläutert.
- Bei in diesem Abschnitt enthaltenen Befehlsbeispielen wird davon ausgegangen, dass die Befehle von `C:\extracted` ausgeführt werden.
- Bei den Befehlszeilenschaltern und -parametern ist die Groß- und Kleinschreibung zu beachten.
- Stellen Sie sicher, dass Werte, die ein oder mehrere Sonderzeichen enthalten, z. B. eine Leerstelle in der Befehlszeile, zwischen in Escape-Zeichen gesetzte Anführungszeichen gesetzt werden.
- Verwenden Sie diese Installationsprogramme zur Installation der Clients. Nutzen Sie dazu eine skriptgesteuerte Installation, Batchdateien oder eine andere verfügbare Push-Technologie.
- Der Neustart wurde in den Befehlszeilenbeispielen unterdrückt. Es ist jedoch ein abschließender Neustart erforderlich.

  Hinweis: Die richtlinienbasierte Verschlüsselung kann erst nach dem Neustart des Computers beginnen.

- Protokolldateien – Windows erstellt eindeutige Installationsprotokolldateien des untergeordneten Installationsprogramms für den angemeldeten Benutzers unter „%Temp%“ mit dem folgenden Verzeichnispfad `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. Der Standard-MSI-Befehl kann dazu verwendet werden, um eine Protokolldatei durch die Verwendung von `/l*v C:\<beliebiges verzeichnis>\<beliebiger protokolldateiname>.log` zu erstellen.

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

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

ANMERKUNG:

Mit `/v` stehen die Microsoft Standardoptionen zur Verfügung. Eine Liste der Optionen finden Sie in diesem Artikel.

Option	Erläuterung
`/q`	Kein Fortschrittsdialogfeld, führt nach Abschluss der Installation selbstständig einen Neustart durch
`/qb`	Fortschrittsdialogfeld mit der Schaltfläche **Abbrechen,** fordert zum Neustart auf

Option	Erläuterung
/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
/norestart	Neustart unterdrücken

- 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 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 die *Endpoint Security Suite Enterprise-Hilfe* für weitere Informationen zur Verwendung von Advanced Threat Prevention. Hier können Sie auf die Hilfe zugreifen: `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help`.

Treiber installieren

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

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

Encryption installieren

- Lesen Sie den Abschnitt Encryption-Anforderungen, wenn Ihr Unternehmen ein Zertifikat verwendet, das von einer Stammstelle signiert wurde, z. B. EnTrust oder Verisign. Zur Aktivierung der Zertifikatsprüfung muss eine Registrierungseinstellung auf dem Client-Computer geändert werden.
- 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 Encryption-Installationsprogramm kann wie folgt ermittelt werden:
  - **Über Ihr Dell FTP-Konto** – Suchen Sie das Installationspaket in der Datei Endpoint-Security-SuiteEnt-1.x.x.xxx.zip und extrahieren Sie dann die untergeordneten Installationsprogramme aus dem Master-Installationsprogramm. Suchen Sie nach dem Extrahieren die Datei unter `C:\extracted\Encryption`.
  - **ANMERKUNG:** Dell Encryption-Protokolle geben nicht an, ob eine Installation aufgrund unzureichenden Speicherplatzes fehlschlägt.

Installation über die Befehlszeile

- Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

Parameter
SERVERHOSTNAME=<ServerName> (Vollqualifizierter Domänenname des Dell Server für erneute Aktivierung)
POLICYPROXYHOSTNAME=<RGKName> (Vollqualifizierter Domänenname des Standard-Richtlinien-Proxys)
MANAGEDDOMAIN=<MyDomain> (Für das Gerät zu verwendende Domäne)
DEVICESERVERURL=<DeviceServerName/SecurityServerName> (Zur Aktivierung verwendet URL; enthält normalerweise Servernamen, Port und xapi)
GKPORT=<NewGKPort> (Gatekeeper-Port)
MACHINEID=<MachineName> (Computername)
RECOVERYID=<RecoveryID> (Wiederherstellungs-ID)
REBOOT=ReallySuppress (Null ermöglicht automatische Neustarts, ReallySuppress deaktiviert den Neustart)
HIDEOVERLAYICONS=1 (0 aktiviert Overlay-Symbole, 1 deaktiviert Overlay-Symbole)
HIDESYSTRAYICON=1 (0 aktiviert das Symbol im Infobereich, 1 deaktiviert das Symbol im Infobereich)
ENABLE_FDE_LM=1 (Erlaubt die Installation von Dell Encryption auf einem Computer mit aktiver Full Disk Encryption)
EME=1 (Installieren im Modus Encryption External Media)

Eine Liste der grundlegenden .msi-Schalter und Anzeigeoptionen, die in Befehlszeilen verwendet werden können, finden Sie unter Installation unter Verwendung der untergeordneten Installationsprogramme.

- Die folgende Tabelle zeigt Details zusätzlicher optionaler Parameter im Zusammenhang mit der Aktivierung.

Parameter
SLOTTEDACTIVATON=1 (0 deaktiviert verzögerte/geplante Aktivierungen, 1 aktiviert verzögerte/geplante Aktivierungen)
SLOTINTERVAL=45,120 (plant Aktivierungen anhand der Angabe x,x, wobei der erste Wert die untere Grenze des Zeitplans und der zweite Wert die obere Grenze ist – in Sekunden)
CALREPEAT=600 (MUSS gleich dem oder höher als der in SLOTINTERVAL festgelegte obere Grenzwert sein. Anzahl der Sekunden, die Encryption wartet, bevor ein Aktivierungsversuch basierend auf SLOTINTERVAL generiert wird.)

Beispiel für eine Befehlszeile

ANMERKUNG: Ersetzen Sie `DEVICESERVERURL=https://server.organization.com`**:8081/xapi** (ohne den nachgestellten Schrägstrich), wenn Sie einen Security Management Server in einer Version vor v7.7 haben.

- Im folgenden Beispiel wird Dell Encryption mit den Standardparametern installiert (Encryption, Für Freigabe verschlüsseln, kein Dialogfeld, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
```

MSI-Befehl:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- Im folgenden Beispiel werden Encryption und die Option „Für Freigabe verschlüsseln“ installiert, das Dell Encryption-Infobereichssymbol und die Überlagerungssymbole werden ausgeblendet, es gibt keine Dialogfelder, keine Statusanzeige und keinen Neustart und die Installation erfolgt im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ HIDESYSTRAYICON=1
  HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
  ```

  MSI-Befehl:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
  ```

Beispiel für eine Befehlszeile zur ausschließlichen Installation von Encryption External Media

- Installation im Hintergrund, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  MSI-Befehl:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- Installation im Hintergrund, kein Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

  MSI-Befehl:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" EME="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/" MANAGEDDOMAIN="ORGANIZATION"
  ```

- **ANMERKUNG:**

  Im Dialogfeld „Info“ des Clients wird die Versionsnummer der Software angezeigt, nicht jedoch, ob Encryption (vollständig) oder nur Encryption External Media installiert ist. Gehen Sie zum Auffinden dieser Informationen zu `C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log`, und machen Sie den folgenden Eintrag ausfindig:

  [<Datum/Zeitstempel> DeviceInfo: < >] ***Shield-Informationen - SM=Nur External Media***, SB=DELL, UNF=FQUN, last sweep={0, 0}

Beispiel für eine Befehlszeile, um Encryption External Media in Vollversion von Encryption zu konvertieren

ANMERKUNG: Das Konvertieren von Encryption External Media in Encryption (vollständige Installation) wird bei Upgrades nicht unterstützt.

- Eine Entschlüsselung wird beim Konvertieren von Encryption External Media in die Vollversion von Encryption nicht benötigt.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ REINSTALL=ALL EME=0
  REINSTALLMODE=vamus /qn"
  ```

  MSI-Befehl:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
REINSTALL="ALL" EME="0" REINSTALLMODE="vamus"
```

- **Beispiel für eine Befehlszeile für die Installation von Dell Encryption mit vollständiger Datenträgerverschlüsselung**

  \Verschlüsselung

- Im folgenden Beispiel wird Dell Encryption mit den Standardparametern installiert (Encryption, Für Freigabe verschlüsseln, kein Dialogfeld, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  Dann:

  \Encryption Management Agent

  Im folgenden Beispiel wird eine remote verwaltete vollständige Datenträgerverschlüsselung installiert und eine Installation auf einem mit Dell Encryption geschützten Computer ermöglicht (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **Beispiel für eine Befehlszeile zur Installation von Encryption External Media mit vollständiger Datenträgerverschlüsselung.**

  \Verschlüsselung

  Im folgenden Beispiel wird nur Encryption External Media installiert (Installation im Hintergrund, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption.`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Dann:

  \Encryption Management Agent

  Im folgenden Beispiel wird eine remote verwaltete vollständige Datenträgerverschlüsselung installiert und eine Installation auf einem mit Dell Encryption geschützten Computer ermöglicht (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **Beispiel für eine Befehlszeile zur Installation von Encryption External Media über eine bestehende Installation mit vollständiger Datenträgerverschlüsselung.**

  Im folgenden Beispiel wird Encryption External Media über eine bestehende Installation mit vollständiger Datenträgerverschlüsselung installiert, mit Installation im Hintergrund, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis `C:\Programme\Dell\Dell Data Protection`.

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
  norestart /qn"
  ```

- **Beispiel für eine Befehlszeile zur Installation eines remote-verwalteten Verschlüsselungsclients über eine vorhandene Installation mit vollständiger Datenträgerverschlüsselung.**

Im folgenden Beispiel wird Dell Encryption mit den Standardparametern über eine vorhandene Installation von Full Disk Encryption installiert (Encryption-Client, Encrypt for Sharing, kein Dialogfeld, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`) und Installationsprotokolle in `C:\Dell`. **Anmerkung:** Für erfolgreiche Protokollerstellung muss das Verzeichnis `C:\Dell` vor der Installation vorhanden sein.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
norestart /qn /l*v C:\Dell\DellEncryptionInstall.log"
```

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

DDPE_XXbit_setup.exe /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

Full Disk Encryption installieren

- Lesen Sie den Abschnitt Anforderungen für Full Disk Encryption, wenn Ihr Unternehmen ein Zertifikat verwendet, das von einer Stammstelle signiert wurde, z. B. EnTrust oder Verisign. Zur Aktivierung der SSL/TLS-Vertrauensprüfung muss eine Registrierungseinstellung auf dem Client-Computer geändert werden.
- Benutzer melden sich mit ihren Windows-Anmeldeinformationen an der PBA an.

Installation über die Befehlszeile

- Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

Parameter
CM_EDITION=1 (Remote-Verwaltung)
INSTALLDIR=(Ändern des Installationsziels)
SERVERHOST=(securityserver.organization.com)
SERVERPORT=8888
SECURITYSERVERHOST=(securityserver.organization.com)
SECURITYSERVERPORT=8443
FEATURE=FDE
ENABLE_FDE_LM=1 (ermöglicht die Installation einer vollständigen Datenträgerverschlüsselung auf einem Computer mit aktiver Dell Encryption)

Eine Liste der grundlegenden .msi-Schalter und Anzeigeoptionen, die in Befehlszeilen verwendet werden können, finden Sie unter Installation unter Verwendung der untergeordneten Installationsprogramme.

Beispiel für eine Befehlszeile

Encryption Management Agent

- Im folgenden Beispiel wird Full Disk Encryption remote verwaltet installiert (automatische Installation, kein Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 FEATURE=FDE SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /
norestart /qn"
```

- **Encryption Management Agent**

- Im folgenden Beispiel wird eine remote verwaltete vollständige Datenträgerverschlüsselung installiert und eine Installation auf einem mit Dell Encryption geschützten Computer ermöglicht (automatische Installation, kein Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
  ```

- **Beispiel für eine Befehlszeile zur Installation einer vollständigen Datenträgerverschlüsselung und von Encryption External Media.**

  Verschlüsselung

  Im folgenden Beispiel wird nur Encryption External Media installiert (Installation im Hintergrund, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption.`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Dann:

  Encryption Management Agent

  Im folgenden Beispiel wird eine remote verwaltete vollständige Datenträgerverschlüsselung installiert und eine Installation auf einem mit Dell Encryption geschützten Computer ermöglicht (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
  ```

Encryption auf Serverbetriebssystem installieren

Es gibt zwei Methoden zum Installieren von Encryption auf einem Serverbetriebssystem. Wählen Sie eine der beiden folgenden Methoden aus:

- Encryption auf einem Serverbetriebssystem interaktiv installieren

  Encryption auf Serverbetriebssystemen kann nur interaktiv auf Computern installiert werden, die Serverbetriebssysteme ausführen. Installation auf Computern mit Nicht-Serverbetriebssystemen muss über die Befehlszeile durchgeführt werden, mit dem festgelegten Parameter SERVERMODE=1.

- Encryption auf einem Serverbetriebssystem über die Befehlszeile installieren

Virtuelles Benutzerkonto

- Als Teil der Installation wird ein **virtuelles Serverbenutzerkonto** ausschließlich für die Verwendung von Encryption auf einem Serverbetriebssystem erstellt. Passwort und DPAPI-Authentifizierung werden deaktiviert, sodass nur der virtuelle Serverbenutzer auf Verschlüsselungsschlüssel zugreifen kann.

Vor der Installation

- Bei dem die Installation durchführenden Benutzerkonto muss es sich um einen Domänen-Benutzer mit Berechtigungen auf Administratorebene handeln.
- Um diese Anforderung außer Kraft zu setzen oder um Encryption auf Serverbetriebssystemen auf Servern ohne Domäne oder mit mehreren Domänen auszuführen, setzen Sie die *ssos.domainadmin.verify*-Eigenschaft in der Datei application.properties auf *Falsch*. Die Datei ist in den folgenden Dateipfaden gespeichert, basierend auf dem Dell Server, den Sie verwenden:

  Security Management Server - <*installation dir*>/Security Server/conf/application.properties

  Security Management Server Virtual – /opt/dell/server/security-server/conf/application.properties

- Der Server muss Portsteuerungen unterstützen.

  Die 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 nicht und der Benutzer kann den Computer nicht verwenden, wenn vor dem Anwenden der Richtlinie keine Remote Desktop-Verbindung eingerichtet wurde.

- Für eine erfolgreiche Aktivierung muss der Computer mit dem Netzwerk verbunden sein.
- Wenn das Trusted Platform Module (TPM) verfügbar ist, wird es zum Versiegeln des Allzweckschlüssels auf Dell Hardware verwendet. Wenn kein TPM verfügbar ist, wird die Microsoft Data Protection API (DPAPI) zum Schutz des Allzweckschlüssels verwendet.

  Beim Installieren eines neuen Betriebssystems auf einem Dell Computer mit TPM der Serververschlüsselung ausführt, deaktivieren Sie das TPM im BIOS. Eine Anleitung finden Sie in diesem Artikel.

- Die Installationsprotokolldatei befindet sich im Verzeichnis „%temp%“ des Benutzers unter `C:\Users\<user name>\AppData\Local\Temp`. Um die richtige Protokolldatei ausfindig zu machen, suchen Sie nach einem Dateinamen, der mit MSI beginnt und mit der Erweiterung .log endet. Die Datei enthält einen Datums-/Zeitstempel der Zeit der Ausführung des Installationsprogramms.
- Verschlüsselung wird nicht auf Servern unterstützt, die Teil von verteilten Dateisystemen (DFS) sind.

Extrahieren Sie das untergeordnete Installationsprogramm

- Zum Installieren von Encryption auf einem Serverbetriebssystem müssen Sie zuerst das untergeordnete Installationsprogramm **DDPE_xxbit_setup.exe** aus dem Master-Installationsprogramm extrahieren. Weitere Informationen finden Sie unter Untergeordnete Installer aus dem Master Installer extrahieren.

Interaktiv installieren

- Verwenden Sie diese Anweisungen zur interaktiven Installation von Encryption auf einem Serverbetriebssystem. In diesem Installationsprogramm sind die für die Softwareverschlüsselung erforderlichen Komponenten enthalten.

1. Suchen Sie die Datei **DDPE_XXbit_setup.exe** im Ordner `C:\extracted\Encryption`. Kopieren Sie sie auf den lokalen Computer.
2. Wenn Sie Encryption auf einem Serverbetriebssystem installieren, doppelklicken Sie auf **DDPE_XXbit_setup.exe**, um das Installationsprogramm zu starten.

   ANMERKUNG:

   Wenn Encryption auf einem Serverbetriebssystem auf einem Computer installiert wird, auf dem ein Serverbetriebssystem wie beispielsweise Windows Server 2012 R2 ausgeführt wird, installiert das Installationsprogramm automatisch im SERVERMODUS.

3. Klicken Sie im Begrüßungsdialogfeld auf **Weiter**.
4. Lesen Sie auf dem Lizenzvereinbarungsbildschirm die Lizenzvereinbarung, stimmen Sie den Bedingungen zu, und klicken Sie auf **Weiter**.

5. Wählen Sie *Lokaler Dell Management Server* und klicken Sie auf **Weiter**.

6. Klicken Sie auf **Weiter** für die Installation im Standardverzeichnis.
7. Klicken Sie auf **Weiter**, um das *Verwaltungstyp*-Dialogfeld zu überspringen.
8. Geben Sie im Feld *Security Management Server-Name* den vollständigen qualifizierten Hostnamen des Dell Servers ein, mit dem der Zielbenutzer verwaltet werden soll (z. B. *server.organization.com)* bzw. validieren Sie ihn.

   Geben Sie den Domänennamen in das Feld *Verwaltete Domäne* (z. B. Organisation) ein. Klicken Sie auf **Weiter**.
9. Geben Sie unter Richtlinien-Proxy-Hostname und -Port die Informationen ein bzw. validieren Sie sie und klicken Sie auf **Weiter**.
10. Geben Sie unter Geräte-Server-URL die Informationen ein bzw. validieren Sie sie und klicken Sie auf **Weiter**.
11. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

    Die Installation kann mehrere Minuten dauern.
12. Wenn die Konfiguration abgeschlossen ist, klicken Sie auf **Fertigstellen**.

    Damit ist die Installation abgeschlossen.
13. Starten Sie den Computer neu. Dell empfiehlt das kurzfristige Verschieben des Neustarts nur, wenn Zeit benötigt wird, um Ihre Arbeit zu speichern und Anwendungen zu schließen. Die Verschlüsselung kann erst nach dem Neustart des Computers beginnen.

Über die Befehlszeile installieren

Suchen Sie das Installationsprogramm in `C:\extracted\Encryption`.

- Verwenden Sie die Datei **DDPE_xxbit_setup.exe** für die Installation oder die Aktualisierung. Nutzen Sie dazu eine skriptgesteuerte Installation, Batchdateien oder eine andere in Ihrem Unternehmen verfügbare Push-Technologie.

Schalter

Die folgende Tabelle umfasst die für die Installation verfügbaren Schalter.

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

Schalter	Erläuterung
/a	Administrative Installation
/s	Im Hintergrund

Parameter

Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

Komponente	Protokolldatei	Befehlszeilenparameter
Alle	/l*v [vollständiger Pfad] [Dateiname].log *	SERVERHOSTNAME=<Security Management Server Name>
		SERVERMODE=1
		POLICYPROXYHOSTNAME=<RGK Name>
		MANAGEDDOMAIN=<My Domain>
		DEVICESERVERURL=<Activation Server Name>
		GKPORT=<New GK Port>
		MACHINEID=<Machine Name>
		RECOVERYID=<Recovery ID>
		REBOOT=ReallySuppress
		HIDEOVERLAYICONS=1
		HIDESYSTRAYICON=1
		EME=1

ANMERKUNG:

Der Neustart kann zwar unterbunden werden, ist jedoch letztendlich erforderlich. Die Verschlüsselung kann erst nach dem Neustart des Computers beginnen.

Optionen

Die folgende Tabelle umfasst die Anzeigeoptionen, die am Ende des Arguments, das an den /v-Schalter weitergegeben wird, festgelegt werden können.

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

Option	Erläuterung
ANMERKUNG: Verwenden Sie **/q** und **/qn** nicht in derselben Befehlszeile. Verwenden Sie nur **!** und - nach **/qb**.	

- Der Befehlszeilenparameter SERVERMODE=1 wird nur während neuer Installationen berücksichtigt. Der Parameter wird bei Deinstallationen ignoriert.
- Geben Sie einen Wert ein, der eines oder mehrere Sonderzeichen, z. B. eine Leerstelle, zwischen in Escape-Zeichen gesetzten Anführungszeichen enthält.
- Der Parameter DEVICESERVERURL unterscheidet zwischen Groß- und Kleinschreibung.

Beispiel einer Installation über die Befehlszeile

- Im folgenden Beispiel wird Encryption im Serverbetriebssystemmodus mit den Standardparametern installiert (Encryption, automatische Installation, „Für Freigabe verschlüsseln“, kein Dialog, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis von `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  MSI-Befehl:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn
  REBOOT="ReallySuppress" SERVERMODE="1" SERVERHOSTNAME="server.organization.com"
  POLICYPROXYHOSTNAME="rgk.organization.com" MANAGEDDOMAIN="ORGANIZATION"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- Das folgende Beispiel installiert Encryption im Serverbetriebssystemmodus mit einer Protokolldatei und Standardparametern (Encryption, automatische Installation, „Für Freigabe verschlüsseln“, kein Dialog, keine Fortschrittsleiste, kein Neustart, Installation im Standardverzeichnis von `C:\Program Files\Dell\Dell Data Protection\Encryption`) und gibt einen benutzerdefinierten Protokolldateinamen an, der mit einer Zahl endet (DDP_ssos-090.log), die erhöht wird, wenn die Befehlszeile mehr als einmal auf demselben Server ausgeführt wird. Wenn Sie das Protokoll nicht im Standardverzeichnis mit der ausführbaren Datei speichern möchten, geben Sie den vollständigen neuen Speicherpfad im Befehl an. Beispiel: Mit dem Befehl /l*v C:\Logs\DDP_ssos-090.log werden Protokolle in C:\Logs erstellt.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /l*v DDP_ssos-090.log /
  norestart/qn"
  ```

  MSI-Befehl:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn SERVERMODE="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/
  xapi/" /l*v DDP_ssos-090.log /norestart/qn"
  ```

Starten Sie den Computer nach der Installation neu. Dell empfiehlt das kurzfristige Verschieben des Neustarts nur, wenn Zeit benötigt wird, um Ihre Arbeit zu speichern und Anwendungen zu schließen. Die Verschlüsselung kann erst nach dem Neustart des Computers beginnen.

Aktivieren

- Stellen Sie sicher, dass es sich beim Computernamen des Servers um den Endpunktnamen handelt, der in der Verwaltungskonsole angezeigt werden soll.
- Ein interaktiver Benutzer mit Domänenadministrator-Anmeldeinformationen muss sich für die Erstaktivierung mindestens einmal auf dem Server anmelden. Der angemeldete Benutzertyp kann ein Domänen- oder Nicht-Domänen-Benutzer, über eine Remote-Desktop-Verbindung verbunden oder ein interaktiver Benutzer am Server sein, aber die Aktivierung erfordert Domänen-Administrator-Anmeldeinformationen.
- Nach dem Neustart nach der Installation wird der Aktivierungsdialog angezeigt. Der Administrator muss die Domänen-Administrator-Anmeldeinformationen mit einem Benutzernamen im Format User Principal Name (UPN, Benutzerprinzipalnamen) eingeben. Encryption wird auf Serverbetriebssystemen nicht automatisch aktiviert.
- Bei der Erstaktivierung wird ein virtuelles Serverbenutzerkonto erstellt. Nach der Erstaktivierung wird der Computer neu gestartet, sodass die Geräteaktivierung beginnen kann.

- Während der Authentifizierungs- und Geräteaktivierungsphase wird dem Computer eine eindeutige Computer-ID zugewiesen, Verschlüsselungsschlüssel werden erstellt und gebündelt und eine Beziehung zwischen dem Verschlüsselungsschlüsselpaket und dem virtuellen Serverbenutzer wird hergestellt. Das Verschlüsselungsschlüsselpaket verknüpft die Verschlüsselungsschlüssel und Richtlinien mit dem neuen virtuellen Serverbenutzer, um eine untrennbare Beziehung zwischen den verschlüsselten Daten, dem spezifischen Computer und dem virtuellen Serverbenutzer zu erstellen. Nach der Geräteaktivierung wird der virtuelle Serverbenutzer in der Verwaltungskonsole als SERVER-USER@<*fully qualified server name*> angezeigt. Weitere Informationen zur Aktivierung finden Sie unter Aktivierung auf einem Serverbetriebssystem.

ANMERKUNG:

Wenn Sie den Server nach der Aktivierung umbenennen, ändert sich sein Anzeigename in der Verwaltungskonsole nicht. Wenn jedoch Encryption auf Serverbetriebssystemen nach der Änderung des Servernamens erneut aktiviert wird, erscheint der neue Servername in der Verwaltungskonsole.

Bei jedem Neustart wird ein Aktivierungsdialog angezeigt, mit dem der Benutzer zur Aktivierung von Encryption auf einem Serverbetriebssystem aufgefordert wird. Zum Abschluss der Aktivierung gehen Sie wie folgt vor:

1. Melden Sie sich entweder am Server oder über die Remote-Desktop-Verbindung auf dem Server an.
2. Geben Sie den Benutzernamen eines Domänenadministrators im UPN-Format ein sowie ein Kennwort und klicken Sie auf **Aktivieren**. Hierbei handelt es sich um den gleichen Aktivierungsdialog, der auch bei jedem Neustart eines nicht aktivierten Systems angezeigt wird.

   Der Dell Server stellt einen Verschlüsselungsschlüssel für die Computer-ID aus, erstellt das **virtuelle Serverbenutzerkonto**, erstellt einen Verschlüsselungsschlüssel für das Benutzerkonto, bündelt die Verschlüsselungsschlüssel und erstellt die Beziehung zwischen dem Verschlüsselungspaket und dem virtuellen Serverbenutzerkonto.
3. Klicken Sie auf **Schließen**.

   Nach der Aktivierung beginnt die Verschlüsselung.
4. Nachdem die Verschlüsselungssuche abgeschlossen wurde, starten Sie den Computer neu, um Dateien, die zuvor verwendet wurden, zu verarbeiten. Dies ist ein wichtiger Schritt, der der Sicherheit dient.

   ANMERKUNG:

   Wenn die Richtlinie *Sichere Windows-Anmeldeinformationen* aktiviert wird, verschlüsselt Encryption auf Serverbetriebssystemen die `\Windows\system32\config`-Dateien einschließlich der Windows-Anmeldeinformationen. Die Dateien in `\Windows\system32\config` werden auch dann verschlüsselt, wenn die Richtlinie *SDE-Verschlüsselung aktiviert* deaktiviert ist. Standardmäßig ist die Richtlinie *Sichere Windows-Anmeldeinformationen* ausgewählt.

   ANMERKUNG:

   Nach dem Computerneustart ist für die Authentifizierung des allgemeinen Verschlüsselungsschlüssels *immer* der Computerschlüssel des geschützten Servers erforderlich. Der Dell Server gibt einen Entschlüsselungsschlüssel für den Zugriff auf die Verschlüsselungsschlüssel und Richtlinien im Vault zurück. (Die Schlüssel und Richtlinien sind für den Server und nicht den Benutzer bestimmt.) Ohne den Computerschlüssel des Servers kann der allgemeine Verschlüsselungsschlüssel nicht entsperrt werden und der Computer kann keine Richtlinienaktualisierungen beziehen.

Aktivierung bestätigen

Öffnen Sie von der lokalen Konsole aus den **Info**-Dialog, um zu bestätigen, dass Encryption auf Serverbetriebssystemen installiert und authentifiziert wurde und sich im Servermodus befindet. Wenn die Encryption-Client-ID **rot** ist, wurde die Verschlüsselung noch nicht aktiviert.

Virtueller Serverbenutzer

- In der Verwaltungskonsole finden Sie einen geschützten Server unter seinem Computernamen. Darüber hinaus verfügt jeder geschützte Server über sein eigenes virtuelles Serverbenutzerkonto. Jedes Konto hat einen eindeutigen statischen Benutzernamen und einen eindeutigen Computernamen.
- Das virtuelle Serverbenutzerkonto wird ausschließlich von Encryption auf Serverbetriebssystemen verwendet und ist ansonsten für den Betrieb des geschützten Servers transparent. Der virtuelle Serverbenutzer wird mit dem Verschlüsselungsschlüsselpaket und dem Richtlinien-Proxy verknüpft.
- Nach der Aktivierung ist das virtuelle Serverbenutzerkonto das Benutzerkonto, das aktiviert und dem Server zugeordnet ist.

- Nach Aktivierung des virtuellen Serverbenutzerkontos werden alle zukünftigen Serveranmelde- und -abmeldebenachrichtigungen ignoriert. Stattdessen authentifiziert der Computer den virtuellen Serverbenutzer automatisch während des Hochfahrens und lädt anschließend den Computerschlüssel vom Dell Server herunter.

Advanced Threat Prevention-Client installieren

- **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.

  ANMERKUNG: Vor der Installation von Advanced Threat Prevention müssen die Zielordner für die Installation und die Protokolle vorhanden sein.

- Die Installationsprogramme müssen in einer bestimmten Reihenfolge ausgeführt werden. Werden die Komponenten in der falschen Reihenfolge installiert, kommt es zu einer fehlerhaften Installation. Führen Sie die Installationsprogramme in der folgenden Reihenfolge aus:

1. **(Nur auf einem Workstation-Betriebssystem)** \Encryption Management Agent – Advanced Threat Prevention erfordert den Encryption Management Agent.

   (Nur auf einem Serverbetriebssystem) Komponente Dell Encryption Management Agent, wie in Installation über die Befehlszeile gezeigt.

2. Advanced Threat Prevention-Client, gemäß Beschreibung unter Installation über die Befehlszeile.
3. Advanced Threat Prevention-Plug-in, gemäß Beschreibung unter Installation über die Befehlszeile.

- Das Advanced Threat Prevention-Client-Installationsprogramm befindet sich unter:
  - **Über Ihr Dell-FTP-Konto** – Suchen Sie das Installationspaket in der Datei „Endpoint-Security-Suite-Ent-2.x.x.xxx.zip“, und extrahieren Sie dann die untergeordneten Installationsprogramme aus dem Master-Installationsprogramm. Nach dem Extrahieren finden Sie die Datei unter `C:\extracted\Advanced Threat Prevention\WinXXR\` und `C:\extracted\Advanced Threat Prevention\WinNtAll\`.
- Das Encryption Management Agent-Installationsprogramm kann wie folgt bezogen werden:
  - **Über Ihr Dell-FTP-Konto** – Suchen Sie das Installationspaket in der Datei „Endpoint-Security-Suite-Ent-2.x.x.xxx.zip“, und extrahieren Sie dann die untergeordneten Installationsprogramme aus dem Master-Installationsprogramm. Nach dem Extrahieren finden Sie die Datei unter `C:\extracted\Encryption Management Agent`.

Installation über die Befehlszeile

- Für die Installation sind MSI-Basisbefehle verfügbar.
- Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

Parameter
CM_EDITION=1 <Remote Management>
INSTALLDIR=<change the installation destination>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>
REBOOT=ReallySuppress <suppresses the reboot>

Parameter
FEATURE=BASIC <***erforderlich*** auf einem Server-Betriebssystem; kann auch (optional) auf einem Workstation-Betriebssystem verwendet werden; verhindert SED-Verwaltung und BitLocker Manager Installation>

Eine Liste der grundlegenden .msi-Schalter und Anzeigeoptionen, die in Befehlszeilen verwendet werden können, finden Sie unter Installation unter Verwendung der untergeordneten Installationsprogramme.

Beispiel für eine Befehlszeilen

- Im folgenden Beispiel wird der grundlegende Encryption Management Agent ohne SED-Verwaltung oder BitLocker Manager installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"FEATURE=BASIC
  CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- Im folgenden Beispiel wird Advanced Threat Prevention installiert (automatische Installation, kein Neustart, Installationsprotokolldatei und Installationsordner in den angegebenen Speicherorten).

  ```
  MSIEXEC.EXE /I "ATP_CSF_Plugins_x64.msi" /qn REBOOT="ReallySuppress" APPFOLDER="C:
  \Program Files\Dell\Dell Data Protection\Advanced Threat Prevention\Plugins"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\ATP_Plugins_x64.msi.log"
  ```

  und

  ```
  "\Advanced Threat Prevention\WinNtAll\ATP_AgentSetup.exe" /s EXTRACT_INSTALLERS /v"/qb!"
  ```

ANMERKUNG: Diese Komponenten dürfen nur über die Befehlszeile installiert werden. Wenn Sie doppelklicken, um diese Komponente zu installieren, wird eine Dell-fremde, nicht verwaltete Version des Produkts installiert, die nicht unterstützt wird. Wenn dies versehentlich erfolgte, gehen Sie zu „Programme hinzufügen/entfernen“, und deinstallieren Sie diese Version.

Beispielskript

Im folgenden Beispiel wird Advanced Threat Prevention ohne SED-Verwaltung oder BitLocker Manager installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

:: Installation von Encryption Management Agent

".\Encryption Management Agent\EMAgent_64bit_setup.exe" /s /v" FEATURE=BASIC CM_EDITION=1 SERVERHOST=%SERVER% SERVERPORT=8888 SECURITYSERVERHOST=%SERVER% SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /norestart /qn"

:: Installation von ATP-Plugins

MSIEXEC.EXE /I "Advanced Threat Prevention\Win64R\ATP_CSF_Plugins_x64.msi" /qn REBOOT=ReallySuppress APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Prevention\Plugins" ARPSYSTEMCOMPONENT=1 /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\ATP_CSF_Plugins_x64.msi.log"

:: Installation von Advanced Threat Prevention

".\Advanced Threat Prevention\WinNtAll\ATP_AgentSetup.exe" /s EXTRACT_INSTALLERS /v"/qb!"

Installieren von Client Firewall und Web Protection

- Überprüfen Sie vor der Installation die Client Firewall und Web Protection Anforderungen.
- **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.

  ANMERKUNG: Der Encryption Management Agent **muss** vor der Installation von Client Firewall und Web Protection installiert werden.

  ANMERKUNG: Ausgabeverzeichnisse **müssen** vorhanden sein, bevor Sie die folgenden Befehle ausführen.

- Die Installationsprogramme müssen in einer bestimmten Reihenfolge ausgeführt werden. Werden die Komponenten in der falschen Reihenfolge installiert, kommt es zu einer fehlerhaften Installation. Führen Sie die Installationsprogramme in absteigender Reihenfolge in Installation über die Befehlszeile durch.

  Befehle von untergeordneten Installationsprogrammen **müssen** aus ihren extrahierten Verzeichnissen ausgeführt werden oder es treten Fehler auf.

Installation über die Befehlszeile

- Die folgende Tabelle enthält die für die Datei **`EnsMgmtSdkInstaller.exe`** erforderlichen Parameter.

Parameter	Beschreibung
LoadCert	Lädt das Zertifikat am angegebenen Verzeichnis.
InstallSDK	Installiert den SDK am angegebenen Speicherort.
RemoveRightClick	Entfernt die Rechtsklickoption für Benutzer.
RemoveMcTray	Entfernt den Infobereich.

- Die folgende Tabelle listet die für die Datei **`EPsetup.exe`** erforderlichen Parameter auf.

Parameter	Beschreibung
ADDLOCAL="fw,wc"	Identifiziert die zu installierenden Module: fw=Client-Firewall wc=Web-Schutz
„HIPS“ überschreiben	Installation von Host Intrusion Prevention nicht durchführen.
INSTALLDIR	Kein standardmäßiges Installationsverzeichnis.
nocontentupdate	Weist das Installationsprogramm an, die Inhaltsdateien im Rahmen der Installation nicht automatisch zu aktualisieren. Dell empfiehlt, umgehend nach der Installation eine Aktualisierung einzuplanen.
nopreservesettings	Keine Einstellungen speichern.

- Die folgende Tabelle enthält die für die Datei **`DellThreatProtection.msi`** erforderlichen Parameter.

Parameter	Beschreibung
Reboot=ReallySuppress	Neustart wird unterdrückt.
ARP	0 = Kein Eintrag unter Programme hinzufügen/entfernen 1 = Eintrag unter Programme hinzufügen/entfernen

Zum Installieren oder Aktualisieren verwenden Sie den folgenden Workflow:

- **Beispiel für eine Befehlszeile**

  \Threat Protection\EndPointSecurity

  Im folgenden Beispiel werden Web Protection und Client Firewall mit Standard-Parametern (Hintergrundmodus, Installation von Client Firewall und Web Protection, Überschreiben der Host Intrusion Prevention, keine Inhaltsaktualisierung, keine Speicherung der Einstellungen unter C:\ProgramData\Dell\Dell Data Protection) installiert.

  ```
  ".\Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /
  nocontentupdate /qb! /L*v"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\"
  ```

  Dann:

\Threat Protection\ThreatProtection\WinXXR

- Im folgenden Beispiel wird der Client mit den Standard-Parametern installiert (Unterdrückung des Neustarts, keine Dialogfelder, keine Fortschrittsleiste, kein Eintrag in die Liste der Programme in der Systemsteuerung).

  ```
  "Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi" /qn
  REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
  ```

  Dann:

  \Threat Protection\SDK

- Durch den folgenden Befehl werden die Standardparameter für das Zertifikat geladen.

  ```
  "Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -LoadCert >"C:\ProgramData\Dell\Dell Data
  Protection\Installer Logs\McAfeeSDKInstallerBeforeEndPoint.log"
  ```

  Dann:

  \Threat Protection\SDK

- Im folgenden Beispiel wird der SDK deinstalliert.

  ```
  "Threat Protection\SDK\EnsMgmtSDKInstaller.exe" -InstallSDK -RemoveRightClick
  -RemoveMcTray >> "<OUTPUTDIRECTORY>\McAfeeSDKInstallerAfterEndPoint.log"
  ```

SED Manager und PBA Advanced Authentication installieren

- Überprüfen Sie die SED-Anforderungen, wenn Ihr Unternehmen ein Zertifikat verwendet, das von einer Stammstelle, wie z. B. EnTrust oder Verisign, signiert wurde. Zur Aktivierung der SSL/TLS-Vertrauensprüfung muss eine Registrierungseinstellung auf dem Client-Computer geändert werden.
- Benutzer melden sich mit ihren Windows-Anmeldeinformationen an der PBA an.
- Die Installationsprogramme für SED Manager und PBA Advanced Authentication befinden sich unter:
  - **Über Ihr Dell FTP-Konto** – Suchen Sie das Installationspaket in der Datei Endpoint-Security-Suite-Ent-2.x.x.xxx.zip und extrahieren Sie dann die untergeordneten Installationsprogramme aus dem Master-Installationsprogramm. Nach dem Extrahieren finden Sie die Datei unter `C:\extracted\Encryption Management Agent`.

Installation über die Befehlszeile

- Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

Parameter
CM_EDITION=1 <Remote Management>
INSTALLDIR=<change the installation destination>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Eine Liste der grundlegenden .msi-Schalter und Anzeigeoptionen, die in Befehlszeilen verwendet werden können, finden Sie unter Installation unter Verwendung der untergeordneten Installationsprogramme.

Die folgenden Beispielbefehle installieren oder aktualisieren den Encryption Management Agent.

Beispiel für eine Befehlszeile

\Encryption Management Agent

- Im folgenden Beispiel werden SED Manager, der Encryption Management Agent und die lokale Sicherheitskonsole über Remoteverwaltung installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

BitLocker Manager installieren

- **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.

- Überprüfen Sie Anforderungen für den BitLocker Manager-Client, wenn Ihr Unternehmen ein Zertifikat verwendet, das von einer Stammstelle, wie z. B. EnTrust oder Verisign, signiert wurde. Zur Aktivierung der SSL/TLS-Vertrauensprüfung muss eine Registrierungseinstellung auf dem Client-Computer geändert werden.
- Die BitLocker Manager-Installationsprogramme können wie folgt bezogen werden:
  - **Über Ihr Dell FTP-Konto** – Suchen Sie das Installationspaket in der Datei Endpoint-Security-Suite-Ent-2.x.x.xxx.zip und extrahieren Sie dann die untergeordneten Installationsprogramme aus dem Master-Installationsprogramm. Nach dem Extrahieren finden Sie die Datei unter `C:\extracted\Encryption Management Agent`.

Installation über die Befehlszeile

- Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

Parameter
CM_EDITION=1 <Remote Management>
INSTALLDIR=<change the installation destination>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
FEATURE=BLM <install BitLocker Manager only>
FEATURE=BLM,SED <install BitLocker Manager with SED>
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Eine Liste der grundlegenden .msi-Schalter und Anzeigeoptionen, die in Befehlszeilen verwendet werden können, finden Sie unter Installation unter Verwendung der untergeordneten Installationsprogramme.

Beispiel für eine Befehlszeile

- Im folgenden Beispiel wird nur BitLocker Manager installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
FEATURE=BLM /norestart /qn"
```

- Im folgenden Beispiel wird BitLocker Manager mit SED installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM,SED /norestart /qn"
  ```

- **Beispiel für eine Befehlszeile für die Installation von BitLocker Manager und Dell Encryption**

  Im folgenden Beispiel wird nur BitLocker Manager installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  Dann:

  Im folgenden Beispiel wird der Client mit den Standardparametern installiert (Encryption-Client, für Freigabe verschlüsseln, kein Dialogfeld, keine Statusanzeige, automatischer Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

7

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 Endpoint Security Suite EnterpriseMaster-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

Option	Erläuterung
/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

Web Protection und Firewall deinstallieren

Wenn Web Protection und Firewall nicht installiert sind, fahren Sie mit Encryption Client deinstallieren fort.

Deinstallation über die Befehlszeile

- Nach der Extraktion aus dem Endpoint Security Suite Enterprise-Master-Installationsprogramm befindet sich das Web Protection und Firewall-Client-Installationsprogramm unter `C:\extracted\Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi`.
- Wechseln Sie in den Bereich „Programme hinzufügen/entfernen“ der Systemsteuerung, und deinstallieren Sie die folgenden Komponenten in der angegebenen Reihenfolge.
  - McAfee Endpoint Security Firewall
  - McAfee Endpoint Security Web Control
  - McAfee Agent
- Dann:
- Im folgenden Beispiel werden Web Protection und Firewall deinstalliert.

```
MSIEXEC.EXE /x "DellThreatProtection.msi"
```

Advanced Threat Prevention deinstallieren

Deinstallation über die Befehlszeile

- Im folgenden Beispiel wird der Advanced Threat Prevention-Client deinstalliert. ***Dieser Befehl muss von einer administrativen Eingabeaufforderung ausgeführt werden.***

  ```
  wmic path win32_product WHERE (CAPTION LIKE "%%CYLANCE%%") call uninstall
  ```

  Fahren Sie den Computer herunter und starten Sie ihn anschließend neu. Deinstallieren Sie daraufhin die Komponente Dell Encryption Management Agent.

- **ANMERKUNG:** Wenn Sie den SED-Client installiert haben oder die Preboot-Authentifizierung aktiviert haben, folgen Sie den Deinstallationsanweisungen unter SED-Client deinstallieren.

  Im folgenden Beispiel wird nur die Komponente Dell Encryption Management Agent deinstalliert, nicht aber der SED-Client.

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

Full Disk Encryption 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 Schlüssel für Full Disc Encryption entsperrt.
- Full Disk Encryption deinstallieren

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 **Full Disk Encryption** aus der Gruppe **Windows Encryption** aus.
9. Ändern Sie **Full Disk Encryption** und die Richtlinie 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 Full Disk Encryption und PBA Advanced Authentication nach der Deaktivierung von PBA.

Installieren des Clients für Full Disk Encryption

Deinstallation über die Befehlszeile

- Nach der Extraktion aus dem Master-Installationsprogramm befindet sich Full Disk Encryption unter `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
  - Im folgenden Beispiel wird Full Disk Encryption 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.

SED Manager 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 SED Manager.

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 SED Manager und PBA Advanced Authentication nach der Deaktivierung von PBA.

SED-Client deinstallieren

Deinstallation über die Befehlszeile

- Nach der Extraktion aus dem Master-Installationsprogramm befindet sich das Installationsprogramm für SED Manager unter `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
  - Im folgenden Beispiel wird SED Manager 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.

Encryption und Encryption auf einem Serverbetriebssystem 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.
- Encryption und Encryption External Media aktualisieren den Dell Server durch Ändern des Status zu *Ungeschützt* zu Beginn eines 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 verwalteten Berichten erwartungsgemäß der Status *Ungeschützt* erscheint.

Verfahren

- **Vor der Deinstallation** finden Sie weitere Informationen unter (Optional) Encryption Removal Agent-Protokolldatei anlegen. Diese Protokolldatei erleichtert das Troubleshooting, die unter Umständen beim Deinstallieren/Entschlüsseln auftreten. Falls Sie Dateien während der Deinstallation nicht entschlüsseln möchten, müssen Sie keine Encryption Removal Agent-Protokolldatei anlegen.

- 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.
- Führen nach Abschluss der Deinstallation aber vor dem Neustart des Computers WSScan aus, um sicherzustellen, dass alle Daten entschlüsselt wurden. Siehe WSScan verwenden, um Anweisungen zu erhalten.
- Führen Sie gelegentlich Überprüfen des Encryption-Removal-Agent-Status durch. Die Datenentschlüsselung läuft noch, falls der Encryption Removal Agent-Dienst weiterhin im Dialogfeld „Dienste“ angezeigt wird.

Deinstallation über die Befehlszeile

- Sobald es aus dem Endpoint Security Suite EnterpriseMaster-Installationsprogramm extrahiert wurde, befindet sich das Encryption-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 – Leise: erforderlich bei msiexec-Variablen, die /q oder /qn enthalten. 0 – nicht leise: nur möglich, wenn msiexec-Variablen mit /q nicht in der Befehlszeilensyntax vorhanden sind
Erforderliche Eigenschaften	
DA_KM_PATH	Geben Sie den vollständig qualifizierten Pfad zum Keybundle an.
DA_KM_PW	Das auf dem Keybundle festgelegte Kennwort.
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 Nutzer muss in der Key Server-Liste des Security Management Server enthalten sein.

Parameter	Auswahl
DA_RUNASPWD	Kennwort für den RUNAS-Nutzer.
FORENSIC_ADMIN	Das forensische Administratorkonto auf dem Dell Server, das für forensische Anfragen für Deinstallationen oder Schlüssel verwendet werden kann.
FORENSIC_ADMIN_PWD	Das Kennwort für das Konto des Typs „Forensischer Administrator“.
Optionale Eigenschaften	
SVCLOGONUN	Benutzername im UPN-Format zur Anmeldung beim Encryption Removal Agent-Dienst als Parameter.
SVCLOGONPWD	Kennwort für die Anmeldung als Nutzer.

- Im folgenden Beispiel werden im Hintergrund Encryption 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 Encryption 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.

- Im folgenden Beispiel wird Encryption im Hintergrund mithilfe vorab heruntergeladener Schlüssel unter C:\Users\administrator\Desktop\Admin\ mit dem forensischen Administratorkennwort deinstalliert und Protokolle in C:\SheildUninstall geschrieben.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENT=1 DA_KM_PATH=C:
  \Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v c:
  \ShieldUninstall.log /qn /norestart"
  ```

  MSI-Befehl

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" CMG_DECRYPT=2 CMGSILENT=1
  DA_KM_PATH=C:\Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v
  c:\ShieldUninstall.log /qn /norestart
  ```

ANMERKUNG:

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 Kennwort.
3. Nach Abschluss der Deinstallation im Hintergrund entfernen Sie das temporäre Konto dann aus der Liste der Administratoren oder ändern das entsprechende Kennwort.

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"
```

BitLocker Manager deinstallieren

Deinstallation über die Befehlszeile

- Sobald es aus dem Endpoint Security Suite EnterpriseMaster-Installationsprogramm extrahiert wurde, befindet sich das BitLocker Manager-Installationsprogramm unter `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- Im folgenden Beispiel wird BitLocker Manager im Hintergrund deinstalliert.

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

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

8

Data Security-Deinstallationsprogramm

Deinstallieren von Endpoint Security Suite Enterprise

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

ANMERKUNG: Bei der Deinstallation von FDE empfiehlt Dell einen Neustart des Computers nach Abschluss der Deaktivierung von FDE, um Probleme mit dem Ruhezustand des Computers zu verhindern.

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

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

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

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

Klicken Sie auf **Weiter**.

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

Erforderliche Abhängigkeiten werden automatisch ausgewählt oder gelöscht.

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

Wählen Sie **Encryption Removal Agent – Schlüssel 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.

9

Gängige Szenarien

- Um jeden Client einzeln zu installieren, müssen die untergeordneten ausführbaren Dateien zuerst aus dem Endpoint Security Suite EnterpriseMaster-Installationsprogramm extrahiert werden, wie unter Extrahieren der untergeordneten Installationsprogramme aus dem Master-Installationsprogramm erläutert.
- Die Komponente für das untergeordnete Installationsprogramm für Advanced Threat Prevention darf nur über die Befehlszeile installiert werden. Wenn Sie doppelklicken, um diese Komponente zu installieren, wird eine Dell-fremde, nicht verwaltete Version des Produkts installiert, die nicht unterstützt wird. Wenn dies versehentlich erfolgte, gehen Sie zu „Programme hinzufügen/entfernen“, und deinstallieren Sie diese Version.
- Bei den Befehlszeilenschaltern und -parametern ist die Groß- und Kleinschreibung zu beachten.
- Stellen Sie sicher, dass Werte, die ein oder mehrere Sonderzeichen enthalten, z. B. eine Leerstelle in der Befehlszeile, zwischen in Escape-Zeichen gesetzte Anführungszeichen gesetzt werden.
- Verwenden Sie diese Installationsprogramme zur Installation der Clients. Nutzen Sie dazu eine skriptgesteuerte Installation, Batchdateien oder eine andere verfügbare Push-Technologie.
- Der Neustart wurde in den Befehlszeilenbeispielen unterdrückt. Es ist jedoch ein abschließender Neustart erforderlich. Die Verschlüsselung kann erst nach dem Neustart des Computers beginnen.
- Protokolldateien – Windows erstellt eindeutige Installationsprotokolldateien des untergeordneten Installationsprogramms für den angemeldeten Benutzers unter „%Temp%“ mit dem folgenden Verzeichnispfad `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. Der Standard-MSI-Befehl kann dazu verwendet werden, um eine Protokolldatei durch die Verwendung von `/l*v C:\<any directory>\<any log file name>.log` zu erstellen.

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

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

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

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

Option	Erläuterung
/qn	Keine Benutzeroberfläche

- 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 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. Sie können über den folgenden Pfad auf die Hilfe zugreifen: `<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS`
  - Siehe *Endpoint Security Suite Enterprise-Hilfe* für weitere Informationen zur Verwendung der Funktionen von Advanced Threat Prevention. Hier können Sie auf die Hilfe zugreifen: `<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Prevention\Help`.

Encryption Client und Advanced Threat Prevention

- Im folgenden Beispiel werden die SED-Verwaltung und der Encryption Management Agent installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`). Diese Komponente installiert den Encryption Management Agent, der von Advanced Threat Prevention benötigt wird.

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Dann:

  Dann:

- Im folgenden Beispiel wird Advanced Threat Prevention installiert (automatische Installation, kein Neustart, Installationsprotokolldatei und Installationsordner in den angegebenen Speicherorten).

  ```
  MSIEXEC.EXE /I "ATP_CSF_Plugins_x64.msi" /qn REBOOT="ReallySuppress" APPFOLDER="C:
  \Program Files\Dell\Dell Data Protection\Advanced Threat Prevention\Plugins"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\AdvancedThreatProtectionPlugins.msi.log"
  ```

  und

  ```
  ATP_AgentSetup.exe" /s EXTRACT_INSTALLERS /v"/qb!"
  ```

- Im folgenden Beispiel wird Encryption mit den standardmäßigen Parametern installiert (Encryption und Für Freigabe verschlüsseln, keine Dialogfelder, keine Statusanzeige, kein Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
  ```

- In den folgenden Beispielen werden die ***optionalen*** Funktionen, Web Protection und Firewall, installiert.
- **\Threat Protection\SDK**

  Durch den folgenden Befehl werden die Standardparameter für das Zertifikat geladen.

  ```
  EnsMgmtSdkInstaller.exe -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\McAfeeSDKInstallerBeforeEndPoint.log"
  ```

  ANMERKUNG:

  Bei einem Upgrade kann dieses Installationsprogramm nicht übersprungen werden.

  Dann:

  \Threat Protection\EndPointSecurity

- Im folgenden Beispiel werden die *optionalen* Funktionen Web Protection und Firewall mit Standard-Parametern (Hintergrundmodus, Installation von Threat Protection, Client Firewall und Web Protection, Überschreiben der Host Intrusion Prevention, keine Inhaltsaktualisierung, keine Speicherung der Einstellungen) installiert.

```
"Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /
nocontentupdate /nopreservesettings /qn
```

Dann:

\Threat Protection\ThreatProtection\WinXXR

- Im folgenden Beispiel wird der Client mit den Standard-Parametern installiert (Unterdrückung des Neustarts, keine Dialogfelder, keine Fortschrittsleiste, kein Eintrag in die Liste der Programme in der Systemsteuerung).

  ```
  "DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
  ```

  \Threat Protection\SDK

- Im folgenden Beispiel wird der SDK deinstalliert.

  ```
  EnsMgmtSdkInstaller.exe "C:\Program Files\Dell\Dell Data
  Protection\Threat Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick
  -RemoveMcTray >"C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\McAfeeSDKInstallerAfterEndPoint.log"
  ```

SED Manager und Encryption External Media

- Im folgenden Beispiel werden der SED Manager, der Encryption Management Agent und die lokale Sicherheitskonsole installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Dann:

- Im folgenden Beispiel wird nur Encryption External Media installiert (automatische Installation, kein Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

BitLocker Manager und Encryption External Media

- BitLocker Manager und Encryption External Media interagieren basierend auf einer Verschlüsselungssequenz. Wenn ein mit BitLocker Manager verschlüsseltes Laufwerk in einen Computer mit Encryption External Media eingesetzt wird, **muss** das Kennwort von BitLocker Manager eingegeben werden, bevor Encryption External Media das Laufwerk verschlüsseln und lesen kann.
- Wenn Encryption External Media auf einem Laufwerk aktiv ist, kann die BitLocker Manager-Verschlüsselung auf das gleiche Laufwerk angewendet werden.
- Im folgenden Beispiel wird BitLocker Manager installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  Dann:

- Im folgenden Beispiel wird nur Encryption External Media installiert (automatische Installation, kein Neustart, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

BitLocker Manager und Advanced Threat Prevention

- Im folgenden Beispiel wird BitLocker Manager installiert (automatische Installation, kein Neustart, kein Eintrag in der Liste der Programme in der Systemsteuerung, Installation im Standardverzeichnis `C:\Program Files\Dell\Dell Data Protection`). Diese Komponente installiert den Encryption Management Agent, der von Advanced Threat Prevention benötigt wird.

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  Dann:

- Im folgenden Beispiel wird Advanced Threat Prevention installiert (automatische Installation, kein Neustart, Installationsprotokolldatei und Installationsordner in den angegebenen Speicherorten).

  ```
  MSIEXEC.EXE /I "ATP_CSF_Plugins_x64.msi" /qn REBOOT="ReallySuppress"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\ATP.log" APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat
  Prevention"
  ```

  und

  ```
  "\Advanced Threat Prevention\WinNtAll\ATP_AgentSetup.exe" /s EXTRACT_INSTALLERS /v"/qb!"
  ```

10

Bereitstellung eines Mandanten

Ein Tenant muss im Dell Server bereitgestellt werden, bevor die Durchsetzung von Advanced Threat Prevention-Richtlinien aktiv wird.

Voraussetzungen

- Muss durch einen Administrator mit der Systemadministratorrolle durchgeführt werden.
- Muss über eine Verbindung mit dem Internet verfügen, um auf dem Dell Server bereitgestellt zu werden.
- Muss über eine Verbindung mit dem Internet auf dem Client verfügen, um die Online-Dienst-Integration von Advanced Threat Prevention in der Verwaltungskonsole anzuzeigen.
- Die Bereitstellung basiert auf einem Token, das im Rahmen der Bereitstellung aus einem Zertifikat generiert wird.
- Die Lizenzen für Advanced Threat Prevention müssen auf dem Dell Server vorhanden sein.

Bereitstellung eines Mandanten

1. Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.
2. Klicken Sie im linken Bereich der Verwaltungskonsole auf Verwaltung > Servicemanagement.
3. Klicken Sie auf **Advanced Threat Protection-Dienst einrichten**. Importieren Sie Ihre Advanced Threat Prevention Lizenzen, wenn zu diesem Zeitpunkt ein Fehler auftritt.
4. Die geführte Einrichtung beginnt, sobald die Lizenzen importiert wurden. Klicken Sie zum Starten auf **Weiter**.
5. Lesen Sie die EULA, stimmen Sie ihr zu und klicken Sie dann auf **Weiter**.
6. Geben Sie die Anmeldeinformationen für den Dell Server ein, um den Mandanten bereitzustellen. Klicken Sie auf **Weiter**. *Die Bereitstellung eines vorhandenen Mandanten der Marke Cylance wird nicht unterstützt.*
7. Laden Sie das Zertifikat herunter. Dies ist erforderlich, um eine Wiederherstellung im Falle von Notfallszenarien mit dem Dell Server durchzuführen. Dieses Zertifikat wird nicht automatisch gesichert. Sichern Sie das Zertifikat auf einem sicheren Speicherplatz auf einem anderen Computer. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie das Zertifikat gesichert haben, und klicken dann Sie auf **Weiter**.
8. Die Einrichtung ist abgeschlossen. Klicken Sie auf **OK**.

11

Konfigurieren der automatischen Aktualisierung des Advanced Threat Prevention Agenten

Sie können sich in der Verwaltungskonsole anmelden, um automatische Aktualisierungen für den Advanced Threat Prevention-Agenten zu erhalten. Durch die Anmeldung für den Empfang automatischer Agent-Aktualisierungen können Clients Aktualisierungen automatisch herunterladen und über den Advanced Threat Prevention Dienst anwenden. Aktualisierungen werden monatlich herausgegeben.

ANMERKUNG:

Die automatischen Aktualisierungen des Agenten werden ab Dell Server Version 9.4.1 unterstützt.

Automatische Aktualisierungen für den Agenten empfangen

So melden Sie sich an, um automatische Agent-Aktualisierungen zu erhalten:

1. Klicken Sie im linken Bereich der Verwaltungskonsole auf **Verwaltung** > **Dienstverwaltung**.
2. Auf der Registerkarte *Advanced Threats* unter *Automatische Agent-Aktualisierung* klicken Sie auf die Schaltfläche **Ein** und dann auf die Schaltfläche **Einstellungen speichern**.

   Es kann einige Minuten dauern, bis die Bestückung mit Informationen abgeschlossen ist und die automatischen Aktualisierungen angezeigt werden.

Beenden des Empfangs von automatischen Agent-Aktualisierungen

So beenden Sie den Empfang von automatischen Agent-Aktualisierungen:

1. Klicken Sie im linken Bereich der Verwaltungskonsole auf **Verwaltung** > **Dienstverwaltung**.
2. Auf der Registerkarte *Advance Threats* unter *Automatische Agent-Aktualisierung* klicken Sie auf die Schaltfläche **Aus** und dann auf die Schaltfläche **Einstellungen speichern**.

12

Vorinstallationskonfiguration für die SED-UEFI und BitLocker Manager

TPM initialisieren

- Für diesen Vorgang müssen Sie Mitglied der lokalen Administratorgruppe oder dergleichen sein.
- Der Computer muss mit einem kompatiblen BIOS und TPM ausgestattet sein.
- Folgen Sie den Anweisungen unter http://technet.microsoft.com/en-us/library/cc753140.aspx.

Pre-Installation Konfiguration für den UEFI-Computern

Aktivieren der Netzwerkkonnektivität während der UEFI-Preboot-Authentifizierung

Damit die Preboot-Authentifizierung auf einem Computer mit UEFI-Firmware erfolgreich verläuft, muss die PBA mit Netzwerkkonnektivität ausgerüstet sein. Auf Computern mit UEFI-Firmware ist standardmäßig erst dann Netzwerkkonnektivität verfügbar, wenn das Betriebssystem geladen wurde. Dies geschieht in der Regel nach dem PBA-Modus.

Mithilfe des folgenden Verfahrens wird die Netzwerkkonnektivität während der PBA für UEFI-fähige Computer aktiviert. Da die Konfigurationsschritte bei den verschiedenen UEFI-Computermodellen voneinander abweichen, ist das folgende Verfahren als allgemeines Beispiel zu verstehen.

1. Starten Sie den Computer in die UEFI-Firmware-Konfiguration.
2. Drücken Sie während des Startvorgangs dauerhaft die Taste F2, bis rechts oben auf dem Bildschirm eine Meldung wie „Startmenü wird geöffnet“ angezeigt wird.
3. Geben Sie nach Aufforderung das BIOS-Administrator-Passwort ein.

   ANMERKUNG:

   Auf einem neuen Computer erhalten Sie diese Aufforderung nicht, weil noch kein BIOS-Passwort eingerichtet worden ist.
4. Wählen Sie die Option **Systemkonfiguration** aus.
5. Wählen Sie die Option **Integrierte NIC** aus.
6. Aktivieren Sie das Kontrollkästchen **UEFI-Netzwerkstapel aktivieren**.
7. Wählen Sie entweder die Option **Aktiviert** oder **Mit PXE aktiviert**.
8. Wählen Sie die Option **Übernehmen** aus.

   ANMERKUNG:

   Für Computer *ohne* UEFI-Firmware ist keine Konfiguration erforderlich.

Deaktivierung von Legacy-Option-ROMs

Stellen Sie sicher, dass die Einstellung **Legacy-Option-ROMs aktivieren** im BIOS deaktiviert wurde.

1. Starten Sie den Computer neu.
2. Drücken Sie während des Neustarts wiederholt **F12**, um die Start-Einstellungen des UEFI-Computers aufzurufen.

3. Drücken Sie die Taste mit dem Pfeil nach unten, markieren Sie die Option **BIOS-Einstellungen**, und drücken Sie die **Eingabetaste**.
4. Wählen Sie **Einstellungen** > **Allgemein** > **Erweiterte Startoptionen**.
5. Heben Sie die Markierung des Kontrollkästchens **Legacy-Option-ROMs aktivieren** auf, und klicken Sie auf **Übernehmen**.

Vorinstallationskonfiguration zum Einrichten einer BitLocker PBA-Partition

- Die PBA-Partition muss **vor** der Installation von BitLocker Manager eingerichtet werden.
- Schalten Sie das TPM ein und aktivieren Sie es, **bevor** Sie BitLocker Manager installieren. BitLocker Manager übernimmt die Zuweisung des TPM (kein Neustart erforderlich). Wenn das TPM bereits zugewiesen ist, leitet BitLocker Manager den Einrichtungsvorgang für die Verschlüsselung ein. Wichtig ist, dass das TPM „zugewiesen“ und aktiviert ist.
- Sie müssen die Festplattenpartition ggf. manuell einrichten. Weitere Informationen finden Sie in der Beschreibung von Microsoft zum BitLocker-Laufwerksvorbereitungs-Tool.
- Verwenden Sie zum Einrichten der PBA-Partition den Befehl BdeHdCfg.exe. Der Parameter „Standard“ gibt an, dass das Befehlszeilentool dasselbe Verfahren wie der BitLocker-Einrichtungsassistent befolgt.

  ```
  BdeHdCfg -target default
  ```

  ANMERKUNG:

  Weitere Optionen für den BdeHdCfg-Befehl finden Sie unter BdeHdCfg.exe-Referenzmaterial von Microsoft.

13

Festlegen des Dell Server über die Registrierung

- Wenn Ihre Clients über Dell Digital Delivery berechtigt sind, befolgen Sie diese Anweisungen, um eine Registrierung über Gruppenrichtlinienobjekte einzurichten, um den Dell Server für die Verwendung nach der Installation einzurichten.
- Die Workstation muss ein Mitglied der Organisationseinheit sein, in der die Gruppenrichtlinienobjekte angewendet werden, oder die Registrierungseinstellungen müssen manuell auf dem Endpunkt festgelegt werden.
- Achten Sie bitte darauf, dass der ausgehende Port 443 für die Kommunikation mit dem Dell Server mit cloud.dell.com verfügbar ist. Wenn Port 443 (aus irgendeinem Grund) gesperrt ist, schlägt der Erhalt der Berechtigung fehl und eine Berechtigung wird aus dem verfügbaren Pool verwendet.

  ANMERKUNG: Wenn Sie diesen Registrierungswert nicht festlegen, wenn Sie versuchen, über Dell Digital Delivery zu installieren oder keinen Server im Master-Installationsprogramm angeben, wird die Aktivierungs-URL standardmäßig auf 199.199.199.199 festgelegt.

Manuelles Einstellen des Registrierungsschlüssels

Für Endpunkte, die nicht mit der Domäne verbunden sind oder kein Gruppenrichtlinienobjekt festgelegt werden kann, ist es nicht möglich, einen Registrierungsschlüssel für die Aktivierung bei einem bestimmten Dell Server während der Installation festzulegen.

1. Geben Sie in das Suchfeld in der Taskleiste **regedit** ein, und klicken Sie dann mit der rechten Maustaste darauf und wählen **Als Administrator ausführen** aus.
2. Navigieren Sie zu dieser Position und erstellen Sie den folgenden Registrierungsschlüssel:

   HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection

   REG_SZ: Server

   Wert: <FQDN oder IP-Adresse des Dell Server>

3. Installieren Sie die Verschlüsselung über Dell Digital Delivery oder das Master-Installationsprogramm.

Erstellen des Gruppenrichtlinienobjekts

1. Klicken Sie auf dem Domain Controller, auf dem die Clients verwaltet werden sollen, auf **Start** > **Verwaltung** > **Gruppenrichtlinienverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, für die Sie die Richtlinie anwenden möchten, und wählen Sie **Gruppenrichtlinienobjekt in dieser Domäne erstellen** und **Hier verknüpfen** aus.
3. Geben Sie einen Namen für das neue Gruppenrichtlinienobjekt ein, wählen Sie unter „Anfangs-GPO-Quelle“ „(keine)“ aus, und klicken Sie auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf das neu erstellte Gruppenrichtlinienobjekt, und wählen Sie **Bearbeiten** aus.
5. Der Group Policy Management Editor wird geladen. Rufen Sie **Computerkonfiguration** > **Einstellungen** > **Windows-Einstellungen** > **Registrierung** auf.
6. Klicken Sie mit der rechten Maustaste auf die Registrierung und wählen Sie **Neu** > **Registrierungseintrag** aus. Nehmen Sie die folgenden Einstellungen vor:

   Action: Create

   Hive: HKEY_LOCAL_MACHINE

   Key Path: SOFTWARE\Dell\Dell Data Protection

   Value name: Server

   Value type: REG_SZ

   Wertedaten: <IFQDN oder IP-Adresse des Dell Server>

7. Klicken Sie auf **OK**.
8. Melden Sie sich von der Workstation ab und dann wieder an, oder führen Sie **`gpupdate /force`** aus, um die Gruppenrichtlinie zu übernehmen.

14

Untergeordnete Installationsprogramme extrahieren

- Zur Einzelinstallation der Clients müssen zunächst die untergeordneten ausführbaren Dateien aus dem Installationsprogramm extrahiert werden.
- 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 **DDSSuite.exe** auf den lokalen Computer.
2. Öffnen Sie am gleichen Speicherort wie dem der Datei **DDSSuite.exe** eine Eingabeaufforderung und geben Sie Folgendes ein:

   ```
   DDSSuite.exe /s /z"\"EXTRACT_INSTALLERS=C:\Extracted""
   ```

   Der Extraktionspfad darf maximal 63 Zeichen enthalten.

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

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

15

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.

  Der Key Server ist ein Dienst, der überwacht, ob Clients eine Verbindung über ein Socket herstellen. Wenn ein Client einen Verbindungsversuch unternimmt, wird mithilfe von Kerberos-APIs eine sichere Verbindung ausgehandelt, authentifiziert und verschlüsselt (wenn keine sichere Verbindung ausgehandelt werden kann, wird die Client-Verbindung getrennt).

  Der Key Server überprüft dann auf dem Security Server (früher Device Server), ob der Benutzer, der den Client ausführt, auf Schlüssel zugreifen darf. Diesen Zugriff erfolgt über einzelnen Domänen in der Verwaltungskonsole.

- 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).

   Das Format von „superadmin“ kann eine beliebige Methode für die Authentifizierung am Security Management Server darstellen. Der SAM-Kontoname, der UPN oder das Format „DOMÄNE\Benutzername“ sind akzeptabel. Jede Methode, die sich beim Security Management Server authentifizieren kann, ist akzeptabel, da für dieses Benutzerkonto eine Überprüfung zur Autorisierung bei Active Directory erforderlich ist.

   Beispiel: In einer Umgebung mit mehreren Domänen würde die Eingabe eines SAM-Kontonamens wie „mmustermann“ vermutlich fehlschlagen, da der Security Management Server „mmustermann“ nicht authentifizieren kann, weil er

den Namen nicht findet. In einer Umgebung mit mehreren Domänen wird der UPN empfohlen, obwohl das Format „DOMÄNE\Benutzername“ akzeptabel ist. In einer Umgebung mit einer Domäne kann der SAM-Kontoname verwendet werden.

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.

Beispielkonfigurationsdatei

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key=”port” value=”8050" /> [TCP-Port, den der Key Server hört. Die Standardeinstellung ist 8050.]

<add key="maxConnections" value="2000" /> [Anzahl der vom Key Server zugelassenen aktiven Sockelverbindungen]

<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [Security Server (früher: Device Server) URL (das Format lautet 8081/xapi für Security Management Server vor Version 7.7)]

<add key="verifyCertificate" value="false" /> [Bei „true“ werden Zertifikate überprüft. Legen Sie „false“ fest, wenn keine Überprüfung erfolgen soll oder selbstsignierte Zertifikate verwendet werden.]

<add key=”user” value=”superadmin” /> [Der für die Kommunikation mit dem Security Server verwendete Benutzername. Für diesen Benutzer muss in der Verwaltungskonsole die Administratorrolle ausgewählt sein. Das Format von „superadmin“ kann eine beliebige Methode für die Authentifizierung am Security Management Server darstellen. Der SAM-Kontoname, der UPN oder das Format „DOMÄNE\Benutzername“ sind akzeptabel. Jede Methode, die sich beim Security Management Server authentifizieren kann, ist akzeptabel, da für dieses Benutzerkonto eine Überprüfung zur Autorisierung bei Active Directory erforderlich ist. Beispiel: In einer Umgebung mit mehreren Domänen würde die Eingabe eines SAM-Kontonamens wie „mmustermann“ vermutlich fehlschlagen, da der Security Management Server „mmustermann“ nicht authentifizieren kann, weil er den Namen nicht findet. In einer Umgebung mit mehreren Domänen wird der UPN empfohlen, obwohl das Format „DOMÄNE\Benutzername“ akzeptabel ist. In einer Umgebung mit einer Domäne kann der SAM-Kontoname verwendet werden.]

<add key="cacheExpiration" value="30" /> [Wie oft (in Sekunden) der Dienst überprüfen soll, wer Schlüssel abrufen darf. Der Dienst unterhält einen Cache und verfolgt dessen Alter. Wenn der Cache älter ist als der Wert, erhält er eine neue Liste. Wenn ein Benutzer eine Verbindung herstellt, muss der Key Server autorisierte Benutzer vom Security Server herunterladen. Wenn kein Cache mit diesen Benutzern existiert oder die Liste in den letzten x Sekunden nicht heruntergeladen wurde, wird sie erneut heruntergeladen. Es erfolgt keine Abfrage, doch dieser Wert bestimmt, wie alt die Liste werden kann, bevor sie bei Bedarf aktualisiert wird.]

<add key="epw" value="encrypted value of the password" /> [Das für die Kommunikation mit dem Security Management Server verwendete Passwort. Wenn das Superadmin-Passwort geändert wurde, muss es auch hier geändert werden.]

</appSettings>

</configuration>

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.

16

Verwenden Sie das administrative Dienstprogramm zum Herunterladen (CMGAd)

- Mit diesem Dienstprogramm können Sie Schlüsseldatenpakete zur Verwendung auf einem Computer herunterladen, der nicht mit einem Dell Server verbunden ist.
- Je nachdem, welche Befehlszeilenparameter an die Anwendung übergeben werden, verwendet das Dienstprogramm eine der folgenden Methoden zum Herunterladen von Schlüsseldatenpaketen:
  - 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 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/.

   Dell Admin: Name des Administrators mit forensischen Zugriffsrechten, z. B. „hschmidt“ (aktiviert in der Verwaltungskonsole)

   Passwort: Forensisches Administrator-Passwort

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

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

   ANMERKUNG:

   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 verschiedene Informationen, die von diesem Dienstprogramm verwendet werden.

   Klicken Sie auf **Weiter**.

3. Geben Sie unter *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 Admin-Modus

Der Security Management Server Virtual verwendet den Key Server nicht, d. h. im Admin-Modus kann kein Schlüsselpaket über den 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

   ANMERKUNG:

   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 verschiedene Informationen, die von diesem Dienstprogramm verwendet werden.

   Klicken Sie auf **Weiter**.

3. Geben Sie unter *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**.

17

Encryption auf einem Serverbetriebssystem konfigurieren

Encryption auf einem Serverbetriebssystem aktivieren

ANMERKUNG:

Encryption auf Serverbetriebssystemen wandelt Benutzerverschlüsselung in allgemeine Verschlüsselung um.

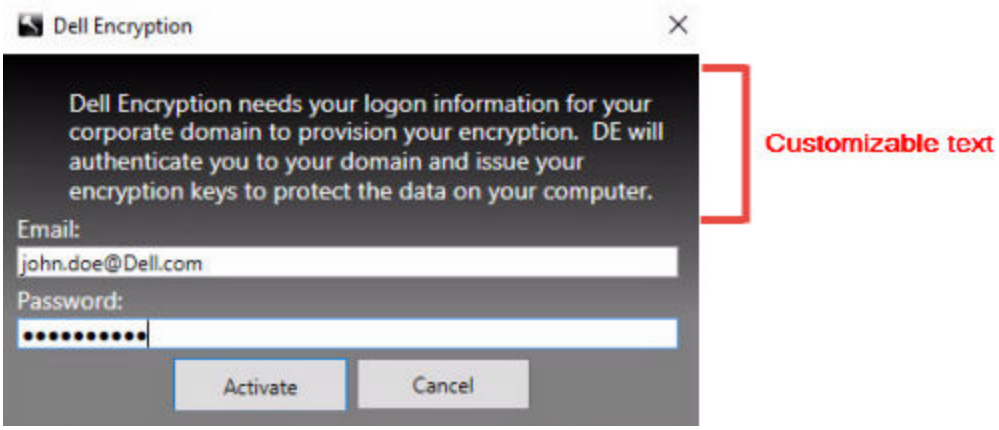
1. Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.
2. Wählen Sie **Endpunkt-Gruppe** (oder **Endpunkt**) aus, suchen Sie nach dem zu aktivierenden Endpunkt oder der zu aktivierenden Endpunkt-Gruppe, wählen Sie **Sicherheitsrichtlinien** und anschließend die Richtlinienkategorie **Serververschlüsselung** aus.
3. Legen Sie die folgenden Richtlinien fest:
   - Serververschlüsselung – **Auswählen**, um Encryption auf einem Serverbetriebssystem und zugehörige Richtlinien zu aktivieren.
   - SDE-Verschlüsselung aktiviert – **Auswählen**, um SDE-Verschlüsselung einzuschalten.
   - Verschlüsselung aktiviert – **Auswählen**, um allgemeine Verschlüsselung einzuschalten.
   - Windows-Anmeldeinformationen sichern – Diese Richtlinie wird standardmäßig **ausgewählt**.

     Wenn die Richtlinie *Windows-Anmeldeinformationen sichern* **ausgewählt** ist (Standardeinstellung), werden alle im Ordner „\Windows\system32\config files“ enthaltenen Dateien verschlüsselt, einschließlich der Windows-Anmeldeinformationen. Um zu verhindern, dass die Windows-Anmeldeinformationen verschlüsselt werden, setzen Sie die Richtlinie *Windows-Anmeldeinformationen sichern* auf **nicht ausgewählt**. Die Verschlüsselung der Windows-Anmeldeinformationen findet unabhängig von der Einstellung der Richtlinie *SDE-Verschlüsselung aktiviert* statt.
4. Speichern Sie die Richtlinien und aktivieren Sie sie.

Aktivierung des Anmeldedialogfelds anpassen

Das Dialogfeld „Anmeldung zur Aktivierung“ wird in folgenden Fällen angezeigt:

- Wenn sich ein unverwalteter Benutzer anmeldet.
- Wenn der Benutzer „Aktivieren der Dell Encryption“ im Menü des Verschlüsselungssymbols im Infobereich auswählt.



Einrichten von Encryption External Media-Richtlinien

Der ***verschlüsselnde Ursprungscomputer*** ist der Computer, der ein Wechselmedium ursprünglich verschlüsselt. Wenn der Ursprungscomputer ein ***geschützter Server*** – ein Server mit Encryption auf einem Serverbetriebssystem, installiert und aktiviert – ist und der geschützte Server zuerst erkennt, dass ein Wechselmedium angeschlossen ist, wird der Benutzer aufgefordert, das Wechselmedium zu verschlüsseln.

- Richtlinien für Encryption External Media steuern den Zugriff von Wechselmedien auf den Server, Authentifizierung, Verschlüsselung und mehr.
- Die Portsteuerungsrichtlinien wirken sich zum Beispiel auf Wechselmedien aus, die sich auf geschützten Servern befinden, indem sie den Zugriff und die Nutzung der USB-Ports des Servers durch USB-Geräte steuern.

Die Richtlinien für die Verschlüsselung von Wechselmedien finden Sie in der Verwaltungskonsole unter der Technologiegruppe *Serververschlüsselung*.

Encryption auf einem Serverbetriebssystem und externen Medien

Wenn die Richtlinie *EMS-Verschlüsseln externer Datenträger* **ausgewählt** ist, werden externe Datenträger verschlüsselt. Encryption verbindet das Gerät mit dem geschützten Server durch den Computerschlüssel und mit dem Benutzer durch den Benutzer-Roaming-Schlüssel des Besitzers/Benutzers des Wechselmediums. Alle Dateien, die zum Wechselmedium hinzugefügt werden, werden dann mit diesen Schlüsseln verschlüsselt, wobei es keine Rolle spielt, mit welchem Computer das Wechselmedium verbunden ist.

ANMERKUNG:

Encryption auf einem Serverbetriebssystem konvertiert die Benutzerverschlüsselung in allgemeine Verschlüsselung, außer auf Wechselmedien. Auf Wechselmedien wird die Verschlüsselung mit dem Benutzer-Roaming-Schlüssel durchgeführt, der mit dem Computer verknüpft ist.

Wenn der Benutzer der Verschlüsselung eines Wechselmediums nicht zustimmt, kann der Zugriff des Benutzers auf das Gerät bei/während der Verwendung auf dem geschützten Server auf *blockiert*, *Nur Schreiben* oder *Vollzugriff* eingestellt werden. Die Richtlinien des geschützten Servers legen auf ungeschützten Wechselmedien die Zugriffsebene fest.

Richtlinienaktualisierungen finden beim erneuten Einsetzen eines Wechselmediums in den geschützten Ursprungsserver statt.

Authentifizierung und externe Datenträger

Die Richtlinien des geschützten Servers legen die Authentifizierungsfunktionalität fest.

Nach Verschlüsselung eines Wechselmediums kann auf dem geschützten Server nur der Besitzer/Benutzer des Wechselmediums darauf zugreifen. Andere Benutzer können auf die verschlüsselten Dateien auf dem Wechselmedium nicht zugreifen.

Mit lokaler automatischer Authentifizierung können die geschützten Wechselmedien automatisch authentifiziert werden, wenn sie an den geschützten Server angeschlossen werden und der Eigentümer des betreffenden Mediums angemeldet ist. Wenn die automatische Authentifizierung deaktiviert ist, muss der Besitzer/Benutzer den Zugriff auf das geschützte Wechselmedium authentifizieren.

Handelt es sich beim ursprünglich verschlüsselnden Computer des Wechselmediums um einen geschützten Server, muss sich der Besitzer/Benutzer bei Verwendung auf nicht ursprünglich für die Verschlüsselung verwendeten Computern immer am Wechselmedium anmelden, ungeachtet der Encryption External Media-Richtlinieneinstellungen, die auf den anderen Computern definiert wurden.

Weitere Informationen über Serververschlüsselungs-Portsteuerung und Encryption External Media-Richtlinien finden Sie unter AdminHelp.

Anhalten von Encryption auf einem Serverbetriebssystem

Das Anhalten eines verschlüsselten Servers verhindert den Zugriff auf seine verschlüsselten Daten nach einem Neustart. Der virtuelle Serverbenutzer kann nicht deaktiviert werden. Stattdessen wird der Computerschlüssel des verschlüsselten Servers deaktiviert.

ANMERKUNG:

Durch Deaktivieren des Serverendpunktes wird der Server nicht unmittelbar angehalten. Die Deaktivierung findet dann statt, wenn der Schlüssel zum nächsten Mal angefordert wird, dies ist in der Regel beim nächsten Neustart des Servers der Fall.

ANMERKUNG:

Mit Vorsicht verwenden. Das Anhalten eines verschlüsselten Servers kann je nach Richtlinieneinstellungen und abhängig davon, ob der geschützte Server angehalten wird, während er vom Netzwerk getrennt ist, Instabilität zur Folge haben.

Voraussetzungen

- Helpdesk-Administratorrechte, die in der Verwaltungskonsole zugewiesen sind, sind erforderlich, um einen Endpunkt zu deaktivieren.
- Der Administrator muss in der Verwaltungskonsole angemeldet sein.

Klicken Sie im linken Bereich der Verwaltungskonsole auf **Bestückungen** > **Endpunkte**.

Suchen oder wählen Sie einen Hostnamen aus und wählen Sie anschließend die Registerkarte **Details und Aktionen** aus.

Klicken Sie unter *Servergerätesteuerung* auf **Sperren** und dann auf **Ja**.

ANMERKUNG:

Klicken Sie auf die Schaltfläche **Reaktivieren**, um Encryption auf Serverbetriebssystemen den Zugriff auf die verschlüsselten Daten auf dem Server zu ermöglichen, nachdem dieser neu gestartet wurde.

18

Verzögerte Aktivierung konfigurieren

Der Encryption-Client mit verzögerter Aktivierung unterscheidet sich von der Encryption-Client-Aktivierung auf zwei Arten:

Gerätebasierte Verschlüsselungsrichtlinien

Die Encryption-Client-Richtlinien sind benutzerbasiert; die Verschlüsselungsrichtlinien von Encryption-Client mit verzögerter Aktivierung sind gerätebasiert. Benutzerverschlüsselung wird in allgemeine Verschlüsselung konvertiert. Diese Differenz ermöglicht es dem Benutzer, ein persönliches Gerät zur Verwendung innerhalb der Domain der Organisation mitzubringen, während die Organisation ihre Sicherheit durch zentral verwaltete Verschlüsselungsrichtlinien aufrecht erhält.

Aktivierung

Beim Encryption-Client erfolgt die Aktivierung automatisch. Wenn Endpoint Security Suite Enterprise mit verzögerter Aktivierung installiert ist, ist die automatische Aktivierung deaktiviert. Stattdessen entscheidet der Benutzer, ob und wann die Verschlüsselung aktiviert werden soll.

ANMERKUNG:

Bevor ein Benutzer die Organisation dauerhaft verlässt und während seine E-Mail-Adresse immer noch aktiv ist, muss der Benutzer den Encryption-Entfernungsagenten ausführen und den Encryption-Client auf seinem persönlichen Computer deinstallieren.

Individuelle Einrichtung der verzögerten Aktivierung

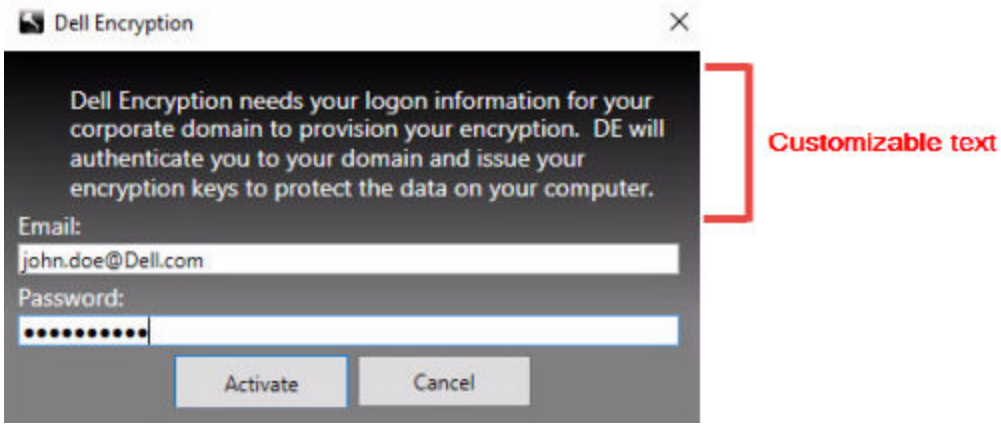
Mit diesen Client-seitigen Aufgaben kann die verzögerte Aktivierung individuell eingerichtet werden.

- Fügen Sie zum Dialogfeld „Anmeldung zur Aktivierung“ einen Haftungsausschluss hinzu
- Deaktivieren Sie die automatische Reaktivierung (optional)

Fügen Sie zum Dialogfeld „Anmeldung zur Aktivierung“ einen Haftungsausschluss hinzu

Das Dialogfeld „Anmeldung zur Aktivierung“ erscheint zu folgenden Zeitpunkten:

- Wenn sich ein unverwalteter Benutzer anmeldet.
- Wenn der Benutzer „Aktivieren der Dell Encryption“ im Menü des Verschlüsselungssymbols im Infobereich auswählt.



Computer für Installation vorbereiten

Wenn die Daten mit einem nicht von Dell stammenden Verschlüsselungsprodukt verschlüsselt sind, entschlüsseln Sie die Daten vor der Installation des Encryption-Clients mithilfe der vorhandenen Verschlüsselungssoftware und deinstallieren Sie anschließend die vorhandene Verschlüsselungssoftware. Wenn der Computer nicht automatisch neu startet, führen Sie einen Neustart des Computers durch.

Erstellen Sie ein Windows-Kennwort

Dell empfiehlt, ein Windows-Kennwort einzurichten (sofern noch nicht vorhanden), um den Zugriff auf Ihre verschlüsselten Daten zu beschränken. Wenn Sie den Computer durch ein Kennwort schützen, können sich andere nicht ohne dieses Kennwort bei Ihrem Benutzerkonto anmelden.

Deinstallieren Sie frühere Versionen des Encryption-Clients

Stoppen oder halten Sie vor der Deinstallation einer früheren Version des Encryption-Clients einen Verschlüsselungsdurchgang, falls erforderlich, an.

Wenn auf dem Computer eine Version von Dell Encryption ausgeführt wird, die älter als Version 8.6 ist, deinstallieren Sie den Encryption-Client von der Befehlszeile aus. Anleitungen hierzu finden Sie unter *Verschlüsselung und Encryption-Server-Client deinstallieren*.

ANMERKUNG:

Wenn Sie planen, sofort nach der Deinstallation die neueste Version des Encryption-Clients zu installieren, ist es nicht erforderlich, den Encryption-Entfernungsagenten zur Entschlüsselung der Dateien auszuführen.

Führen Sie für das Upgrade einer früheren Version des Encryption-Clients, der mit verzögerter Aktivierung installiert wurde, eine Deinstallation mit dem Data Security-Deinstallationsprogramm oder den untergeordneten Installationsprogrammen aus. Diese Deinstallationsmethode ist selbst dann möglich, wenn OPTIN deaktiviert ist.

ANMERKUNG:

Wenn zuvor keine Benutzer aktiviert wurden, löscht der Encryption-Client die OPTIN-Einstellung aus dem SDE-Vault, da die Einstellung noch aus einer vorherigen Installation stammt. Der Encryption-Client blockiert verzögerte Aktivierungen, wenn Benutzer die Aktivierung zuvor durchgeführt haben, aber der OPTIN-Flag nicht im SDE-Vault eingerichtet ist.

Encryption mit verzögerter Aktivierung installieren

Um den Encryption-Client mit verzögerter Aktivierung zu installieren, müssen Sie den Encryption-Client mit dem Parameter OPTIN=1 installieren. Weitere Informationen zur Client-Installation mit dem Parameter OPTIN=1 finden Sie unter Encryption installieren.

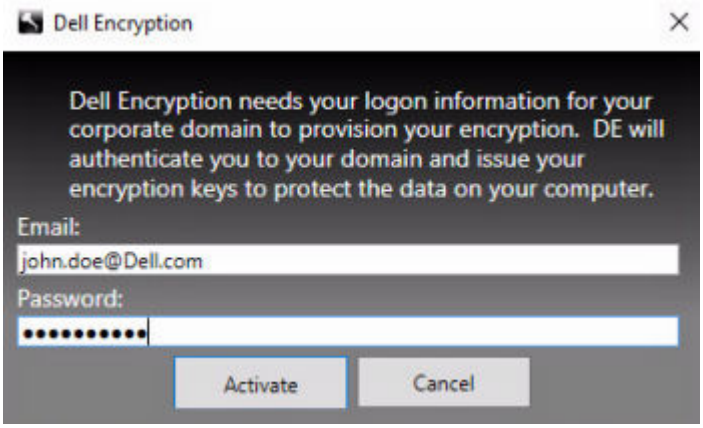
Encryption mit verzögerter Aktivierung aktivieren

- Die Aktivierung ordnet einen Domainbenutzer einem lokalen Benutzerkonto und einem bestimmten Computer zu.
- Mehrere Benutzer können die Aktivierung auf demselben Computer durchführen, sofern Sie eindeutige lokale Konten verwenden und über eindeutige Domain-E-Mail-Adressen verfügen.
- Ein Benutzer kann den Encryption-Client nur einmal pro Domainkonto aktivieren.

Vor Aktivierung des Encryption-Clients:

- Melden Sie sich bei dem lokalen Konto an, dass Sie am häufigsten nutzen. Die Daten, die mit diesem Konto in Verbindung stehen, sind die Daten, die verschlüsselt werden.
- Verbinden Sie sich mit dem Netzwerk Ihres Unternehmens.

1. Melden Sie sich an der Arbeitsstation oder am Server an.
2. Geben Sie Ihre Domain-E-Mail-Adresse und Ihr Kennwort ein und klicken Sie auf **Aktivieren**.



ANMERKUNG:

Persönliche oder E-Mail-Adressen, die nicht zur Domain gehören, können nicht für die Aktivierung verwendet werden.

3. Klicken Sie auf **Schließen**.

   Der Dell Server kombiniert das Verschlüsselungsschlüsselpaket mit den Anmeldeinformationen des Benutzers und mit der eindeutigen ID (Maschinen-ID) des Computers. Dadurch erstellt er eine unknackbare Beziehung zwischen dem Schlüsselpaket, dem entsprechenden Computer und dem Benutzer.

4. Starten Sie den Computer, um mit dem Verschlüsselungsdurchgang zu beginnen.

ANMERKUNG:

Die lokale Verwaltungskonsole, auf die über das Symbol im Infobereich zugegriffen werden kann, zeigt die vom Server gesendeten Richtlinien und nicht die effektive Richtlinie.

Fehlerbehebung bei verzögerter Aktivierung

Fehlerbehebung bei Aktivierung

Problem: Kein Zugriff auf bestimmte Dateien und Ordner

Wenn auf bestimmte Dateien und Ordner nicht zugegriffen werden kann, ist das ein Anzeichen dafür, dass der Benutzer nicht mit dem Konto angemeldet ist, mit dem er sich aktiviert hat, sondern mit einem anderen.

Das Dialogfeld „Anmeldung zur Aktivierung“ erscheint automatisch, obwohl der Benutzer sich zuvor aktiviert hat.

Mögliche Lösung

Melden Sie sich ab und dann wieder mit den Anmeldeinformationen des aktivierten Kontos an und versuchen Sie erneut, auf die Dateien zuzugreifen.

Falls es tatsächlich dazu kommen sollte, dass der Encryption-Client den Benutzer nicht authentifizieren kann, bittet das Dialogfeld „Anmeldung zur Aktivierung“ den Benutzer für die Authentifizierung und den Zugriff auf Verschlüsselungsschlüssel um Anmeldeinformationen. Zur Verwendung der automatischen Reaktivierungsfunktion müssen die BEIDEN Registrierungsschlüssel *AutoReactivation* und *AutoPromptForActivation* aktiviert sein. Obwohl die Funktion standardmäßig aktiviert ist, kann sie manuell deaktiviert werden. Weitere Informationen finden Sie unter Automatische Reaktivierung deaktivieren.

Fehlermeldung: Fehlerhafte Server-Authentifizierung

Der Server war nicht dazu in der Lage, die E-Mail-Adresse und das Kennwort zu authentifizieren.

Mögliche Lösungen

- Verwenden Sie die E-Mail-Adresse, die der Organisation zugeordnet ist. Persönliche E-Mail-Adressen können nicht zur Aktivierung verwendet werden.
- Geben Sie die E-Mail-Adresse und das Kennwort ein und stellen Sie sicher, dass keine Tippfehler enthalten sind.
- Bitten Sie den Administrator darum, zu überprüfen, dass das E-Mail-Konto aktiv und nicht gesperrt ist.
- Bitten Sie den Administrator darum, das Domainkennwort des Benutzers zurückzusetzen.

Fehlermeldung: Netzwerkverbindungsfehler

Der Encryption-Client konnte nicht mit dem Dell Server kommunizieren.

Mögliche Lösungen

- Verbinden Sie sich direkt mit dem Netzwerk der Organisation und nehmen Sie die Aktivierung erneut vor.
- Wenn für die Verbindung mit dem Netzwerk ein VPN-Zugriff erforderlich ist, überprüfen Sie die VPN-Verbindung und versuchen Sie es 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 und wieder anschließen:

  Trennen Sie den Computer vom Netzwerk.

  Verbinden Sie ihn wieder mit dem Netzwerk.

  Starten Sie den Computer neu.

  Versuchen Sie sich erneut mit dem Netzwerk zu verbinden.

  Fehlermeldung: Legacy-Server wird nicht unterstützt

  Die Verschlüsselung kann nicht mit einem Legacy-Server aktiviert werden; der Dell Server muss Version 9.1 oder höher sein.

  Mögliche Lösung

- 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]

  Fehlermeldung: Domainbenutzer bereits aktiviert

  Ein zweiter Benutzer hat sich auf dem lokalen Computer angemeldet und versucht, die Aktivierung mit einem Domainkonto durchzuführen, das bereits aktiviert wurde.

  Ein Benutzer kann den Encryption-Client nur einmal pro Domainkonto aktivieren.

  Mögliche Lösung

  Entschlüsseln und deinstallieren Sie den Encryption-Client, während Sie als zweiter aktivierter Benutzer angemeldet sind.

  Fehlermeldung: Allgemeiner Serverfehler

  Auf dem Server ist ein Fehler aufgetreten.

  Mögliche Lösung

  Der Administrator sollte die Serverprotokolle überprüfen, um sicherzustellen, dass die Dienste ausgeführt werden.

  Der Benutzer sollte die Aktivierung später durchführen.

Extras

CMGAd

Verwenden Sie das Dienstprogramm CMGAd, bevor Sie den Encryption-Entfernungsagenten zum Abrufen des Verschlüsselungsschlüsselpakets starten. Sie finden das Dienstprogramm CMGAd und die zugehörige Anleitung auf dem Dell Installationsmedium (Dell-Offline-Admin-XXbit)

Protokolldateien

In `C:\ProgramData\Dell\Dell Data Protection\Encryption` finden Sie die Protokolldatei mit dem Namen **CmgSysTray**.

Suchen Sie nach dem Begriff „Ergebnis der manuellen Aktivierung“.

Der Fehlercode steht in derselben Zeile, gefolgt von „Status =“; der Status gibt den Fehler an.

19

Fehlerbehebung

Alle Clients – Fehlerbehebung

- **Endpoint Security Suite Enterprise master-Installationsprogramm-Protokolldateien** befinden sich unter `C:\ProgramData\Dell\Dell Data Protection\Installer`.
- Windows erstellt für den angemeldeten Benutzer eindeutige Installationsprotokolldateien des untergeordneten Installationsprogramms im Verzeichnis „%temp%“ unter `C:\Users\<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). Dell Access ist nicht kompatibel mit dieser Suite von Produkten.

Alle Clients – Schutzstatus

Eine neue Methode zur Feststellung des Schutzstatus eines Geräts wurde im Dell Server Version 9.8.2 implementiert. Zuvor wurde im Bereich „Endgerät-Schutzstatus“ im Dashboard der Verwaltungskonsole nur der Verschlüsselungsstatus des Geräts angezeigt.

Ab Dell Server Version 9.8.2 wird der Status „Geschützt“ 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.
- Self-Encrypting Drive Manager ist installiert und aktiviert und die PBA ist aktiviert.
- Full Disk Encryption ist installiert und aktiviert und PBA ist aktiviert.
- BitLocker Manager ist installiert sowie aktiviert und die Verschlüsselung wurde abgeschlossen.
- Dell Encryption (Mac) ist installiert sowie aktiviert und *Verschlüsselung mit FileVault for Mac* wurde umgesetzt.
- Dell Encryption (Windows) ist installiert und aktiviert, die richtlinienbasierte Verschlüsselung wurde für den Endpunkt eingerichtet und die Gerätesuchläufe sind abgeschlossen.

Dell Encryption – Fehlerbehebung (Client und Server)

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 von Encryption für Server-Betriebssysteme 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 „Aktivierung“ wird angezeigt, wenn einer von zwei Workflows auftritt:

- Ein neuer (nicht verwalteter) Benutzer meldet sich am Computer an.
- Ein neuer Benutzer klickt im Infobereich mit der rechten Maustaste auf das *Encryption*-Symbol und wählt *Dell Encryption aktivieren*.

  Der Ablauf für die erstmalige Aktivierung ist wie folgt:

1. Der Benutzer meldet sich an.
2. Bei Erkennung eines neuen (nicht verwalteten) Benutzers wird das Dialogfenster *Aktivieren* 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 *Encryption*-Symbol und wählt *Dell Encryption aktivieren*.
5. Der Benutzer gibt die Anmeldeinformationen des Domänenadministrators im Dialogfenster für die Aktivierung ein.

ANMERKUNG:

Die Anforderung für die Domänenadministrator-Anmeldeinformationen ist eine Sicherheitsmaßnahme, die verhindert, dass Encryption für Server-Betriebssysteme auf nicht unterstützten Serverumgebungen eingeführt wird. 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 Encryption für Serverbetriebssysteme 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 Encryption für Serverbetriebssysteme authentifiziert ist und sich im Servermodus befindet.
- 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 Informationen zur Richtlinie *ntervall für Neuversuch nach Netzwerkfehler*finden Sie in der Administratorhilfe, verfügbar in der Verwaltungskonsole.

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.

Erstellen einer Encryption Removal Agent-Protokolldatei (optional)

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

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=DWORD:2

  0: Keine Protokollierung

  1: Protokolliert Fehler, die den Betrieb des Dienstes verhindern

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

  3: Protokolliert Informationen über alle zu entschlüsselnden Datenträger und Dateien

  5: Protokolliert Informationen zum Debuggen

TSS-Version suchen

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

Encryption External Media und PCS Interaktionen

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

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

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

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

WSScan verwenden

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

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

Ausführen von WSScan

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

ODER

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

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

Verwenden der WSScan-Befehlszeile

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r]
[-u[a][-|v]] [-d<delimeter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

Schalter	Erläuterung
Laufwerk	Zu durchsuchendes Laufwerk. Falls keine Angabe gemacht wird, werden standardmäßig alle lokalen Festplattenlaufwerke durchsucht. Kann ein zugeordnetes Netzwerklaufwerk sein.
-ta	Alle Laufwerke durchsuchen
-tf	Festplattenlaufwerke durchsuchen (Standardeinstellung)
-tr	Wechseldatenträger durchsuchen
-tc	CDROMs/DVDROMs durchsuchen
-s	Hintergrundbetrieb

Schalter	Erläuterung
-o	Ausgabedateipfad
-a	An Ausgabedatei anhängen. Die Ausgabedatei wird standardmäßig abgeschnitten.
-f	Berichtsformat angeben (Bericht, fest, begrenzt).
-r	WSScan ohne Administratorrechte ausführen. **In diesem Modus sind einige Dateien möglicherweise nicht sichtbar.**
-u	Einbeziehen unverschlüsselter Dateien in die Ausgabedatei. Dieser „-u“-Switch ist hochempfindlich. Entweder müssen zuerst „u“ gefolgt von „a“ eingegeben (bzw. ausgelassen) werden, oder die Eingabe muss mit „-“ oder „v“ abgeschlossen werden.
-u-	Nur verschlüsselte Dateien in die Ausgabedatei einbeziehen
-ua	Auch Berichte über unverschlüsselte Dateien erstellen, aber Richtlinien für alle Benutzer anwenden, um das Feld zur Verschlüsselung anzuzeigen.
-ua-	Berichte nur über unverschlüsselte Dateien erstellen, aber Richtlinien für alle Benutzer anwenden, um das Feld zur Verschlüsselung anzuzeigen.
-uv	Berichte nur über unverschlüsselte Dateien erstellen, die die Richtlinie verletzen, d. h. Status = Nein, Verschlüsselung = Ja.
-uav	Berichte nur über unverschlüsselte Dateien (Status = Nein, Verschlüsselung = Ja) unter Anwendung der Richtlinien für alle Benutzer erstellen.
-d	Angabe des Trennzeichens für begrenzte Ausgabe.
-q	Angabe der Werte, die für begrenzte Ausgabe in Anführungszeichen gesetzt werden müssen.
-e	Erweiterte Verschlüsselungsfelder in begrenzte Ausgabe aufnehmen.
-x	Ausschließen eines Verzeichnisses vom Suchvorgang. Mehrere Ausschlüsse sind möglich.
-y	Ruhemodus (in Millisekunden) zwischen Verzeichnissen. Durch diesen Schalter werden Suchvorgänge verlangsamt, allerdings ist der Prozessor potenziell reaktiver.

WSScan-Ausgabe

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

Beispiel der Ausgabe:

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

Ausgabe	Erläuterung
Zeitstempel	Das Datum und die Uhrzeit der Durchsuchung der Datei.
Verschlüsselungstyp	Die Art der Verschlüsselung für die Datei. **SysData**: SDE-Schlüssel. **Benutzer:** Benutzer-Verschlüsselungscode. **Allgemein:** Allgemeiner Verschlüsselungscode.

Ausgabe	Erläuterung
	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

Verwenden von WSProbe

Das Suchdienstprogramm ist zur Verwendung mit allen Versionen von Encryption vorgesehen, außer Encryption External Media-Richtlinien. Mit dem Suchdienstprogramm haben Sie folgende Möglichkeiten:

- Durchsuchen oder Planen der Durchsuchung eines verschlüsselten Computers. Das Suchdienstprogramm befolgt die Richtlinie zur Workstation-Scanpriorität.
- Deaktivieren oder aktivieren Sie vorübergehend die Anwendungsdaten-Verschlüsselungsliste des aktuellen Benutzers.
- Hinzufügen der privilegierten Liste Prozessnamen oder Entfernen derselben.
- Fehlersuche nach den Anweisungen des Dell ProSupports

Ansätze für die Datenverschlüsselung

Beim Festlegen von Richtlinien zur Verschlüsselung von Daten auf Windows-Geräten stehen Ihnen mehrere Ansätze zur Verfügung:

- Der erste Ansatz besteht darin, das Standardverhalten des Clients zu übernehmen. Wenn Sie Ordner in „Allgemein verschlüsselte Ordner“ oder „Benutzerverschlüsselte Ordner“ angeben oder „Meine Dokumente verschlüsseln“, „Persönliche Outlook-Ordner verschlüsseln“, „Temporäre Dateien verschlüsseln“, „Temporäre Internetdateien verschlüsseln“ oder „Windows-Auslagerungsdatei verschlüsseln“ auf „Wahr“ einstellen, werden die betroffenen Dateien bei Erstellung oder Anmeldung eines verwalteten Benutzers (nach der Erstellung eines nicht verwalteten Benutzer) verschlüsselt. Der Client durchsucht auch Ordner, die in diesen Richtlinien angegeben sind oder sich auf sie beziehen, auf mögliche Verschlüsselung/Entschlüsselung, wenn ein Ordner umbenannt wird oder wenn der Client Änderungen an diesen Richtlinien erhält.
- Sie können auch „Arbeitsstation bei Anmeldung durchsuchen“ auf „ausgewählt“ setzen. Wenn „Arbeitsstation bei Anmeldung durchsuchen“ auf „ausgewählt“ eingestellt ist, vergleicht der Client bei der Benutzeranmeldung die Art und Weise, in der Dateien in derzeit und zuvor verschlüsselten Ordnern verschlüsselt sind, mit den Benutzerrichtlinien und nimmt gegebenenfalls die nötigen Änderungen vor.
- Wenn Sie Dateien verschlüsseln möchten, die Ihre Verschlüsselungskriterien erfüllen, aber vor Inkrafttreten Ihrer Verschlüsselungsrichtlinien erstellt wurden, die Leistung jedoch nicht durch häufiges Durchsuchen beeinträchtigen möchten, können Sie mit diesem Dienstprogramm die Durchsuchung des Computers durchführen oder einplanen.

Voraussetzungen

- Das Windows-Gerät, mit dem gearbeitet werden soll, muss verschlüsselt sein.
- Der Benutzer, mit dem gearbeitet werden soll, muss angemeldet sein.

Verwenden des Suchdienstprogramms

WSProbe.exe befindet sich auf den Installationsmedien.

Syntax

```
wsprobe [path]
wsprobe [-h]
wsprobe [-f path]
wsprobe [-u n] [-x process_names] [-i process_names]
```

Parameter

Parameter	Um die SSL/TLS-Vertrauensprüfung für BitLocker Manager zu
Pfad	Gibt optional einen bestimmten Pfad auf dem Gerät an, der auf mögliche Verschlüsselung/Entschlüsselung durchsucht werden soll. Wenn kein Pfad angegeben wird, durchsucht dieses Dienstprogramm alle Ordner, auf die sich Ihre Verschlüsselungsrichtlinien beziehen.
-h	Zeigt die Befehlszeilenhilfe an.
-f	Fehlersuche nach den Anweisungen des Dell ProSupports
-u	Deaktiviert oder aktiviert vorübergehend die Anwendungsdaten-Verschlüsselungsliste des Benutzers. Diese Liste ist nur wirksam, wenn „Verschlüsselung aktiviert“ für den aktuellen Benutzer ausgewählt ist. Geben Sie 0 zur Deaktivierung oder 1 zur Reaktivierung an. Die aktuelle Richtlinie wird bei der nächsten Anmeldung in Kraft gesetzt.
-x	Fügt der privilegierten Liste Prozessnamen hinzu oder entfernt sie. Die Computer- und Installationsprogramm-Prozessnamen in dieser Liste sowie die, die Sie mit diesem Parameter oder mit HKLM\Software\CREDANT\CMGShield\EUWPrivilegedList hinzufügen, werden ignoriert, wenn sie in der Anwendungsdaten-Verschlüsselungsliste angegeben sind. Trennen Sie Prozessnamen durch Kommas. Wenn Ihre Liste eine oder mehrere Leerstellen enthält, müssen Sie die Liste in doppelte Anführungszeichen setzen.
-i	Entfernt Prozessnamen, die zuvor der privilegierten Liste hinzugefügt wurden (hartcodierte Prozessnamen können Sie nicht entfernen). Trennen Sie Prozessnamen durch Kommas. Wenn Ihre Liste eine oder mehrere Leerstellen enthält, müssen Sie die Liste in doppelte Anführungszeichen setzen.

Überprüfen des Encryption-Removal-Agent-Status

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

- **Warten auf SDE-Deaktivierung** – Encryption ist noch installiert und/oder konfiguriert. Die Entschlüsselung beginnt erst nach der Deinstallation von Encryption.
- **Erste Suche** – Dieser Dienst führt eine erste Suche durch und berechnet die Anzahl verschlüsselter Dateien und Bytes. Die erste Suche wird nur einmal durchgeführt.
- **Entschlüsselungssuche** – Dieser Dienst entschlüsselt Dateien und stellt möglicherweise eine Anfrage zur Entschlüsselung gesperrter Dateien.
- **Entschlüsselung bei Neustart (teilweise)** – Die Entschlüsselungssuche ist abgeschlossen, und einige gesperrte Dateien (aber nicht alle) werden beim nächsten Neustart entschlüsselt.

- **Entschlüsselung bei Neustart** – Die Entschlüsselungssuche ist abgeschlossen, und alle gesperrten Dateien werden beim nächsten Neustart entschlüsselt.
- **Nicht alle Dateien konnten entschlüsselt werden** – Die Entschlüsselungssuche ist abgeschlossen, aber es konnten nicht alle Dateien entschlüsselt werden. Dieser Status kann folgende Gründe haben:
  - Die gesperrten Dateien wurden nicht für die Entschlüsselung vorgesehen, weil sie entweder zu groß sind oder ein Fehler bei der Anfrage nach ihrer Freigabe auftrat.
  - Während der Entschlüsselung der Dateien trat ein Eingabe-/Ausgabefehler auf.
  - Die Dateien konnten nicht richtliniengemäß entschlüsselt werden.
  - Die Dateien waren zur Verschlüsselung markiert.
  - Während der Entschlüsselungssuche trat ein Fehler auf.
  - In sämtlichen Fällen wird eine Protokolldatei erstellt, sofern mindestens LogVerbosity=2 eingestellt ist (und die Protokollierung aktiviert wurde). Zur Fehlerbehebung sollten Sie die Ausführlichkeitsstufe auf 2 einstellen (LogVerbosity=2) und den Encryption Removal Agent-Dienst neu starten, um eine weitere Entschlüsselungssuche zu erzwingen. Weitere Anweisungen finden Sie unter Encryption Removal Agent-Protokolldatei erstellen (optional).
- **Vollständig** – Die Entschlüsselungssuche wurde abgeschlossen. Der Dienst, die ausführbare Datei, der Treiber und die ausführbare Treiberdatei werden beim nächsten Neustart des Computers gelöscht.

Advanced Threat Prevention – Fehlerbehebung

Produktcode mit Windows PowerShell ermitteln

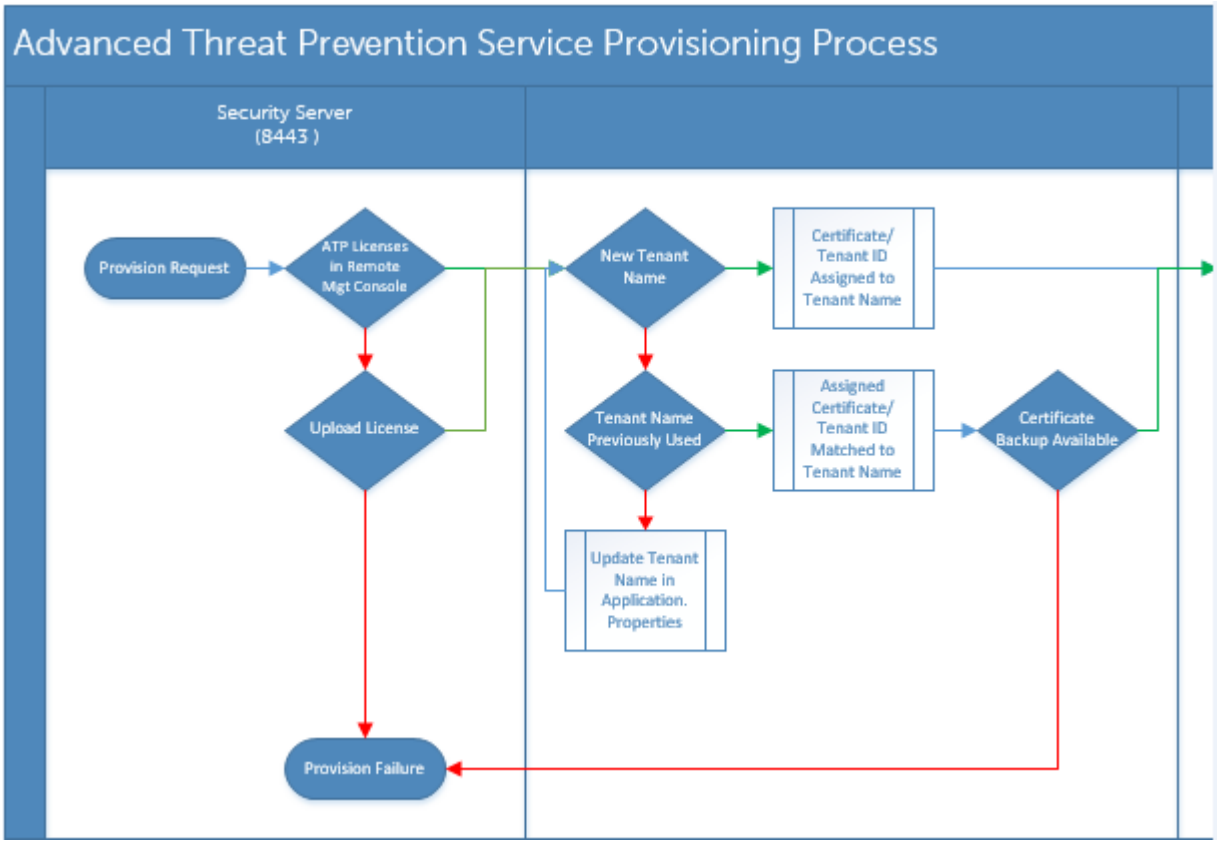
- Sie können den Produktschlüssel über dieses Verfahren leicht identifizieren, wenn er sich in der Zukunft ändern sollte.

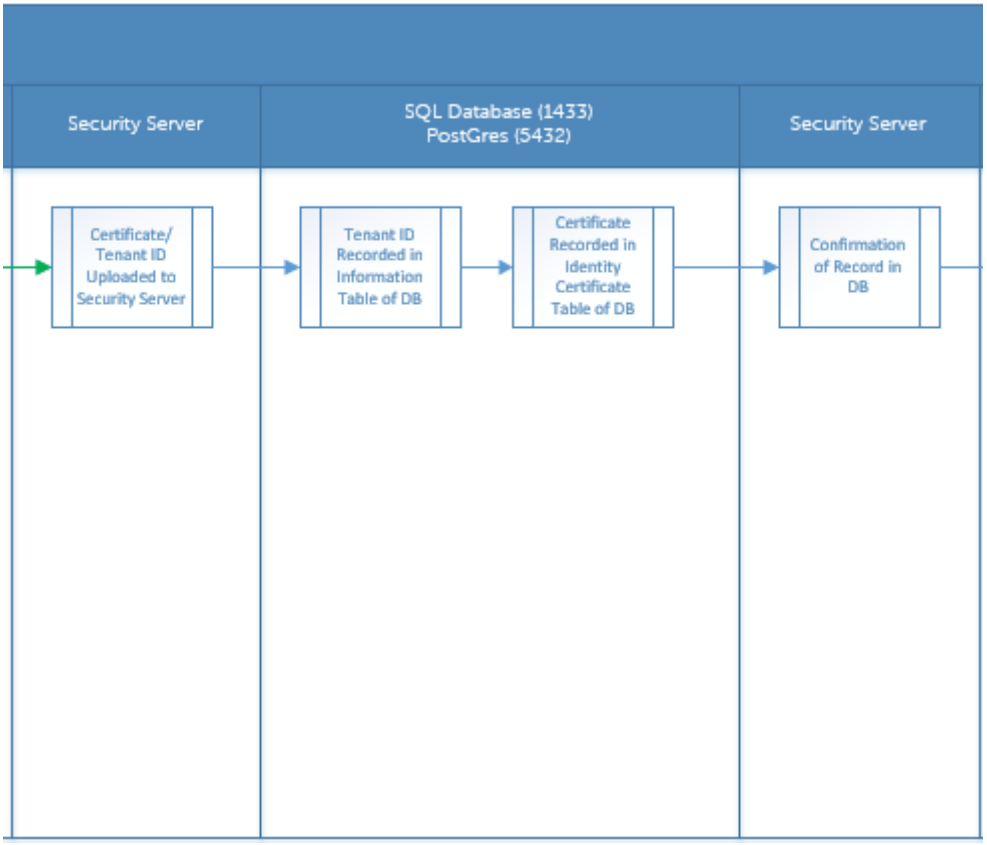
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

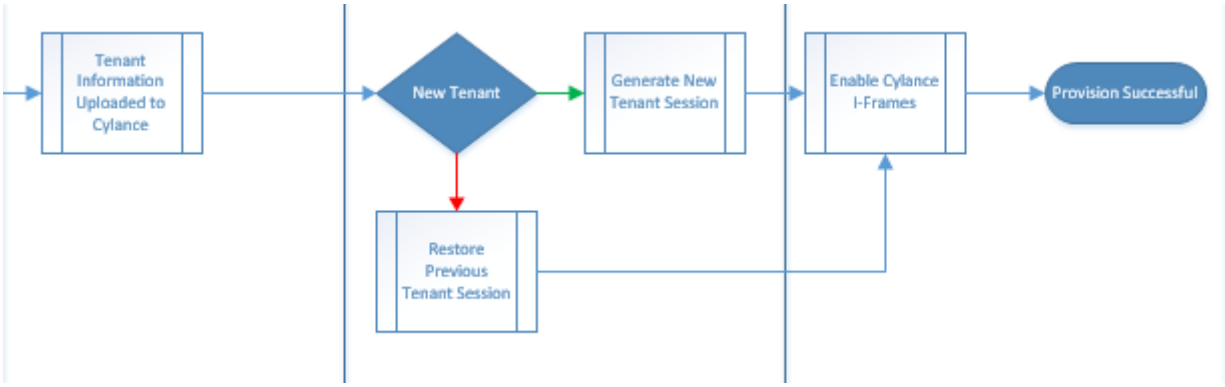
  Der vollständige Pfad und der MSI-Dateiname (der konvertierte HEX-Namen der Datei) werden ausgegeben.

Bereitstellung von Advanced Threat Prevention und Agentenkommunikation

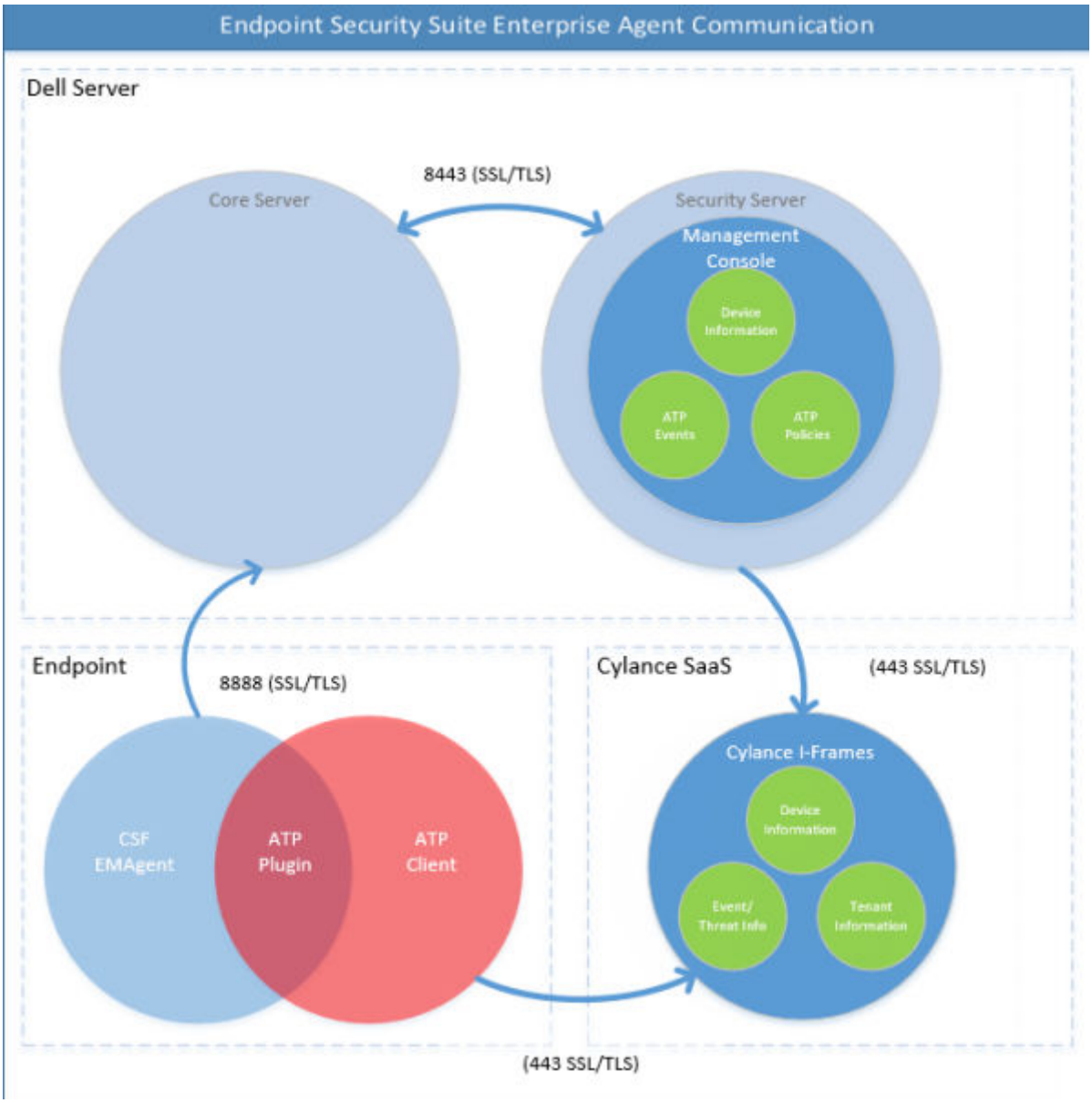
Die folgenden Diagramme veranschaulichen die Bereitstellung des Advanced Threat Prevention Dienstes.


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB

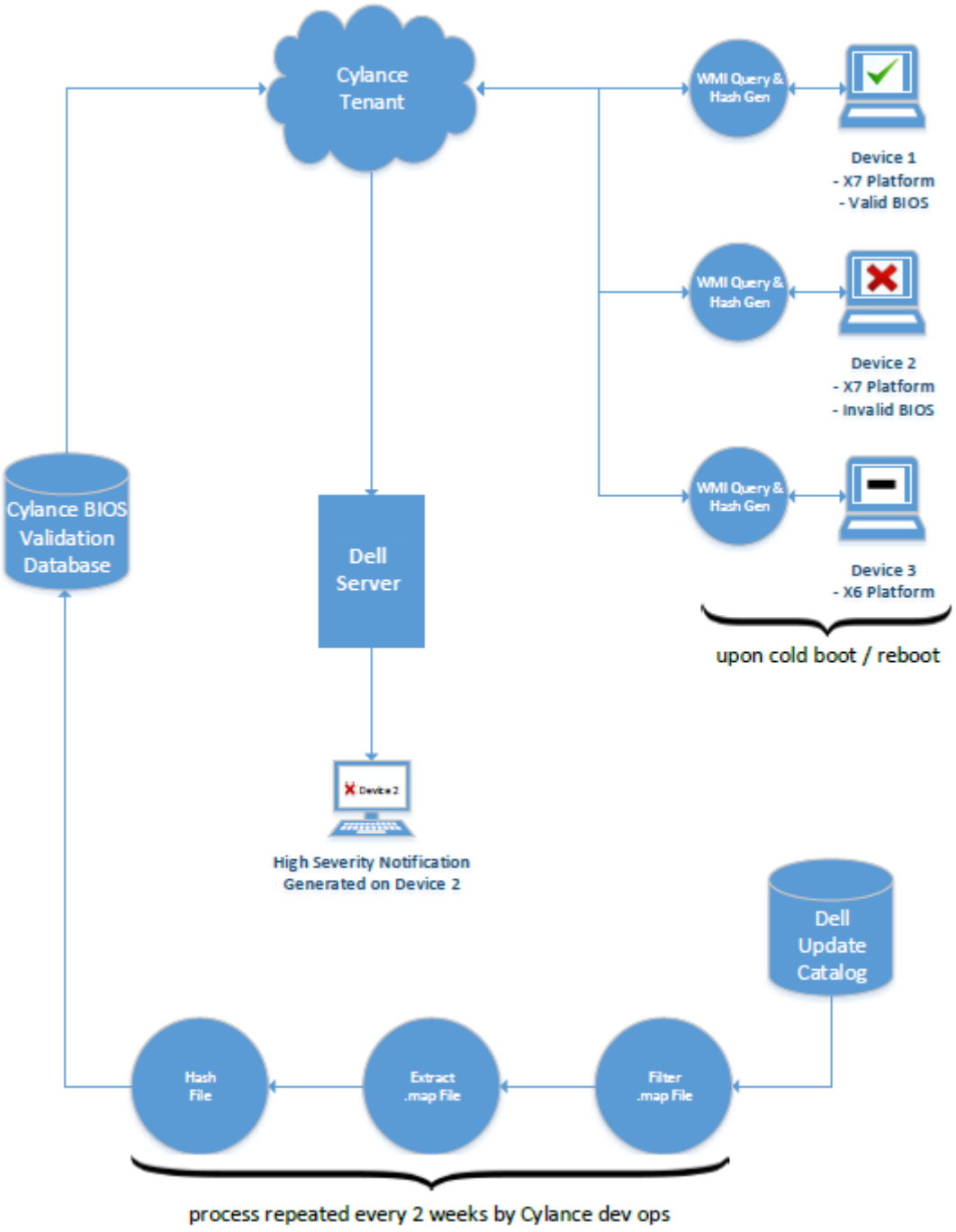


Das folgende Diagramm veranschaulicht die Agentenkommunikation für Advanced Threat Prevention.



Integritätsüberprüfung des BIOS-Abbildes

Das folgende Diagramm veranschaulicht die Integritätsüberprüfung des BIOS-Abbildes. Eine Liste der Dell Computermodelle, auf denen die Integritätsüberprüfung des BIOS-Abbildes unterstützt wird, finden Sie unter Anforderungen – Integritätsüberprüfung des BIOS-Abbilds.



SED-Fehlerbehebung

Den ersten Zugriffscode verwenden

- Diese Richtlinie wird zur Anmeldung bei einem Computer verwendet, wenn kein Netzwerkzugriff verfügbar und dadurch auch der Zugriff auf den Dell Server und Active Directory (AD) nicht möglich ist. Verwenden Sie die Richtlinie *Erster Zugriffscode* nur, wenn es keine andere Möglichkeit gibt. Dell rät von dieser Vorgehensweise für die Anmeldung ausdrücklich ab. Die Verwendung der Richtlinie *Erster Zugriffscode* bietet nicht dasselbe Maß an Sicherheit wie die normale Authentifizierungsmethode mit Benutzernamen, Domäne und Kennwort.

  Neben der geringeren Sicherheit des Anmeldeverfahrens wird bei der Aktivierung eines Benutzers über *Erster Zugriffscode* kein entsprechender Eintrag des Benutzers, der auf dem Computer aktiviert wird, auf dem Dell Server erstellt. Das bedeutet,

dass kein Antwortcode vom Dell Server erstellt werden kann, wenn der Benutzer das Kennwort falsch eingibt oder die Selbsthilfe-Fragen nicht beantworten kann.

- Der *erste Zugriffscode* kann nur **ein** Mal – unmittelbar nach der Aktivierung – verwendet werden. Nach der Anmeldung eines Benutzers steht der *erste Zugriffscode* nicht mehr zur Verfügung. Die erste Domänenanmeldung nach der Eingabe des *ersten Zugriffscodes* wird zwischengespeichert, und das Eingabefeld für den *ersten Zugriffscode* wird nicht mehr angezeigt.
- Der *Erste Zugriffscode* wird **nur** unter den folgenden Umständen angezeigt:
  - Ein Benutzer wurde nicht in der PBA aktiviert.
  - Der Client hat keine Verbindung zum Netzwerk oder Dell Server.

Ersten Zugriffscode verwenden

1. Richten Sie in der Verwaltungskonsole einen Wert für den **Ersten Zugriffscode** ein.
2. Speichern und aktivieren Sie die Richtlinie.
3. Starten Sie den lokalen Computer.
4. Geben Sie den **ersten Zugriffscode** ein, wenn der Bildschirm „Zugriffscode“ angezeigt wird.
5. Klicken Sie auf den **blauen Pfeil**.
6. Klicken Sie auf **OK**, wenn der Bildschirm mit „Rechtshinweise“ angezeigt wird.
7. Melden Sie sich mit den Benutzerdaten für den Computer bei Windows an. Diese Anmeldedaten müssen zur Domäne gehören.
8. Öffnen Sie nach der Anmeldung die Data Security Console und überprüfen Sie, ob der PBA-Benutzer richtig erstellt worden ist.

   Klicken Sie dazu im Menü oben auf **Protokoll**, und suchen Sie nach der Meldung *PBA-Benutzer für <DOMAIN\Username> erstellt*, welche angibt, dass der Vorgang erfolgreich war.
9. Fahren Sie den Computer herunter und starten Sie ihn neu.
10. Geben Sie auf dem Anmeldebildschirm den Benutzernamen, die Domäne und das Kennwort ein, die zuvor für die Anmeldung bei Windows verwendet wurden.

    Dabei muss das gleiche Benutzernamen-Format wie bei der Erstellung des PBA-Benutzers verwendet werden. Wenn Sie also das Format „DOMÄNE/Benutzername“ verwendet haben, müssen Sie DOMÄNE/Benutzername für den Benutzernamen eingeben.
11. Klicken Sie auf **Anmelden**, wenn der Bildschirm „Rechtshinweise“ angezeigt wird.

    Windows wird gestartet, und der Computer kann wie gewohnt verwendet werden.

PBA-Protokolldatei für die Fehlerbehebung erstellen

- Zur Behebung von PBA-Fehlern ist u. U. eine PBA-Protokolldatei erforderlich, beispielsweise in den folgenden Fällen:
  - Das Symbol der Netzwerkverbindung wird nicht angezeigt, obwohl Sie sicher sind, dass eine Netzwerkverbindung besteht. Die Protokolldatei enthält DHCP-Informationen zur Behebung des Problems.
  - Das Symbol der Dell Serververbindung wird nicht angezeigt. Die Protokolldatei enthält Informationen, die eine Diagnose von Problemen mit der Verbindung erleichtern.
  - Die Authentifizierung schlägt trotz Eingabe der richtigen Anmeldedaten fehl. Die Protokolldatei und die Serverprotokolle für Dell Server enthalten Informationen, die eine Diagnose des Problems erleichtern.

Protokolle während des PBA-Starts (Alt-PBA) erfassen

1. Legen Sie im Stammverzeichnis eines USB-Laufwerks einen Ordner namens **`\CredantSED`** an.
2. Erstellen Sie im Ordner **`\CredantSED`** eine Datei namens „actions.txt“.
3. Fügen Sie in actions.txt die folgende Zeile ein:

   ```
   get logs
   ```
4. Speichern und schließen Sie die Datei.

   Schließen Sie das USB-Laufwerk nicht an den ausgeschalteten Computer an. Falls das USB-Laufwerk bereits an den ausgeschalteten Computer angeschlossen ist entfernen Sie es bitte.
5. Schalten Sie den Computer ein, um das Problem zu reproduzieren. Schließen Sie das USB-Laufwerk an den Computer an, von dem die Protokolle während dieses Schritts erfasst werden sollen.
6. Lassen Sie das USB-Laufwerk fünf bis zehn Sekunden lang angeschlossen und entfernen Sie es dann.

Im Ordner **\CredantSED** wird die Datei „credpbaenv.tgz“ mit den erforderlichen Protokollen erstellt.

Protokolle während des PBA-Starts (UEFI-PBA) erfassen

1. Erstellen Sie eine Datei mit der Bezeichnung **PBAErr.log** im Stammverzeichnis des USB-Laufwerks.
2. Setzen Sie das USB-Laufwerk **vor dem** Einschalten des Computers ein.
3. Entfernen Sie das USB-Laufwerk **nach** der Reproduzierung des Problems in Bezug auf die Erforderlichkeit der Protokolle.

Die Datei „PBAErr.log“ wird in Echtzeit aktualisiert und geschrieben.

Dell ControlVault-Treiber

Aktualisieren von Treibern und Firmware für Dell ControlVault

- Die auf Dell-Computern werkseitig installierte(n) Treiber und Firmware für Dell ControlVault sind nicht mehr aktuell und müssen anhand des folgenden Verfahrens in der angegebenen Reihenfolge aktualisiert werden.
- Wenn Sie während der Client-Installation aufgefordert werden, das Installationsprogramm zu schließen, um die Dell ControlVault-Treiber zu installieren, können Sie diese Meldung ignorieren und die Client-Installation fortsetzen. Die Dell ControlVault-Treiber (und die zugehörige Firmware) können nach dem erfolgreichen Abschluss der Client-Installation aktualisiert werden.

Herunterladen der aktuellen Treiber

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

Installieren des Dell ControlVault-Treibers

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

   ANMERKUNG:

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

3. Klicken Sie zum Fortsetzen des Vorgangs auf **Weiter**.
4. Klicken Sie auf **OK**, um die Treiberdateien in den Standardordner `C:\Dell\Drivers\<New Folder>` zu entpacken.
5. Klicken Sie auf **Ja**, um die Erstellung eines neuen Ordners zu genehmigen.
6. Klicken Sie auf **OK**, wenn die Nachricht angezeigt wird, dass die Dateien erfolgreich entpackt wurden.
7. Nach dem Entpacken wird der Ordner angezeigt, der die entpackten Dateien enthält. Ist dies nicht der Fall, gehen Sie zu dem Ordner, in den Sie die Dateien entpackt haben. Der Ordner ist als **JW22F** bezeichnet
8. Doppelklicken Sie auf die Datei **CVHCI64.MSI**, um das Treiberinstallationsprogramm zu starten. [Die Datei **CVHCI64.MSI** in diesem Beispiel bezieht sich auf ein 64-Bit-System. Bei einem 32-Bit-System wählen Sie die Datei CVHCI32.MSI aus].
9. Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.
10. Klicken Sie auf **Weiter** für die Installation im Standardverzeichnis von `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. Wählen Sie die Option **Abschließen** aus, und klicken Sie auf **Weiter**.
12. Klicken Sie auf **Installieren**, um mit der Installation der Treiber zu beginnen.

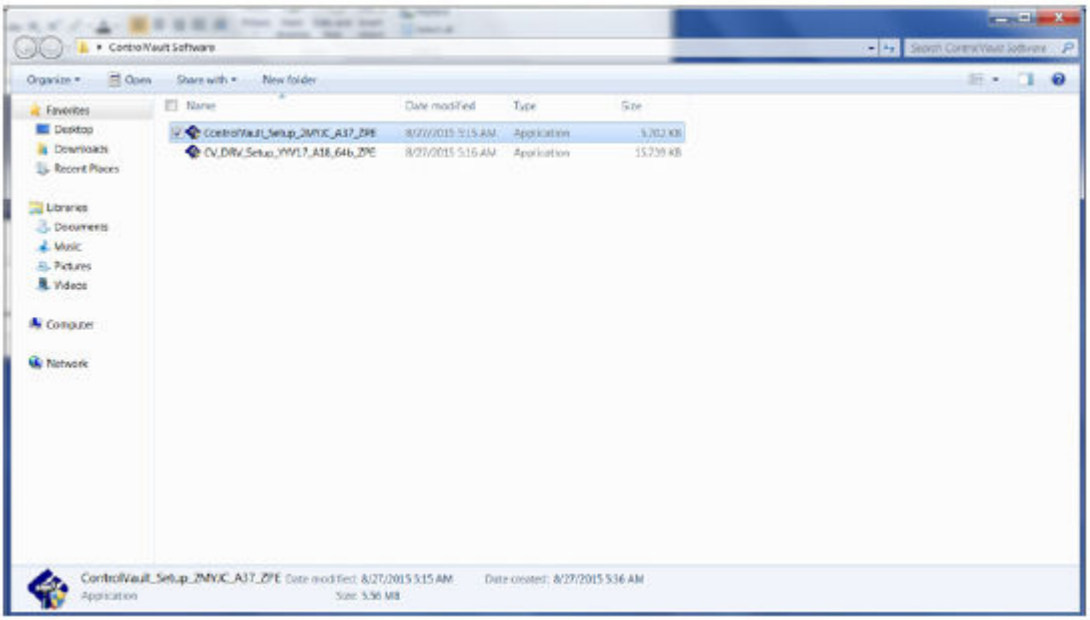
13. Aktivieren Sie optional das Kontrollkästchen, um die Protokolldatei für das Installationsprogramm anzuzeigen. Klicken Sie zum Beenden des Assistenten auf **Fertig stellen**.

Überprüfen der Treiberinstallation

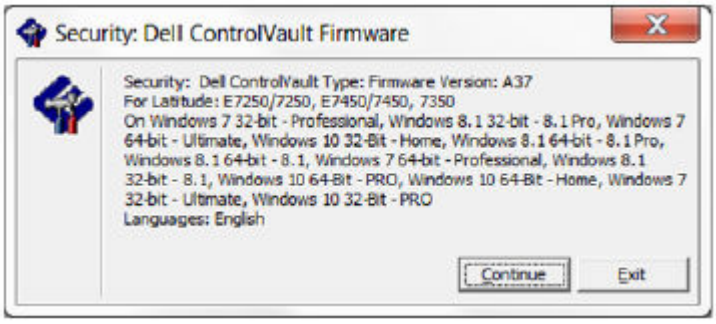
- Der Device Manager zeigt je nach Betriebssystem und Hardwarekonfiguration ein Dell ControlVault-Gerät (sowie weitere Geräte) an.

Installieren der Dell ControlVault-Firmware

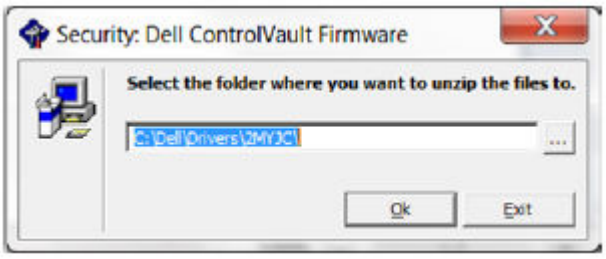
1. Gehen Sie zu dem Ordner, in den Sie die Firmware-Installationsdatei abgelegt haben.



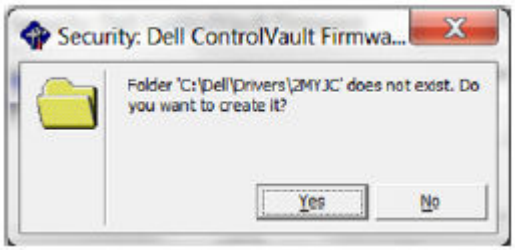
2. Doppelklicken Sie auf die Dell ControlVault-Firmware, um die selbstextrahierende ausführbare Datei aufzurufen.
3. Klicken Sie zum Fortsetzen des Vorgangs auf **Weiter**.



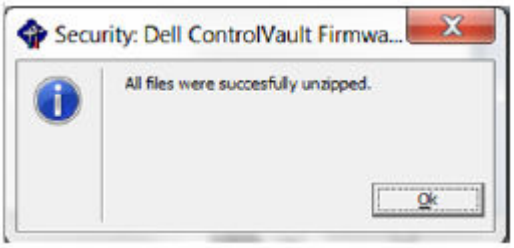
4. Klicken Sie auf **OK**, um die Treiberdateien in den Standardordner `C:\Dell\Drivers\<New Folder>` zu entpacken.



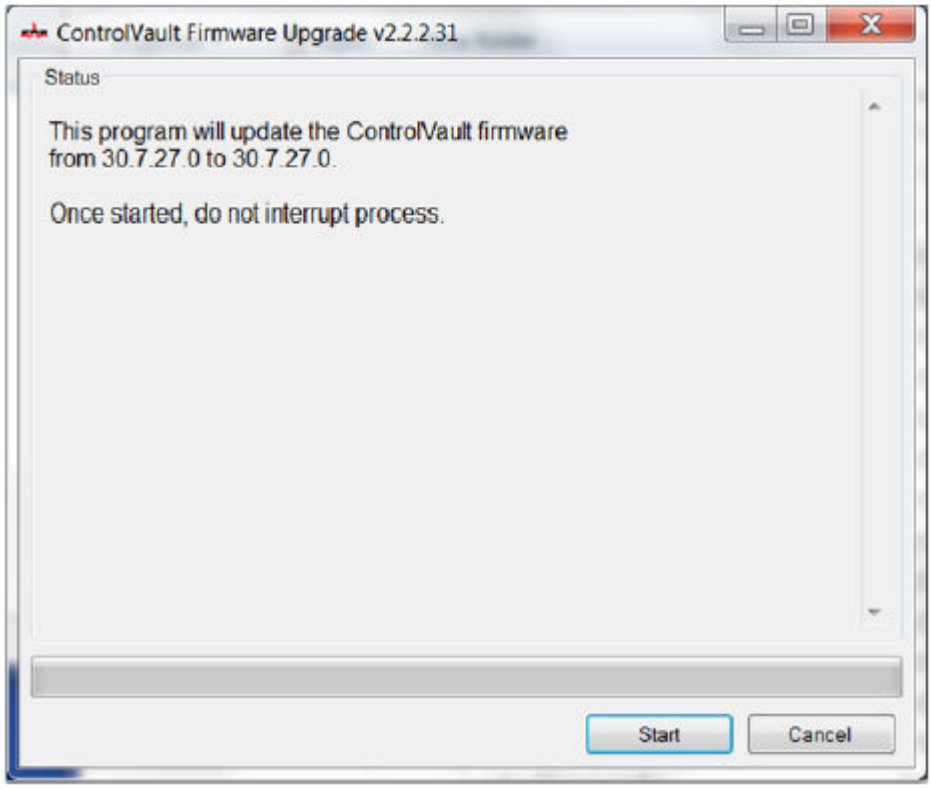
5. Klicken Sie auf **Ja**, um die Erstellung eines neuen Ordners zu genehmigen.



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



7. Nach dem Entpacken wird der Ordner angezeigt, der die entpackten Dateien enthält. Ist dies nicht der Fall, gehen Sie zu dem Ordner, in den Sie die Dateien entpackt haben. Wählen Sie den Ordner **Firmware** aus.
8. Doppelklicken Sie auf die Datei **ushupgrade.exe**, um das Firmware-Installationsprogramm zu starten.
9. Klicken Sie zum Starten der Firmware auf **Start**.



ANMERKUNG:

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

Es werden verschiedene Statusmeldungen angezeigt.

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

    Das Update der Treiber und der Firmware für Dell ControlVault ist damit abgeschlossen.

UEFI Computers

Fehlerbehebung bei Problemen mit der Netzwerkverbindung

- Damit die Preboot-Authentifizierung auf einem Computer mit UEFI-Firmware erfolgreich verläuft, muss der PBA-Modus mit Netzwerkkonnektivität ausgerüstet sein. Auf Computern mit UEFI-Firmware ist standardmäßig erst dann Netzwerkkonnektivität verfügbar, wenn das Betriebssystem geladen wurde. Dies geschieht in der Regel nach dem PBA-Modus. Wenn das in Konfiguration für UEFI-Computer vor der Installation beschriebene Verfahren auf dem Computer erfolgreich abgeschlossen und korrekt konfiguriert wurde, wird das Netzwerkverbindungssymbol im Preboot-Authentifizierungsbildschirm angezeigt, wenn der Computer mit dem Netzwerk verbunden ist.

- Falls das Symbol für die Netzwerkverbindung während der Preboot-Authentifizierung trotzdem nicht angezeigt wird, überprüfen Sie, ob das Netzkabel ordnungsgemäß an den Computer angeschlossen ist. Falls das Kabel nicht angeschlossen oder locker war, starten Sie den Computer neu, um einen Neustart des PBA-Modus zu bewirken.

TPM und BitLocker

Fehlercodes für TPM und BitLocker

Konstante/Wert	Beschreibung
TPM_E_ERROR_MASK 0x80280000	Dies ist eine Fehlermaske, die zum Konvertieren der TPM-Hardwarefehler in Win-Fehler verwendet wird.
TPM_E_AUTHFAIL 0x80280001	Authentifizierung fehlgeschlagen
TPM_E_BADINDEX 0x80280002	Der Index für ein PCR, DIR oder ein anderes Register ist falsch.
TPM_E_BAD_PARAMETER 0x80280003	Ein oder mehrere Parameter sind falsch.
TPM_E_AUDITFAILURE 0x80280004	Ein Vorgang wurde erfolgreich abgeschlossen, aber beim Überwachen des Vorgangs ist ein Fehler aufgetreten.
TPM_E_CLEAR_DISABLED 0x80280005	Das Flag zum Deaktivieren des Löschens ist gesetzt, und für alle Löschvorgänge ist jetzt ein physikalischer Zugriff erforderlich.
TPM_E_DEACTIVATED 0x80280006	Aktivieren Sie das TPM.
TPM_E_DISABLED 0x80280007	Aktivieren Sie das TPM.
TPM_E_DISABLED_CMD 0x80280008	Der Zielbefehl wurde deaktiviert.

Konstante/Wert	Beschreibung
TPM_E_FAIL 0x80280009	Der Vorgang ist fehlgeschlagen.
TPM_E_BAD_ORDINAL 0x8028000A	Die Ordnungszahl war unbekannt oder nicht konsistent.
TPM_E_INSTALL_DISABLED 0x8028000B	Die Option zum Installieren eines Besitzers ist deaktiviert.
TPM_E_INVALID_KEYHANDLE 0x8028000C	Das Schlüsselhandle kann nicht interpretiert werden.
TPM_E_KEYNOTFOUND 0x8028000D	Das Schlüsselhandle zeigt auf einen ungültigen Schlüssel.
TPM_E_INAPPROPRIATE_ENC 0x8028000E	Unzulässiges Verschlüsselungsschema.
TPM_E_MIGRATEFAIL 0x8028000F	Fehler bei der Migrationsautorisierung.
TPM_E_INVALID_PCR_INFO 0x80280010	Die PCR-Informationen konnten nicht interpretiert werden.
TPM_E_NOSPACE 0x80280011	Kein Platz zum Laden des Schlüssels.
TPM_E_NOSRK 0x80280012	Es ist kein Speicherstammschlüsselsatz (SRK) vorhanden.
TPM_E_NOTSEALED_BLOB 0x80280013	Ein verschlüsseltes BLOB ist ungültig oder wurde nicht mit diesem TPM erstellt.
TPM_E_OWNER_SET 0x80280014	Das TPM verfügt bereits über einen Besitzer.
TPM_E_RESOURCES 0x80280015	Das TPM verfügt nicht über ausreichend interne Ressourcen, um die angeforderte Aktion auszuführen.
TPM_E_SHORTRANDOM 0x80280016	Eine zufällige Zeichenfolge war zu kurz.
TPM_E_SIZE 0x80280017	Das TPM verfügt nicht über ausreichend Speicherplatz, um den Vorgang auszuführen.
TPM_E_WRONGPCRVAL 0x80280018	Der benannte PCR-Wert stimmt nicht mit dem aktuellen PCR-Wert überein.
TPM_E_BAD_PARAM_SIZE 0x80280019	Das paramSize-Argument für den Befehl hat einen falschen Wert.

Konstante/Wert	Beschreibung
TPM_E_SHA_THREAD 0x8028001A	Es ist kein SHA-1-Thread vorhanden.
TPM_E_SHA_ERROR 0x8028001B	Die Berechnung kann nicht fortgesetzt werden, da beim vorhandenen SHA-1-Thread bereits ein Fehler aufgetreten ist.
TPM_E_FAILEDSELFTEST 0x8028001C	Vom TPM-Hardwaregerät wurde beim internen Selbsttest ein Fehler gemeldet. Starten Sie den Computer neu, um das Problem zu beheben. Falls das Problem weiterhin besteht, muss ggf. die TPM-Hardware oder die Hauptplatine ersetzt werden.
TPM_E_AUTH2FAIL 0x8028001D	Die Autorisierung für den zweiten Schlüssel in einer 2-Schlüsselfunktion war nicht erfolgreich.
TPM_E_BADTAG 0x8028001E	Der für einen Befehl gesendete Tagwert ist ungültig.
TPM_E_IOERROR 0x8028001F	Beim Übermitteln von Informationen an das TPM ist ein E/A-Fehler aufgetreten.
TPM_E_ENCRYPT_ERROR 0x80280020	Beim Verschlüsselungsprozess ist ein Problem aufgetreten.
TPM_E_DECRYPT_ERROR 0x80280021	Der Entschlüsselungsprozess wurde nicht abgeschlossen.
TPM_E_INVALID_AUTHHANDLE 0x80280022	Ein ungültiges Handle wurde verwendet.
TPM_E_NO_ENDORSEMENT 0x80280023	Für das TPM ist kein Endorsement Key (EK) installiert.
TPM_E_INVALID_KEYUSAGE 0x80280024	Die Verwendung eines Schlüssels ist unzulässig.
TPM_E_WRONG_ENTITYTYPE 0x80280025	Der festgelegte Einheitstyp ist nicht zulässig.
TPM_E_INVALID_POSTINIT 0x80280026	Der Befehl wurde relativ zu TPM_Init und einem nachfolgenden TPM_Startup in der falschen Reihenfolge empfangen.
TPM_E_INAPPROPRIATE_SIG 0x80280027	Signierte Daten können keine zusätzlichen DER-Informationen enthalten.
TPM_E_BAD_KEY_PROPERTY 0x80280028	Die Schlüsseleigenschaften in TPM_KEY_PARMs werden von diesem TPM nicht unterstützt.
TPM_E_BAD_MIGRATION 0x80280029	Die Migrationseigenschaften dieses Schlüssels sind falsch.

Konstante/Wert	Beschreibung
TPM_E_BAD_SCHEME 0x8028002A	Die Signatur oder das Verschlüsselungsschema für diesen Schlüssel ist falsch oder in dieser Situation nicht zulässig.
TPM_E_BAD_DATASIZE 0x8028002B	Die Größe des Datenparameters (oder BLOB-Parameters) ist unzulässig oder nicht mit dem Schlüssel konsistent, auf den verwiesen wird.
TPM_E_BAD_MODE 0x8028002C	Ein Modusparameter ist ungültig, z. B. capArea oder subCapArea für TPM_GetCapability, phsicalPresence-Parameter für TPM_PhysicalPresence oder migrationType für TPM_CreateMigrationBlob.
TPM_E_BAD_PRESENCE 0x8028002D	Die physicalPresence-Bits oder die physicalPresenceLock-Bits haben den falschen Wert.
TPM_E_BAD_VERSION 0x8028002E	Das TPM kann diese Version der Funktion nicht ausführen.
TPM_E_NO_WRAP_TRANSPORT 0x8028002F	Das TPM berücksichtigt keine eingeschlossenen Transportsitzungen.
TPM_E_AUDITFAIL_UNSUCCESSFUL 0x80280030	Bei der TPM-Überwachungskonstruktion ist ein Fehler aufgetreten, und der zugrunde liegende Befehl hat auch einen Fehlercode zurückgegeben.
TPM_E_AUDITFAIL_SUCCESSFUL 0x80280031	Bei der TPM-Überwachungskonstruktion ist ein Fehler aufgetreten, und der zugrunde liegende Befehl war erfolgreich.
TPM_E_NOTRESETABLE 0x80280032	Es wird versucht, ein PCR-Register zurückzusetzen, das nicht über ein Resettable-Attribut verfügt.
TPM_E_NOTLOCAL 0x80280033	Es wird versucht, ein PCR-Register zurückzusetzen, das erfordert, dass Ort und Ortsänderer nicht Teil eines Befehlstransports sind.
TPM_E_BAD_TYPE 0x80280034	Das BLOB zum Erstellen der Identität wurde nicht richtig typisiert.
TPM_E_INVALID_RESOURCE 0x80280035	Beim Speichern des Kontexts entsprach der identifizierte Ressourcentyp nicht der tatsächlichen Ressource.
TPM_E_NOTFIPS 0x80280036	Das TPM versucht, einen Befehl auszuführen, der nur im FIPS-Modus verfügbar ist.
TPM_E_INVALID_FAMILY 0x80280037	Der Befehl versucht, eine ungültige Familien-ID zu verwenden.
TPM_E_NO_NV_PERMISSION 0x80280038	Die Berechtigung zum Ändern des permanenten Speichers ist nicht verfügbar.
TPM_E_REQUIRES_SIGN 0x80280039	Der Vorgang erfordert einen signierten Befehl.
TPM_E_KEY_NOTSUPPORTED	Falscher Vorgang zum Laden eines permanenten Schlüssels.

Konstante/Wert	Beschreibung
0x8028003A	
TPM_E_AUTH_CONFLICT 0x8028003B	Das BLOB "NV_LoadKey" erfordert eine Besitzerautorisierung und eine BLOB-Autorisierung.
TPM_E_AREA_LOCKED 0x8028003C	Der permanente Bereich ist gesperrt und nicht beschreibbar.
TPM_E_BAD_LOCALITY 0x8028003D	Der Ort für den Vorgang ist falsch.
TPM_E_READ_ONLY 0x8028003E	Der permanente Bereich ist schreibgeschützt und daher nicht beschreibbar.
TPM_E_PER_NOWRITE 0x8028003F	Der permanente Bereich ist nicht schreibgeschützt.
TPM_E_FAMILYCOUNT 0x80280040	Fehlende Übereinstimmung beim Familienanzahlwert.
TPM_E_WRITE_LOCKED 0x80280041	Der permanente Bereich wurde bereits beschrieben.
TPM_E_BAD_ATTRIBUTES 0x80280042	Konflikt bei den Attributen des permanenten Bereichs.
TPM_E_INVALID_STRUCTURE 0x80280043	Das Strukturtag und die Version sind ungültig oder inkonsistent.
TPM_E_KEY_OWNER_CONTROL 0x80280044	Der Schlüssel wird vom TPM-Besitzer kontrolliert und kann nur vom TPM-Besitzer entfernt werden.
TPM_E_BAD_COUNTER 0x80280045	Das Zählerhandle ist ungültig.
TPM_E_NOT_FULLWRITE 0x80280046	Beim Schreibvorgang wird nicht der gesamte Bereich beschrieben.
TPM_E_CONTEXT_GAP 0x80280047	Die Lücke zwischen den gespeicherten Kontextanzahlwerten ist zu groß.
TPM_E_MAXNVWRITES 0x80280048	Die maximale Anzahl von permanenten Schreibvorgängen ohne Besitzer wurde überschritten.
TPM_E_NOOPERATOR 0x80280049	Es ist kein AuthData-Operatorwert festgelegt.
TPM_E_RESOURCEMISSING 0x8028004A	Die Ressource, auf die der Kontext zeigt, ist nicht geladen.
TPM_E_DELEGATE_LOCK	Die Delegatverwaltung ist gesperrt.

Konstante/Wert	Beschreibung
0x8028004B	
TPM_E_DELEGATE_FAMILY 0x8028004C	Es wurde versucht, eine andere als die delegierte Familie zu verwalten.
TPM_E_DELEGATE_ADMIN 0x8028004D	Die Verwaltung der Delegierungstabelle ist nicht aktiviert.
TPM_E_TRANSPORT_NOTEXCLUSIVE 0x8028004E	Es wurde ein Befehl außerhalb einer exklusiven Transportsitzung ausgeführt.
TPM_E_OWNER_CONTROL 0x8028004F	Es wird versucht, einen kontrollierten Schlüssel ohne Besitzer im Kontext zu speichern.
TPM_E_DAA_RESOURCES 0x80280050	Der DAA-Befehl hat keine verfügbaren Ressourcen zum Ausführen des Befehls.
TPM_E_DAA_INPUT_DATA0 0x80280051	Fehler bei der Konsistenzprüfung des DAA-Parameters "inputData0".
TPM_E_DAA_INPUT_DATA1 0x80280052	Fehler bei der Konsistenzprüfung des DAA-Parameters "inputData1".
TPM_E_DAA_ISSUER_SETTINGS 0x80280053	Fehler bei der Konsistenzprüfung für DAA_issuerSettings.
TPM_E_DAA_TPM_SETTINGS 0x80280054	Fehler bei der Konsistenzprüfung für DAA_tpmSpecific.
TPM_E_DAA_STAGE 0x80280055	Der vom gesendeten DAA-Befehl angegebene atomare Prozess ist nicht der erwartete Prozess.
TPM_E_DAA_ISSUER_VALIDITY 0x80280056	Die Validitätsprüfung des Herausgebers hat eine Inkonsistenz ergeben.
TPM_E_DAA_WRONG_W 0x80280057	Eine Konsistenzprüfung auf W ist fehlgeschlagen.
TPM_E_BAD_HANDLE 0x80280058	Das Handle ist ungültig.
TPM_E_BAD_DELEGATE 0x80280059	Die Delegierung ist falsch.
TPM_E_BADCONTEXT 0x8028005A	Das Kontext-BLOB ist ungültig.
TPM_E_TOOMANYCONTEXTS 0x8028005B	Das TPM enthält zu viele Kontexte.
TPM_E_MA_TICKET_SIGNATURE	Fehler bei der Überprüfung der Migrationsautoritätssignatur.

Konstante/Wert	Beschreibung
0x8028005C	
TPM_E_MA_DESTINATION 0x8028005D	Das Migrationsziel wurde nicht authentifiziert.
TPM_E_MA_SOURCE 0x8028005E	Die Migrationsquelle ist falsch.
TPM_E_MA_AUTHORITY 0x8028005F	Die Migrationsautorität ist falsch.
TPM_E_PERMANENTEK 0x80280061	Es wurde versucht, den EK zu widerrufen, der EK kann jedoch nicht widerrufen werden.
TPM_E_BAD_SIGNATURE 0x80280062	Die Signatur des CMK-Tickets ist ungültig.
TPM_E_NOCONTEXTSPACE 0x80280063	In der Kontextliste ist kein Platz für weitere Kontexte verfügbar.
TPM_E_COMMAND_BLOCKED 0x80280400	Der Befehl wurde geblockt.
TPM_E_INVALID_HANDLE 0x80280401	Das angegebene Handle wurde nicht gefunden.
TPM_E_DUPLICATE_VHANDLE 0x80280402	Das TPM hat ein doppeltes Handle zurückgegeben, und der Befehl muss neu gesendet werden.
TPM_E_EMBEDDED_COMMAND_BLOCKED 0x80280403	Der Befehl im Transport wurde blockiert.
TPM_E_EMBEDDED_COMMAND_UNSUPPORTED 0x80280404	Der Befehl im Transport wird nicht unterstützt.
TPM_E_RETRY 0x80280800	Das TPM ist zu ausgelastet, um sofort auf den Befehl zu reagieren, aber der Befehl kann zu einem späteren Zeitpunkt erneut gesendet werden.
TPM_E_NEEDS_SELFTEST 0x80280801	SelfTestFull wurde nicht ausgeführt.
TPM_E_DOING_SELFTEST 0x80280802	Das TPM führt gerade einen vollständigen Selbsttest aus.
TPM_E_DEFEND_LOCK_RUNNING 0x80280803	Das TPM wehrt Verzeichnisangriffe ab und befindet sich in einer Zeitüberschreitungsperiode.
TBS_E_INTERNAL_ERROR 0x80284001	Ein interner Softwarefehler ist aufgetreten.
TBS_E_BAD_PARAMETER	Mindestens ein Eingabeparameter ist ungültig.

Konstante/Wert	Beschreibung
0x80284002	
TBS_E_INVALID_OUTPUT_POINTER 0x80284003	Ein angegebener Ausgabezeiger ist ungültig.
TBS_E_INVALID_CONTEXT 0x80284004	Das angegebene Kontexthandle bezieht sich nicht auf einen gültigen Kontext.
TBS_E_INSUFFICIENT_BUFFER 0x80284005	Der angegebene Ausgabepuffer ist zu klein.
TBS_E_IOERROR 0x80284006	Bei der Kommunikation mit TPM ist ein Fehler aufgetreten.
TBS_E_INVALID_CONTEXT_PARAM 0x80284007	Mindestens ein Kontextparameter ist ungültig.
TBS_E_SERVICE_NOT_RUNNING 0x80284008	Der TBS-Dienst wird nicht ausgeführt und konnte nicht gestartet werden.
TBS_E_TOO_MANY_TBS_CONTEXTS 0x80284009	Ein neuer Kontext konnte nicht erstellt werden, das bereits zu viele offene Kontexte vorhanden sind.
TBS_E_TOO_MANY_RESOURCES 0x8028400A	Eine neue virtuelle Ressource konnte nicht erstellt werden, da bereits zu viele offene virtuelle Ressource vorhanden sind.
TBS_E_SERVICE_START_PENDING 0x8028400B	Der TBS-Dienst wurde gestartet, wird jedoch noch nicht ausgeführt.
TBS_E_PPI_NOT_SUPPORTED 0x8028400C	Die physikalische Anwesenheitsschnittstelle wird nicht unterstützt.
TBS_E_COMMAND_CANCELED 0x8028400D	Der Befehl wurde abgebrochen.
TBS_E_BUFFER_TOO_LARGE 0x8028400E	Der Eingabe- oder Ausgabepuffer ist zu groß.
TBS_E_TPM_NOT_FOUND 0x8028400F	Auf diesem Computer wurde kein kompatibles TPM-Sicherheitsgerät gefunden.
TBS_E_SERVICE_DISABLED 0x80284010	Der TBS-Dienst wurde deaktiviert.
TBS_E_NO_EVENT_LOG 0x80284011	Es ist kein TCG-Ereignisprotokoll verfügbar.
TBS_E_ACCESS_DENIED 0x80284012	Der Aufrufer verfügt nicht über die erforderlichen Sicherheitsrechte, um den angeforderten Vorgang durchführen zu können.

Konstante/Wert	Beschreibung
TBS_E_PROVISIONING_NOT_ALLOWED 0x80284013	Die TPM-Bereitstellungsaktion ist aufgrund der angegebenen Kennzeichnungen nicht zulässig. Für eine erfolgreiche Bereitstellung muss unter Umständen eine von mehreren verschiedenen Aktionen ausgeführt werden. Die Aktion der TPM-Verwaltungskonsole ("Start" -> "tpm.msc") zur Herstellung der TPM-Bereitschaft ist dabei möglicherweise hilfreich. Weitere Informationen finden Sie in der Dokumentation zur Win32_Tpm WMI-Methode 'Provision'. (Möglicherweise erforderliche Aktionen: Importieren des TPM-Besitzerautorisierungswerts in das System, Aufrufen der WMI-Methode "Win32_Tpm" für die TPM-Bereitstellung und Angeben von TRUE für "ForceClear_Allowed" oder für "PhysicalPresencePrompts_Allowed" (gemäß Angabe durch den Wert, der unter "Zusätzliche Informationen" zurückgegeben wird) oder Ausführen der TPM-Aktivierung im System-BIOS.)
TBS_E_PPI_FUNCTION_UNSUPPORTED 0x80284014	Die angeforderte Methode wird von der physischen Anwesenheitsschnittstelle dieser Firmware nicht unterstützt.
TBS_E_OWNERAUTH_NOT_FOUND 0x80284015	Der angeforderte TPM OwnerAuth-Wert wurde nicht gefunden.
TBS_E_PROVISIONING_INCOMPLETE 0x80284016	Die TPM-Bereitstellung wurde nicht abgeschlossen. Wenn Sie weitere Informationen zum Abschluss der Bereitstellung benötigen, rufen Sie die Win32_Tpm-WMI-Methode für die Bereitstellung des TPM ("Provision") auf, und lesen Sie die angezeigten Informationen.
TPMAPI_E_INVALID_STATE 0x80290100	Die Befehlspuffer befindet sich nicht im richtigen Zustand.
TPMAPI_E_NOT_ENOUGH_DATA 0x80290101	Die Befehlspuffer enthält nicht genügend Daten für die Anforderung.
TPMAPI_E_TOO_MUCH_DATA 0x80290102	Die Befehlspuffer enthält keine weiteren Daten.
TPMAPI_E_INVALID_OUTPUT_POINTER 0x80290103	Mindestens ein Ausgabeparameter ist NULL oder ungültig.
TPMAPI_E_INVALID_PARAMETER 0x80290104	Mindestens ein Eingabeparameter ist ungültig.
TPMAPI_E_OUT_OF_MEMORY 0x80290105	Für diese Anforderung ist nicht genügend Arbeitsspeicher verfügbar.
TPMAPI_E_BUFFER_TOO_SMALL 0x80290106	Der angegebene Puffer war zu klein.
TPMAPI_E_INTERNAL_ERROR 0x80290107	Ein interner Fehler wurde festgestellt.

Konstante/Wert	Beschreibung
TPMAPI_E_ACCESS_DENIED 0x80290108	Der Aufrufer verfügt nicht über die erforderlichen Sicherheitsrechte, um den angeforderten Vorgang durchführen zu können.
TPMAPI_E_AUTHORIZATION_FAILED 0x80290109	Die angegebenen Autorisierungsinformationen sind ungültig.
TPMAPI_E_INVALID_CONTEXT_HANDLE 0x8029010A	Das angegebene Kontexthandle ist ungültig.
TPMAPI_E_TBS_COMMUNICATION_ERROR 0x8029010B	Bei der Kommunikation mit TBS ist ein Fehler aufgetreten.
TPMAPI_E_TPM_COMMAND_ERROR 0x8029010C	TPM hat ein unerwartetes Ergebnis zurückgeliefert.
TPMAPI_E_MESSAGE_TOO_LARGE 0x8029010D	Die Nachricht ist zu lang für das Codierungsschema.
TPMAPI_E_INVALID_ENCODING 0x8029010E	Die Codierung des BLOB wurde nicht erkannt.
TPMAPI_E_INVALID_KEY_SIZE 0x8029010F	Die Schlüsselgröße ist ungültig.
TPMAPI_E_ENCRYPTION_FAILED 0x80290110	Der Verschlüsselungsvorgang ist fehlgeschlagen.
TPMAPI_E_INVALID_KEY_PARAMS 0x80290111	Die Schlüsselparameterstruktur ist ungültig.
TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB 0x80290112	Bei den bereitgestellten Daten, die angefordert wurden, scheint es sich nicht um ein gültiges Migrationsautorisierungs-BLOB zu handeln.
TPMAPI_E_INVALID_PCR_INDEX 0x80290113	Der angegebene PCR-Index ist ungültig.
TPMAPI_E_INVALID_DELEGATE_BLOB 0x80290114	Bei den angegebenen Daten scheint es sich nicht um ein gültiges Delegat-BLOB zu handeln.
TPMAPI_E_INVALID_CONTEXT_PARAMS 0x80290115	Mindestens ein angegebener Kontextparameter war ungültig.
TPMAPI_E_INVALID_KEY_BLOB 0x80290116	Bei den angegebenen Daten scheint es sich nicht um ein gültiges Schlüssel-BLOB zu handeln.
TPMAPI_E_INVALID_PCR_DATA 0x80290117	Die angegebenen PCR-Daten sind ungültig.
TPMAPI_E_INVALID_OWNER_AUTH 0x80290118	Das Format des Besitzers der Authentifizierungsdaten ist ungültig.

Konstante/Wert	Beschreibung
TPMAPI_E_FIPS_RNG_CHECK_FAILED 0x80290119	Die generierte Zufallszahl hat die FIPS RNG-Prüfung nicht bestanden.
TPMAPI_E_EMPTY_TCG_LOG 0x8029011A	Das TCG-Ereignisprotokoll enthält keine Daten.
TPMAPI_E_INVALID_TCG_LOG_ENTRY 0x8029011B	Ein Eintrag im TCG-Ereignisprotokoll war ungültig.
TPMAPI_E_TCG_SEPARATOR_ABSENT 0x8029011C	Es wurde kein TCG-Trennzeichen gefunden.
TPMAPI_E_TCG_INVALID_DIGEST_ENTRY 0x8029011D	Ein Digestwert in einem TCG-Protokolleintrag stimmte nicht mit den Hashdaten überein.
TPMAPI_E_POLICY_DENIES_OPERATION 0x8029011E	Der angeforderte Vorgang wurde von der aktuellen TPM-Richtlinie blockiert. Wenden Sie sich an den Systemadministrator, wenn Sie Hilfe benötigen.
TBSIMP_E_BUFFER_TOO_SMALL 0x80290200	Der angegebene Puffer war zu klein.
TBSIMP_E_CLEANUP_FAILED 0x80290201	Der Kontext konnte nicht bereinigt werden.
TBSIMP_E_INVALID_CONTEXT_HANDLE 0x80290202	Das angegebene Kontexthandle ist ungültig.
TBSIMP_E_INVALID_CONTEXT_PARAM 0x80290203	Ein ungültiger Kontextparameter wurde angegeben.
TBSIMP_E_TPM_ERROR 0x80290204	Bei der Kommunikation mit TPM ist ein Fehler aufgetreten.
TBSIMP_E_HASH_BAD_KEY 0x80290205	Es wurde kein Eintrag mit dem angegebenen Schlüssel gefunden.
TBSIMP_E_DUPLICATE_VHANDLE 0x80290206	Das angegebene virtuelle Handle stimmt mit einem virtuellen Handle überein, das bereits verwendet wird.
TBSIMP_E_INVALID_OUTPUT_POINTER 0x80290207	Der Zeiger auf den zurückgegebenen Handlespeicherort war NULL oder ungültig.
TBSIMP_E_INVALID_PARAMETER 0x80290208	Ein oder mehrere Parameter sind ungültig.
TBSIMP_E_RPC_INIT_FAILED 0x80290209	Das RPC-Subsystem konnte nicht initialisiert werden.
TBSIMP_E_SCHEDULER_NOT_RUNNING 0x8029020A	Die TBS-Zeitplanung wird nicht ausgeführt.

Konstante/Wert	Beschreibung
TBSIMP_E_COMMAND_CANCELED 0x8029020B	Der Befehl wurde abgebrochen.
TBSIMP_E_OUT_OF_MEMORY 0x8029020C	Es war nicht genügend Arbeitsspeicher verfügbar, um die Anforderung zu erfüllen.
TBSIMP_E_LIST_NO_MORE_ITEMS 0x8029020D	Die angegebene Liste ist leer, oder die Iteration hat das Ende der Liste erreicht.
TBSIMP_E_LIST_NOT_FOUND 0x8029020E	Das angegebene Element wurde nicht in der Liste gefunden.
TBSIMP_E_NOT_ENOUGH_SPACE 0x8029020F	Das TPM verfügt nicht über genügend Speicherplatz, um die angeforderte Ressource zu laden.
TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS 0x80290210	Es werden zu viele TPM-Kontexte verwendet.
TBSIMP_E_COMMAND_FAILED 0x80290211	Der TPM-Befehl ist fehlgeschlagen.
TBSIMP_E_UNKNOWN_ORDINAL 0x80290212	Der TBS erkennt die angegebene Ordnungszahl nicht.
TBSIMP_E_RESOURCE_EXPIRED 0x80290213	Die angegebene Ressource ist nicht mehr verfügbar.
TBSIMP_E_INVALID_RESOURCE 0x80290214	Der Ressourcentyp stimmte nicht überein.
TBSIMP_E_NOTHING_TO_UNLOAD 0x80290215	Es können keine Ressourcen entladen werden.
TBSIMP_E_HASH_TABLE_FULL 0x80290216	Der Hashtabelle können keine neuen Einträge hinzugefügt werden.
TBSIMP_E_TOO_MANY_TBS_CONTEXTS 0x80290217	Ein neuer TBS-Kontext konnte nicht erstellt werden, da bereits zu viele offene Kontexte vorhanden sind.
TBSIMP_E_TOO_MANY_RESOURCES 0x80290218	Eine neue virtuelle Ressource konnte nicht erstellt werden, da bereits zu viele offene virtuelle Ressource vorhanden sind.
TBSIMP_E_PPI_NOT_SUPPORTED 0x80290219	Die physikalische Anwesenheitsschnittstelle wird nicht unterstützt.
TBSIMP_E_TPM_INCOMPATIBLE 0x8029021A	TBS ist nicht kompatibel mit der TPM-Version, die im System gefunden wurde.
TBSIMP_E_NO_EVENT_LOG 0x8029021B	Es ist kein TCG-Ereignisprotokoll verfügbar.

Konstante/Wert	Beschreibung
TPM_E_PPI_ACPI_FAILURE 0x80290300	Beim Versuch, die BIOS-Antwort auf einen physischen Anwesenheitsbefehl zu erhalten, wurde ein allgemeiner Fehler festgestellt.
TPM_E_PPI_USER_ABORT 0x80290301	Der Benutzer konnte die TPM-Vorgangsanforderung nicht bestätigen.
TPM_E_PPI_BIOS_FAILURE 0x80290302	Aufgrund des BIOS-Fehlers konnte der angeforderte TPM-Vorgang nicht erfolgreich ausgeführt werden (z. B. ungültige TPM-Vorgangsanforderung, BIOS-Kommunikationsfehler beim TPM).
TPM_E_PPI_NOT_SUPPORTED 0x80290303	Das BIOS unterstützt die Anwesenheitsschnittstelle nicht.
TPM_E_PPI_BLOCKED_IN_BIOS 0x80290304	Der Befehl für physische Anwesenheit wurde von den aktuellen BIOS-Einstellungen blockiert. Der Systembesitzer kann möglicherweise die BIOS-Einstellungen neu konfigurieren, um den Befehl zuzulassen.
TPM_E_PCP_ERROR_MASK 0x80290400	Dies ist eine Fehlermaske zum Konvertieren von Plattformkryptografieanbieter-Fehlern in Win-Fehler.
TPM_E_PCP_DEVICE_NOT_READY 0x80290401	Der Plattformkryptografieanbieter ist momentan nicht bereit. Er muss vollständig bereitgestellt werden, um betriebsbereit zu sein.
TPM_E_PCP_INVALID_HANDLE 0x80290402	Das für den Plattformkryptografieanbieter angegebene Handle ist ungültig.
TPM_E_PCP_INVALID_PARAMETER 0x80290403	Ein für den Plattformkryptografieanbieter angegebener Parameter ist ungültig.
TPM_E_PCP_FLAG_NOT_SUPPORTED 0x80290404	Ein für den Plattformkryptografieanbieter angegebenes Kennzeichen wird nicht unterstützt.
TPM_E_PCP_NOT_SUPPORTED 0x80290405	Der angeforderte Vorgang wird von diesem Plattformkryptografieanbieter nicht unterstützt.
TPM_E_PCP_BUFFER_TOO_SMALL 0x80290406	Der Puffer ist zu klein, um alle Daten aufzunehmen. Es wurden keine Informationen in den Puffer geschrieben.
TPM_E_PCP_INTERNAL_ERROR 0x80290407	Unerwarteter interner Fehler im Plattformkryptografieanbieter.
TPM_E_PCP_AUTHENTICATION_FAILED 0x80290408	Fehler bei der Autorisierung der Verwendung eines Anbieterobjekts.
TPM_E_PCP_AUTHENTICATION_IGNORED 0x80290409	Die Autorisierung für das Anbieterobjekt wurde vom Plattformkryptografiegerät ignoriert, um einen Wörterbuchangriff abzuwehren.
TPM_E_PCP_POLICY_NOT_FOUND 0x8029040A	Die referenzierte Richtlinie wurde nicht gefunden.

Konstante/Wert	Beschreibung
TPM_E_PCP_PROFILE_NOT_FOUND 0x8029040B	Das referenzierte Profil wurde nicht gefunden.
TPM_E_PCP_VALIDATION_FAILED 0x8029040C	Die Validierung war nicht erfolgreich.
PLA_E_DCS_NOT_FOUND 0x80300002	Der Sammlungssatz wurde nicht gefunden.
PLA_E_DCS_IN_USE 0x803000AA	Der Sammlungssatz oder eine der Abhängigkeiten wird bereits verwendet.
PLA_E_TOO_MANY_FOLDERS 0x80300045	Der Sammlungssatz konnte nicht gestartet werden, da zu viele Ordner vorhanden sind.
PLA_E_NO_MIN_DISK 0x80300070	Es ist nicht genügend freier Speicherplatz verfügbar, um den Sammlungssatz zu starten.
PLA_E_DCS_ALREADY_EXISTS 0x803000B7	Der Sammlungssatz ist bereits vorhanden.
PLA_S_PROPERTY_IGNORED 0x00300100	Der Eigenschaftswert wird ignoriert.
PLA_E_PROPERTY_CONFLICT 0x80300101	Konflikt beim Eigenschaftswert.
PLA_E_DCS_SINGLETON_REQUIRED 0x80300102	Die aktuelle Konfiguration für diesen Sammlungssatz erfordert, dass er genau eine Sammlung enthält.
PLA_E_CREDENTIALS_REQUIRED 0x80300103	Es ist ein Benutzerkonto erforderlich, um die Eigenschaften des aktuellen Sammlungssatzes zu übernehmen.
PLA_E_DCS_NOT_RUNNING 0x80300104	Der Sammlungssatz wird nicht ausgeführt.
PLA_E_CONFLICT_INCL_EXCL_API 0x80300105	In der Liste der APIs zum Ein-/Ausschließen wurde ein Konflikt erkannt. Sie dürfen in der Liste der einzuschließenden und in der Liste der auszuschließenden APIs nicht die gleiche API angeben.
PLA_E_NETWORK_EXE_NOT_VALID 0x80300106	Der angegebene ausführbare Pfad bezieht sich auf eine Netzwerkfreigabe oder einen UNC-Pfad.
PLA_E_EXE_ALREADY_CONFIGURED 0x80300107	Der angegebene Pfad zur ausführbaren Datei ist bereits für die API-Ablaufverfolgung konfiguriert.
PLA_E_EXE_PATH_NOT_VALID 0x80300108	Der angegebene Pfad zur ausführbaren Datei ist nicht vorhanden. Stellen Sie sicher, dass der angegebene Pfad richtig ist.
PLA_E_DC_ALREADY_EXISTS 0x80300109	Der Datensammler ist bereits vorhanden.

Konstante/Wert	Beschreibung
PLA_E_DCS_START_WAIT_TIMEOUT 0x8030010A	Zeitüberschreitung beim Warten auf die Startbenachrichtigung des Datensammlersatzes.
PLA_E_DC_START_WAIT_TIMEOUT 0x8030010B	Zeitüberschreitung beim Warten auf die Startbenachrichtigung des Datensammlers.
PLA_E_REPORT_WAIT_TIMEOUT 0x8030010C	Zeitüberschreitung beim Warten auf den Abschluss des Berichtgenerierungstools.
PLA_E_NO_DUPLICATES 0x8030010D	Elementduplikate sind nicht zulässig.
PLA_E_EXE_FULL_PATH_REQUIRED 0x8030010E	Wenn Sie die ausführbare Datei angeben, die Sie verfolgen möchten, müssen Sie einen vollständigen Pfad zu der ausführbaren Datei und nicht nur einen Dateinamen angeben.
PLA_E_INVALID_SESSION_NAME 0x8030010F	Der angegebene Sitzungsname ist ungültig.
PLA_E_PLA_CHANNEL_NOT_ENABLED 0x80300110	Der Ereignisprotokollkanal Microsoft-Windows-Diagnosis-PLA/Operational muss aktiviert sein, um diesen Vorgang auszuführen.
PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED 0x80300111	Der Ereignisprotokollkanal Microsoft-Windows-TaskScheduler muss aktiviert sein, um diesen Vorgang auszuführen.
PLA_E_RULES_MANAGER_FAILED 0x80300112	Fehler bei der Ausführung des Regelmanagers.
PLA_E_CABAPI_FAILURE 0x80300113	Fehler beim Komprimieren oder Extrahieren der Daten.
FVE_E_LOCKED_VOLUME 0x80310000	Dieses Laufwerk ist durch die BitLocker-Laufwerkverschlüsselung gesperrt. Sie müssen das Laufwerk über die Systemsteuerung entsperren.
FVE_E_NOT_ENCRYPTED 0x80310001	Das Laufwerk ist nicht verschlüsselt.
FVE_E_NO_TPM_BIOS 0x80310002	Das BIOS hat nicht korrekt mit dem TPM kommuniziert. Anweisungen zum Aktualisieren des BIOS erhalten Sie vom Computerhersteller.
FVE_E_NO_MBR_METRIC 0x80310003	Das BIOS hat nicht korrekt mit dem Master Boot Record (MBR) kommuniziert. Anweisungen zum Aktualisieren des BIOS erhalten Sie vom Computerhersteller.
FVE_E_NO_BOOTSECTOR_METRIC 0x80310004	Eine erforderliche TPM-Messung fehlt. Befindet sich eine startfähige CD oder DVD im Computer, entfernen Sie diese, starten Sie den Computer neu, und aktivieren Sie BitLocker erneut. Falls das Problem weiterhin besteht, stellen Sie sicher, dass der MBR (Master Boot Record) aktuell ist.

Konstante/Wert	Beschreibung
FVE_E_NO_BOOTMGR_METRIC 0x80310005	Der Startsektor des Laufwerks ist nicht mit der BitLocker-Laufwerkverschlüsselung kompatibel. Verwenden Sie das Tool "Bootrec.exe" in der Windows-Wiederherstellungsumgebung, um den Start-Manager (BOOTMGR) zu aktualisieren oder zu reparieren.
FVE_E_WRONG_BOOTMGR 0x80310006	Der Start-Manager des Betriebssystems ist nicht mit der BitLocker-Laufwerkverschlüsselung kompatibel. Verwenden Sie das Tool "Bootrec.exe" in der Windows-Wiederherstellungsumgebung, um den Start-Manager (BOOTMGR) zu aktualisieren oder zu reparieren.
FVE_E_SECURE_KEY_REQUIRED 0x80310007	Für die Ausführung des Vorgangs ist mindestens eine sichere Schlüsselschutzvorrichtung erforderlich.
FVE_E_NOT_ACTIVATED 0x80310008	Die BitLocker-Laufwerkverschlüsselung ist für dieses Laufwerk nicht aktiviert. Aktivieren Sie BitLocker.
FVE_E_ACTION_NOT_ALLOWED 0x80310009	Die BitLocker-Laufwerkverschlüsselung konnte die angeforderte Aktion nicht ausführen. Dieses Problem kann auftreten, wenn zwei Anforderungen gleichzeitig gesendet werden. Warten Sie einen Moment, und wiederholen Sie anschließend die Aktion.
FVE_E_AD_SCHEMA_NOT_INSTALLED 0x8031000A	Die Gesamtstruktur des Active Directory-Domänendienstes enthält nicht die erforderlichen Attribute und Klassen zum Hosten der BitLocker-Laufwerkverschlüsselung oder der TPM-Informationen. Wenden Sie sich an den Domänenadministrator, um zu überprüfen, ob die erforderlichen Active Directory-Schemaerweiterungen für BitLocker installiert wurden.
FVE_E_AD_INVALID_DATATYPE 0x8031000B	Der Typ der Daten, die aus Active Directory abgerufen wurden, wurde nicht erwartet. Die BitLocker-Wiederherstellungsinformationen fehlen möglicherweise oder sind beschädigt.
FVE_E_AD_INVALID_DATASIZE 0x8031000C	Die Größe der Daten, die aus Active Directory abgerufen wurden, wurde nicht erwartet. Die BitLocker-Wiederherstellungsinformationen fehlen möglicherweise oder sind beschädigt.
FVE_E_AD_NO_VALUES 0x8031000D	Das aus Active Directory gelesene Attribut enthält keine Werte. Die BitLocker-Wiederherstellungsinformationen fehlen möglicherweise oder sind beschädigt.
FVE_E_AD_ATTR_NOT_SET 0x8031000E	Das Attribut wurde nicht festgelegt. Überprüfen Sie, ob Sie an einem Domänenkonto angemeldet sind, mit dem Informationen in Active Directory-Objekte geschrieben werden können.
FVE_E_AD_GUID_NOT_FOUND 0x8031000F	Das angegebene Attribut wurde in Active Directory-Domänendienste nicht gefunden. Wenden Sie sich an den Domänenadministrator, um zu überprüfen, ob die erforderlichen Active Directory-Schemaerweiterungen für BitLocker installiert wurden.
FVE_E_BAD_INFORMATION 0x80310010	Die BitLocker-Metadaten für das verschlüsselte Laufwerk sind ungültig. Versuchen Sie, das Laufwerk zu reparieren, um wieder Zugriff zu erhalten.

Konstante/Wert	Beschreibung
FVE_E_TOO_SMALL 0x80310011	Das Laufwerk kann nicht verschlüsselt werden, da nicht genügend freier Speicherplatz verfügbar ist. Löschen Sie alle nicht benötigten Daten auf dem Laufwerk, um zusätzlichen Speicherplatz freizugeben, und wiederholen Sie anschließend den Vorgang.
FVE_E_SYSTEM_VOLUME 0x80310012	Das Laufwerk kann nicht verschlüsselt werden, da es Informationen zum Systemstart enthält. Erstellen Sie eine gesonderte Partition, die als Systemlaufwerk mit den Startinformationen verwendet wird, und eine zweite Partition, die als Betriebssystem-Laufwerk verwendet wird. Verschlüsseln Sie anschließend das Betriebssystem-Laufwerk.
FVE_E_FAILED_WRONG_FS 0x80310013	Das Laufwerk kann nicht verschlüsselt werden, da das Dateisystem nicht unterstützt wird.
FVE_E_BAD_PARTITION_SIZE 0x80310014	Das Dateisystem ist größer als die Partitionsgröße in der Partitionstabelle. Das Laufwerk ist möglicherweise beschädigt oder wurde manipuliert. Für die Verwendung des Laufwerks mit BitLocker muss die Partition neu formatiert werden.
FVE_E_NOT_SUPPORTED 0x80310015	Das Laufwerk kann nicht verschlüsselt werden.
FVE_E_BAD_DATA 0x80310016	Die Daten sind ungültig.
FVE_E_VOLUME_NOT_BOUND 0x80310017	Das angegebene Datenlaufwerk ist nicht für die automatische Entsperrung auf dem aktuellen Computer konfiguriert und kann nicht automatisch entsperrt werden.
FVE_E_TPM_NOT_OWNED 0x80310018	Sie müssen das TPM zuerst initialisieren, bevor Sie die BitLocker-Laufwerkverschlüsselungs verwenden können.
FVE_E_NOT_DATA_VOLUME 0x80310019	Der gewünschte Vorgang kann auf einem Betriebssystem-Laufwerk nicht ausgeführt werden.
FVE_E_AD_INSUFFICIENT_BUFFER 0x8031001A	Der Puffer, der an eine Funktion übergeben wurde, war zu klein, um die zurückgegebenen Daten aufzunehmen. Erhöhen Sie die Puffergröße vor der erneuten Ausführung der Funktion.
FVE_E_CONV_READ 0x8031001B	Ein Lesevorgang beim Konvertieren des Laufwerks war nicht erfolgreich. Das Laufwerk wurde nicht konvertiert. Aktivieren Sie BitLocker erneut.
FVE_E_CONV_WRITE 0x8031001C	Ein Schreibvorgang beim Konvertieren des Laufwerks war nicht erfolgreich. Das Laufwerk wurde nicht konvertiert. Aktivieren Sie BitLocker erneut.
FVE_E_KEY_REQUIRED 0x8031001D	Mindestens eine BitLocker-Schlüsselschutzvorrichtung ist erforderlich. Der letzte Schlüssel auf dem Laufwerk kann nicht gelöscht werden.
FVE_E_CLUSTERING_NOT_SUPPORTED	Clusterkonfigurationen werden von der BitLocker-Laufwerkverschlüsselung nicht unterstützt.

Konstante/Wert	Beschreibung
0x8031001E	
FVE_E_VOLUME_BOUND_ALREADY 0x8031001F	Das angegebene Laufwerk ist bereits für die automatische Entsperrung auf dem aktuellen Computer konfiguriert.
FVE_E_OS_NOT_PROTECTED 0x80310020	Das Laufwerk des Betriebssystems wird nicht durch BitLocker-Laufwerkverschlüsselung geschützt.
FVE_E_PROTECTION_DISABLED 0x80310021	Die BitLocker-Laufwerkverschlüsselung wurde für dieses Laufwerk angehalten. Alle für das Laufwerk konfigurierten BitLocker-Schlüsselschutzvorrichtungen werden effektiv deaktiviert, und das Laufwerk wird automatisch mithilfe eines unverschlüsselten Schlüssels entsperrt.
FVE_E_RECOVERY_KEY_REQUIRED 0x80310022	Für das zu sperrende Laufwerk sind keine Schlüsselschutzvorrichtungen für eine Verschlüsselung verfügbar, da der BitLocker-Schutz derzeit angehalten ist. Aktivieren Sie BitLocker wieder, um das Laufwerk zu sperren.
FVE_E_FOREIGN_VOLUME 0x80310023	BitLocker keine Datenlaufwerke mithilfe des TPM schützen. Der TPM-Schutz kann nur mit dem Laufwerk des Betriebssystems verwendet werden.
FVE_E_OVERLAPPED_UPDATE 0x80310024	Die BitLocker-Metadaten für das verschlüsselte Laufwerk können nicht aktualisiert werden, da sie für eine Aktualisierung durch einen anderen Vorgang gesperrt waren. Wiederholen Sie den Vorgang.
FVE_E_TPM_SRK_AUTH_NOT_ZERO 0x80310025	Die Autorisierungsdaten für den Speicherstammschlüsselsatz (SRK) des TPM sind nicht null und daher nicht mit BitLocker kompatibel. Initialisieren Sie das TPM, bevor Sie es mit BitLocker verwenden.
FVE_E_FAILED_SECTOR_SIZE 0x80310026	Der Laufwerkverschlüsselungsalgorithmus kann für diese Sektorgröße nicht verwendet werden.
FVE_E_FAILED_AUTHENTICATION 0x80310027	Das Laufwerk kann mit dem bereitgestellten Schlüssel nicht entsperrt werden. Überprüfen Sie, ob Sie den richtigen Schlüssel bereitgestellt haben, und wiederholen Sie den Vorgang.
FVE_E_NOT_OS_VOLUME 0x80310028	Das angegebene Laufwerk ist nicht das Laufwerk des Betriebssystems.
FVE_E_AUTOUNLOCK_ENABLED 0x80310029	Die BitLocker-Laufwerkverschlüsselung kann für das Laufwerk des Betriebssystems erst deaktiviert werden, wenn das Feature für automatisches Entsperren für die dem Computer zugeordneten integrierten Datenlaufwerke und die Wechseldatenlaufwerke deaktiviert wurde.
FVE_E_WRONG_BOOTSECTOR 0x8031002A	Der Startsektor der Systempartition führt keine TPM-Messungen aus. Verwenden Sie das Tool "Bootrec.exe" in der Windows-Wiederherstellungsumgebung, um den Startsektor zu aktualisieren oder zu reparieren.
FVE_E_WRONG_SYSTEM_FS 0x8031002B	Betriebssystem-Laufwerke für BitLocker-Laufwerkverschlüsselung müssen mit dem NTFS-

Konstante/Wert	Beschreibung
	Dateisystem formatiert werden, um eine Verschlüsselung vorzunehmen. Konvertieren Sie das Laufwerk in NTFS, und aktivieren Sie anschließend BitLocker.
FVE_E_POLICY_PASSWORD_REQUIRED 0x8031002C	Für die Gruppenrichtlinieneinstellungen muss vor dem Verschlüsseln des Laufwerks ein Wiederherstellungskennwort angegeben werden.
FVE_E_CANNOT_SET_FVEK_ENCRYPTED 0x8031002D	Der Algorithmus und der Schlüssel für die Laufwerkverschlüsselung können nicht für ein zuvor verschlüsseltes Laufwerk festgelegt werden. Zum Verschlüsseln des Laufwerks mit der BitLocker-Laufwerkverschlüsselung muss die vorherige Verschlüsselung entfernt und anschließend BitLocker aktiviert werden.
FVE_E_CANNOT_ENCRYPT_NO_KEY 0x8031002E	Das angegebene Laufwerk kann mit der BitLocker-Laufwerkverschlüsselung nicht verschlüsselt werden, da kein Verschlüsselungsschlüssel verfügbar ist. Fügen Sie zum Verschlüsseln des Laufwerks eine Schlüsselschutzvorrichtung hinzu.
FVE_E_BOOTABLE_CDDVD 0x80310030	Im Computer wurde ein startbarer Datenträger (CD oder DVD) erkannt. Entfernen Sie den Datenträger, und starten Sie den Computer neu, bevor Sie BitLocker konfigurieren.
FVE_E_PROTECTOR_EXISTS 0x80310031	Die Schlüsselschutzvorrichtung kann nicht hinzugefügt werden. Für das Laufwerk ist nur eine Schlüsselschutzvorrichtung dieses Typs zulässig.
FVE_E_RELATIVE_PATH 0x80310032	Die Datei für das Wiederherstellungskennwort wurde nicht gefunden, da ein relativer Pfad angegeben wurde. Wiederherstellungskennwörter müssen in einem vollqualifizierten Pfad gespeichert werden. Im Pfad können für den Computer konfigurierte Umgebungsvariablen verwendet werden.
FVE_E_PROTECTOR_NOT_FOUND 0x80310033	Die angegebene Schlüsselschutzvorrichtung wurde auf dem Laufwerk nicht gefunden. Verwenden Sie eine andere Schlüsselschutzvorrichtung.
FVE_E_INVALID_KEY_FORMAT 0x80310034	Der bereitgestellte Wiederherstellungsschlüssel ist beschädigt und kann nicht für den Zugriff auf das Laufwerk verwendet werden. Zur Wiederherstellung des Zugriffs muss eine alternative Wiederherstellungsmethode, beispielsweise ein Wiederherstellungskennwort, ein Datenwiederherstellungs-Agent oder eine Sicherungsversion des Wiederherstellungsschlüssels verwendet werde.
FVE_E_INVALID_PASSWORD_FORMAT 0x80310035	Das Format des Wiederherstellungskennworts ist ungültig. BitLocker-Wiederherstellungskennwörter umfassen 48 Stellen. Stellen Sie sicher, dass das Wiederherstellungskennwort das korrekte Format aufweist, und wiederholen Sie den Vorgang.
FVE_E_FIPS_RNG_CHECK_FAILED 0x80310036	Fehler bei der Prüfung des Zufallszahlen-Generators.
FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD 0x80310037	Durch die Gruppenrichtlinieneinstellung, die FIPS-Kompatibilität erfordert, wird die Generierung oder

Konstante/Wert	Beschreibung
	Verwendung eines lokalen Wiederherstellungskennworts durch die BitLocker-Laufwerkverschlüsselung verhindert. Bei der Ausführung im FIPS-kompatiblen Modus stehen folgende BitLocker-Wiederherstellungsoptionen zur Verfügung: Ein auf einem USB-Laufwerk gespeicherter Wiederherstellungsschlüssel oder eine Wiederherstellung über einen Datenwiederherstellungs-Agent.
FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT 0x80310038	Durch die Gruppenrichtlinieneinstellung, für die FIPS-Kompatibilität erforderlich ist, wird das Speichern des Wiederherstellungskennworts in Active Directory verhindert. Bei der Ausführung im FIPS-kompatiblen Modus stehen folgende BitLocker-Wiederherstellungsoptionen zur Verfügung: Ein auf einem USB-Laufwerk gespeicherter Wiederherstellungsschlüssel oder eine Wiederherstellung über einen Datenwiederherstellungs-Agent. Überprüfen Sie die Konfiguration der Gruppenrichtlinieneinstellungen.
FVE_E_NOT_DECRYPTED 0x80310039	Das Laufwerk muss zum Ausführen dieses Vorgangs vollständig entschlüsselt werden.
FVE_E_INVALID_PROTECTOR_TYPE 0x8031003A	Die angegebene Schlüsselschutzvorrichtung kann nicht für den Vorgang verwendet werden.
FVE_E_NO_PROTECTORS_TO_TEST 0x8031003B	Auf dem Laufwerk sind keine Schlüsselschutzvorrichtungen zum Ausführen des Hardwaretests vorhanden.
FVE_E_KEYFILE_NOT_FOUND 0x8031003C	Der BitLocker-Startschlüssel oder das Wiederherstellungskennwort wurde auf dem USB-Gerät nicht gefunden. Stellen Sie sicher, dass Sie über das korrekte USB-Gerät verfügen und dass es am Computer an einem aktiven USB-Anschluss angeschlossen ist. Starten Sie den Computer neu, und wiederholen Sie den Vorgang. Falls das Problem weiterhin besteht, fordern Sie vom Computerhersteller Anweisungen zum Upgrade des BIOS an.
FVE_E_KEYFILE_INVALID 0x8031003D	Der BitLocker-Startschlüssel oder die Wiederherstellungskennwortdatei ist beschädigt oder ungültig. Überprüfen Sie, ob Sie über den korrekten Startschlüssel oder die Wiederherstellungskennwortdatei verfügen, und wiederholen Sie den Vorgang.
FVE_E_KEYFILE_NO_VMK 0x8031003E	Der BitLocker-Verschlüsselungsschlüssel konnte nicht aus dem Startschlüssel oder dem Wiederherstellungskennwort abgerufen werden. Überprüfen Sie, ob Sie über den korrekten Startschlüssel oder die Wiederherstellungskennwortdatei verfügen, und wiederholen Sie den Vorgang.
FVE_E_TPM_DISABLED 0x8031003F	Das TPM ist deaktiviert. Das TPM muss aktiviert und initialisiert werden und über einen gültigen Besitz verfügen, bevor es mit der BitLocker-Laufwerkverschlüsselung verwendet werden kann.
FVE_E_NOT_ALLOWED_IN_SAFE_MODE 0x80310040	Die BitLocker-Konfiguration des angegebenen Laufwerks kann nicht verwaltet werden, da der Computer derzeit im abgesicherten Modus betrieben wird. Im abgesicherten Modus kann die BitLocker-Laufwerkverschlüsselung nur zur Wiederherstellung verwendet werden.

Konstante/Wert	Beschreibung
FVE_E_TPM_INVALID_PCR 0x80310041	Das Laufwerk konnte vom TPM nicht entsperrt werden, da die Systemstartinformationen geändert wurden oder eine PIN nicht korrekt angegeben wurde. Stellen Sie sicher, dass das Laufwerk nicht manipuliert wurde und dass Änderungen an Systemstartinformationen durch eine vertrauenswürdige Quelle verursacht wurden. Nachdem überprüft wurde, ob ein sicherer Zugriff auf das Laufwerk möglich ist, entsperren Sie das Laufwerk mithilfe der BitLocker-Wiederherstellungskonsole. Halten Sie BitLocker anschließend an, und setzen Sie die Funktion wieder fort, um die Systemstartinformationen zu aktualisieren, die dem Laufwerk von BitLocker zugeordnet werden.
FVE_E_TPM_NO_VMK 0x80310042	Der BitLocker-Verschlüsselungsschlüssel konnte nicht aus dem TPM abgerufen werden.
FVE_E_PIN_INVALID 0x80310043	Der BitLocker-Verschlüsselungsschlüssel konnte nicht über das TPM oder die PIN abgerufen werden.
FVE_E_AUTH_INVALID_APPLICATION 0x80310044	Eine Startanwendung hat sich geändert, nachdem die BitLocker-Laufwerkverschlüsselung aktiviert wurde.
FVE_E_AUTH_INVALID_CONFIG 0x80310045	Die Einstellungen für die Startkonfigurationsdaten wurden geändert, nachdem die BitLocker-Laufwerkverschlüsselung aktiviert wurde.
FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED 0x80310046	Die Verwendung von unverschlüsselten Schlüsseln ist gemäß der Gruppenrichtlinieneinstellung, die FIPS-Kompatibilität erfordert, untersagt. Dadurch wird das Anhalten von BitLocker auf dem Laufwerk verhindert. Weitere Informationen erhalten Sie vom Domänenadministrator.
FVE_E_FS_NOT_EXTENDED 0x80310047	Das Laufwerk kann von der BitLocker-Laufwerkverschlüsselung nicht verschlüsselt werden, da sich das Dateisystem nicht bis zum Ende des Laufwerks erstreckt. Partitionieren Sie das Laufwerk neu, und wiederholen Sie den Vorgang.
FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED 0x80310048	Die BitLocker-Laufwerkverschlüsselung kann nicht auf dem Laufwerk des Betriebssystems aktiviert werden. Anweisungen zum Aktualisieren des BIOS erhalten Sie vom Computerhersteller.
FVE_E_NO_LICENSE 0x80310049	Diese Windows-Version enthält keine BitLocker-Laufwerkverschlüsselung. Aktualisieren Sie das Betriebssystem, um die BitLocker-Laufwerkverschlüsselung zu verwenden.
FVE_E_NOT_ON_STACK 0x8031004A	Die BitLocker-Laufwerkverschlüsselung kann nicht verwendet werden, da wichtige BitLocker-Systemdateien fehlen oder beschädigt sind. Verwenden Sie die Windows-Starthilfe, um die Dateien auf dem Computer wiederherzustellen.
FVE_E_FS_MOUNTED 0x8031004B	Eine Sperrung des Laufwerks ist nicht möglich, solange es verwendet wird.

Konstante/Wert	Beschreibung
FVE_E_TOKEN_NOT_IMPERSONATED 0x8031004C	Das mit dem aktuellen Thread verknüpfte Zugriffstoken ist kein imitiertes Token.
FVE_E_DRY_RUN_FAILED 0x8031004D	Der BitLocker-Verschlüsselungsschlüssel kann nicht abgerufen werden. Stellen Sie sicher, dass das TPM aktiviert ist und der Besitz übernommen wurde. Besitzt der Computer kein TPM, überprüfen Sie, ob das USB-Laufwerk angeschlossen und verfügbar ist.
FVE_E_REBOOT_REQUIRED 0x8031004E	Der Computer muss vor der Fortsetzung der BitLocker-Laufwerkverschlüsselung neu gestartet werden.
FVE_E_DEBUGGER_ENABLED 0x8031004F	Bei aktiviertem Startdebugging ist keine Laufwerkverschlüsselung möglich. Verwenden Sie das Befehlszeilentool "bcdedit", um das Startdebugging zu deaktivieren.
FVE_E_RAW_ACCESS 0x80310050	Es wurde keine Aktion durchgeführt, weil sich die BitLocker-Laufwerkverschlüsselung im Rohzugriffsmodus befindet.
FVE_E_RAW_BLOCKED 0x80310051	Die BitLocker-Laufwerkverschlüsselung kann den RAW-Zugriffsmodus für dieses Volume nicht aktivieren, da das Laufwerk derzeit verwendet wird.
FVE_E_BCD_APPLICATIONS_PATH_INCORRECT 0x80310052	Der in den Startkonfigurationsdaten (BCD) für eine durch die BitLocker-Laufwerkverschlüsselung integritätsgeschützte Anwendung angegebene Pfad ist falsch. Überprüfen und korrigieren Sie die BCD-Einstellungen, und wiederholen Sie den Vorgang.
FVE_E_NOT_ALLOWED_IN_VERSION 0x80310053	Die BitLocker-Laufwerkverschlüsselung kann nur zu beschränkten Bereitstellungs- oder Wiederherstellungszwecken verwendet werden, wenn der Computer in Vorinstallations- oder Wiederherstellungsumgebungen ausgeführt wird.
FVE_E_NO_AUTOUNLOCK_MASTER_KEY 0x80310054	Der Hauptschlüssel für das automatische Aufheben der Sperre war auf dem Laufwerk des Betriebssystems nicht verfügbar.
FVE_E_MOR_FAILED 0x80310055	Fehler beim Aktivieren des Löschens des Systemspeichers beim Neustart des Computers.
FVE_E_HIDDEN_VOLUME 0x80310056	Das verborgene Laufwerk kann nicht verschlüsselt werden.
FVE_E_TRANSIENT_STATE 0x80310057	BitLocker-Verschlüsselungsschlüssel wurden ignoriert, da das Laufwerk einen vorübergehenden Status aufwies.
FVE_E_PUBKEY_NOT_ALLOWED 0x80310058	Auf diesem Laufwerk sind keine Schutzvorrichtungen zulässig, die auf dem öffentlichen Schlüssel basieren.
FVE_E_VOLUME_HANDLE_OPEN 0x80310059	Auf diesem Laufwerk wird bereits ein BitLocker-Laufwerkverschlüsselungsvorgang ausgeführt. Schließen Sie alle Vorgänge ab, bevor Sie diesen Vorgang fortsetzen.

Konstante/Wert	Beschreibung
FVE_E_NO_FEATURE_LICENSE 0x8031005A	Die Version von Windows bietet keine Unterstützung für dieses Feature der BitLocker-Laufwerkverschlüsselung. Aktualisieren Sie das Betriebssystem, um das Feature zu verwenden.
FVE_E_INVALID_STARTUP_OPTIONS 0x8031005B	Die Gruppenrichtlinieneinstellungen für BitLocker-Startoptionen stehen in Konflikt und können nicht angewendet werden. Weitere Informationen erhalten Sie von Ihrem Systemadministrator.
FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED 0x8031005C	Die Gruppenrichtlinieneinstellungen lassen keine Erstellung eines Wiederherstellungskennworts zu.
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED 0x8031005D	Die Gruppenrichtlinieneinstellungen erfordern das Erstellen eines Wiederherstellungskennworts.
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED 0x8031005E	Die Gruppenrichtlinieneinstellungen lassen keine Erstellung eines Wiederherstellungsschlüssels zu.
FVE_E_POLICY_RECOVERY_KEY_REQUIRED 0x8031005F	Die Gruppenrichtlinieneinstellungen erfordern das Erstellen eines Wiederherstellungsschlüssels.
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED 0x80310060	Die Gruppenrichtlinieneinstellungen lassen nicht die Verwendung einer PIN beim Start zu. Wählen Sie eine andere BitLocker-Startoption.
FVE_E_POLICY_STARTUP_PIN_REQUIRED 0x80310061	Die Gruppenrichtlinieneinstellungen erfordern die Verwendung einer PIN beim Start. Wählen Sie diese BitLocker-Startoption.
FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED 0x80310062	Die Gruppenrichtlinieneinstellungen lassen nicht die Verwendung eines Startschlüssels zu. Wählen Sie eine andere BitLocker-Startoption.
FVE_E_POLICY_STARTUP_KEY_REQUIRED 0x80310063	Die Gruppenrichtlinieneinstellungen erfordern die Verwendung eines Startschlüssels. Wählen Sie diese BitLocker-Startoption.
FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064	Die Gruppenrichtlinieneinstellungen lassen keine Verwendung eines Startschlüssels und einer PIN zu. Wählen Sie eine andere BitLocker-Startoption.
FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED 0x80310065	Die Gruppenrichtlinieneinstellungen erfordern die Verwendung eines Startschlüssels und einer PIN. Wählen Sie diese BitLocker-Startoption.
FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED 0x80310066	Die Gruppenrichtlinie lässt die Verwendung eines ausschließlichen TPM-Schutzes beim Start nicht zu. Wählen Sie eine andere BitLocker-Startoption.
FVE_E_POLICY_STARTUP_TPM_REQUIRED 0x80310067	Die Gruppenrichtlinieneinstellungen erfordern die Verwendung eines ausschließlichen TPM-Schutzes beim Start. Wählen Sie diese BitLocker-Startoption.
FVE_E_POLICY_INVALID_PIN_LENGTH 0x80310068	Die bereitgestellte PIN erfüllt nicht die minimalen oder maximalen PIN-Längenanforderungen.

Konstante/Wert	Beschreibung
FVE_E_KEY_PROTECTOR_NOT_SUPPORTED 0x80310069	Die Schlüsselschutzvorrichtung wird durch die derzeit auf dem Laufwerk installierte Version der BitLocker-Laufwerkverschlüsselung nicht unterstützt. Aktualisieren Sie das Laufwerk, um die Schlüsselschutzvorrichtung hinzuzufügen.
FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED 0x8031006A	Die Gruppenrichtlinieneinstellungen lassen keine Kennworterstellung zu.
FVE_E_POLICY_PASSPHRASE_REQUIRED 0x8031006B	Die Gruppenrichtlinieneinstellungen erfordern die Erstellung eines Kennworts.
FVE_E_FIPS_PREVENTS_PASSPHRASE 0x8031006C	Aufgrund einer Gruppenrichtlinieneinstellung, die eine FIPS-Kompatibilität erfordert, konnten keine Kennwörter generiert oder verwendet werden. Weitere Informationen erhalten Sie vom Domänenadministrator.
FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED 0x8031006D	Dem Betriebssystem-Laufwerk kann kein Kennwort hinzugefügt werden.
FVE_E_INVALID_BITLOCKER_OID 0x8031006E	Die BitLocker-Objektkennung (OID) auf dem Laufwerk ist offensichtlich ungültig oder beschädigt. Verwenden Sie "manage-BDE", um die OID auf dem Laufwerk zurückzusetzen.
FVE_E_VOLUME_TOO_SMALL 0x8031006F	Das Laufwerk ist zu klein, um mit der BitLocker-Laufwerkverschlüsselung geschützt zu werden.
FVE_E_DV_NOT_SUPPORTED_ON_FS 0x80310070	Der ausgewählte Ermittlungslaufwerktyp ist nicht mit dem Dateisystem auf dem Laufwerk kompatibel. BitLocker To Go-Ermittlungslaufwerke müssen auf mit FAT formatierten Laufwerken erstellt werden.
FVE_E_DV_NOT_ALLOWED_BY_GP 0x80310071	Der ausgewählte Ermittlungslaufwerktyp ist laut Gruppenrichtlinieneinstellungen des Computers nicht zulässig. Stellen Sie sicher, dass gemäß den Gruppenrichtlinieneinstellungen die Erstellung von Ermittlungslaufwerken für die Verwendung mit BitLocker To Go möglich ist.
FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED 0x80310072	Gemäß Gruppenrichtlinieneinstellungen ist die Verwendung von Benutzerzertifikaten, z. B. Smartcards, für die BitLocker-Laufwerkverschlüsselung nicht zulässig.
FVE_E_POLICY_USER_CERTIFICATE_REQUIRED 0x80310073	Die Gruppenrichtlinieneinstellungen erfordern die Verwendung eines gültigen Benutzerzertifikats, z. B. eine Smartcard, das mit der BitLocker-Laufwerkverschlüsselung verwendet werden muss.
FVE_E_POLICY_USER_CERT_MUST_BE_HW 0x80310074	Die Gruppenrichtlinieneinstellungen erfordern die Verwendung einer Smartcard-basierten Schlüsselschutzvorrichtung mit der BitLocker-Laufwerkverschlüsselung.
FVE_E_POLICY_USER_CONFIGURE_FDV_AUTOUNLOCK_NOT_ALLOWED 0x80310075	Gemäß Gruppenrichtlinieneinstellungen ist keine automatische Entsperrung von durch BitLocker geschützten integrierten Datenlaufwerken zulässig.

Konstante/Wert	Beschreibung
FVE_E_POLICY_USER_CONFIGURE_RDV_AUTOUNLOCK_NOT_ALLOWED 0x80310076	Gemäß Gruppenrichtlinieneinstellungen ist keine automatische Entsperrung von durch BitLocker geschützten Wechseldatenlaufwerken zulässig.
FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED 0x80310077	Gemäß Gruppenrichtlinieneinstellungen ist keine Konfiguration der BitLocker-Laufwerkverschlüsselung auf Wechseldatenlaufwerken zulässig.
FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED 0x80310078	Gemäß Gruppenrichtlinieneinstellungen ist keine Aktivierung der BitLocker-Laufwerkverschlüsselung auf Wechseldatenlaufwerken zulässig. Wenden Sie sich an den Systemadministrator, wenn Sie BitLocker aktivieren möchten.
FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED 0x80310079	Gemäß Gruppenrichtlinieneinstellungen ist die Deaktivierung der BitLocker-Laufwerkverschlüsselung auf Wechseldatenlaufwerken nicht zulässig. Wenden Sie sich an den Systemadministrator, wenn Sie BitLocker deaktivieren möchten.
FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH 0x80310080	Das Kennwort entspricht den Vorgaben für die Mindestkennwortlänge. Standardmäßig müssen Kennwörter aus mindestens acht Zeichen bestehen. Erkundigen Sie sich beim Systemadministrator nach den in Ihrer Organisation geltenden Vorgaben für die Kennwortlänge.
FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE 0x80310081	Das Kennwort erfüllt nicht die vom Systemadministrator festgelegten Komplexitätsanforderungen. Fügen Sie Groß-/Kleinbuchstaben, Zahlen und Symbole hinzu.
FVE_E_RECOVERY_PARTITION 0x80310082	Das Laufwerk kann nicht verschlüsselt werden, da es für die Windows-Systemwiederherstellungsoptionen reserviert ist.
FVE_E_POLICY_CONFLICT_FDV_RK_OFF_AUK_ON 0x80310083	Die BitLocker-Laufwerkverschlüsselung kann aufgrund von in Konflikt stehenden Gruppenrichtlinieneinstellungen nicht für das Laufwerk verwendet werden. BitLocker kann nicht für das automatische Entsperren von integrierten Datenlaufwerken konfiguriert werden, wenn die Optionen zur Wiederherstellung durch den Benutzer deaktiviert sind. Sollen durch BitLocker geschützte integrierte Datenlaufwerke nach einer Schlüsselüberprüfung automatisch entsperrt werden, bitten Sie den Systemadministrator, den Einstellungskonflikt vor dem Aktivieren von BitLocker zu beheben.
FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON 0x80310084	Die BitLocker-Laufwerkverschlüsselung kann aufgrund von in Konflikt stehenden Gruppenrichtlinieneinstellungen nicht für das Laufwerk verwendet werden. BitLocker kann nicht für das automatische Entsperren von Wechseldatenlaufwerken konfiguriert werden, wenn die Option zur Wiederherstellung durch den Benutzer deaktiviert ist. Sollen durch BitLocker geschützte Wechseldatenlaufwerke nach einer Schlüsselüberprüfung automatisch entsperrt werden, bitten Sie den Systemadministrator, den Einstellungskonflikt vor dem Aktivieren von BitLocker zu beheben
FVE_E_NON_BITLOCKER_OID 0x80310085	Aufgrund des Attributs für die erweiterte Schlüsselverwendung (Enhanced Key Usage, EKU) des

Konstante/Wert	Beschreibung
	angegebenen Zertifikats kann selbiges nicht für die BitLocker-Laufwerkverschlüsselung verwendet werden. Zertifikate müssen für die Verwendung von BitLocker nicht zwingend über ein EKU-Attribut verfügen, ist jedoch eines konfiguriert, muss es auf einen Objektbezeichner (OID) festgelegt sein, der mit dem für BitLocker konfigurierten OID übereinstimmt.
FVE_E_POLICY_PROHIBITS_SELFSIGNED 0x80310086	Die BitLocker-Laufwerkverschlüsselung kann aufgrund von Gruppenrichtlinieneinstellungen nicht für das Laufwerk in seiner derzeitigen Konfiguration angewendet werden. Das für die Laufwerkverschlüsselung angegebene Zertifikat ist selbstsigniert. Gemäß den aktuellen Gruppenrichtlinieneinstellungen ist die Verwendung von selbstsignierten Zertifikaten nicht zulässig. Rufen Sie in der Zertifizierungsstelle ein neues Zertifikat ab, bevor Sie BitLocker aktivieren.
FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED 0x80310087	Die BitLocker-Verschlüsselung kann aufgrund von in Konflikt stehenden Gruppenrichtlinieneinstellungen nicht für das Laufwerk verwendet werden. Wenn der Schreibzugriff auf nicht durch BitLocker geschützte Laufwerke verweigert wird, kann die Verwendung eines USB-Startschlüssels nicht als Bedingung festgelegt werden. Bitten Sie den Systemadministrator, die Richtlinienkonflikte vor dem Aktivieren von BitLocker zu beheben.
FVE_E_CONV_RECOVERY_FAILED 0x80310088	Die BitLocker-Laufwerkverschlüsselung kann aufgrund in Konflikt stehender Gruppenrichtlinieneinstellungen für Wiederherstellungsoptionen auf Betriebssystem-Laufwerken nicht für das Laufwerk verwendet werden. Das Speichern von Wiederherstellungsinformationen in Active Directory-Domänendienste kann nicht angefordert werden, wenn die Generierung von Wiederherstellungskennwörtern nicht zulässig ist. Bitten Sie den Systemadministrator, die Richtlinienkonflikte vor dem Aktivieren von BitLocker zu beheben.
FVE_E_VIRTUALIZED_SPACE_TOO_BIG 0x80310089	Die angeforderte Virtualisierungsgröße ist zu groß.
FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON 0x80310090	Die BitLocker-Laufwerkverschlüsselung kann aufgrund in Konflikt stehender Gruppenrichtlinieneinstellungen für Wiederherstellungsoptionen auf Betriebssystem-Laufwerken nicht für das Laufwerk verwendet werden. Das Speichern von Wiederherstellungsinformationen in Active Directory-Domänendienste kann nicht angefordert werden, wenn die Generierung von Wiederherstellungskennwörtern nicht zulässig ist. Bitten Sie den Systemadministrator, die Richtlinienkonflikte vor dem Aktivieren von BitLocker zu beheben.
FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON 0x80310091	Die BitLocker-Laufwerkverschlüsselung kann aufgrund in Konflikt stehender Gruppenrichtlinieneinstellungen für Wiederherstellungsoptionen auf integrierten Datenlaufwerken nicht für das Laufwerk verwendet werden. Das Speichern von Wiederherstellungsinformationen in Active Directory-Domänendienste kann nicht angefordert werden, wenn die Generierung von Wiederherstellungskennwörtern nicht zulässig ist. Bitten Sie

Konstante/Wert	Beschreibung
	den Systemadministrator, die Richtlinienkonflikte vor dem Aktivieren von BitLocker zu beheben.
FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON 0x80310092	Die BitLocker-Laufwerkverschlüsselung kann aufgrund in Konflikt stehender Gruppenrichtlinieneinstellungen für Wiederherstellungsoptionen auf Wechseldatenlaufwerken nicht für das Laufwerk verwendet werden. Das Speichern von Wiederherstellungsinformationen in Active Directory-Domänendienste kann nicht angefordert werden, wenn die Generierung von Wiederherstellungskennwörtern nicht zulässig ist. Bitten Sie den Systemadministrator, die Richtlinienkonflikte vor dem Aktivieren von BitLocker zu beheben.
FVE_E_NON_BITLOCKER_KU 0x80310093	Aufgrund des Schlüsselverwendungsattributs (Key Usage, KU) des angegebenen Zertifikats kann selbiges nicht für die BitLocker-Laufwerkverschlüsselung verwendet werden. Zertifikate müssen für die Verwendung von BitLocker nicht zwingend über ein KU-Attribut verfügen, ist jedoch eines konfiguriert, muss es entweder auf "Schlüsselverschlüsselung" oder auf "Schlüsselvereinbarung" festgelegt sein.
FVE_E_PRIVATEKEY_AUTH_FAILED 0x80310094	Der private Schlüssel, der dem angegebenen Zertifikat zugeordnet ist, kann nicht autorisiert werden. Die Autorisierung für den privaten Schlüssel wurde entweder nicht bereitgestellt, oder die bereitgestellte Autorisierung war ungültig.
FVE_E_REMOVAL_OF_DRA_FAILED 0x80310095	Das Zertifikat des Datenwiederherstellungs-Agenten muss mit dem Zertifikat-Snap-In entfernt werden.
FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME 0x80310096	Dieses Laufwerk wurde mit der Version der BitLocker-Laufwerkverschlüsselung verschlüsselt, die in Windows Vista und Windows Server 2008 enthalten ist. Diese Version unterstützt keine organisatorischen Bezeichner. Aktualisieren Sie die Laufwerkverschlüsselung mithilfe des Befehls „manage-bde -upgrade“ auf die neueste Version, um organisatorische Bezeichner für das Laufwerk anzugeben.
FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME 0x80310097	Das Laufwerk kann nicht gesperrt werden, da es auf diesem Computer automatisch entsperrt wird. Entfernen Sie die Schutzvorrichtung für das automatische Entsperren, um dieses Laufwerk zu sperren.
FVE_E_FIPS_HASH_KDF_NOT_ALLOWED 0x80310098	Die standardmäßige BitLocker-Schlüsselableitungsfunktion "SP800-56A" für ECC-Smartcards wird von der verwendeten Smartcard nicht unterstützt. Aufgrund der Gruppenrichtlinieneinstellung, durch die die FIPS-Kompatibilität vorgeschrieben wird, kann von BitLocker keine andere Ableitungsfunktion zur Verschlüsselung verwendet werden. In durch FIPS eingeschränkten Umgebungen muss eine FIPS-kompatible Smartcard verwendet werden.
FVE_E_ENH_PIN_INVALID 0x80310099	Der BitLocker-Verschlüsselungsschlüssel konnte nicht über das TPM oder die erweiterte PIN abgerufen werden. Verwenden Sie eine nur aus Zahlen bestehende PIN.
FVE_E_INVALID_PIN_CHARS	Die angeforderte PIN des TPM enthält ungültige Zeichen.

Konstante/Wert	Beschreibung
0x8031009A	
FVE_E_INVALID_DATUM_TYPE 0x8031009B	Die auf dem Laufwerk gespeicherten Verwaltungsinformationen enthielten einen unbekannten Typ. Wenn Sie eine alte Version von Windows verwenden, greifen Sie von der aktuellen Version aus auf das Laufwerk zu.
FVE_E_EFI_ONLY 0x8031009C	Das Feature wird nur auf EFI-Systemen unterstützt.
FVE_E_MULTIPLE_NKP_CERTS 0x8031009D	Auf dem System wurde mehr als ein Netzwerkschlüssel-Schutzvorrichtungszertifikat gefunden.
FVE_E_REMOVAL_OF_NKP_FAILED 0x8031009E	Das Netzwerkschlüssel-Schutzvorrichtungszertifikat muss mithilfe des Zertifikate-Snap-Ins entfernt werden.
FVE_E_INVALID_NKP_CERT 0x8031009F	Im Netzwerkschlüssel-Schutzvorrichtungszertifikatspeicher wurde ein ungültiges Zertifikat gefunden.
FVE_E_NO_EXISTING_PIN 0x803100A0	Dieses Laufwerk ist nicht mit einer PIN geschützt.
FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH 0x803100A1	Geben Sie die korrekte aktuelle PIN ein.
FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100A2	Sie müssen mit einem Administratorkonto angemeldet sein, um die PIN oder das Kennwort ändern zu können. Klicken Sie auf den Link, um die PIN oder das Kennwort als Administrator zurückzusetzen.
FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED 0x803100A3	BitLocker hat PIN- und Kennwortänderungen nach zu vielen fehlgeschlagenen Anforderungen deaktiviert. Klicken Sie auf den Link, um die PIN oder das Kennwort als Administrator zurückzusetzen.
FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII 0x803100A4	Der Systemadministrator hat festgelegt, dass Kennwörter nur druckbare ASCII-Zeichen enthalten dürfen. Dies schließt Buchstaben ohne Akzentzeichen (A-Z, a-z), Ziffern (0-9), Leerzeichen, arithmetische Zeichen, allgemeine Zeichensetzung, Trennzeichen und die folgenden Symbole ein: # $ & @ ^ _ ~.
FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE 0x803100A5	Die BitLocker-Laufwerkverschlüsselung unterstützt Verschlüsselung, bei der nur verwendeter Speicherplatz verschlüsselt wird, nur für Speicher, der für schlanke Speicherzuweisung geeignet ist.
FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE 0x803100A6	Das Löschen von freiem Speicher bei schlanker Speicherzuweisung wird von der BitLocker-Laufwerkverschlüsselung nicht unterstützt.
FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE 0x803100A7	Die erforderliche Länge des Authentifizierungsschlüssels wird vom Laufwerk nicht unterstützt.
FVE_E_NO_EXISTING_PASSPHRASE	Dieses Laufwerk ist nicht mit einem Kennwort geschützt.

Konstante/Wert	Beschreibung
0x803100A8	
FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH 0x803100A9	Geben Sie das korrekte aktuelle Kennwort ein.
FVE_E_PASSPHRASE_TOO_LONG 0x803100AA	Das Kennwort darf maximal 256 Zeichen enthalten.
FVE_E_NO_PASSPHRASE_WITH_TPM 0x803100AB	Eine Kennwortschlüssel-Schutzvorrichtung kann nicht hinzugefügt werden, da auf dem Laufwerk eine TPM-Schutzvorrichtung vorhanden ist.
FVE_E_NO_TPM_WITH_PASSPHRASE 0x803100AC	Eine TPM-Schlüsselschutzvorrichtung kann nicht hinzugefügt werden, da auf dem Laufwerk eine Kennwortschutzvorrichtung vorhanden ist.
FVE_E_NOT_ALLOWED_ON_CSV_STACK 0x803100AD	Dieser Befehl kann nur über den Koordinatorknoten für das angegebene CSV-Volume ausgeführt werden.
FVE_E_NOT_ALLOWED_ON_CLUSTER 0x803100AE	Dieser Befehl kann nicht für ein Volume ausgeführt werden, das Teil eines Clusters ist.
FVE_E_EDRIVE_NO_FAILOVER_TO_SW 0x803100AF	BitLocker wurde aufgrund der Konfiguration der Gruppenrichtlinie nicht auf die Verwendung der BitLocker-Softwareverschlüsselung zurückgesetzt.
FVE_E_EDRIVE_BAND_IN_USE 0x803100B0	Das Laufwerk kann nicht von BitLocker verwaltet werden, da die Hardwareverschlüsselungsfunktion des Laufwerks bereits verwendet wird.
FVE_E_EDRIVE_DISALLOWED_BY_GP 0x803100B1	Laut Gruppenrichtlinieneinstellungen ist keine Verwendung von hardwarebasierter Verschlüsselung zulässig.
FVE_E_EDRIVE_INCOMPATIBLE_VOLUME 0x803100B2	Das angegebene Laufwerk unterstützt keine hardwarebasierte Verschlüsselung.
FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING 0x803100B3	BitLocker kann nicht während der Laufwerkverschlüsselung oder -entschlüsselung aktualisiert werden.
FVE_E_EDRIVE_DV_NOT_SUPPORTED 0x803100B4	Ermittlungsvolumes werden für Volumes, die Hardwareverschlüsselung verwenden, nicht unterstützt.
FVE_E_NO_PREBOOT_KEYBOARD_DETECTED 0x803100B5	Keine Preboot-Tastatur erkannt. Der Benutzer kann möglicherweise nicht die erforderlichen Angaben zum Entsperren des Volumes machen.
FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED 0x803100B6	Es wurde keine Preboot-Tastatur oder Windows-Wiederherstellungsumgebung gefunden. Der Benutzer kann möglicherweise nicht die erforderlichen Angaben zum Entsperren des Volumes machen.
FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE 0x803100B7	Die Gruppenrichtlinieneinstellungen verlangen die Erstellung einer Start-PIN, aber auf dem Gerät ist keine Preboot-Tastatur verfügbar. Der Benutzer kann möglicherweise nicht

Konstante/Wert	Beschreibung
	die erforderlichen Angaben zum Entsperren des Volumes machen.
FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE 0x803100B8	Die Gruppenrichtlinieneinstellungen verlangen die Erstellung eines Wiederherstellungskennworts, aber auf dem Gerät ist weder eine Preboot-Tastatur noch die Windows-Wiederherstellungsumgebung verfügbar. Der Benutzer kann möglicherweise nicht die erforderlichen Angaben zum Entsperren des Volumes machen.
FVE_E_WIPE_CANCEL_NOT_APPLICABLE 0x803100B9	Derzeit wird kein freier Speicher gelöscht.
FVE_E_SECUREBOOT_DISABLED 0x803100BA	BitLocker kann für die Plattformintegrität kein sicheres Starten verwenden, da diese Funktion deaktiviert wurde.
FVE_E_SECUREBOOT_CONFIGURATION_INVALID 0x803100BB	BitLocker kann für die Plattformintegrität kein sicheres Starten verwenden, da die Konfiguration für sicheres Starten nicht den Anforderungen für BitLocker entspricht.
FVE_E_EDRIVE_DRY_RUN_FAILED 0x803100BC	Vom Computer wird keine hardwarebasierte BitLocker-Verschlüsselung unterstützt. Erkundigen Sie sich beim Hersteller des Computers nach Firmwareupdates.
FVE_E_SHADOW_COPY_PRESENT 0x803100BD	BitLocker kann auf dem Volume nicht aktiviert werden, da es eine Volumeschattenkopie enthält. Entfernen Sie alle Volumenschattenkopien, bevor Sie das Volume verschlüsseln.
FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS 0x803100BE	Die BitLocker-Laufwerkverschlüsselung kann nicht auf das Laufwerk angewendet werden, da die Gruppenrichtlinieneinstellung für die erweiterten Startkonfigurationsdaten ungültige Daten enthält. Lassen Sie die ungültige Konfiguration vom Systemadministrator entfernen, bevor Sie erneut versuchen, BitLocker zu aktivieren.
FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE 0x803100BF	Die Firmware des PCs unterstützt keine Hardwareverschlüsselung.
FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED 0x803100C0	BitLocker hat Kennwortänderungen nach zu vielen fehlgeschlagenen Anforderungen deaktiviert. Klicken Sie auf den Link, um das Kennwort als Administrator zurückzusetzen.
FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100C1	Sie müssen mit einem Administratorkonto angemeldet sein, um das Kennwort zu ändern. Klicken Sie auf den Link, um das Kennwort als Administrator zurückzusetzen.
FVE_E_LIVEID_ACCOUNT_SUSPENDED 0x803100C2	Das Wiederherstellungskennwort kann von BitLocker nicht gespeichert werden, da das angegebene Microsoft-Konto derzeit angehalten ist.
FVE_E_LIVEID_ACCOUNT_BLOCKED 0x803100C3	Das Wiederherstellungskennwort kann von BitLocker nicht gespeichert werden, da das angegebene Microsoft-Konto derzeit blockiert ist.

Konstante/Wert	Beschreibung
FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES 0x803100C4	Dieser Computer wurde nicht zur Unterstützung der Geräteverschlüsselung bereitgestellt. Aktivieren Sie BitLocker auf allen Volumes, um die Geräteverschlüsselungsrichtlinie zu erfüllen.
FVE_E_DE_FIXED_DATA_NOT_SUPPORTED 0x803100C5	Dieser Computer kann die Geräteverschlüsselung nicht unterstützen, da nicht vorhandene feste Datenvolumes vorhanden sind.
FVE_E_DE_HARDWARE_NOT_COMPLIANT 0x803100C6	Dieser Computer erfüllt nicht die Hardwareanforderungen zum Unterstützen der Geräteverschlüsselung.
FVE_E_DE_WINRE_NOT_CONFIGURED 0x803100C7	Dieser Computer kann die Geräteverschlüsselung nicht unterstützen, da die Windows-Wiederherstellungsumgebung (WinRE) nicht ordnungsgemäß konfiguriert ist.
FVE_E_DE_PROTECTION_SUSPENDED 0x803100C8	Auf dem Volume ist der Schutz zwar aktiviert, aber angehalten. Dies ist wahrscheinlich darauf zurückzuführen, dass ein Update auf das System angewendet wurde. Wiederholen Sie den Vorgang nach einem Neustart.
FVE_E_DE_OS_VOLUME_NOT_PROTECTED 0x803100C9	Dieser Computer wurde nicht zur Unterstützung der Geräteverschlüsselung bereitgestellt.
FVE_E_DE_DEVICE_LOCKEDOUT 0x803100CA	Die Gerätesperre wurde aufgrund zu vieler ungültiger Kennworteingaben ausgelöst.
FVE_E_DE_PROTECTION_NOT_YET_ENABLED 0x803100CB	Der Schutz wurde auf dem Volume nicht aktiviert. Zur Aktivierung ist ein verbundenes Konto erforderlich. Wenn Sie bereits über ein verbundenes Konto verfügen und dieser Fehler auftritt, finden Sie im Ereignisprotokoll weitere Informationen.
FVE_E_INVALID_PIN_CHARS_DETAILED 0x803100CC	Die PIN darf nur Zahlen von 0 bis 9 enthalten.
FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE 0x803100CD	Der Schutz für Hardwarewiedergabe kann von BitLocker nicht verwendet werden, da kein Indikator auf dem PC verfügbar ist.
FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH 0x803100CE	Fehler bei der Statusüberprüfung der Gerätesperrung aufgrund von nicht übereinstimmenden Indikatoren.
FVE_E_BUFFER_TOO_LARGE 0x803100CF	Der Eingabepuffer ist zu groß.

20

Glossar

Aktivieren – Eine Aktivierung erfolgt, wenn der Computer beim Dell Server registriert wurde und mindestens einen Satz mit Richtlinien erhalten hat.

Active Directory (AD) – Ein Verzeichnisdienst von Microsoft für Windows-Domänennetzwerke.

Advanced Threat Prevention – Das Produkt Advanced Threat Prevention ist der Virenschutz der nächsten Generation, der algorithmische Wissenschaft und maschinelles Lernen einsetzt, um bekannte sowie unbekannte Cyber-Bedrohungen zu identifizieren, zu klassifizieren und von der Ausführung bzw. der Beschädigung von Endpunkten abzuhalten. Die optionale Client-Firewall-Funktion überwacht die Datenübertragung zwischen Computer und Ressourcen im Netzwerk und im Internet und fängt potenziell verdächtige Datenübertragungen ab. Die optionale Web-Schutz-Funktion blockiert basierend auf den Sicherheitsbewertungen und Berichten für Websites unsichere Websites und Downloads von diesen Websites, während online navigiert wird und Suchvorgänge ausgeführt werden.

Anwendungsdatenverschlüsselung – ADE (Application Data Encryption) verschlüsselt jede Datei, die von einer geschützten Anwendung geschrieben wird, mit einer Aufhebung der Kategorie 2. Das bedeutet, dass jedes Verzeichnis mit einem Schutz der Kategorie 2 oder höher oder jeder Ort, an dem bestimmte Erweiterungen mit Kategorie 2 oder höher geschützt sind, nicht durch ADE verschlüsselt werden.

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.

Im Cache gespeicherte Anmeldedaten – Gespeicherte Anmeldedaten werden in die PBA-Datenbank aufgenommen, wenn ein Benutzer sich mit Active Directory authentifiziert. Die Benutzerdaten werden gespeichert, damit die Anmeldung auch ohne Verbindung zu Active Directory funktioniert (beispielsweise bei Verwendung des Laptops außerhalb der Geschäftszeiten).

Allgemeine Verschlüsselung – Der allgemeine Schlüssel macht verschlüsselte Dateien allen verwalteten Benutzern auf dem Gerät zugänglich, auf dem sie erstellt wurden.

Deaktivieren – Die Deaktivierung erfolgt, wenn SED Manager 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 Dienst innerhalb von Encryption schützt Wechseldatenträger und externe Speichergeräte.

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

Endpunkt – Je nach Kontext ein Computer, ein mobiles Gerät oder ein externer Datenträger.

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

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

Preboot-Authentifizierung (PBA) – Die Preboot-Authentifizierung dient als Erweiterung des BIOS oder der Systemstart-Firmware und schafft eine sichere, manipulationsgeschützte Umgebung außerhalb des Betriebssystems als vertrauenswürdige Authentifizierungsebene. Die PBA unterbindet den Zugriff auf die Festplatte und somit auch auf das Betriebssystem, bis der Benutzer die richtigen Anmeldeinformationen eingibt.

Skriptsteuerung – Die Skriptsteuerung schützt Geräte, indem die Ausführung bösartiger Skripte gesperrt wird.

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

Serverbenutzer – Ein virtuelles Benutzerkonto, das durch Encryption erstellt wird und für die Verarbeitung von Verschlüsselungsschlüsseln und Richtlinienaktualisierungen auf einem Serverbetriebssystem 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.

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

Trusted Platform Module (TPM) – Das TPM ist ein Sicherheits-Chip mit drei Hauptfunktionen: sicherer Speicher, Messung und Bestätigung. Beim Encryption-Client wird das TPM für den sicheren Speicher genutzt. Das TPM kann auch verschlüsselte Container für den Software Vault bereitstellen.

Benutzerverschlüsselung – Der Benutzerschlüssel macht Dateien nur dem Benutzer zugänglich, der sie erstellt hat, und zwar nur auf dem Gerät, auf dem sie erstellt wurden. Bei Ausführung von Dell Server Encryption wird die Benutzerverschlüsselung in eine allgemeine Verschlüsselung konvertiert. Für Wechselmedien wird eine Ausnahme gemacht; Dateien werden bei Einsetzen in einen Server mit installiertem Encryption mit dem Benutzer-Roaming-Schlüssel verschlüsselt.