# DriveLock

## Release Notes 2019.2 SP1

DriveLock SE 2020

# Inhaltsverzeichnis

# 1 Release Notes 2019.2 SP1

Die Release Notes enthalten wichtige Informationen zur neuen Version von DriveLock. Ebenfalls sind in den Release Notes Änderungen oder Ergänzungen enthalten, die es kurzfristig nicht mehr in die Dokumentation geschafft haben.

Diese und weitere Anleitungen finden Sie auch unter www.drivelock.help.

## 1.1 Konventionen

In diesem Dokument werden durchgängig folgende Konventionen und Symbole verwendet, um wichtige Aspekte hervorzuheben oder Objekte zu visualisieren.

> Achtung: Roter Text weist auf Risiken hin, die beispielsweise zu Datenverlust führen können

> Hinweis: Hinweise und Tipps enthalten nützliche Zusatzinformationen.

**Menüeinträge** oder die **Namen von Schaltflächen** sind fett dargestellt. *Kursive Schrift* repräsentiert Felder, Menüpunkte und Querverweise.

`Systemschrift` stellt Nachrichten oder Befehle auf Basis der Kommandozeile dar.

Ein Pluszeichen zwischen zwei Tasten bedeutet, dass diese gleichzeitig gedrückt werden müssen: „ALT + R" beispielsweise signalisiert das Halten der ALT-Taste, während R gedrückt wird. Ein Komma zwischen mehreren Tasten fordert ein Nacheinander-Drücken der jeweiligen Tasten. „ALT, R, U" bedeutet, dass zunächst die ALT-Taste, dann die R- und zuletzt die U-Taste betätigt werden muss.

## 1.2 Verfügbare Dokumentation

> Hinweis: Aufgrund von Umstrukturierung und Aktualisierung wird unsere Dokumentation in Zukunft häufiger und unabhängig von DriveLock-Releases auf den neuesten Stand gebracht. Auf unserem Dokumentationsportal drivelock.help finden Sie unsere aktuellsten Versionen.

Die DriveLock Dokumentation besteht derzeit aus diesen Dokumenten mit folgenden Inhalten:

- **DriveLock QuickStart Guide**
  Die Anleitung beschreibt die notwendigen Schritte um DriveLock mit dem DriveLock QuickStart Assistenten aufzusetzen. Der DriveLock QuickStart Assistent kann

verwendet werden, um die Installation und Konfiguration einer grundlegenden DriveLock-Umgebung zu vereinfachen.

- **DriveLock Installationshandbuch**
  Dieses Dokument beschreibt die verfügbaren Installationspakete und verschiedenen Installationsschritte der einzelnen Komponenten. Es ist das erste Dokument nach den Release Notes, welches Sie bei einer Neuinstallation lesen sollten.
- **DriveLock Administrationshandbuch**
  Das Administrationshandbuch beschreibt die Architektur von DriveLock, die verschiedenen Komponenten und dokumentiert die komplette Administration von DriveLock über die DriveLock Management Konsole (DMC). Dieses Dokument ist für Administratoren von DriveLock gedacht, die sich mit allen einzelnen Funktionen vertraut machen möchten.
- **DriveLock Control Center Benutzerhandbuch**
  In diesem Handbuch wird die Konfiguration und Verwendung des DriveLock Control Centers (DCC) beschrieben. Dieses Handbuch ist für Administratoren und für Anwender gedacht, die das DriveLock Control Center verwenden.

  Hinweis: Bitte beachten Sie, dass das DriveLock Control Center (DCC) noch in diesem Jahr vom DriveLock Operations Center (DOC) abgelöst wird.

- **DriveLock Benutzerhandbuch**
  Das DriveLock Benutzerhandbuch beinhaltet die Dokumentation aller Funktionen, die für den Endanwender zur Verfügung stehen (Temporäre Freigabe, Verschlüsselung und private Netzwerkprofile). Das Benutzerhandbuch dient Endanwendern zur Orientierung bei den für sie zur Verfügung stehenden Möglichkeiten.
- **DriveLock Security Awareness**
  Dieses Handbuch beschreibt die neuen Security Awareness Funktionen, welche auch die Basis des Produktes DriveLock Smart SecurityEducation bilden.
- **DriveLock Linux-Agent**

  Dieses Handbuch beschreibt die Installation und Konfiguration des DriveLock Agenten auf Linux-Betriebssystemen.
- **DriveLock BitLocker Management**

  Das Handbuch beschreibt die Funktionalität und Konfiguration von DriveLock BitLocker Management sowie die notwendigen Einstellungen, die für die Fest-

plattenverschlüsselung mit Microsoft BitLocker in einer DriveLock-Umgebung zur Verfügung stehen.
Das Kapitel **DriveLock Pre-Boot-Authentifizierung** beschreibt die Vorgehensweise, um die DriveLock PBA zur Authentifizierung von Benutzern einrichten und verwenden zu können, sowie Lösungswege zur Wiederherstellung bzw. Notfallanmeldung.
Das Kapitel **BitLocker To Go** beschreibt die Konfigurationseinstellungen, die notwendig sind, um mit BitLocker To Go verschlüsselte Laufwerke mit DriveLock zu verwalten.

# 2 Update von DriveLock

Wenn Sie auf höhere Versionen von DriveLock aktualisieren, beachten Sie bitte folgende Informationen.

## 2.1 Update des DriveLock Agenten

**Beachten Sie bitte folgendes, wenn Sie den DriveLock Agenten auf eine neuere Version aktualisieren:**

1. Vor dem DriveLock Agent-Update:
   - Prüfen Sie, ob der DriveLock Update Service **dlupdate** auf dem System vorhanden ist und entfernen Sie diesen gegebenenfalls.
   - Wenn Sie den Agenten mit Hilfe des Autoupdate-Mechanismus von DriveLock aktualisieren, setzen Sie in der DriveLock Richtlinie die **Einstellungen** für die **Automatische Aktualisierung** folgendermaßen:
     - Wählen Sie die Option **Zur Aktualisierung des Agenten neu starten** aus und setzen den Wert für eine Verzögerung durch einen Benutzer auf **0**, um die Zeit zu einem Neustart des Rechners möglichst kurz zu halten.
   - Setzen Sie außerdem folgende **Einstellungen**:
     - **DriveLock-Agentendienste im Nicht-beenden-Modus starten**: Deaktiviert
     - **Kennwort zum Deinstallieren von DriveLock**: Nicht konfiguriert
   - Wenn Sie eine Festplattenverschlüsselung im Einsatz haben, muss die Verzögerung für eine mögliche Deinstallation in den Verschlüsselungseinstellungen auf mindestens 5 Tage gesetzt werden.
   - Bei der Verwendung von BitLocker Management muss vor der Aktualisierung folgendes beachtet werden (Details finden Sie in der BitLocker Management Dokumentation auf DriveLock Online Help):
     Die neue Einstellung für die Verschlüsselung **Keine Entschlüsselung durchführen** verhindert eine mögliche Änderung des Verschlüsselungsstatus der DriveLock Agenten. Vor der Aktualisierung ist es daher notwendig, dass diese Option in der aktuellen Verschlüsselungsrichtlinie aktiviert und die Richtlinie im Anschluss gespeichert und veröffentlicht wird.
2. Während des DriveLock Agent-Updates:
   - Führen Sie die Aktualisierung mit einem privilegierten Adminstrator-Konto durch. Das ist beim Autoupdate bereits automatisch der Fall.

3. Nach dem DriveLock Agent-Update:
    - Zur Aktualisierung der Treiberkomponenten ist ein Neustart nach dem DriveLock Agent-Update erforderlich. Fügen Sie diesen Schritt bei einer Aktualisierung durch eine Softwareverteilung in den Update-Ablauf ein bzw. starten Sie den aktualisierten Rechner manuell neu.

## 2.2 Update der DriveLock Komponenten

### Generelle Informationen zum Update auf die aktuelle Version

- Das DriveLock Installationshandbuch beschreibt alle notwendigen Schritte, die bei einem Update auf die aktuellste Version durchzuführen sind.
- Die DriveLock Management Konsole und das DriveLock Control Center werden jeweils in eigenen Verzeichnissen installiert. Dadurch werden Wechselwirkungen bei einem automatischen Update dieser Komponenten vermieden.

> Hinweis: Das DriveLock Control Center benötigt für die Fernwartung einige Komponenten der DriveLock Management Konsole. Beide Komponenten müssen dabei die gleiche Versionsnummer haben, die auch mit der Version des installierten DES übereinstimmen muss.

### Wichtige Information zu Zertifikaten

In der Version 2019.2 befindet sich das neue Tool **ChangeDesCert.exe** im Programmverzeichnis des DriveLock Enterprise Services (DES) unter C:\Program Files\CenterTools\DriveLock Enterprise Service\ChangeDesCert.exe. Beachten Sie dazu folgendes: Wenn Sie ein vorhandenes DES-Server-Zertifikat mit dem Tool austauschen möchten, muss das neue Zertifikat in den Computer-Zertifikatspeicher importiert und der private Schlüssel als exportierbar konfiguriert werden.

> Achtung: Das bestehende selbst-signierte DES-Zertifikat kann bei einem Update von Version 7.x auf 2019.1 nicht mehr verwendet werden und wird durch ein neu erzeugtes Zertifikat ersetzt. Dieses kann dann automatisch als selbst-signiertes Zertifikat erstellt und im Zertifikatsspeicher des Computers gespeichert werden.
> Bei einem Update von 2019.1 auf 2019.2 können Sie das selbst-signierte DES-Zertifikat hingegen weiter verwenden.

### Update der Disk Protection

Nach dem Update des DriveLock Agenten wird eine ggf. vorhandene Disk Protection Installation ohne Neuverschlüsselung automatisch auf die neueste Version aktualisiert. Nach dem Update der Disk Protection muss ggf. ein Neustart erfolgen.

Wir haben weitere Informationen, die für ein Update der DriveLock Disk Protection bzw. ein Update des Betriebssystems bei einer installierten DriveLock Disk Protection wichtig sind, in einem eigenen Dokument für Sie zusammengestellt. Dieses finden sie ebenfalls auf unserer Webseite www.drivelock.help.

# 3 Systemvoraussetzungen

Die in diesem Abschnitt genannten Werte stellen Empfehlungen und Mindestanforderungen dar. Je nach Konfiguration von DriveLock, der verwendeten Komponenten und Funktionen sowie Ihrer Systemumgebungen können die tatsächlichen Voraussetzungen davon abweichen.

> Hinweis: Microsoft veröffentlicht regelmäßig Software-Patches für seine Softwareprodukte am sogenannten Microsoft Patchday, Patch oder Update Tuesday. DriveLock unterstützt diese Microsoft-Updates vollständig mit den unter DriveLock Agent (Abschnitt Unterstützte Plattformen) beschriebenen Microsoft Betriebssystemversionen.

## 3.1 DriveLock Agent

Bevor Sie den DriveLock Agenten in Ihrem Unternehmensnetzwerk verteilen/installieren, stellen Sie bitte sicher, dass die Computer folgende Voraussetzungen erfüllen, um eine vollständige Funktionalität zu gewährleisten:

**Hauptspeicher:**

- mind. 4 GB RAM

**Freier Festplattenspeicherplatz:**

- ca. 1 GB bei durchschnittlichen Richtlinien ohne eigene Videodateien
- mindestens 2 GB bei der Verwendung von Security Awareness Kampagnen mit Videosequenzen (Security Awareness Content AddOn)

> Hinweis: Der benötigte Festplattenplatz hängt stark von der Konfiguration der DriveLock Agenten über Richtlinien und den darin vorhandenen Einstellungen und verwendeten Funktionalitäten ab. Daher ist eine genaue Vorgabe an dieser Stelle nicht möglich und der zu berücksichtigende Wert sollte vor einem unternehmensweiten Roll-Out in einer Teststellung mit wenigen Systemen überprüft und ermittelt werden.

**Benötigte Windows-Komponenten:**

- .NET Framework 4.5.2 oder neuer (Für Security Awareness Kampagnen allgemein)
- KB3140245 muss auf Windows 7 installiert sein
  Weitere Informationen dazu finden Sie hier und hier.
  Ohne dieses Update kann WinHTTP keine TLS Einstellungen ändern und der Fehler

12175 erscheint in dlwsconsumer.log und DLUpdSvx.log.

- KB3033929 (SHA-2 code signing support) muss auf Windows 7 64-bit installiert sein.

**Unterstützte Plattformen:**

DriveLock unterstützt folgende Windows Versionen für die aufgelisteten Agenten-Versionen:

| OS-Version | 2019.2 | 2019.1 | 7.9.6 |
|---|---|---|---|
| Windows 10 Pro | | | |
| Windows 10-1909 | + | + | - |
| Windows 10-1903 | + | + | - |
| Windows 10-1809 | + | + | + |
| Windows 10-1803 | + | + | + |
| Windows 10-1709 | - | + | + |
| Windows 10-1703 | - | + | + |
| Windows 10-1607 | - | + | + |
| Windows 10 Enterprise | | | |
| Windows 10 Enterprise-1909 | + | + | - |
| Windows 10 Enterprise-1903 | + | + | - |
| Windows 10 Enterprise-1809 | + | + | + |
| Windows 10 Enterprise-1709 | + | + | + |
| Windows 10 Enterprise-1703 | - | + | + |
| Windows 10 Enterprise-1607 | - | + | + |
| Windows 10 Enterprise LTSB/LTSC | | | |

| OS-Version | 2019.2 | 2019.1 | 7.9.6 |
|---|---|---|---|
| Windows 10 Enterprise 2019 LTSC | + | + | + |
| Windows 10 Enterprise 2016 LTSB | + | + | + |
| Windows 10 Enterprise 2015 LTSB | + | + | + |
| Windows Server | | | |
| Windows Server 2019 | + | + | + |
| Windows Server 2016 | + | + | + |
| Windows Server 2012 R2 | + | + | + |
| Windows Server 2012 | + | + | + |
| Windows Server 2008 R2 SP1 | + | + | + |
| Windows Server 2008 SP2 | + | + | + |
| Ältere Windows Versionen | | | |
| Windows 8.1 | + | + | + |
| Windows 7 SP1 | + | + | + |
| Windows XP | Support Lizenz notwendig | Support Lizenz notwendig | Support Lizenz notwendig |

Achtung: Wir empfehlen allen Kunden, unsere aktuellste Version zu installieren.

Der DriveLock Agent ist verfügbar für Intel X86 basierte Systeme (32-Bit und 64-Bit Architektur). Für den Einsatz des DriveLock Agenten wird ein 64-Bit System empfohlen. Server-Betriebssysteme werden ausschließlich unter 64-Bit getestet.

Hinweis: Beachten Sie bitte auch die Hinweise zum DriveLock Agent-Update.

### Einschränkungen

- DriveLock Disk Protection ist nur für den Betrieb unter XP, welches in bestimmten Geldautomaten verwendet wird, freigegeben.
- Windows XP Embedded: Der DriveLock Virtual Channel und der DriveLock Agent dürfen nicht auf dem gleichen Client installiert sein.
- Auf Windows 7 Systemen mit TPM wird DriveLock BitLocker Management nur für 64-Bit Systeme unterstützt, nicht für 32 Bit.
- Disk Protection UEFI und GPT Partitioning ist unterstützt für Festplatten bis max. 2 TB für Windows 8.1 64-Bit oder neuer und UEFI Version V2.3.1 oder neuer.
- Der Agenten-Status ist ab Version 2019.2 ein separater Optionseintrag und muss explizit konfiguriert werden. Die Standardeinstellung ist, keinen Status anzuzeigen.

Hinweis: Microsoft hat den Support für ihr Betriebssystem Windows 7 zum Januar 2020 eingestellt. DriveLock wird Windows 7 mit einer regulären Client-Lizenz jedoch bis auf weiteres unterstützen. Wir informieren unsere Kunden rechtzeitig, wenn Windows 7 unter den erweiterten Legacy-Support gestellt werden sollte. Dies wird frühestens nach DriveLock Version 2020.2 der Fall sein

### Citrix Umgebungen

Der DriveLock Agent benötigt die folgenden Systemvoraussetzungen, damit die DriveLock Device Control Funktionalität grundsätzlich genutzt werden kann:

- XenApp 6.5 Hotfix Roll Up 4 oder neuer (ICA).
- Windows Terminal Server 2012 oder 2016 (RDP).
- DriveLock File Protection ist unter Citrix Terminal Server nicht unterstützt.

Achtung: Beachten Sie bitte die Änderungen der Citrix-Produktnamen. Weitere Informationen finden Sie unter https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/1808/whats-new.html (Referenz zur Citrix-Namensänderung: EI-768 (INC04120))

## 3.2 DriveLock Management Console und Control Center

Hinweis: Bitte installieren Sie die beiden Management Komponenten auf dem gleichen Rechner, da das DCC auf einige der von der DriveLock Management Konsole bereitgestellten Dialoge zurückgreift.

Bevor Sie die beiden Programme auf einem Rechner installieren, stellen Sie bitte sicher, dass der Computer für eine vollständige Funktionalität diese Voraussetzungen erfüllt.

**Hauptspeicher:**

- mind. 4 GB RAM

**Freier Festplattenspeicherplatz:**

- ca. 350 MB

**Benötigte zusätzliche Windowskomponenten:**

- .NET Framework 4.5.2 oder höher
- Für Fernverbindungen über das DCC wird Internet Explorer 11 oder neuer benötigt

**Unterstützte Plattformen:**

Die beiden DriveLock 2019.2 Management Konsolen wurden getestet und freigegeben auf den aktuellsten Ständen der Windows Versionen, die zum Zeitpunkt des Release offiziell verfügbar waren und die bei Microsoft das Ende des Service-Zeitraumes noch nicht erreicht haben. Im Kapitel DriveLock Agent finden Sie eine Auflistung der Windows Versionen, die DriveLock unterstützt.

Die beiden DriveLock Management Konsolen sind verfügbar für Intel X86 basierte Systeme (32-Bit und 64-Bit Architektur). Für den Einsatz im Unternehmen wird ein 64-Bit System empfohlen. Server-Betriebssysteme werden ausschließlich unter 64-Bit getestet.

### 3.3 DriveLock Enterprise Service

Bevor Sie den DriveLock Enterprise Service auf einem Rechner installieren, stellen Sie bitte sicher, dass der Computer für eine vollständige Funktionalität diese Voraussetzungen erfüllt.

**Hauptspeicher:**

- mind. 8 GB RAM

**Freier Festplattenspeicherplatz:**

- mind. 4 GB, bei der Verwendung von Security Awareness Content (Video) wird ein freier Speicher von mind. 15 GB empfohlen.
- Soll auf dem Server gleichzeitig noch eine SQL-Datenbank betrieben werden, sind zusätzlich zu der dafür notwendigen Festplattenkapazität auch noch mind. 10 GB für die Speicherung der DriveLock Daten vorzusehen.

**Benötigte zusätzliche Windowskomponenten:**

- .NET Framework 4.5.2 oder höher

Hinweis: Die Größe der DriveLock Datenbank wird maßgeblich von der Anzahl und dem Zeitraum der gespeicherten DriveLock Events beeinflusst und kann je nach Systemumgebung stark variieren. Eine genaue Vorgabe ist daher an dieser Stelle nicht möglich. Genaue Werte sollten in einer Teststellung mit den geplanten Einstellungen über einen Zeitraum von mindestens einigen Tagen ermittelt werden. Diese können dann als Grundlage für die Berechnung der benötigten Speicherkapazität dienen.

**Unterstützte Plattformen:**

- Windows Server 2012 R2 64-Bit (Mindestvoraussetzung für das DriveLock Operations Center)
- Windows Server 2016 64-Bit
- Windows Server 2019 64-Bit

Auf einem Windows 10 Client Betriebssystem sollte ein DES nur als Testinstallation betrieben werden.

Achtung: Ab DriveLock Version 2020.1 wird keine 32-Bit-Version des DES mehr ausgeliefert.

**Unterstützte Datenbanken:**

- SQL-Server 2012 (Mindestvoraussetzung für das DriveLock Operations Center)
- SQL-Server 2014
- SQL-Server 2016
- SQL-Server 2017
- SQL-Server 2019
- SQL-Server Express 2012 oder neuer (für Installationen mit bis zu 200 Clients und Testinstallationen)

Achtung: Oracle Support EOL - Seit Version 2019.1 wird Oracle als Datenbank nicht mehr unterstützt. Das neue DOC und DriveLock 2019.2 funktioniert nur noch mit Microsoft SQL-Server. Auch zukünftige DriveLock Versionen werden nur noch Microsoft SQL-Server unterstützen.

Achtung: Für die Datenbankverbindung zwischen dem DriveLock Operations Center und der Datenbank wird eine TCP/IP Verbindung benötigt.

**Weitere Einschränkungen in Version 2019.2:**

- Der Service-Account, unter dem der verlinkte DES betrieben wird, benötigt Zugriff auf den privaten Schlüssel des DES-Zertifikates im Computerkonto.

# 4 Versionshistorie

Die Versionshistorie gibt einen Überblick über alle Neuerungen, Änderungen und Fehlerbehebungen seit Ausgabe der letzten DriveLock Version.

## 4.1 Version 2019.2 SP1

DriveLock 2019.2 SP1 ist ein Service Pack Release.

### 4.1.1 Neue Funktionen

#### DriveLock Linux Agent

Mit Version 2019.2 SP1 unterstützt DriveLock die Zuweisung von zentral gespeicherten Richtlinien auf DriveLock Agenten mit dem Betriebssystem Linux.

Der Funktionsumfang der Linux-Unterstützung beschränkt sich in dieser Version auf das Sperren von externen Geräten und Laufwerken, die über eine USB-Schnittstelle mit den Linux-Clients verbunden werden. DriveLock Administratoren haben somit die Möglichkeit, die Verwendung von externen Geräten und Laufwerken auch auf DriveLock Linux-Agenten so zu reglementieren, dass die Client-Computer zuverlässig vor Angriffen durch Schadsoftware geschützt sind.

Weitere Informationen sowie Anleitungen zur Installation und Konfiguration finden Sie in der Dokumentation zum DriveLock Linux-Agenten auf DriveLock Online Help.

#### BitLocker Management

Zusätzlich zur Einstellung für die Verzögerung der Entschlüsselung besteht nun auch die Möglichkeit, die Entschlüsselung komplett zu deaktivieren. Das hat den Vorteil, dass nach einem Update gar nicht erst entschlüsselt wird, sondern der Verschlüsselungsstatus gleich bleibt. Dadurch wird verhindert, dass sich die DriveLock Agenten kurzzeitig in einem ungeschützten Zustand befinden.

### 4.1.2 Fehlerbehebungen

#### Wichtige Fehlerkorrekturen in dieser Version

Dieses Kapitel enthält Informationen zu Fehlern, die mit der vorliegenden DriveLock-Version 2019.2 SP1 nun behoben sind.

Als Referenz dienen EI-Nummern, sofern vorhanden.

| Referenz | Agenten-Fernkontrolle |
|---|---|
| EI-749 | Eine Agentenfernverbindung über das DCC ist jetzt unabhängig vom angewendeten Filter möglich. |

| Referenz | Device Control |
|---|---|
| | Ein Popup, das fälschlicherweise angezeigt wurde, wird jetzt nicht mehr angezeigt, wenn ein neues Dokument gespeichert wird. |
| EI-776 | Der Fehler beim Laden von Smartphones nach der Installation von DriveLock ist behoben. |
| EI-489 | Ein Problem bei Terminal Servern, bei dem in seltenen Fällen unkonfigurierte Netzwerklaufwerke geblockt wurden, ist jetzt behoben. |

| Referenz | Disk Protection |
|---|---|
| EI-756 | Hardwarekompatibilitätsprobleme bei DELL 7400 2in1 Modelreihen in Verbindung mit Disk Protection wurden behoben. |

| Referenz | DriveLock Agent |
|---|---|
| | Die Prüfung des Anforderungscodes findet jetzt bereits bei der Eingabe statt. |

| Referenz | DriveLock Control Center (DCC) |
|---|---|
| EI-760 | Reporting/Forensik: Der Wert ADSPath wird in der DCC jetzt korrekt angezeigt. |

| Referenz | Encryption 2-Go |
|---|---|
| EI-639 | DriveLock Mobile für MAC OS verschlüsselt das Verzeichnis DriveLock.app nicht mehr. |
| EI-643 | Bei Benutzung eines verschlüsselten USB Gerätes wird die CPU jetzt nicht mehr zu stark belastet. |

| Referenz | File Protection |
|---|---|
| EI-825; EI-884; EI-876 | Verschiedene Fehler, die zum Absturz des File Protection-Treibers führten, wurden behoben. |
| EI-868 | Netzwerklaufwerke können jetzt wieder umbenannt werden, wenn File Protection aktiv ist |
| EI-537 | Zentral verwaltete Verzeichnisse können jetzt nur noch durch den Administrator komplett entschlüsselt werden. |
| EI-628 | Der Dialog zur automatischen Entschlüsselung wird nun jedes Mal bei USB-Verschlüsselung mit File Protection angezeigt. |

| Referenz | Gruppen und Berechtigungen |
|---|---|
| EI-791 | Bei der Auswertung der Gruppenzugehörigkeit wird nun auch der Global Catalog-Server korrekt abgefragt. |

| Referenz | Management Konsole (DMC) |
|---|---|
| | Die MMC kann jetzt auch sehr große CSV Dateien (> 100 kB) importieren. |

| Referenz | Lizenzierung |
|---|---|
| | Bei Aktualisierung einer Lizenz erfolgt nun keine Zuweisung mehr auf alle Computer. |

| Referenz | SB-Freigabe |
|---|---|
| EI-844 | Der SB-Freigabe-Assistent erlaubt jetzt keine Eingabe von Zeiten in der Vergangenheit mehr. |
| EI-538 | Die SB-Freigabe wird jetzt auch beendet (durch Anklicken der Check-box) wenn der Benutzer über RDP mit dem Rechner verbunden ist. |

| Referenz | Thin Clients |
|---|---|
| EI-794 | Der Absturz des Explorers, der in Zusammenhang mit Terminal Ser-vern auftrat, ist jetzt behoben. |

## 4.2 Version 2019.2 HF1

DriveLock 2019.2 HF1 ist ein Maintenance Release.

### 4.2.1 Fehlerbehebungen

#### Wichtige Fehlerkorrekturen in dieser Version

Dieses Kapitel enthält Informationen zu Fehlern, die mit der vorliegenden DriveLock-Version 2019.2 HF1 nun behoben sind.

Als Referenz dienen EI-Nummern, sofern vorhanden.

| Referenz | BitLocker Management |
|---|---|
| | Durch einen vom Agent geblockten Registry-Schlüssel war es möglich, dass lokale Gruppenrichtlinien nicht mehr ordnungsgemäß aktualisiert werden konnten. Dies hatte zur Folge, dass einzelne Gruppenrichtlinien gelöscht wurden und dadurch Anwendungen möglicherweise nicht mehr funktioniert haben. |

| Referenz | Device Control |
|---|---|
| | Die Funktionalität von Laufwerks- und Gerätelisten war nicht vorhanden, weil die Geräte bzw. Laufwerke auf den Listen bei Auswertung der Richtlinien nicht korrekt ermittelt wurden. |
| EI-820 | Die Gerätekontrolle mittels VolumeID funktionierte nicht korrekt. |

| Referenz | DriveLock Agent |
|---|---|
| EI-812 | Die Verbindung zum "Benachrichtigungsdienst für Systemereignisse" kann auf Windows 7 wiederhergestellt werden. Die Fehlermeldung im Explorer erscheint jetzt nicht mehr. |

| Referenz | DriveLock Control Center |
|---|---|
| EI-765, EI-749 | Die Einstellung "FQDN für Agentverb. verwenden" im DCC funktioniert wieder. |

| Referenz | Ereignisse |
|---|---|
| | Ereignisfilter-Definitionen lassen sich jetzt auch für Ereignisse ohne Parameter erzeugen. |

| Referenz | File Protection |
|---|---|
| EI-825 | Pfadangaben bzw. Dateinamen mit mehr als 384 Zeichen führen zu einem Blue Screen im File-Encryption-Treiber. Dieser Fehler wird im nächsten Release behoben sein. |

| Referenz | Richtlinien |
|---|---|
| EI-752 | Die DriveLock-Konfigurationsdateien wurden zwar korrekt geladen, aber der entsprechende Pfad wurde nicht für die Auswertung der Richtlinien herangezogen. |

## 4.3 Version 2019.2

DriveLock 2019.2 ist ein Feature Release.

### 4.3.1 Neue Funktionen und Verbesserungen

Die Version 2019.2 enthält eine Vielzahl an neuen Funktionalitäten und Verbesserungen. Der folgende Abschnitt bieten Ihnen einen ersten Überblick über die Neuerungen.

#### Applikationskontrolle

Diese Version stellt verbesserte Funktionen zur Malware-Abwehr bereit, indem die Whitelist-Technologie für alle Assets verbessert wurde:

- Besserer Schutz vor Angriffen ohne Dateien (file-less attacks) - Blockieren spezifischer Kindprozesse
- Application Control kann jetzt auch andere ausführbaren Dateien (z.B. .APPX - MSI, MST, MSP - PS1, BAT, CMD, VBS, JS, OCX, OCX) kontrollieren

Nun können Sie legitime Programme (für die ein Whitelist-Eintrag besteht) auf tatsächlich benötigte Aktionen und Berechtigungen weiter einschränken, um es Angreifern noch schwerer zu machen. Somit stellen Sie sicher, dass nur autorisierte Software und Skripte ausgeführt werden. Außerdem kontrollieren Sie jetzt auch den Zugriff auf Scripting-Tools (wie MS PowerShell, VBS, Python und Kommandozeile).

Die neue Anwendungs-Berechtigung bringt folgende Vorteile:

- Verhindern, dass aus einer erlaubten Anwendung heraus eine weitere Anwendung (bzw. Prozess, Skript) gestartet wird, die eine potentielle Gefahr für das System darstellen könnte
- Festlegen, welche Art von Zugriff einer bestimmten Anwendung erlaubt wird (z.B. lesend oder schreibend auf Dateien oder auf die Registry zuzugreifen).

#### Neue DriveLock Pre-Boot-Authentifizierung (PBA) mit BitLocker Support

Mit der Version 2019.2 steht eine neue DriveLock PBA zur Verfügung, die die bisherige DriveLock UEFI PBA ersetzt. Diese moderne PBA kann sowohl mit BitLocker als auch mit DriveLock Disk Protection verschlüsselten Laufwerken zusammenarbeiten. Die neue DriveLock PBA ist derzeit nur für Windows 10 64-Bit-Systeme verfügbar, die auf der UEFI-Plattform laufen. Um die neue PBA für BitLocker nutzen zu können, ist eine separate Lizenzoption notwendig (BitLocker PBA Add-On). Diese Lizenz setzt eine BitLocker Management Lizenz voraus. Folgende Funktionalitäten sind in dieser neuen PBA auch für eine BitLocker Verschlüsselung vorhanden:

- Anmeldung mit Benutzername/Kennwort
- Notfallanmeldung bei vergessenem Passwort per Challenge-Response Verfahren
- Single-Sign-On an Windows Anmeldung
- Anmeldung mit Smartcard und eToken
- Unterstützung verschiedener Tastatur-Layouts und ein virtuelles Keyboard
- Wechselbare PBA-Hintergrundbilder

**BitLocker To Go**

Ebenfalls neu ist die erzwungene Verschlüsselung von externen USB-Speichermedien mit BitLocker To Go. BitLocker To Go kann nun als weitere Verschlüsselung für die erzwungene Verschlüsselung ausgewählt werden.

Für die Authentifizierung steht wie auch bei der Container-Verschlüsselung Encryption 2-Go entweder ein Benutzer- oder ein zentrales administratives Passwort zur Verfügung. Mit letzterer Option können Sie so erzwingen, dass auf Daten nur innerhalb des Unternehmens zugegriffen werden kann. Bereits anderweitig mit BitLocker To Go verschlüsselte USB-Laufwerke werden bei der erzwungenen Verschlüsselung als schon verschlüsselt erkannt und nicht mehr neu verschlüsselt.

Recovery-Informationen zur Wiederherstellung verschlüsselter Daten werden wie sonst auch zum DES hochgeladen und dort zentral und sicher verschlüsselt gespeichert.

**Security Awareness**

Unter anderem bietet Security Awareness folgende Neuerungen:

- Security-Awareness-Kampagnen können jetzt vom Benutzer nach Bedarf ausgewählt und angesehen werden
- Administratoren können einen Vollbildmodus zur Anzeige der Kampagnen erzwingen
- mp4-Videodateien können als Inhalt ausgewählt werden
- Mehr Überwachungsmöglichkeiten bei der Durchführung von Kampagnen

**Endpoint Detection & Response (EDR)**

Endpoint Detection & Response bietet absolute Transparenz und Kontrolle über Endgeräte. Verbessert durch Analytik und Automatisierung, erfasst es automatisch sicherheitsrelevante Operationen.

Die verfügbaren automatisierten Response-Funktionen sind konfigurierbar, um adäquat auf Vorkommnisse zu reagieren. Abhängig von der Anwendung kann die Reaktion auf Fehler bei

Endpunkten automatisch erfolgen. Dafür wurde die gesamte Anzeige und Konfiguration der DriveLock Ereignisse überarbeitet. Zusätzlich können nun mehrere Ereignisse in Regeln parametrisiert zusammengefasst und daraus Security-Alerts generiert werden. Zusätzlich können auf dem Agenten geeignete Response-Maßnahmen zur Behebung des Security-Issues eingeleitet werden.

Security-Alerts können sowohl bei Häufigkeit von Events als auch ihres zeitlichen Auftretens ausgelöst werden - also durch Kombination verschiedener Ereignisfilter innerhalb einer definierten relativen Zeitspanne.

**Neuerungen im DriveLock Operations Center (DOC)**

Im DOC können Sie nun weitere 'out of the box' Dashboards anlegen für Security Awareness, Applikationskontrolle und BitLocker. Alle benötigten Widgets sind bereits auf den jeweiligen Dashboards enthalten, können aber nach Belieben angeordnet werden.

Das DOC bietet verschiedene neue Ansichten:

- Gruppen: Lassen Sie sich in dieser Ansicht die Gruppenmitgliedschaften anzeigen, fügen Sie Rechner neuen Gruppen hinzu oder kontrollieren Sie die Richtlinien, die auf bestimmte Gruppen zugewiesen sind.
- SecAware: Diese Ansicht liefert eine Übersicht über alle Kampagnen sowie deren Status. In dieser Ansicht erhalten Sie auch eine Schnelleinführung über eine Tour, die Sie jederzeit neu starten können.
- EDR: Hier werden die unterschiedlichen Alerts angezeigt und nach Schweregrad und Kategorie sortiert. Die EDR-Ansicht ermöglicht eine kontinuierliche Überwachung Ihrer Endpoints.

Desweiteren können nun zusätzliche administrative Aufgaben über das DOC gestartet werden, wie z.B. das (De-)Aktivieren des Agenten-Tracing. Mithilfe von Schnellfiltern können Sie ohne Aufwand nach bestimmten Eigenschaften filtern.

Darüber hinaus sind viele weitere Verbesserungen und neue Auswertungs- und Anzeigemöglichkeiten in dieser Version hinzugekommen.

Das DOC lässt sich nun auch folgendermaßen öffnen:

- Direkt aus Ihrem Browser, indem Sie im Browser manuell die URL **https://server:port** eingeben (als Beispiel: https://dlserver.dlse.local:4568)
- Wählen Sie im Installationsverzeichnis von DriveLock die Datei `DOC X64.msi` zur Installation aus. Im Startmenü wird Ihnen anschließend unter **DriveLock** der Eintrag

**Operations Center** angezeigt. Alternativ dazu können Sie die `DriveLock.OperationsCenter.exe` manuell starten. Das DOC wird in einer DriveLock-eigenen browserbasierten Oberfläche geöffnet.

### Zusätzliche Verbesserungen in dieser DriveLock Version

- Direkte Unterstützung von sog. Datenschleusen, wie zum Beispiel die Koramis Datenschleuse
- Laufwerks- und Geräteklassenregeln können nun auch gefiltert werden
- Mehr Bearbeitungsmöglichkeiten im Self-Service, z.B. Offline Unlock auch ohne Netzwerkverbindung

### 4.3.2 Fehlerbehebungen

#### Wichtige Fehlerkorrekturen in dieser Version

Dieses Kapitel enthält Informationen zu Fehlern, die in der vorliegenden DriveLock-Version behoben sind. Als Referenz dienen dabei unsere External Issues (EI), falls vorhanden.

| Referenz | Agenten-Fernkontrolle |
|---|---|
| EI-613 | Die Agenten-Fernkontrolle verwendet nur noch sichere Ports für die Verbindung. |
| EI-729 | Wenn SSL bei Aktualisierung einer Richtlinie erzwungen (oder sogar deaktiviert) wird, deaktiviert der Agent automatisch den Port 6064 sobald die Richtlinie aktualisiert ist. |
| EI-517 | Der neue Menüeintrag **Verbinden als** im Kontextmenü eines DriveLock Agenten dient zur Einstellung des Ports und Verwendung von HTTPS. Im DriveLock Control Center kann der Port in den Einstellungen gesetzt werden. |

| Referenz | Applikationskontrolle |
|---|---|
| EI-731 | Das lokale Whitelist-Tray-Symbol wird nun in der Remote Desktop Session (RDP) angezeigt. |

| Referenz | BitLocker Management |
|---|---|
| EI-666 | Der Fehler beim Verschlüsseln eines Systemlaufwerks [0x8031002c] wurde durch Anpassen der Registry-Werte für die Gruppenrichtlinien behoben. |
| EI-740 | Bestehende BitLocker Managed Environments (z.B. MBAM) können jetzt zusammen mit DriveLock betrieben werden. Dazu muss in der Registry folgender DWORD-Wert hinzugefügt werden: `HKEY_LOCAL_MACHINE \SOFTWARE \CenterTools \DLStatus \RegProtectionLevel` (Anm.: ohne Leerzeichen!). Weisen Sie den Wert 1 zu. Beachten Sie, dass diese Änderung erst durchgeführt werden kann, nachdem der Agent beendet worden ist. Anschließend muss das System neu gestartet werden. |

| Referenz | DriveLock Control Center (DCC) |
|---|---|
| EI-734 | Der Anmeldebildschirm für das DriveLock Control Center wurde erweitert, so dass der deutsche Text für den Benutzernamen nicht mehr abgeschnitten wird. |

| Referenz | Device Control |
|---|---|
| EI-735 | Der Registrierungsschlüssel "IsAppTermServ" geht beim Upgrade des Agenten nicht mehr verloren. |
| EI-461 | Die Dateifilter-Einstellungen (Inhaltsscanner) sind für Portable Media-Geräte jetzt erlaubt und werden nicht mehr ignoriert. |

| Referenz | Disk Protection |
|---|---|
| EI-277 | Ein Domänenwechsel nach einem WOL führt nicht mehr zu einer Veränderung der Domäne. |
| EI-231 | In der Richtlinie kann der Eintrag für Verschlüsselungszertifikate jetzt auf **nicht konfiguriert** gesetzt werden. |
| EI-579 | Disk-Protection-Zertifikate können jetzt aus der Dateiablage in der Richtlinie gelöscht werden. |

| Referenz | Encryption-2-Go |
|---|---|
| EI-137 | Die Größenbeschränkung für verschlüsselte Laufwerke lässt sich jetzt einstellen. |

| Referenz | File Protection |
|---|---|
| EI-646 | CSV-Dateien können jetzt verschlüsselt werden. |
| EI-640 | Die Schaltfläche **Benutzername und Kennwort** ist jetzt aktivierbar und standardmäßig ausgewählt. |

| Referenz | File Protection |
|---|---|
| EI-737 | DLFldEnc stürzt nicht mehr beim Kopieren von Dateien ab. |
| EI-426 | Bei der Verschlüsselung einer externen Festplatte mit DriveLock File Protection und Ausführung einer Defragmentierung durch Windows, werden jetzt alle Dateien korrekt verschlüsselt und das NTFS-Dateisystem nicht mehr beschädigt. |
| EI-112 | File-Protection-Benutzer mit Leserechten können jetzt verschlüsselte Ordner mounten. |
| EI-626 | Wenn File Protection lizenziert ist und kein Encryption-2-Go benötigt wird, gibt es jetzt keine Warn-/Fehlermeldung mehr bei der Konfiguration der Whitelistregeln für das Laufwerk. |
| EI-653 | Ein Benutzer mit DriveLock-Zertifikat erhält jetzt beim Versuch, einen verschlüsselten Ordner zu mounten, keinen Fehler mehr. |

| Referenz | Gruppen und Berechtigungen |
|---|---|
| EI-570 | Zentrale File-Protection-Gruppenberechtigungen überschreiben keine Einzelbenutzerberechtigungen mehr, wenn ein einzelner Benutzer in der hinzugefügten Gruppe enthalten ist. |
| EI-633 | AD-Gruppen können nun aus statischen DriveLock-Gruppen entfernt werden. |

| Referenz | Management Konsole (DMC) |
|---|---|
| EI-96 | Das richtige Sicherheitsprotokoll wird jetzt in der GUI für den Transfer zwischen Server und Agent angezeigt. |
| EI-738 | Innerhalb der DMC (Agentenfernkontrolle) wird keine LocalHashes.dhb mit 0 Byte mehr auf Client-Seite erstellt, was zu einem Ereignisfehler 222 führte. |
| EI-321 | Die Warnung "Es ist kein DriveLock Enterprise Service verfügbar, da keine gültige Serververbindung konfiguriert ist" erscheint nicht mehr während der Verwendung der DMC. |
| EI-726 | Der Gerätescanner zeigt jetzt alle gescannten Computer an. |

| Referenz | Richtlinien |
|---|---|
| EI-660 | Die Ereignisanzeige wurde nach Auswahl eines automatischen DriveLock Agenten-Updates mit Ereignissen der Event-ID 362 'überflutet'. Dieser Fehler ist behoben, die Verarbeitung von Ereignissen wurde verbessert. |
| | Die Option **Zentral gespeicherte Richtlinien bei Veröffentlichung an Agent pushen** in den Server-Einstellungen kann jetzt ohne Fehler verwendet werden. |
| EI-617 | Wenn beim Zuweisen von einer großen Anzahl von Richtlinien der Status mithilfe des Kommandozeilenbefehls `-showstatus` überprüft werden sollte, wurde der Anzeigetext abgeschnitten. Dieser Fehler ist jetzt behoben |
| EI-676 | Bei einer Richtlinie, die auf einer Computergruppenzuordnung basiert, wird jetzt der AD-Gruppenname in der Agenten-Benutzeroberfläche angezeigt statt fälschlicherweise der AD-Identifier. |

| Referenz | SB-Freigabe |
|---|---|
| EI-718 | Im SB-Freigabe-Assistent ist es nicht mehr möglich, eine Zeitangabe in der Vergangenheit einzugeben. |
| EI-717 | Beim Exportieren einer SB-Gruppe in eine CSV-Datei werden jetzt die Umlaute (wie äöü) korrekt gespeichert. |

| Referenz | Security Awareness |
|---|---|
| | Kampagnen werden jetzt nur den in der Richtlinie definierten Benutzern angezeigt und nicht allen Benutzern. |

| Referenz | System-Management |
|---|---|
| EI-516 | Für die Kommunikation zwischen DriveLock Agenten und DES kann in den Agentenfernkontroll-Einstellungen jetzt nicht mehr derselbe Port für Agentenfernkontrolle bzw. HTTPS eingetragen werden. |

# 5 Bekannte Einschränkungen

Dieses Kapitel enthält bekannte Einschränkungen der vorliegenden DriveLock-Version. Bitte lesen Sie diese Informationen sorgfältig, um unnötigen Test- und Supportaufwand zu vermeiden.

## 5.1 Lizenzaktivierung

Derzeit ist eine Lizenzaktivierung über einen Proxy-Server, bei dem eine explizite Anmeldung erforderlich ist, leider nicht möglich.

## 5.2 DriveLock Management Konsole (DMC)

In einigen Situationen kann es beim Hinzufügen eines zweiten Benutzers, nachdem bereits ein Benutzer hinzugefügt wurde, zu einem Absturz der Konsole kommen. Das Problem wird durch den Microsoft-Dialog (AD Picker) verursacht.

Nach unseren Recherchen scheint es sich bei diesem Fehler um ein bekanntes Problem unter Windows 10 zu handeln, Details dazu finden Sie hier.

Sobald Microsoft diesen Fehler behoben hat, werden wir dieses offene Problem nochmals untersuchen.

### Wichtige Update-Information:

Bei einem Update von DriveLock Version 7.7.x auf höhere Versionen muss folgender Workaround durchgeführt werden, um die DMC zu aktualisieren: Benennen Sie die `DLFdeRecovery.dll` vor Beginn des Updates um und installieren Sie dann die DMC.

## 5.3 Installation der Management Komponenten über Gruppenrichtlinien

Die Installation der DriveLock Management Konsole, des DriveLock Control Center und des DriveLock Enterprise Service über Microsoft Gruppenrichtlinien ist nicht möglich. Verwenden Sie zur Installation den DriveLock Installer (siehe DriveLock Installationshandbuch).

## 5.4 DriveLock Device Scanner

Der im Produkt integrierte Device Scanner kann in allen Umgebungen problemlos verwendet werden, die ausschließlich den Standardmandant "Root" eingerichtet haben. Das trifft für die meisten Kundeninstallationen zu.

Haben Sie eine Umgebung mit mehreren Mandanten eingerichtet, erhalten Sie eine Fehlermeldung beim Anzeigen und Speichern der Scan-Ergebnisse.

## 5.5 Manuelle Updates

Wenn zur Verteilung der Richtlinien nicht GPO verwendet wird, schlägt ein manueller Update des Agent unter Windows 8.1 und höher fehl, sofern DriveLock Agent.msi aus dem Windows Explorer (z.B. per Doppelklick) und ohne Berechtigungen eines lokalen Administrators gestartet wurde. Starten sie das MSI-Paket aus einem administrativen Command Fenster per msiexec oder nutzen Sie  DLSetup.exe.

### Update von DriveLock Version 2019.1 auf 2019.2

Wird ein Client-Update manuell über das Starten von msiexec oder DLSetup.exe durchgeführt, kann es vorkommen, dass sich der Windows Explorer nicht korrekt beendet. In der Folge verschwindet die Benutzeroberfläche von Windows (schwarzer Bildschirm) und wird auch nach dem Agent-Update nicht neu gestartet. In diesem Fall muss über den Task-Manager der Explorer manuell gestartet werden bzw. ein Reboot initiiert werden.

## 5.6 Self Service Freigabe

Wenn Sie den Self Service Assistenten verwenden, um Apple iPhone Geräte freizugeben, ist es nach Beendigung der Freigabe immer noch möglich, manuell Bilder vom iPhone Gerät zu kopieren, solange das Gerät verbunden ist.

## 5.7 DriveLock, iOS und iTunes

DriveLock erkennt und kontrolliert Apple-Geräte neuerer Generation (z.B. iPod Touch, iPhones oder iPads). Bei älteren Geräten, welche ausschließlich als USB-Laufwerk erkannt werden, können keine detaillierten Sperren vorgenommen werden (z.B. alter iPod Nano).

DriveLock und iTunes von Apple verwenden sehr ähnliche Multicast DNS Responder um Komponenten im Netzwerk automatisch zu erkennen. Bei der Installation von iTunes bzw. DriveLock ist die Installationsreihenfolge wichtig:

- Sofern DriveLock noch nicht installiert ist, kann iTunes ohne weiteres installiert werden. Wird im Nachhinein DriveLock installiert, ist auch hier nichts weiter zu beachten.
- Ist DriveLock bereits vorhanden, muss vor der Installation von iTunes die entsprechende Komponente von DriveLock mit dem Befehl drivelock -stopdnssd deaktiviert werden, bevor iTunes installiert wird. Ansonsten kommt es bei der Installation von iTunes zu einem Fehler und die Installation ist nicht erfolgreich.

Beim Aktualisieren von iOS-Betriebssystemen ist darauf zu achten, dass nach dem Update eine erneute Synchronisation (Musik, Bilder usw.) stattfindet, welche nur durchgeführt werden kann, wenn keine der zu synchronisierenden Daten gesperrt werden.

## 5.8 Universal Camera Devices

Unter Windows 10 gibt es eine neue Geräteklasse, die sofern keine speziellen Gerätetreiber installiert wurden, für angeschlossene bzw. eingebaute Web-Kameras verwendet wird: Universal Cameras.

Diese Geräteklasse kann derzeit noch nicht mit DriveLock verwaltet werden.

> Hinweis: Um diese Geräte zu kontrollieren, installieren Sie bitte den mitgelieferten Treiber des Herstellers. Danach wird das Gerät automatisch der richtigen Geräteklasse zugeordnet.

### 5.8.1 Windows Portable Devices (WPD)

Sperren von "Windows Portable Devices" oder “Tragbaren Mediengeräten” führte dazu, dass manche Windows Mobile Geräte auch nicht mehr mit dem "Windows Mobile Device Center" synchronisiert werden konnten, selbst wenn das spezielle Gerät in einer Whitelist-Regel freigegeben war.

Windows ab Windows Vista und neuer benutzt ein neues „User-mode Driver Framework“ für diese Art von Geräten. DriveLock beinhaltet inzwischen einen derartigen Treiber.

Aufgrund einer Fehlfunktion im Betriebssystem von Microsoft ist dieser jedoch auf folgenden Systemen deaktiviert:

- Windows 8
- Windows 8.1 ohne den Hotfix KB3082808
- Windows 10 älter als Version 1607

### 5.8.2 CD-ROM Laufwerke

Eine Verwendungsrichtlinie für CD-ROM-Laufwerke wird nur ein Mal angezeigt, wenn eine CD erstmalig eingelegt wird. Weitere CDs, die in dieses Laufwerk eingelegt werden, werden zwar geblockt, aber die Verwendungsrichtlinie erscheint nicht mehr. Wenn DriveLock neu gestartet wird, erscheint die Verwendungsrichtlinie wieder.

> Hinweis: Grund hierfür ist, dass DriveLock nur das eigentliche Gerät in der Richtlinie erkennt (CD-ROM-Laufwerk), nicht aber den Inhalt (CD-ROM).

## 5.9 DriveLock Disk Protection

### Disk Protection und DriveLock Operations Center (DOC)

Im DOC werden Status-Informationen von mit DriveLock Disk Protection verschlüsselten Festplatten ab Version 2019.2 SP1 korrekt angezeigt. Dabei zeigt die Inventory-Komponente den Verschlüsselungsstatus und die Verschlüsselungsmethode der Festplatten im DOC an.

> Hinweis: Beachten Sie, dass bis einschließlich Version 2019.2 Disk Protection Kunden für die Überwachung ihrer Systemumgebung die Funktionalität des DriveLock Control Centers verwenden sollten.

### Inplace Update auf Windows 10 1903

Haben Sie vor dem Update auf eine aktuelle Windows 10 Version eine bestimmte Anzahl automatischer Logins für die PBA aktiviert (dlfdecmd ENABLEAUTOLOGON <n>), ist die automatische Anmeldung währen des Upgradeprozesses durchgehend aktiv. Da jedoch während des Vorgangs der Zähler <n> nicht aktualisiert werden kann, empfehlen wir diesen lediglich auf 1 zu setzen, so das unmittelbar nach dem Windows Inplace Upgrade die Benutzeranmeldungen in der PBA wieder erforderlich sind.

Wenn Sie während des Updates Benutzeranmeldungen an der PBA deaktivieren möchten setzen Sie daher den Zähler auf 1, damit nach dem Update nach einem weiteren Neustart nur einmal eine automatische Anmeldung erfolgt und anschließend wieder eine Benutzeranmeldung an der PBA erfolgen muss.

### Antiviren Software

Es ist möglich, dass die Installation der DriveLock Disk Protection aufgrund einer Antivirus Software fehlschlägt, weil das ausgeblendete Verzeichnis `C:\SECURDSK` durch die Software in Quarantäne genommen wird. In diesem Falle sollten Sie für den Zeitraum der Installation den Virenschutz temporär ausschalten. Wir empfehlen, dieses Verzeichnis grundsätzlich als Ausnahme für den Virenscanner zu definieren.

### Applikationskontrolle

Es wird dringend empfohlen, die Applikationskontrolle, sofern diese im Whitelist-Modus aktiv ist, für den Zeitraum der Disk Protection Installation zu deaktivieren, um zu verhindern dass für die Installation notwendige Programme gesperrt werden.

### Ruhezustand

Hibernation funktioniert nicht, während eine Festplatte ver- oder entschlüsselt wird. Nach der vollständigen Ver- oder Entschlüsselung muss Windows einmal neu gestartet werden,

damit Hibernation wieder funktioniert.

**UEFI-Modus**

> Hinweis: Nicht alle Hardwarehersteller implementieren UEFI vollständig. Es ist notwendig, den UEFI Modus nicht mit UEFI Versionen kleiner 2.3.1 zu verwenden.

Die mit 2019.2 verfügbare neue PBA steht derzeit nur für Windows 10 Systeme zur Verfügung, da die für die Festplattenverschlüsselungskomponenten benötigten Treibersignaturen von Microsoft nur für dieses Betriebssystem gelten.

Die Pre-Boot-Authenication (PBA) für den UEFI-Modus unterstützt noch nicht generisch alle PS/2 Eingabegeräte.

Unter VMWare Workstation 15 und auch bei einigen wenigen Hardwareherstellern ergaben unsere Testergebnisse Konflikte durch Maus- und Keyboadtreiber der UEFI Firmware, so dass keine Tastatureingabe in der PBA möglich ist. In diesem Fall können Sie beim Start des Rechners mit Hilfe der Taste "k" das Laden der Drivelock-PBA-Treiber einmalig verhindern. Nach der Windows-Anmeldung auf dem Client können Sie dann in einer Administrator-Kommandozeile den Befehl `dlsetpb /disablekbddrivers` ausführen, um die Drivelock-PBA-Treiber dauerhaft deaktivieren. Bitte beachten Sie dass dadurch in der Anmeldemaske der PBA das Standardkeyboardlayout der Firmware geladen ist, was in den meisten Fällen eine EN-US Belegung hat, wodurch die Sonderzeichen abweichen können.

Folgende Punkte sind weiterhin zu beachten:

- DriveLock 7.6.6 und höher unterstützt UEFI Secure Boot.
- Firmwareupdates können bewirken, dass NVRAM-Variablen des Mainboards gelöscht werden, die DriveLock benötigt. Daher empfehlen wir unbedingt, vor der Installation der DriveLock PBA / FDE die Firmware-Updates für das Mainboard /UEFI einzuspielen (auch bei neu gekauften Geräten oder bei Bugfixes)
- 32 Bit Windows und DriveLock kann nicht auf ein 64 Bit fähiges System installiert werden. Es muss die 64 Bit Version von Windows und DriveLock eingesetzt werden.
- Die maximale Größe einer Festplatte ist weiterhin auf maximal 2 TB beschränkt.
- Auf manchen HP Rechnern ist Windows immer wieder an Postion 1 der UEFI Bootreihenfolge und die DriveLock PBA muss im UEFI Boot-Menü manuell ausgewählt werden. In solchen Fällen und bei Problemen muss man Fast Boot im UEFI ausschalten, damit die DriveLock PBA an Position 1 bleibt.

- Windows 10 Version 1703 (Creators Update) entfernt beim Herunterfahren in den Ruhezustand in vielen Fällen den DriveLock Eintrag für die PBA aus dem UEFI Boot-Menü. Die DriveLock PBA wird dann nicht mehr gestartet und Windows kann von der verschlüsselten Systemplatte nicht mehr starten. Im August 2017 hat Microsoft Update KB4032188 veröffentlicht, das dieses Problem behebt. Das Update KB4032188 wird von Windows automatisch installiert, kann aber auch manuell geladen werden: Link zum Download.
  Installieren Sie KB4032188 oder ein späteres Update, das KB4032188 ersetzt, bevor Sie DriveLock Disk Protection für UEFI installieren.
  Wenn Sie auf Windows 10 Version 1703 aktualisieren und DriveLock Disk Protection bereits installiert ist, fügen Sie KB4032188 zum Creators Update hinzu, bevor Sie aktualisieren.

**BIOS-Modus**

In sehr seltenen Fällen kann es vorkommen, dass die Standardeinstellung der DriveLock Disk Protection nicht ordnungsgemäß funktioniert und das System nicht mehr reagiert. In diesem Fall starten Sie einfach den Rechner neu, während Sie die `SHIFT-Taste` gedrückt halten, um temporär die 16-bit Pre-Boot Umgebung zu nutzen.

Durch ein Problem in Windows 10 Version 1709 und neuer kann DriveLock Disk Protection für BIOS die richtige Festplatte nicht erkennen, wenn mehr als eine Festplatte im System verbaut ist. Deshalb ist Disk Protection für BIOS nicht für Windows 10 1709 Systeme mit mehr als einer Festplatte freigegeben. Sobald Microsoft einen Fix liefert wird diese Einschränkung aufgehoben.

Hinweis: Im Support Portal ist für Kunden ein zusätzliches technisches Whitepaper mit Informationen zum Update auf eine neuere Windows Version bei installiertem DriveLock Disk Protection verfügbar.

**Workaround für Windows Update von 1709 auf 1903 bei gleichzeitiger Verschlüsselung von Laufwerk C: mit Disk Protection:**

Referenz: EI-686

1. Entschlüsseln von Laufwerk C:
2. Update Windows 10 von 1709 auf 1903 durchführen
3. Verschlüsseln von Laufwerk C:

**Voraussetzungen für Disk Protection:**

Disk Protection ist für Windows 7 auf UEFI Systemen nicht freigegeben.

### Workaround für DriveLock Update von 7.7.x mit Disk Protection bei aktivierter PBA auf Version 2019.2 SP1

Führen Sie zunächst ein Update von 7.7.x auf Version 7.9.x durch. Dann erst führen Sie das Update auf Version 2019.2 aus. Kontaktieren Sie unseren Support bei weiteren Fragen.

## 5.10 DriveLock File Protection

### Microsoft OneDrive

Mit Microsoft OneDrive kann Microsoft Office Dateien direkt mit OneDrive synchronisieren, ohne die Dateien zuerst in den lokalen Ordner zu speichern. In dem Fall ist der DriveLock Verschlüsselungstreiber nicht involviert und die Office-Dateien werden in der Cloud nicht verschlüsselt. Um dieses Verhalten zu unterbinden, deselektieren Sie **Office 2016 nutzen, um Dateien die ich öffne zu synchronisieren** oder ähnliche Einstellungen in OneDrive. Es muss eingestellt werden, dass Office-Dateien, wie auch andere Dateien immer lokal gespeichert werden.

### NetApp

Es besteht derzeit eine Inkompatibilität zwischen dem Verschlüsselungstreiber von DriveLock und bestimmten NetApp SAN-Treibern bzw. Systemen, die sich noch nicht genauer eingrenzen lassen. Prüfen Sie bitte vor Einsatz der File Protection in dieser Systemumgebung die von Ihnen benötigte Funktionalität. Wir sind an dieser Stelle gerne behilflich, um das Problem gegebenenfalls genauer mit Ihnen zu untersuchen.

### Windows 10-Clients mit Kaspersky Endpoint Security 10.3.0.6294

Der Blue-Screen-Fehler nach Aktivierung von DriveLock File Protection (DLFldEnc.sys) bleibt weiterhin bestehen.

### Zugriff auf verschlüsselte Ordner

- Der Zugriff auf verschlüsselte Ordner auf Laufwerken, die nicht mit Laufwerksbuchstaben sondern als Volume Mountpoint gemounted sind, wird nicht unterstützt.
- Performance-Einbrüche bei umfangreichen Kopiervorgängen ("Backups") auf verschlüsselte Ordner bzw. große verschlüsselte Laufwerke können durch Abschalten der Überprüfung auf unverschlüsselte Dateien auf diesen Laufwerken verhindert werden. (Referenz: EI-763, EI-767)

### Office 365-Dateien

Wenn der Pfad zum verschlüsselten Ordner mehr als 128 Zeichen lang ist, kann das Öffnen heruntergeladener Office 365-Dateien fehlschlagen. (EI-941)

### eMMC Flash Memory

DriveLock File Protection unterstützt keine Speichermedien des Typs eMMC Flash Memory. (EI-828)

### Distributed File System (DFS)

DriveLock File Protection unterstützt derzeit keine Speicherung von verschlüsselten Verzeichnissen auf Netzlaufwerken mit Distributed File System (DFS).

## 5.11 Verschlüsselung

### Vorgabe der Verschlüsselungsmethode bei erzwungener Verschlüsselung eines externen Speichermediums

Wenn ein Administrator die Verschlüsselungsmethode nicht vorgegeben hat, erscheint auf dem DriveLock Agenten beim Verbinden des externen Speichermediums ein Dialog zur Auswahl der Verschlüsselungsmethode (Encryption-2-Go, Disk Protection, BitLocker To Go). In manchen Fällen erscheint dieser Dialog jedoch fälschlicherweise auch bei SD-Karten-Lesern ohne Medium. Wir arbeiten an einer Lösung des Problems.

## 5.12 DriveLock Mobile Encryption

### DriveLock Mobile Encryption: NTFS/EXFAT

Containerdateien, die mit NTFS oder exFAT formatiert wurden, können zur Zeit mit der Mobile Encryption Application nur gelesen werden. Wir empfehlen hierfür die Verwendung von BitLocker To Go oder die Formatierung mit dem FAT Dateisystem.

## 5.13 BitLocker Management

### Unterstützte Editionen und Versionen

DriveLock BitLocker Management wird auf folgenden Systemen unterstützt:

- Windows 7 SP1 Enterprise und Ultimate, 64-Bit, TPM-Chip ist erforderlich
- Windows 8.1 Pro und Enterprise, 32/64-Bit
- Windows 10 Pro und Enterprise, 32/64-Bit

### Vorhandene BitLocker Umgebung

> Hinweis: Möchten Sie eine bereits vorhandenen Systemumgebung verwalten, die bereits mit BitLocker verschlüsselte Computer enthält, müssen diese seit Version 2019.1 nicht mehr zuvor über die vorhandene BitLocker Verwaltung bzw. die Gruppenrichtlinien entschlüsselt werden. DriveLock erkennt die BitLocker Verschlüsselung automatisch und erzeugt neue Wiederherstellungsinformationen. Eine automatische Ent- und Verschlüsselung wird nur dann durchgeführt, wenn der in der DriveLock Richtlinie konfigurierte Verschlüsselungsalgorithmus sich vom derzeitigen Algorithmus unterscheidet.

Anschließend ist eine Verwaltung durch DriveLock BitLocker Management möglich und eine sichere Speicherung und Verwendung der Wiederherstellungsinformationen gewährleistet.

### Verwendung von Passwörtern

DriveLock BitLocker Management vereinfacht die missverständliche Unterscheidung zwischen PINs, Passphrases und Passwörtern, indem nur noch der Begriff "Passwort" verwendet wird. Gleichzeitig wird ein solches Passwort automatisch im richtigen BitLocker Format benutzt, entweder als PIN oder als Passphrase.

Da Microsoft jedoch unterschiedliche Anforderungen an die Komplexität von PIN und Passphrase stellt, gelten für das Passwort folgende Einschränkungen:

- Mindestlänge: 8 Zeichen
- Maximale Länge: 20 Zeichen

> Achtung: Sie sollten beachten, dass bei Verwendung der BitLocker eigenen PBA diese nur englische Tastaturlayouts zur Verfügung stellt und daher Sonderzeichen als Bestandteil des Passwortes zu Anmeldeproblemen führen können.

### Verschlüsselung von erweiterten Festplatten

Aufgrund von Einschränkungen bei Microsoft BitLocker können externe Festplatten (Datendisks) nicht verschlüsselt werden, wenn Sie den Modus "Nur TPM (kein Passwort)" gewählt haben, da BitLocker bei diesen erweiterten Laufwerken die Eingabe eines Passwortes (BitLocker Sprachgebrauch: Passphrase) erwartet.

### Gruppenrichtlinienkonfiguration

Aufgrund einer technischen Einschränkung können keine computer-spezifischen Passwörter über das DriveLock Control Center gesetzt werden, wenn Sie die DriveLock BitLocker Konfiguration per Gruppenrichtlinien an die Agenten verteilt haben.

In diesem Fall ignoriert der DriveLock Agent die dafür notwendigen maschinenspezifischen Richtlinien.

## 5.14 DriveLock Operations Center (DOC)

### Mehrfachauswahl von Rechnern in der Computer-Ansicht

Wenn Sie in der Computer-Ansicht mehrere Rechner markieren und dann im Menü rechts oben den Befehl **Aktionen auf Computer ausführen** auswählen, um den Diagnoseprozess (Tracing) für diese Rechner zu aktivieren, wird der Diagnoseprozess nur für den ersten markierten Rechner gestartet. Für die anderen wird weder der Diagnoseprozess gestartet, noch eine Fehlermeldung angezeigt.

### Anmeldung am DOC für Benutzer, die aus einer AD-Gruppe entfernt wurden

Eine Anmeldung am DOC funktioniert weiterhin, selbst wenn der Benutzer bereits aus einer AD-Gruppe entfernt wurde und somit nicht mehr die Berechtigung zur Anmeldung am DOC hatte. Grund hierfür ist, dass die Gruppenmitgliedschaften für einen Benutzer aus dem Gruppen-Token gelesen werden. Diese Information werden nur in einem bestimmten Intervall vom System aktualisiert.

## 5.15 DriveLock Security Awareness

### Änderung der Inhalte für das Security Awareness Content AddOn

Seit Version 2019.1 werden keine niederländischen Kampagneninhalte mehr unterstützt. Stattdessen bietet DriveLock französische Inhalte an.

> Achtung: Bitte beachten Sie, dass die niederländischen Inhalte bei einem Update auf 2019.1 bzw. auch auf 2019.2 automatisch vom DES gelöscht werden.

### Security Awareness auf IGEL-Clients

Auf IGEL-Clients kann Security Awareness in der Version 2019.2 nicht verwendet werden. Wir arbeiten an einer Lösung und werden diese in einem der nächsten Releases anbieten.

## 5.16 Antivirus

### Antivirus allgemein

Seit der Version 7.8 ist der OnDemand Scanner (Cyren) aus Lizenzgründen nicht mehr Bestandteil des Produktes. Kunden mit einer bestehenden Avira-Lizenz können bis zum Ablauf der Lizenz für den Scan externer Laufwerke weiterhin den Avira AV-Scanner verwenden.

### Avira Antivirus

Seit der Version 7.9. von DriveLock wird Avira Antivirus nicht länger unterstützt.

## 5.17 DriveLock und Thin Clients

Folgende Einschränkungen sollten beim Einsatz von DriveLock und Thin Clients beachtet werden:

- Security Awareness Kampagnen können nicht innerhalb einer Thin Client Session abgespielt werden
- Die Option "Unbenutzten Speicher auf dem verschlüsselten Medium auffüllen" funktioniert bei der Verschlüsselung eines DriveLock Containers über einen Thin Client nicht zuverlässig.

## 5.18 DriveLock WebSecurity

Seit der Version 2019.1 ist DriveLock WebSecurity nicht mehr Bestandteil des Produktes. Kunden mit einer bestehenden WebSecurity-Lizenz können bis zum Ablauf der Lizenz weiterhin die Version 7.9 verwenden.

# 6 End-Of-Life-Ankündigungen

DriveLock informiert Sie rechtzeitig per Newsletter, wenn ein Support- und Wartungsende für eine bestimmte DriveLock-Version ansteht.

Hinweis: Wir empfehlen allen Kunden, auf die neueste DriveLock Version zu aktualisieren.

**Folgende Versionen sind derzeit vom End-Of-Life betroffen:**

| Version | Support / Code-Korrekturen bis: | Kunden-Support besteht bis: |
|---|---|---|
| 7.8 | Dezember 2019 | Juni 2020 |
| 7.7 | Juli 2019 | Januar 2020 |

**Full Support / Code Correction:**

Kurz nach Erscheinen einer neuen Produktversion plus 12 Monate. Der volle DriveLock-Produkt-Support für das vorherige Release wird für ein ganzes Jahr ab dem Release einer neuen Produktversion fortgesetzt. Kritische Wartungsupdates werden in dieser Zeit weiterhin veröffentlicht; Code-Korrekturen bei Fehlern und kritischen Problemen.

**Continued Customer Care Support:**

Der kontinuierliche Produkt-Support wird für 18 Monate nach der Veröffentlichung einer neuen Produktversion fortgesetzt. Alle aktuellen Wartungs-Updates werden verfügbar sein. Nach Ablauf des Full Support (12 Monate) werden jedoch keine neuen Updates veröffentlicht. Beantwortung von Anfragen per Telefon, E-Mail und Self-Service – zur Verfügung gestellt vom DriveLock Product Support Team und den dazugehörigen Webseiten für technische Unterstützung.

# 7 Testinstallation von DriveLock

Sie können DriveLock - den Agenten, die Management Konsole, das Control Center, den Enterprise Service und Microsoft SQL Express - gemeinsam auf einem Computer installieren. So ist ein erster Test von DriveLock mit minimalen Hardwareanforderungen möglich.

> Hinweis: Auf der Webseite www.drivelock.help finden Sie einen Quick-Start Guide, der Sie durch die Erstinstallation führt. Dieser zeigt Ihnen auch, wie Sie auf einfache Weise mit Hilfe des Quick-Start Assistenten eine Testinstallation und initiale Konfiguration erstellen können.

Wenn Sie die DriveLock Software von der Website www.drivelock.de heruntergeladen haben, ist bereits eine 30-Tage Testlizenz enthalten. Erfolgt die Installation auf einem einzigen Rechner mit lokaler Richtlinie, müssen Sie in der Konfiguration auch keine Lizenz angeben. Installieren Sie den Agenten einzeln auf verschiedenen Rechnern und erfolgt die Konfiguration über eine Gruppenrichtlinie, eine zentral gespeicherte Richtlinie bzw. eine Konfigurationsdatei oder wollen Sie auch die Festplattenverschlüsselung testen, können Sie die mit der DriveLock Management Konsole installierte 30-Tage-Testlizenz verwenden (Standardpfad: C:\Program Files\CenterTools\DriveLock MMC\Tools\AgentTrial.lic). Verwenden Sie den Quick-Start Assistenten, wird diese automatisch in die erzeugte Richtlinie importiert.

# Copyright