DriveLock

Release Notes 2020.2

DriveLock SE 2021

Inhaltsverzeichnis

1 Release Notes 2020.2

Die Release Notes enthalten wichtige Informationen zu neuen Funktionen und Fehlerbehebungen in der aktuellen 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.
  Das Kapitel **DriveLock Operations Center (DOC)** enthält einen Überblick über die Ansichten und Funktionalitäten der browser-basierten Benutzeroberfläche.
- **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 Ereignisse**
  Diese Dokumentation enthält eine Auflistung aller aktuellen DriveLock Ereignisse mit Beschreibung.
- **DriveLock Security Awareness**
  Dieses Handbuch beschreibt die neuen Security Awareness Funktionen, welche auch die Basis des Produktes DriveLock Smart SecurityEducation bilden.
- **DriveLock Linux-Agenten**
  Dieses Handbuch beschreibt die Installation und Konfiguration des DriveLock Agenten auf Linux-Betriebssystemen.

- **DriveLock BitLocker Management**

  Dieses Handbuch beschreibt alle notwendigen Konfigurationseinstellungen und die Funktionalität, die DriveLock für die Festplattenverschlüsselung mit Microsoft BitLocker zur Verfügung stellt.

  - **DriveLock Pre-Boot-Authentifizierung**
    Das Kapitel beschreibt die Vorgehensweise, um die DriveLock PBA zur Authentifizierung von Benutzern einrichten und verwenden zu können, sowie Lösungswege zur Wiederherstellung bzw. Notfallanmeldung.
  - **DriveLock Netzwerk-Pre-Boot-Authentifizierung**
    Das Kapitel beschreibt die Konfiguration für die Pre-Boot-Authentifizierung innerhalb eines Netzwerks.
  - **DriveLock BitLocker To Go**
    Dieses Kapitel beschreibt alle notwendigen Konfigurationseinstellungen, um BitLocker To Go in DriveLock zu integrieren.

- **DriveLock Application Control**

  Dieses Handbuch ersetzt ab Version 2020.1 das im Administrationshandbuch enthaltene Kapitel Applikationskontrolle. Dieses Kapitel bleibt bis auf weiteres als Referenz für ältere Versionen dort verfügbar, wird aber nicht mehr aktualisiert.

- **Microsoft Defender Integration**
  In diesem Handbuch wird die Integration und Konfiguration von Microsoft Defender in DriveLock beschrieben.

- **Vulnerabilty Scan**

  Dieses Handbuch beschreibt die neue Schwachstellenscan-Funktionalität, ihre Konfigurationseinstellungen und Verwendung im DriveLock Operations Center (DOC) und in der DriveLock Management Konsole.

2 Update von DriveLock

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

2.1 Migration der Datenbanken

Bei dem Update von DriveLock 2020.1 (oder älter) auf 2020.2 werden die beiden DriveLock-Datenbanken zusammengeführt. Die Daten aus der DriveLock-DATA Datenbank werden in die DriveLock Datenbank migriert.

Ab Version 2020.2 wird die DriveLock-DATA Datenbank nicht mehr verwendet und kann nach der Migration archiviert bzw. gelöscht werden. Dies betrifft sowohl die "root" Haupt-Datenbanken wie auch jeweils die Mandanten-Datenbanken, falls welche verwendet werden.

Gegebenenfalls müssen selbsterstellte SQL Jobs, die für Wartung und Backup zuständig sind, angepasst werden. Dies betrifft auch eventuelle selbst erstellte Abfragen und Tools, die die DriveLock-DATA verwenden.

Database Migration Wizard

Der Wizard wird automatisch vom Datenbank Installation Wizard nach einem erfolgreichem Update gestartet.

> Achtung: Bitte sichern Sie vor der Datenbankmigration alle DriveLock Datenbanken!

- Der Migration Wizard analysiert alle DriveLock Datenbanken, prüft ob bzw. wie viele Daten migriert werden können und macht einen Vorschlag zur Konfiguration der Migration anhand der gefundenen Daten.

  > Hinweis: Die Migration selbst kann jederzeit unterbrochen und wieder fortgeführt werden. Es gehen keine Daten verloren.

- Daten, die aus der DriveLock-DATA Datenbank in die DriveLock Datenbank migriert werden, sind folgende:
  - EDR Kategorien
  - EDR Alerts
  - Ereignisdaten
  - Security Awareness Sessions

> Hinweis: Falls Sie EDR Kategorien angelegt haben, müssen diese migriert werden, um die EDR Funktionalität nach dem Update zu gewährleisten. Ereignisse, EDR Alerts und Security Awareness Sessions können auch später migriert werden. Es wird empfohlen, zuerst nur die wichtigen Daten zu migrieren und die Migration der Massendaten auf ein Zeitfenster zu legen, wo die Aktivität gering ist.

2.1.1 Voraussetzungen für die erfolgreiche Migration

Der Database Migration Wizard muss als Administrator gestartet werden, damit er auf den Registry-Bereich der DES Konfiguration zugreifen und gegebenenfalls den DES Dienst starten kann.

Beachten Sie folgendes bei Remote-SQL Servern:

- Der Database Migration Wizard verwendet den Microsoft Distributed Transaction Coordinator (MSDTC), um die Datenintegrität über Datenbanken hinweg bei der Migration zu gewährleisten.
- Bei Remote SQL Servern ist eine Konfiguration von MSDTC eventuell nötig.

> Hinweis: Eine Fehlermeldung wird angezeigt, sollte dieser Schritt notwendig sein.

- MSDTC Konfiguration: https://docs.microsoft.com/en-us/troubleshoot/windows-server/application-management/enable-network-dtc-access
- MSDTC Firewall Konfiguration: https://docs.microsoft.com/en-us/troubleshoot/windows-server/application-management/configure-dtc-to-work-through-firewalls

2.1.2 Durchführung der Migration

Die bereits gesetzten Standardoptionen im Database Migration Wizard können übernommen werden, Änderungen sind nur in Spezialfällen empfohlen.

Folgende Schritte werden dabei durchlaufen:

1. Verbindung zur Haupt-Datenbank herstellen
   Im ersten Schritt wird ein Verbindungstest zur DriveLock Haupt-Datenbank durchgeführt, wobei die Verbindungsdaten aus der Registry ausgelesen werden.

> Hinweis: Wählen Sie die Schaltfläche **Advanced Mode**, falls Sie die Standardeinstellungen ändern wollen (siehe 3.).

2. Analyse der Daten
   Im Anschluss an den Verbindungstest wird eine Analyse der Daten in den Datenbanken vorgenommen.
   Aus der Haupt-DriveLock Datenbank werden die Verbindungsparameter zu den Ereignis-Datenbanken und, falls vorhanden, den Mandant-Datenbanken ermittelt.
   Der Wizard prüft die Verbindung und Version zu jeder Datenbank. Die Datenbanken müssen auf den aktuellen Stand sein, damit eine Migration unterstützt wird.

   > Hinweis: Falls die Version einer Datenbank nicht aktuell sein sollte, bitte mit dem Datenbank Installation Wizard die Datenbank aktualisieren und die Migration erneut starten.

3. Konfiguration der Migration
   Dieser Schritt wird ausschließlich im **Advanced Mode** angezeigt. Die Konfiguration der Migration wird pro Mandant vorgenommen und bietet folgende Änderungsmöglichkeiten:
   - Datenbanken vorbereiten
     Dies führt die Datenbankwartung (Indexpflege) auf beiden Datenbanken durch und bereitet zusätzlich die Ereignisdaten für eine performantere Migration vor.
   - Ereignisdaten migrieren
     Dies migriert die Ereignisse, wie sie in den Reports in DCC / DOC ausgewertet werden können.
     - Ereignisse nach der Migration verarbeiten
       Dies ist nötig, um aus den Ereignissen die Verknüpfungen zu den anderen Daten wie z.B. Computer, Benutzer, Laufwerke, Geräte, etc. herzustellen. Diese werden in DCC Forensics und DOC verwandte Entitäten angezeigt. Die Verarbeitung dieser Daten kann bei größeren Datenmengen eine Zeit dauern. Dies passiert beim laufenden DriveLock Enterprise Server im Hintergrund.
     - Daten vor der Migration prüfen
       Diese Einstellung prüft, ob die Daten in der Ziel-Datenbank vor der Migration bereits existieren, was vorkommen kann, wenn die Migration zu einem späteren Zeitpunkt vorgenommen wird. Dies kann abgeschaltet werden,

um die Migration zu beschleunigen. Bei auftretenden Fehlern ist es empfohlen, die Migration dann mit Prüfung der Daten zu wiederholen. Es gehen im Fehlerfall keine Daten verloren.

- Security Awareness Sessions migrieren
- EDR Kategorien
- EDR Alerts
- Konfiguration der Batch-Größen

4. Migration
   - Die Datenbanken werden je nach Mandant der Reihe nach migriert. Die Migration kann gestoppt und erneut gestartet werden. Die Ausgabe zeigt den Fortschritt der Migration.
   - Migrierte Daten werden aus der Quell-Datenbank (hier die Ereignis-Datenbank) gelöscht.
   - Nach erfolgreicher Migration wird der DriveLock Enterprise Service gestartet.

> Hinweis: Wenn die Migration abgeschlossen ist, werden die Ereignis-Datenbanken nicht mehr gebraucht und können archiviert bzw. gelöscht werden.

2.2 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.

2.3 Allgemeine 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 Release Notes enthalten zusätzlich besonders wichtige Punkte, die Sie bei einer Aktualisierung beachten sollten.

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.

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.

2.3.1 Update der DriveLock Management Konsole (DMC)

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` um und installieren Sie dann die DMC neu.

2.3.2 Update der Disk Protection

Nach dem Update des DriveLock Agenten wird eine ggf. vorhandene FDE Installation ohne Neuverschlüsselung automatisch auf die neueste Version aktualisiert. Nach dem Update der FDE 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.

Diese finden sie ebenfalls auf unserer Webseite www.drivelock.help.

2.4 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 Befehlsfenster 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.

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.

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	2020.2	2020.1	2019.2
Windows 10 Pro			
Windows 10 20H2	+	+	+
Windows 10-2004	+	+	+
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 20H2	+	+	+
Windows 10-2004	+	+	+

OS-Version	2020.2	2020.1	2019.2
Windows 10-1909	+	+	+
Windows 10-1903	-	+	+
Windows 10-1809	+	+	+
Windows 10-1803	+	+	+
Windows 10-1709	-	+	+
Windows 10-1703	-	-	-
Windows 10-1607	-	-	-
Windows 10 Enterprise LTSB/LTSC			
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	+(*)	+(*)	+

OS-Version	2020.2	2020.1	2019.2
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 not-wendig	Support Lizenz not-wendig	Support Lizenz not-wendig
Folgende Linux Derivate und neuere Versionen (eigene DriveLock Lizenz)			
CentOS Linux 8	+	+	+
Debian 7	+	+	+
Fedora 31	+	+	+
IGEL OS ab Version 10	+	+	+
Red Hat Enterprise Linux 5	+	+	+

OS-Version	2020.2	2020.1	2019.2
SUSE 15.1	+	+	+
Ubuntu 18.04	+	+	+

(*): Bitte beachten Sie den wichtigen Hinweis unter Unterstützte Plattformen.

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

Hinweis: Weitere Informationen zum Linux Client und den Limitierungen der Funktionalität entnehmen Sie bitte der separat verfügbaren Linux-Dokumentation.

Der Windows 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.

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.
- BitLocker Management wird auf Windows 7 Systemen mit TPM und nur für 64-Bit unterstützt.
- 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.
- DriveLock Disk Protection ist für Windows 10 ab Version 1703 freigegeben (siehe Bekannte Einschränkungen).
- 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 Win-

dows 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 7.15 oder neuer (ICA).
- Windows Server 2012 R2 oder 2016 (RDP).
- Das Anlegen von durch DriveLock File Protection verschlüsselten Ordnern auf dem Terminal Service ist nicht unterstützt.

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 Mananagement 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 2020.1 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 / CPU:

- mind. 8 GB RAM, CPU x64 mit 2,0GHz und EM64T (Extended Memory Support)

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.

Benötigte DriveLock API Services Ports (DOC/MQTT):

- 5370, 6369 und 4369: Diese drei Ports sollten nicht durch andere Server-Dienste belegt werden, sie müssen jedoch nicht von außen erreichbar sein (nur intern)
- 8883: Die Agenten verbinden sich auf diesen Port mit dem DES, um per Agentenfernsteuerung erreichbar zu sein. Die Freigabe in der lokalen Firewall des Rechners erfolgt automatisch durch das DES-Installationsprogramm.

Unterstützte Plattformen:

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

> Achtung: Windows Server 2012 R2 erfordert eine Installation von SQL Express 2017, bevor DriveLock Version 2020.1 erfolgreich installiert werden kann.

- 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:

> Hinweis: Bitte entnehmen Sie die Systemvoraussetzungen für die Installation der SQL-Datenbank bzw. von SQL-Express der entsprechenden Microsoft Dokumentation.

- SQL-Server 2012 (Mindestvoraussetzung für das DriveLock Operations Center) oder neuer
- SQL-Server Express 2014 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 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.

3.4 DriveLock Operations Center Applikation

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

> Hinweis: Das DriveLock Operations Center kann auch als Web-Anwendung über einen Browser gestartet werden. Dafür ist eine Installation der DOC Applikation (DOC.exe) nicht notwendig.

Hauptspeicher:

- mind. 4 GB RAM

Freier Festplattenspeicherplatz:

- ca. 250 MB

Benötigte zusätzliche Windowskomponenten:

- .NET Framework 4.5.2 oder höher

Unterstützte Plattformen:

Die DriveLock Operations Center Applikation wurde 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.

Das DriveLock Operations Center ist nur für Intel X86 basierte 64-Bit Systeme verfügbar.

3.5 DriveLock in Arbeitsgruppen-Umgebungen (ohne AD)

Grundsätzlich kann DriveLock auch ohne Active Directory eingesetzt werden. Dabei ist u.a. folgendes zu beachten:

- Das Rechte- und Rollen-Prinzip kann für die Administratoren / Helpdesk-Mitarbeiter nur aus lokalen Benutzern aufgebaut werden
- Zuweisungen von Richtlinien und Whitelist-Regeln auf AD-Gruppen, AD-Benutzer, AD-OUs sind nicht möglich, sondern nur auf lokale Objekte (Computernamen und Benutzer)
- Die Namensauflösung muss funktionieren, da vom DriveLock Control Center (DCC) über den NETBIOS/FQDN Namen auf die Clients zugegriffen wird (wichtig für Helpdesk Aktivitäten)
- Wenn DNSSD deaktiviert ist, müssen die Clients bekannt sein, da es kein AD Inventory gibt (wichtig für die Agenten-Fernkontrolle in der Management Konsole)
- In Arbeitsgruppen-Umgebungen ist eine Anmeldung am DriveLock Operations Center (DOC) nicht möglich (nur mit AD-Konto)
- Mit der Agenten-Fernkontrolle kann nur dann auf Clients zugegriffen werden (inkl. Push Install), wenn alle Clients mit einem administrativen Standardbenutzer installiert werden

- Üblich sind Umgebungen ohne DES Server (nur DriveLock Agent mit lokaler Konfiguration) oder DES Server, die eine Konfigurationsdatei per HTTP Webserver verteilen

4 Versionshistorie

Die Versionshistorie enthält alle Änderungen und Neuerungen gegenüber der vorherigen DriveLock Version 2020.1.

4.1 Version 2020.2

DriveLock 2020.2 ist ein Feature Release.

4.1.1 Neue Funktionen und Verbesserungen

Die Version 2020.2 enthält viele neuen Funktionalitäten und Verbesserungen.

DriveLock Management Konsole

- Konfigurationsfilter: Aus den Parametern Computer, Zeit und Benutzer können zentrale Konfigurationsfilter erstellt werden. Über diese können jetzt Einstellungen, die innerhalb der Richtlinie bisher nur einmalig konfiguriert werden konnten, mehrfach für diese Gruppen eingestellt werden.

DriveLock Enterprise Service (DES)

- Das Tool ChangeDesCert.exe prüft, ob das vom DES bisher verwendete Zertifikat im System existiert und zeigt eine entsprechende Warnung an, wenn die Option zum Generieren eines neuen Zertifikats gewählt wird.
  Das DriveLock Enterprise Service Setup bietet standardmäßig an, das bisher verwendete Zertifikat weiter zu verwenden, wenn es im System existiert.

DriveLock Datenbanken

- Zusammenlegung der beiden bisher getrennten DriveLock Datenbanken zu einer gemeinsamen Datenbank mit Hilfe des Database Migration Wizard.

DriveLock Application Control

- Die Konfiguration von Anwendungsregeln wurde vereinfacht, über einen neuen Regeltyp (Datei-Eigenschaften-Regel) können nun verschiedene Regeltypen miteinander kombiniert werden.

> Hinweis: Wenn in einer Richtlinie aus einer älteren DriveLock Version (vor 20.2) bereits eine oder mehrere dieser Einzelregeln (Pfad, Eigentümer, Hash) verwendet wurden, werden diese automatisch zu einer Datei-Eigenschaften-Regel konvertiert, wobei die in den Einzelregeln gesetzten Eigenschaften übernommen werden. Datei-Eigenschaften-Regel sind kompatibel mit DriveLock Agenten vor Version 2020.2, sofern nur Kombinationen von Eigenschaften geprüft werden, die exakt den Einstellungsmöglichkeiten der jeweiligen alten Regeltypen entsprechen.

Microsoft Defender Integration

- Die Durchführung eines Defender Scans kann vom Benutzer verzögert werden
- Microsoft Defender kann über die temporäre Freigabe zeitlich befristet deaktiviert werden

DriveLock BitLocker Management

- Für die BitLocker-PBA können jetzt auch nur Zahlen verwendet werden. Für Systeme mit TPM ist dabei auch die Eingabe von 6 statt der üblichen 8 Ziffern möglich.
- Die Verschlüsselung mit BitLocker kann vom Benutzer verzögert werden

DriveLock Pre-Boot-Authentifizierung (PBA)

- DriveLock PBA unterstützt nun auch CardOS 5.0 / 5.3 Smartcards mit dem Standard DriveLock Middleware Profil PKCS#15

DriveLock Operations Center (DOC)

- Die DOC Benutzeroberfläche wurde optimiert und Listenansichten und zeitliche Darstellungen sind nun mit neuen Funktionalitäten ausgestattet, die mehr Flexibilität bei der Auswahl von Daten erlauben.

DriveLock Endpoint Detection & Response (EDR)

- Der Agent kann die Ereignisse weiterer Ereignisprovider (z.B. Windows Eventlog oder Produkte von Drittanbietern) an den zentralen DES senden. Diese lassen sich auch bei Alarmen (EDR) verwenden und mit anderen Ereignissen konsolidieren
- Vordefinierte Anwendungsregeln basierend auf MITRE ATT&CK® können hinzugefügt werden

Vulnerability Scan

- Der Schwachstellenscan kann über die Agenten-Fernkontrolle gestartet werden.

4.1.2 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) Nummern, sofern vorhanden.

Referenz	Device Control
EI-1228, EI-1235, EI-1236	Die Definition der Office-Dateiformate wurde anhand der jeweiligen Spezifikation erweitert.
EI-1220	Die benutzerdefinierte Meldung wird jetzt statt der Standardmeldung angezeigt, wenn ein Apple-Gerät durch eine Basis-Regel geblockt wurde.
	Ein Fehler im DriveLock Dateisystemfilter-Treiber wurde behoben, der einen BSOD beim Einstecken eines USB-Sticks verursacht hat.

Referenz	Disk Protection
	Die Deinstallation des DriveLock Agenten bricht ab, wenn auf dem System DriveLock Disk Protection installiert ist. Dem Benutzer wird eine entsprechende Meldung angezeigt, dass DriveLock Disk Protection erst deinstalliert werden muss, bevor der DriveLock Agent deinstalliert werden kann. Bisher ist die Deinstallation des DriveLock Agenten in diesem Fall ohne Fehlermeldungen fehlgeschlagen.

Referenz	DriveLock Agent
EI-1137	Google Drive-Laufwerke wurden von DriveLock gesperrt.
EI-815	In der Anzeige der Application Whitelist wurde zur Arbeits-erleichterung eine Spalte hinzugefügt, um den Hash der einzelnen Dateien anzeigen zu können.
EI-769	Fehler behoben, bei dem Japanisch als Sprache für die Agenten-Benutzeroberfläche ausgewählt werden konnte. Japanisch wird nicht mehr unterstützt.
EI-1179	Ein Wechsel des Netzwerkspeicherorts führte nicht sofort zu einer Neukonfiguration von MQTT. Dadurch konnte zeitweise der Agent per Agenten-Fernkontrolle u.U. nicht erreicht werden.
EI-1179	Agenten die zwischen verschiedenen DES Servern gewechselt haben, konnten zeitweise nicht per MQTT erreicht werden, da sie vom DES das falsche Serverzertfikat für die MQTT Kommunikation bekommen haben.
EI-1065	Teilweise haben Filter auf AD Gruppen und AD OUs nur korrekt funktioniert, wenn eine Verbindung zum AD bestand.
EIs: 1066, 1075, 1080, 1090, 1116, 1156	Am Update-Mechanismus wurden eine Reihe von Ver-besserungen vorgenommen.
EI-1182	Die Agentenfernkontrolle über den DES konnte unter Umständen scheitern, wenn der Agent zu einem Linked DES verbunden ist und die Fernkontrolle nur per MQTT möglich ist. Dies trat auf, wenn der Benutzer unter dem der Linked DES läuft keine Rechte auf dem zentralen DES hatte.

Referenz	DriveLock Agent
EI-932	Fehler behoben, bei dem ein DriveLock Agent in manchen Fällen in einen inkonsistenten Status geriet, wenn dieser im Nicht-beenden-Modus konfiguriert wurde.

Referenz	DriveLock Enterprise Service (DES)
	Bisher war es möglich, das DriveLock Enterprise Setup auszuführen, ohne ein Zertifikat anzugeben. Dieser Fehler ist nun behoben. Entweder muss ein Zertifikat gewählt werden oder es muss explizit angegeben werden, dass ein neues generiert werden soll.
EI-1095	Das Passwort für den DES Benutzer kann nun einen Strichpunkt enthalten. Vorher haben solche Passwörter zum Abbruch des DES Setups geführt.
EI-1122	Fehler beim Hinzufügen von lizenzierten Computern zum Server behoben.
EI-1097	Die Beschreibung (AD) des Computers wird beim Inventar nun korrekt gespeichert.
EI-1197	Fehler behoben bei der Konfiguration von Richtlinienzuweisungen auf sehr lange OU Namen.
EI-1171	Der Datenbank-Installationsassistent erkennt jetzt die konfigurierten Client SecurityProtocol Einstellungen (TLS).
EI-1246	Der Datenbank-Installationsassistent erkennt jetzt Einstellungen

Referenz	DriveLock Enterprise Service (DES)
	von verlinkten DES und trifft die passende Vorauswahl.
EI-1164	Ein Fehler bei Auswertung der Zertifikatsperrliste wurde behoben.
EI-1202	Performance-Verbesserungen beim Verarbeiten von AgentAlives (Agenten-Statusmeldung) und beim Speichern von Ereignissen

Referenz	DriveLock Management Konsole (DMC)
EI-1049	In manchen Fällen wurden in der DMC im Knoten Betrieb unter Agenten-Fernkontrolle Rechner mit dem Namen des vorherigen Eintrags angezeigt.
EI-1150	Fehler bei der Lizenzaktivierung in der DMC über Proxy behoben. Die DMC verwendet Proxy-Einstellungen, die über den Internet Explorer gesetzt werden. Der über den DriveLock Befehl `set-proxy` eingetragene Proxy wird nicht berücksichtigt.
EI-1133	Beim Speichern einer GPO kam es ggf. zu einem Fehler, dass ein Pfad nicht gefunden werde konnte.
EI-1135	Beim Speichern einer GPO kam es ggf. fälschlicherweise zu einem Fehler, der Aufrufer habe keine ausreichenden Rechte.
EI-1151	Beim Arbeiten im DriveLock File Protection Knoten war in einigen Dialogen immer der Root-Mandant vorausgewählt statt des tatsächlich gerade benutzten Mandanten.

Referenz	DriveLock Operations Center (DOC)
	Filter, die über einen Kontextmenübefehl gesetzt wurden, können nur in der Hauptansicht zurückgesetzt werden. In anderen Ansichten müssen Sie 'Aktualisieren' klicken, um die Filter zurückzusetzen.

Referenz	DriveLock Pre-Boot-Authentifizierung
EIs: 1103, 1106, 1110, 1138, 1160, 1170, 1178	Für einige Probleme mit internen Tastaturen in der PBA wurde ein Workaround eingebaut.
EI-1218	Single-Sign-On über die DriveLock PBA schlug fehl, wenn das Kennwort eines Benutzers außerhalb von DriveLock geändert wurde und zusätzlich SafeGuard-Dateiverschlüsselung (Credential Provider) auf einem System vorhanden war.

Referenz	EDR
EI-1241	Ereignisse, die generiert wurden, wenn keine Verbindung zum DES möglich war, wurden nicht in allen Fällen nachträglich zum DES geschickt.
EI-1240	Das Ereignis 257 (Datei gelöscht) wurde nicht in allen Fällen erzeugt.
EI-1154	Ein Fehler bei der Formulierung des Ereignisses 474 wurde behoben.

Refe-renz	Encryption-2-Go
EI-1204	Seit Windows 10 notifiziert Windows ein Entsperren des Benutzers als einen erneuten Logon und nicht als ein Entsperren. Im Zusammenhang mit der DriveLock-PBA und Enc2Go wird dadurch z.B. ein gerade laufendes Backup abgebrochen. Damit ein Entsperren wieder als Benutzer-initiiertes Entsperren erkannt werden kann, muss folgende GPO gesetzt sein: Windows Registry Editor Version 5.00 • ; Computer Configuration -> Windows Settings -> Security Settings ->• ; Local Policies -> Security Options "Interactive logon: Do not display last user name"• ; Set to "Enabled": asks to unlock the machine only to currently logged user• ; https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-display-last-user-name• [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]• "dontdisplaylastusername"=dword:00000001

	File Protection
EI-1146	Der Speicherverlust wurde behoben.
	Der Code wurde erweitert, um Kopieren/Verschieben zur Stammfreigabe zuzulassen.

	File Protection
EI-1111; EI-1279	Sophos SAVSERVICE.EXE wird als Backup App gehandhabt.
EI-1159	Beim Herunterfahren des Rechners konnte der FFE-Treiber nicht immer entfernt werden, da Windows den DriveLock-Dienst verfrüht beendet.
EI-1143	Problem beim Kopieren von Outlook Messages auf Netzwerk wurde behoben.

Referenz	Konfiguration (Richtlinien)
EI-1005	Der Agent wertet jetzt keine Gruppenrichtlinienobjekte mehr aus, wenn zentral gespeicherte Richtlinien bzw. Konfigurationsdateien vorhanden sind.

Referenz	Lizenzierung
EI-1192	In der mitgelieferten File-Protection-Testlizenz betrug die Anzahl der File-Protection-Lizenzen 0 statt 10.
EI-1099	Beim Öffnen einer Richtlinie in der DMC war auch mit gültiger Lizenz kurzzeitig die Warnung zu sehen, dass man "nur" mit einer Testlizenz arbeitet.

Referenz	Security Awareness
EI-1057	Die Security Awareness-Ansicht im DriveLock Operations Center (DOC) wird jetzt unabhängig von der Lizenzprüfung immer angezeigt.

5 Bekannte Einschränkungen

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

Lizenzaktivierung

Derzeit ist eine Lizenzaktivierung über einen Proxy-Server, bei dem eine explizite Anmeldung erforderlich ist, leider nicht möglich. In derartigen Umgebungen können Sie auf unsere telefonische Aktivierung zurückgreifen.

5.1 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.

5.2 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).

5.3 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.

5.4 DriveLock Device Control

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.

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

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).

Verwendung einer lokalen Richtlinie

Einige Einstellungen werden beim Speichern oder Exportieren einer lokalen Richtlinie nicht korrekt übernommen und können daher beim Testen dieser Einstellungen auf dem einzelnen Rechner nicht zu den gewünschten Ergebnisse führen. Bitte verwenden Sie für Ihre Tests daher eine der anderen Konfigurationsmöglichkeiten (Konfigurationsdatei, Gruppenrichtlinie oder zentral gespeicherte Richtlinie), die von dieser Einschränkung nicht betroffen sind.

5.5 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.

5.6 DriveLock Disk Protection

Disk Protection und DriveLock Operations Center (DOC)

Im DOC werden die Status-Informationen von mit DriveLock Disk Protection verschlüsselten Festplatten nicht korrekt angezeigt. Bis einschließlich DriveLock 2019.2 empfehlen wir daher die Überwachung des Disk Protection Status im DriveLock Control Centers.

Bis einschließlich DriveLock 2019.2 sollten Disk Protection Kunden für die Überwachung ihrer Systemumgebung die Funktionalität des DriveLock Control Centers verwenden.

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.

Neustart nach Installation der PBA auf Toshiba PORTEGE Z930:

Referenz: EI-751

Nach Aktivierung von Disk Protection mit PBA und Neustart des o.g. Notebooks, kann Windows nicht gestartet und somit das Notebook nicht verschlüsselt werden. Wir arbeiten an einer Lösung dieser Einschränkung.

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

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.

5.7 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, wählen Sie **Office 2016 nutzen, um Dateien die ich öffne zu synchronisieren** oder ähnliche Einstellungen in OneDrive ab. 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.

Ordnerverschlüsselung abbrechen

- Es wird nicht empfohlen, die Ver-/Entschlüsselung von Ordnern abzubrechen. Falls dies dennoch passiert (ist), löschen Sie die Datenbankdatei nicht, da sonst der Status der aktiven Dateien verloren geht.

File Protection und USB-Laufwerke

- Die Funktionalität, ein angeschlossenes USB-Laufwerk mit DriveLock File Protection vollständig zu verschlüsseln, kann für Laufwerke, die bereits einen verschlüsselten Ordner enthalten, nicht durchgeführt werden. In diesem Fall erscheint die Meldung " Cannot read management information from the encrypted folder".

Distributed File System (DFS)

- DriveLock File Protection unterstützt grundsätzlich auch die Speicherung von verschlüsselten Verzeichnissen auf Netzlaufwerken mit Distributed File System (DFS). Da DFS und das zugrundeliegende Speichersystem jedoch kundenspezifische Eigenheiten aufweisen können, empfehlen wir vor dem Einsatz einen ausführlichen Test von verschlüsselten Verzeichnissen. . Der Zugriff auf den als Laufwerk gemappten Ordner wird verweigert, wenn für das Mapping nicht der DFS Referenz Member gewählt wurde.

5.8 DriveLock Pre-Boot-Authentifizierung

Damit die Netzwerk-Funktionalität der DriveLock PBA zum Einsatz kommen kann, muss Hardware das TCP4 UEFI Protokoll unterstützen. Es kann daher auf manchen Systemen zu Pro-

blemen kommen, wenn das UEFI-BIOS nicht die benötigten Netzwerkverbindungen unterstützt.

Dies ist konkret bei folgendem System der Fall: Fujitsu LifeBook E459. (EI-1303)

5.9 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.

5.10 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

DriveLock Mobile Encryption (Encryption-2-Go) kann nicht für NTFS/EXFAT-Container verwendet werden.

5.11 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. In bestimmten Fällen sind auch 6 Zeichen (Zahlen) möglich, mehr hierzu in der aktuellen BitLocker Management Dokumentation auf DriveLock Online Help.
- 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.

Verschlüsselung auf Windows 7 Agenten

Bei der Verwendung der in DriveLock 2020.2 hinzugekommenen Ausführungsoptionen auf Windows 7 Agenten kann folgender Fehler auftreten: BitLocker verschlüsselt unter Windows 7 nicht, wenn die Optionen "wenn der Bildschirmschoner konfiguriert und aktiv ist" und "wenn keine Anwendung im Vollbildmodus ausgeführt wird" aktiviert sind.

5.12 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. Wir arbeiten an einer Lösung dieser Einschränkung.

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 aktualisiert. Wir arbeiten an einer Lösung dieser Einschränkung.

Keine Installation der DOC.exe starten, während die Festplattenverschlüsselung mit File Protection durchgeführt wird

Vermeiden Sie unbedingt, die DOC.exe gleichzeitig auf einer Festplatte zu installieren, die gerade mit File Protection verschlüsselt wird. (Referenz: EI-1025)

Ansichtseinstellungen im DOC

Da die DOC Ansichten in der neuen Version 2020.2 optimiert wurden, müssen bei einem Update von Version 2020.1 unter Umständen benutzerdefinierte Ansichtseinstellungen neu konfiguriert werden.

5.13 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.

5.14 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.

5.15 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.

5.16 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.

Für folgende Versionen gelten die entsprechenden End-Of-Life-Daten (EoL):

Version	Kunden-Support besteht bis:
7.9 und 2019.1	EoL Dezember 2020
2019.2	Mai 2022
2020.1	Dezember 2021
2020.2	Mai 2023

Supportzyklen:

Wir passen den Supportzeitraum einer neuen Produktversion an die Supportlaufzeit der Windows 10 Enterprise Edition an, welche im selben Zeitraum des Jahres veröffentlicht wurde (Release Frühjahr: ca. 18 Monate, Release Herbst: ca. 30 Monate). Mit dem Erscheinen einer neuen Version veröffentlichen wir gleichzeitig das Supportende dieser Version.

Wartungsupdates und Code-Korrekturen für Fehlern und kritischen Problemen werden in diesem Zeitraum veröffentlicht. Ebenfalls erfolgt die 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.

Upgrades:

Kunden mit früheren Produktversionen und gültigem Wartungsvertrag können die Umgebung auf die neueste Produktversion aktualisieren.

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