DriveLock Release Notes

Release Notes 2021.2

DriveLock SE 2021

Inhaltsverzeichnis

1 RELEASE NOTES 2021.2 5

1.1 Konventionen 5

1.2 Verfügbare Dokumentation 5

2 SYSTEMVORAUSSETZUNGEN 8

2.1 DriveLock Agent 8

2.2 DriveLock Management Konsole (DMC) 15

2.3 DriveLock Enterprise Service 16

2.4 DriveLock Operations Center (DOC) 18

2.5 DriveLock in Arbeitsgruppen-Umgebungen (ohne AD) 18

3 UPDATE VON DRIVELOCK 20

3.1 Migration der Datenbanken 20

3.1.1 Voraussetzungen für die erfolgreiche Migration 21

3.1.2 Durchführung der Migration 21

3.2 Update des DriveLock Agenten 23

3.3 Update des DriveLock Enterprise Service (DES) 24

3.4 Allgemeine Informationen zum Update auf die aktuelle Version 24

3.5 Manuelle Updates 25

4 VERSIONSHISTORIE 27

4.1 Version 2021.2 27

4.1.1 Neue Funktionen 27

4.1.2 Verbesserungen und Änderungen 30

4.1.3 Fehlerbehebungen 2021.2 31

4.2 Version 2021.1 38

4.2.1 Fehlerbehebungen 2021.1 HF1 38

4.2.2 Fehlerbehebungen 2021.1 39

4.3 Version 2020.2 45

4.3.1 Fehlerbehebungen 2020.2 45
4.4 Version 2020.1 54
4.4.1 Fehlerbehebungen 2020.1 54
4.4.2 Fehlerbehebungen 2020.1 HF1 62
4.4.3 Fehlerbehebungen 2020.1 HF2 65
4.4.4 Fehlerbehebungen 2020.1 HF3 66
4.5 Version 2019.2 70
4.5.1 Fehlerbehebungen 2019.2 70
4.5.2 Fehlerbehebungen 2019.2 HF1 76
4.5.3 Fehlerbehebungen 2019.2 SP1 78
4.5.4 Fehlerbehebungen 2019.2 HF3 82
5 BEKANNTE EINSCHRÄNKUNGEN 84
5.1 DriveLock Management Konsole (DMC) 84
5.2 Bekannte Einschränkungen des Agenten 84
5.3 DriveLock Enterprise Service (DES) 84
5.4 Installation der Management Komponenten über Gruppenrichtlinien 84
5.5 Self Service Freigabe 84
5.6 DriveLock, iOS und iTunes 85
5.7 DriveLock Device Control 85
5.8 DriveLock Disk Protection 86
5.9 DriveLock File Protection 89
5.10 DriveLock Pre-Boot-Authentifizierung 90
5.11 Verschlüsselung 91
5.12 DriveLock Mobile Encryption 91
5.13 BitLocker Management 92
5.14 DriveLock Operations Center (DOC) 93
5.15 DriveLock Security Awareness 94

5.16 DriveLock und Thin Clients 94

6 END-OF-LIFE-ANKÜNDIGUNGEN 96

7 TESTINSTALLATION VON DRIVELOCK 98

COPYRIGHT 99

1 Release Notes 2021.2

Die Release Notes enthalten wichtige Informationen zu neuen Funktionen, Verbesserungen und Fehlerbehebungen in der aktuellen Version von DriveLock. Ebenfalls sind in den Release Notes Änderungen oder Ergänzungen enthalten, die noch nicht in der Dokumentation erfasst sind.

Die gesamte DriveLock Dokumentation finden Sie auf DriveLock Online 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 Installationshandbuch

Dieses Dokument beschreibt die verschiedenen Installationsschritte der einzelnen DriveLock Komponenten. Beachten Sie, dass für DriveLock Managed Security Services Kunden andere Informationen zur Installation zur Verfügung stehen.

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).

> Hinweis: Das Administrationshandbuch befindet sich derzeit in Überarbeitung. Vorübergehend stellen wir deshalb zwei Varianten mit unterschiedlichen Inhalten zur Verfügung. Einige Inhalte sind derzeit nur auf Deutsch verfügbar, die englische Version wird schnellstmöglich nachgereicht.

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 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.

DriveLock BitLocker Management

Dieses Handbuch beschreibt alle notwendigen Konfigurationseinstellungen und die Funktionalität, die DriveLock für die Festplattenverschlüsselung mit Microsoft BitLocker zur Verfügung stellt. Folgende Themen sind in diesem Handbuch dokumentiert:

- **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 DOC Companion

Dies ist eine kurze Einführung in das Tool DOC Companion, das als Schnittstelle zwischen dem DriveLock Operations Center (DOC) und der DriveLock Management Console (DMC) dient.

Microsoft Defender Management

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

DriveLock Ereignisse

Diese Dokumentation enthält eine Auflistung aller aktuellen DriveLock Ereignisse mit Beschreibung.

DriveLock Linux-Agenten

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

DriveLock Security Awareness

Dieses Handbuch beschreibt die Security Awareness Funktionen, welche auch die Basis des Produktes DriveLock Security Awareness Content bilden.

Vulnerability Scanner

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

DriveLock Control Center Handbuch

Hinweis: Ab Version 2021.2 wird das DriveLock Control Center (DCC) Handbuch nicht mehr zum Download angeboten, weil das DCC nicht mehr im Produkt enthalten ist.

2 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.

2.1 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 4.6.2 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	2021.2	2021.1	2020.2	2020.1	2019.2
Windows 10 Pro					
Windows 10 21H2	+	+	+	+	+
Windows 10 21H1	+	+	+	+	+
Windows 10 20H2	+	+	+	+	+
Windows 10-2004	+	+	+	+	+
Windows 10-1909	-	+	+	+	+
Windows 10-1903	-	-	-	+	+
Windows 10-1809	-	-	-	+	+
Windows 10-1803	-	-	-	-	+
Windows 10-1709	-	-	-	-	-

OS-Version	2021.2	2021.1	2020.2	2020.1	2019.2
Windows 10-1703	-	-	-	-	-
Windows 10-1607	-	-	-	-	-
Windows 10 Enterprise					
Windows 10 21H2	+	+	+	+	+
Windows 10 20H2	+	+	+	+	+
Windows 10-2004	+	+	+	+	+
Windows 10-1909	+	+	+	+	+
Windows 10-1903	-	-	-	+	+
Windows 10-1809	-	+	+	+	+
Windows 10-1803	-	+	+	+	+

OS-Version	2021.2	2021.1	2020.2	2020.1	2019.2
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					

OS-Version	2021.2	2021.1	2020.2	2020.1	2019.2
Windows Server 2022	+	+	+	+	+
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					

OS-Version	2021.2	2021.1	2020.2	2020.1	2019.2
Windows 8.1	+	+	+	+	+
Windows 7 SP1	+	+	+	+	+
Windows XP	Support Lizenz not-wendig	Support Lizenz not-wendig	Support Lizenz not-wendig	Support Lizenz not-wendig	Support Lizenz not-wendig
Folgende Linux Derivate und neuere Versionen (eigene DriveLock Lizenz)					
CentOS 8	+	+	+	+	+
Debian 11	+	+	+	+	+
Fedora 34	+	+	+	+	+
IGEL OS 11.05	+	+	+	+	+
Red Hat Enter-prise Linux 5	+	+	+	+	+
SUSE	+	+	+	+	+

OS-Version	2021.2	2021.1	2020.2	2020.1	2019.2
15.3					
Ubuntu 20.04	+	+	+	+	+

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

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

Der Windows DriveLock Agent ist verfügbar für AMD/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: Sobald Windows 11 unsere Testphase komplett durchlaufen hat und für die neueste DriveLock Version validiert wurde, werden wir dies bekanntgeben. Für Version 2021.2 ist dies derzeit noch nicht der Fall.

Hinweise zu Linux

- DriveLock Application Control benötigt für den Einsatz auf Linux-Agenten Linux Kernel Version > 5.
- Application Control kann mit IGEL OS nicht verwendet werden.

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

Einschränkungen

- DriveLock Disk Protection ist für den Betrieb unter XP nur dann freigegeben, wenn es in bestimmten Geldautomaten verwendet wird.
- 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 nur 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.
- Disk Protection ist für Windows 10 ab Version 1703 für die zuvor genannten Windows Versionen 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 Windows 7 unter den erweiterten Legacy-Support gestellt werden sollte. Dies wird frühestens nach DriveLock Version 2021.2 der Fall sein.

Hinweis: Wir empfehlen beim Einsatz von Windows 7 die neueste Version zu verwenden. DriveLock unterscheidet nicht zwischen Standard-Windows-Lizenz oder ESU (Extended Security Update key). (Referenz EI-1349)

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.

2.2 DriveLock Management Konsole (DMC)

Bevor Sie die DriveLock Management Konsole 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 4.8 oder höher

Unterstützte Plattformen:

Die Management Konsole 2021.2 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.

Achtung: Ab dem Release der Version 2021.2 wird die DMC nur noch auf einem 64-Bit Windows Betriebssystem unterstützt, wir liefern daher kein 32-Bit Installationsprogramm mehr aus.

2.3 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 4.8 oder höher ist Voraussetzung für die Installation!

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)

> Hinweis: 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
- Windows Server 2022 64-Bit

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

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

Unterstützte Datenbanken:

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

> Achtung: Der DES benötigt den **Microsoft SQL-Server 2012 Native Client Version 11.4.7001.0**. Ist diese Komponente noch nicht installiert, geschieht dies automatisch vor der eigentlichen Installation des DES. Wenn eine ältere Version bereits installiert ist, wird diese automatisch aktualisiert.

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

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

2.4 DriveLock Operations Center (DOC)

Mit der Version 2021.2 wird kein MSI-Installationsprogramm für eine lokale Installation des DriveLock Operations Center (DOC.exe) mehr ausgeliefert. Alle Funktionen, die zusätzlich zur Webanwendung in der DOC.exe zur Verfügung standen, wurden auf andere Weise in unsere DOC-Plattform integriert (DOC Companion). Somit entfällt die Notwendigkeit einer zusätzlichen Applikation.

Hinweis: Das web-basierte DriveLock Operations Center ist in der Installation des DES enthalten und keine eigenständige Komponente. Es wird über einen Browser aufgerufen.

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

Bitte beachten Sie auch folgende Hinweise.

2.5 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 Operations Center (DOC) 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

3 Update von DriveLock

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

3.1 Migration der Datenbanken

Bei dem Update von DriveLock 2020.1 (oder älter) auf 2020.2 oder neuer 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-Installationsassistent nach einem erfolgreichen 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.

3.1.1 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

3.1.2 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 aktuellem Stand sein, damit eine Migration unterstützt wird.

   > Hinweis: Falls die Version einer Datenbank nicht aktuell sein sollte, bitte mit dem Database Migration 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.
       Die Ereignisse werden im DCC unter Forensics und im DOC unter 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.

3.2 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 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.

3.3 Update des DriveLock Enterprise Service (DES)

Beim Update des DES von Version 2021.1 auf höhere Versionen ist folgendes zu beachten:

Um die Aktualisierung erfolgreich durchführen zu können, benötigen Sie eine gültige Lizenz inklusive Wartung. Diese muss in Ihrem aktuell laufenden System in der Datenbank des DES gespeichert sein oder über die DMC erneuert und hochgeladen werden, bevor die Aktualisierung gestartet wird.

3.4 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 oder höher 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 oder höher auf neuere Versionen 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.

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.

Update von 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.

3.5 Manuelle Updates

Wenn zur Verteilung der Richtlinien nicht GPO verwendet wird, schlägt ein manuelles Update des Agenten 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 älteren auf neuere DriveLock Versionen

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. Dies betrifft vor allem Kunden, die Clientmanagement-Software verwenden, die möglicherweise die `msiexec` in einer Benutzer-Session ausführen. Das Problem lässt sich dadurch beheben, dass man dem msiexec-Aufruf folgende Parameter mitgibt:

- `MSIRESTARTMANAGERCONTROL=Disable`
- `MSIRMSHUTDOWN=2`

4 Versionshistorie

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

4.1 Version 2021.2

4.1.1 Neue Funktionen

DriveLock 2021.2 enthält folgende neue Funktionalitäten:

DriveLock Operations Center (DOC)

- Eine Richtlinie kann nun direkt aus dem DriveLock Operations Center editiert werden, ohne dass dafür eine DMC lokal auf dem Rechner installiert sein muss. Der Start des Richtlinien-Editors erfolgt über den neuen DriveLock **DOC Companion**, welcher bei der ersten Nutzung heruntergeladen und eingerichtet wird.
- Über diesen neuen DOC Companion können auch alle Funktionen der Agentenfernkontrolle direkt aus dem DOC ausgeführt werden. Auch dafür ist keine lokal installierte DMC mehr notwendig.
- Autorisierte Benutzer können über verschiedenen Ansichten im DOC einzelne oder mehrere Laufwerke permanent für alle oder bestimmte Computer oder Benutzer freigeben.
- Bei einem Laufwerk wird in der Detailansicht nun zusätzlich die Richtlinie, deren Version und der Name der Whitelist-Regel angezeigt, wenn es für dieses Laufwerk bereits eine solche Regel gibt.
- Autorisierte Benutzer können nun direkt im DOC eine neue Richtlinie erstellen oder löschen. Auch können sie direkt im DOC eine Richtlinie einer bestimmten Gruppe zuweisen und eine Zuweisung entfernen oder temporär deaktivieren.
- Single Sign-On am DOC: Die Anmeldung am DOC kann über externe Identitätsprovider erfolgen, z.B. Azure AD, die über den SAML Standard angesprochen werden (gilt nur für Managed Services Kunden, nicht für On-Premise Installationen).
- Die DOC-Berichte können nun per E-Mail an einen beliebigen Adressatenkreis in regelmäßigen Abständen und automatisch versendet werden.

BitLocker Management

- Wiederherstellungszertifikate für den Zugriff auf Wiederherstellungsdaten (wie zum Beispiel BitLocker Wiederherstellungsschlüssel) können in der DriveLock Datenbank gespeichert werden. Berechtigte Benutzer können auf diese direkt aus dem DOC

heraus zugreifen. Dadurch wird der Prozess für den Zugriff auf diese sensiblen Informationen vereinfacht und kann durch die Vergabe von Berechtigungen individuell freigegeben werden.

- BitLocker Wiederherstellungsschlüssel können nun in einem zuvor festgelegten Intervall automatisch ausgetauscht und in der DriveLock Datenbank gesichert werden, um sich noch besser vor Missbrauch dieser Daten zu schützen.
- Der regelmäßige Wechsel von BitLocker Kennwörtern durch den Benutzer wird nun durch DriveLock unterstützt.
- BitLocker Kennwörter können optional nun ebenfalls in der DriveLock Datenbank gesichert werden.
- Die BitLocker Verschlüsselung kann nun mit Hilfe eines zentralen Kennwortes nach Ablauf eines zuvor festgelegten Zeitraums auch ohne die Eingabe eines Benutzerkennwortes automatisiert gestartet werden.

DriveLock Pre-Boot-Authentifizierung

- Die DriveLock Pre-Boot Authentifizierung kann nun für eine bestimmte Anzahl von Neustarts oder während eines festgelegten Zeitraums automatisch übersprungen werden, um Installationsprozesse zu vereinfachen.
- Unterstützung für Benutzer, die bei der Eingabe ihres Benutzernamens am Anfang oder Ende zufällige Leerzeichen hinzufügen.

Microsoft Defender Management

- Dateien, die durch den Microsoft Defender AntiVirus in die Quarantäne verschoben wurden, können nun über die Agentenfernkontrolle wieder freigegeben werden

Protokollierung

- Zusätzliche Ebenen und Kontexte für die Protokollierung können jetzt in einer Richtlinie eingestellt werden. Diese erlauben eine wesentlich einfachere und schnellere Analyse von Fehlern.
- Log- bzw. Trace-Dateien von DriveLock können nun über das DOC von einem bestimmten Computer zentral angefordert und entweder in die DriveLock Datenbank oder sogar direkt zum DriveLock Support hochgeladen werden, ohne dass dafür ein Fernzugriff auf den Rechner notwendig ist.
- Sie können den DLSupportAgent jetzt auch verwenden, um per Kommandozeile die aktuellen Trace-Dateien hochzuladen.

DriveLock Linux Agenten

- Der Linux-Agent unterstützt nun das Erstellen lokaler Whitelistregeln, Regeln für Hash-Datenbanken und das Einschränken von Dateiregeln auf Benutzerebene (Applikationskontrolle).
- Geräte und Applikationen können nun unter Linux temporär freigegeben werden.
- Der Linux-Agent wertet jetzt bei der Lizenzierung konfigurierte Module aus.
- Der Linux-Agent unterstützt die neue, über Token gesicherte Installation.
- Die zusätzlichen Protokollierungsebenen können auch für Linux-Agenten gesetzt werden.

4.1.2 Verbesserungen und Änderungen

Verbesserungen und Änderungen in der Version 2021.2

> Hinweis: Mit diesem Release löst das DriveLock Operations Center (DOC) mit seiner modernen Web-Oberfläche endgültig das DriveLock Control Center (DCC) ab. Sämtliche Funktionen, die Sie aus dem DCC kennen, sind jetzt im DOC verfügbar.
> Die Weiterentwicklung des DCC wird eingestellt, es wird nicht mehr automatisch mit ausgeliefert. Sie können das Installationsprogramm für das DCC der Version 2021.2 über unser Supportportal (für berechtigte Benutzer) bzw. den Sie betreuenden Partner erhalten. Es enthält nach jetzigem Stand keine Änderungen im Vergleich zur aktuellen Version.

- Sie können neue Anforderungen oder Ideen, wie wir unser Produkt für Sie verbessern können, jetzt ganz einfach über das DriveLock Kundenforum mitteilen. Sie finden es unter https://drivelock.uservoice.com.
- Für die DriveLock PBA kann nun per Richtlinie vorgegeben werden, welche Treiber für Tastaturen bzw. für Smartcard verwendet werden sollen und ob eine bestehende Einstellung nicht verändert werden soll.
- Es ist jetzt keine Verschlüsselte-Medien-Regel mehr nötig, um verschlüsselte Laufwerke zu erlauben. Die gesetzten Berechtigungen für ein Laufwerk greifen jetzt auch bei Medien, für die Verschlüsselung erzwungen wird.
- Die Remote-Unterstützung für TeamViewer Quick Support wurde deaktiviert (Referenz EI-1612)
- Die Seitenleiste für die Hauptnavigation im DOC wurde neugestaltet und um die neuen Funktionen erweitert.
- Einige Elemente der Detailansichten im DOC wurden verbessert und um zusätzliche Informationen ergänzt, wie zum Beispiel die Aktivitätsanzeige bei den Laufwerken.
- Aktionen, die über das DOC für einen bestimmten Computer gestartet wurden, werden direkt ausgeführt.
- Sie können nun über das DOC auch auf ältere Wiederherstellungsinformationen zugreifen.
- Die Aktualisierung der DriveLock Richtlinien ist nun für einen Computer auch über das DriveLock Taskleisten-Symbol möglich.
- Die Installation von DriveLock Agenten kann nun zusätzlich durch ein Sicherheitstoken abgesichert werden, um eine irrtümliche oder missbräuchliche Installation zusätzlich zu erschweren. Hierbei ist jedoch zu beachten, dass die Verwendung von

Sicherheitstokens nicht zusammen mit verschlüsselten Ereignissen verwendet werden kann.

- Das DOC enthält im Bereich Defender Management weitere Widgets und überarbeitete Ansichten zum Zeitverlauf.

4.1.3 Fehlerbehebungen 2021.2

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2021.2 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Referenz	BitLocker Management / DriveLock PBA
EI-1594	Eine Zeitüberschreitung im BLM-Wiederherstellungsassistenten wird jetzt vermieden, wenn zu viele Wiederherstellungsinformationseinträge in der DES-Datenbank vorhanden sind
EI-1663	Die Zuweisung einer Richtlinie ohne gültige BitLocker Management-Lizenz konnte dazu führen, dass bereits verschlüsselte Systeme wieder entschlüsselt wurden und eine gegebenenfalls vorhandene DriveLock-PBA entfernt wurde.
EI-1386	Wenn Elemente der Systemsteuerung bereits über entsprechende Registry-Einträge ausgeblendet waren, wurden diese wieder angezeigt, sobald BitLocker Management über eine Richtlinie aktiviert wurde.
	Wenn der Autorisierungstyp in der Richtlinie von 'Kennwort' zu 'DriveLock-PBA' umgestellt wurde, wurden die Notfall-Anmeldungsdaten nicht oder erst nach dem nächsten Neustart zum DES hochgeladen.
EI-1396	Bei der Übernahme von bestehenden BitLocker-Umgebungen war es möglich, dass das neu zu vergebende Kennwort doppelt abgefragt wurde.

Referenz	BitLocker Management / DriveLock PBA
	Wenn das automatische Entsperren von Datenlaufwerken ausgeschaltet war, konnten Kennwörter nicht mehr durch den Agenten geändert werden, solange die jeweiligen Datenlaufwerke gesperrt waren.
EI-1431	Die BitLocker-Verschlüsselung wurde gestartet, ohne dass die erfolgreiche Übermittlung der Wiederherstellungsdaten zum DES abgewartet wurde.
EI-1616	Wenn zum Zeitpunkt der Ermittlung des Laufwerkstatus kein DES erreichbar ist, wurde kein weiterer Versuch unternommen, diesen hochzuladen.
	Die Notfallanmeldung an der DriveLock-PBA war in einzelnen Fällen nicht möglich, wenn das Hochladen der Daten wegen fehlender Verbindung zum DES fehlgeschlagen war.
	BitLocker-verschlüsselte USB-Laufwerke haben in einigen Fällen die Disk Protection-Installation verhindert.

Referenz	Defender Management
	Ein Problem beim Wechsel des Scantyps von Windows Defender wurde behoben.
EI-1485	In manchen Fällen hat der Agent Microsoft Defender fälschlicherweise als deaktiviert gemeldet (Defender Event 698: "Microsoft Defender ist deaktiviert"). Dieser Fehler ist jetzt behoben.

Referenz	Defender Management
EI-1644	Der Agent meldet eine erfolgreiche Aktualisierung der Defender Signatur jetzt sofort an den DES. Bisher wurde diese Information nur einmal am Tag gesendet und im DOC teilweise eine veraltete Signatur angezeigt.

Referenz	Device Control
EI-1578	Das Erstellen von Gerätelisten für Apple-Geräte in der DMC ist jetzt wieder möglich.
EI-1626	Dateizugriffe durch Prozesse, die global von Schattenkopien, Berichten und Filtern ausgeschlossen sind, werden jetzt bereits auf Treiberebene ausgefiltert, um Zugriffskonflikte mit Virenscannern zu vermeiden.
EI-1436	Beim CD-Brennen wurden Schattenkopien erzeugt, auch wenn in den entsprechenden Filtern Schattenkopien deaktiviert waren.
	Im Knoten Geräte fehlte die Bildlaufleiste in der Taskpad-Ansicht der Management Konsole.

Referenz	Disk Protection
EI-1730	Das Tool dlefi.exe funktioniert jetzt in der Windows PE-Umgebung.

Referenz	DriveLock Agent
	Bei der Verwendung der SB-Freigabe auf Agenten, die mit einem verknüpften DES Server verbunden sind, wurde ein Fehler behoben, der die Remote-Freigabe eines anderen Computers verhinderte.
EI-1645	Ein Performance-Problem, das auftrat, wenn ein USB-Stick eingesteckt wurde während der Agent im Simulationsmodus lief, ist jetzt behoben.
EI-1501	Das Ereignis 461 wurde in bestimmten Konfigurationen irrtümlicherweise gesendet, wenn der Zeitplan auf "Beim Systemstart" gesetzt wurde. Dies ist jetzt behoben.
EI-1540	Die Agentenoberfläche zeigt jetzt den korrekten Richtlinienstatus an, wenn Gruppenrichtlinienobjekte (GPOs) verwendet werden.
EI-1622	Die Drivelock.exe unterstützt nun Kommandozeilenaufrufe (mit -ArgumentList) aus dem " Start-Process"-Aufruf der Powershell.
EI-1518	Bei der Anmeldung eines weiteren Benutzers hat DriveLock nicht mehr reagiert, wenn ein CD-Brenner vorhanden war.
EI-1569	Bestimmte Dateiausschlüsse bei Dateifiltern haben nicht funktioniert.
EI-1682	Auf bestimmtem Lenovo Computern stürzte der Agent beim Einsammeln der Verschlüsselungsinformationen von den Laufwerken ab. Dieser Fehler ist jetzt behoben.
EI-1618	Wenn ein Client aufgrund eines Wechsels des Netzwerkstandorts zu einem anderen DES wechselte, verwendete die MQTT-Ver-

Referenz	DriveLock Agent
	bindung weiterhin den vorherigen DES. Dies ist jetzt behoben.
EI-1558	Das Erstellen eines bootfähigen USB-Laufwerks mit Rufus schlug fehl oder dauerte sehr lange, weil es vom DriveLock Agenten blockiert wurde.

Referenz	DriveLock Enterprise Service (DES)
EI-1532	Es wurde ein Problem mit zu hoher CPU Auslastung auf verknüpften DES gelöst. Dieses trat unter Umständen auf, wenn der verknüpfte DES nicht auf die Ports 4568 bzw. 8883 auf dem zentralen DES zugreifen konnte.
	Es wurde ein Fehler behoben, der zu Handle Leaks im DES führte.

Referenz	DriveLock Operations Center (DOC)
EI-1384	Das Anfordern des Bitlocker-Wiederherstellungsschlüssels über das DOC führt jetzt zum Erneuern des Wiederherstellungschlüssels auf dem Agenten und nicht länger dazu, dass im Dialog zum Kennwort-Wechsel auf dem Agenten das alte Kennwort benötigt wird.
EI-1498	Der Wert im Feld Ver-/Entschlüsselung wird durchgeführt im Widget Verschlüsselungsinformation wird jetzt korrekt angezeigt.

Referenz	EDR/Ereignisse
	Eine Änderung der Anzeigetexte von Ereignisquellen von Drittanbietern wird jetzt in der Datenbank gespeichert.
	Die Anzeige der Namen von Ereignisparametern in der DMC wurde verbessert.

	File Protection
EI-356	Wenn die Berechtigungen eines Benutzers im Knoten Zentral verwaltete Ordner auf "Nur Lesen" gesetzt wurden, wurden sie nach erneutem Öffnen des Dialogs wieder auf "Schreiben" geändert. Dies ist jetzt behoben.
EI-1664	Der Knoten File Protection in der Richtlinie enthält auch Einstellungen, die für Encryption 2-Go benötigt werden. Dennoch war der Knoten mit einer reinen Encryption 2-Go-Lizenz nicht verfügbar.
EI-1068	Das Öffnen, Ändern und Speichern eines Office-Dokuments in einem verschlüsselten Ordner in einer gemounteten Netzwerkfreigabe verursacht jetzt keine Fehler mehr.
	Der Bluescreen beim Zugriff von einem anderen Computer ohne DriveLock auf einen gemounteten verschlüsselten Ordner in einem Computer mit DriveLock wurde behoben.
EI-1543	Ein Problem wurde behoben, das zu beschädigten Excel-Dateien führen konnte, wenn diese aus einem verschlüsselten Ordner geöffnet wurden.
EI-1562	File Protection arbeitet jetzt korrekt mit kennwortgeschützten

	File Protection
	Excel-Dateien.
EI-1574	Einige Ereignisse von File Protection wurden nicht protokolliert. Dies ist jetzt behoben.

Referenz	Security Awareness
EI-1614	Die Security Awareness Library wird jetzt nur noch in der jeweiligen Session des Benutzers geöffnet.

4.2 Version 2021.1

4.2.1 Fehlerbehebungen 2021.1 HF1

DriveLock 2021.1 HF1 ist ein Maintenance Release.

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2021.1 HF1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Referenz	DriveLock Agent
EI-1517	Wenn auf dem Reiter Awareness bei der Angabe von Verwendungsrichtlinien die Option "Als anderer Benutzer autorisieren" manuell gesetzt war, wurde diese bei der Auswertung nicht berücksichtigt (das Verhalten entsprach dem einer nicht aktivierten Option).
EI-1534	Das Perfomance-Problem wurde behoben.

	File Protection
EI-387, EI-1086, EI-1148	Ein Rechteproblem, bei dem die volle Kontrolle über Netzwerkfreigaben erforderlich war, wurde behoben. (Dasselbe gilt für alle zugehörigen EIs).

Referenz	DriveLock Management Console
EI-1516	Nach dem Upgrade auf DriveLock 2021.1 konnten die Optionen für die Client-Compliance und die Hard- und Software-Inventarisierung nicht mehr konfiguriert werden, wenn keine Lizenz für den Vulnerability Scanner vorhanden war (obwohl diese Funktionen nicht von einer Lizenz abhängen sollten).

4.2.2 Fehlerbehebungen 2021.1

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2021.1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Referenz	BitLocker Management
	Die Konfiguration der BitLocker-Kennwortkomplexität wurde nicht richtig gespeichert, wenn zuerst eine Komplexitätseinstellung vorgenommen und anschließend die Kennwortkomplexität deaktiviert wurde.
	Das Kennwort für Datenpartitionen wurde doppelt geändert, sofern gleichzeitig auch das der Systempartition geändert wurde. Dadurch konnte es bei der Übernahme bestehender BitLocker-Umgebungen zu dem Fehler kommen, dass einzelne Datenpartitionen erst nach einem Reboot übernommen wurden.
EI-1312	Eine bestehende Konfiguration zum Sichern der BitLocker-Wiederherstellungsschlüssel im Active Directory wurde nach der Installation von DriveLock so überschrieben, dass das Sichern danach nicht mehr möglich war.
EI-1388	Die Übernahme bestehender BitLocker-Umgebungen konnte für Partitionen fehlschlagen, bei denen nur ein Protektor vorhanden war.
	Die Übernahme von BitLocker-verschlüsselten Systemen ist fehlgeschlagen, wenn keine Protektoren vorhanden waren. Nach der Installation von Windows 10 werden System- und Datenpartitionen unter bestimmten Voraussetzungen mit BitLocker vorverschlüsselt, ohne dass Protektoren angelegt werden.
EI-1342	Bei bestimmten Einstellungen in der Windows-Gruppenrichtlinie konnte das BitLocker-Kennwort von Datenpartitionen nicht durch BitLocker Management gesetzt werden.
EI-1337	Unter bestimmten Umständen konnte der Wechsel des Pre-Boot-

Referenz	BitLocker Management
	Authentifizierungstyps bei BitLocker nicht ausgeführt werden. Betroffen waren nur Systeme, bei denen keine Neuverschlüsselung erforderlich war.
	Das Beenden des Agenten-Dienstes wurde durch die BitLocker Management-Komponente stark verzögert. In Einzelfällen konnte das auch zu einem Absturz des Dienstes führen.
	Bei in der Richtlinie festgelegten Optionen zum Pausieren der BitLocker-Verschlüsselung konnte es trotz des Eintretens eines solchen Ereignisses dazu kommen, dass die Verschlüsselung fortgesetzt wurde.
	Bei der Übernahme bestehender BitLocker-Umgebungen mit mindestens einer gesperrten Datenpartition war es möglich, dass die Schaltfläche zum Entsperren nach bereits erfolgtem Entsperrvorgang nochmals gedrückt werden konnte. Dadurch war es nicht mehr möglich, den Assistenten zu beenden.
EI-1395, EI-1396, EI-1416	Bei der Übernahme von BitLocker-verschlüsselten Laufwerken wurde das Kennwort zweimal abgefragt, wenn sowohl der Systemprotektor als auch der Verschlüsselungsalgorithmus geändert werden musste.
EI-1418	War die Systemsteuerung über eine Systemrichtlinie auf bestimmte Elemente eingeschränkt, wurde diese Einstellung überschrieben, sobald DriveLock BitLocker Management aktiviert wurde.
EI-1464	Wenn die Lizenz für BitLocker Management gefehlt hat, war es möglich, dass ein zuvor verschlüsseltes System entschlüsselt wurde, obwohl die Einstellung 'Bei Konfigurationsänderungen nicht entschlüsseln' gesetzt war.

Referenz	Defender Management
	Wenn der Aufschubdialog für den Start des Defender-Scans angezeigt wurde, war es nicht mehr möglich, den DriveLock-Dienst zu beenden.
	Der Aufschubdialog für den Defender-Scan konnte angezeigt werden, obwohl kein Aufschub konfiguriert war.
	Die Anzeige der Dateien in Quarantäne auf dem Reiter Defender des Agenten-Fernkontrolldialogs hat fehlerhafte und gekürzte Einträge enthalten. Außerdem war nur ein Teil des Textes sichtbar, da der Tooltip-Text gefehlt hat.

Referenz	Device Control
EI-1323, EI-1336, EI-1341	Dateidefinitionen für mehrere Dateitypen wurden vom Dateifilter falsch verarbeitet.
EI-1220	Ein Fehler wurde behoben, der bei der Verarbeitung von benutzerdefinierten Nachrichten beim Sperren von iPhone- und Android-Geräten auftrat.
EI-1294	Bei Laufwerksregeln gibt es jetzt eine Reihenfolge, welche Regel Priorität hat.

Referenz	DriveLock Agent
EI-1321	Unter bestimmten Umständen war es nicht möglich, eine Aktion auf dem Agenten auszuführen, wenn die MMC und das DOC gleichzeitig gestartet und für die Agentenfernkontrolle verwendet wurden. Wenn am Windows ein Benutzer angemeldet war, der keine Rechte für die Agentenfernkontrolle hatte, war es nicht möglich

Referenz	DriveLock Agent
	aus dem DOC heraus Agentenfernkontrolle zu verwenden, selbst wenn der am DOC angemeldete Benutzer Rechte dazu hatte.

Referenz	DriveLock Enterprise Service (DES)
EI-1302	Im DriveLock Enterprise Service Setup ist es möglich, Benutzer aus einer anderen vertrauenswürdigen Gesamtstruktur ('trusted forest model') auszuwählen.
EI-1355	Ein Fehler wurde behoben, der zum Absturz des DES führen konnte, wenn ein Computer gelöscht wurde.

Referenz	DriveLock Pre-Boot-Authentifizierung
	Wenn die Systempartition nicht verschlüsselt, die DriveLock-PBA jedoch installiert werden sollte, wurden keine Emergency Logon-Daten hochgeladen.
	Wenn bei aktivierter DriveLock-PBA lediglich Datenpartitionen, nicht aber die Systempartition verschlüsselt wurden, wurde das Kennwort für die Datenpartitionen nicht abgefragt. Dies ist jedoch nötig, weil in diesem Fall Datenpartitionen nicht automatisch entsperrt werden und ein manuelles Entsperren mit einem Benutzerkennwort erforderlich ist.
	Bei mit BitLocker vorverschlüsselten Laufwerken wurde die Installation der DriveLock-PBA gestartet und mit einem Fehler beendet.
EI-1243	Nach der Aktivierung der Netzwerk-PBA wurde das Systemlaufwerk trotz bereits eingerichteter DriveLock-PBA entschlüsselt und anschließend neu verschlüsselt.
EI-1287	Bei der Verwendung des Windows-Schnellstarts wurden Daten-

Referenz	DriveLock Pre-Boot-Authentifizierung
	partitionen nach dem Starten nicht mehr automatisch entsperrt. In Umgebungen mit eingerichteter DriveLock-PBA war der BitLocker-Wiederherstellungsschlüssel zum Entsperren notwendig.

Referenz	EDR/Ereignisse
	Im Text zum Ereignis 635 hat der Fehlercode zum Eingrenzen des Fehlers gefehlt. Das Ereignis informiert darüber, dass das Setzen des BitLocker-Kennworts fehlgeschlagen ist.
	Ein Fehler wurde behoben, durch den das Speichern einer neuen Alert-Kategorie in einer zentral gespeicherten Richtlinie fehl-schlug.

Referenz	Encryption-2-Go
EI-1212	Der Umgang mit unvollständigen Wie-derherstellungsinformationen wurde korrigiert.

	File Protection
EI-1259	Ein Fehler mit einem BSOD in der Terminal-Server-Umgebung wurde behoben.
EI-1163	Ein Fehler wurde behoben, bei dem das Kopieren von XML-Dateien auf SMB 3.0 Cluster-Freigaben die XML-Datei beschädigte.

Referenz	Konfiguration (Richtlinien)
EI-376	Der Benutzer wurde nicht darauf hingewiesen, dass in der Ser-

Referenz	Konfiguration (Richtlinien)
	verkonfiguration das unsichere HTTP-Protokoll ausgewählt war.
EI-1346	Das Caching von AD-Informationen wurde verbessert. Auch wenn keine AD-Informationen vorhanden sind, können DriveLock Gruppen und Zuweisungen zentral gespeicherter Richtlinien verwendet werden, so lange diese nicht von AD-Informationen abhängig sind.
	Einige Einstellungen wurden beim Speichern oder Exportieren einer lokalen Richtlinie nicht korrekt übernommen. Dies ist jetzt behoben.

Referenz	Lizenzierung
EI-1150	Die Lizenzaktivierung in der MMC funktioniert jetzt auch bei Verwendung eines Proxyservers.

Referenz	System Management
EI-1307	Der Netzwerkname des Computers wird, sofern verfügbar, vom Agenten jetzt als FQDN zurückgeliefert und der NetBIOS Name nur noch verwendet, wenn es keinen FQDN gibt. Damit funktioniert die Fernsteuerung von Agenten robuster, da auch Rechner in anderen Domänen gefunden werden.

4.3 Version 2020.2

4.3.1 Fehlerbehebungen 2020.2

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2020.2 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.
EI-1188	Auf die Speicherkarte in einer Digitalkamera, die mit USB-Kabel an den Fat-Client oder Thin-Client angeschlossen ist, kann jetzt zugegriffen werden, wenn der Registry-Wert `MtpRestartTimeout (REG_DWORD)` im Registry-Schlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\CenterTools\DLSettings\Devices` auf 3000 (ms) gesetzt ist. Hinweis: Beachten Sie bitte, dass seit Windows 10 Update 2020 unter Umständen nur dann auf die Kamera zugegriffen werden kann, wenn im Citrix Workspace der virtuelle Kanal Allgemein (Generic) verwendet wird.
EI-1230	Nach Verbinden eines USB-Sticks konnte es zu einem Bluescreen kommen. Dies ist jetzt behoben.

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 Arbeitserleichterung 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

Referenz	DriveLock Agent
	funktioniert, wenn eine Verbindung zum AD bestand.
EIs: 1066, 1075, 1080, 1090, 1116, 1156	Am Update-Mechanismus wurden eine Reihe von Verbesserungen 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.
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 Control Center (DCC)
EI-1068, EI-1069, EI-1091, EI-1076	Im DCC wird in der Spalte ConfigID jetzt der Name und die Version der Richtlinien angezeigt anstelle der GUID.

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.

Referenz	DriveLock Enterprise Service (DES)
EI-1095	Das Kennwort für den DES Benutzer kann nun einen Strichpunkt enthalten. Vorher haben solche Kennwörter 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 Richt-linienzuweisungen auf sehr lange OU Namen.
EI-1171	Der Datenbank-Installationsassistent erkennt jetzt die kon-figurierten Client SecurityProtocol Einstellungen (TLS).
EI-1246	Der Datenbank-Installationsassistent erkennt jetzt Einstellungen von verlinkten DES und trifft die passende Vorauswahl.
EI-1164	Ein Fehler bei Auswertung der Zertifikatsperrliste wurde beho-ben.
EI-1202	Performance-Verbesserungen beim Verarbeiten von AgentAlives (Agenten-Statusmeldung) und beim Speichern von Ereignissen

Referenz	File Protection
EI-1216	Beim Entschlüsseln von verschlüsselten Ordnern konnte es zum Absturz eines Dienstes (DLFfeGui) kommen. Dies ist jetzt beho-ben.

Referenz	File Protection
EI-1143, EI-1163	Während des Mountens eines verschlüsselten Ordners startet jetzt nicht mehr der Dienst zum Nachverschlüsseln unverschlüsselter Dateien.

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 `setproxy` 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

Referenz	DriveLock Operations Center (DOC)
	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.

Referenz	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.
EI-1111; EI-	Sophos SAVSERVICE.EXE wird als Backup App gehandhabt.

	File Protection
1279	
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.

4.4 Version 2020.1

4.4.1 Fehlerbehebungen 2020.1

Dieses Kapitel enthält Informationen zu Fehlern, die in der DriveLock Version 2020.1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Referenz	BitLocker Management / DriveLock Pre-Boot-Authentifizierung
EI-891	In der Übersicht für die Festplattenverschlüsselung wurde die Pre-Boot-Authentifizierung als deaktiviert angezeigt, obwohl die BitLocker-PBA ausgewählt war.
EI-872 , EI-989	Der Firmware-Tastaturtreiber wird, sofern möglich, jetzt durch einen neueren Treiber ersetzt, der Layouts unterstützt.
EI-946	Der Credential Provider für die NetIQ Client Login Extension funktionierte unter Windows 10 nicht korrekt mit DriveLock zusammen. Benutzer wurden nicht zur Pre-Boot-Authentifizierung hinzugefügt.

Referenz	Device Control
EI-453	Beim Hinzufügen einer neuen Dateityp-Definition erschien fälschlicherweise ein Warnung, dass für diesen Typ bereits eine Dateityp-Definition existiere.
EI-819	Laufwerks- und Gerätelisten wurden nicht mehr in der Richtlinie abgespeichert und waren somit nicht mehr einsetzbar.
EI-540	Brenn-Geräte werden jetzt besser erkannt und Brennen für Benutzer mit Schreibzugriff auf CD/DVD-ROM ist jetzt aktiviert.

Referenz	Device Control
EI-776	Die Abhängigkeiten des MTP-Treibers, die das Laden des MTP-Treibers verhinderten, wurden entfernt.
EI-859	Eine irreführende Nachricht bzgl. des Freigabestatus eines iPhones wird jetzt nicht mehr angezeigt.

Referenz	Disk Protection
EI-915	Ein neuer PS2 Tastatur-/Maus-Kombitreiber ersetzt Tastaturtreiber. Splash-Screen wurde angepasst. Tastatur-Layoutliste gekürzt und umsortiert. ESC-Taste schließt nun nicht nur offene Menüs, sondern aktiviert auf die F1-Tasten-Funktion (Kennwort-Login).
EI-756	Bei mehreren Dell-Notebooks wurde das SSO-Datenübertragungsverhalten (BSOD) korrigiert.
EI-995	SSO für die Token-Anmeldung ist in DriveLock Credential Provider festgelegt.
EI-914	Wenn eine Lizenz aus einer Richtlinie für Disk Protection oder BitLocker-Managemententfernt wurde, die separate Installationsschritte erfordert und diese Schritte bereits ausgeführt wurden, zeigte der DriveLock Agent ein fehlerhaftes Verhalten. Dies ist jetzt behoben.

Referenz	DriveLock Control Center (DCC)
EI-721	Fehler bei der Anzeige der Lizenzinformationen behoben
EI-997	Fehler beim Laden des DCC Helpdesk behoben, was bei großer Anzahl von Computern mit FDE RecoveryDaten auftreten konnte.
EI-749	Im Helpdesk des DCC konnte bei einer gefilterten Liste nicht auf einen Agenten verbunden werden, welcher nicht in der Liste auftauchte.

Referenz	DriveLock Enterprise Service (DES)
EI-896	Das Utility ChangeDesCert funktioniert jetzt auch korrekt wenn mehrfach hintereinander ein Zertifikat mit dem Menübefehl "Select" ausgewählt wurde.
EI-931	Der DES (MQTT) versucht nicht länger auf dem Port 8083 und 8084 zu hören. Um Konflikte zu reduzieren wird anstatt Port 8080 jetzt Port 18082 verwendet. Dieser Port wird nur lokal verwendet.
EI-977	Die Performance beim Abfragen von Konfigurationseinstellungen zur Agentenfernsteuerung (MQTT) durch den Agenten auf dem DES wurde durch Caching verbessert.
EI-773, EI-998, EI-754	Performance-Verbesserungen am DES (Alive und Ereignisverarbeitung)
EI-1024, EI-977	Der Fehler im DES bzw. in der MQTT Konfiguration, der zu erhöh-

Referenz	DriveLock Enterprise Service (DES)
	ter Last am DES Rechner führte, wurde behoben.
EI-874	Der Fehler im DES, der zu stark erhöhtem Speicherverbrauch bei der Auflistung von vielen Richtlinien geführt hat, wurde behoben.
EI-937	Ein Fehler bei der Verarbeitung von Dateizugriff-Ereignissen mit langen Pfadnamen wurde behoben.

Referenz	DriveLock Operations Center (DOC)
EI-907	Das DOC unterstützt jetzt die Anmeldung von Benutzern aus Childdomänen und Domänen, die per Forest Trust eingebunden sind.
EI-922	Der Menübefehl, mit dem das DOC aus dem DCC heraus zu starten ist, funktioniert jetzt auch wenn der DES Server einen sehr langen FQDN (fully qualified domain name) hat.
EI-1000	Der aufgetretene Fehler ist durch Verwendung von Microsoft Edge Version 81.0.416.64 (Offizieller Build) (64-Bit) behoben.
EI-1006	DriveLock Agenten können jetzt über die Eigenschaft "Festplattenverschlüsselungsstatus" gruppiert werden.

Referenz	Encryption-2-Go
EI-506	DriveLock Mobile Encryption (Encryption-2-Go und File Pro-

Referenz	Encryption-2-Go
	tection) kann jetzt auf Apple OS X und Mac OS X ohne Einschränkungen verwendet werden.
EI-761	In Version 2020.1 wurde ein Workaround für FAT 32 eingebaut, mit dem das beschriebene Problem gelöst wird.

Referenz	File Protection
EI-763, EI-767	Treiber wurde überarbeitet, um potentielle Synchronisationsprobleme zu beheben.
EI-941	Problem beim Download von Office 365 Dateien in verschlüsselte Ordner mit Pfadnamen > 128 Zeichen wurde behoben.
EI-825	Im Treiber wurde soweit wie möglich limitierende statische durch dynamische Speicher-Allokation ersetzt, um Probleme mit langen Dateinamen zu vermeiden.
EI-952	Der für das Löschen eines verschlüsselten Ordners notwendige Unmount lief völlig unsynchronisiert ab. Dies wurde verbessert.
EI-953	Der für das Umbenennen eines verschlüsselten Ordners notwendige Unmount lief völlig unsynchronisiert ab. Dies wurde verbessert.
EI-954	Der zum Entschlüsseln erforderliche Unmount fehlte und wird jetzt durchgeführt.

Referenz	File Protection
EI-955	Der für das Kopieren und Verschieben erforderliche Unmount fehlte und wird nun durchgeführt.
EI-956	Die Einstellungen für die Shell-Erweiterungen werden jetzt korrekt ausgewertet.
EI-537	Verbesserte Erkennung von zentral verwalteten verschlüsselten Ordnern
EI-940	Die nicht initialisierte Ereignis-Variable CloudId wird nun initialisiert

Referenz	Konfiguration
EI-752	Der DriveLock Agent kann jetzt erfolgreich mit Richtlinien-Konfigurationsdateien (.cfg) auf UNC Pfaden arbeiten.
EI-803	Die Konfiguration über die Konfigurationsdatei funktionierte nicht.
EI-398	Richtlinien ohne Lizenzinformationen konnten die Lizenzinformationen beeinflussen.

Referenz	Management Konsole
EI-999, EI-990	Das Laden der Richtlinienzuweisungen in der Management Konsole erfolgte zu langsam.

Referenz	Management Konsole
EI-827	Beim Hinzufügen neuer Lizenzen in der Management Konsole wurden neu hinzugekommene Module automatisch für sämtliche Computer aktiviert.
EI-719	In der Management Konsole wurde bei der Vorschau der Kontaktinformationen für den Offline Unlock Wizard ein zu langer Text einfach abgeschnitten.
EI-864	Die Management Konsole verwendet beim Zugriff aufs Internet jetzt den Proxy, der in den Internet-Explorer Einstellungen konfiguriert ist.

Referenz	Mobile Encryption
EI-643	Optimierungen für den Verschlüsselungstreiber wurden bereits in Version 2019.2 durchgeführt
EI-639	DriveLock MAC-Anwendungen werden auf Windows-Rechnern nicht mehr verschlüsselt.

Referenz	SB-Freigabe
EI-538	Der Self-Service auf dem Agenten wird jetzt wie konfiguriert beendet wenn sich ein Benutzer in einer RDP-Sitzung abmeldet.
EI-762	Die Icons für die Wizard-Banners müssen eine Größe von 49x49 Pixeln haben - da sie bisher nur 48x48 Pixel groß waren, wurden unschöne weiße Linien in die Bilder hinzugefügt.

Referenz	SB-Freigabe
EI-724	Beim Offline Unlock Wizard konnte man zur nächsten Seite weiter springen, auch wenn man noch keine freizugebenden Module ausgewählt hatte.
EI-867	Beim erstmaligen Erreichen der Dialogseite, auf der die Dauer der Deaktivierung von Richtlinieneinstellungen gesetzt wird, wurde bisher die aktuelle Uhrzeit eingetragen. Wenn man dann eine Seite zurück und wieder vor ging, stand demnach eine Zeit aus der Vergangenheit auf der Dialogseite. Es wird jetzt bei jedem Erreichen der Seite die aktuelle Zeit eingetragen, jeweils erhöht um die maximal erlaubte Freigabedauer.
EI-759	Unter gewissen Umständen schlug die temporäre Freigabe des Agenten fehl mit "Zugriff zum DriveLock-Agenten verweigert".
EI-991	Die SB-Freigabe funktioniert nicht auf Computern, die von der OU identifiziert wurden.

Referenz	Security Awareness
EI-810	Built-in Bilder von Security Awareness waren nur in englisch vorhanden.

4.4.2 Fehlerbehebungen 2020.1 HF1

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2020.1 HF1 behoben sind.

Als Referenz dienen EI-Nummern, sofern vorhanden.

Referenz	Application Control
	Wenn man bei der Einstellung **Verzeichnisse, die für die lokale Whitelist gelernt werden sollen** die Option **Einstellen auf feste Liste** ausgewählt hatte und dann einen Ordner ausschließen wollte, führte dies zu ungültigen Einträgen (leere Einträge oder erstes Zeichen abgeschnitten).
	Ordner für Anwendungsregeln waren nach einem Neustart der MMC nur auf erster Ebene sichtbar - Unterordner in tieferer Ebene waren zwar immer noch vorhanden, aber nicht mehr sichtbar.

	Device Control
EI-1070	Bei bestimmten Konfigurationen konnte in einem Zeitraum von Millisekunden nach dem Verbinden eines Laufwerks mittels eines Skripts darauf zugegriffen werden. Dieser Fehler ist behoben.

Referenz	DriveLock Control Center (DCC)
EI-1055	Für Benutzer konfigurierte OU-Filter funktionieren jetzt auch für Ereignis-Reports.

Referenz	DriveLock Enterprise Service (DES)
	DriveLock Service-Konto benötigt keine Administrator-Rechte mehr auf dem Linked DES.

Referenz	DriveLock Management Konsole (DMC)
	Der Mandantenname der Richtlinie wird jetzt mitgeschickt, damit beim Lesen von Laufwerksinformationen vom Remote-Client kein Fehler auftritt.

	DriveLock Operations Center (DOC)
	Die Anzeige eines Computers in der Computer-Detailansicht des DOC funktionierte nicht korrekt (Server-Fehler), wenn der Name oder Pfad der OU ein Hochkommata enthielt.

Referenz	DriveLock Pre-Boot-Authentifizierung
	Für die Installation der DriveLock PBA wurde die Fehlerbehandlung verbessert.
	Bei Änderungen an den Anmeldemethoden für die Pre-Boot-Authentifizierung konnte es vorkommen, dass die PBA nicht richtig installiert wurde.
EI-1071	Einige MMC-Einstellungen für die DriveLock PBA wurden nicht richtig gespeichert. Betroffen sind die Seiten "Benut-

Referenz	DriveLock Pre-Boot-Authentifizierung
	zersynchronisation" und "Benutzer".
	Der Bluescreen nach PBA-Anmeldung am verschlüsselten Rechner (Windows 10 2004 BIOS) erscheint nicht mehr.

Referenz	File Protection
EI-1053	Der Menüeintrag "[DriveLock File Protection]" kann jetzt über das Taskleistensymbol des DriveLock Agenten deaktiviert werden.
EI-1064	Die File & Folder Encryption in Kombination mit der Full Disk Encryption kann nach einem Windows Inplace Upgrade einen Bluescreen BugCheck 7F, {8, ...} erzeugen. Das Windows Inplace Upgrade ändert die Reihenfolge, in der der FFE-Treiber geladen wird. Dies wird beim ersten Booten nach dem Upgrade korrigiert, aber der Bluescreen kann einmal auftreten.

Referenz	Microsoft Defender
	Beim Einstellen eines bestimmten Wochentags für den Defender Scan wurde anschließend jeweils der nächste Wochentag angezeigt (also z.B. Freitag statt Donnerstag). Abgespeichert und ausgewertet wurde aber der tatsächliche Wochentag.

4.4.3 Fehlerbehebungen 2020.1 HF2

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2020.1 HF2 behoben sind.

Als Referenz dienen EI-Nummern, sofern vorhanden.

Referenz	DriveLock Pre-Boot-Authentifizierung
	Ein Problem wurde behoben, bei dem der Benutzer in bestimmten Situationen nach der Anmeldung an der DriveLock PBA aufgefordert wurde, einen BitLocker Recovery Key einzugeben.

4.4.4 Fehlerbehebungen 2020.1 HF3

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2020.1 HF3 behoben sind.

Als Referenz dienen EI-Nummern, sofern vorhanden.

Referenz	DriveLock Agent
EI-1147	Verbesserte Zugriffszeit auf Netzwerkfreigaben, wenn keine detaillierten Informationen benötigt werden.
EI-1123	Fehler bei der Verwendung der Agenten-Fernkontrolle behoben, der bei Novell eDirectory auftrat.
EI-1084	Nach dem Abrufen des Wiederherstellungsschlüssels war es möglich, dass dieser nach dem Reboot nicht ausgetauscht wurde. Sofern die Eingabe eines Kennworts nötig war, wurde auch der Kennwortdialog nicht angezeigt.
EI-1117, EI-1145	Der Dateisystemfilter hat zu viel blockiert.

Referenz	Application Control
EI-1124	Die Option **Vertrauenswürdiger Prozess (diese Anwendung sowie alle von ihr gestarteten Anwendungen ("Child-Prozesse") werden zugelassen)** war ausgegraut. Sie ist jetzt wieder verfügbar in der Standard Applikationskontrolle ohne Predictive Whitelisting.

Referenz	BitLocker Management
EI-1100	Wenn ein Computer mit aktivierter Fast Startup-Option in Windows 10 nur heruntergefahren wurde, konnten Datenpartitionen nach dem erneuten Booten nicht mehr automatisch von BitLocker Management entsperrt werden.
	Für BitLocker-verschlüsselte Computer ohne TPM ist das nachträgliche Ändern des Kennworts für das Systemlaufwerk fehlgeschlagen.

Referenz	Device Control
EI-1118	Der Dateisystem-Filtertreiber wurde geändert, um das Blockieren von Geräten zu verhindern.
EI-1155	Die Erkennung von CD/DVD-Brennern wurde erweitert.
EI-1121	Der Mandantenname der Richtlinie wird jetzt mitgeschickt, damit beim Lesen von Geräteinformationen vom Remote-Client kein Fehler auftritt.

Referenz	Encryption 2-Go
EI-1107	Der Dateisystem-Filtertreiber wurde geändert, um das Blockieren von Geräten zu verhindern.

Referenz	DriveLock Enterprise Service (DES)
EI-1095	Das Kennwort für den DES Benutzer kann jetzt einen Strichpunkt enthalten. Vorher haben solche Kennwörter zum Abbruch des DES-Setups geführt.
EI-1136	Fehler beim Start des DriveLock Enterprise Service behoben, wenn eine große Anzahl noch nicht verarbeiteter Ereignisse in der Datenbank existieren.
	Beim DES-Setup wurde eine fehlerhafte Protokolldatei geschrieben.

Referenz	File Protection
EI-1051, EI-1064	Wenn eine Änderung in der Ladereihenfolge der Dateisystemfilter festgestellt wird, die sich auf den DriveLock File Encryption-Treiber auswirkt, wird diese Änderung jetzt korrigiert und die Dateiverschlüsselung fordert einen Neustart an.

Referenz	DriveLock Management Konsole (DMC)
EI-1139	Bei Whitelist-Regeln wurden die Kommentare für die erlaubten Seriennummern nicht korrekt in der Richtlinie abgespeichert und somit nach erneutem Öffnen der Richtlinie nicht mehr angezeigt.

Referenz	Microsoft Defender
EI-1114	Die Einstellungen für Microsoft Defender konnten nicht mehr konfiguriert werden, sie blieben immer auf "Nicht konfiguriert".

Referenz	Netzwerk-Pre-Boot-Authentifizierung
EI-1134	Eine Netzwerk-PBA-Anmeldung war in der Zeit von 18:12h bis 24:00h (UTC) nicht möglich. Ein dafür benötigter Zeitstempel wurde falsch berechnet.

Referenz	SB-Freigabe
	Nicht-Standard-ASCII-Zeichen können bei der Angabe eines Grundes für die Selbstbedienung wieder verwendet werden

4.5 Version 2019.2

4.5.1 Fehlerbehebungen 2019.2

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2019.2 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.

Referenz	BitLocker Management
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

Referenz	Disk Protection
	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.
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.

Referenz	File Protection
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.

Referenz	Management Konsole (DMC)
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.

4.5.2 Fehlerbehebungen 2019.2 HF1

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2019.2 HF1 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.

4.5.3 Fehlerbehebungen 2019.2 SP1

Wichtige Fehlerkorrekturen in dieser Version

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2019.2 SP1 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.

Referenz	File Protection
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 Checkbox) wenn der Benutzer über RDP mit dem Rechner ver-

Referenz	SB-Freigabe
	bunden ist.

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

4.5.4 Fehlerbehebungen 2019.2 HF3

Wichtige Fehlerkorrekturen in dieser Version

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2019.2 HF3 behoben sind.

Als Referenz dienen EI-Nummern, sofern vorhanden.

Referenz	Device Control
EI-540	Die Erkennung von Brenngeräten und Einstellung korrekter Zugriffsrechte auf das Laufwerk wurden verbessert.
EI-1028	Das Netzlaufwerk wird auf Terminal-Servern nicht mehr mit der angewandten Whitelist-Regel gesperrt: 0000000000-C0D0-C0D0-0001-000000000000000A
EI-1070	Bei bestimmten Konfigurationen konnte in einem Zeitraum von Millisekunden nach dem Verbinden eines Laufwerks mittels eines Skripts darauf zugegriffen werden. Dieser Fehler ist behoben.

Referenz	DriveLock Control Center (DCC)
EI-1055	Für Benutzer konfigurierte OU-Filter funktionieren jetzt auch für Ereignis-Reports.

Referenz	File Protection
EI-1053	Der Menüeintrag "[DriveLock File Protection]" konnte über das Taskleistensymbol des DriveLock Agenten nicht deaktiviert werden. Dies ist jetzt möglich.

Referenz	DriveLock Pre-Boot-Authentifizierung
	Ein Problem wurde behoben, bei dem der Benutzer in bestimmten Situationen nach der Anmeldung an der DriveLock PBA aufgefordert wurde, einen BitLocker Recovery Key einzugeben.

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 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 Bekannte Einschränkungen des Agenten

Update/Installation/Deinstallation des Agenten unter Windows 7 x64

Nach einem Update, einer Installation oder Deinstallation des DriveLock Agenten unter Windows 7 x64 stürzt der Explorer (explorer.exe) ab. Dies tritt nur unter bestimmten Umständen auf, wenn die Windows-Eingabeaufforderung mit Admin-Rechten geöffnet und das System seit dem Update/Installation/Deinstallation des Agenten nicht neu gestartet wurde.

5.3 DriveLock Enterprise Service (DES)

Das DES-Setup kann fehlschlagen, wenn Zertifikate verwendet werden, die mit OpenSSL erstellt wurden.

5.4 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).

5.5 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.

5.6 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.

5.7 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).

Kurzfristig gesperrte Dateien

Wenn ein Dateifilter konfiguriert ist und der Zugriff für bestimmte Benutzer oder Gruppen erlaubt ist, können Dateien auf dem USB-Stick während der Konfigurationsaktualisierung für kurze Zeit gesperrt sein.

5.8 DriveLock Disk Protection

Windows Inplace Upgrade

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, damit nach dem Upgrade 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 seit Version 2019.2 verfügbare PBA steht nur für Windows 10 Systeme zur Verfügung, da die für die Festplattenverschlüsselungskomponenten benötigten Treibersignaturen von Microsoft nur für dieses Betriebssystem gelten.
- Mit der PBA für den UEFI-Modus können unter Umständen Probleme bei PS/2 Eingabegeräten (z.B. eingebauten Tastaturen) auftreten.
- 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 Keyboard-Treiber dauerhaft zu 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.
  Mit Einführung des Kombi-Treibers ab Version 2020.1 wird das Problem auf einigen Systemen gelöst (u.a. VM Ware Workstation 15).
  Weitere Informationen zu Abkürzungs- und Funktionstasten finden Sie im entsprechenden Kapitel in der BitLocker Management Dokumentation auf DriveLock Online Help.

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 Position 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.

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.

5.9 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.

Zeitliches Problem mit Office-Dateien

- Office-Dateien, die größer als 8 MB sind, werden beschädigt, wenn sie direkt nach dem Kopieren von einer FFE-Netzwerkfreigabe mit und ohne Laufwerkszuordnung und DFS geöffnet werden. Wir empfehlen eine Wartezeit von 20-30 Sekunden, je nach Größe der Dateien. (Referenz EI-1469)

5.10 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 Problemen kommen, wenn das UEFI-BIOS nicht die benötigten Netzwerkverbindungen unterstützt. Dies ist konkret bei folgenden Systemen der Fall:
  - Fujitsu LifeBook E459. (Referenz: EI-1303)
  - Fujitsu LifeBook U772

- Acer Spin SP11-33
- Acer Spin SP513-53N
- Dell Inspirion 7347

- Bei einigen DELL-Geräten weicht die Implementierung der Zeitzählung vom Standard ab und kann zu einer längeren Zeitspanne als erwartet führen. Dieses hardwarebedingte Problem können wir leider nicht programmatisch lösen. (Referenz: EI-1668)
- DriveLock verwendet standardmäßig einen eigenen UEFI-Treiber für Tastaturen (entweder einen einfachen oder einen Kombi-Treiber mit Mausunterstützung), um auch innerhalb der PBA internationale Tastaturlayouts anzubieten. Dieser wird mit Hilfe einer UEFI-Standard Schnittstelle geladen. Bei manchen Modellen ist diese im UEFI-Standard vorgegebene Schnittstelle nicht korrekt oder gar nicht implementiert. Für diesen Fall kann das Laden des DriveLock Treibers deaktiviert werden, entweder über den Kommandozeilenbefehl “dlsetpb /KD-” oder seit DriveLock 2021.2 über eine Einstellung innerhalb der Richtlinie.
  In diesem Fall wird der vom Hersteller implementierte Standardtreiber verwendet, welcher in der Regel nur ein englisches Tastaturlayout unterstützt.
- Wenn Sie zu einem bereits verschlüsselten System weitere unverschlüsselte Festplatten hinzufügen, müssen die neuen Festplatten immer nach den bereits existierenden Festplatten angesprochen werden, um zu vermeiden, dass Zugriffsprobleme auf das EFS auftreten oder die Synchronisation der Benutzer fehlschlägt. (Referenz: EI-1762)

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

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

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 Kennwörtern

DriveLock BitLocker Management vereinfacht die missverständliche Unterscheidung zwischen PINs, Passphrases und Kennwörtern, indem nur noch der Begriff "Kennwort" verwendet wird. Gleichzeitig wird ein solches Kennwort 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 Kennwort 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 Kennwortes 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 Kennwort)" gewählt haben, da BitLocker bei diesen erweiterten Laufwerken die Eingabe eines Kennwortes (BitLocker Sprachgebrauch: Passphrase) erwartet.

Gruppenrichtlinienkonfiguration

Aufgrund einer technischen Einschränkung können keine computer-spezifischen Kennwörter 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.

Wechsel von Disk Protection zu BitLocker Management

Disk Protection muss mittels entsprechender Richtlinieneinstellung entfernt werden, bevor BitLocker Management einsetzbar ist.

Verschlüsselung mit BitLocker To Go

Nach der Verschlüsselung eines USB-Sticks mit administrativen Kennwort wurde dieser nicht verbunden. Um das Problem zu lösen, muss der USB-Stick zuerst entfernt und dann wieder eingesteckt werden.

5.14 DriveLock Operations Center (DOC)

Alte Versionen der DOC.exe werden nicht mehr unterstützt

Wenn Sie auf Version 2021.2 aktualisieren, empfehlen wir eine aktive Deinstallation alter DOC.exe Versionen. Diese alten Versionen funktionieren nicht mehr mit einem aktualisierten DES und werden daher nicht mehr unterstützt.

Versionskonflikt beim Aufrufen des RSoP

Wenn auf einem DriveLock Agenten Version 2021.2 installiert ist, wird für die korrekte Anzeige des RSoPs auch mindestens Version 2021.2 für die DriveLock Management Konsole (DMC) benötigt.

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.

Export von Listen zu Excel

Die mögliche zu exportierende Anzahl von Listen ist abhängig von den verfügbaren Ressourcen. Es wird empfohlen, die Filter so zu setzen, dass nicht mehr als 20.000 Einträge exportiert werden. Bei einer höheren Anzahl von Einträgen kann es vorkommen, dass die Aktion abgebrochen wird oder die exportierte Liste leer bleibt. (EI-1379)

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 eine aktuellere Version als 2019.1 automatisch vom DES gelöscht werden.

5.16 DriveLock und Thin Clients

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

- 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.
- Die Option "Unbenutzten Speicher auf dem verschlüsselten Medium auffüllen" funk-

tioniert bei der Verschlüsselung eines DriveLock Containers über einen Thin Client nicht zuverlässig.

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 - kein Support mehr
2019.2	Mai 2022
2020.1	Dezember 2021
2020.2	Mai 2023
2021.1	November 2022
2021.2	Mai 2024

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 Fehler und kritische Probleme 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

Wenn Sie sich DriveLock im Detail ansehen und das Produkt testen wollen, können Sie über die DriveLock Webseite eine Teststellung beantragen. Folgen Sie hierzu einfach den Links auf unserer Webseite https://www.drivelock.de/.

Wir stellen Ihnen einen cloudbasierten Mandanten zur Verfügung. Somit können Sie sich vollständig auf den DriveLock Agenten und die Schutzfunktionalität von DriveLock konzentrieren.

Nachdem Sie sich für einen Test registriert haben, schicken wir Ihnen verschiedene Emails mit Informationen zur Unterstützung Ihres Tests. Eine Zusammenfassung hierzu finden Sie auf https://www.drivelock.de/cloud-testversion-information.

Sollten Sie weitere Informationen und Unterstützung bei Ihren Tests benötigen, wenden Sie sich bitte an info@drivelock.com / sales@drivelock.com.

Copyright

Die in diesen Unterlagen enthaltenen Angaben und Daten, einschließlich URLs und anderen Verweisen auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, Organisationen, Produkte, Personen und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Personen oder Ereignissen ist rein zufällig. Die Verantwortung für die Beachtung aller geltenden Urheberrechte liegt allein beim Benutzer. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der DriveLock SE kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht. Es ist möglich, dass DriveLock SE Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von DriveLock SE eingeräumt. Weitere in diesem Dokument aufgeführte tatsächliche Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

© 2021 DriveLock SE. Alle Rechte vorbehalten.