DriveLock

Release Notes 2020.1 HF3

DriveLock SE 2020

Inhaltsverzeichnis

1 Release Notes 2020.1 HF3

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

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

1.1 Konventionen

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

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

> Hinweis: Hinweise und Tipps enthalten nützliche Zusatzinformationen.

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

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

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

1.2 Verfügbare Dokumentation

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

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

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

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

- **DriveLock Installationshandbuch**
  Dieses Dokument beschreibt die verfügbaren Installationspakete und verschiedenen Installationsschritte der einzelnen Komponenten. Es ist das erste Dokument nach den Release Notes, welches Sie bei einer Neuinstallation lesen sollten.
- **DriveLock Administrationshandbuch**
  Das Administrationshandbuch beschreibt die Architektur von DriveLock, die verschiedenen Komponenten und dokumentiert die komplette Administration von DriveLock über die DriveLock Management Konsole (DMC). Dieses Dokument ist für Administratoren von DriveLock gedacht, die sich mit allen einzelnen Funktionen vertraut machen möchten.
- **DriveLock Control Center Benutzerhandbuch**
  In diesem Handbuch wird die Konfiguration und Verwendung des DriveLock Control Centers (DCC) beschrieben. Dieses Handbuch ist für Administratoren und für Anwender gedacht, die das DriveLock Control Center verwenden.
  In diesem Handbuch finden Sie auch eine Kurzeinführung in das **DriveLock Operations Center**.
- **DriveLock Benutzerhandbuch**
  Das DriveLock Benutzerhandbuch beinhaltet die Dokumentation aller Funktionen, die für den Endanwender zur Verfügung stehen (Temporäre Freigabe, Verschlüsselung und private Netzwerkprofile). Das Benutzerhandbuch dient Endanwendern zur Orientierung bei den für sie zur Verfügung stehenden Möglichkeiten.
- **DriveLock Ereignisse**
  Diese Dokumentation enthält eine Auflistung aller aktuellen DriveLock Ereignisse mit Beschreibung.
- **DriveLock Security Awareness**
  Dieses Handbuch beschreibt die neuen Security Awareness Funktionen, welche auch die Basis des Produktes DriveLock Smart SecurityEducation bilden.
- **DriveLock Linux**
  Dieses Handbuch beschreibt die Installation und Konfiguration des DriveLock Agenten auf Linux-Betriebssystemen.

- **DriveLock BitLocker Management**

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

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

- **DriveLock Application Control**

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

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

- **Vulnerabilty Scan**

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

2 Update von DriveLock

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

2.1 Update des DriveLock Agenten

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

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

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

2.2 Update der DriveLock Komponenten

Generelle Informationen zum Update auf die aktuelle Version

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

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

Wichtige Information zu Zertifikaten

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

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

Update der Disk Protection

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

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

3 Systemvoraussetzungen

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

3.1 DriveLock Agent

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

Hauptspeicher:

- mind. 4 GB RAM

Freier Festplattenspeicherplatz:

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

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

Benötigte Windows-Komponenten:

- .NET Framework 4.5.2 oder neuer (Für Security Awareness Kampagnen allgemein)
- KB3140245 muss auf Windows 7 installiert sein
  Weitere Informationen dazu finden Sie hier und hier.
  Ohne dieses Update kann WinHTTP keine TLS Einstellungen ändern und der Fehler 12175 erscheint in dlwsconsumer.log und DLUpdSvx.log.
- KB3033929 (SHA-2 code signing support) muss auf Windows 7 64-bit installiert sein.

Unterstützte Plattformen:

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

OS-Version	2020.1	2019.2	2019.1	7.9.6
Windows 10 Pro				
Windows 10-2004	+	+	-	-
Windows 10-1909	+	+	+	-
Windows 10-1903	+	+	+	-
Windows 10-1809	+	+	+	+
Windows 10-1803	-	+	+	+
Windows 10-1709	-	-	+	+
Windows 10-1703	-	-	+	+
Windows 10-1607	-	-	+	+
Windows 10 Enterprise				
Windows 10-2004	+	+	-	-
Windows 10-1909	+	+	+	-
Windows 10-1903	+	+	+	-

OS-Version	2020.1	2019.2	2019.1	7.9.6
Windows 10-1809	+	+	+	+
Windows 10-1709	+	+	+	+
Windows 10-1703	-	-	+	+
Windows 10-1607	-	-	+	+
Windows 10 Enterprise LTSB/LTSC				
Windows 10 Enterprise 2019 LTSC	+	+	+	+
Windows 10 Enterprise 2016 LTSB	+	+	+	+
Windows 10 Enterprise 2015 LTSB	+	+	+	+
Windows Server				
Windows Server 2019	+	+	+	+
Windows Server 2016	+	+	+	+
Windows Server 2012 R2	+(*)	+	+	+

OS-Version	2020.1	2019.2	2019.1	7.9.6
Windows Server 2012	-	+	+	+
Windows Server 2008 R2 SP1	-	+	+	+
Windows Server 2008 SP2	-	+	+	+
Ältere Windows Versionen				
Windows 8.1	+	+	+	+
Windows 7 SP1	+	+	+	+
Windows XP	Support Lizenz not-wendig	Support Lizenz not-wendig	Support Lizenz not-wendig	Support Lizenz not-wendig
Linux Derivate (eigene DriveLock Lizenz)				
CentOS Linux 8	+	+	-	-
Debian 7	+	+	-	-
Fedora 31	+	+	-	-
IGEL OS ab Version 10	+	+	-	-

OS-Version	2020.1	2019.2	2019.1	7.9.6
Red Hat Enterprise Linux 5	+	+	-	-
SUSE 15.1	+	+	-	-
Ubuntu 19.10	+	+	-	-

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

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

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

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

Einschränkungen

- DriveLock Disk Protection ist nur für den Betrieb unter XP, welches in bestimmten Geldautomaten verwendet wird, freigegeben.
- Windows XP Embedded: Der DriveLock Virtual Channel und der DriveLock Agent dürfen nicht auf dem gleichen Client installiert sein.
- BitLocker Management wird auf Windows 7 Systemen mit TPM und nur für 64-Bit unterstützt.
- Disk Protection UEFI und GPT Partitioning ist unterstützt für Festplatten bis max. 2 TB für Windows 8.1 64-Bit oder neuer und UEFI Version V2.3.1 oder neuer.
- DriveLock Disk Protection ist für Windows 10 ab Version 1703 freigegeben (siehe Bekannte Einschränkungen).
- Der Agenten-Status ist ab Version 2019.2 ein separater Optionseintrag und muss explizit konfiguriert werden. Die Standardeinstellung ist, keinen Status anzuzeigen.

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

Citrix Umgebungen

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

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

3.2 DriveLock Management Console und Control Center

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

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

Hauptspeicher:

- mind. 4 GB RAM

Freier Festplattenspeicherplatz:

- ca. 350 MB

Benötigte zusätzliche Windowskomponenten:

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

Unterstützte Plattformen:

Die beiden DriveLock 2020.1 Management Konsolen wurden getestet und freigegeben auf den aktuellsten Ständen der Windows Versionen, die zum Zeitpunkt des Release offiziell verfügbar waren und die bei Microsoft das Ende des Service-Zeitraumes noch nicht erreicht

haben. Im Kapitel DriveLock Agent finden Sie eine Auflistung der Windows Versionen, die DriveLock unterstützt.

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

3.3 DriveLock Enterprise Service

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

Hauptspeicher / CPU:

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

Freier Festplattenspeicherplatz:

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

Benötigte zusätzliche Windowskomponenten:

- .NET Framework 4.5.2 oder höher

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

Benötigte DriveLock API Services Ports (DOC/MQTT):

- 18082 und 18083: Diese beiden Ports sollten nicht durch andere Server-Dienste belegt werden, sie müssen jedoch nicht von außen erreichbar sein (nur intern)
- 8883: Die Agenten verbinden sich auf diesen Port mit dem DES, um per Agentenfernsteuerung erreichbar zu sein. Die Freigabe in der lokalen Firewall des Rechners erfolgt automatisch durch das DES-Installationsprogramm.

Unterstützte Plattformen:

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

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

- Windows Server 2016 64-Bit
- Windows Server 2019 64-Bit

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

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

Unterstützte Datenbanken:

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

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

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

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

3.4 DriveLock Operations Center Applikation

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

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

Hauptspeicher:

- mind. 4 GB RAM

Freier Festplattenspeicherplatz:

- ca. 250 MB

Benötigte zusätzliche Windowskomponenten:

- .NET Framework 4.5.2 oder höher

Unterstützte Plattformen:

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

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

4 Versionshistorie

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

4.1 Version 2020.1 HF3

DriveLock 2020.1 HF3 ist ein Maintenance Release.

4.1.1 Fehlerbehebungen

Wichtige Fehlerkorrekturen in dieser Version

Dieses Kapitel enthält Informationen zu Fehlern, die mit der vorliegenden DriveLock Version 2020.1 HF3 nun 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**

Referenz	Application Control
	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 Passwort für den DES Benutzer kann jetzt einen Strichpunkt enthalten. Vorher haben solche Passwörter 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 Console
EI-1139	Bei Whitelist-Regeln wurden die Kommentare für die erlaubten

Referenz	DriveLock Management Console
	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

4.2 Version 2020.1 HF2

DriveLock 2020.1 HF2 ist ein Maintenance Release.

4.2.1 Fehlerbehebungen

Wichtige Fehlerkorrekturen in dieser Version

Dieses Kapitel enthält Informationen zu Fehlern, die mit der vorliegenden DriveLock Version 2020.1 HF2 nun 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.

4.3 Version 2020.1 HF1

DriveLock 2020.1 HF1 ist ein Maintenance Release.

4.3.1 Wichtige Update-Information

Inventarisierung

Die Inventarisierung ist ab Version 2020.1 HF1 unabhängig vom Lizenztyp im Produkt vorhanden und kann über die Richtlinieneinstellung **Inventarisierung und Schwachstellenscan** aktiviert werden. Da diese Funktionalität unter Umständen den Datenverkehr erhöht, kann der Zeitraum für das Sammeln von Inventarisierungsdaten eingegrenzt werden.

Schwachstellenscan

- Der Schwachstellenscan kann nur mit einer Installation der Version 2020.1 HF1 vollumfänglich eingesetzt werden. Diese Version muss auch auf DriveLock Agenten installiert sein.
- Für den Schwachstellenscan wird Windows ab Version 8.1 vorausgesetzt.

4.3.2 Fehlerbehebungen

Wichtige Fehlerkorrekturen in dieser Version

Dieses Kapitel enthält Informationen zu Fehlern, die mit der vorliegenden DriveLock Version 2020.1 HF1 nun 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 Console
	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 "Benutzersynchronisation" 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 Version 2020.1

DriveLock 2020.1 ist ein Feature Release.

4.4.1 Neue Funktionen und Verbesserungen

Die Version 2020.1 enthält eine Vielzahl an neuen Funktionalitäten und Verbesserungen.

- Neu: DriveLock Schwachstellen-Scan (ab Version 2020.1 HF1)
- Neu: Netzwerkfähigkeit der DriveLock Pre-Boot Authentifizierung inklusive direktem Login am Active Directory
- Neu: Self-Service Portal für Anwender, die Zugangsdaten zum Anmelden an der PBA vergessen haben
- Neu: Die komplette Verwaltung von Microsoft's Defender Antivirus ist in DriveLock integriert
- Das DriveLock Operations Center bietet zahlreiche neue Ansichten, Reports und Verwaltungsfunktionen
- Zusätzliche Schutzfunktionen und automatische Konfigurationsmöglichkeiten in DriveLock's Applikationskontrolle mit automatischem Lernen von Anwendungsverhalten

Der folgende Abschnitt bieten Ihnen einen ersten Überblick über die Neuerungen.

Microsoft Defender Management

Mit Microsoft Defender Antivirus lassen sich nicht nur Einstellungen rund um den Schutz vor Schadsoftware tätigen, sondern auch einige weitergehende Optionen zur Ausführung von Programmen. Durch die Integration in DriveLock wird für diese Konfiguration nur noch die DriveLock Management Konsole benötigt, mit der sich das Ganze nicht nur viel einfacher umsetzen, sondern auch leichter mit den um einiges umfangreicheren Sicherheitsfunktionen der DriveLock Applikationskontrolle abstimmen lässt. In Kombination mit der DriveLock Schnittstellenkontrolle ist die Freigabe von externen Laufwerken für Benutzer an das Ergebnis eines detaillierten Scans gebunden: Entdeckt Microsoft Defender Antivirus Schadsoftware, erfolgt keine Freigabe. Weitere Automatisierungen sind in Verbindung mit DriveLock Endpoint Detection and Response möglich. Erkennt Microsoft Defender Antivirus eine Bedrohung, so kann zum Beispiel der Rechner per Skript heruntergefahren werden oder es wird automatisch eine DriveLock Sicherheitskampagne mit den nächsten Schritten angezeigt.

Eine der neuen Ansichten im DOC umfasst auch Microsoft Defender Antivirus Statusberichte über aktuelle Bedrohungen und den Zustand der Clients. Zusammen mit der überarbeiteten Oberfläche, neuen Filterfunktionen, der grafischen Darstellung der Sicherheitslage und dem

erweiterten Navigationsbereich im DOC erhalten Administratoren einen besseren Überblick über die Bedrohungen in ihrem Unternehmen. Gefundene Bedrohungen lassen sich genauer analysieren und bei Bedarf kann der Nutzer die Benachrichtigung bei Falschmeldungen oder irrelevanten Meldungen unterdrücken. Damit werden Administratoren nicht mit irrelevanten Meldungen abgelenkt und können sich auf andere Aufgaben konzentrieren.

Vulnerability Scan

> Achtung: Voraussetzung für den Einsatz des Schwachstellen-Scans ist eine Installation der Version 2020.1 HF1 (auch für den DriveLock Agenten).

Der neue Schwachstellen-Scan sucht auf einem Computersystem automatisiert und regelmäßig nach bisher bekannten Windows-Schwachstellen. Dabei greifen wir auf eine mehrmals täglich aktualisierte Datenbank zurück. Die gefundenen Ergebnisse werden dann im DriveLock Operations Center (DOC) in einer eigenen neuen Ansicht und mit Bewertung des Risikos und der Auswirkungen angezeigt, einschließlich fehlender Patches, veralteter Softwareprogramme oder Bibliotheken mit bekannten Schwachstellen. Dadurch können Security-Teams das Sicherheitsniveau im Unternehmen genauer einschätzen und auf Basis der Bewertungen automatische Benachrichtigungen einstellen.

DriveLock Operations Center

Nach dem Start des DriveLock Operations Center fällt einem gleich die überarbeitete Oberfläche und der erweiterte Navigationsbereich auf. Die Verwendung wurde noch einfacher und intuitiver gestaltet, damit die Anwender die Aufgaben unkompliziert und schnell erledigen können.

Informationen über einzelne Computer können nun übersichtlich auf einer einzigen groß dargestellten Seite angezeigt werden. Auch die einzelnen Ansichten lassen sich für jeden Anwender einrichten. Diese Grafiken ermöglichen gleichzeitig auch ein intuitives Filtern und Drill-Down zu den wichtigen Daten.

Ein erweitertes, rollen-basiertes Berechtigungsmodell lässt ein genau an die Organisationsstruktur angepasstes Sicherheitskonzept zu. Das Besondere: Welche Daten ein Benutzer innerhalb des DOC sieht, kann ebenfalls konfiguriert werden. So sehen Nutzer mit verschiedenen Rollen nur die Computer und die damit verbundenen Daten aus ihrem Zuständigkeitsbereich.

Netzwerk-fähige Pre-Boot-Authentifizierung (PBA)

Mit der Netzwerk-Pre-Boot Authentifizierung können DriveLock Kunden erstmals völlig neue Anwendungsszenarien umsetzen. Benutzer melden sich nun direkt und ohne vorherige Synchronisation am Active Directory an, sofern der Rechner direkt mit dem Firmennetzwerk verbunden ist. Gerade bei Mehr-Benutzer Laptops entfällt die bisher notwendige Provisionierung. Im Notfall kann sich auch ein anderer Benutzer an einem verschlüsselten Rechner anmelden. „Wake-On-LAN" mit automatischer Softwareverteilung im Unternehmen wird so zusammen mit der DriveLock Festplattenverschlüsselung einfach gelöst und erlaubt, auch stationäre Systeme leicht und effizient gegen Diebstahl zu schützen.

Web-basiertes Self-Service Portal

Ebenfalls neu ist das DriveLock Self-Service Portal für Endanwender. Der Benutzer kann rund um die Uhr über einen normalen Browser, der auch in allen Smartphones zur Verfügung steht, das Self-Service Portal aufrufen. Mit der richtigen Beantwortung von drei zuvor eingerichteten Fragen und einer zusätzlichen TAN identifiziert er sich hier auch ohne Passwort.

Applikationskontrolle

Mit der Verbesserung der Applikationskontrolle zielt DriveLock darauf ab, Administratoren den Arbeitsalltag zu erleichtern. So ist bei der Konfiguration nun nicht mehr so viel Wissen über das Verhalten einzelner Anwendungen nötig. Beispielsweise, welche Bibliotheken diese aufrufen oder in welche Verzeichnisse Daten geschrieben werden. All das übernimmt DriveLock, indem es das Verhalten der Anwendung durch temporäres Monitoring lernt. Dabei wird die zuvor festgelegte Anwendung oder der definierte Ordner über einen Zeitraum automatisch daraufhin überwacht, welche Aktionen die Applikation ausführt. Der Administrator erstellt dann aus diesen Daten passende Anwendungsregeln für die Whitelist. Untypisches Verhalten wird dadurch sofort unterbunden und Benutzer können bestehende Sicherheitsmaßnahmen nicht umgehen. Zudem können Benutzer genau dann, wenn eine Anwendung etwas Unerwartetes macht, entsprechend darauf hingewiesen werden. Das reicht von einfachen Meldungen bis hin zum Start einer Security Awareness Kampagne. Das schafft nicht nur Transparenz, sondern sorgt kontinuierlich und nachhaltig dafür, dass Anwender sich sicherheitsbewusster verhalten und dabei laufend dazulernen.

Zusätzliche Verbesserungen in dieser DriveLock Version

- Bei den Security Awareness Kampagnen wurde die Zuordnung zum Benutzer optimiert, damit bereits abgespielte Kampagnen nicht wiederholt werden auch wenn der Benutzer den Rechner wechselt

- Im DOC können Kunden auch die aktuellen Statusmeldungen unserer Festplattenverschlüsselung Disk Protection einsehen die Notfallanmeldung für einzelne Computer direkt aus der Computeransicht heraus starten.
- In der DriveLock Management Konsole wurden die beiden Ansichten zu den aktuell verfügbaren DriveLock MSI-Paketen zu einer einzigen zusammengeführt.
- Eine Policy-Zuweisung zu einer Computergruppe kann nun deaktiviert werden, es ist nicht mehr notwendig die Zuweisung zu löschen.
- Das gleiche gilt auch für Laufwerks-Whitelistregeln, die nun einfach aktiviert oder deaktiviert werden können.
- Für BitLocker To Go gibt es zusätzliche Optionen, die die Sichtbarkeit von BitLocker To Go Startmenü-, Kontextmenü- oder Trayicon-Menü-Einträge für Benutzer festlegen
- Für die Problembehebung kann man die Verschlüsselungseinstellungen von BitLocker für einzelne Computer temporär deaktivieren oder anpassen.
- Sowohl die Management Konsole als auch das Control Center können DriveLock Benutzerkonten aus dem DOC für Berechtigungen verwenden
- Das Layout und das Startverhalten der DriveLock PBA wurde optimiert und ein verbesserter Treiber für Keyboard und Maus-Unterstützung implementiert.

4.4.2 Fehlerbehebungen

Wichtige Fehlerkorrekturen in dieser Version

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

Referenz	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 (Passwort-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 erhöhter Last am DES Rechner führte, wurde behoben.

Referenz	DriveLock Enterprise Service (DES)
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 Child-domänen 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 "Fest-plattenverschlüsselungsstatus" gruppiert werden.

Referenz	Encryption-2-Go
EI-506	DriveLock Mobile Encryption (Encryption-2-Go und File Pro-tection) kann jetzt auf Apple OS X und Mac OS X ohne Ein-schränkungen verwendet werden.

Referenz	Encryption-2-Go
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.
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

Referenz	File Protection
	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.
EI-827	Beim Hinzufügen neuer Lizenzen in der Management Konsole wurden neu hinzugekommene Module automatisch für sämtliche Computer aktiviert.

Referenz	Management Konsole
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.
EI-724	Beim Offline Unlock Wizard konnte man zur nächsten Seite weiter springen, auch wenn man noch keine freizugebenden Module ausgewählt hatte.

Referenz	SB-Freigabe
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.

5 Bekannte Einschränkungen

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

5.1 Lizenzierung

Lizenzaktivierung

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

5.2 DriveLock Management Konsole (DMC)

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

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

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

Wichtige Update-Information:

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

5.3 Installation der Management Komponenten über Gruppenrichtlinien

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

5.4 DriveLock Device Scanner

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

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

5.5 Manuelle Updates

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

Update von DriveLock Version 2019.1 auf 2019.2

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

5.6 Self Service Freigabe

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

5.7 DriveLock, iOS und iTunes

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

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

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

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

5.8 Universal Camera Devices

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

Diese Geräteklasse kann derzeit noch nicht mit DriveLock verwaltet werden.

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

5.9 Windows Portable Devices (WPD)

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

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

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

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

5.10 CD-ROM Laufwerke

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

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

5.11 DriveLock Disk Protection

Unterschiedliche Verschlüsselungsprodukte

- DriveLock Disk Protection kann nicht gleichzeitig mit anderen Festplattenverschlüsselungsprodukten (Fremdprodukten) eingesetzt werden. Sollte auf einem DriveLock Agenten bereits ein entsprechendes Fremdprodukt installiert sein, darf dort keine Richtlinie mit Disk Protection-Einstellungen oder -Lizenz zugewiesen werden.

Inplace Update auf Windows 10 1903

- Haben Sie vor dem Update auf eine aktuelle Windows 10 Version eine bestimmte Anzahl automatischer Logins für die PBA aktiviert (dlfdecmd ENABLEAUTOLOGON <n>), ist die automatische Anmeldung währen des Upgradeprozesses durchgehend aktiv. Da jedoch während des Vorgangs der Zähler <n> nicht aktualisiert werden kann, empfehlen wir diesen lediglich auf 1 zu setzen, so das unmittelbar nach dem Windows Inplace Upgrade die Benutzeranmeldungen in der PBA wieder erforderlich sind.
  Wenn Sie während des Updates Benutzeranmeldungen an der PBA deaktivieren möchten setzen Sie daher den Zähler auf 1, damit nach dem Update nach einem weiteren Neustart nur einmal eine automatische Anmeldung erfolgt und anschließend wieder eine Benutzeranmeldung an der PBA erfolgen muss.

Antiviren Software

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

Applikationskontrolle

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

Ruhezustand

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

UEFI-Modus

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

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

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

  Unter VMWare Workstation 15 und auch bei einigen wenigen Hardwareherstellern ergaben unsere Testergebnisse Konflikte durch Maus- und Keyboadtreiber der UEFI Firmware, so dass keine Tastatureingabe in der PBA möglich ist. In diesem Fall können Sie beim Start des Rechners mit Hilfe der Taste "k" das Laden der Drivelock-PBA-Treiber einmalig verhindern. Nach der Windows-Anmeldung auf dem Client können Sie dann in einer Administrator-Kommandozeile den Befehl `dlsetpb /disablekbddrivers` ausführen, um die Drivelock-PBA-Treiber dauerhaft deaktivieren. Bitte beachten Sie dass dadurch in der Anmeldemaske der PBA das Standardkeyboardlayout der Firmware geladen ist, was in den meisten Fällen eine EN-US Belegung hat, wodurch die Sonderzeichen abweichen können.
  Folgende Punkte sind weiterhin zu beachten:
  - DriveLock 7.6.6 und höher unterstützt UEFI Secure Boot.
  - Firmwareupdates können bewirken, dass NVRAM-Variablen des Mainboards gelöscht werden, die DriveLock benötigt. Daher empfehlen wir unbedingt, vor der Installation der DriveLock PBA / FDE die Firmware-Updates für das Mainboard /UEFI einzuspielen (auch bei neu gekauften Geräten oder bei Bugfixes)
  - 32 Bit Windows und DriveLock kann nicht auf ein 64 Bit fähiges System installiert werden. Es muss die 64 Bit Version von Windows und DriveLock eingesetzt werden.
  - Die maximale Größe einer Festplatte ist weiterhin auf maximal 2 TB beschränkt.
  - Auf manchen HP Rechnern ist Windows immer wieder an Postion 1 der UEFI Bootreihenfolge und die DriveLock PBA muss im UEFI Boot-Menü manuell ausgewählt werden. In solchen Fällen und bei Problemen muss man Fast Boot im UEFI ausschalten, damit die DriveLock PBA an Position 1 bleibt.

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

BIOS-Modus

- In sehr seltenen Fällen kann es vorkommen, dass die Standardeinstellung der DriveLock Disk Protection nicht ordnungsgemäß funktioniert und das System nicht mehr reagiert. In diesem Fall starten Sie einfach den Rechner neu, während Sie die `SHIFT-Taste` gedrückt halten, um temporär die 16-bit Pre-Boot Umgebung zu nutzen.
  Durch ein Problem in Windows 10 Version 1709 und neuer kann DriveLock Disk Protection für BIOS die richtige Festplatte nicht erkennen, wenn mehr als eine Festplatte im System verbaut ist. Deshalb ist Disk Protection für BIOS nicht für Windows 10 1709 Systeme mit mehr als einer Festplatte freigegeben. Sobald Microsoft einen Fix liefert wird diese Einschränkung aufgehoben.

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

eMMC Flash Memory

- DriveLock Disk Protection (Full Disk Encryption) unterstützt keine Speichermedien des Typs eMMC Flash Memory. (Referenz: EI-828)

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

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

3. Verschlüsseln von Laufwerk C:
   (Referenz: EI-686)

Voraussetzungen für Disk Protection:

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

Neustart nach Installation der PBA auf Toshiba PORTEGE Z930:

- 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. (Referenz: EI-751)

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

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

5.12 DriveLock File Protection

Microsoft OneDrive

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

NetApp

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

Windows 10-Clients mit Kaspersky Endpoint Security 10.3.0.6294

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

Zugriff auf verschlüsselte Ordner

- Der Zugriff auf verschlüsselte Ordner auf Laufwerken, die nicht mit Laufwerksbuchstaben sondern als Volume Mountpoint gemounted sind, wird nicht unterstützt.

eMMC Flash Memory

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

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 laufenden Dateien verloren geht.

Erstellen einer neuen Datei in einem Ordner, der zuvor gelöscht wurde

- Ein weiterer Zugriff auf einen Ordner nach einem fehlgeschlagenen Unmount kann zu unvorhersehbarem Verhalten führen. Sie sollten in diesem Fall geöffnete Dateien schließen und das Unmounten erneut versuchen
- Unmounten eines leeren verschlüsselten Ordners schlägt fehl

Entschlüsselung eines verschlüsselten Ordners

- Nachdem die Entschlüsselung eines verschlüsselten Ordners aufgrund geöffneter Dateien fehlgeschlagen ist, ist es überhaupt nicht möglich, den Ordner zu entschlüsseln, selbst nachdem die geöffneten Dateien geschlossen wurden. Um dies zu umgehen, muss der Ordner manuell unmountet werden, bevor der Entschlüsselungsassistent erneut aufgerufen wird.

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.

5.13 DriveLock Pre-Boot-Authentifizierung

Das EURO-Zeichen "€", das eine deutsche Tastatur bei der Eingabe der Kombination "Alt Gr" und "e" liefert, wird bei der Anmeldung in der DriveLock-PBA nicht erkannt.

5.14 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.

5.15 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

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

5.16 BitLocker Management

Unterschiedliche Verschlüsselungsprodukte

- DriveLock BitLocker Management kann nicht gleichzeitig mit anderen Festplattenverschlüsselungsprodukten (Fremdprodukten) eingesetzt werden. Sollte auf einem DriveLock Agenten bereits ein entsprechendes Fremdprodukt installiert sein, darf dort keine Richtlinie mit BitLocker Management-Einstellungen oder -Lizenz zugewiesen werden.

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

- Möchten Sie eine bereits vorhandenen Systemumgebung verwalten, die bereits mit BitLocker verschlüsselte Computer enthält, müssen diese seit Version 2019.1 nicht mehr zuvor über die vorhandene BitLocker Verwaltung bzw. die Gruppenrichtlinien entschlüsselt werden. DriveLock erkennt die BitLocker Verschlüsselung automatisch und

erzeugt neue Wiederherstellungsinformationen. Eine automatische Ent- und Verschlüsselung wird nur dann durchgeführt, wenn der in der DriveLock Richtlinie konfigurierte Verschlüsselungsalgorithmus sich vom derzeitigen Algorithmus unterscheidet. Anschließend ist eine Verwaltung durch DriveLock BitLocker Management möglich und eine sichere Speicherung und Verwendung der Wiederherstellungsinformationen gewährleistet.

Verwendung von Passwörtern

- DriveLock BitLocker Management vereinfacht die missverständliche Unterscheidung zwischen PINs, Passphrases und Passwörtern, indem nur noch der Begriff "Passwort" verwendet wird. Gleichzeitig wird ein solches Passwort automatisch im richtigen BitLocker Format benutzt, entweder als PIN oder als Passphrase.
  Da Microsoft jedoch unterschiedliche Anforderungen an die Komplexität von PIN und Passphrase stellt, gelten für das Passwort folgende Einschränkungen:
  - Mindestlänge: 8 Zeichen
  - Maximale Länge: 20 Zeichen

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

Verschlüsselung von erweiterten Festplatten

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

Gruppenrichtlinienkonfiguration

- Aufgrund einer technischen Einschränkung können keine computer-spezifischen Passwörter über das DriveLock Control Center gesetzt werden, wenn Sie die DriveLock BitLocker Konfiguration per Gruppenrichtlinien an die Agenten verteilt haben.
  In diesem Fall ignoriert der DriveLock Agent die dafür notwendigen maschinenspezifischen Richtlinien.

BitLocker To Go mit Windows 7

- Die Verschlüsselung eines USB-Sticks mit BitLocker To Go in Windows 7 kann über eine Stunde dauern, im Vergleich dazu dauert dies unter Windows 10 nur wenige Minuten.

5.17 DriveLock Operations Center (DOC)

Mehrfachauswahl von Rechnern in der Computer-Ansicht

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

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

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

5.18 DriveLock Security Awareness

Änderung der Inhalte für das Security Awareness Content AddOn

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

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

Security Awareness auf IGEL-Clients

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

5.19 Antivirus

Antivirus allgemein

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

Avira Antivirus

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

5.20 DriveLock und Thin Clients

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

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

5.21 DriveLock WebSecurity

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

6 End-Of-Life-Ankündigungen

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

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

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

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

Supportzyklen:

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

Wartungsupdates und Code-Korrekturen für Fehlern und kritischen Problemen werden in diesem Zeitraum veröffentlicht. Ebenfalls erfolgt die Beantwortung von Anfragen per Telefon, E-Mail und Self-Service – zur Verfügung gestellt vom DriveLock Product Support Team und den dazugehörigen Webseiten für technische Unterstützung.

Upgrades:

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

7 Testinstallation von DriveLock

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

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

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

Copyright

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.

© 2020 DriveLock SE. Alle Rechte vorbehalten.