DriveLock Release Notes

Release Notes 2024.1

DriveLock SE 2024

Inhaltsverzeichnis

1 DriveLock Release Notes 2024.1

Build: 2024.1.1

Datum: 21.06.2024

Die DriveLock Release Notes enthalten wichtige Informationen zu Fehlerbehebungen in dieser Version, sowie zu bekannten Einschränkungen. Zudem enthalten sie einen Überblick über die Systemvoraussetzungen für den Einsatz von DriveLock, sowie unsere End-Of-Life-Ankündigungen.

Eine detaillierte Beschreibung der Neuerungen, Verbesserungen und Änderungen befindet sich im Kapitel **Was ist neu?** in der DriveLock Dokumentation auf DriveLock Online Help.

Links zu den Release Notes der vergangenen und noch unterstützten Versionen finden Sie im Menü **Archiv** auf DriveLock Online Help.

Beachten Sie bitte die allgemeinen Informationen zur Aktualisierung auf neue Versionen im Kapitel **Aktualisierung von DriveLock** in der DriveLock Dokumentation auf DriveLock Online Help.. Wichtige Information für die Aktualisierung auf Version 2024.1: Beim Datenbank-Update muss mit einem erhöhten Speicherbedarf und Zeitaufwand gerechnet werden.

1.1 Neuerungen, Verbesserungen und Änderungen

Im folgenden finden Sie eine Auflistung der in 2024.1 enthaltenen Neuerungen, Verbesserungen und Änderungen.

Eine detaillierte Beschreibung finden Sie im Kapitel **Was ist neu?** in der DriveLock Online Hilfe auf DriveLock Online Help.

Neuerungen:

- Erweiterte Flexibilität im Richtlinienmanagement: Einführung der Möglichkeit, mehr als eine DOC-managed Policy sowie verschiedene Arten von Richtlinien zu verwalten, die spezifische Moduleinstellungen und Zuweisungen ermöglichen.
- Einstellungen für das Server- und Mandanten-Management im DOC: Die Einstellungen für Server und Mandanten, sowie einige globale Einstellungen, werden jetzt über das DOC verwaltet.
- Optimierte Verwaltung von Laufwerken und Geräten im DOC: Neben den Regeln können nun weitere Einstellungen für Laufwerke direkt im DOC verwaltet werden. Zudem ist es jetzt möglich, Device-Regeln und -Einstellungen für Device-Klassen im DOC zu erstellen.

- Security Awareness-Funktionen und Auswertungen: Bessere Auswertungen von Kampagnen sowie Berichterstattung für einzelner Kampagnen und zugewiesenen Gruppen bis hin zu Reports.
- macOS-Agent: Der Package Installer kann jetzt für die Softwareverteilung verwendet werden
- Mobile Encryption Application (MEA): Schreibzugriff bei exFAT-formatierten Containern für alle von DriveLock unterstützten Betriebssysteme
- Freigabe-Anforderung im DOC: Über einen neuen Kontextmenübefehl am DriveLock Agenten lässt sich jetzt die Freigabe von gesperrten Geräten und Laufwerken bequem durchführen. Im DOC können diese Freigabe-Anforderungen sofort bearbeitet werden und die freigegebenen Geräte/Laufwerke in eine entsprechende Richtlinie eingefügt werden.
- Zentral verwaltete Ordner: Möglichkeit, verschlüsselte zentrale Ordner vom Agenten aus zu erstellen und die Ordner- und Benutzerberechtigungen im DOC zentral zu verwalten
- Neues Start-Dashboard und neue Widgets im DOC: Im DOC wird jetzt automatisch nur das "HOME" Dashboard erstellt; weitere müssen manuell hinzugefügt werden. Neue Widgets und verbesserte Ansichten erleichtern die Übersicht und Visualisierung von Daten, wobei zwischen Listen- und Kartenansichten gewechselt werden kann.
- Der DriveLock Agent für IGEL OS 12 ist jetzt im IGEL App-Portal verfügbar
- Automatische Telemetrie-Datenerhebung: Zur Optimierung von DriveLock werden automatisch Telemetriedaten erhoben und an eine zentrale Datenbank gesendet. Diese Funktion ist ab dieser Version standardmäßig aktiviert, kann jedoch bei Bedarf manuell deaktiviert werden.

Verbesserungen und Änderungen:

- Änderung des Standardverhaltens bei der Aktualisierung des DriveLock Agenten
- Änderungen bei der Richtlinienkonfiguration
- Anzeige der Historie von Laufwerks- und Geräteaktivitäten im DOC
- Automatische AD-Inventarisierung
- COM- und LPT-Ports (serielle und parallele Schnittstellen) werden ab dieser Version nicht mehr standardmäßig geblockt
- Device Scanner-Funktionalität nicht mehr verfügbar

- Geräteklassen können jetzt benutzerdefiniert erstellt werden
- Gerätelisten können jetzt mehrere Geräteklassen enthalten
- Navigationsansicht im DOC jetzt manuell auswählbar
- Option zur Aufhebung der Datenmaskierung in Berichten
- Verbesserung der DriveLock MEA für macOS
- Verbesserte Performance beim Schwachstellen-Scan
- Verbesserte Zuordnung der Richtlinien-IDs
- Verhinderung der Entschlüsselung von Ordnern im alten Format, die mit File Protection verschlüsselt wurden

1.2 Fehlerbehebungen

DriveLock 2024.1 ist eine Hauptversion.

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2024.1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Achtung: Bitte beachten Sie, dass es bei bestimmten Themen durch Einspielen der Aktualisierung zu Verhaltensänderungen im Produkt kommen kann. Bitte überprüfen Sie Ihre Einstellungen, ob Ihre bestehende Umgebung hiervon betroffen ist, bevor Sie eine Aktualisierung durchführen. Diese Themen sind mit folgendem Warnsymbol gekennzeichnet ⚠

	BitLocker Management (BLM)
	Bei der Übernahme einer bestehenden BitLocker-Umgebung konnte es vorkommen, dass ein existierender Wiederherstellungsschlüssel nicht ersetzt wurde. Dadurch wurde die betreffende Partition im DOC als "BitLocker" statt als "DriveLock BitLocker" gekennzeichnet.
	Bei entsprechend konfigurierter Richtlinie wurde der Dialog zum Verzögern der Verschlüsselung auch dann angezeigt, wenn lediglich Protektoren ersetzt werden sollten.
	Bei der Übernahme einer bestehenden BitLocker-verschlüsselten Partition wurde der Wiederherstellungsschlüssel in manchen Fällen nicht zum DES hochgeladen.
	Externe Laufwerke, die bereits mit BitLocker Management verschlüsselt waren, wurden bei Zuweisung einer Entschlüsselungs-Richtlinie von BLM entschlüsselt.
	Nach der Zuweisung einer Entschlüsselungs-Richtlinie wurde eine nicht verwaltete, mit BitLocker verschlüsselte Datenpartition zwar nicht entschlüsselt, eine bestehende automatische Entsperrung wurde jedoch entfernt.

	BitLocker Management (BLM)
	Bei der Übernahme bestehender BitLocker-Umgebungen konnte es vorkommen, dass die Systempartition nicht vollständig übernommen wurde.
EI-2669	Bei Aktualisierung des DriveLock-Agenten der Version 20.2 oder älter wurde der Kennwortdialog wieder angezeigt, wenn in der Richtlinie neben der BitLocker-PBA angegeben war, dass das Kennwort vom Benutzer eingegeben werden soll und dass eine Übernahme unter Beibehaltung des bestehenden Algorithmus erfolgen soll.
EI-2647	Bei der Abfrage der BitLocker-Informationen kam es zu einem Absturz des Agenten, wenn die Laufwerksinformationen infolge eines Defekts nicht mehr korrekt gelesen werden konnten.
	Wenn sich ein Benutzer abgemeldet hat, solange der Dialog zur Eingabe eines BLM-Kennworts sichtbar war, wurde dieser bei einer erneuten Anmeldung nicht wieder angezeigt.
EI-2591	Nach dem Entschlüsseln eines Computers durch Überschreiben der Richtlinie war es nicht mehr möglich, dies zurückzunehmen, da die entsprechende Schaltfläche zum Überschreiben anschließend dauerhaft ausgegraut war.

	Defender Management
	Um mehrfach gelistete Quarantäne-Dateien mit dem gleichen Pfad voneinander unterscheiden zu können, wurde ein Zeitstempel vorangestellt.

	Defender Management
EI-2689	Der im DOC angezeigte Defender Status wurde manchmal nicht aktualisiert, obwohl der DriveLock Agent seinen Status an den DES übermittelt hat. Dieser Fehler wurde behoben.

	Device Control
EI-1630 ⚠	Einige Fehler im Zusammenhang mit Dateifilter-Vorlagen wurden behoben: • In Filtervorlagen definierte Hash-Werte für Dateiausschlüsse wurden ignoriert. Nur der Dateiname war entscheidend und das System konnte durch Umbenennung von Dateien getäuscht werden. • Die Hash-Erstellung ist auf die ersten 64k der Datei beschränkt. Ordnerausschlüsse funktionierten in einigen seltenen Fällen nicht, wenn der Name des ausgeschlossenen Ordners Teil des Namens der ausführbaren Datei war.
EI-2691	Der Fehler, der Schreibkontingente auf Leseanfragen angewendet hat, wurde behoben.
EI-1679	Der Simulationsmodus für die Datei-Filterung ist implementiert für Begrenzung der Dateigröße, Kontingent, sowie andere Einstellungen, z.B. Erweiterung(en) gesperrt/erlaubt. Wenn Quota-Einstellungen mit anderen Einstellungen kombiniert werden und eine Datei aufgrund anderer Einstellungen gesperrt ist, werden die Lese- oder Schreibzugriffe auf die gesperrte Datei nicht auf die Quota angerechnet, um die Quota-Abrechnung nicht zu verfälschen. Das Erstellen von Schattenkopien wird in dieser Weise nicht angepasst, d. h. eine im Simulationsmodus geöffnete und geschriebene Datei, die ansonsten blockiert worden wäre, wird als

	Device Control
	Schattenkopie erstellt.
EI-2324	Die Handhabung des Papierkorbs (recycle bin) beim Content Scan wurde modifiziert, um ExFat zu unterstützen.
EI-1885	Geräte-Ereignisse für USB-Controller wurden erzeugt, auch wenn die USB-Controller nicht von DriveLock kontrolliert wurden, aber einige andere Klassen (USB-Drucker, Blackberry, ...) von DriveLock kontrolliert wurden.

Referenz	Disk Protection
	Die Agenten-Fernkontrolle für Disk Protection hat einen fehlerhaften Verschlüsselungsstatus angezeigt, wenn zusätzlich BitLocker Management lizenziert war.
	Der Status, dass alle Laufwerke vollständig verschlüsselt sind, wurde manchmal zu früh gemeldet.

Referenz	DriveLock Agent
	Die Fehler, dass Screen-Reader teilweise Texte in der Benutzeroberfläche in der falschen Reihenfolge vorgelesen haben, wurden behoben.
EI-2677	Bei temporärer Freigabe eines Computers über eine bestimmte Zeitspanne wurde nach Hibernation (oder Reboot mit aktivem Fastboot) die Zeitspanne weitergeführt, auch wenn sie evtl. mitt-

Referenz	DriveLock Agent
	lerweile abgelaufen war.

Referenz	DriveLock Enterprise Service (DES)
EI-2569	Die maximale Länge des Betreffs, der von DriveLock versendeten Emails kann jetzt konfiguriert werden.
	Bei verknüpften DES werden beim ersten Dienststart nach dem Update die Zeitpläne jetzt korrekt verarbeitet.

Referenz	DriveLock Management Konsole (DMC)
EI-2716	Die DMC stürzte ab, wenn versucht wurde, Geräte über eine Remote-Verbindung zu einem Agenten in eine Computervorlage zu importieren.

Referenz	DriveLock Operations Center (DOC)
	Es ist jetzt möglich, die Spaltenbreite in der Detailansicht und der Objektansicht zu ändern.
EI-2353	Eine Anmeldung am DOC mit Benutzernamen, die Umlaute enthalten, funktioniert jetzt.
EI-2644	Das Widget "Ereignisse gruppiert nach Typ" zeigte alle Ereignisse (inklusive der Audit-Ereignisse), aber beim Drilldown wur-

Referenz	DriveLock Operations Center (DOC)
	den nur die "normalen" Ereignisse angezeigt, was dann nicht zu der zuvor gezeigten Anzahl passte. Jetzt gibt es ein separates Widget "Audit-Ereignisse gruppiert nach Typ".
EI-2694	Die API-Dokumentation wurde verbessert, so dass jetzt leichter zu erkennen ist, welche URL und Ports verwendet werden müssen.
	Im Dialog zum Löschen von Rollenzuweisungen fehlten die Checkboxen zum Auswählen der zu löschenden Rollen.

Referenz	DriveLock Pre-Boot-Authentifizierung (PBA)
EI-2638	Nach erfolgter Selbstlöschung war es möglich, dass einzelne Benutzer weiterhin in der Lage waren, sich an der DriveLock-PBA anzumelden.
EI-2577	Die Funktion 'Selbstlöschung' wurde nicht ausgeführt, obwohl der DES bereits seit mehr als den in der Richtlinie angegebenen Tagen nicht erreichbar war.
	Unmittelbar nach der Einrichtung hat die Notfallanmeldung an der PBA nicht funktioniert, wenn in der Richtlinie angegeben war, dass die Verschlüsselung erst nach erfolgreicher Anmeldung an der PBA erfolgen soll.

Referenz	File Protection (FFE)
EI-2701	Ein Blue-Screen-Fehler (BSOD), der auftrat, wenn die SID eines Benutzers nicht abgerufen werden konnte, wurde behoben.
	Der Fehler, dass ein Benutzer mit Lesezugriff auf DFS-Laufwerke schreiben konnte, wurde behoben.
	Mounten des ISO aus einem verschlüsselten Netzwerkordner funktioniert jetzt mit allen Formaten.
	In früheren Versionen führte der Abbruch der Entschlüsselung von verschlüsselten Ordnern zu einer Mischung aus unverschlüsselten und verschlüsselten Dateien und einer umbenannten Datenbankdatei in diesem Ordner. Die Datenbankdatei wird nun wiederhergestellt, und beim Mounten des Ordners wird der Zustand konsolidiert und die unverschlüsselten Dateien werden verschlüsselt, bevor Sie die Entschlüsselung erneut starten können. Achtung: Es wird weiterhin nicht empfohlen, die Ver-/Entschlüsselung von Ordnern abzubrechen.
	In einem vollständig verschlüsselten Laufwerk X: dürfen Dateien in System Ordnern, z.B. \System Volume Information, nicht verschlüsselt werden. Der Check auf unverschlüsselte Dateien berücksichtigt dies nun.
EI-2580	Wenn ein File Protection-Ordner gemountet wurde, während gleichzeitig ein leeres Smartcard-Lesegerät an den Computer angeschlossen war, konnte es vorkommen, dass der Verbindungsassistent abstürzte.

Referenz	File Protection (FFE)
	Wenn der Wiederherstellungsassistent für einen zentral verwalteten Ordner über das Tray-Symbol gestartet wurde, verhielt sich der Assistent so, als ob es sich nicht um einen zentral verwalteten Ordner handelte
EI-2665	Die Drivelock.exe erzeugte Dump-Dateien, wenn ein Fehler beim Zugriff auf ein bestimmtes Gerät auftrat (es handelte sich nicht um einen Absturz, sondern nur um die Erzeugung unnötiger Dump-Dateien).
	Es war möglich, einen zentral verwalteten Ordner ohne entsprechende Berechtigung zu entschlüsseln. Dieser Fehler ist jetzt behoben.
	Die Prüfung auf unverschlüsselte Dateien funktionierte nicht bei von OneDrive synchronisierten Dateien, die noch nicht heruntergeladen waren.
EI-2544, EI-2687	Bei installiertem File Protection traten bei Microsoft Office und im Windows Startmenü zeitweise Darstellungsprobleme auf.

Referenz	Encryption 2Go
EI-2704	Die Encryption 2Go-Wiederherstellung funktionierte nicht bei Verwendung einer Zertifikatsdatei.
EI-2589	Ein verschlüsselter Container wurde nicht automatisch formatiert, wenn nicht FAT als Dateisystem gewählt wurde. Dieser Fehler ist jetzt behoben.

Referenz	Gruppen
	Die Filterung dynamischer Gruppen auf AD-Eigenschaften funktionierte nicht.

Referenz	Security Awareness
EI-2587	Es war nicht fehlerfrei möglich, Security-Awareness-Kampagnen auf Terminal Servern in mehreren Sessions gleichzeitig auszuführen, da in allen weiteren Sessions ein veraltetes, nicht unterstütztes Browser-Plugin verwendet wurde.

1.3 Bekannte Einschränkungen

1.3.1 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
- Windows 11 Pro und Enterprise, 32/64-Bit

Vorhandene BitLocker Umgebung

Wenn Sie eine bereits vorhandene Systemumgebung verwalten wollen, 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 im Kapitel Kennwortoptionen in der aktuellen 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.

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.

1.3.2 BitLocker To Go

Verschlüsselung mit BitLocker To Go

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

Erzwungene Verschlüsselung mit BitLocker To Go

- Bei der erzwungenen Verschlüsselung (BitLocker To Go) ist der unverschlüsselte Zugriff nur bis zur nächsten Konfigurationsaktualisierung möglich.

1.3.3 Datenmaskierung

Datenmaskierung auf macOS

- Bitte beachten Sie, dass die Datenmaskierung noch nicht für den macOS-Agenten implementiert ist.

1.3.4 Device Control

Quotierung /Dateifilter-Vorlagen

- Auf dem Reiter Quotierung werden die geschriebenen bzw. gelesenen Bytes pro Zeiteinheit gezählt, nicht die eigentlichen Dateien. Daher wird die Erstellung neuer Dateien mit 0 Bytes nicht blockiert.
- Bei der Anzahl zählt jede geöffnete Datei, auch für dieselbe Datei, und Größen werden kumuliert.
- Die Lesequotierung hat Vorrang vor der Schreibquotierung, da ein Lesevorgang vor dem Schreibvorgang erforderlich ist und blockiert wird, wenn die Lesequotierung bereits überschritten ist.
- Das Verhalten der Quoten ist anwendungsspezifisch und hängt davon ab, wie eine Anwendung eine Datei für eine scheinbar einfache Lese- oder Schreibanforderung des Benutzers öffnet. Eine Datei kann zwischengespeichert oder mehrfach geöffnet oder vor der eigentlichen Lese-/Schreibverarbeitung dupliziert oder umbenannt werden, z. B. verbraucht Wordpad bei jedem Öffnen die Anzahl der Dateien um 3. Störende Prozesse, die im Namen des Benutzers handeln (AV), können das geplante Verhalten weiter verfälschen.

Dateifilter bei Archiv-Dateien

- Wenn eine im Dateifilter ausgeschlossene Datei in eine Archiv-Datei kopiert wird, wird die komplette Archiv-Datei gelöscht. Wir empfehlen, Archiv-Dateien nicht direkt auf

den kontrollierten Volumes zu bearbeiten, sondern auf der lokalen Festplatte, wo i.d.R. kein Dateifilter gesetzt ist. (Referenz EI-2651)

Lange Seriennummern

Laufwerke mit Seriennummern, die länger als 63 Zeichen sind, können nicht durch eine Whitelist-Regel mit erforderlicher Seriennummer oder einer Standardrichtlinie gesperrt bzw. entsperrt werden.

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.

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).

1.3.5 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 während 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 finden Sie im Kapitel Abkürzungs- und Funktionstasten in der DriveLock 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.

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.

1.3.6 DriveLock Enterprise Service (DES)

Registrierung von verknüpften DES

Ein verknüpfter DES kann nur dann registriert werden, wenn der Benutzer keine Multifaktor-Authentifizierung (MFA) aktiviert hat.

1.3.7 DriveLock Operations Center (DOC)

Alte Versionen der DOC.exe werden nicht mehr unterstützt

Ab Version 2021.2 ist eine manuelle Deinstallation alter DOC.exe Versionen notwendig. Diese alten Versionen funktionieren nicht mehr mit einem aktualisierten DES und werden daher nicht mehr unterstützt.

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 hat. Grund hierfür ist, dass die Gruppenmitgliedschaften für einen Benutzer aus dem Gruppen-Token gelesen werden. Diese Information werden nur in einem bestimmten Intervall aktualisiert.

Anmeldung mit Windows-Authentifizierung für Benutzer der 'Protected Users' Gruppe

- Eine Anmeldung am DOC über die Windows-Authentifizierung ist nicht möglich, wenn ein Benutzer zur Sicherheitsgruppe "Geschützte Benutzer" gehört. Eine Anmeldung über ein Kennwort funktioniert jedoch in diesem Fall.
- Eine Anmeldung am DOC über die Windows-Authentifizierung ist auch nicht möglich, wenn sich Benutzer mit einer Smartcard bei Windows angemeldet haben. Dies wird derzeit nicht unterstützt. (Referenz EI-2597)

1.3.8 DriveLock Pre-Boot-Authentifizierung

- Damit die Netzwerk-Funktionalität der DriveLock PBA zum Einsatz kommen kann, muss Hardware das TCP4 UEFI Protokoll unterstützen. Es kann daher auf manchen Systemen zu 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
- Die UEFI-Firmware von Gastsystemen in Hyper-V-Umgebungen stellt das Zertifikat "Microsoft Corporation UEFI CA 2011" nicht zur Verfügung, das für die Nutzung der DriveLock-PBA auf Hyper-V-Clients mit aktiviertem SecureBoot zwingend erforderlich ist. Daher wird die DriveLock PBA derzeit nicht auf Microsoft Hyper-V Clients unterstützt. (Referenz EI-2194)
- 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.
- 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)

- Wenn die PBA installiert ist, bietet der Windows-Anmeldebildschirm zwar die Anmeldung für andere Benutzer an, zeigt aber aufgrund der dafür in Windows genutzten Funktion "Schneller Benutzerwechsel" und deren Implementierung durch Microsoft nicht den Benutzer an, der beim letzten Mal angemeldet war. (Referenz: EI-1731)
- Achtung: Bei einer Zeitumstellung (z.B. Winter- auf Sommerzeit) kann es zu einer Abweichung der Server- und Systemzeit kommen, wenn Ihre DriveLock Agenten vor der Umstellung heruntergefahren wurden (somit also die 'alte' Zeit verwenden), aber die Zeit auf Ihrem Server bereits umgestellt wurde. In diesem Fall wird die Anmeldung an der Netzwerk-PBA blockiert. Die Endbenutzer müssen einmalig eine andere Anmelde-Methode auswählen (Benutzername-/Kennworteingabe) bzw. die Systemzeit einstellen. Sobald beide Zeiten synchronisiert sind, wird die Anmeldung an der Netzwerk-PBA wieder funktionieren. (Referenz EI-1817)
- Für die DriveLock PBA werden SmartCard-Leser vorausgesetzt, die eine CCID V1.1 konforme Schnittstelle haben.

1.3.9 Encryption 2-Go

Dateifilter

- Durch den Dateifilter blockierte Dateien können in Archive kopiert werden, die auf verschlüsselten Datenträgern gespeichert sind. (Referenz EI-2650)

1.3.10 Erzwungene 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.

1.3.11 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.
- Das Löschen verschlüsselter Ordner im lokalen OneDrive-Verzeichnis kann unter Umständen dazu führen, dass ein leerer Ordner übrig bleibt.

FireEye

- Das Produkt FireEye kann einen Blue-Screen-Fehler (BSOD) auslösen.

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

- Die Verwendung von File Protection in neuen Format (PFE) und Kaspersky auf demselben System kann zu einem Blue-Screen-Fehler (BSOD) führen, je nachdem, welche Einstellungen in der AV-Software verwendet werden. (Referenz EI-2524)

Zugriff auf verschlüsselte Ordner

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

Zugriff auf verschlüsselte Dateien

- Ein Blue-Screen-Fehler (BSOD) kann auftreten, wenn auf verschlüsselte Dateien zugegriffen wird. (Neues Format, automatischer Modus). (Referenz EI-2698)

Kopieren von Daten auf einen mit neuem Format verschlüsselten Netzwerkordner

- Der Blue-Screen-Fehler (BSOD) MUP_BUGCHECK_NO_FILECONTEXT kann beim Kopieren von 20-40 MB in einen verschlüsselten Netzwerkordner auftreten. (Neues Format, automatischer Modus) (Referenz EI-2684)

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".
- Wenn ein Wechseldatenträger (USB-Stick) verschlüsselt ist, kann das Entfernen des Geräts dazu führen, dass der gerade verschlüsselte Ordner nicht mehr geöffnet werden kann. Wird in diesem Fall das Gerät außerhalb formatiert und wieder angeschlossen, kann eine anschließende neue Erstverschlüsselung aufgrund des vorherigen Deaktivierungsfehlers hängen bleiben.
  Wenn ein solcher Arbeitsablauf erwünscht ist, empfehlen wir, entweder den Ordner vor dem Entfernen zu trennen oder das Gerät "sicher" zu entfernen (z. B. durch Auswerfen) und eine mögliche Ablehnung zu berücksichtigen, d. h. offene Dateien zu schließen.

Auf unverschlüsselte Dateien prüfen

- Wenn die Funktion 'CheckForUnencryptedFiles' nach erfolgreichem Mounten unverschlüsselte Dateien in Netzwerkordnern findet, schlägt die anschließende Erstverschlüsselung dieser Dateien fehl.

Wir empfehlen, den Vorgang abzubrechen, dann den Ordner zu trennen und erneut zu mounten. Die Prüfung und Erstverschlüsselung ist in diesem zweiten Durchlauf erfolgreich.

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. Bitte beachten Sie den Hinweis im Kapitel Update der DriveLock Komponenten. .

> Achtung: Wenn Sie bisher eine Version älter als 2021.2 verwendet haben, stellen Sie vor dem Update auf Version 2023.1 sicher, dass keine verschlüsselten Ordner auf DFS-Netzlaufwerken vorhanden sind.

1.3.12 SB-Freigabe

Wenn Sie den SB-Freigabe-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.

1.3.13 Thin Clients

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

- Auf IGEL-Clients kann Security Awareness nicht verwendet werden.

1.4 End-Of-Life-Ankündigungen

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

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

Version	On-Premise-Kunden-Support besteht bis:	Cloud-Kunden-Support besteht bis:
Alle Versionen vor 2022.1	EoL - kein Support mehr	EoL - kein Support mehr
2022.2	Juni 2025	EoL - kein Support mehr
2023.1	Entwicklungssupport *1: Dezember 2024 Produktsupport *2 : Juni 2025	EoL - kein Support mehr
2023.2	Entwicklungssupport *1: Juni 2025 Produktsupport *2 : Dezember 2025	Bis zum Release einer auf 2024.1 folgenden Version
2024.1	derzeit aktuelle Version	derzeit aktuelle Version

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

Support-Lebenszyklus:

Seit Version 2023.1 ist der Support-Lebenszyklus für neue DriveLock-Produktversionen folgendermaßen: Sobald eine neue Produktversion veröffentlicht wird, geben wir das End-Of-Life (EOL) der **Vorgängerversion** bekannt.

*1 Ab dem Datum der EOL-Ankündigung bietet DriveLock für weitere 12 Monate vollen Support für diese Version. Dies beinhaltet kritische Wartungsupdates, Codefixes für Fehler und kritische Probleme.

Nach Ablauf des vollen Supports (12 Monate) wird DriveLock keine neuen Updates mehr für diese Version veröffentlichen.

*2 Der DriveLock-Produktsupport steht jedoch für weitere 6 Monate zur Beantwortung von Telefon-, E-Mail- und Self-Service-Anfragen zur Verfügung.

Dies gilt für alle On-Premise Versionen ab Version 2023.1.

Upgrades:

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

Abkündigung von Funktionen:

- Version 2024.1 ist die letzte Version, die den Vulnerability Scan für Windows 8.x und älter unterstützt.
- Version 2024.1 ist die letzte Version, die automatische Push-Gruppen und OUs für die Push-Installation der DriveLock Agenten unterstützt. Alle anderen Funktionen und Einstellungen der Push-Installation sind bereits im DriveLock Operations Center verfügbar, weshalb der komplette Knoten in Version 2024.2 aus der DriveLock Management Konsole entfernt wird.
- Version 2024.1 unterstützt die Novell Directory Services (NDS) nicht mehr.
- Version 2024.1 unterstützt die Verwendung der Device Scanner Datenbank nicht mehr.
- Das DriveLock Control Center (DCC) wurde nur bis Mai 2024 offiziell unterstützt und ist jetzt abgekündigt.

Hinweis: **TLS 1.2**: Bitte stellen Sie sicher, dass bis 31. Oktober 2024 alle Betriebssysteme, auf denen DriveLock eingesetzt wird, TLS1.2 unterstützen.

2 Systemvoraussetzungen für den Betrieb von DriveLock

Die hier 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

Der DriveLock Agent kann auf verschiedenen Versionen von Windows, Linux und MacOS installiert werden.

Betriebssystem	Versionen
Windows 11	Ab 21H2, nur Editionen Pro / Enterprise
Windows 10	Ab 20H2, nur Editionen Pro / Enterprise
Windows 10 LTSC	alle LTSC-Versionen bis Ablauf des jeweiligen Extended Support
Windows Server	2016, 2019, 2022
Windows 7	Windows 7 SP1 Enterprise / Ultimate mit Extended Support. Hinweis: Eine zusätzliche Legacy Support Lizenz wird für den Betrieb auf Windows 7 Systemen benötigt.
Linux	CentOS 8, Debian 11, Fedora 34, IGEL OS 11.05, Red Hat Enterprise Linux 5, Suse 15.3, Ubuntu 20.04 oder neuere Versionen
macOS	ab Version Catalina (10.15) mit Intel (x86_64) und Apple Silicon (arm64) Architekturen

Der Windows DriveLock Agent ist grundsätzlich 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 unterstützt. Einschränkungen der einzelnen Funktionen sind weiter unten beschrieben.

Achtung: Beachten Sie, dass .NET Framework 4.7.2 für die Anzeige von Security Awareness-Kampagnen auf den DriveLock Agenten vorausgesetzt wird.

Folgende Tabelle bietet Ihnen einen Überblick über den Funktionsumfang, der auf einem bestimmten Betriebssystem verfügbar ist.

- Vollständiger Funktionsumfang: (✓)
- Reduzierter Funktionsumfang: (⓪)
- Keine Unterstützung: (☒)

Feature	Betriebssystem / Funktionen				
	Windows 10 / 11	Windows Server	Windows 7	Linux	Mac OS
Device Control	✓	✓	⓪	⓪	⓪
Application Control	✓	✓	✓	⓪	☒
Encryption 2-Go	✓	✓	✓	⓪	⓪
BitLocker To Go	✓	✓	⓪	☒	☒
BitLocker Management	✓	✓	⓪	☒	☒
Security Awareness Multimedia-Kampagnen	✓	✓	✓	☒	☒
Defender Management	✓	✓	☒	☒	☒

Feature	Betriebssystem / Funktionen				
Vulnerability Management	✓	✓	✓	☒	☒
Security Configuration Management	✓	✓	✓	☒	☒
Disk Protection	✓(*)	☒	☒	☒	☒
File Protection	✓	✓	⓪	☒	☒

(*): Disk Protection ist auf Windows 10 und neuer nur noch für UEFI-Systeme freigegeben, die BIOS-Unterstützung ist abgekündigt.

Hinweis: Security Awareness: Bitte beachten Sie, dass ab Version 22.1 Content-AddOn-Pakete nur dann korrekt angezeigt werden können, wenn auf den Agenten Microsoft Edge WebView2 installiert ist . Folgen Sie bitte dem Download-Link: https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section. Bei Windows 11 ist Microsoft Edge WebView2 bereits automatisch installiert.

Details zu Einschränkungen für Betriebssysteme, bei denen nur ein Teil der DriveLock Features genutzt werden kann:

1. **Einschränkungen Windows Server**
   - Die DriveLock Pre-Boot Authentifizierung steht für Server-Betriebssysteme nicht zur Verfügung.
   - Einstellungen für den Microsoft Defender können erst ab Windows Server 2016 verwendet werden.
2. **Einschränkungen Windows 7**

   Stellen Sie sicher, dass der letzte verfügbare Patch-Stand auf dem Windows 7 Client installiert ist.

- Generell:
  - Nach einem Update, einer Installation oder Deinstallation des DriveLock Agenten unter Windows 7 x64 stürzt der Explorer (explorer.exe) möglicherweise ab. Dies tritt nur dann auf, wenn die Windows-Eingabeaufforderung mit Admin-Rechten geöffnet und das System seit dem Update/Installation/Deinstallation des Agenten nicht neu gestartet wurde.
  - KB3140245 muss auf Windows 7 installiert sein
    Weitere Informationen dazu finden Sie unter 'Update-Prozess' und 'Update-Katalog'.
    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.
  - DriveLock Service ergänzt fehlende Registry-Werte für TLS 1.2 Verbindungen auf Computern mit Windows 7.
    Folgende Registry-Werte sind neben dem KB3140245 die Voraussetzung für die Kommunikation mit dem DES:
    - `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]"Enabled"=dword:00000001`
    - `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]"Enabled"=dword:00000001`
    - `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\WinHttp] "DefaultSecureProtocols"=dword:00000800`

      Hinweis: Falls der Wert `DefaultSecureProtocols` schon existiert, addieren Sie den Wert `0x00000800` für TLS 1.2 hinzu.

- BitLocker Management:
  - Nur für Windows 7 SP1 Enterprise und Ultimate verfügbar, 64-Bit - TPM-Chip ist erforderlich
  - 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.
- BitLocker To Go:
  - Nur für Windows 7 SP1 Enterprise und Ultimate verfügbar
- Device Control:
  - Die Bluetooth-Optionen in den Sperreinstellungen für Geräte können unter Windows 7 nicht verwendet werden.
- File Protection:
  - Unter Windows 7 steht für das neue Verschlüsselungsformat nur die eingeschränkte Funktionalität und für das alte Verschlüsselungsformat nur der bisherige Legacy Treiber nur zur Verfügung. Das passende Verschlüsselungsformat wird automatisch ausgewählt.
- Security Awareness Multimedia-Kampagnen:
  - Um auch Security Awareness Multimedia-Kampagnen anzeigen zu können, wird eine lokale Installation von WebView2 für Windows 7 benötigt. Weitere Informationen dazu sind hier zu finden: https://docs.microsoft.com/en-us/microsoft-edge/webview2/

3. **Einschränkungen macOS**

- Device Control:
  In dieser Version können nur USB-angeschlossene Laufwerke, die aufgrund ihrer Hardware ID identifiziert werden, blockiert oder zugelassen werden.
  Zusätzlich sind derzeit folgende Einschränkungen zu berücksichtigen:
  - Eigene Regeltypen für Whitelisting müssen konfiguriert werden (Hardware ID statt Product ID/Vendor)
  - Keine Freigabe für bestimmte Benutzer oder Benutzergruppen
  - Kein Dateifilter und Auditing
  - Keine erzwungene Verschlüsselung
  - Keine Freigabe von bereits mit Encryption 2-Go verschlüsselten Lauf-

werken

- Keine Self-Service Funktionalität

- Encryption 2-Go:
  - Für macOS steht wie bisher für die Entschlüsselung von externen USB-Laufwerken die Mobile Encryption Application (MEA) zur Verfügung.
  - Der macOS-Agent ist noch nicht in der Lage, Laufwerke mit einem Encryption 2-Go Container automatisch zu verschlüsseln.

  Weitere Informationen zum macOS-Agent entnehmen Sie bitte der separat verfügbaren macOS-Dokumentation auf DriveLock Online Help.

4. **Einschränkungen Linux**
   - Device Control:
     - Eigene Regeltypen für Whitelisting müssen konfiguriert werden (Hardware ID statt Product ID/Vendor)
     - Keine Freigabe für bestimmte Benutzer oder Benutzergruppen
     - Kein Dateifilter und Auditing
     - Keine erzwungene Verschlüsselung
   - Application Control:
     - DriveLock Application Control benötigt für den Einsatz auf Linux-Agenten Linux Kernel Version > 5.
     - Application Control kann nicht zusammen mit IGEL OS verwendet werden.
     - Keine der Application Behavior Control Funktionen stehen unter Linux zur Verfügung.
   - Encryption 2-Go:
     - Container bzw. verschlüsselte USB-Laufwerke können nicht erstellt, sondern nur verbunden werden.

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

5. **Einschränkungen für Terminal Server Umgebungen und Thin-Clients**
   - Der DriveLock Agent benötigt folgende Systemvoraussetzungen, damit die DriveLock Device Control Funktionalität grundsätzlich genutzt werden kann:

    - XenApp 7.15 oder neuer (ICA).
    - Windows Server 2016 oder neuer (RDP).
- Security Awareness Kampagnen für Benutzer bei der Anmeldung und bei ICA-Laufwerksverbindungen stehen bei der Verwendung von Thin-Clients ohne installiertem DriveLock Agenten nicht zur Verfügung.

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.

> Achtung: Setzen Sie immer die DriveLock Management Konsole (DMC) ein, die zur Version des DriveLock Enterprise Servers (DES) passt.

Hauptspeicher:

- mind. 4 GB RAM

Freier Festplattenspeicherplatz:

- ca. 350 MB

Benötigte zusätzliche Windowskomponenten:

- .NET Framework 4.8 oder höher

Unterstützte Plattformen:

Die Management Konsole 2024.1 wurde getestet und freigegeben auf den aktuellen Ständen der 64-bit 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.

2.3 DriveLock Enterprise Service

> Hinweis: Diese Information betrifft nur DriveLock On-Premise-Installationen.

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 2016 64-Bit
- Windows Server 2019 64-Bit
- Windows Server 2022 64-Bit

Auf einem Windows 10/11 Client Betriebssystem sollte ein DES nur als Testinstallation betrieben werden.

Achtung: Der DES steht ausschließlich als 64-bit Anwendung zur Verfügung.

Unterstützte Datenbanken:

- DriveLock benötigt ab Version 2024.1 mindestens SQL Server 2016 SP1 oder neuer. Die Datenbank muss einen Kompatibilitätsgrad von 130 oder höher haben.
- SQL-Server Express 2016 oder neuer für Installationen mit bis zu 200 Clients und Testinstallationen

- 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)

Hinweis: Diese Information betrifft nur DriveLock On-Premise-Installationen.

Das web-basierte DriveLock Operations Center ist in der Installation des DES enthalten und keine eigenständige Komponente. Es wird über einen Browser aufgerufen. Über den DOC Companion kann auf den DriveLock Richtlinien-Editor zugegriffen werden.

SQL-Server 2016 oder neuer ist Mindestvoraussetzung für das DriveLock Operations Center.

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

Copyright