

DriveLock Release Notes

Release Notes 2026.2

DriveLock SE 2026



Inhaltsverzeichnis

1 DRIVELOCK RELEASE NOTES 2026.2 4

1.1 Neuerungen, Verbesserungen und Änderungen 5

1.2 Fehlerbehebungen 13

1.3 Bekannte Einschränkungen und Hinweise 20

1.3.1 BitLocker Management 20

1.3.2 BitLocker To Go 22

1.3.3 Containerverschlüsselung (Encryption 2-Go) 22

1.3.4 Device Control 22

1.3.5 Festplattenverschlüsselung (Disk Protection) 26

1.3.6 Hinweise zu Virenscannern 29

1.3.7 DriveLock Enterprise Service (DES) 31

1.3.8 DriveLock Inventarisierung 31

1.3.9 DriveLock Operations Center (DOC) 31

1.3.10 DriveLock Pre-Boot-Authentifizierung 33

1.3.11 Dateiverschlüsselung (File Protection) 35

1.3.12 macOS Agent 36

1.3.13 Self-Service 37

1.3.14 Thin Clients 37

1.4 Empfehlungen 38

1.4.1 Sicherheitseinstellungen für den DriveLock Agenten 38

1.4.2 Verwendung von zentral gespeicherten Richtlinien 38

1.4.3 Verwendung vertrauenswürdiger Zertifikate 39

1.4.4 Lizenzverwaltung im DOC 39

1.5 End-Of-Life-Informationen 39

1.5.1 Versionsspezifische Abkündigungen 42

2 SYSTEMVORAUSSETZUNGEN FÜR DEN BETRIEB VON DRIVELOCK 43

2.1 DriveLock Agent 43
2.2 DriveLock Management Konsole (DMC) 51
2.3 DriveLock Enterprise Service (DES) 51
2.4 DriveLock Operations Center (DOC) 53
3 SECURITY BULLETINS 55
COPYRIGHT 56

1 DriveLock Release Notes 2026.2

Build: 26.2.2.19872

Datum: 18.11.2026

Die DriveLock Release Notes enthalten wichtige Informationen zu Neuerungen, Änderungen und Fehlerbehebungen in der Hauptversion 2026.2, 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 in 2026.2 befindet sich im Kapitel **Was ist neu?** in der DriveLock Dokumentation auf DriveLock Online Help.

> Hinweis: Diese Version enthält interne Verbesserungen zur Stabilitäts- und Sicherheitsoptimierung. Wir empfehlen ein Update auf die aktuelle Version.

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.

1.1 Neuerungen, Verbesserungen und Änderungen

Im Folgenden finden Sie eine Übersicht über die Neuerungen, Verbesserungen und Änderungen in DriveLock Version 2026.2.

Diese Version enthält Sicherheitsverbesserungen, Stabilitätsoptimierungen und Weiterentwicklungen bestehender Funktionen.

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

> Achtung: Mit jeder Version wird zusätzliche Funktionalität aus der DriveLock Management Console (DMC) in das DriveLock Operations Center (DOC) überführt. Dabei kann es zu leichten Unterschieden im Verhalten kommen, da bestimmte Funktionen im DOC technisch anders umgesetzt sind als in der DMC. Bitte stellen Sie sicher, dass alle Agenten auf die aktuelle Version aktualisiert wurden, bevor Sie die neuen DOC-Funktionalitäten produktiv einsetzen.

> Achtung: Durch das Einspielen der Aktualisierung kann es bei bestimmten Themen zu Verhaltensänderungen im Produkt kommen. Bitte überprüfen Sie Ihre Einstellungen, um festzustellen, ob Ihre bestehende Umgebung davon betroffen ist, bevor Sie die Aktualisierung durchführen. Diese Themen sind mit folgendem Warnsymbol gekennzeichnet: ⚠

Application Control (AC)

- ⚠ SHA-224-Unterstützung entfällt: Der Hashalgorithmus SHA-224 wird bei Hashberechnungen in Application Control und Device Control nicht mehr unterstützt.
- ⚠ Geändertes Reporting von Skriptausführungen: Skriptausführungen werden nicht mehr über die bisherigen Dateizugriffsereignisse 650 und 651 gemeldet, sondern über die neuen Ereignisse 795 und 796 mit zusätzlichen Informationen.
- Ausgehende Netzwerkverbindungen blockieren: Application Control unterstützt jetzt das Blockieren ausgehender Netzwerkverbindungen über Anwendungs-Verhaltensregeln.

Awareness mit DriveLock Aware

- Mit DriveLock Aware steht Cloud-Kunden eine neue Awareness-Lösung auf Basis der AwareGo-Plattform zur Verfügung. Sie kombiniert verhaltensbasierte Risikoanalysen (Human Risk Assessment) mit zielgerichteten Security-Awareness-Trainings.

Betriebssysteme

- Erweiterte Unterstützung für Windows on Arm: DriveLock unterstützt nun auch unter Windows 11 auf Arm64-basierten Systemen Application Control, Device Control, Drive Control, Application Behavior Control, Microsoft Defender Management und Firewall Management sowie die Inventarisierung und lokale Benutzer und Gruppen. Siehe Systemvoraussetzungen.

BitLocker Management

- Die zusätzliche Speicherung von BitLocker-Wiederherstellungsschlüsseln in Active Directory Domain Services (AD DS) oder Microsoft Entra ID kann jetzt über eine Einstellung im DriveLock Operations Center (DOC) aktiviert werden. Die Wiederherstellungsschlüssel werden weiterhin auch auf dem DriveLock Enterprise Service (DES) gespeichert.

Dateiverschlüsselung (File Protection)

- Für verschlüsselte File-Protection-Ordner kann jetzt eine benutzerdefinierte Readme-Datei verwendet werden. Dazu muss die Datei FfeReadMe.pdf im Dateispeicher hinterlegt werden. Sie ersetzt die standardmäßige Readme-Datei.

Defender Management

- Microsoft Defender Antivirus im DOC konfigurieren: Microsoft Defender Antivirus und seine Einstellungen können jetzt direkt im DriveLock Operations Center (DOC) über den Richtlinieneditor konfiguriert werden. Dabei stehen sämtliche bisher unterstützten Gruppenrichtlinieneinstellungen (GPO) zur Verfügung. Zusätzlich kann der aktuelle Status von Microsoft Defender Antivirus auf den DriveLock Agenten im DOC eingesehen werden.
- Signatur-Updates für Microsoft Defender im DOC starten: Signatur-Updates für Microsoft Defender können jetzt auch direkt über das DriveLock Operations Center (DOC) gestartet werden.

Device Control (DC)

- ⚠ Wenn für ein Gerät keine Geräteregeln vorhanden sind, steuert die Einstellung **Ereignisse für Geräte dieses Typs melden** der jeweiligen Geräteklasse jetzt zusätzlich die Ereignisgenerierung. (Referenz EI-3225)
- Bei Verwendung von Hashlisten in Laufwerks-Identifikations-Dateien können Dateien, die nicht in der Hashliste enthalten sind, jetzt gelöscht oder umbenannt werden.

DOC Companion

- Aktualisierung des DOC Companion: Nach dem Update auf DriveLock 26.2 muss auch der DOC Companion aktualisiert werden, damit er weiterhin funktioniert.
  Wichtig: Wenn Sie den DOC Companion über den Offline-Installer installiert haben, stellen Sie sicher, dass die neue Version installiert wird.

DriveLock Agent

- Verbesserte Agentenaktualisierung: Bei der Aktualisierung des DriveLock Agenten wurde die Behandlung beschädigter MSI-Produktregistrierungen verbessert. (Referenz: EI-3288)
- Benachrichtigungsart auswählen: Benutzer können jetzt über das DriveLock Tray-Menü festlegen, ob Benachrichtigungen als DriveLock-Popups oder als Windows-Toast-Benachrichtigungen angezeigt werden.
- Die Schaltfläche für Security Awareness wurde aus der DriveLock Mobile Encryption Application (MEA) entfernt.
- Die Agenten-Fernkontrolle über den DES mittels HTTP wird nicht mehr unterstützt. Die Kommunikation über den DES mittels MQTT/HTTPS ist weiterhin möglich.
- Automatische Reaktivierung von WLAN-Adaptern: WLAN-Adapter werden jetzt automatisch wieder aktiviert, sobald die Einstellung **WiFi-Verbindungen sperren, wenn der Computer mit einem LAN verbunden ist** deaktiviert wird. (Referenz EI-3351)
- ⚠ Geänderte Berechtigungen für die Agenten-Fernkontrolle: Berechtigungen für die Agenten-Fernkontrolle müssen jetzt explizit konfiguriert werden. Sind keine Berechtigungen hinterlegt, erhalten lokale Administratoren und Domänenadministratoren nicht mehr automatisch Zugriff auf die Agenten-Fernkontrolle.
  Wichtig: Prüfen Sie die bestehenden Berechtigungseinstellungen und konfigurieren Sie bei Bedarf die erforderlichen Zugriffsberechtigungen.

DriveLock Enterprise Service (DES)

- Benutzername und Kennwort für die Proxy-Authentifizierung des DES können jetzt direkt in den Servereinstellungen des DOC konfiguriert werden. (Referenz: EI-3385)
- ⚠ Erhöhte Sicherheitsanforderungen beim E-Mail-Versand: Für den E-Mail-Versand über den DES muss das Zertifikat des Mailservers von Windows als vertrauenswürdig eingestuft werden. Selbstsignierte Zertifikate, denen Windows nicht vertraut, werden nicht mehr akzeptiert.

- Die Richtlinienverarbeitung in On-Premise-Installationen wurde sicherheitsrelevant optimiert. Managed-Cloud-Umgebungen sind davon nicht betroffen.
- Die Berechtigungsprüfung für administrative Funktionen wurde verbessert.
- Die Protokollierung sicherheitsrelevanter Informationen wurde in On-Premise-Installationen weiter abgesichert.
- ⚠ Vertrauenswürdige Zertifikate für DES und verknüpfte DES: Die Vertrauenswürdigkeit der Zertifikate wird bei der Kommunikation zwischen dem zentralen DES und verknüpften DES-Servern verbindlich geprüft.
- Der DES unterstützt jetzt Zertifikate mit hohen Iterationswerten für die Schlüsselableitung, beispielsweise für Client-Zertifikate bei der Übertragung von Daten an Syslog. Der zulässige Maximalwert kann über einen Konfigurationsparameter angepasst werden. (Referenz EI-3287)
- Bei der Syslog-Konfiguration kann das Feld **Optionaler Hostname für den TLS-Verbindungsaufbau** jetzt leer bleiben. In diesem Fall wird automatisch der unter **Serveradresse** angegebene Hostname verwendet. Ist dort eine IP-Adresse eingetragen, muss der Hostname für den TLS-Verbindungsaufbau weiterhin explizit angegeben werden.
- Der DES unterstützt jetzt SQL-Anmeldungen für die Verbindung zur Datenbank. Dadurch kann der DES auch eine Verbindung zu SQL Server-Instanzen herstellen, die sich außerhalb einer Active Directory-Domäne befinden.
- Bei der Konfiguration des Mailservers kann jetzt festgelegt werden, ob die TLS-Verschlüsselung über STARTTLS oder direkt beim Verbindungsaufbau erfolgt. Alternativ kann die TLS-Methode automatisch anhand des verwendeten Ports ausgewählt werden.
- Erweiterte Konfiguration der Datenbankverbindung: Im DriveLock Server-Installationsassistenten können jetzt zusätzliche Parameter für die Datenbankverbindung konfiguriert werden.

DriveLock Freigaben

- Offline-Freigabe nur bei entsprechender Konfiguration verfügbar: Die Option zur Offline-Freigabe wird in der Benutzeroberfläche jetzt nur noch angezeigt, wenn Offline-Freigaben für den betreffenden Laufwerkstyp oder die betreffende Geräteklasse konfiguriert sind.

DriveLock Gruppen

- Neues Filterkriterium für Windows-Dienste: Mit dem neuen Filterkriterium **Dienststatus** können Sie den Status eines Windows-Dienstes anhand seines internen Dienstnamens prüfen, beispielsweise bei der Definition dynamischer Computergruppen.

DriveLock Operations Center (DOC)

- LISA – der neue DriveLock AI Assistant: Mit LISA steht im DriveLock Operations Center (DOC) jetzt ein KI-gestützter Assistent zur Verfügung. Benutzer können Fragen direkt im DOC stellen und erhalten KI-generierte Antworten zur Unterstützung bei der Arbeit mit DriveLock.
- Mit der neuen Vorlagenbibliothek im DriveLock Operations Center (DOC) stehen vorkonfigurierte Regeln, Richtlinien, Filter, Dashboards und Bundles zur Verfügung. Die Vorlagen basieren auf typischen Anwendungsfällen und bewährten Konfigurationen. Sie können als eigenständige Kopien übernommen und anschließend an die jeweilige Umgebung angepasst werden.
  Bitte beachten Sie, dass die Vorlagenbibliothek ausschließlich in DriveLock Managed Services zur Verfügung steht.
- ⚠ Die Paketverwaltung erfolgt jetzt im DriveLock Operations Center (DOC). Dort können Sie DriveLock Installationspakete verwalten und festlegen, welche Paketversionen für die Installation und automatische Aktualisierung von DriveLock Komponenten verwendet werden.
  Wichtig: Nach der Aktualisierung des DES muss die Paketverwaltung im DOC neu konfiguriert werden.
- Datenexport für Berichte: Berichtsdaten können jetzt auch im JSON- oder CSV-Format exportiert werden. Der Datenexport steht für Kreisdiagramme, Balkendiagramme, horizontale Balkendiagramme und Listen zur Verfügung. Dabei kann gewählt werden, ob nur die Daten oder zusätzlich der Bericht als PDF ausgegeben werden soll.
- ⚠ Import und Export von Konfigurationen ohne Prüfsummenprüfung: Beim Import und Export von Konfigurationen, beispielsweise Dashboards, Widgets und externen Links, wird keine Prüfsummenprüfung mehr durchgeführt. Dadurch können exportierte Konfigurationen manuell bearbeitet und anschließend wieder importiert werden.
  Wichtig: Fehlerhafte Änderungen an exportierten Konfigurationen können beim erneuten Import zu inkonsistenten Daten in der Datenbank führen. (Referenz: EI-3387)
- Zeitliche Gültigkeit von Regeln im DOC: Regeln können jetzt auch im DriveLock Operations Center (DOC) auf bestimmte Uhrzeiten oder Datumsbereiche begrenzt

werden. Diese Funktion war bisher nur in der DriveLock Management Konsole (DMC) verfügbar.

- Kommentare für Gruppenmitglieder bearbeiten: Im DriveLock Operations Center (DOC) können Kommentare zu Gruppenmitgliedern jetzt auch nachträglich bearbeitet werden. Bisher war die Eingabe eines Kommentars nur beim Hinzufügen eines Gruppenmitglieds möglich.
- Konfigurationsfilter im DOC: Die bisher aus der DriveLock Management Konsole (DMC) bekannten Konfigurationsfilter können jetzt auch im DriveLock Operations Center (DOC) erstellt und verwendet werden. Damit lassen sich unterschiedliche Einstellungen innerhalb einer Richtlinie abhängig von bestimmten Computern, Benutzern oder Zeiträumen anwenden.
- Listen- und Kartenansicht im DOC: Die meisten Ansichten im DriveLock Operations Center (DOC) können jetzt wahlweise als Listen- oder Kartenansicht dargestellt werden. Zudem wurden die Sortier- und Filtermöglichkeiten erweitert.
- Erweiterte Datenmaskierung: Personenbezogene Daten in Dateipfaden, ausgewählten Eigenschaften und einzelnen Ereignisparametern können jetzt gezielt maskiert werden. Mithilfe regulärer Ausdrücke (RegEx) lassen sich auch einzelne Bestandteile eines Werts maskieren.
- Verbesserte Dashboard-Funktionen: Die Dashboards im DriveLock Operations Center (DOC) wurden hinsichtlich Benutzerfreundlichkeit und Bedienung weiter optimiert.

DriveLock Richtlinien

- Erweiterte Verwaltung von Inhaltstypen in Richtlinien: Erlaubte Inhaltstypen können jetzt auch bei bestehenden Richtlinien hinzugefügt oder entfernt werden. Außerdem lassen sich Inhaltstypen beim Import, Export und Klonen von Richtlinien gezielt auswählen.

Linux Agent

- Linux Agenten unterstützen Application Control und Dateifilter nun auch auf NTFS3-Dateisystemen.
- Die FIPS-konforme Verschlüsselung wird jetzt auch unter Linux unterstützt.
- Linux Agenten unterstützen jetzt neben Samba Winbind auch SSSD für die Anbindung an Active Directory. Außerdem können neben AD-Benutzern und -Gruppen jetzt auch AD-Computerobjekte verwendet werden.
  Damit stehen folgende Funktionen zur Verfügung:

- Zuweisung von Richtlinien und Lizenzen anhand der AD- bzw. OU-Zugehörigkeit des Computers
- Verwendung von AD-Benutzern und -Gruppen in Device-Control-Regeln
- Erstellung dynamischer Computergruppen anhand von AD-Eigenschaften
- Übermittlung von Active Directory-Inventardaten an den DES
- Unterstützung von AD-Benutzern auf IGEL OS: AD-Benutzer können sich anmelden und in Device-Control-Regeln verwendet werden, ohne dass der Computer Mitglied einer AD-Domäne sein muss.

- Linux Agenten unterstützen jetzt Offline-Freigaben, mit denen gesperrte Laufwerke und Geräte temporär freigegeben werden können.

macOS Agent

- Temporäre Online-Freigabe von USB-Laufwerken unter macOS: Über das DriveLock Operations Center (DOC) können jetzt alle oder einzelne USB-Laufwerke auf macOS-Computern temporär freigegeben werden, sofern der Computer online ist.
- macOS Agenten unterstützen jetzt Offline-Freigaben, mit denen gesperrte Laufwerke temporär freigegeben werden können.

System Management

- Mit dem neuen System Management können Sie administrative Aufgaben auf verwalteten Computern automatisieren und definierte Compliance-Anforderungen durchsetzen.
  - Aktionen im DOC konfigurieren: Im DriveLock Operations Center (DOC) können Sie jetzt PowerShell- und Batch-Skripte als Aktionen erstellen und verwalten. Aktionen können Parameter enthalten und sowohl in Remote-Aufgaben und Compliance-Enforcement-Regeln als auch als Reaktion auf Ereignisse verwendet werden. Die Parameterwerte legen Sie bei der jeweiligen Verwendung fest.
  - ⚠ Ausführungsdauer von Aktionen: Für PowerShell- und Batch-Skripte gilt jetzt eine maximale Ausführungsdauer. Der Standardwert beträgt 60 Sekunden. Nach Ablauf dieser Zeit kann das Skript automatisch beendet werden, wenn die entsprechende Option aktiviert ist. Prüfen Sie die Einstellungen bestehender Aktionen und passen Sie diese bei Bedarf an.
  - Remote-Aufgaben: Mit Remote-Aufgaben können Sie Aktionen auf verwalteten Computern bei Bedarf direkt aus dem DOC auslösen. Die Aufgaben werden über Richtlinien verteilt und stehen im Kontextmenü eines Computers zur Verfügung,

sobald der DriveLock Agent sie an den DES gemeldet hat.

- Compliance-Enforcement-Regeln: Mit Compliance-Enforcement-Regeln können Sie definierte Zustände auf verwalteten Computern automatisch überprüfen und bei Abweichungen Aktionen ausführen lassen. So kann beispielsweise eine fehlende Datei durch ein Skript erstellt werden.

1.2 Fehlerbehebungen

DriveLock 2026.2 ist eine Hauptversion.

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2026.2 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Referenz	Application Control (AC)
EI-3284	Ein Problem wurde behoben, bei dem Application Control den Hash ausführbarer Dateien auf Netzwerkfreigaben bei bestimmten Berechtigungskonfigurationen nicht berechnen konnte.
	Ein Problem wurde behoben, bei dem die Signaturprüfung für bestimmte Dateitypen (z. B. PS1- und MSI-Dateien) nicht funktionierte, wenn die Signatur einen SHA-256-Digest verwendete.

Referenz	BitLocker Management (BLM)
	Ein Problem wurde behoben, bei dem sich die Option „Immer Downlevel-Logon-Namen während Single-Sign-on verwenden“ nicht mehr aktivieren ließ.
	Ein Problem wurde behoben, bei dem die BitLocker-PBA im DOC fälschlicherweise als „Aktiv“ angezeigt wurde, obwohl der Schutz des Systemlaufwerks deaktiviert war.
EI-3298	Ein Problem wurde behoben, durch das die BitLocker-Schlüsselwiederherstellung über das DOC nicht möglich war.

Referenz	BitLocker To Go
	Die Auswahl "<Lokaler Computer>" im Reiter "Automatische Entsperrung Computer" der erzwungenen BitLocker To Go-Verschlüsselung führte nicht zum automatischen Entsperren.
EI-3118	Ein Problem wurde behoben, bei dem die Verschlüsselung mit BitLocker To Go fehlschlagen konnte, wenn eine Windows-Richtlinie die Verwendung eines erweiterten XTS-Verschlüsselungsalgorithmus vorschrieb.
EI-3402	Ein Problem wurde behoben, bei dem der DriveLock Agent nach der Verschlüsselung eines Laufwerks mit BitLocker To Go unvollständige Wiederherstellungsinformationen übermitteln konnte.

Referenz	Containerverschlüsselung (Encryption 2-Go)
	Ein Problem wurde behoben, das Administrator-Kennwörter in Richtlinien für die Containerverschlüsselung betraf.

Referenz	Dateiverschlüsselung (File Protection)
	Ein Problem wurde behoben, bei dem unter bestimmten Umständen beim Erstellen eines verschlüsselten Ordners auf dem DriveLock Agenten ein Fehler auftrat.
EI-3375	Ein Problem wurde behoben, bei dem sich verwaltete Ordner in File Protection nach der Erneuerung von Benutzerzertifikaten nicht mehr verwalten ließen.

Referenz	Dateiverschlüsselung (File Protection)
EI-3321	Ein Problem wurde behoben, bei dem der Mobile Encryption Agent beim Lesen verschlüsselter Dateien beschädigte Dateien erzeugen konnte.
	Ein Problem wurde behoben, bei dem der konfigurierte Ordnername für die erzwungene Verschlüsselung bei Verwendung einer Benutzerauswahl-Regel doppelt in den Zielpfad übernommen wurde, z. B. D:\secure\secure statt D:\secure.

Referenz	Device Control (DC)
	Ein Problem wurde behoben, bei dem Benutzer ohne die erforderlichen Berechtigungen bei temporären Freigaben die Option zum Hinzufügen von Laufwerken oder Geräten aus dem Inventar angezeigt bekamen.
EI-3366	Ein Problem wurde behoben, bei dem die Benachrichtigung über das bevorstehende Ende einer temporären Freigabe die konfigurierte Dauer statt der tatsächlich verbleibenden Zeit anzeigte.

Referenz	Disk Protection
	Ein Problem wurde behoben, bei dem Volumes, die mit Disk Protection verschlüsselt waren, nach einem Neustart fälschlicherweise als „Unverschlüsselt“ angezeigt wurden.

Referenz	DriveLock Agent
EI-3248	Ein Problem wurde behoben, bei dem bestimmte Ereignisse von Drittanbietern nicht an den DES übertragen wurden, obwohl sie in der Richtlinie ausgewählt waren.
	Die Parameter mancher Dritthersteller-Ereignisse wurden zum Teil fehlerhaft oder in falscher Reihenfolge dargestellt.
EI-3288	Ein Problem bei der Aktualisierung des DriveLock Agenten wurde behoben, bei dem die Installation unter bestimmten Umständen mit dem Fehler 1603 fehlschlug. Dabei konnte die bisherige Agentenversion entfernt werden, ohne dass die neue Version installiert wurde.
	Ein Problem wurde behoben, bei dem der Prozess des DriveLock Dienstes im Windows-Task-Manager auf einigen Windows 11-Systemen mit einem falschen Symbol angezeigt wurde.
	Ein Problem wurde behoben, bei dem der DriveLock Agent bei der Verarbeitung eines MQTT-Ereignisses abstürzen konnte.

Referenz	DriveLock Enterprise Service (DES)
EI-3381	Ein Problem bei der Auswahl von Organisationseinheiten (OUs) für Rollenzuweisungen wurde behoben.
	Ein Fehler bei den Regeln für die Verarbeitung und Weiterleitung von Ereignissen wurde behoben.

Referenz	DriveLock Gruppenverwaltung
EI-3405	Ein Problem wurde behoben, bei dem Verweise auf Active Directory-Gruppen in statischen DriveLock-Benutzergruppen ungültige Daten enthalten konnten.

Referenz	DriveLock Management Konsole (DMC)
	Ein Problem wurde behoben, bei dem Benutzer-Verhaltensregeln aus mit DOC verwalteten Richtlinien in der RSOP-Ansicht eines Agenten nicht angezeigt wurden. Beim Öffnen dieser Richtlinien in der DMC waren die Regeln bereits sichtbar.
	Ein Problem wurde behoben, bei dem die DMC unter bestimmten Umständen abstürzte, wenn nach einem Benutzer in Microsoft Entra ID gesucht wurde.

Referenz	DriveLock Operations Center (DOC)
	Ein Problem wurde behoben, bei dem der Task „Agent konfigurieren“ im Kontextmenü eines Computers nicht angezeigt wurde.
	Ein Problem wurde behoben, bei dem der Tab „Temporäre Freigaben“ auch für Benutzer ohne die erforderlichen Berechtigungen angezeigt wurde. Beim Öffnen des Tabs wurde eine Fehlermeldung angezeigt.
EI-3332	Ein Problem wurde behoben, bei dem Sonderzeichen in Kennwörtern über die Funktion „Kennwort lokaler Benutzer anzeigen“

Referenz	DriveLock Operations Center (DOC)
	nicht angezeigt wurden.
	Ein Problem wurde behoben, bei dem für die Abfrage von Gruppen im Objektauswahldialog des DOC falsche Berechtigungen erforderlich waren. Für die Abfrage ist nun die Leseberechtigung für die Gruppenverwaltung (GroupManagement Read) erforderlich.
EI-3280	Spezielle Benutzerbenachrichtigungstexte für Laufwerksregeln und Anwendungslisten-Regeln werden jetzt korrekt am Agenten angezeigt.
EI-3370	Ein Problem wurde behoben, bei dem komplexe Berichte beim Versand per E-Mail leer waren.
EI-3372	Ein Problem wurde behoben, bei dem der E-Mail-Versand über SMTP-Server ohne Benutzerauthentifizierung fehlschlug.

Referenz	DriveLock Pre-Boot Authentifizierung (PBA)
	Ein Problem wurde behoben, bei dem in seltenen Fällen die Netzwerk-Logon-Konfiguration der Pre-Boot Authentication (PBA) beim Herunterfahren des Systems erneut auf dem Server registriert wurde. Dadurch funktionierte der Netzwerk-Logon in der PBA nicht mehr.

Referenz	Freigaben / Self-Service
EI-3222	Ein Problem wurde behoben, bei dem die Benutzerauthentifizierung über Self-Service unter bestimmten Umständen mit der Fehlermeldung „Zugriff verweigert“ fehlschlug.

Referenz	Linux Agenten
	Ein Problem wurde behoben, bei dem der Linux Agent unter bestimmten Umständen abstürzen konnte, wenn ein Konfigurationsfilter konfiguriert war.

1.3 Bekannte Einschränkungen und Hinweise

1.3.1 BitLocker Management

Windows Inplace Upgrade

> Achtung: Bitte beachten Sie, dass die BitLocker-Verschlüsselung bei einem Inplace Upgrade temporär von Microsoft deaktiviert und nach Abschluss automatisch wieder aktiviert wird. Wenn jedoch nach Abschluss des Upgrades noch ein bootfähiges Medium (z.B. CD-ROM) verbunden ist, bleibt die temporäre Deaktivierung weiterhin bestehen und die Verschlüsselung muss wieder manuell aktiviert 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 10 Pro und Enterprise, 32/64-Bit
  - Windows 11 Pro und Enterprise, 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 externen 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 Containerverschlüsselung (Encryption 2-Go)

Falsche Berechnung des Speicherbedarfs bei erzwungener Verschlüsselung unter macOS

- Bei Verwendung einer Regel für erzwungene Verschlüsselung mit konfiguriertem freiem Speicherplatz auf dem Zielmedium kann die Größe eines neuen Containers unter Umständen nicht korrekt berechnet werden.

Eingeschränkte Leistung bei der Verschlüsselung von exFAT-Laufwerken unter macOS

- Die Verschlüsselung von exFAT-formatierten Laufwerken mit Encryption 2 Go kann unter macOS deutlich langsamer erfolgen als bei FAT32-formatierten Laufwerken. Als Workaround müssen auf exFAT-Laufwerken unter macOS erstellte verschlüsselte Container zunächst auf einem Windows-Agenten 26.1 mit Encryption-2-Go-Lizenz eingebunden werden. Anschließend können sie unter Windows ohne Einschränkungen verwendet werden. (Referenz: EI-3138)

1.3.4 Device Control

Lizenzeinstellungen

- Wenn Sie seit Version 2020.2 keine Änderungen an den Lizenzeinstellungen vorgenommen haben, treten Probleme bei der Migration der Lizenzeinstellungen auf. Lösung: Nehmen Sie entweder direkt vor dem **Update** eine Änderung vor (z.B. Hinzufügen und Entfernen eines Computers) oder stellen Sie nach dem Update die Laufwerks- und Geräteaktivierung wieder korrekt ein. (Referenz EI-3123)

Blockierte Geräte bei Verwendung von Citrix Workspace

- In Kombination mit Citrix Workspace kann es auf manchen Computern vorkommen, dass Geräte nicht gestartet werden können, weil Windows den DriveLock-Treiber `DLDevFlt.sys` nicht laden kann. Vermutlich verursacht der Citrix USB Monitor Driver

`ctxusbmon.sys` Probleme beim Entladen von `DLDevFlt.sys`.

> Hinweis: Es liegen Hinweise vor, dass das Problem mit einer neueren Version von Citrix Workspace behoben wurde. Wir empfehlen daher, Citrix Workspace auf die neueste Version zu aktualisieren. Sollte das Problem weiterhin bestehen, eröffnen Sie bitte ein Supportticket bei Citrix.

Mögliche Workarounds, falls die Aktualisierung das Problem nicht behebt:
Da das Problem vermutlich mit dem Entladen von `DLDevFlt.sys` zusammenhängt, können Sie versuchen, das Entladen des Treibers zu verzögern oder zu verhindern. Wenn das Problem nur auftritt, wenn Geräte von DriveLock blockiert werden, aktivieren Sie die Einstellung **Blockierte Geräte im Device Manager deaktivieren**. Falls DriveLock keine Geräte blockiert oder diese Einstellung das Problem nicht behebt, können Sie alternativ die Einstellung **Entfernung von Geräten melden** verwenden. Dabei bleibt der Treiber geladen, bis das Gerät wieder entfernt wird. Beachten Sie hierzu die Hinweise in der Beschreibung dieser Funktion. (Referenz EI-2825)

Quotierung /Dateifilter

- Schreib-Filter sollten restriktiver als Lese-Filter konfiguriert werden. Unter Windows können Schreibzugriffe abhängig vom Anwendungsfall auch Leseberechtigungen voraussetzen, wodurch Leseeinschränkungen unter Umständen umgangen werden können. (Referenz: EI-3130)
- 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.
- 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 Quotierungen ist anwendungsspezifisch und hängt davon ab, wie eine Anwendung eine Datei für eine scheinbar einfache Lese- oder Schreibanforderung eines Benutzers öffnet. Eine Datei kann zwischengespeichert, mehrmals geöffnet, dupliziert oder umbenannt werden, bevor die eigentliche Lese-/Schreibverarbeitung erfolgt. Störende Prozesse, die im Auftrag des Benutzers (z. B. AV) ausgeführt werden, können das geplante Verhalten zusätzlich verfälschen. In Version 2025.1 wird nur die erste in einer Reihe identischer Erstellungen einer Datei auf die „Anzahl der Dateien“ angerechnet. (Identisch bedeutet: gleicher Benutzer, gleicher Pro-

zess und gleiche Zugriffsart – Lesen oder Schreiben.) Dies ermöglicht eine deutlich sinnvollere Nutzung der Quotenanzahl „Anzahl der Dateien“ als in früheren Versionen.

Dateifilter bei Archiv-Dateien (Containerdateien)

- Die Erkennung verschachtelter eingebetteter Dateien in PDF-Dateien ist technisch nicht möglich.
- 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-2650)
- Die Erkennung des Kennwortschutzes für OpenOffice-Dokumente in Containerdateien wird derzeit nicht unterstützt.
- Beachten Sie bitte folgende Hinweise:
  - Ein nicht standardmäßiges Anwendungs- und Verschiebeverhalten kann zu unerwarteten Ergebnissen führen, z. B. öffnet 7zip die Zip-Datei und zeigt Abschnitte einer verbotenen EXE-Datei im Analysemodus an. (Referenz EI-2651)
  - WebDAV-Laufwerke werden weiterhin nicht unterstützt.
  - Hash-Ausschlüsse werden in Archiven nicht angewendet.
  - Der Simulationsmodus beinhaltet kein Scannen von Inhalten.
  - Beim Verschieben eines Archivs von einem ungefilterten Speicherort wird auch dieses QuellArchiv gelöscht, wenn das ZielArchiv blockiert wird.

  Beachten Sie außerdem, dass
  - Archive bis zu einer Verschachtelungsebene von 2 gescannt werden, d.h. zip1/-zip2 wird gescannt, aber zip1/zip2/zip3 wird blockiert,
  - Größe bzw. Anzahl der enthaltenen Dateien nicht begrenzt sind; daher kann es trotz eines variablen, an die komprimierte Größe angepassten Timeouts zu einer Zeitüberschreitung während des Scans kommen,
  - Zeitüberschreitungen und andere Fehler, z.B. wenn das Archiv aus irgendeinem Grund nicht zum Scannen geöffnet werden kann, nicht zu einer Blockierung des Zugriffs führen.

Inhaltsprüfung

- Unter bestimmten Umständen kann das Blockieren des Löschens einer Datei technisch nicht umgesetzt werden. In den Vorgängerversionen wurde in diesen Fällen trotzdem ein Ereignis für das Blockieren des Löschens erzeugt, obwohl die Datei

bereits gelöscht war.
Lösung: Da das Löschen einer Datei, die aufgrund ihres Inhalts durch die Inhaltsprüfung als unerwünscht eingestuft wird, nicht grundsätzlich ein Fehler ist, entfällt nun die Inhaltsprüfung und damit auch die Erzeugung des Ereignisses.

- Die Inhaltsüberprüfung ist in Ordnern, die mit File Protection verschlüsselt wurden, nicht möglich und daher dort deaktiviert.

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.

Samsung Shield T7

- Die Seriennummern für Samsung Shield T7 unter Windows werden spiegelverkehrt ausgelesen. Dies gilt möglicherweise für alle USB-SCSI-Massenspeichergeräte (UAS).

Kumulative Windows Server 2022 Security Updates auf Terminal Server

- Wenn nach Installation bzw. Update des Drivelock Agenten auf den betroffenen Windows Servern weiterhin Fehler auftreten, sind folgende manuelle Schritte notwendig (Referenz EI-2639):
  - **Bei aktivierter MTP-Kontrolle:**

    Stoppen Sie die DriveLock Agent Services und des DriveLock Health Monitors (z. B. net stop drivelock & net stop dlhm) vor Einspielen des Windows Updates. Diese werden nach dem Neustart wieder automatisch gestartet.
    Starten Sie DriveLock gegebenenfalls manuell, wenn kein automatischer Neustart erfolgen sollte.

  - **Bei nicht aktivierter MTP-Kontrolle:**

    Nach dem Update von einer älteren DriveLock Agenten-Version müssen Sie einmalig in der Kommandozeile folgende Befehle ausführen: `drivelock -regmtpfltinf` und `drivelock -unregmtpfltinf`.

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 Festplattenverschlüsselung (Disk Protection)

Wichtige Information

- Disk Protection wird für Windows 7 oder älter nicht mehr unterstützt.

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 DriveLock PBA steht für Windows 10 und 11 zur Verfügung, da die für die Festplattenverschlüsselungskomponenten benötigten Treibersignaturen von Microsoft nur für diese Betriebssysteme 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 Boot-reihenfolge 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.

1.3.6 Hinweise zu Virenscannern

In Zusammenhang mit Antiviren-Software kann es unter Umständen notwendig sein, Ausschlüsse zu definieren.

Unter Umständen schlägt die Installation der DriveLock Disk Protection aufgrund installierter Antivirensoftware fehl, 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.

> Hinweis: Dasselbe gilt, wenn auf einem System mehrere mit Disk Protection verschlüsselte Partitionen vorhanden sind – unabhängig davon, ob es sich um logische Partitionen auf demselben Medium oder um separate Festplatten bzw. SSDs handelt.

Falls es zu weiteren unerwarteten Problemen mit Antiviren-Software kommen sollte, finden Sie im Folgenden eine Liste der ausführbaren Dateien, Verzeichnisse und Dienste, die von DriveLock verwendet werden:

Dateien und Verzeichnisse für DriveLock:

- "C:\SECURDSK" (EFS)
- "C:\Program Files\CenterTools\DriveLock" (Anwendungsverzeichnis)
- "C:\ProgramData\CenterTools DriveLock" (Cache/Arbeitsverzeichnis)

Prozesse/Dienste für DriveLock:

- **DriveLock**

  Anzeigename: DriveLock
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\DriveLock.exe"

- **dlhm**

  Anzeigename: DriveLock Health Monitor
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\DLHM.exe"

- **StorageEncryptionService**

  Anzeigename: DriveLock Full Disk Encryption Encryptor
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\DlFdeEncSvc.exe"

- **ClientDataManager**

  Anzeigename: DriveLock Full Disk Encryption Manager

Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\DlFdeMgr.exe"

- **dlupdate**

  Anzeigename: DriveLock Update and Installation
  Ausführbarer Pfad: "C:\Windows\DLUpdSvc.exe"

- **dessvc**

  Anzeigename: DriveLock Enterprise Service
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DES.exe"

- **DESTray**

  Funktion: Wird in der Taskleiste mit dem DES-Symbol angezeigt
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DESTray.exe"

- **DesRestarter**

  Funktion: Startet den DES-Dienst neu
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DesRestarter.exe"

- **FESFDS**

  Funktion: OSR-Service
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\FESF\FesfDs.exe"

- **FESFPolicy**

  Funktion: OSR-Service
  Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock\FESF\FESFPolicy.exe"

Microsoft Defender for Endpoint und verschlüsselte Netzwerkordner

- Auf Clients mit installiertem **Microsoft Defender for Endpoint** kann beim Kopieren von Daten in einen verschlüsselten Netzwerkordner (File Protection: neues Format, automatischer Modus) unter bestimmten Umständen der Blue-Screen-Fehler (BSOD) **MUP_BUGCHECK_NO_FILECONTEXT** auftreten, ausgelöst durch **MsSense.exe**.
  Um den BSOD zu vermeiden, sollten für verschlüsselte Netzwerkordner entsprechende EDR-Ausschlüsse (**EDR Exclusions**) in Microsoft Defender for Endpoint konfiguriert werden, damit der Prozess MsSense.exe diese Ordner nicht scannt. Die Konfiguration erfolgt unter **Settings > Endpoints > Rules > EDR Exclusions** in Microsoft Defender for Endpoint. (Referenzen EI-2684, EI-3167)

Windows 10-Clients mit Kaspersky Endpoint Security 10.3.0.6294

- Die Verwendung von File Protection im neuen Format (PFE) zusammen mit Kaspersky Endpoint Security auf demselben System kann – abhängig von den Einstellungen der Antiviren-Software – zu einem Blue-Screen-Fehler (BSOD) führen. (Referenz EI-2524)

1.3.7 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.

Windows Server 2016: Zertifikat wird bei der DES-Installation nicht erstellt

- Unter Windows Server 2016 wird bei Verwendung des alten DES-Installationsassistenten kein Zertifikat erstellt, auch wenn die entsprechende Option ausgewählt wurde. Fehlt das Zertifikat, kann der DES nicht verwendet werden.
  Workaround: Führen Sie den Installationsassistenten erneut aus und wählen Sie die Option zum Ändern oder Erneuern des Zertifikats. Dabei wird ein neues Zertifikat erstellt.

1.3.8 DriveLock Inventarisierung

Doppelte Einträge in CSV-Exporten (DOC) (Referenz EI-3131)

Beim Export großer Datenmengen aus dem DOC (z. B. Computer, Laufwerke, Geräte) kann es vorkommen, dass der CSV-Export doppelte Einträge enthält, wenn sich die zugrunde liegende Liste während des laufenden Exports ändert (z. B. durch neu hinzugefügte Objekte).

Workaround:

- Duplikate können in der CSV-Datei einfach gelöscht werden.
- Um Duplikate möglichst zu vermeiden, empfehlen wir:
  - die Ansicht/Abfrage nach einer Spalte zu sortieren, die sich selten ändert (z. B. Name oder ID), und
  - den Exportumfang so zu begrenzen, dass weniger Datensätze exportiert werden (z. B. durch Filterung oder kleinere Teilmengen).

1.3.9 DriveLock Operations Center (DOC)

⚠ Angepasste Prüfung von Rollenberechtigungen auf Gruppen und Richtliniensammlungen

- Bei Gruppen werden die Rollenberechtigungen jetzt im Kontext der Gruppe bzw. OU geprüft. Bisher war es möglich, zu allen Gruppen Computer hinzuzufügen oder zu

löschen, auch wenn der Benutzer nur Rechte auf einer bestimmten Gruppe bzw. OU hatte. Mit Version 2024.2 wurde die Rechteprüfung angepasst und beachtet jetzt die Einschränkung auf die jeweilige Gruppe bzw. OU. Wenn Sie auf alle Gruppen bzw. OU Rechte vergeben wollen, können Sie das Recht "Gruppen verwalten" global vergeben. Bei Richtliniensammlungen verhält es sich analog. Hier wird das Recht "Richtliniensammlung verwalten" geprüft.

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)

1.3.10 DriveLock Pre-Boot-Authentifizierung

- Damit die Netzwerk-Funktionalität der DriveLock PBA zum Einsatz kommen kann, muss Hardware das TCP4 UEFI Protokoll unterstützen. Es kann daher auf manchen Systemen zu Problemen kommen, wenn das UEFI-BIOS nicht die benötigten Netzwerkverbindungen unterstützt. Dies ist konkret bei folgenden Systemen der Fall:
  - Fujitsu LifeBook E459. (Referenz: EI-1303)
  - Fujitsu LifeBook U772
  - Acer Spin SP11-33
  - Acer Spin SP513-53N
  - Dell Inspirion 7347
- 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.

1.3.11 Dateiverschlüsselung (File Protection)

ISO-Dateien können in verschlüsselten Ordnern nicht gemountet werden

- ISO-Dateien, die sich in verschlüsselten Ordnern befinden, können unter Windows derzeit nicht gemountet werden.

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.

Zugriff auf verschlüsselte Ordner

- Der Zugriff auf verschlüsselte Ordner auf Laufwerken, die nicht mit Laufwerksbuchstaben sondern als Volume Mountpoint gemounted sind, wird nicht unterstützt.
- File Protection kann nicht verwendet werden, wenn sich der verschlüsselte Ordner in einem verschlüsselten Container befindet.

Sperren von Dateiteilbereichen auf Netzwerkfreigaben

- Um mögliche Kompatibilitätsprobleme mit manchen Programmen zu lösen, kann ab Version 2024.2 die Einstellung "Dateien auf Netzwerkfreigaben, für die Dateibereichssperren nicht modifiziert werden" als Workaround verwendet werden.

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 die Speicherung von verschlüsselten Verzeichnissen im neuen Format 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.

1.3.12 macOS Agent

Datenmaskierung auf macOS

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

DriveLock Mobile App

- Unter macOS wird beim Verschieben eines Ordners innerhalb der Mobile Encryption Application (MEA) in einen Unterordner innerhalb dieses Ordners der verschobene

Ordner vollständig gelöscht.

1.3.13 Self-Service

- 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.

1.3.14 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 Empfehlungen

1.4.1 Sicherheitseinstellungen für den DriveLock Agenten

Für zusätzliche Sicherheit beim Betrieb der DriveLock Agenten empfehlen wir, die folgenden beiden Optionen gemeinsam zu aktivieren.

Konfiguration: DOC → Einstellungen → Installationen → Sicherheitseinstellungen

- **Beitrittstoken:**

  Neue Agenten können dem Mandanten nur beitreten, wenn sie ein gültiges, mandantenspezifisches Token vorweisen. Dies verhindert unautorisierte Installationen.

- **Agentenidentität verifizieren:**

  Der DriveLock Enterprise Service prüft die Identität jedes Agenten, um sicherzustellen, dass gemeldete Daten tatsächlich vom entsprechenden Gerät stammen.

Weitere Informationen finden Sie im Kapitel **Sicherheitseinstellungen für Agenteninstallationen** in der DriveLock Dokumentation auf DriveLock Online Help.

1.4.2 Verwendung von zentral gespeicherten Richtlinien

Bei der Arbeit mit DriveLock, insbesondere für die Verteilung der Konfigurationseinstellungen zum Schutz des DriveLock Agenten auf Ihren Client Computern, empfehlen wir die Verwendung von zentral gespeicherten Richtlinien.

Im Vergleich zu Gruppenrichtlinienobjekten (GPO) bieten diese deutlich mehr Sicherheit, flexiblere Zuweisungsoptionen und funktionieren unabhängig von Active Directory – auch über das Internet.

Weitere Informationen finden Sie im Kapitel **Verteilung der DriveLock Konfigurationseinstellungen** in der DriveLock Online Hilfe auf DriveLock Online Help.

1.4.3 Verwendung vertrauenswürdiger Zertifikate

Prüfen Sie bei bestehenden Installationen, ob die Zertifikate für die Kommunikation zwischen dem zentralen DriveLock Enterprise Service (DES) und verknüpften DES-Servern die Anforderungen an die Vertrauenswürdigkeit erfüllen. Ab Version 26.2 wird diese bei der Kommunikation verbindlich geprüft. Dies gilt auch für DriveLock Enterprise Service Status.

Die Verwendung selbstsignierter Zertifikate wird nicht empfohlen. Sie können jedoch weiterhin verwendet werden, sofern sie die erforderlichen Zertifikatseigenschaften aufweisen und auf den beteiligten Systemen als vertrauenswürdig eingestuft werden.

Weitere Informationen zu den Zertifikatsanforderungen und zur Verwendung selbstsignierter Zertifikate finden Sie unter Zertifikatsprüfung bei der Kommunikation zwischen DES-Servern.

Die Kommunikation zwischen DriveLock Agenten und dem DES ist von dieser Änderung nicht betroffen.

1.4.4 Lizenzverwaltung im DOC

Es wird empfohlen, DriveLock Lizenzen im DriveLock Operations Center (DOC) zu verwalten und nicht über DMC-verwaltete Richtlinien.

Beim Import eines Lizenzschlüssels über die DMC kann es vorkommen, dass die Lizenz zwar im DOC angezeigt, jedoch nicht vollständig in DOC-verwaltete Richtlinien übernommen wird. Ist der DriveLock Enterprise Service (DES) offline, erhalten die Agenten in diesem Fall keine Lizenz über die Richtlinie.

1.5 End-Of-Life-Informationen

DriveLock informiert Sie rechtzeitig per Newsletter, wenn ein Support- und Wartungsende für eine bestimmte DriveLock-Version ansteht. Weitere Informationen finden Sie auch unter versionsspezifische Abkündigungen.

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

Version	On-Premise-Kunden-Support besteht bis:	Cloud-Kunden-Support:
Alle Versionen vor 2024.2	EoL - kein Support mehr	-

Version	On-Premise-Kunden-Support besteht bis:	Cloud-Kunden-Support:
2024.2	Entwicklungssupport *1: Juni 2026 Produktsupport *2 : Dezember 2026	-
2025.1	Entwicklungssupport *1: Dezember 2026 Produktsupport *2 : Juni 2027	-
2025.2	Entwicklungssupport *1: Juni 2027 Produktsupport *2 : Dezember 2027	
2026.1	Entwicklungssupport *1: Dezember 2027 Produktsupport *2 : Juni 2028	Support verfügbar
2026.2	derzeit aktuelle Version	Support verfügbar

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.

1.5.1 Versionsspezifische Abkündigungen

Neben unseren aktuellen DriveLock End-Of-Life-Informationen weisen wir Sie hier auf versionsspezifische Abkündigungen hin.

Abkündigung von Funktionen:

- Aufgrund des bevorstehenden End-of-Life (EoL) von Windows Server 2016 im Januar 2027 wird das Betriebssystem ab 2026.2 nicht mehr unterstützt.
- Die feste Zuweisung zentral gespeicherter Richtlinien (CSPs) zu DriveLock Agenten wird abgekündigt.
- Die Verwendung von Anwendungsvorlagen in der DMC wird abgekündigt.
- In einer der nächsten Versionen wird das alte Verschlüsselungsformat für File Protection nicht mehr unterstützt werden.
- Die bisher verwendeten Security-Awareness-Inhalte werden zum 31. Dezember 2026 eingestellt. Für zukünftige Awareness-Trainings kann Human Risk & Training mit AwareGo-basierten Trainingsinhalten verwendet werden.

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 11 LTSC	alle LTSC-Versionen bis Ablauf des jeweiligen Extended Support
Windows 10	Ab 20H2, nur Editionen Pro / Enterprise
Windows 10 LTSC	alle LTSC-Versionen bis Ablauf des jeweiligen Extended Support
Windows Server	2016/2019/2022/2025 (Standard oder Datacenter) mit Desktop Experience
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	Debian 13, Fedora 44, IGEL OS 12.8, AlmaLinux/Red Hat Enterprise Linux 10, SUSE 16, Ubuntu 26.04 LTS oder neuere Versionen.
macOS	ab macOS 14 Sonoma mit Intel (x86_64) oder Apple Silicon (arm64) Architekturen

- Der Windows DriveLock Agent unterstützt x86-basierte Systeme (32-Bit und 64-Bit) sowie Windows 11 auf Arm64-basierten Systemen. Für x86-basierte Systeme wird eine 64-Bit-Architektur empfohlen. Windows Server wird ausschließlich auf 64-Bit-Systemen unterstützt. Der verfügbare Funktionsumfang hängt vom Betriebssystem und der Architektur ab.
- Der Agenten-Installer setzt das Microsoft .NET Framework 4 (Client Profile) voraus, das auf aktuellen Windows-Betriebssystemen bereits vorhanden ist. Unter Windows 7 muss es manuell installiert werden. (Referenz: EI-2869)



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: ◒

Keine Unterstützung:✕

Feature	Betriebssystem / Funktionen				
	Windows 10 / 11	Windows Server	Windows 11 Arm64 (*1)	Linux	macOS
Drive Control	✓	✓	✓	◒	◒
Device Control	✓	✓	✓	◒	✕
Application Control	✓	✓	✓	◒	✕
Application Behavior Control	✓	✓	✓	✕	✕
Containerverschlüsselung (Encryption 2-Go)	✓	✓	✕	◒	◒
BitLocker To Go	✓	✓	✕	✕	✕
BitLocker Management	✓	✓	✕	✕	✕

Feature	Betriebssystem / Funktionen				
Security Awareness Multimedia-Kampagnen	✓	✓	✕	✕	✕
Defender Management	✓	✓	✓	✕	✕
Vulnerability Management	✓	✓	✕	✕	✕
Security Configuration Management	✓	✓	✕	✕	✕
Festplattenverschlüsselung (Disk Protection)	✓(*)	✕	✕	✕	✕
Dateiverschlüsselung (File Protection)	✓	✓	✕	✕	✕

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

(*1): Unter Windows 11 auf Arm64-basierten Systemen werden zusätzlich die Inventarisierung, Firewall Management sowie lokale Benutzer und Gruppen unterstützt.

Weitere Informationen zu Systemvoraussetzungen für unterschiedliche DriveLock Module:

- **Security Awareness:** Bitte beachten Sie, dass ab Version 2022.1 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.

- **File Protection:** Ab Version 2024.1 wird das aktuelle Microsoft Visual C++ Redistributable v14 vorausgesetzt. Folgen Sie bitte diesem Download-Link.
- **DriveLock Pre-Boot-Authentifizierung (PBA)**: Für die Installation werden 40 MB freier Speicherplatz in der EFI-Systempartition (ESP) vorausgesetzt.

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**
   - Laufwerkskontrolle:
     - Dateifilter mit Einschränkungen
     - Keine Freigabe von bereits mit Encryption 2-Go verschlüsselten Laufwerken
     - Self-Service mit Einschränkungen
   - Gerätekontrolle wird nicht unterstützt
   - 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 kann Laufwerke mit einem Encryption 2-Go Container automatisch verschlüsseln, jedoch steht noch nicht die für Windows Funktionalität vollumfänglich zur Verfügung.

   Weitere Informationen zum macOS-Agenten entnehmen Sie bitte dem Themenblock macOS in der DriveLock Online Dokumentation.

4. **Einschränkungen Linux**
   - Laufwerkskontrolle:
     - Ab Version 2025.2 werden Dateifilter in Laufwerksregeln unterstützt. Im Vergleich zu Windows stehen jedoch noch nicht alle Optionen zur Verfügung.
   - 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.

Weitere Informationen zum Linux Client und den Limitierungen der Funktionalität entnehmen Sie bitte dem Themenblock Linux in der DriveLock Online Dokumentation.

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 2026.2 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 (DES)

> 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 10.0 Runtime (Microsoft Download Link)
- ASP.NET 10.0 Core Runtime (Microsoft Download Link)
- .NET Desktop Runtime 10.0 (Microsoft Download Link)

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.

Achtung: Zur Aktualisierung von Version 2021.2 (oder früher) muss zunächst auf Version 2024.2 und dann erst auf eine neuere Version aktualisiert werden.

Benötigte DriveLock Services Ports:

Port	Verwendung
1883; 3004; 4370; 5370; 6369; 3003; 4567; 4766; 18083; 18084	Diese lokalen Ports dürfen nicht durch andere Server-Dienste belegt werden. Sie werden nur intern verwendet und müssen nach außen nicht freigegeben werden.
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.
4568	Dieser Port wird hauptsächlich für das DriveLock Operations Center (DOC) verwendet.

Port	Verwendung
6066; 6067	Diese Ports werden für die Übertragung von Management- und Statusinformationen der Agenten verwendet.

Unterstützte Plattformen:

- Windows Server 2016/2019/2022/2025 (Standard oder Datacenter) mit Desktop Experience

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

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

Unterstützte Datenbanken:

- Für den Betrieb von DriveLock wird Microsoft SQL Server 2017 oder höher vorausgesetzt. Die Datenbank muss einen Kompatibilitätsgrad von 140 oder höher haben. Referenzen: EI-3074; EI-3204; EI-3188
- 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.

3 Security Bulletins

Eine umfassende Liste unserer aktuellen Security Bulletins finden Sie jetzt auf DriveLock Online Help.



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.

© 2026 DriveLock SE. Alle Rechte vorbehalten.

