DriveLock Release Notes

Release Notes 2026.1 Patch 1

DriveLock SE 2026

Inhaltsverzeichnis

1 DriveLock Release Notes 2026.1 Patch 1

Build: 26.1.3.16176

Datum: 17.08.2026

Die DriveLock Release Notes enthalten wichtige Informationen zu Änderungen und Fehlerbehebungen in dieser Patch-Version 2026.1 Patch 1. Ebenfalls finden Sie hier auch Informationen zu Neuerungen, Änderungen und Fehlerbehebungen in der Hauptversion, sowie einen Überblick über die Systemvoraussetzungen für den Einsatz von DriveLock und unsere End-Of-Life-Ankündigungen.

Eine detaillierte Beschreibung der Neuerungen in 2026.1 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 Patch-Version 2026.1 Patch 1

1.1.1 Verbesserungen und Änderungen

Im folgenden finden Sie eine Auflistung der in 2026.1 Patch 1 enthaltenen Neuerungen und Änderungen.

DriveLock Enterprise Service (DES)

- Für den E-Mail-Versand werden selbst signierte Zertifikate nicht mehr unterstützt. Das Zertifikat des Mailservers muss als vertrauenswürdig in Windows eingestuft sein.
- 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.
- 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-3294)

Linux Agenten

- Linux-Agenten unterstützen Application Control und Dateifilter nun auch auf NTFS3-Dateisystemen.

macOS Agenten

- Die Funktion „Angemeldete Benutzer“ wird nun auch für die Containerverschlüsselung (Encryption 2-Go) unter macOS unterstützt.

1.1.2 Fehlerbehebungen

DriveLock 2026.1 Patch 1 ist eine Patch-Version.

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Patch-Version 2026.1 Patch 1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Referenz	Application Control (AC)
EI-3299	Ein Problem wurde behoben, bei dem Application Control den Hash ausführbarer Dateien auf Netzwerkfreigaben bei bestimmten Berechtigungskonfigurationen nicht berechnen konnte.

	BitLocker Management
	Ein Problem wurde behoben, durch das die Option „Immer Downlevel-Logon-Namen während Single-Sign-On verwenden“ nicht aktiviert werden konnte.
EI-3300	Ein Problem wurde behoben, durch das die BitLocker-Schlüsselwiederherstellung über das DOC nicht möglich war.

Referenz	DriveLock Containerverschlüsselung (Encryption 2-Go)
	Ein Fehler bei der FIPS-konformen Containerverschlüsselung wurde behoben. Die Erstellung neuer Container und die Neuverschlüsselung von USB-Sticks funktionieren wieder mit der Einstellung "Nur FIPS-Verschlüsselung (kompatibel bis 25.2, Linux/macOS)".
	Ein Problem wurde behoben, das Administrator-Kennwörter in Richtlinien für die Containerverschlüsselung betraf.

	DriveLock Dateiverschlüsselung (File Protection)
	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	DriveLock Management Konsole (DMC)
	Ein Problem wurde behoben, bei dem Benutzer-Verhaltensregeln in der RSOP-Ansicht von Agenten für mit DOC verwaltete Richtlinien nicht angezeigt wurden.

	DriveLock Operations Center (DOC)
	Ein Problem wurde behoben, bei dem für die Abfrage von Gruppen im Objektauswahldialog des DOC falsche Berechtigungen erforderlich waren. Für die Abfrage von Gruppen sind nun Leseberechtigungen für die Gruppenverwaltung erforderlich.
	Ein Problem wurde behoben, bei dem der Tab „Temporäre Freigaben“ auch für Benutzer ohne die erforderlichen Berechtigungen angezeigt wurde.
	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-3302	Spezielle Benutzerbenachrichtigungstexte für Laufwerksregeln und Anwendungslisten-Regeln werden jetzt korrekt am Agenten angezeigt.
EI-3310	Ein Problem wurde behoben, bei dem die Tabs „Temporäre Freigaben“ und „Freigabe-Anforderungen“ im DOC nur angezeigt wurden, wenn sowohl eine Application-Control- als auch eine Device-Control-Lizenz aktiv war.

	macOS Agent
	Die Anzeige des Agentenstatus auf macOS-Clients in Domänenumgebungen wurde korrigiert.
	Ein Problem wurde behoben, bei dem für lokale macOS-Benutzer ein falscher Domänenname gespeichert und angezeigt wurde.
	Ein Problem wurde behoben, bei dem die Eigenschaft 'Betriebssystemsprache' im Computerinventar des DOC nicht angezeigt wurde.

1.2 Hauptversion 2026.1

1.2.1 Neuerungen, Verbesserungen und Änderungen

Im folgenden finden Sie eine Auflistung der in 2026.1 enthaltenen Neuerungen, Verbesserungen und Änderungen.

Mit diesem Release wurden Verbesserungen umgesetzt, welche die Sicherheit und Stabilität der Anwendung weiter erhöhen. Durch gezielte Optimierungen und Verfeinerungen bereits bestehender Sicherheitsmechanismen steht die neue Version jetzt mit einem noch stärkeren Schutz vor potenziellen Risiken zur Verfügung. Ebenso wurden Maßnahmen ergriffen, damit das Produkt nun noch robuster und performanter ist und insgesamt für ein noch reibungsloseres Nutzererlebnis sorgt.

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

- Die Erstellung von Application-Control-Regeln im erweiterten Modus wurde im DOC optimiert. Anstelle mehrerer separater Regeln wird nun eine einzelne Regel mit verschachtelten Filtern erzeugt.
- Freigabe-Anforderungen können nun auch für ausführbare Dateien verwendet werden. Dadurch können Benutzer temporäre Freigaben für durch Application Control blockierte ausführbare Dateien anfordern.
- Anwendungslisten können jetzt auch im DriveLock Operations Center (DOC) erstellt und bearbeitet werden.

- Im DriveLock Operations Center (DOC) stehen jetzt Benutzer-Verhaltensregeln zur Verfügung. Mit diesen Regeln können Sie festlegen, welche Aktionen Benutzer mit Anwendungen oder Skripten ausführen dürfen.
- Application Control unterstützt jetzt das Ignorieren von Prozessverhalten. Für ausgewählte Anwendungen können DLL-Ladevorgänge, Dateizugriffe oder Registry-Zugriffe von der Überwachung, Auswertung und Lernfunktion ausgeschlossen werden. Die Funktion kann nicht zusammen mit dem Trust-/Learn-Modus verwendet werden. (Referenz EI-3094)
- Application Control enthält die neue Einstellung 'Dateizugriffskonflikte vermeiden'. Wenn diese aktiviert ist, werden konkurrierende Dateizugriffe anderer Prozesse während eines Dateizugriffs durch Application Control kurzzeitig verzögert, um Dateizugriffskonflikte zu vermeiden. (Referenz EI-3115)

Awareness

- Für Awareness-Kampagnen stehen zwei neue Dashboard-Widgets zur Verfügung. Diese ermöglichen eine Übersicht über den Status und die Ergebnisse eigener Kampagnen. (Referenz EI-2953)
- Mit Human Risk & Training steht jetzt eine Integration zur AwareGo-Plattform für Sicherheitsbewertungen und Security-Awareness-Trainings zur Verfügung.

Containerverschlüsselung

- Die Rückgabecodes von DLCrypt.exe wurden überarbeitet, um eine eindeutigere Auswertung von Erfolgs- und Fehlerzuständen zu ermöglichen.
- Benutzerauswahl-Regeln für die erzwungene Verschlüsselung können nun direkt in mit dem DOC verwalteten Richtlinien konfiguriert werden.
- ⚠ Die FIPS-konforme Verschlüsselung wurde überarbeitet; AES-XTS-256 wird nun als zusätzliches Verschlüsselungsverfahren unterstützt. Bitte beachten Sie dazu den Hinweis in den Einschränkungen.

Dateiverschlüsselung (File Protection)

- ⚠ Das Standardverhalten für die Kennwort-Komplexität bei verschlüsselten Ordnern wurde geändert. Standardmäßig werden nun die unter Kennwortanforderungen definierten Kennwortrichtlinien verwendet. Dies betrifft auch die Containerverschlüsselung.

Defender Management

- Das DOC und die API unterstützen jetzt das Starten von Microsoft Defender Offline-Scans. Beim Auslösen des Scans können Benachrichtigungen für den Benutzer sowie Aufschuboptionen konfiguriert werden.

Device Control (DC)

- ⚠ Verhaltensänderung: COM- und LPT-Ports werden nur noch behandelt, wenn entsprechende Einstellungen in der MMC konfiguriert sind. (Referenz EI-3129)
- Die Containerdatei-Prüfung unterstützt jetzt zusätzlich Office- und PDF-Dokumente. In diesem Zusammenhang wurde die bisherige Bezeichnung 'Archive' in 'Containerdateien' geändert.
- ⚠ Verhaltensänderung: MTP-Geräte und Medien-Abspielgeräte werden in DOC und MMC nun der Geräteklasse 'Smartphones' zugeordnet. Für die Freigabe solcher Geräte ist daher künftig die Berechtigung zur Freigabe von Smartphones erforderlich. Eine Freigabe ausschließlich mit der Berechtigung für Geräte ist nicht mehr möglich.
- Blockierte Zugriffe auf MTP-Geräte durch Windows-Dienste oder andere Prozesse in Session 0 werden nicht mehr gemeldet, wenn die erforderlichen Berechtigungen fehlen. Diese Änderung betrifft ausschließlich das Reporting. (Referenz: EI-3097)
- In Laufwerksregeln im DOC kann nun für einzelne Laufwerkseinträge ein Laufwerkstyp definiert werden. Dadurch können Regeln, die für mehrere Laufwerke eines Herstellers gelten, gezielt auf bestimmte Laufwerkstypen wie z. B. CD/DVD-Laufwerke oder USB-Laufwerke eingeschränkt werden.
- Die Einstellungen zur Anwendung von Laufwerksregeln auf Wechselmedien, Festplatten und CD/DVD-Laufwerke können nun auch im DOC konfiguriert werden. Die Konfiguration erfolgt dabei spezifisch für die jeweiligen Laufwerkstypen innerhalb einer Regel.
- Für Laufwerksregeln im DOC kann nun konfiguriert werden, dass Regeln nur für bestimmte angemeldete Benutzer oder Benutzergruppen angewendet werden.
  Bitte beachten Sie, dass auf Systemen mit mehreren gleichzeitig angemeldeten Benutzern, z. B. auf Terminalservern, das Verhalten von der erwarteten Regelanwendung abweichen kann.
- Die Verarbeitung von erlaubten und blockierten Geräten unter Windows wurde verbessert. Dadurch werden Gerätezustände zuverlässiger erkannt und unnötige Geräte-Neustarts reduziert.

- Blockierungen aufgrund von Dateifiltern und Quotenbeschränkungen werden nun durch eigene Ereignisse protokolliert.
- Um Datenverlust zu vermeiden, werden blockierte Archive jetzt zunächst in den temporären Ordner des Benutzers (Unterordner „DLDeleted“) kopiert und dort analysiert, bevor sie auf das Ziellaufwerk verschoben werden, auf dem der Dateifilter aktiv ist.
- Archive werden beim Kopieren oder Verschieben in überwachte Speicherorte nun vor der Ablage am Zielort geprüft. Dadurch wird verhindert, dass ungeprüfte Archive auf entfernten Wechselmedien zurückbleiben.

DriveLock Agent

- Benutzerdefiniertes Logo im Dialog für Freigabeanforderung: Ab Version 26.1 kann im Dialog für Freigabeanforderung ein eigenes Banner (DLUserDlgBanner.png) angezeigt werden.
- Administratoren können jetzt einen zusätzlichen Menüeintrag im Kontextmenü des DriveLock-Agenten bereitstellen, über den Benutzer Benachrichtigungen vorübergehend deaktivieren können.

DriveLock Enterprise Service (DES)

- Die Visual-C++-Laufzeitbibliotheken wurden aktualisiert. Für die vollständige Übernahme der Änderungen ist nach der Aktualisierung auf Version 26.1 ein Neustart des Servers erforderlich. (Referenz EI-3071)
- Das Senden von Ereignissen an einen Syslog-Dienst wurde beschleunigt. Zusätzlich kann nun konfiguriert werden, wie Ereignisse im Datenstrom getrennt werden. (Referenz EI-3232)
- Die Sicherheitsmechanismen für Cloud-Verbindungstests in On-Premise-Umgebungen wurden verbessert.
- Die Richtlinienverarbeitung in On-Premise-Installationen wurde sicherheitsrelevant optimiert. Managed-Cloud-Umgebungen sind davon nicht betroffen.
- Die Protokollierung sicherheitsrelevanter Informationen wurde in On-Premise-Installationen weiter abgesichert.
- Die Berechtigungsprüfung für administrative Funktionen wurde verbessert.
- Für die Schema-Erweiterung 'CVE-Liste' können nun benutzerdefinierte Felder definiert werden.
- Für ausführbare Dateien können nun benutzerdefinierte Felder über Schema-Erweiterungen definiert werden.

- Das Umbenennen geklonter Computer wurde im Zusammenhang mit aktiviertem Beitritts- oder Identitätstoken verbessert. Zudem wurde die Verarbeitung von Master-Images überarbeitet, um Probleme beim Umbenennen zu reduzieren.
- Für das Löschen von Computern steht nun ein eigenes Ereignis zur Verfügung, um entsprechende Vorgänge besser nachvollziehen zu können. (EI-3100)
- Im Server Setup Wizard kann die Installation nun auch dann fortgesetzt werden, wenn der erforderliche Datenbank-Kompatibilitätsgrad nicht überprüft werden kann.

DriveLock Freigaben

- ⚠ Das Übertragungsformat für Offline-Freigaben wurde überarbeitet und verbessert. Insbesondere wurde die Zeitspanne für die Eingabe von Response-Codes auf 60 Minuten begrenzt.
- Offline-Freigaben können nun auch in mit dem DOC verwalteten Richtlinien konfiguriert werden. Für diese Konfiguration sind keine zusätzlichen Kennwort- oder Zertifikatseinstellungen erforderlich.
- Die Freigaben-Ansicht im DOC wurde erweitert. Administratoren können nun alle Freigaben sowie die zugehörigen Ereignisse und Objekte der ausgewählten Freigabe zentral anzeigen.
- ⚠ Die Konfiguration von Freigabe-Anforderungen wurde erweitert. Freigabe-Anforderungen werden nun auf Ebene der Laufwerkstypen und Geräteklassen konfiguriert und sind standardmäßig deaktiviert. Benutzer können Freigabe-Anforderungen nur noch erstellen, wenn diese zuvor für den jeweiligen Laufwerkstyp oder die entsprechende Geräteklasse aktiviert wurden. Zusätzlich wurde die Benutzerführung für Freigaben und Freigabe-Anforderungen verbessert.
- Temporäre Freigaben können jetzt in DOC detailliert verfolgt und analysiert werden.

DriveLock Management Konsole (DMC)

- Die DriveLock Management Konsole wurde erweitert, sodass Microsoft-Entra-ID-Benutzer nun direkt ausgewählt werden können. (Referenz EI-3161)

DriveLock Operations Center (DOC)

- Benutzerbenachrichtigungen können jetzt direkt im DriveLock Operations Center mehrsprachig konfiguriert und angepasst werden. Neben Standardmeldungen lassen sich auch benutzerdefinierte Benachrichtigungstexte erstellen und verwalten. Benutzerdefinierte Benachrichtigungen sind standardmäßig aktiviert.

- Für Mitglieder von Microsoft-Entra-ID-Gruppen wird nun der Benutzerprinzipalname (UPN) angezeigt.
- Benutzerdefinierte Computereigenschaften können nun durch Agenteneigenschaften befüllt werden.
- Beim Hinzufügen eines Laufwerks/Geräts (z.B. aus einem Ereignis oder einer Freigabe-Anforderung) zu einer Regel können jetzt auch mehrere Regeln gleichzeitig ausgewählt werden.
- Die Agentenidentität wird aus Sicherheitsgründen nicht mehr im Klartext angezeigt. Die Spalte „Agentenidentität" zeigt stattdessen an, ob eine Identität an den Server gemeldet wurde.
- Dateityp-Definitionen können nun auch im DriveLock Operations Center (DOC) erstellt, bearbeitet und importiert werden. Zusätzlich wurde die Erstellung eigener Dateityp-Definitionen vereinfacht, indem Dateiinhalte direkt analysiert und verglichen werden können.
- Der Dialog zum Hinzufügen von Widgets wurde überarbeitet. Eine neue Navigation sowie zusätzliche Filter erleichtern das Auffinden und Hinzufügen von Widgets. Zudem können Widgets nun per Doppelklick hinzugefügt werden, ohne dass der Dialog geschlossen wird.
- Im Menü Inventar steht nun zusätzlich zur Computerliste eine Übersicht aller Agentenaktionen zur Verfügung, sodass deren Status zentral überwacht werden kann.
- Beim Erstellen von Regeln kann nun direkt ein vorhandener oder neuer Ordner als Speicherort ausgewählt werden. Dadurch lassen sich Regeln bereits bei der Erstellung strukturiert organisieren.
- Weitere aus dem Richtlinien-Editor der DriveLock Management Konsole bekannte Agenteneinstellungen stehen nun auch im DOC zur Verfügung.
- Die Verschlüsselungsfunktionen im DriveLock Operations Center wurden in einem zentralen Bereich Verschlüsselung zusammengeführt. Administratoren können nun BitLocker Management, BitLocker To Go, Festplattenverschlüsselung, Containerverschlüsselung und Dateiverschlüsselung über eine einheitliche Navigationsstruktur verwalten.

DriveLock Pre-Boot-Authentifizierung (PBA)

- Drivelock unterstützt jetzt Microsoft UEFI CA 2023 signierte Bootloader. Sollte ein Update des Microsoft UEFI CA Zertifikats stattfinden, wird Drivelock automatisch die

PBA aktualisieren. (Referenz EI-2983)

DriveLock Richtlinien

- Richtlinien und Richtlinieninhalte können nun im DOC importiert und exportiert werden. Vor dem Import werden die geplanten Änderungen angezeigt. Außerdem erkennt das DOC fehlende DriveLock-Gruppen und kann diese bei Bedarf automatisch anlegen.

Linux Agent

- IGEL-OS-Clients melden nach einer Active-Directory-Anmeldung nun den korrekten Benutzernamen.
- Self-Service-Regeln werden nun auch für Linux-Agenten unterstützt. Benutzer mit entsprechenden Berechtigungen können Self-Service-Freigaben direkt über die Freigabeoberfläche des Linux-Agenten starten.
- Die Unterstützung temporärer Freigaben für Linux-Agenten wurde erweitert. Es können nun einzelne Laufwerke, einzelne Geräte sowie benutzerdefinierte Geräteklassen freigegeben werden. Zudem werden mehrere gleichzeitig aktive Freigaben unterstützt.
- Unter Linux wird beim vollständigen Blockieren eines Laufwerks nun auch das neue Ereignis 787 generiert – anstelle des bisher verwendeten Ereignisses 111.
- Lokale Linux-Benutzer werden nun als Objekte im Server angelegt. Sie werden im DOC angezeigt und können in Regeln verwendet werden. (Referenz EI-3228)
- Der Linux-Agent informiert Benutzer nun über Beginn, bevorstehendes Ende und Ablauf einer temporären Freigabe.

macOS Agent

- Das DOC enthält jetzt Anleitungen zur Bereitstellung des macOS-Agenten über MDM-Systeme wie Microsoft Intune oder JAMF.
- Die Containerverschlüsselung unter macOS unterstützt ab Version 26.1 Benutzerauswahl-Regeln für die erzwungene Verschlüsselung.
- Dateifilter in der Laufwerkskontrolle werden nun auch unter macOS unterstützt. Benutzer-/Prozessausschlüsse, Hash-basierte Dateiausschlüsse sowie Schattenkopien werden unter macOS derzeit nicht unterstützt.
- Die Funktion 'Angemeldete Benutzer' für Laufwerksregeln wird nun auch unter macOS unterstützt.

- Die Laufwerkskontrolle unter macOS unterstützt nun benutzer- und gruppenbasierte Regeln, einschließlich der Verwendung von Active-Directory-Benutzern und -Gruppen.
- Der Agentenstatus-Dialog wurde für macOS und Linux vereinheitlicht.
- Die Laufwerkskontrolle unter macOS unterstützt nun Self-Service-Freigaben. Die automatische Beendigung einer Freigabe bei Benutzerabmeldung wird derzeit noch nicht unterstützt.
- Die Benutzeroberfläche für Laufwerks-Freigabe-Anforderungen auf macOS wurde vereinheitlicht und entspricht nun dem plattformübergreifenden Bedienkonzept. Offline-Freigaben werden auf macOS derzeit nicht unterstützt.
- Die Startzeit des macOS-Agenten wurde optimiert. (Referenz EI-3255)

Rollen und Berechtigungen

- Die Berechtigungen der Rolle „Administrator“ für Infrastruktur- und Servereinstellungen wurden überarbeitet.

1.2.2 Fehlerbehebungen

DriveLock 2026.1 ist eine Hauptversion.

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2026.1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Referenz	Application Control (AC)
EI-3155	Ein Fehler, durch den nachträgliche Änderungen an verschachtelten Filtern von AC-Regeln beim Speichern der Hauptregel wieder verlorengingen, wurde behoben.

	Awareness
EI-3181	Ein Fehler bei der Anzeige von Awareness-Content-Paketen wurde behoben.

	BitLocker Management (BLM)
EI-3112	Nach der Eingabe des BitLocker-Kennworts war es möglich, dass keine Verschlüsselung gestartet oder das Kennwort nicht geändert wurde.
EI-3043	Ein Problem bei der BitLocker-Wiederherstellung über die Schlüssel-ID im DOC wurde behoben, bei dem kein Kennwort für den Zertifikatszugriff eingegeben werden konnte.
	Während der Entschlüsselung von BitLocker-verschlüsselten Partitionen wurde in einigen Fällen das Ereignis 658 (BitLocker-Verschlüsselung wurde ausgesetzt) gemeldet.

	BitLocker Management (BLM)
EI-3035	Ein Fehler wurde behoben, der das Zurücksetzen des BitLocker-Kennwortes über das DOC unmöglich machte.
EI-3201	Ein Fehler wurde behoben, durch das BitLocker-Wiederherstellungszertifikatdateien im DOC nicht verwendet werden konnten.
	Auf den Fehler bei der Kennwortänderung wegen eines eingelegten Installationsmediums wird nun mit einer Fehlermeldung hingewiesen.
	Wurden die Kennwortvoraussetzungen deaktiviert, blieb die Option zur Verwendung eines Wörterbuchs fälschlicherweise aktiviert. Dieses Problem wurde behoben.

	Device Control (DC)
	Ein Problem wurde behoben, durch das Quoten auf Netzwerkfreigaben nicht funktionierten.
	Ein mit der Treiber-Caching-Implementierung in Version 25.1 eingeführtes Problem wurde behoben, bei dem Ereignisse aus Inhaltsprüfungen nur für den zuerst zugreifenden Prozess erzeugt wurden. Die Ereigniserstellung ist nun prozessbezogen, sodass blockierte und erlaubte Zugriffe korrekt abgebildet werden, während das Caching-Verhalten der Inhaltsprüfung unverändert bleibt.
EI-3122	Bei Verwendung eines Defender-Scans in einer Laufwerksregel wurde ein blockiertes Laufwerk nach einem erfolgreichen Scan

	Device Control (DC)
	fälschlicherweise entsperrt. Dieses Problem wurde behoben.
	Wenn bei der temporären Freigabe die Option zum Anzeigen der Verwendungsrichtlinie nicht aktiviert ist, wird jetzt die Verwendungsrichtlinie der eigentlichen Laufwerksregel deaktiviert.
	Ein Problem wurde behoben, durch das die Freigabe eines Remote-Computers über Self-Service nicht funktionierte, wenn ein explizites Benutzerkonto verwendet wurde.

	DriveLock Agent
EI-3072; EI-3071	Die im DriveLock Agent Installer enthaltenen Visual C++-Laufzeitbibliotheken wurden aktualisiert. Dadurch wurde ein sporadisch auftretender Installationsfehler des Agenten mit dem Fehlercode 1603 behoben.
	Die temporäre Freigabe funktioniert jetzt wieder korrekt, wenn die Option „Freigabe beenden, wenn sich der Benutzer abmeldet" aktiviert ist.
EI-3051	Beim Starten des DriveLock Agenten konnte die Lizenzprüfung in seltenen Fällen zu einem Absturz führen.

	DriveLock Database
EI-3073	Ein Fehler wurde behoben, der bei der Installation einer neuen Datenbank im Zusammenhang mit der Abfrage vorhandener

	DriveLock Database
	Datenbankbenutzerrollen auftreten konnte.

Referenz	DriveLock Enterprise Service (DES)
EI-3119	Ein Problem wurde behoben, durch das das Ereignis 787 (Laufwerk blockiert) nicht in der Aktivitätshistorie des Laufwerks angezeigt wurde.
	Die Validierung von Ereignisdaten wurde bei aktivierter Überprüfung der Agentenidentität verbessert, sodass nicht autorisierte Ereignisse nun korrekt abgewiesen werden.
EI-3085	Die Offline-Freigabe funktioniert jetzt wieder korrekt, wenn schwache Challenge/Response-Codes verwendet werden.
	Die Überprüfung der Agentenidentität wurde korrigiert, um unautorisierten Zugriff unter bestimmten Umständen zu verhindern.
EI-3135	Ein Fehler in der DLSetup.exe wurde behoben, der unter bestimmten Umständen zu einem Abbruch der DES-Installation führte.
	DriveLock On-Premise: Ein Sicherheitsproblem wurde behoben, durch das nicht autorisierte Benutzer mittels URL-Manipulation auf Konfigurationsdaten des DES zugreifen konnten.
	Eine Schwachstelle wurde behoben, die unter bestimmten Umständen das Einschleusen von SQL-Code ermöglichte.

Referenz	DriveLock Enterprise Service (DES)
	Auf dem DES wurden beim Zugriff auf lokale Ressourcen zusätzliche Prüfungen integriert, um nicht autorisierte Dateizugriffe zu verhindern.
	Ein potenzieller Absturz im DES während der Initialisierung der Log-Datei wurde behoben.
	Ein Problem bei der Aktualisierung von API Tokens wurde behoben
EI-3157	Ein Fehler wurde behoben, durch den die Weiterleitung bestimmter Application-Control-Ereignisse an einen Syslog-Dienst fehlschlagen konnte.
	Ein Fehler bei den Regeln für die Verarbeitung und Weiterleitung von Ereignissen wurde behoben.
EI-3274	Ein Problem wurde behoben, bei dem der Pfad zur ausführbaren Datei des DriveLock Enterprise Service während der Installation nicht korrekt in Anführungszeichen gesetzt wurde.

Referenz	DriveLock Management Konsole (DMC)
EI-3070	Beim Zugriff auf den Knoten „Richtlinienzuweisungen“ trat eine Fehlermeldung auf, wenn man nicht im Root-Mandanten angemeldet war. Dieses Problem wurde behoben.

Referenz	DriveLock Operations Center (DOC)
EI-3086	Die Offline-Freigabe eines Computers im DOC wurde immer für 135 Minuten angewendet – unabhängig vom ausgewählten Zeitraum. Dieses Verhalten wurde korrigiert.
EI-3068	In der rekursiven Ansicht von Regeln im DOC war nicht erkennbar, welchem Unterordner eine Regel zugeordnet ist. Dieses Problem wurde behoben; optional kann nun eine zusätzliche Spalte mit Ordnerinformationen eingeblendet werden.
EI-3069	Die Aktion „Hinzufügen zu einer Regel“ konnte nicht korrekt ausgeführt werden, wenn sich Regeln innerhalb von Unterordnern einer Richtlinie befanden. In diesem Fall wurden nur Regeln ohne Unterordner angezeigt oder keine. Dieses Problem wurde behoben; die Auswahl zeigt nun auch die Unterordnerstruktur an.
EI-3061	Ein Fehler beim Setzen von Rolleneigenschaften wurde behoben.
	Ein Problem wurde behoben, durch das Benutzer ohne die Rollenberechtigung „Richtlinien-Einstellungen verwalten“ im DOC keine Geräte oder Laufwerke zu Regeln hinzufügen konnten.
	Ein Problem wurde behoben, durch das die Spalten „Erstelldatum“ und „Änderungsdatum“ bei einer großen Anzahl von Regeln leer blieben.
EI-3133	Freigabeanforderungen werden nun unabhängig von der Berechtigung „Ereigniszusatzdaten bearbeiten“ korrekt angezeigt.
	Ein Problem wurde behoben, durch das beim Anlegen einer Anwendungsregel für Linux im DOC keine Aktion ausgeführt wurde.

Referenz	DriveLock Operations Center (DOC)
EI-3143	Ein Problem wurde behoben, durch das in der Liste der Gruppenmitgliedsdefinitionen im DOC nicht nach der Spalte „Name“ gefiltert werden konnte.
EI-3156	Ein Problem wurde behoben, durch das die Seriennummer bei bestimmten Ereignissen beim Hinzufügen eines Geräts zu einer Regel oder beim Neuerstellen einer Regel nicht übernommen wurde.
	Bei Richtlinien mit sehr vielen Versionen war es im DOC unter Umständen nicht möchlich, alte Versionen zu löschen.
EI-3110	Die Spalte "Zeitstempel des letzten Ereignisses" war unter Umständen leer.
EI-3095	Ein Fehler im DOC-Objektauswahldialog wurde behoben, durch den Domänen nicht korrekt angezeigt wurden.
EI-3093	Ein Fehler im DOC-Objektauswahldialog wurde behoben, der bei Benutzern mit eingeschränkten Berechtigungen auftreten konnte.
EI-3226	Ein Anzeigefehler in der Syslog-Konfiguration des DOC wurde behoben, bei dem der Statusschalter nicht korrekt dargestellt wurde.

Referenz	DriveLock Pre-Boot Authentication
EI-3087	Die automatische Anmeldung an der Netzwerk-PBA konnte fehl-

Referenz	DriveLock Pre-Boot Authentication
	schlagen, weil die dazu nötigen Benutzer nicht mehr eingetragen waren.
	Ein Problem wurde behoben, durch das die Installation der DriveLock PBA fehlerhaft sein konnte, wenn in der Richtlinie ein manueller Neustart festgelegt war.
EI-3096	Die Anzahl der Neustarts ohne Anmeldung an der PBA wurde vom DriveLock Agenten in manchen Fällen fehlerhaft interpretiert und im DOC falsch angezeigt.
EI-3162	Nach der automatischen Anmeldung in der Netzwerk-PBA und der anschließenden Anmeldung an Windows konnte es vorkommen, dass das eine automatische Anmeldung mit dem Maschinenkonto weiterhin möglich war.

Referenz	Encryption 2-Go
EI-3125	Ein Problem wurde behoben, durch das das Erstellen eines Containers auf einem mit exFAT formatierten USB-Stick länger dauerte als vorgesehen.

Referenz	File Protection (FFE)
	Beim Kopieren einer Datei aus einem verschlüsselten Netzwerkordner in einen unverschlüsselten Netzwerkordner im Modus „Altes Format“ wurde die Datei nicht entschlüsselt. Dieses Problem wurde behoben.

Referenz	File Protection (FFE)
	Im DOC war es nicht mehr möglich, Benutzer zu zentral verwalteten Ordnern hinzuzufügen.

	Inventarisierung
EI-3121	Ein Problem wurde behoben, durch das Benutzer im DOC nicht der korrekten Active-Directory-Struktur zugeordnet wurden und in der Domain-Spalte ein falscher Wert angezeigt wurde.

	Vulnerability Scan
EI-3145	Ein Fehler beim Synchronisieren von CVE Einträgen wurde behoben.

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 auf Version 2025.2** 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 kommt es auf manchen Computern dazu, dass Geräte nicht gestartet werden können, weil Windows den Drivelock Treiber `DLDevFlt.sys` nicht laden kann. Anscheinend verursacht der "Citrix USB Monitor Driver"

ctxusbmon.sys Probleme beim Entladen des `DLDevFlt.sys`.
Empfohlenes Vorgehen: Eröffnen Sie ein Supportticket bei Citrix.
Mögliche Workarounds bis Citrix das Problem behoben hat:

1. Deinstallieren Sie Citrix Workspace.
2. Da das Problem dadurch verursacht wird, dass `DLDevFlt.sys` nicht entladen werden kann, können Sie versuchen es dadurch zu umgehen, indem Sie den `DLDevFlt.sys` nur verzögert oder gar nicht entladen lassen. Wenn das Problem nur in Fällen besteht, wenn Geräte von DriveLock blockiert werden, so können Sie dies erreichen, indem Sie die Einstellung "Blockierte Geräte im Device Manager deaktivieren" einschalten. Falls DriveLock keine Geräte blockiert oder diese Einstellung keinen Erfolg bringt, können Sie die Einstellung "Entfernung von Geräten melden" verwenden, da hierbei der Treiber geladen bleibt bis das Gerät wieder entfernt wird (bitte beachten Sie die Hinweise bei der Beschreibung dieses neuen Features). (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 Prozess 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 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.

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.

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.

1.3.7 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).

1.3.8 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)

1.3.9 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.

1.3.10 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.

1.3.11 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.

1.3.12 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.

1.3.13 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 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)

1.5 Empfehlungen

1.5.1 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.

1.5.2 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.

1.5.3 Verwendung vertrauenswürdiger Zertifikate

Für die Kommunikation zwischen verknüpften DES-Servern und dem zentralen DES ist ab Version 26.2 die Verwendung vertrauenswürdiger Zertifikate notwendig. Ab dieser Version werden hierfür keine selbst signierten Zertifikate mehr unterstützt. Die Verbindung der Agenten zum zentralen DES ist davon nicht betroffen.

1.6 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	-
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	Support verfügbar
2026.1	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.

1.6.1 Versionsspezifische Abkündigungen

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

Abkündigung von Funktionen:

- 2026.1 ist die letzte Version, in der File Protection auf 32-bit Systemen und auf Windows 7 eingesetzt werden kann.
- 2026.1 ist die letzte Version, in der die DriveLock Mobile Encryption Anwendung (MEA) auf 32-bit Systemen eingesetzt werden kann.
- 2026.1 ist die letzte Version, in der SHA-224 als Hash-Algorithmus eingesetzt werden kann.
- 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 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.
- 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	Linux	Mac OS
Drive Control	✓	✓	◒	◒
Device Control	✓	✓	◒	✕
Application Control	✓	✓	◒	✕
Application Behavior Control	✓	✓	◒	✕
Containerverschlüsselung (Encryption 2-Go)	✓	✓	◒	◒
BitLocker To Go	✓	✓	✕	✕
BitLocker Management	✓	✓	✕	✕
Security Awareness Multimedia-Kampagnen	✓	✓	✕	✕

Feature	Betriebssystem / Funktionen			
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.

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\Cur-`

```
rentCon-
trolSet\Con-
trol\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Server]"Enabled"=dword:00000001
```

- `[HKEY_LOCAL_MACHINE\SOFTWARE\Mi-`
  `cro-`
  `soft\Win-`
  `dows\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 2026.1 Patch 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 (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