DriveLock Release Notes

Release Notes 2025.1

DriveLock SE 2025

Inhaltsverzeichnis

1 DriveLock Release Notes 2025.1

Build: 2025.1.2.57596

Datum: 16.06.2025

Die DriveLock Release Notes enthalten wichtige Informationen zu Neuerungen, Änderungen und Fehlerbehebungen in der Hauptversion 2025.1, 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 2025.1 befindet sich im Kapitel **Was ist neu?** in der DriveLock Dokumentation auf DriveLock Online Help.

> Achtung: Die Hauptversion 2025.1 enthält grundlegende Backend-Änderungen, die das Systemverhalten erheblich beeinflussen können. Wir raten unseren Kunden daher nachdrücklich, ihre individuellen Anwendungsfälle vor dem Produktiveinsatz eingehend zu testen.

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 Auflistung der in 2025.1 enthaltenen Neuerungen, Verbesserungen und Änderungen

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

Hinweis: 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.

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)

- Neu im DOC: Regeln zur Anwendungs- und Verhaltenskontrolle können nun festlegen, ob Ereignisse generiert werden.
- Der Dateipfad-Filter in AC-Regeln verwendet jetzt immer einen Wildcard-Vergleich; bestehende Regeln werden automatisch konvertiert.
- ⚠ Der Dateipfad-Filter in AC-Regeln unterstützt jetzt mehrere Werte (Pfadangaben). Bei der Auswertung muss einer der angegebenen Pfade zutreffen. Bitte beachten Sie, dass dies nicht mit älteren Agenten kompatibel ist!

BitLocker Management

- Laufwerksübersicht im DOC: Eine vorübergehende Aussetzung der BitLocker-Verschlüsselung wird jetzt für Partitionen angezeigt.

Device Control (DC)

- Während des Lernvorgangs für angeschlossene Geräte können jetzt Ereignisse erzeugt werden – auch unter Linux.
- Das Neulernen von Geräten kann direkt im DOC angestoßen werden. Auch unter Linux einstellbar.

- Geräteklassen können nun Benutzerberechtigungen enthalten.
- Das Auslösen eines Ereignisses beim Entfernen eines Geräts kann nun pro Geräteklasse konfiguriert werden.
- DriveLock-Benutzergruppen können für MTP-Geräte verwendet werden.
- Die Ereignisanzeige in der DOC-Regelansicht wurde verbessert.
- Archiv-Scans unterstützen jetzt neben ZIP und RAR auch 7z.
- Audit-Ereignisse für Dateioperationen werden reduziert – nur ein Ereignis pro Benutzer/Prozess/Zugriffstyp.

DriveLock Agent

- Erweiterte Duplikaterkennung: Einzelne Parameter können jetzt bei der Duplikatsprüfung ausgeschlossen werden.
- Das Einsammeln von Benutzerzertifikaten während der AD-Inventarisierung kann nun optional deaktiviert werden. (EI-2891)

DriveLock Enterprise Service (DES)

- Entra-ID-Gruppen synchronisieren jetzt auch bei Namensduplikaten; das Objekt mit höherer Object-ID bleibt.
- Zeitstempel werden jetzt im eindeutigen ISO-8601-Format exportiert.
- Granularere Konfiguration der Active-Directory-Synchronisation: Objekte können nun auch per DistinguishedName gefiltert werden.
- Der Server-Installationsassistent erlaubt nur noch Datenbank-Sortierungen ohne Unterscheidung von Groß- und Kleinschreibung. Sortierungen, die diese Unterscheidung berücksichtigen, werden nicht unterstützt.

File Protection

- Neue Option ‚Symbol für verschlüsselte Dateien anzeigen' zeigt jetzt ein Overlay für verschlüsselte Dateien.

DriveLock Operations Center (DOC)

- ⚠ Einige der globalen Einstellungen aus der DMC können jetzt direkt im DOC konfiguriert werden. Beachten Sie, dass Agenten vor Nutzung aktualisiert werden sollten.
- Gemeldete Mitglieder einer Gruppe können jetzt auch im DOC exportiert werden.
- Im DOC wurden einige neue Widgets für Vulnerability Scan hinzugefügt.

- Im DOC wurden bei den Filterkriterien für dynamische Gruppen die Option „Registry-Schlüssel existiert“ (Ja/Nein) hinzugefügt.
- Das Active Directory Inventar kann jetzt im DOC neu geladen und der Objekt-Auswahl-Dialog aktualisiert werden.
- Eigene und öffentliche Berichte können jetzt dupliziert und bearbeitet werden.
- Im DOC werden nun nur Regeln im ausgewählten Ordner angezeigt. Mit der entsprechenden Einstellung werden auch Unterordner-Regeln angezeigt.
- Es ist jetzt möglich, nach mehreren Spalten zu sortieren, indem die Shift-Taste gedrückt und auf die Spaltenüberschriften geklickt wird.
- In der Computer-Detailansicht wird nun die Liste aller Alerts angezeigt, die diesem Computer zugeordnet sind. Unter 'Zugehörige Objekte' wird zusätzlich die Anzahl der Alerts aufgeführt.
- Das Computer-Kontextmenü wurde neu strukturiert und in Kategorien gegliedert.
- Die Multifaktor-Authentifizierung (MFA) kann nun rollenbasiert erzwungen werden. Zusätzlich ist es möglich, die MFA-Abfrage bei jeder Anmeldung verpflichtend zu machen. (EI-2632)
- Dashboards können jetzt Rollen zugeordnet werden – Benutzer erhalten sie automatisch entsprechend ihrer Rolle.
- Dashboard- und Widget-Vorlagen können jetzt zentral verwaltet werden:
  - Integrierte Vorlagen (nur lesbar)
  - Eigene Vorlagen voll bearbeitbar (Erstellen, Lesen, Ändern, Löschen - 'CRUD'-Funktionalität)
- Benutzer können Dashboard-Tabs hinzufügen, umsortieren und entfernen.
- Widget-Daten werden jetzt standardmäßig für 300 Sekunden gecacht – mit Option zur Deaktivierung pro Tab.
- Automatische Aktualisierung von Widgets: Benutzer können für jeden Dashboard-Tab festlegen, ob Widgets ihre Daten automatisch aktualisieren sollen. Die Aktualisierung erfolgt nicht gleichzeitig für alle Widgets.

DriveLock API

- Die DriveLock API bietet jetzt neue Funktionen zum Zurücksetzen der Agenten-ID und zur Vorbereitung einer Neuinstallation durch einmalige Änderung der Agenten-ID.

- Die DriveLock API unterstützt jetzt das Markieren eines Computers als Basis-Image, um Konflikte mit Agenten-IDs bei geklonten Systemen zu vermeiden.

DriveLock Ereignisse

- Die Konfiguration von Ereignissen kann jetzt auch im DOC vorgenommen werden.

DriveLock Richtlinien

- ⚠ Die Ausführung der Richtlinienlöschung erfolgt jetzt richtlinienweise. Dadurch können bestimmte Richtlinien – etwa besonders restriktive – erhalten bleiben, auch wenn ein Rechner über einen längeren Zeitraum offline war.
- Der Agent prüft keine Richtliniensignaturen mehr; die Signierung kann in der MMC deaktiviert werden. Siehe EoL-Ankündigungen.

Linux Agent

- Es ist jetzt möglich, Einstellungen für den Proxyserver direkt auf dem Linux Agenten setzen.
- Beachten Sie, dass das IgelOS 12.5-Basissystem jetzt Voraussetzung für die einwandfreie Funktion der DriveLock IgelOS App 25.1 ist.
- Linux Agenten unterstützen jetzt die Anzeige und Bestätigung von Verwendungsrichtlinien mit Kennwortoptionen.
- Linux Agenten können jetzt die Freigabe von gesperrten Laufwerken und Geräten anfordern.

Lizenzierung

- Für die Online-Aktualisierung von Lizenzen gibt es jetzt neue Lizenzeinstellungen.
- Benutzersitzungen auf Terminalservern gehen jetzt nicht mehr in die Lizenzzählung ein. Die neue Spalte „Terminal Server-Computer“ zeigt die Anzahl der gemeldeten Terminalserver mit aktivem Agenten.

macOS Agent

- Auf macOS wurden zusätzliche Optionen für Encryption2-Go hinzugefügt, z. B. Admin-Kennwort, Datensicherung, Speicherplatzfüllung und automatisches Mounten.
- macOS Agenten können jetzt die Freigabe von gesperrten Laufwerken anfordern.
- macOS Agenten unterstützen jetzt die Anzeige und Bestätigung von Verwendungsrichtlinien mit Kennwortoptionen.

Self-Service

- Im Self-Service-Assistent können Benutzern jetzt vordefinierte Gründe zur Auswahl angeboten werden.

Vulnerability Management

- Das Herunterladen der Schwachstellenkataloge für Agenten, deren Internetverbindung nicht stabil ist, sowie das Melden der Ergebnisse an den DES wurden verbessert. (EI-2480)

1.2 Fehlerbehebungen

DriveLock 2025.1 ist eine Hauptversion.

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2025.1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

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

	Application Control (AC)
EI-2886	Bei Setzen der Eigenschaft "Dauer der Lernphase für das lokale Lernen" in der DriveLock Management Konsole (DMC) wurde der gesetzte Wert in der Liste falsch angezeigt - z.B. "604800 Tage" statt "7 Tage".
EI-2653	Es wurde ein Workaround gefunden für einen Fehler im Anti-Keylogger-Treiber des Omnissa Horizon Clients, durch den der Horizon Client nicht gestartet werden konnte, wenn AC aktiv war.

	BitLocker Management (BLM)
EI-2970	BitLocker-Wiederherstellungsschlüssel im DOC waren für einige Administratoren nicht auslesbar. Dieses Problem ist nun behoben.
	In seltenen Fällen wurden lokal zum Hochladen auf den DES gespeicherte Wiederherstellungsdaten entweder nicht erstellt oder nach dem Erstellen entfernt. Das führte dazu, dass auch das Auslösen eines erneuten Hochladevorgangs im DOC fehlschlug.
	Nach der Wiederaufnahme einer pausierten Verschlüsselung war

	BitLocker Management (BLM)
	es möglich, dass auch externe Festplatten verschlüsselt wurden.
EI-2873	Allein durch die Zuweisung einer BLM-Lizenz wurden Windows-Richtlinien für BitLocker geändert, wodurch die Funktionalität einer parallel installierten BitLocker-Management-Lösung unter bestimmten Umständen eingeschränkt oder verhindert wurde.
	Nach der Installation der DriveLock PBA und der Verschlüsselung der Systempartition wurde die BitLocker-Verschlüsselung bis zum nächsten Neustart vorübergehend ausgesetzt.
	Die Wiederherstellung von BitLocker und BitLocker To Go über die API funktioniert jetzt wieder, wenn die Wiederherstellungsdaten über eine Protector-ID referenziert werden.

Referenz	BitLocker To Go
	Im Kontextmenü des Agenten fehlten einige Icons (BitLocker To Go).
	Ereignis 111 wurde auch dann gemeldet, wenn ein leerer SD-Kartenleser vorhanden war und BitLocker To Go mit erzwungener Verschlüsselung konfiguriert war.

	Datenbank
EI-2919	Ein Fehler wurde behoben, bei dem die Lizenzauswertung im DOC zu Datenbank-Sperren führen konnte, wenn der Server

	Datenbank
	unter hoher Last stand.

	Device Control (DC)
EI-2971	Der Fehler, dass unkontrollierte MTP-Geräte von Device Control geblockt wurden, ist behoben.
	Bei Geräten mit mehreren Hardware-IDs wurden alle außer der ersten ID ignoriert.
	Bisher wurde das Umbenennen einer Datei nur dann verhindert, wenn dabei eine erlaubte Datei in eine gesperrte Erweiterung umbenannt wurde. Dieses Verhalten wurde erweitert: Ein Umbenennen wird nun auch dann blockiert und rückgängig gemacht, wenn es zu einem Inhaltskonflikt führen würde.
	Beim Erstellen einer Geräte-Regel in der DMC wurden beim Browsen nach einem installierten Gerät nur die erste kompatible ID übernommen. Die übrigen kompatiblen IDs wurden ignoriert.
	Wenn keine erzwungene Verschlüsselung mit Encryption 2-Go oder BitLocker To Go eingestellt war, wurde der Eintrag 'Verschlüsseln' nicht im Kontextmenü für dieses Laufwerk angezeigt.
	Performance-Probleme (z.B. keine Reaktion oder Absturz des Computers), die durch wiederholtes Öffnen und dadurch wiederholtes Scannen der gleichen Datei im Kontext eines einzelnen Benutzeraufrufs provoziert wurden sind behoben.

	Device Control (DC)
	Änderungen durch Lese-, Schreib-, Umbenennungs- oder ähnliche Anforderungen, die bereits vor dem Inhalts-Scan wirksam wurden und im Scan als unerwünscht erkannt werden, werden nun zuverlässiger zurückgenommen.

Referenz	DriveLock Enterprise Service (DES)
EI-2907	Es wurde ein Fehler beim E-Mail-Versand behoben, der auftrat, wenn der Text Zeilenumbrüche enthielt. Dies betraf hauptsächlich den Versand von Benachrichtigungs-E-Mails für Ereignisse von Drittanbietern vom Server aus.
EI-2853	Ein Fehler wurde behoben, bei dem das Hinzufügen eines Laufwerks oder Geräts zu einer Regel nicht korrekt als letzte Aktion für das Laufwerk oder Gerät angezeigt wurde.
EI-2900	Die Auswertung der Lizenznutzung für Computer, die über die API gelöscht wurden, wurde korrigiert.
	Änderungen am Loglevel über das DesTray wirken sich nur auf den aktuell laufenden DES-Dienst aus. Um die Einstellungen dauerhaft zu übernehmen, verwenden Sie bitte die Option im DOC unter *Backend -> Server -> Allgemein -> Debug-Tracing*

Referenz	DriveLock Management Konsole (DMC)
EI-2823	Die DMC hat beim Lesen lokaler Laufwerke für Laufwerksregeln keine Leerzeichen von Hersteller- und Produkt-ID entfernt.

Referenz	DriveLock Operations Center (DOC)
	Beim Editieren einer bestehenden Richtlinienzuweisung konnte keine andere Richtlinie ausgewählt werden, wenn zuvor nicht die Spalte 'Richtlinientyp' eingeblendet worden war.
EI-2856	Im DOC fehlte der Eintrag 'Verschlüsselung' im Navigationsmenü wenn nur BitLocker 2 Go als Verschlüsselungsmodul in der Lizenz vorhanden war.
	Das Exportieren von Listen ist nicht mehr größenbeschränkt und funktioniert somit auch für den Export von sehr vielen Listeneinträgen.

Referenz	DriveLock Pre-Boot Authentication
EI-2799	Der Challenge/Response-Code für den PBA-Notfall-Login ohne Benutzernamen blieb bisher nach der Verwendung unverändert, wenn die SSO-Richtlinie deaktiviert war. Dieses Verhalten wurde korrigiert.

Referenz	Encryption 2Go
EI-2757	Der unverschlüsselte Zugriff auf Laufwerke wurde nur bis zur folgenden Aktualisierung der Konfiguration ermöglicht.

Referenz	File Protection (FFE)
EI-2681	Ein Fehler bei der Cache-Verwaltung im alten FFE-Format, der zu einer Verletzung der gemeinsamen Nutzung mit dem Foxit PDF Creator Snap-In führte, wurde behoben.
EI-2911	Ein Leistungsproblem beim Anmelden an einer RDP-Terminalserver-Sitzung in Kombination mit FSLogix wurde behoben.
	Wenn der FFE-Modus „Altes Format“ in Windows 11 24H2 verwendet wird, erzeugen ältere DriveLock-Versionen einen BSOD in FltMgr.sys, wenn sie auf verschlüsselte Ordner zugreifen. Dieser BSOD wird vom DL FFE-Treiber ausgelöst und ist behoben. (Microsoft gibt an, dass die Änderung, die nicht berücksichtigt wurde, bereits mit Windows 11 22H2 eingeführt wurde, wir sehen den BSOD jedoch nur mit Windows 11 24H2.) Zur Vermeidung von Fehlern aufgrund zukünftiger Erweiterungen der Windows-Struktur FSRTL_ADVANCED_FCB_HEADER halten wir uns jetzt an eine Version dieser Struktur, die unseren Anforderungen entspricht.

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.

BitLocker Management-Verschlüsselungszertifikate

- Die Aufgabe ‚Zertifikat exportieren' erzeugt falsche Dateinamen beim Export von Verschlüsselungszertifikaten aus einer BitLocker Management-Richtlinie.

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 Device Control

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).

Quotierung /Dateifilter-Vorlagen

- Auf dem Reiter Quotierung werden die geschriebenen bzw. gelesenen Bytes pro Zeiteinheit gezählt, nicht die eigentlichen Dateien. Daher wird die Erstellung neuer Dateien mit 0 Bytes nicht blockiert.
- 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

- Wenn eine im Dateifilter ausgeschlossene Datei in eine Archiv-Datei kopiert wird, wird die komplette Archiv-Datei gelöscht. Wir empfehlen, Archiv-Dateien nicht direkt auf den kontrollierten Volumes zu bearbeiten, sondern auf der lokalen Festplatte, wo i.d.R. kein Dateifilter gesetzt ist. (Referenz EI-2651)
- 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-2650)
  - 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. (Referenz DL-7643)

  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.

Device Control im DOC

- Im DOC unter Sicherheitskontrollen -> Laufwerke -> Ereignisse fehlt die Anzeige für das Ereignis 120: Serielle Schnittstelle gesperrt.
- Beim Erstellen von Geräte-Regeln für manche Ereignisse (z.B. EventId120) kann es vorkommen, dass die Informationen aus den Parameter des Ereignisses (z.B. Hardware ID) nicht korrekt in die Regel übernommen werden.

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).

1.3.4 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.

1.3.5 DriveLock Enterprise Service (DES)

Registrierung von verknüpften DES

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

1.3.6 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)

1.3.7 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.

1.3.8 Erzwungene Verschlüsselung

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.

1.3.9 File Protection

Microsoft OneDrive

- Mit Microsoft OneDrive kann Microsoft Office Dateien direkt mit OneDrive synchronisieren, ohne die Dateien zuerst in den lokalen Ordner zu speichern. In dem Fall ist der DriveLock Verschlüsselungstreiber nicht involviert und die Office-Dateien werden in der Cloud nicht verschlüsselt. Um dieses Verhalten zu unterbinden, wählen Sie **"Office 2016 nutzen, um Dateien, die ich öffne, zu synchronisieren"** oder ähnliche Einstellungen in OneDrive ab. Es muss eingestellt werden, dass Office-Dateien, wie auch andere Dateien immer lokal gespeichert werden.
- Das Löschen verschlüsselter Ordner im lokalen OneDrive-Verzeichnis kann unter Umständen dazu führen, dass ein leerer Ordner übrig bleibt.

FireEye

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

NetApp

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

Windows 10-Clients mit Kaspersky Endpoint Security 10.3.0.6294

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

Zugriff auf verschlüsselte Ordner

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

- File Protection kann nicht verwendet werden, wenn sich der verschlüsselte Ordner in einem verschlüsselten Container befindet.

Kopieren von Daten auf einen mit neuem Format verschlüsselten Netzwerkordner

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

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.

1.3.10 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.

1.3.11 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.

1.3.12 Thin Clients

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

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

1.4 End-Of-Life-Ankündigungen

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

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

Version	On-Premise-Kunden-Support besteht bis:	Cloud-Kunden-Support besteht bis:
Alle Versionen vor 2022.2	EoL - kein Support mehr	EoL - kein Support mehr
2022.2	Juni 2025	EoL - kein Support mehr
2023.1	kein Entwicklungssupport mehr *1 Produktsupport *2 : Juni 2025	EoL - kein Support mehr
2023.2	Entwicklungssupport *1: Juni 2025 Produktsupport *2 : Dezember 2025	EoL - kein Support mehr
2024.1	Entwicklungssupport *1: Dezember 2025 Produktsupport *2 : Juni 2026	EoL - kein Support mehr
2024.2	Entwicklungssupport *1: Juni 2026 Produktsupport *2 : Dezember 2026	Bis zum Release einer auf 2025.1 folgenden Version
2025.1	derzeit aktuelle Version	derzeit aktuelle Version

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

Support-Lebenszyklus:

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

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

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

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

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

Upgrades:

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

Abkündigung von Funktionen:

- Mit Version 2025.1 werden keine Richtliniensignaturzertifikate mehr geprüft.
- Version 2025.1 ist die letzte Version, welche die in der DriveLock Management Konsole (DMC) verfügbare Energieverwaltung unterstützt.

Hinweis: **TLS 1.2**: Bitte stellen Sie sicher, dass alle Betriebssysteme, auf denen DriveLock eingesetzt wird, ab sofort TLS1.2 unterstützen.

2 Systemvoraussetzungen für den Betrieb von DriveLock

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

2.1 DriveLock Agent

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

Betriebssystem	Versionen
Windows 11	Ab 21H2, nur Editionen Pro / Enterprise
Windows 10	Ab 20H2, nur Editionen Pro / Enterprise
Windows 10 LTSC	alle LTSC-Versionen bis Ablauf des jeweiligen Extended Support
Windows Server	2016, 2019, 2022
Windows 7	Windows 7 SP1 Enterprise / Ultimate mit Extended Support. Hinweis: Eine zusätzliche Legacy Support Lizenz wird für den Betrieb auf Windows 7 Systemen benötigt.
Linux	Debian 12, Fedora 40, IGEL OS 11.05, Red Hat Enterprise Linux 5, SUSE 15.4, Ubuntu 24.04, AlmaLinux OS 9.4 oder neuere Versionen Voraussetzung für die einwandfreie Funktion der DriveLock IgelOS App 25.1 ist das IgelOS 12.5-Basissystem.
macOS	ab Version Ventura (Version 13) mit Intel (x86_64) und Apple Silicon (arm64) Architekturen

Der Windows DriveLock Agent ist grundsätzlich verfügbar für AMD-/Intel X86-basierte Systeme (32-Bit und 64-Bit Architektur). Für den Einsatz des DriveLock Agenten wird ein 64-Bit System empfohlen. Server-Betriebssysteme werden ausschließlich unter 64-Bit unterstützt. Einschränkungen der einzelnen Funktionen sind weiter unten beschrieben.

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

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

Vollständiger Funktionsumfang: ✓

Reduzierter Funktionsumfang: ◒

Keine Unterstützung:✕

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

Feature	Betriebssystem / Funktionen				
Vulnerability Management	✓	✓	✓	✕	✕
Security Configuration Management	✓	✓	✓	✕	✕
Disk Protection	✓(*)	✕	✕	✕	✕
File Protection	✓	✓	◒	✕	✕

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

Hinweis: Security Awareness: Bitte beachten Sie, dass ab Version 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.

Hinweis: Für File Protection wird ab Version 2024.1 das aktuelle Microsoft Visual C++ Redistributable vorausgesetzt. Folgen Sie bitte diesem Download-Link.

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

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

2. **Einschränkungen Windows 7**

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

   - Generell:
     - Nach einem Update, einer Installation oder Deinstallation des DriveLock Agenten unter Windows 7 x64 stürzt der Explorer (explorer.exe) möglicherweise ab. Dies tritt nur dann auf, wenn die Windows-Eingabeaufforderung mit Admin-Rechten geöffnet und das System seit dem Update/Installation/Deinstallation des Agenten nicht neu gestartet wurde.
     - KB3140245 muss auf Windows 7 installiert sein
       Weitere Informationen dazu finden Sie unter 'Update-Prozess' und 'Update-Katalog'.
       Ohne dieses Update kann WinHTTP keine TLS Einstellungen ändern und der Fehler 12175 erscheint in dlwsconsumer.log und DLUpdSvx.log.
     - KB3033929 (SHA-2 code signing support) muss auf Windows 7 64-bit installiert sein.
     - DriveLock Service ergänzt fehlende Registry-Werte für TLS 1.2 Verbindungen auf Computern mit Windows 7.
       Folgende Registry-Werte sind neben dem KB3140245 die Voraussetzung für die Kommunikation mit dem DES:
       - `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]"Enabled"=dword:00000001`
       - `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]"Enabled"=dword:00000001`
       - `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\WinHttp] "DefaultSecureProtocols"=dword:00000800`

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

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

3. **Einschränkungen macOS**
   - Device Control:
     - Keine Freigabe für bestimmte Benutzer oder Benutzergruppen
     - Kein Dateifilter und Auditing
     - Keine Freigabe von bereits mit Encryption 2-Go verschlüsselten Laufwerken
     - Keine Self-Service Funktionalität
   - Encryption 2-Go:

- Für macOS steht wie bisher für die Entschlüsselung von externen USB-Laufwerken die Mobile Encryption Application (MEA) zur Verfügung.
- Der macOS-Agent 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-Agent entnehmen Sie bitte dem Themenblock macOS in der DriveLock Online Dokumentation.

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

   Weitere Informationen zum Linux Client und den Limitierungen der Funktionalität entnehmen Sie bitte 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 2025.1 wurde getestet und freigegeben auf den aktuellen Ständen der 64-bit Windows-Versionen, die zum Zeitpunkt des Release offiziell verfügbar waren und die bei Microsoft das Ende des Service-Zeitraumes noch nicht erreicht haben. Im Kapitel DriveLock Agent finden Sie eine Auflistung der Windows Versionen, die DriveLock unterstützt.

2.3 DriveLock Enterprise Service

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

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

Hauptspeicher / CPU:

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

Freier Festplattenspeicherplatz:

- mind. 4 GB, bei der Verwendung von Security Awareness Content (Video) wird ein freier Speicher von mind. 15 GB empfohlen.

- Soll auf dem Server gleichzeitig noch eine SQL-Datenbank betrieben werden, sind zusätzlich zu der dafür notwendigen Festplattenkapazität auch noch mind. 10 GB für die Speicherung der DriveLock Daten vorzusehen.

Benötigte zusätzliche Windowskomponenten:

- .NET Framework 4.8 oder höher ist Voraussetzung für die Installation!
- .NET 8.0 Runtime (Microsoft Download Link)
- ASP.NET 8.0 Core Runtime (Microsoft Download Link)
- .NET Desktop Runtime 8.0 (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.

Port	Verwendung
4568	Dieser Port wird hauptsächlich für das DriveLock Operations Center (DOC) verwendet.
6066; 6067	Diese Ports werden für die Übertragung von Management- und Statusinformationen der Agenten verwendet.

Unterstützte Plattformen:

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

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

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

Unterstützte Datenbanken:

- DriveLock benötigt ab Version 2024.1 mindestens SQL Server 2016 SP1 oder neuer. Die Datenbank muss einen Kompatibilitätsgrad von 130 oder höher haben.
- SQL-Server Express 2016 oder neuer für Installationen mit bis zu 200 Clients und Testinstallationen
- Der DES benötigt den **Microsoft SQL-Server 2012 Native Client Version 11.4.7001.0**. Ist diese Komponente noch nicht installiert, geschieht dies automatisch vor der eigentlichen Installation des DES. Wenn eine ältere Version bereits installiert ist, wird diese automatisch aktualisiert.

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

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

2.4 DriveLock Operations Center (DOC)

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

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

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

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

3 Security Bulletins

3.1 Security Bulletin #22-001 - ZLIB external library vulnerability

First published: **21th April 2022**

Last updated: **3rd June 2022**

Severity: **Low**

Summary

A vulnerability has been found in the implementation of the ZLIB library. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- DriveLock 2019.2
- DriveLock 2020.2
- DriveLock 2021.1
- DriveLock 2021.2
- DriveLock 2022.1

Description

The detected vulnerability in ZLIB before version 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. DriveLock uses this library mainly to decompress previously packed files, which doesn't affect security due to the nature of this vulnerability.

The DriveLock Support Companion uses the library to pack all collected DriveLock log data files into a single ZIP file. If one of these files would have been manipulated to make use of the detected vulnerability, this would only cause the DriveLock Support Companion to crash.

A full list of related CVEs is available listed in the following section.

References

- NIST: https://nvd.nist.gov/vuln/detail/CVE-2018-25032

Mitigation

This vulnerability can be mitigated by not using the DriveLock Support Agent to collect all trace files or use the DOC to collect and upload the trace files.

How to update your environment

A patch for DriveLock 2022.1 and our latest long-term support release 2021.2 has been released. Customers can update their DriveLock agents to one of these two versions.
We recommend to always use the latest available version.

3.2 Security Bulletin #22-002 - Log4net external library vulnerability

---

First published: **4th July 2022**

Last updated: **4th July 2022**

Severity: **Low**

Summary

A vulnerability has been found in the implementation of the Log4net library. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- DriveLock 2020.2
- DriveLock 2021.1
- DriveLock 2021.2
- DriveLock 2022.1

Description

Apache log4net versions before 2.0.10 do not disable XML external entities when parsing log4net configuration files. This allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files.

DriveLock uses Log4Net to create log files for the client security awareness viewer component and the DES.

A full list of related CVEs is available listed in the following section.

References

- NIST: https://nvd.nist.gov/vuln/detail/CVE-2018-1285

Mitigation

This vulnerability can be mitigated by explicitly limit access to the XML configuration files (read only).

How to update your environment

Beginning with our next long-term support release 2022.2 DriveLock will use an updated version 2.0.14 for creating log files with Log4Net. Customers can update to this version as soon as it has been released.

3.3 Security Bulletin #22-003 - DotNetZip.Semvered external library vulnerability

---

First published: **4th July 2022**

Last updated: **4th July 2022**

Severity: **Low**

Summary

A vulnerability has been found in the implementation of DotNetZip.Semvered before 1.11.0. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- DriveLock 2020.2
- DriveLock 2021.1
- DriveLock 2021.2
- DriveLock 2022.1

Description

DotNetZip.Semvered before 1.11.0 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.

The DriveLock security awareness component and the DES use this component to unzip content, which was previously packed by DriveLock itself.

A full list of related CVEs is available listed in the following section.

References

- NIST: https://nvd.nist.gov/vuln/detail/CVE-2018-1002205

Mitigation

Beginning with our next release 2022.2 DriveLock will use a different library for handling ZIP files. Customers can then update to this version.

How to update your environment

All customers can update their environment as soon our new version DriveLock 2022.2 has been officially released.

3.4 Security Bulletin #22-004 - Node.js external library vulnerability

---

First published: **13th July 2022**

Last updated: **13th July 2022**

Severity: **None**

Summary

A vulnerability has been found in the implementation of Node.js. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- DriveLock 2020.2
- DriveLock 2021.1
- DriveLock 2021.2
- DriveLock 2022.1

Description

The detected vulnerabilities in in Node.js allow execution of arbitrary code by a remote & anonymous attacker, which can be used to manipulate or circumvent security mechanisms.

The vulnerabilities **CVE-2022-32212**, CVE-2022-32213, CVE-2022-32214, CVE-2022-32215, CVE-2022-32222, **CVE-2022-32223** are collected in WID-SEC-2022-0621, the vulnerabilities with classification “High” are written in bold.

CVE-2022-32212: Only vulnerable via the command-line switch `node --inspect`, which enables the debugging interface of node and is not used by the DES server. It's not possible

to pass arbitrary arguments to the node runtime for a remote user, therefore this vulnerability cannot be exploited.

CVE-2022-32213, CVE-2022-32214, CVE-2022-32215: HTTP Request Smuggling is not possible because the node http api is behind a reverse proxy which does its own header parsing and validation.

CVE-2022-32222: Not applicable because it only affects Linux systems and the attacker would need local access to the DES.

CVE-2022-32223: The attacker needs local access to the DES server and needs write access to the DES service's user profile. Using the DES server alone, there is no way to exploit this remotely.

References

- BSI: https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2022-0621
- Node.js: https://nodejs.org/en/blog/vulnerability/july-2022-security-releases/

Mitigation

Drivelock cannot be targeted using these exploits.

How to update your environment

Customers do not need to update their environment.
Nevertheless we always recommend to use the latest available version.

3.5 Security Bulletin #22-005 - OpenSSL 3.0 external library vulnerability

---

First published: **4th November 2022**

Last updated: **4th November 2022**

Severity: **None**

Summary

Two vulnerabilities have been found in the implementation of OpenSSL. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- No DriveLock product is affected

Description

The detected vulnerabilities (CVE-2022-3602 and CVE-2022-3786) in OpenSSL allow execution of arbitrary code using a buffer overrun which can be triggered in X.509 certificate verification, specifically in name constraint checking.

References

- OpenSSL: https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/
- NIST: https://nvd.nist.gov/vuln/detail/CVE-2022-3602
- NIST: https://nvd.nist.gov/vuln/detail/CVE-2022-3786

Mitigation

Drivelock cannot be targeted using these exploits.

How to update your environment

Customers do not need to update their environment.
Nevertheless we always recommend to use the latest available version.

Copyright