DriveLock Release Notes

Release Notes 2023.1HF1

DriveLock SE 2023

Inhaltsverzeichnis

1 Konventionen

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

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

Hinweis: Hinweise und Tipps enthalten nützliche Zusatzinformationen.

Menüeinträge oder die **Namen von Schaltflächen** sind fett dargestellt.

Kursive Schrift repräsentiert Felder oder Titel von referenzierten Dokumenten.

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

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

2 Informationen zu 2023.1 HF1

In den Release Notes finden Sie wichtige Informationen zu Fehlerbehebungen in der Hotfix-Version 2023.1 HF1 und zu Neuerungen, Verbesserungen und Fehlerbehebungen in der Hauptversion 2023.1. Ebenfalls enthalten sind Systemvoraussetzungen, bekannte Einschränkungen und weitere wichtige Ankündigungen.

Die gesamte DriveLock Dokumentation, sowie Links zu den Release Notes der vergangenen und noch unterstützten Versionen finden Sie auf DriveLock Online Help.

> Hinweis: Beachten Sie bitte, dass einige Informationen in diesen Release Notes nur für DriveLock On-Premise relevant sind.

3 Version 2023.1

3.1 Hotfix-Version HF1 (Build 23.1.3)

3.1.1 Fehlerbehebungen 2023.1 HF1

DriveLock 2023.1 HF1 ist eine Hotfix-Version.

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2023.1 HF1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

Referenz	Defender Management
EI-2514	Wenn für die DriveLock Ereignisse 684 und 697 die Option "Ereignisse speichern mit E-Mail" gesetzt war, wurden in manchen Fällen für gefundene Bedrohungen weder Ereignisse generiert noch E-Mails versendet.

Referenz	Device Control
EI-2513	Wenn keine Verbindung zum AD-Controller verfügbar war, konnte die Ereignisverarbeitung sehr langsam werden und zu Zeitüberschreitungen führen, wenn die Dateien auf Übereinstimmung mit dem Dateifilter geprüft wurden.

Referenz	Disk Protection
EI-2491	Der Windows-Boot blieb hängen, wenn eine Disk Protection-Entschlüsselung mit aktiviertem Netzwerk-Pre-Boot durch einen Neustart unterbrochen wurde.

Referenz	DriveLock Agent
EI-2506	Nach der Aktualisierung des Agenten waren einige verbundene Geräte je nach Konfiguration der Gerätesteuerung manchmal deaktiviert.

Referenz	DriveLock Operations Center (DOC)
	Die Funktionalität zum Anzeigen der Kennwörter von lokalen Benutzern funktionierte nicht, wenn man in der Richtlinie für die Benutzer keinen vollen Namen ('full name') eingetragen hatte.
	Wenn man aus einem Ereignis eine Laufwerksregel erstellen wollte, waren die Felder im Dialog (Hersteller-ID, Produkt-ID, Hardware-ID, Seriennummer) noch nicht mit den entsprechenden Werten aus dem Ereignis befüllt.

Referenz	DriveLock Richtlinien
	Unter Umständen konnte es passieren, dass die im DOC erzeugten Anwendung-/Laufwerksregeln verschwanden. Dies geschah, wenn die Standardrichtlinie in der DMC veröffentlicht wurde und z.B. im Namen oder im Kommentar einer Regel ein | vorkam.

Referenz	SB-Freigabe
	Bei der SB-Freigabe wurde der Assistent für die erzwungene Verschlüsselung angezeigt. Dieser Fehler ist jetzt behoben.

3.2 Hauptversion

3.2.1 Neuerungen

Verbessertes DOC-Design und Benutzerführung

- Das DriveLock Operations Center hat sowohl eine neue Struktur als auch ein neues Look & Feel. Die Menüstruktur ist an die DriveLock Module angelehnt, ermöglicht einen schnellen Einstieg und spiegelt die sogenannten Kritischen Sicherheitskontrollen (CSC) wider, welche Maßnahmen für einen besseren Schutz vor Angriffen bieten. Auf horizontaler Ebene sorgen Tabs für mehr Übersicht und eine zukunftssichere Erweiterbarkeit.

Verbessertes Management von Security-Awareness-Kampagnen

- Unternehmen können Security Awareness Kampagnen mit klaren Zielen, Inhalten, Start- und Enddaten sowie gezielten Empfängern jetzt sehr viel leichter erstellen, verwalten und auswerten. Eine Audit-Trail-Funktion hilft bei Sicherheitsaudits, Kampagnenergebnisse und historische Trends nachzuverfolgen. Mit der entsprechenden Rolle ausgestattet können Personalabteilungen aus dem DOC heraus eigenständig Kampagnen verwalten und mittels neuer Benutzergruppen Inhalte gezielt an die Abteilungen ausrollen.

Erweiterungen für BitLocker und BitLocker To Go

- Es ist jetzt noch einfacher, bereits gemanagte BitLocker Umgebungen in DriveLock zu übernehmen und abzulösen. Bei einer Re-Provisionierung übernimmt DriveLock bereits existierende Datenpartitionen. Externe Medien (z.B. USB-Sticks), die bereits BitLocker To Go verschlüsselt sind, können jetzt von DriveLock übernommen und verwaltet werden, ohne erneut verschlüsselt werden zu müssen. Zudem kann DriveLock extern angeschlossene gesperrte Speichermedien und Datenpartitionen lesen, auch wenn sich kein DriveLock Agent darauf befindet oder die ursprüngliche Zuordnung zu einem Endpoint unbekannt ist. Alle Anwendungsfälle entsprechen höchsten Sicherheitsstandards.

Einheitliche Laufwerksregeln für alle Betriebssysteme

- Das DOC unterstützt nun alle Betriebssysteme mit nur einer Laufwerksregel. Die Hardware-ID wird jetzt als Laufwerkskriterium von DriveLock Agenten auf Windows, Linux und macOS unterstützt. Sie kann jetzt auch in Laufwerkslisten mit der Seriennummer kombiniert werden. Das führt zur schnelleren zentralen Verwaltung für heterogene Endgeräte mit nur einer Laufwerks-Konfiguration.

Erweitertes Management von Bluetooth-Geräten

- Das erweiterte Management von Bluetooth-Geräten ermöglicht es Administratoren, Bluetooth-Geräte genauso einfach wie andere Technologien zu steuern. Sie können Regeln erstellen, z. B. das Sperren von Tastaturen, aber das Zulassen von Mäusen, die Steuerung nach Gerätetyp oder Hersteller und die Verwaltung von Bluetooth-Klassen und -Diensten. Dies vereinfacht die Konfiguration und beseitigt Komplexität. Insgesamt ermöglicht unsere Lösung eine optimierte Verwaltung von Bluetooth-Geräten in nur wenigen Schritten.

Mac-Agent mit Proxy-Unterstützung

- Der DriveLock macOS-Agent bietet nun die Proxy-Unterstützung, die für den Einsatz in Unternehmensumgebungen unerlässlich ist, sei es durch automatische Konfiguration über PAC/WPAD oder manuelle Konfigurationsmöglichkeiten. Darüber hinaus gewährleistet die protokollspezifische Proxy-Unterstützung die Kompatibilität und sichere Kommunikation für die Protokolle HTTP(S), SOAP und MQTT und erfüllt damit die individuellen Anforderungen der einzelnen Protokolle.

Domänenübergreifende Verwaltung von Endpoints

- Dynamische Gruppen können jetzt auf den Distinguished Name (DN) des Computers sowie auf den DN der Gruppen, in denen der Computer Mitglied ist, filtern. Dies erleichtert die Verwaltung komplexer Verzeichnisinfrastrukturen, wenn Computer über den Umfang ihres Verzeichnisdienstes erreichbar sind.

Sichere Kennwortverwaltung für temporäre lokale Administratorkonten

- Das Configuration Management Modul bietet die Verwaltung lokaler Benutzerkonten, einschließlich temporärer lokaler Admin-Konten mit automatisch generierten und sicheren Kennwörtern, die täglich geändert werden können. Helpdesk-Anwender können nun den Endbenutzern das (tages-) aktuelle lokale Admin-Kennwort im DOC einsehen und übergeben. Das gilt auch für die Kennworthistorie. Letzteres ist nützlich, wenn beispielsweise eine virtuelle Maschine auf einen früheren Snapshot zurückgesetzt wird und das damals gültige Kennwort benötigt wird. Um diese Aufgabe auszuführen, benötigt der Helpdesk eine entsprechende Rolle und Rechte im DOC, und Bestandskunden müssen zuvor ein Zertifikat im DOC speichern. Damit gehen die Fähigkeiten über die von Microsoft LAPS (Local Administrator Password Solution) hinaus.

Erzwingen komplexer Kennwortanforderungen für DOC-Konten

- Cloud-Kunden können jetzt eine Kennwortrichtlinie konfigurieren, die den jeweiligen Security-Anforderungen entspricht. Für DOC-Konten, die kein Single Sign-On (SSO)

verwenden, können komplexe Kennwortregeln durchgesetzt werden, sowie die Wiederverwendung der letzten Kennwörter verhindert werden.

Arbeiten mit Benutzergruppen

- Analog zur Erstellung von Computergruppen können jetzt auch statische Benutzergruppen konfiguriert werden. Diese sind besonders von Vorteil für die Zuweisung und Kontrolle der Ausführung von Security-Awareness-Kampagnen. Außerdem können sie in Richtlinien in allen Benutzerlisten verwendet werden, in denen bisher schon Azure AD-Gruppen verwendet werden konnten.

Optimierte Azure AD-Synchronisation

- Dies ist nur für Cloud-Kunden relevant. Der Synchronisation zwischen DriveLock und Azure AD wurde auf die für die DriveLock Umgebung relevanten Gruppen reduziert und die Geschwindigkeit verbessert.
- Nach dem Update wird die Azure AD-Synchronisation deaktiviert. Sie müssen die zu synchronisierenden Gruppen auswählen, um die Synchronisation wieder zu aktivieren. Bereits synchronisierte Gruppen bleiben in der DriveLock-Datenbank erhalten, werden jedoch nicht mehr aktualisiert, sofern sie nicht erneut ausgewählt wurden.

E-Mail-Benachrichtigung bei bestimmten Ereignissen

- Die DriveLock-Plattform bietet nun einen E-Mail-Benachrichtigungskanal. Wichtige Ereignisse wie z.B. die Erkennung von Viren werden weitergeleitet. Dies ermöglicht eine effektive Überwachung und Reaktion auf Sicherheitsvorfälle, während gleichzeitig eine Überlastung des E-Mail-Postfachs vermieden wird. Die Möglichkeit, zukünftig weitere Kommunikationskanäle zu integrieren, bietet zusätzlichen Mehrwert und Flexibilität für die Benachrichtigung bei wichtigen Ereignissen.

Windows 7 Legacy Support

- DriveLock unterstützt ab Version 2023.1 Windows 7 Endpoints nur noch mit einer kostenpflichtigen Legacy/Extended Support Lizenz. Unternehmen bekommen im DOC einen entsprechenden Hinweis.

Windows XP

- Windows XP wird ab Version 2023.1 nicht mehr unterstützt.

3.2.2 Verbesserungen und Änderungen

Zusätzlich zu den Neuerungen bietet diese Version weitere Verbesserungen in folgenden Bereichen:

Application Control

- Eine neue Einstellung führt zu einer deutlichen Leistungsverbesserung, weil Regeln jetzt sehr viel schneller ausgewertet werden. (Referenz EI-2429)

Device Control

- Die Inhaltsprüfung für Unicode-Textdateien (<FORMFEED> zulassen; <NUL> nicht zulassen) wurde verbessert. (Referenz EI-2397)

DriveLock Agent

- macOS-Agent: Im DOC im Abschnitt Installationen kann der macOS-Agent einfach über die Kommandozeile mit den entsprechenden Parametern installiert werden (Referenz: EI-2366)
- Die Installation des DriveLock Agent über die DLSetup.exe ist nicht mehr möglich. Der Agent kann über die Kommandozeile mit entsprechenden Parametern installiert und aktualisiert werden. (Referenz EI-2351)
- Die DriveLock Agent (x64).msi unterstützt einen neuen Parameter: REMOVEDATA. Dieser Parameter kann bei der Deinstallation angegeben werden (REMOVEDATA=1), damit nicht nur die Programmdateien sondern auch alle Konfigurationsdaten des Agenten bei der Deinstallation gelöscht werden.
- **Agenten-Fernkontrolle:**
  - Es ist jetzt möglich, sowohl HTTP als auch HTTPS für die Fernkontrolle zu deaktivieren. (Referenz: EI-2121)
  - Der Fernkontrollzugriff auf Agenten kann jetzt durch rollenbasierte Zugriffsrechte gesichert werden. Es wurden zwei neue Rollen bzw. Berechtigungen im DOC hinzugefügt, die bestimmen, ob auf Agenten nur lesend zugegriffen werden kann oder ob auch Änderungen erlaubt sind.

DriveLock Enterprise Service (DES)

- Wenn im DOC ein Benutzer aus einer Domäne hinzugefügt werden soll, auf die der DES keine Berechtigung hat, wird jetzt ein Kennwortdialog angezeigt. Dies betrifft nur die On-Premise-Version von DriveLock. (Referenz EI-2280)

DriveLock Operations Center (DOC)

- Audit-Ereignisse werden jetzt in einer eigenen Registerkarte angezeigt.

DriveLock Pre-Boot-Authentifizierung (PBA)

- Für eine bessere Fehleranalyse wird jetzt ein Ereignis gemeldet (Ereignis Nummer 757), dass die PBA nicht installiert werden konnte, weil die Voraussetzungen für SecureBoot nicht erfüllt sind. Grund ist das fehlende Microsoft Corporation UEFI CA 2011 Zertifikat.

Ereignis-Verschlüsselung

- Ab Version 2023.1 entfällt die Möglichkeit, Einstellungen für die clientseitige Ereignis-Verschlüsselung zu verändern bzw. zu konfigurieren. Ereignisse werden grundsätzlich nicht mehr verschlüsselt. Die Funktion zur Datenmaskierung im DOC löst die bisherige Pseudonymisierung durch Verschlüsselung komplett ab.

Inventarisierung

- Ein neues Ereignis (ID 2710) wird jetzt ausgelöst, wenn ein Computer vom Server ausgewählt wird, um eine AD-Inventarisierung durchzuführen. Dies betrifft nur DriveLock Managed Services. (Referenz EI-2289)

Lizenzierung

- Das Risk&Compliance (EDR) Modul wurde in die Zero Trust Plattform eingegliedert. Die Funktionen "Ereignisfilter auswerten" und "Ereignisse von Drittanbietern abfragen" können jetzt aktiviert oder gezielt deaktiviert werden.
- Die Lizenz für Native OS Security wurde umbenannt in Security Configuration Management. Der Funktionsumfang bleibt davon unberührt und enthält weiterhin Firewall-Management und Verwaltung lokaler Benutzer und Gruppen.

3.2.3 Fehlerbehebungen 2023.1

DriveLock 2023.1 ist eine Hauptversion.

Dieses Kapitel enthält Informationen zu Fehlern, die mit DriveLock Version 2023.1 behoben sind. Als Referenz dienen dabei unsere External Issues (EI) Nummern, sofern vorhanden.

	Application Control
EI-2381	Application Behavior Control hat Umbenennungen und Verschiebungen von Dateien nicht erkannt bzw. geblockt

	Betriebssystem-Management
	Wenn in der Einstellung Betriebssystem-Management unter Lokale Benutzer und Gruppen die Einstellung Lokaler Benutzerverwaltungsmodus auf Maßgebend gesetzt war, wurden Benutzer auf dem Agenten nicht korrekt entfernt, auch wenn sie zuvor in der Richtlinie gelöscht wurden.
EI-2466	Ausgehende Firewall-Verbindungen wurden bisher immer als eingehende Verbindungen protokolliert. Dieser Fehler ist jetzt behoben. Für ausgehende Verbindungen werden nun DriveLock Ereignisse 747 und 748 erzeugt.
EI-2438	Wenn mehrere lokale Benutzer gleichzeitig erstellt oder aktualisiert werden, erhalten sie jetzt nicht mehr alle dasselbe Kennwort.

	BitLocker Management
	Der Befehl "DlFdeCmd.exe cryptstatus" zeigte nicht den richtigen Status für unverschlüsselte Laufwerke an, wenn die Drivelock PBA für Bitlocker installiert war.

	BitLocker Management
	Nach der Aktualisierung von BitLocker Management mit DL-PBA wurden mehrere Ausnahmen ausgelöst und in das NT-Ereignisprotokoll gemeldet. Dieses Verhalten ist jetzt behoben.
	Das Sperren von USB-Sticks mit nicht zugelassenen oder fehlenden BitLocker-Firmen-IDs wurde durch BitLocker Management verhindert, weil entsprechende Windows-Richtlinieneinstellungen entfernt wurden.

	Defender Management
EI-2372	Der im Wizard zum Einrichten von geplanten Scans eingestellte Wochentag wurde falsch ausgewertet und außerhalb des Wizards auch falsch in der DriveLock Management Konsole (DMC) angezeigt (z.B. Mittwoch eingestellt, aber als Donnerstag ausgewertet).
EI-2343	Wenn das Wiederherstellen einer Datei aus der Defender-Quarantäne fehlschlägt und der Grund dafür ist, dass das Originalverzeichnis, aus dem die Datei in die Quarantäne verschoben wurde, nicht mehr existiert, zeigt die MMC jetzt eine entsprechende Fehlermeldung an.
EI-2333	Wenn im Laufwerk kein Medium eingelegt ist, wird keine Überprüfung des Laufwerks ausgelöst und damit auch keine Fehlermeldung über einen fehlgeschlagenen Scan angezeigt.

	Device Control
	Es ist jetzt möglich, die Verwendungsrichtlinie für Laufwerke zu deaktivieren, die noch nicht einsatzbereit sind (z.B. SD-Kartenleser ohne SD-Karte).

Referenz	Disk Protection
	Wenn Dateifiltertreiber von Drittanbietern mit der DriveLock-PBA oder Disk Protection installiert worden sind, wurde in einigen Fällen das DriveLock EFS (Embedded File System) nicht überprüft und repariert (EFS Sanity).
	Nicht alle Partitionen wurden sofort nacheinander verschlüsselt. Dieser Fehler ist jetzt behoben.
	In seltenen Fällen wurde durch ein DriveLock Agent Update ein Service der DriveLock PBA deregistriert.

Referenz	DriveLock Agent
EI-2121	Wenn die Agenten-Fernkontrolle so konfiguriert war, dass nur HTTP verwendet wurde, funktionierte der SB-Service nicht.
EI-2465	Wurde die Einstellung 'Fernzugriff in der Windows Firewall erlauben' deaktiviert, wurden zuvor konfigurierte Firewall-Regeln für Remote-Verbindungen auf den DriveLock Agenten nicht mehr gelöscht.
EI-2006	Bei der Deinstallation des DriveLock Agenten wurden fälsch-

Referenz	DriveLock Agent
	licherweise die Daten für den Zugriff auf BitLocker-verschlüsselte Laufwerke gelöscht.

Referenz	DriveLock Enterprise Service (DES)
EI-2461	Bei der Installation eines neuen verknüpften DES wird jetzt eine vorhandene Konfiguration korrekt erkannt.
EI-2402	Ein Fehler wurde behoben, bei dem der Agentenstatus vom Server nicht verarbeitet werden konnte, wenn für die Konfiguration GPOs verwendet wurden.

Referenz	DriveLock Management Console (DMC)
	Nach dem Anfordern eines Wiederherstellungsschlüssels für BitLocker Management in der DMC wurde keine Agentenaktion erzeugt, so dass der Benutzer auf dem Client nicht zur Eingabe eines neuen BitLocker-Kennworts aufgefordert wurde.
EI-2305	Es war möglich, den Wizard zum Erzeugen eines neuen Mandanten zu starten, auch wenn dann im Laufe des Wizards festgestellt wurde, dass man mangels Berechtigung nicht weiter kommt. Ohne diese Berechtigung lässt sich der Wizard jetzt gar nicht mehr starten.

Referenz	DriveLock Operations Center (DOC)
EI-2475	Bei der Eingabe des Codes, um einen Computer im DOC offline zu entsperren kann es nötig sein, 25 Zeichen einzugeben, je nach Konfiguration reichen aber auch bereits 15. Die Fehlermeldung "ungültiger Code" erschien fälschlicherweise nach manueller Eingabe der ersten 15 Zeichen des eigentlich 25 Zeichen langen Codes. Jetzt erscheint die Meldung generell, solange nicht die ausreichende Anzahl an Zeichen eingegeben wurde oder der 15 bzw. 25 Zeichen lange Code ungültig ist.

Referenz	File Protection (FFE)
EI-2392	Ein Fehler, bei dem der Zugriff auf den Barco Clickshare Button verweigert wurde, ist behoben.
EI-2471	Der BSOD-Fehler, der auftrat, wenn die SID des Benutzers für eine Anfrage nicht abgerufen werden konnte (z.B. aufgrund von Virtualisierung und Umleitung), wurde behoben.
EI-2386	Der Fehler, dass die Verschlüsselung von Office 365 Cloud-Dateien einen Bluescreen-Fehler verursacht, wurde im "alten FFE-Format" behoben.
	Die Wiederherstellung von einem Systemwiederherstellungspunkt funktionierte nicht mit FFE. Dies ist behoben.
	ReFs wird vom "alten FFE-Format" nicht unterstützt.
	Die Zugriffskontrolle für Benutzer mit Lesezugriff funktionierte in der früheren Version 22.2.x nicht, wenn das neue Format ver-

Referenz	File Protection (FFE)
	wendet wurde. Dies ist jetzt behoben.

Referenz	Gruppen / Berechtigungen
EI-2462	Wenn zu viele Gruppenmitgliedschaften vorhanden waren, wurde die Anmeldung eines Benutzers über SAML verhindert. Jetzt werden die effektiven Gruppenmitgliedschaften über die gruppenbasierten Rollenzuweisungen gefiltert. Dies bedingt dass Benutzer sich bei Änderungen an den Rollenzuweisungen erneut anmelden müssen.

Referenz	Lizenzen
EI-2157	Der Fehler bei der Aktivierung der Lizenz unter Verwendung eines Proxy-Servers wurde behoben. Die Eingabe eines Benutzers ist nicht mehr erforderlich.

Referenz	Security Awareness
EI-2439	Security-Awareness-Kampagnen, die in der Richtlinie mit einer festgelegten Sprache erzeugt wurden, wurden auf dem Agenten nicht zwingend mit derselben Sprache angezeigt.
EI-2403	Im Fall einer Security-Awareness-Kampagne vom Typ Test wurden die Parameter des Ereignisses 'Test fehlgeschlagen' für korrekte/falsche Antworten jeweils mit 0 befüllt.

Referenz	Security Awareness
	Unter Umständen wurde der Typ einer Security-Awareness-Kampagne in der Security-Awareness-Bibliothek mit "unbekannt" angegeben.
EI-2313	.NET Framework 4.7.2 ist keine Voraussetzung mehr für den Agenten, sondern nur noch für Security Awareness.

Referenz	Pre-Boot-Authentifizierung
EI-2245	Bei Anforderung der Wiederherstellungsdaten für die PBA-Notfall-Anmeldung im DOC konnte kein alternatives Zertifikat ausgewählt werden, so dass die Wiederherstellung u.U. nicht möglich war.

4 Systemvoraussetzungen

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

4.1 DriveLock Agent

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

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

Der Windows DriveLock Agent ist grundsätzlich verfügbar für AMD-/Intel X86-basierte Systeme (32-Bit und 64-Bit Architektur). Für den Einsatz des DriveLock Agenten wird ein 64-Bit

System empfohlen. Server-Betriebssysteme werden ausschließlich unter 64-Bit unterstützt. Einschränkungen der einzelnen Funktionen sind weiter unten beschrieben.

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

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

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

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

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

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

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

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

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

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

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

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

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

3. **Einschränkungen macOS**

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

werken

- Keine Self-Service Funktionalität

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

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

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

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

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

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

4.2 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 2023.1HF1 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.

4.3 DriveLock Enterprise Service

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

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

Hauptspeicher / CPU:

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

Freier Festplattenspeicherplatz:

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

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

Benötigte zusätzliche Windowskomponenten:

- .NET Framework 4.8 oder höher ist Voraussetzung für die Installation!

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

Benötigte DriveLock API Services Ports (DOC/MQTT):

- 5370, 6369 und 4369: Diese drei Ports sollten nicht durch andere Server-Dienste belegt werden, sie müssen jedoch nicht von außen erreichbar sein (nur intern)
- 8883: Die Agenten verbinden sich auf diesen Port mit dem DES, um per Agentenfernsteuerung erreichbar zu sein. Die Freigabe in der lokalen Firewall des Rechners erfolgt automatisch durch das DES-Installationsprogramm.

Unterstützte Plattformen:

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

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

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

Unterstützte Datenbanken:

- DriveLock benötigt ab Version 2023.1 SQL Server 2016. Die Datenbank muss einen Kompatibilitätslevel 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.

4.4 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.

Bitte beachten Sie auch folgende Hinweise.

5 Update von DriveLock

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

5.1 Update des DriveLock Agenten

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

1. Vor dem DriveLock Agent-Update:
   - Wenn Sie den Agenten nicht mit Hilfe des Autoupdate-Mechanismus von DriveLock aktualisieren, setzen Sie in der DriveLock Richtlinie folgende **Einstellung**:
     - **DriveLock-Agentendienste im Nicht-beenden-Modus starten**: Deaktiviert
   - Wenn Sie eine Festplattenverschlüsselung im Einsatz haben, muss die Verzögerung für eine mögliche Deinstallation in den Verschlüsselungseinstellungen auf mindestens 5 Tage gesetzt werden.
   - Bei der Verwendung von BitLocker Management muss vor der Aktualisierung folgendes beachtet werden:
     Details finden Sie in der BitLocker Management Dokumentation auf DriveLock Online Help
     Die Einstellung für die Verschlüsselung **Keine Entschlüsselung durchführen** verhindert eine mögliche Änderung des Verschlüsselungsstatus der DriveLock Agenten. Vor der Aktualisierung ist es daher notwendig, dass diese Option in der aktuellen Verschlüsselungsrichtlinie aktiviert und die Richtlinie im Anschluss gespeichert und veröffentlicht wird.
   - Bei der Verwendung von Disk Protection muss vor der Aktualisierung folgendes beachtet werden:
     Bei einem Update werden Agenten mit BIOS-Systemen, die Disk Protection bereits installiert haben, nicht mehr aktualisiert und bleiben auf dem jeweiligen Stand, bis die Disk Protection deinstalliert wurde.
2. Während des DriveLock Agent-Updates:
   - Führen Sie die Aktualisierung mit einem privilegierten Administrator-Konto durch. Das ist beim Autoupdate bereits automatisch der Fall.
3. Nach dem DriveLock Agent-Update:

- Wenn Sie File Protection oder Disk Protection verwenden, ist zur Aktualisierung der Treiberkomponenten ein Neustart nach dem DriveLock Agent-Update erforderlich. Der Neustart sollte erst erfolgen, nachdem die entsprechenden Komponenten aktualisiert sind. Fügen Sie diesen Schritt bei einer Aktualisierung durch eine Softwareverteilung in den Update-Ablauf ein bzw. starten Sie den aktualisierten Rechner manuell neu.

5.1.1 Manuelle Updates

- Wenn Sie die `DriveLock Agent.msi` ausführen wollen, muss das aus einem administrativen Befehlsfenster per `msiexec` geschehen. Doppelklick aus dem Windows Explorer funktioniert nicht.
- Wird ein Client-Update manuell über das Starten von `msiexec` durchgeführt, kann es vorkommen, dass sich der Windows Explorer nicht korrekt beendet. In der Folge verschwindet die Benutzeroberfläche von Windows (schwarzer Bildschirm) und wird auch nach dem Agent-Update nicht neu gestartet. In diesem Fall muss über den Task-Manager der Explorer manuell gestartet werden bzw. ein Reboot initiiert werden. Dies betrifft vor allem Kunden, die Clientmanagement-Software verwenden, die möglicherweise die `msiexec` in einer Benutzer-Session ausführen. Das Problem lässt sich dadurch beheben, dass man dem msiexec-Aufruf folgende Parameter mitgibt:
  - `MSIRESTARTMANAGERCONTROL=Disable`
  - `MSIRMSHUTDOWN=2`

5.2 Update des DriveLock Enterprise Service (DES)

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

Beim Update des DES von Version 2021.1 auf höhere Versionen ist folgendes zu beachten:

Um die Aktualisierung erfolgreich durchführen zu können, benötigen Sie eine gültige Lizenz inklusive Wartung. Diese muss in Ihrem aktuell laufenden System in der Datenbank des DES gespeichert sein oder über die DMC erneuert und hochgeladen werden, bevor die Aktualisierung gestartet wird.

5.3 Update der DriveLock Komponenten

Das DriveLock Installationshandbuch beschreibt alle notwendigen Schritte, die bei einem Update auf die aktuellste Version durchzuführen sind. Die Release Notes enthalten zusätzlich besonders wichtige Punkte, die Sie bei einer Aktualisierung beachten sollten.

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

Update der DriveLock Management Konsole (DMC)

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

Update der DriveLock Datenbank

Bei einer Aktualisierung von Version 2020.1 oder älter auf neuere Versionen werden die beiden DriveLock-Datenbanken zusammengeführt. In diesem Fall ist ein zusätzlicher Migrationsschritt nötig. Weitere Informationen finden Sie in dem Technischen Artikel *TA-Datenbankmigration* auf DriveLock Online Help - Technical Articles.

Update von Disk Protection

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

Wir haben weitere Informationen, die für ein Update der DriveLock Disk Protection bzw. ein Update des Betriebssystems bei einer installierten DriveLock Disk Protection wichtig sind, in dem Dokument *TA - Windows 10 Upgrade with Drivelock Disk Protection* für Sie zusammengestellt, ebenfalls auf DriveLock Online Help - Technical Articles.

Update von File Protection auf Version 2023.1

Für die Dateiverschlüsselung wurde ein neues Verschlüsselungsformat eingeführt. Dieses neue Format wird jetzt standardmäßig auf neue DriveLock Agenten angewendet. Bei Bestandsagenten wird das alte Format beibehalten. Das Format wird mit der neuen File Protection-Einstellung **Verwendete Verschlüsselungsformate** geregelt. Sie können bei Bedarf ein bestimmtes Verschlüsselungsformat explizit festlegen.

Hinweis: Neues und altes Verschlüsselungsformat sind nicht kompatibel und müssen in separaten Richtlinien abgebildet werden. Weitere Informationen finden Sie im Kapitel File Protection in der Encryption-Dokumentation auf DriveLock Online Help.

- **DFS-Unterstützung**
  - Die Verschlüsselungsformate **Altes Format** und **Altes Format (alter Treiber)** unterstützen DFS nicht.

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

  - DFS-Freigaben werden mit der Option **Neues Format** unterstützt, auch wenn sie nicht nur den primären Server verwenden. Getestet wurde dies auf Windows Server 2022 und Windows Server 2019.

6 Bekannte Einschränkungen

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

6.1 BitLocker Management

Unterstützte Editionen und Versionen

DriveLock BitLocker Management wird auf folgenden Systemen unterstützt:

- Windows 7 SP1 Enterprise und Ultimate, 64-Bit, TPM-Chip ist erforderlich
- Windows 8.1 Pro und Enterprise, 32/64-Bit
- Windows 10 Pro und Enterprise, 32/64-Bit
- Windows 11 Pro und Enterprise, 32/64-Bit

Vorhandene BitLocker Umgebung

Wenn Sie eine bereits vorhandene Systemumgebung verwalten wollen, die bereits mit BitLocker verschlüsselte Computer enthält, müssen diese seit Version 2019.1 nicht mehr zuvor über die vorhandene BitLocker Verwaltung bzw. die Gruppenrichtlinien entschlüsselt werden. DriveLock erkennt die BitLocker Verschlüsselung automatisch und erzeugt neue Wiederherstellungsinformationen. Eine automatische Ent- und Verschlüsselung wird nur dann durchgeführt, wenn der in der DriveLock Richtlinie konfigurierte Verschlüsselungsalgorithmus sich vom derzeitigen Algorithmus unterscheidet.

Anschließend ist eine Verwaltung durch DriveLock BitLocker Management möglich und eine sichere Speicherung und Verwendung der Wiederherstellungsinformationen gewährleistet.

Verwendung von Kennwörtern

DriveLock BitLocker Management vereinfacht die missverständliche Unterscheidung zwischen PINs, Passphrases und Kennwörtern, indem nur noch der Begriff "Kennwort" verwendet wird. Gleichzeitig wird ein solches Kennwort automatisch im richtigen BitLocker Format benutzt, entweder als PIN oder als Passphrase.

Da Microsoft jedoch unterschiedliche Anforderungen an die Komplexität von PIN und Passphrase stellt, gelten für das Kennwort folgende Einschränkungen:

- Mindestlänge: 8 Zeichen. In bestimmten Fällen sind auch 6 Zeichen (Zahlen) möglich, mehr hierzu in der aktuellen BitLocker Management Dokumentation auf DriveLock

Online Help.

- Maximale Länge: 20 Zeichen

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

Verschlüsselung von erweiterten Festplatten

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

Verschlüsselung auf Windows 7 Agenten

Bei der Verwendung der in DriveLock 2020.2 hinzugekommenen Ausführungsoptionen auf Windows 7 Agenten kann folgender Fehler auftreten: BitLocker verschlüsselt unter Windows 7 nicht, wenn die Optionen "wenn der Bildschirmschoner konfiguriert und aktiv ist" und "wenn keine Anwendung im Vollbildmodus ausgeführt wird" aktiviert sind.

Wechsel von Disk Protection zu BitLocker Management

Disk Protection muss mittels entsprechender Richtlinieneinstellung entfernt werden, bevor BitLocker Management einsetzbar ist.

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.

Irreführende Meldung bei der Aktualisierung von Version 2022.2 auf 2023.1

Wenn in der Richtlinie die Einstellung gesetzt ist, dass Endbenutzer die Verschlüsselung verzögern dürfen, wird beim Aktualisieren von Version 2022.2 auf 2023.1 das Dialogfeld "BitLocker Verschlüsselung" fälschlicherweise angezeigt, obwohl die Festplatten bereits verschlüsselt sind. Sobald die Schaltfläche "Verschlüsseln" geklickt wird, verschwindet das Dialogfeld und es findet weder eine Ver- noch eine Entschlüsselung statt.

6.2 Defender Management

Damit der Schnellscan funktionieren kann, muss ein Benutzer lokal am System angemeldet sein. Eine Anmeldung über eine Remotedesktopverbindungen (RDP-Session) reicht nicht

aus, da bei RDP- bzw. Terminal Server- / Citrix-Sessions keine Defender Management-Aufgaben aus dem DOC heraus durchgeführt werden können. (Referenz EI-2092)

6.3 Device Control

Lange Seriennummern

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

Kurzfristig gesperrte Dateien

Wenn ein Dateifilter konfiguriert ist und der Zugriff für bestimmte Benutzer oder Gruppen erlaubt ist, können Dateien auf dem USB-Stick während der Konfigurationsaktualisierung für kurze Zeit gesperrt sein.

CD-ROM Laufwerke

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

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

6.4 Disk Protection

Windows Inplace Upgrade

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

Antiviren Software

Es ist möglich, dass die Installation der DriveLock Disk Protection aufgrund einer Antivirus Software fehlschlägt, weil das ausgeblendete Verzeichnis `C:\SECURDSK` durch die Software in Quarantäne genommen wird. In diesem Falle sollten Sie für den Zeitraum der Installation

den Virenschutz temporär ausschalten. Wir empfehlen, dieses Verzeichnis grundsätzlich als Ausnahme für den Virenscanner zu definieren.

Applikationskontrolle

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

Ruhezustand

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

UEFI-Modus

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

- Die seit Version 2019.2 verfügbare PBA steht nur für Windows 10 Systeme zur Verfügung, da die für die Festplattenverschlüsselungskomponenten benötigten Treibersignaturen von Microsoft nur für dieses Betriebssystem gelten.
- Mit der PBA für den UEFI-Modus können unter Umständen Probleme bei PS/2 Eingabegeräten (z.B. eingebauten Tastaturen) auftreten.
- Unter VMWare Workstation 15 und auch bei einigen wenigen Hardwareherstellern ergaben unsere Testergebnisse Konflikte durch Maus- und Keyboadtreiber der UEFI Firmware, so dass keine Tastatureingabe in der PBA möglich ist. In diesem Fall können Sie beim Start des Rechners mit Hilfe der Taste "k" das Laden der DriveLock-PBA-Treiber einmalig verhindern. Nach der Windows-Anmeldung auf dem Client können Sie dann in einer Administrator-Kommandozeile den Befehl `dlsetpb /disablekbddrivers` ausführen, um die DriveLock-PBA Keyboard-Treiber dauerhaft zu deaktivieren. Bitte beachten Sie, dass dadurch in der Anmeldemaske der PBA das Standardkeyboardlayout der Firmware geladen ist, was in den meisten Fällen eine EN-US Belegung hat, wodurch die Sonderzeichen abweichen können.
  Mit Einführung des Kombi-Treibers ab Version 2020.1 wird das Problem auf einigen Systemen gelöst (u.a. VM Ware Workstation 15).
  Weitere Informationen zu Abkürzungs- und Funktionstasten finden Sie im entsprechenden Kapitel in der Encryption Dokumentation auf DriveLock Online Help.

Folgende Punkte sind weiterhin zu beachten:

- DriveLock 7.6.6 und höher unterstützt UEFI Secure Boot.
- Firmwareupdates können bewirken, dass NVRAM-Variablen des Mainboards gelöscht werden, die DriveLock benötigt. Daher empfehlen wir unbedingt, vor der Installation der DriveLock PBA / FDE die Firmware-Updates für das Mainboard /UEFI einzuspielen (auch bei neu gekauften Geräten oder bei Bugfixes)
- 32 Bit Windows und DriveLock kann nicht auf ein 64 Bit fähiges System installiert werden. Es muss die 64 Bit Version von Windows und DriveLock eingesetzt werden.
- Die maximale Größe einer Festplatte ist weiterhin auf maximal 2 TB beschränkt.
- Auf manchen HP Rechnern ist Windows immer wieder an Position 1 der UEFI Bootreihenfolge und die DriveLock PBA muss im UEFI Boot-Menü manuell ausgewählt werden. In solchen Fällen und bei Problemen muss man Fast Boot im UEFI ausschalten, damit die DriveLock PBA an Position 1 bleibt.

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

Referenz: EI-686

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

Voraussetzungen für Disk Protection:

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

Neustart nach Installation der PBA auf Toshiba PORTEGE Z930:

Referenz: EI-751

Nach Aktivierung von Disk Protection mit PBA und Neustart des o.g. Notebooks, kann Windows nicht gestartet und somit das Notebook nicht verschlüsselt werden. Wir arbeiten an einer Lösung dieser Einschränkung.

6.5 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

DriveLock Mobile Encryption (Encryption 2-Go) kann NTFS/EXFAT-Container nur zum Lesen verbinden.

6.6 DriveLock Operations Center (DOC)

Alte Versionen der DOC.exe werden nicht mehr unterstützt

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

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

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

6.7 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.

6.8 Erzwungene Verschlüsselung

Vorgabe der Verschlüsselungsmethode bei erzwungener Verschlüsselung eines externen Speichermediums

Wenn ein Administrator die Verschlüsselungsmethode nicht vorgegeben hat, erscheint auf dem DriveLock Agenten beim Verbinden des externen Speichermediums ein Dialog zur Auswahl der Verschlüsselungsmethode (Encryption-2-Go, Disk Protection, BitLocker To Go). In

manchen Fällen erscheint dieser Dialog jedoch fälschlicherweise auch bei SD-Karten-Lesern ohne Medium.

6.9 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.

NetApp

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

Windows 10-Clients mit Kaspersky Endpoint Security 10.3.0.6294

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

Zugriff auf verschlüsselte Ordner

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

Ordnerverschlüsselung abbrechen

- Es wird nicht empfohlen, die Ver-/Entschlüsselung von Ordnern abzubrechen. Falls dies dennoch passiert (ist), löschen Sie die Datenbankdatei nicht, da sonst der Status der aktiven Dateien verloren geht.

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.

Distributed File System (DFS)

- DriveLock File Protection unterstützt grundsätzlich auch die Speicherung von verschlüsselten Verzeichnissen auf Netzlaufwerken mit Distributed File System (DFS). Da DFS und das zugrundeliegende Speichersystem jedoch kundenspezifische Eigenheiten aufweisen können, empfehlen wir vor dem Einsatz einen ausführlichen Test von verschlüsselten Verzeichnissen. Bitte beachten Sie den Hinweis im Kapitel Update der DriveLock Komponenten. .

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

6.10 SB-Freigabe

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

6.11 Thin Clients

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

- Auf IGEL-Clients kann Security Awareness unter Umständen nicht verwendet werden.
- Die Option "Unbenutzten Speicher auf dem verschlüsselten Medium auffüllen" funktioniert bei der Verschlüsselung eines DriveLock Containers über einen Thin Client nicht zuverlässig.

7 DriveLock in verschiedenen Umgebungen

Grundsätzlich ist DriveLock für den Betrieb in Active Directory ausgelegt, weil DriveLock das AD-Rechtekonzept bzw. die -Struktur verwendet. Beispielsweise können Laufwerke für bestimmte Benutzergruppen freigegeben oder Richtlinien auf OUs zugewiesen werden. Es kann aber auch ohne Active Directory eingesetzt werden.

DriveLock ohne Active Directory

Sofern Sie DriveLock ohne Active Directory einsetzen wollen, können Sie dennoch DriveLock Gruppen verwenden und die Azure AD-Integration steht Ihnen ebenfalls zur Verfügung. DriveLock Computergruppen oder Azure AD-Computergruppen können überall verwendet werden, wo auch AD-Computergruppen oder OUs verwendet werden können.

DriveLock und Azure-AD-Benutzergruppen können dagegen nicht überall verwendet werden.

Folgendes ist zu beachten:

- In einer DriveLock on-premises Installation verwenden Sie die lokalen Benutzer des Computers, auf dem der DES installiert ist, um die Umgebung zu verwalten.
- Wenn Sie DriveLock Managed Services verwenden, können Sie für die Anmeldung am DOC eine Azure-AD-Integration verwenden oder eigen Benutzer anlegen. Berechtigungen können hier auch auf Azure-AD-Gruppen vergeben werden.
- Wenn die MQTT-Verbindung zwischen Agenten und DES deaktiviert ist, muss die Namensauflösung (NETBIOS/FQDN Name) funktionieren, um für Helpdesk Aktivitäten auf die Clients zugreifen zu können.

8 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 2021.2	EoL - kein Support mehr	EoL - kein Support mehr
2021.2	Mai 2024	EoL - kein Support mehr
2022.1	September 2023	EoL - kein Support mehr
2022.2	Juni 2025	Bis zum Release einer auf 2023.1 folgenden Version
2023.1	derzeit aktuelle Version	derzeit aktuelle Version

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

Support-Lebenszyklus:

Ab dieser Version passen wir den Support-Lebenszyklus für neue DriveLock-Produktversionen für alle Betriebssysteme an.

Sobald eine neue Produktversion veröffentlicht wird, geben wir das End-Of-Life (EOL) der **Vorgängerversion** bekannt.

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. 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:

- DriveLock 2023.1 ist die letzte Version, welche eine DNS-SD-Unterstützung zum automatischen Auffinden des Agenten bzw. Servers enthält.
- Das DriveLock Control Center (DCC) wird nicht mehr weiterentwickelt und ist auch nicht mehr Bestandteil unseres Produktes. DriveLock 2021.2 ist die letzte Version, die das DCC bis Mai 2024 offiziell unterstützt.

9 DriveLock Dokumentation

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

Die DriveLock Dokumentation besteht derzeit aus folgenden Dokumenten:

DriveLock Installation

Hier finden Sie Informationen für die 'on-premise'-Installation der einzelnen DriveLock Komponenten.

> Hinweis: Beachten Sie, dass für Kunden der DriveLock Managed Security Services andere Informationen zur Installation zur Verfügung stehen.

DriveLock Administration

Hier finden Sie Informationen zum Betrieb von DriveLock, Anleitungen zur Arbeit mit dem DriveLock Operations Center (DOC), der DriveLock Management Konsole (DMC), dem DriveLock Richtlinien Editor, sowie Einstellungen für den DriveLock Enterprise Service (DES) und den DriveLock Agenten. Außerdem erhalten Sie hier Hilfe bei der Konfiguration von globalen und allgemeinen Einstellungen für Laufwerks-und Gerätekontrolle oder Ereignis-und Betriebssystem-Management.

Application Control

Diese Dokumentation enthält alle Informationen, die Sie für den Einsatz der DriveLock Anwendungskontrolle benötigen.

Defender Management

Hier wird die Integration und Konfiguration von Microsoft Defender in DriveLock beschrieben.

DriveLock Encryption

Folgende Themen sind in dieser Dokumentation enthalten:

- **DriveLock BitLocker Management**

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

- **DriveLock Disk Protection**

  Beschreibt alle notwendigen Konfigurationseinstellungen für die DriveLock Disk Protection (früher FDE).

- **DriveLock Pre-Boot-Authentifizierung**

  Beschreibt die Vorgehensweise, um die DriveLock PBA zur Authentifizierung von Benutzern einrichten und verwenden zu können, sowie Lösungswege zur Wiederherstellung bzw. Notfallanmeldung.

- **DriveLock Netzwerk-Pre-Boot-Authentifizierung**

  Beschreibt die Konfiguration für die Pre-Boot-Authentifizierung innerhalb eines Netzwerks.

- **DriveLock BitLocker To Go**

  Beschreibt alle notwendigen Konfigurationseinstellungen, um BitLocker To Go in DriveLock zu integrieren.

- **DriveLock Encryption 2-Go**

  Enthält Informationen, wie die Verschlüsselung externer Datenträger (wie z.B. USB-Sticks oder SD-Karten) mit Encryption 2-Go funktioniert.

- **DriveLock File Protection**

  Enthält Informationen zur Konfiguration der DriveLock File and Folder Encryption sowie zum neuen Verschlüsselungsformat, das ab Version 2022.2 zum Einsatz kommt.

DriveLock Events

Diese Dokumentation enthält eine Auflistung aller aktuellen DriveLock Ereignisse mit Beschreibung.

Linux Agents

Dieses Dokument beschreibt die Installation und Konfiguration des DriveLock Agenten auf Linux-Betriebssystemen.

macOS Agents

Dieses Dokument beschreibt die Installation und Konfiguration des DriveLock Agenten auf macOS-Betriebssystemen.

Security Awareness

Diese Dokumentation beschreibt die Security Awareness-Funktionen, welche auch die Basis des Produktes DriveLock Security Awareness Content bilden.

Vulnerability Management

Diese Dokumentation beschreibt die DriveLock Schwachstellenscan-Funktionalität, Konfigurationseinstellungen und Verwendung im DOC und in der DMC.

10 Testinstallation von DriveLock

Wenn Sie sich DriveLock im Detail ansehen und das Produkt testen wollen, können Sie über die DriveLock Webseite eine Teststellung beantragen. Folgen Sie hierzu einfach den Links auf unserer Webseite https://www.drivelock.com/.

Wir stellen Ihnen einen cloudbasierten Mandanten zur Verfügung. Somit können Sie sich vollständig auf den DriveLock Agenten und die Schutzfunktionalität von DriveLock konzentrieren.

Nachdem Sie sich für einen Test registriert haben, schicken wir Ihnen verschiedene Emails mit Informationen zur Unterstützung Ihres Tests.

Sollten Sie weitere Informationen und Unterstützung bei Ihren Tests benötigen, wenden Sie sich bitte an info@drivelock.com / sales@drivelock.com.

Copyright