



DriveLock macOS Agent

Dokumentation 2022.2

DriveLock SE 2023



Inhaltsverzeichnis

1 DF	RIVELOCK MACOS-UNTERSTÜTZUNG	4
2 SY	STEMVORAUSSETZUNGEN	5
2.1	Unterstützte macOS-Versionen	5
2.2	2 Konfiguration von DriveLock	5
3 IN	STALLATION DES DRIVELOCK MACOS-AGENTEN	6
3.1	I Installationsschritte für macOS 10.15 Catalina, 11 Big Sur und 12 Monterey	6
3.2	2 Installationsschritte für macOS 13 Ventura	8
3.3	B DriveLock Agenten deinstallieren	
4 KC	DNFIGURATIONSEINSTELLUNGEN	12
4.1	Konfigurations- und Statusabfrage	12
4.2	2 Empfohlene Vorgehensweise	14
4.3	B Richtlinieneinstellungen für DriveLock macOS-Agenten	14
2	4.3.1 Globale Einstellungen	
2	4.3.2 Ereignisse	
	4.3.2.1 Ereigniseinstellungen	16
	4.3.2.2 Ereignisfilter-Definitionen	
	4.3.2.2.1 Ereignisfilter-Defintionen anlegen	17
2	4.3.3 Laufwerke	
	4.3.3.1 Laufwerkseinstellungen	
	4.3.3.2 Laufwerks-Whitelist-Regeln	
4.4	Agenten-Fernkontrolle	20
2	4.4.1 Temporäre Freigabe aus der DMC	21
5 M	ACOS-AGENTEN IM DOC	23
5.1	Lizenzstatus im DOC anzeigen	23
5.2	2 Temporäre Freigabe aus dem DOC	
5.3	Beitrittstoken verwenden	24

6 EREIGNISLISTE	
7 MACOS-TOOLS	
COPYRIGHT	

1 DriveLock macOS-Unterstützung

DriveLock unterstützt die Zuweisung von zentral gespeicherten Richtlinien auf DriveLock Agenten mit Betriebssystem Catalina, Big Sur, Monterey und Ventura – sowohl Intel-als auch ARM-Architektur.

Hinweis: Derzeit ist der macOS-Agent auf Anfrage verfügbar. Bitte wenden Sie sich an Ihren DriveLock Vertriebspartner. Ab DriveLock Version 22.2 HF1 können Sie das macOS Agent-Paket auch aus dem Installationsbereich im DriveLock Operations Center (DOC) herunterladen.

Der Funktionsumfang der macOS-Unterstützung beschränkt sich derzeit auf das gezielte Sperren von externen Laufwerken, die über eine USB-Schnittstelle mit den macOS-Clients verbunden werden. Administratoren haben somit die Möglichkeit, die Verwendung von Laufwerken auch auf DriveLock macOS-Agenten so zu reglementieren, dass die Client-Computer zuverlässig vor Angriffen durch Schadsoftware geschützt sind. Zudem können mit der Risk & Compliance-Funktionalität einige DriveLock-Ereignisse ausgewertet und entsprechende Ereignisfilter-Definitionen erstellt werden.

Hinweis: Der DriveLock Agent wird als Systemerweiterung ausgeliefert und unterstützt somit das Apple Endpoint Security Framework. Weitere Informationen zu Systemerweiterungen und Endpoint Security finden Sie hier und hier.

2 Systemvoraussetzungen

2.1 Unterstützte macOS-Versionen

DriveLock unterstützt macOS ab Version Catalina (10.15) mit Intel (x86_64) und Apple Silicon (arm64) Architekturen.

2.2 Konfiguration von DriveLock

Um DriveLock macOS-Agenten in einer DriveLock-Umgebung verwalten und die Verwendung ihrer USB-Schnittstellen steuern zu können, müssen folgende Konfigurationsvoraussetzungen erfüllt sein.

Installation und Konfiguration von DriveLock mit

- DriveLock Management Konsole (DMC) und Richtlinien-Editor bzw. DriveLock Operations Center (DOC) mit DOC Companion: ab Version 2022.2
- DriveLock Enterprise Service (DES): ab Version 2022.2
- DriveLock macOS-Agent (auf den macOS-Clients): ab Version 2022.2

Hinweis: Bitte beachten Sie, dass auf dem DES immer dieselbe DriveLock-Version oder höher installiert ist wie auf dem DriveLock Agenten.

3 Installation des DriveLock macOS-Agenten

3.1 Installationsschritte für macOS 10.15 Catalina, 11 Big Sur und 12 Monterey

Gehen Sie folgendermaßen vor, um den DriveLock macOs-Agenten zu installieren:

- 1. Kopieren Sie die App DriveLock Agent in den Ordner Applications.
- 2. Klicken Sie mit der rechten Maustaste auf die App **DriveLock Agent** und wählen Sie dann **Paketinhalt zeigen**.
- 3. Öffnen Sie im Ordner Inhalt die Bibliothek und wählen Sie hier die Systemerweiterungen.
- 4. Kopieren Sie die Systemerweiterungsdatei com.dri-

velock.agent.extension.systemextension und schieben Sie diese mittels Drag & Drop an folgende Stelle:

Systemeinstellungen -> Sicherheit & Datenschutz -> Datenschutz -> Festplattenvollzugriff (siehe Abbildung)

Hinweis: Dieser Schritt muss manuell durchgeführt werden und sorgt dafür, dass die Systemerweiterung Vollzugriff erhält.

• • • < > IIII Sicherheit	Q Suchen									
Allgemein FileVault Firewall Datenschutz										
Kamera	Erlaube den unten stehenden Apps, auf Daten wie E-Mails,									
J Mikrofon	bestimmte administrative Einstellungen von allen Benutzern auf diesem Mac zuzugreifen.									
·///· Spracherkennung										
Bedienungshilfen	FotoImporter									
Eingabeüberwachung	com.microsoft.autoupdate.helper	l								
Festplattenvollzugriff	sshd-keygen-wrapper									
Dateien und Ordner	Terminal									
Bildschirmaufnahme	+ -									
Medien & Apple Music										
A Homekit										

5. Zur Änderung der Systemeinstellungen müssen Sie Ihr Passwort eingeben.

 Falls noch nicht geschehen, konfigurieren Sie jetzt den DriveLock Enterprise Service (DES). Geben Sie dazu in der App **Terminal** die folgende Kommandozeile ein:

```
% sudo /Applications/DriveLock\ Agent.ap-
p/Contents/MacOS/dlconfig -t tenant_name -s DES_server_url -d
debug_level
Zum Beispiel:% sudo /Applications/DriveLock\ Agent.ap-
p/Contents/MacOS/dlconfig -t root -s https://DES_HOSTNAME:6067
-d 5
```

- Als nächstes starten Sie die App **DriveLock Agent**, um die Erweiterung zu installieren. Die Systemerweiterung wird zunächst geblockt.
- 8. Erlauben Sie das Laden der Systemsoftware von der Anwendung DriveLock Agent auf dem Reiter **Allgemein** unter **Sicherheit & Datenschutz**, in dem Sie **Erlauben** klicken.

Sicherheit & Datenschutz	Q Suchen
Allgemein FileVault Firewall Datenschutz	
Für diesen Benutzer wurde ein Anmeldepasswort festgelegt Passwort ändern .	
🗹 Passwort erforderlich 🛛 5 Minuten 🛛 🧿 nach Beginn des Ruhezustands oder	Bildschirmschoners
Mitteilung bei gesperrtem Bildschirm einblenden Nachricht für gesperrten	Bildschirm festlegen
✓ Automatische Anmeldung deaktivieren	
Apps-Download erlauben von:	
O App Store	
App Store und verifizierten Entwicklern	
Laden der Systemsoftware des Programms Drivel ock Agent" wurde blockiert.	Frlauben
Zum Schützen auf das Schloss klicken.	Weitere Optionen ?

 Überprüfen Sie dann, ob DriveLock End...gent Extension oder com.drivelock.agent.extension unter Systemeinstellungen -> Sicherheit & Datenschutz -> Datenschutz -> Voller Festplattenzugriff eine Berechtigung erhalten hat.

- Hinweis: Die Berechtigung Festplattenvollzugriff ist zwingend erforderlich, damit der Endpoint Security Client (die Blockierfunktion des DriveLock Agenten) funktioniert.
- Eine weitere Möglichkeit, die Installation (und auch die Aktivität) des DriveLock Agenten zu überprüfen, bietet sich in der Aktivitätsanzeige (siehe Abbildung).

Aktivitätsanzeige Alle Prozesse	(X) (i)	⋯ ∨ CPU Speicher	Energie Festp	latte Netzwerk	Q drivelock	8
Prozessname % CPU ~	CPU-Zeit	Threads Reaktivierung	en Art	% GPU GF	PU-Zeit PID	Benutzer:in
com.drivelock.agent.extension 0,9	0,37	15	4 Apple	0,0	0,00 897	root
com.drivelock.agent.notifier 0,0	0,02	2	0 Apple	0,0	0,00 898	demouser
System:	3,22 %	AUSLASTUNG	Threads:	1.562		
Benutzer:in:	13,83 %		Prozesse:	368		
Inaktiv:	82,95 %					
			4			

3.2 Installationsschritte für macOS 13 Ventura

Gehen Sie folgendermaßen vor, um den DriveLock macOs-Agenten auf macOS-Ventura-Clients zu installieren:

- 1. Doppelklicken Sie die DriveLock Agent.dmg Disk-Image-Datei.
- 2. Verschieben Sie die App **DriveLock Agent** mit Drag & Drop in den Ordner **Applications**.



3. Öffnen Sie die App. Klicken Sie auf **Erweiterung installieren**. Diese wird installiert, sobald die entsprechende Bestätigung vorhanden ist.



4. Als erstes wählen Sie im Bereich Systemeinstellungen -> Datenschutz & Sicherheit den Festplattenvollzugriff für die DriveLock Endpoint Agent Extension.

•••	< Festplattenvollzugriff
Q Suchen	Erlaube den Apps unten, auf Daten wie Mail, "Nachrichten", Safari, Home, Time Machine-Backups und bestimmte administrative Einstellungen von allen
🕑 Allgemein	Benutzer:innen auf diesem Mac zuzugreifen.
Erscheinungsbild	OriveLock Endpoint Agent Extension
🔞 Bedienungshilfen	+ -
Controllzentrum	
💽 Siri & Spotlight	
🕛 Datenschutz & Sicherheit	
Schreibtisch & Dock	
🔅 Displays	
😸 Hintergrundbild	
Bildschirmschoner	
길 Energie sparen	
Sperrbildschirm	

5. Als nächstes erlauben Sie das Laden der Systemsoftware des Programms DriveLock Agent.



 Falls noch nicht geschehen, konfigurieren Sie jetzt den DriveLock Enterprise Service (DES). Geben Sie dazu in der App **Terminal** die folgende Kommandozeile ein:

```
% sudo /Applications/DriveLock\ Agent.ap-
p/Contents/MacOS/dlconfig -t tenant_name -s DES_server_url -d
debug_level
Zum Beispiel:% sudo /Applications/DriveLock\ Agent.ap-
p/Contents/MacOS/dlconfig -t root -s https://DES_HOSTNAME:6067
-d 5
```

7. Die Installation ist erfolgreich abgeschlossen, sobald folgende Meldung erscheint:

•••	DriveLock Agent	
	DriveLock Agent	
	Erweiterung installieren	
Die Installation der Erwei Auf Bestätigung wird gew Die Erweiterung wurde e	iterung beginnt 💽 vartet 🛈 rfolgreich installiert √	

8. In der Aktivitätsanzeige können Sie die Installation (und auch die Aktivität) des DriveLock Agenten überprüfen.

3.3 DriveLock Agenten deinstallieren

Der DriveLock Agent lässt sich durch Löschen der DriveLock Agent-App deinstallieren. Allerdings müssen Sie auch die Systemerweiterung wieder löschen (siehe Abbildung) und diese Aktion durch Eingabe Ihres Passworts bestätigen.



4 Konfigurationseinstellungen

4.1 Konfigurations- und Statusabfrage

Folgende Parameter stehen Ihnen in der Konfigurationsdatei zur Verfügung:

```
🛅 demouser — -zsh — 95×18
                                                                                              ] 日
demouser@PengjiesMiniM1 ~ % /Applications/DriveLock\ Agent.app/Contents/MacOS/dlconfig
Usage: /Applications/DriveLock Agent.app/Contents/MacOS/dlconfig [OPTIONS]
Options:
  -c, --config_cert path
                           config cert path
  -s, --server serverurl
                           server url
 -t, --tenant tenantname
                           tenant name
      --jointoken token
                           tenant join token
 -d, --debug off|<0-7>
                           activate/deactivate logging
 -u, --update
                           update the configuration
 -a, --status
                           show status
  -r, --recreatebootdevices re-create boot devices
      --rescanapps
                           re-create local whitelist hashdb
 -V, --version
                           show version
 -S, --getserver
                           show server
  -T, --gettenant
                           show tenant
 -h, --help
                           print this help and exit
demouser@PengjiesMiniM1 ~ %
```

Erläuterungen zu einzelnen Parametern:

Parameter	Beschreibung
-s,server ser- verurl	Gibt den DES an, mit dem der MacOS-Client kom- muniziert
-t,tenant ten- antname	Gibt den Mandanten für Ihren MacOS-Agenten an
jointoken token	Geben Sie hier den Beitrittstoken an, der während der Installation gesetzt wird
-d,debug off <0-7>	Aktiviert oder deaktiviert das Tracing zu Log Dateien, die im Installationsverzeichnis im Unter- ordner log zu finden sind. (Größere Zahl bedeutet detaillierteres Tracing. Standard ist 4 – Info. Der Wert 0 oder off deaktiviert das Tracing).

Parameter	Beschreibung
-u,update	Aktualisiert Ihre Konfiguration, z.B. wenn Sie Ände- rungen an Ihren Richtlinien gemacht haben Der MacOS Agent verbindet sich dann sofort mit dem DES und lädt die Änderungen
-a,status	Zeigt den aktuellen Status des MacOS-Clients an und informiert, wann z.B. der DES zuletzt kontaktiert wurde, welche Richtlinien zugewiesen oder welche DriveLock Module lizenziert sind (siehe Abbildung unten)
-r,recrea- tebootdevices	Erzeugt eine neue Liste von aktuell verbundenen USB-Geräten, die beim Boot immer erlaubt werden sollten

Um sich den Status des macOS-Agenten anzusehen, verwenden Sie die Option -a.

	🛅 demouser — -zsh — 116×33	
[demouser@PengjiesMiniM	l ~ % /Applications/DriveLock\ Agent.app/Contents/MacOS/dlconfig -a] 🖪
Agent Identity:		
Agent version: Computer Name: Computer GUID: Domain Name:	22.2.42210 PengjiesMiniM1 A fritz.box	
OS Name: OS Version:	macOS Monterey 12.6 (21G115)	
Component licensing st	atus:	
Device control: Application Control:	Licensed No	
Agent Configuration &	Status:	
Tenant: Server URL(s): Last server contact at Last inventory at:	pengjie https://cloud/ : 14.11.2022 18:24:46 14.11.2022 18:19:22	
Temporary unlock:	unknown	- 1
Assigned Policies:		- 1
1 CSP ID: 4a8bb386-46 ConfigName: My test Version: 4 Target: macOS_dynam: Status: CSP Success	be-4947-b747-174674c506b6 ic fully Applied	

4.2 Empfohlene Vorgehensweise

Folgende Vorgehensweise ist für die Konfiguration des DriveLock macOS-Agenten empfohlen:

1. Beginnen Sie mit der Erstellung einer DriveLock-Gruppe (statisch oder dynamisch), die Ihre macOS-Agenten umfasst.

Dies erleichtert das spätere Zuweisen der Richtlinie, die Sie für Ihre macOS-Agenten konfigurieren.

Als Gruppendefinition geben Sie hier das Filterkriterium **Betriebssystem-Typ Linux** an.

In der Abbildung unten ist die dynamische **macOS-Gruppe** mit Beschreibung **Alle macOS-Clients** und Filterkriterium **Betriebssystem-Typ = macOS** definiert.

∃ 🗯 DriveL	oc	k		2					
Dashboard		Gr	unnei	n .		+ Gruppenmitglied hinzufügen +			
•්රද Betrieb	~	0	appe						
		Zieher	n Sie eine Sj	paltenüberschrift hierher, um nach	dieser Spalte zu gruppieren	MAC_Group			
allou Adamentariy	Ť		Тур т	Gruppenname	Definition	 Definitionen 			
මැති Konfiguration	^			۹	٩	2 Delinitionen			
		~	8	MAC_Group	and(eq(inv:OsType,Mac))	Betriebssystemtyp = 'Mac'			
			8	Linux_Group	and(eq(inv:OsType,Linux))				

Weitere Informationen zum Thema DriveLock-Gruppen finden Sie unter DriveLock Administrationauf DriveLock Online Help.

- 2. Falls Sie für Ihre DriveLock macOS-Agenten einen anderen Mandanten verwenden wollen, müssen Sie diesen explizit auswählen. Weitere Informationen zur Verwendung von Mandanten finden Sie ebenfalls in der DriveLock Administration.
- 3. Erstellen Sie eine neue zentral gespeicherte Richtlinie für Ihre macOS-Clients, benennen Sie diese entsprechend (z.B. 'macOS-Richtlinie') und nehmen Sie zunächst globale Einstellungen vor.
- 4. Weisen Sie die 'macOS-Richtlinie' Ihrer DriveLock-Gruppe zu. Eine Zuweisung ist auch auf Alle Computer möglich, wenn Sie keine Gruppe verwenden möchten.

4.3 Richtlinieneinstellungen für DriveLock macOS-Agenten

Folgende Einstellungen in der DriveLock Management Konsole sind relevant bei der Konfiguration von Richtlinien, die auf DriveLock macOS-Agenten zugewiesen werden sollen:

- **Globale Einstellungen**: Einstellungen, Server-Verbindungen, Vertrauenswürdige Zertifikate
- **Ereignisse und Alerts**: Ereignisse (Allgemeine Ereignisse, Geräte- und Laufwerks-Ereignisse), Ereignisfilter-Definitionen
- Laufwerke: Sperr-Einstellungen, Laufwerks-Whitelist-Regeln

Achtung: Beachten Sie bitte, dass sich die Einstellungen für Laufwerke und Geräte für DriveLock macOS-Agenten auf die Steuerung der USB-Schnittstelle beschränken.

Wie Sie Ihre 'macOS-Richtlinie' konfigurieren, hängt von Ihren Vorgaben für Ihre DriveLock macOS-Agenten ab.

Ein Beispiel für Geräte-Einstellungen, die jeweils für alle Benutzer der macOS-Clients gelten:

 Wenn Sie die Verwendung von USB-Laufwerken, z.B. USB-Sticks, grundsätzlich sperren wollen, aber spezielle USB-Sticks erlauben wollen, setzen Sie die entsprechenden Sperr-Einstellungen und erstellen dann eine Laufwerks-Regel für die erlaubten USB-Sticks (Whitelist-Modus).

4.3.1 Globale Einstellungen

- 1. Im Unterknoten Einstellungen können folgende Einstellungen gesetzt werden:
 - Lizenz: Fügen Sie hier die Lizenzen hinzu, die Sie für Ihre macOS-Agenten erworben haben.
 - Agentenfernkontroll-Einstellungen und -Berechtigungen: Auf dem Reiter Zugriffsrechte geben Sie die Benutzer an, die explizit Aktionen auf dem macOS-Agenten ausführen dürfen, beispielsweise Änderungen an der Konfiguration vornehmen.
 - Einstellungen zur Übermittlung von Ereignis-Meldungen: Achten Sie in diesem Dialog darauf, dass auf dem Reiter Server die Option Ereignisse an den DriveLock Enterprise Service senden ausgewählt ist. Sie können mit der zweiten Option Agenten-Status zu Server senden angeben, in welchen Intervallen eine Agent alive-Meldung an den DES geschickt wird.
 - Erweiterte Einstellungen für DriveLock Agenten: Auf dem Reiter Intervalle können Sie die Intervalle angeben, in denen die Konfiguration vom Server geladen werden soll.
 - Einstellungen f
 ür die Protokollierung: Protokollierungsgrad, Maximale Protokolldateigr
 öße in MB und Zeit bis zur automatischen L
 öschung alter Protokolldateien
- 2. Im Unterknoten **Server-Verbindungen** können Sie andere Serververbindungen angeben, falls gewünscht.

- 3. Im Unterknoten **Vertrauenswürdige Zertifikate** wählen Sie die Zertifikate für die sichere Kommunikation zwischen der DriveLock Management Konsole bzw. den DriveLock macOS-Agenten und dem DES aus.
- Hinweis: Weitere Informationen zur allen Einstellungen finden Sie im entsprechenden Kapitel unter DriveLock Administration auf DriveLock Online Help.

4.3.2 Ereignisse

Die Risk & Compliance-Funktionalität bietet eine optimierte Darstellung der einzelnen Ereignisse verbunden mit verschiedenen Filtermöglichkeiten.

Für DriveLock macOs-Agenten sind die Ereignisse der Kategorien **Allgemeine Ereignisse** und **Laufwerks-Ereignisse** wichtig. Unter Ereignisse finden Sie eine detaillierte Liste.

Die Ereignisse können in der Windows Ereignisanzeige oder auf dem DriveLock Enterprise Service aufgezeichnet werden, nicht aber in SNMP oder SMTP.

4.3.2.1 Ereigniseinstellungen

Beispiel für die Konfiguration des Laufwerks-Ereignisses 110, das darauf hinweist, dass ein Laufwerk mit dem DriveLock macOS-Agenten verbunden und nicht gesperrt ist.

- Öffnen Sie im Knoten Ereignisse und Alerts den Unterknoten Ereignisse. Doppelklicken Sie unter Laufwerks-Ereignisse das entsprechende Ereignis. Für macOS-Agenten sind derzeit nur die Einstellungen auf dem Reiter Allgemein möglich (siehe Abbildung).
- 2. Standardmäßig ist die Option System-Ereignisanzeige (**Windows Ereignisanzeige**) ausgewählt, zusätzlich können Sie auch **DriveLock Enterprise Service** auswählen, damit die Ereignisse im Ereignisprotokoll auf dem DES gespeichert werden.
- 3. Die Option **Doppelte Ereignisse unterdrücken** lässt sich bei Bedarf ebenfalls auswählen.

4.3.2.2 Ereignisfilter-Definitionen

Auf macOS-Agenten ist es möglich, Ereignisfilter-Definitionen auf die Ereignisse anzuwenden, die für Linux verfügbar sind.

Sie können dabei filtern

- nach Filterkriterien,
- nach Computern (mit Computernamen oder Drivelock-Gruppen)

• und nach Zeiten.

Durch Ereignisfilter-Definitionen lässt sich die Anzahl der Ereignisse in der DOC-Ereignisansicht reduzieren und somit können relevante Ereignisse leichter gefunden werden.

4.3.2.2.1 Ereignisfilter-Defintionen anlegen

Beispiel: Ereignis 238 (Fernkontrollzugriff) - erzeugt im Laufe einer Sitzung eine Vielzahl von Ereignissen. Um die Anzahl zu reduzieren und nur auf bestimmte einzuschränken, geben Sie Filterkriterien mit bestimmten Parametern an.

Gehen Sie folgendermaßen vor:

- Klicken Sie mit der rechten Maustaste auf den Unterknoten Ereignisfilter-Definitionen im Ereignisse und Alerts-Knoten und wählen Neu... aus dem Menü. Eine Liste der verfügbaren Ereignisse wird angezeigt. Wählen Sie das Ereignis 238 aus.
- 2. Setzen Sie auf dem Reiter **Allgemein** Häkchen bei den Optionen **Windows Ereignisanzeige** und **DriveLock Enterprise Service**.
- 3. Wählen Sie auf dem Reiter Filterkriterien die Parameter aus, nach denen gefiltert werden soll. Durch Klicken auf die Schaltfläche Hinzufügen können Sie die entsprechenden Kriterien und die Operatoren auswählen. Im Beispiel oben wäre ein Kriterium der Funktionsname GetAgentStatus. Dann würde der DriveLock Agent nur die betreffenden Ereignisse schicken.



4.3.3 Laufwerke

4.3.3.1 Laufwerkseinstellungen

Öffnen Sie im Knoten **Laufwerke** den Unterknoten **Sperr-Einstellungen** und doppelklicken Sie die Option **USB-angeschlossene Laufwerke**.

Bei den Laufwerkseinstellungen für Ihre macOS-Richtlinie haben Sie zwei Möglichkeiten:

Hinweis: Beachten Sie, dass f
ür macOS-Richtlinien nur die Einstellungen auf dem Reiter Allgemein relevant sind.

- Wählen Sie die bereits voreingestellte Standardoption Sperren für alle Benutzer: Mit dieser Einstellung ist die Verwendung von allen Laufwerken, die über die USB-Schnittstelle verbunden werden, für alle Benutzer blockiert. Sie müssen in diesem Fall eine Whitelist-Regel erstellen, die bestimmte Laufwerke für die Verwendung zulässt.
- Wählen Sie die Option Erlauben (für alle Benutzer): Diese Option ermöglicht zunächst die Verwendung aller Laufwerke, die über die USB-Schnittstelle verbunden werden. In diesem Fall müssen Sie in Ihrer Laufwerks-Regel genau angeben, welche Laufwerke gesperrt werden sollen.

4.3.3.2 Laufwerks-Whitelist-Regeln

Um eine Laufwerks-Regel (als White- oder Blacklist) zu konfigurieren, gehen Sie folgendermaßen vor:

- 1. Öffnen Sie im Knoten Laufwerke den Unterknoten Laufwerks-Whitelist-Regeln. Öffnen Sie das Kontextmenü, wählen Sie Neu und dann Hardware-ID-Regel.
- 2. Geben Sie auf dem Reiter **Allgemein** die Hardware ID des Laufwerks an. Diese besteht aus Vendor ID (VID), Product ID (PID) und Revisionsnummer (REV).
- 3. Wählen Sie auf dem Reiter **Zugriffsrechte** aus, ob das Laufwerk gesperrt oder erlaubt ist (je nach Ihren allgemeinen Sperreinstellungen).

Achtung: Beachten Sie bitte, dass das Sperren mit Zugriff für definierte Benutzer/Gruppen auf macOS-Agenten nicht möglich ist.

In der Abbildung unten ist das USB-Laufwerk mit der Hardware ID USB\VID_058F&PID_ 6387&REV_0105 für die Verwendung gesperrt.

ſ	📑 Default company policy - Zentra	Hersteller ID / Regel	Modulname		Seriennummer		Status	Regel-Typ
١	> 🖑 Globale Einstellungen	Enter text here	Enter text here	Y	Enter text here	Y	Enter text h 🗑	Enter text h 🍸
	Kerreignisse und Alerts Q Laufwerke	Hardware-ID	USB\VID_058F&PID.				Gesperrt	Hardware-ID-R
	Sperr-Einstellungen Laufwerks-Whitelist-Reg	Neue Ausnahme Prop	erties		?	×	:	
	🗟 Whitelist-Regel-Vorla	Netzwerke Ange	emeldete Benutzer	La	ufwerke Awar	eness		
	> 🗟 Dateifilter-Vorlagen	Nachrichten Versch	lüsselung Optionen	L	aufwerks-Scan	Befehle	•	
	📇 Laufwerkslisten	Allgemein Zugriffsn	echte Filter / Schatt	enk	. Zeiten Co	mputer	•	
	Autorisierte Medien	Hardware-ID USB\VI	D_058F&PID_6387&RE	V_(0105			
	> 🖭 Geräte	Diese Art von Begeln b	seiert suf der Windowe	Ham	dware-ID (z B			
	> Netzwerkprofile	"USBSTOR\DiskVendo	pr_Product") und dient d	ler h	Kompatibilität bei de	r		
	> [6] Anwendungen	Migration von anderen	Endgerätesicherheitslös	ung	en auf DriveLock.			
	Verschlüsselung Defender Management	Aktiv						
I								

4.4 Agenten-Fernkontrolle

Öffnen Sie in der DriveLock Management Konsole im Knoten **Betrieb** den Unterknoten **Agenten-Fernkontrolle**. Sie sehen eine Liste der Client-Computer, auf denen der DriveLock Agent installiert ist (siehe Abbildung).

Hinweis: Weitere Informationen zum Thema Agenten-Fernkontrolle finden Sie im Administrationshandbuch auf drivelock.help.

Klicken Sie im Kontextmenü des ausgewählten macOS-Clients auf Verbinden.

Folgende Funktionen der Agenten-Fernkontrolle sind für DriveLock macOS-Agenten relevant:

Trennen	
Temporär freigeben	
RSOP anzeigen	
Agentenkonfiguration	
Inventarisierungsdaten anzeigen	
Lokale Applikationskontroll-Whitelist and	reigen
All Tasks	>
Properties	
Help	

- 1. Trennen der Verbindung
- 2. Temporär freigeben...: weitere Informationen hier.

3. RSOP anzeigen...

Klicken Sie diese Option, um sich eine Zusammenfassung der Richtlinie zeigen zu lassen, die auf den macOS-Agenten zugewiesen ist. Änderungen lassen sich hier nicht durchführen.

4. Agentenkonfiguration...

Hier öffnet sich ein Dialog mit Informationen zur Konfiguration. Sie sehen, von welchem Server Ihr macOS-Agent die zentral gespeicherte Richtlinie erhält und können ggf. einen weiteren Server hinzufügen oder auf dem Reiter **Optionen** einen anderen Mandanten auswählen.

5. Inventarisierungsdaten anzeigen

Klicken Sie diese Option, um Inventarisierungsinformationen zu Ihrem macOS-Agenten zu erhalten (auf den Reitern **Allgemein**, **Laufwerke** und **Netzwerke**).

4.4.1 Temporäre Freigabe aus der DMC

Mithilfe der temporären Freigabe können Sie schnell und zeitlich begrenzt einem verbundenen DriveLock macOS-Agenten den Zugriff auf gesperrte Laufwerke über die Agentenfernkontrolle im der DriveLock Management Konsole (DMC) ermöglichen.

Aus dem DriveLock Operations Center (DOC) heraus geht dies ebenso.

Gehen Sie folgendermaßen vor:

- 1. Wählen Sie im Kontextmenü des macOS-Agenten den Menübefehl **Temporär frei**geben....
- 2. Geben Sie an, für was die Freigabe gelten soll (Laufwerkstypen).

Laufwerke temporär freigeben X
Agent temporär freigeben Bitte wählen Sie, welche Art von Laufwerken / Geräten entspert werden sollen.
Temporäre Freigabe auf Agent ubuntu
Bitte wählen Sie, welche Laufwerke oder Geräte Sie freigeben wollen:
Alle freigeben 🗌 Laufwerkstypen
Gerätetypen
< Back Next > Cancel

3. Dann definieren Sie den Zeitraum für die Freigabe und geben einen Grund für die Frei-

gabe an.

Laufwerke temporär freigeben	×		
Agent temporär freigeben Bitte wählen Sie die Dauer der Aufhebung der Sperre.			
Bitte wählen Sie, wie lange die Freigabe der Agenten dauem soll: Image: Strategy S			
Grund für Freigabe (für Reporting)			
< Back Finish	Cancel		

5 macOS-Agenten im DOC

DriveLock macOS-Agenten werden wie andere DriveLock Agenten im DriveLock Operations Center angezeigt.

Folgende DOC-Ansichten sind für macOS-Agenten relevant:

- **Computer**: Filtern Sie z.B. nach **OS Typ**, um Ihre macOS-Agenten anhand ihres Betriebssystems gruppieren zu lassen. Markieren Sie einen beliebigen macOS-Agenten, um sich Details anzusehen.
- Gruppen: Wenn Sie eine DriveLock Gruppe f
 ür Ihre macOS-Agenten definiert haben, wird diese mit Informationen zu den jeweiligen Mitgliedern und den zugewiesenen Richtlinien hier angezeigt.
- **Ereignisse**: Die Ereignisse, die ein macOS-Agent an den DES schickt, werden in dieser Ansicht aufgelistet.
- **Alerts**: Die Alerts-Ansicht ermöglicht eine kontinuierliche Überwachung und konfigurierbare Reaktion auf sicherheitsrelevante Ereignisse.
- **Benutzer**: In dieser Ansicht sehen Sie eine Auflistung aller Benutzerkonten, die auf das DOC zugreifen dürfen. Es werden auch Status- und Rolleninformationen, sowie Name und Anmeldedaten angezeigt.

5.1 Lizenzstatus im DOC anzeigen

Der macOS-Agent unterstützt per Richtlinie konfigurierte Drivelock-Lizenzen für die Laufwerkskontrolle.

Der Agent aktiviert die Komponenten entsprechend der Lizenz und meldet den korrekten Lizenzstatus an den DriveLock Enterprise Service (DES). Dies kann in den Details des Computers in DOC überprüft werden.

5.2 Temporäre Freigabe aus dem DOC

Es ist möglich, die Laufwerkskontolle auf den macOS-Agenten vom DriveLock Operations Center (DOC) aus mit Hilfe der Aktion **Computer online entsperren** vorübergehend zu entsperren.

Die temporäre Freigabe endet nach dem konfigurierten Zeitlimit. Wenn eine absolute Zeit angegeben wird, überlebt die temporäre Freigabe einen Neustart, wenn die Zeit noch im konfigurierten Zeitraum liegt. Die temporäre Freigabe kann mit der Option Freigabe beenden gestoppt werden.

Für die Gerätekontrolle können alle USB-Laufwerke auf einmal freigeschaltet werden.

5.3 Beitrittstoken verwenden

Die Funktionalität für das abgesicherte Hinzufügen von Agenten mittels eines Beitrittstokens kann auch für macOS-Agenten verwendet werden. Nach der Installation wird hierzu ein Beitrittstoken mit der Option --jointoken gesetzt.

Beispiel: #sudo ./dlconfig -t root -s https://192.168.8.75:6067 --jointoken fa173c1e-6403-439d-8850-f0a71a2fbea7

Sie finden das Beitrittstoken eines macOS-Clients in den Computerdetails im DOC.

6 Ereignisliste

Folgende Tabelle enthält alle macOS-relevanten Ereignisse, die im DriveLock Operations Center (DOC) angezeigt werden. Der Auslöser für jedes der unten aufgelisteten Ereignisse ist DriveLock.

Eine Auflistung aller Ereignisse, die in Zusammenhang mit DriveLock wichtig sind, finden Sie in der Ereignis-Dokumentation auf auf DriveLock Online Help.

Der DriveLock macOS-Agent meldet folgende Ereignisse an den DES:

Ereignis ID	Ebene	Text	Beschreibung
Nummer	Ebene	Text	Beschreibung
105	Information	Dienst gestartet	Der Dienst [Name] wurde gestartet.
108	Information	Dienst beendet	Der Dienst [Name] wurde beendet.
110	Audit	Laufwerk verbunden, nicht gesperrt	Das Laufwerk [Name] ([Kategorie]) wurde dem System hinzugefügt. Es handelt sich um ein [Typ]- Bus-Gerät. Das Laufwerk sollte für diese Benut- zerkennung [gesperr- t/entsperrt] sein. Geräteidentifikation: [ID] [ID] (Rev. [rev]) (Seri- ennummer [Nummer]) Angewendete Whitelist- Regel: [Regel] Bildschirm- Status (Tasten [Win]-[L]): [Status]

Ereignis ID	Ebene	Text	Beschreibung
111	Audit	Laufwerk verbunden und gesperrt	Das Laufwerk [Name] ([Kategorie]) wurde dem System hinzugefügt. Es konnte aufgrund eines Sys- temfehlers nicht gesperrt werden. Es handelt sich um ein [Typ]-Bus-Gerät. Das Laufwerk sollte für diese Benutzerkennung [gesperr- t/entsperrt] sein. Gerä- teidentifikation: [ID] [ID] (Rev. [rev]) (Seriennummer [Nummer]) Angewendete Whitelist-Regel: [Regel] Bildschirm-Status (Tasten [Win]-[L]): [Status]
131	Audit	Temporäre Freigabe	Der {Product} Agent wurde durch einen Administrator temporär freigegeben. Administrator-Computer: [ComputerName] (Ein- deutige ID [Com- puterGuid]). Administratorkennung: [UserName] (Domäne [Domain], SID [SID])
132	Audit	Temporäre Freigabe abgebrochen	Die temporäre Freigabe des {Product} Agenten wurde durch einen Admi- nistrator vorzeitig beendet.

Ereignis ID	Ebene	Text	Beschreibung
			Administrator-Computer: [ComputerName] (Ein- deutige ID [Com- puterGuid]). Administratorkennung: [UserName] (Domäne [Domain], SID [SID]
139	Warnung	Temporäre Freigabe beendet	Die temporäre Freigabe des Agenten wurde been- det, da die konfigurierte Zeit abgelaufen ist.
152	Warnung	Richt- liniendateispeicher-Ent- packfehler	Der Richt- liniendateispeicher [Name] kann nicht entpackt wer- den. Einige Funktionen, welche diese Dateien benö- tigen, werden fehl- schlagen.
153	Warnung	Konfigurationsdatei angewendet	Die Konfigurationsdatei [Name] wurde erfolgreich angewendet.
154	Fehler	Konfigurations-Datei Download-Fehler	Die Konfigurationsdatei [Name] kann nicht her- untergeladen werden. Feh- ler-Code: [Code] Fehler: [Fehler]

DriveLock

Ereignis ID	Ebene	Text	Beschreibung
158	Fehler	Konfigurations-Datei Fehler	Die Konfigurationsdatei [Name] kann nicht gelesen werden. Fehler-Code: [Code] Fehler: [Fehler]
191	Warnung	{PrefixEnterpriseService} ausgewählt	Der {Pre- fixEnterpriseService} [Name] wurde von {Pro- duct} ausgewählt. Ver- bindungs-ID: [ID] Benutzt für: [Inven- tory/Recovery/Events]
192	Warnung	{PrefixEnterpriseService} nicht verfügbar	Es ist kein {Pre- fixEnterpriseService} ver- fügbar, weil keine gültige Verbindung konfiguriert ist.
199	Warnung	Laufwerke temporär frei- gegeben	Folgende Laufwerkstypen wurden durch den Admi- nistrator temporär frei- gegeben: [DriveType1] [DriveType2] [DriveType3] [DriveType4] [DriveType5] [DriveType6] [DriveType7] [DriveType8]
			[DriveType9] [Dri- veType10]

Ereignis ID	Ebene	Text	Beschreibung
200	Warnung	Geräte temporär frei- gegeben	Folgende Geräteklassen wurden durch den Admi- nistrator temporär frei- gegeben: [DeviceTypes]
235	Fehler	SSL: Kann nicht initia- lisiert werden	Das Modul für ver- schlüsselte Kom- munikation (SSL) konnte nicht initialisiert werden. Fehler: [Fehler]
236	Fehler	Fernkontrolle: Kann Ser- ver nicht initialisieren	Die Serverkomponente für Agentenfernkontrolle konnte nicht initialisiert werden. Agen- tenfernkontrolle ist nicht verfügbar. Fehler: [Fehler]
237	Fehler	Fernkontrolle: Interner Fehler	Agentenfernkontrolle: Ein interner SOAP-Kom- munikationsfehler ist auf- getreten. Fehler: [Fehler]
238	Suc- cessAudit	Fernkontrolle: Funktion aufgerufen	Eine Funktion der Agen- tenfernkontrolle wurde auf- gerufen. Aufrufende IP- Adresse: [IP-Adresse] Auf- gerufene Funktion: [Funk- tion]
243	Fehler	Kann Kon-	Eine Kon-

Ereignis ID	Ebene	Text	Beschreibung
		figurationsdatenbank nicht öffnen	figurationsdatenbank konnte nicht geöffnet wer- den. Datenbank-Datei: [Name] Fehler-Code: [Code] Fehler: [Fehler]
246	Fehler	Kann Kon- figurationsstatus nicht speichern	Der {Product}-Agent kann den Konfigurationsstatus nicht speichern, der von anderen {Product}-Kom- ponenten benutzt wird. Fehler-Code: [Code] Feh- ler: [Fehler]
247	Fehler	Kann Konfigurations- Speicher nicht initia- lisieren	Der {Product}-Agent kann den Kon- figurationsdatenbank-Spei- cher nicht initialisieren.
249	Fehler	Konfigurationsdatei: Alles-Sperren-Kon- figuration wird ange- wendet	Eine Konfiguration mit Kon- figurations-Dateien wurde erkannt aber es konnten keine Einstellungen aus einer Kon- figurationsdatenbank gele- sen werden. {Product} wird eine Konfiguration ver- wenden, in der alle Wech- seldatenträger gesperrt sind.

Ereignis ID	Ebene	Text	Beschreibung
250	Warnung	Konfigurationsdatei: Benutze zwi- schengespeicherte Kopie	Die Konfigurationsdatei [Name] konnte nicht von ihrem ursprünglichen Ort geladen werden. Eine lokal zwischengespeicherte Kopie wird benutzt.
251	Fehler	Konfigurationsdatei: Kann nicht extrahiert werden.	Eine {Product}-Kon- figurationsdatei konnte nicht extrahiert werden. Einstellungen aus dieser Datei werden nicht ange- wendet. Datenbankdatei: [Name] Fehler-Code: [Code] Fehler: [Fehler]
264	Fehler	Kann Kon- figurationsdatenbank nicht mit RSoP zusam- menführen	Die Kon- figurationsdatenbank [Name] kann nicht mit dem Richt- linienergebnissatz zusam- mengeführt werden.
287	Fehler	Kein Server für Inven- tarisierung definiert	Es ist kein Server für den Upload von Hard- und Soft- war- einventarisierungsdaten definiert.
288	Information	Inventarisierung erfolg-	Hard- und Soft-

Ereignis ID	Ebene	Text	Beschreibung
		reich	war- einventarisierungsdaten wurden erfolgreich gesam- melt und hochgeladen. DES-Server: [Servername] Verbindungs-ID: [ID]
289	Information	Inventarisierung fehl- geschlagen	Beim Sammeln von Hard- und Soft- war- einventarisierungsdaten ist ein Fehler aufgetreten. DES-Server: [Servername] Verbindungs-ID: [ID] Feh- ler: [Fehler]
294	Fehler	Kann zentral gespei- cherte Richtlinie nicht laden	Die zentral gespeicherte Richtlinie [Name] kann nicht heruntergeladen wer- den. Server: [Name] Fehler: [Fehler]
295	Fehler	Zentral gespeicherte Konfiguration: Kann nicht extrahiert werden.	Eine zentral gespeicherte Richtlinie konnte nicht extrahiert werden. Ein- stellungen aus dieser Datei werden nicht angewendet. Konfigurations-ID: [ID] Feh- ler: [Fehler]
297	Fehler	Zentral gespeicherte	Eine Konfiguration mit zen-

Ereignis ID	Ebene	Text	Beschreibung
		Richtlinie: Alles-Sperren- Konfiguration wird ange- wendet	tral gespeicherter Richt- linie wurde erkannt aber es konnten keine Ein- stellungen vom Server geladen werden. {Product} wird eine Konfiguration verwenden, in der alle Wechseldatenträger gesperrt sind.
299	Information	Zentral gespeicherte Richtlinie her- untergeladen	Die zentral gespeicherte Richtlinie [Name] wurde erfolgreich her- untergeladen. Kon- figurations-ID: [ID] Version: [Version]
443	Fehler	Start einer Komponente fehlgeschlagen	Eine {Product}-Sys- temkomponente konnte auf diesem Computer nicht gestartet werden. Fehlercode: [Code] Fehler- Code: [Code] Fehler: [Feh- ler]] Komponenten-ID: [ID]
520	Fehler	Alle {PrefixES} nicht erreichbar	Die Unter- nehmensrichtlinie kann nicht geladen werden. Alle konfigurierten {Pre- fixEnterpriseService}s sind nicht erreichbar.

O	DriveLock
---	-----------

	6 Ereignisliste
Beschreihu	20

Ereignis ID	Ebene	Text	Beschreibung
521	Fehler	Kann Computer-Token nicht ermitteln	Der Computer-Token kann nicht ermittelt werden. Feh- ler-Code: [Code] Fehler: [Fehler]
522	Fehler	Fehler beim Laden von Richtlinienzuweisungen	Beim Laden der Richt- liniezuweisungen von Ser- ver [Name] ist ein Fehler aufgetreten. Fehler: [Feh- ler]
523	Fehler	Richt- linienintegritätsprüfung fehlgeschlagen	Die Integrität einer zuge- wiesenen Richtlinie konnte nicht überprüft werden. Richtlinien-ID: [ID] Richt- linienname: [Name] Aktu- eller Hashwert: [Wert] Erwarteter Hashwert: [Wert]
533	Warnung	Keine Richtlinie - wurde gelöscht	Die Unter- nehmensrichtlinie wurde gelöscht, da der Computer für eine zu lange Zeit off- line war.
584	Information	Inventarisierung gest- artet	Inventarisierung wurde durch den DES gestartet.
639	Fehler	Server Zertifikat Fehler	Server Zertifikatsfehler auf- getreten. Zertifikat:

Ereignis ID	Ebene	Text	Beschreibung
			[Name]. Fehlermeldung: [Text]

7 macOS-Tools

Folgende Kommandozeilentools stehen für macOS zur Verfügung:

- 1. % sudo systemextensionsctl list: Zeigt die Systemerweiterungen an.
- 2. % sudo launchctl list 6GZR4TWXD2.com.drivelock.agent.extension: Zeigt Details zum Prozess der Erweiterung des Drivelock-Agenten an





Copyright

Die in diesen Unterlagen enthaltenen Angaben und Daten, einschließlich URLs und anderen Verweisen auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, Organisationen, Produkte, Personen und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Personen oder Ereignissen ist rein zufällig. Die Verantwortung für die Beachtung aller geltenden Urheberrechte liegt allein beim Benutzer. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der DriveLock SE kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht. Es ist möglich, dass DriveLock SE Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von DriveLock SE eingeräumt. Weitere in diesem Dokument aufgeführte tatsächliche Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

 $\ensuremath{\mathbb{C}}$ 2023 DriveLock SE. Alle Rechte vorbehalten.

