




DriveLock Linux-Agenten

Handbuch 2021.1

DriveLock SE 2021



Inhaltsverzeichnis

| | |
|--|-----------|
| 1 DRIVELOCK LINUX-AGENT | 4 |
| 2 SYSTEMVORAUSSETZUNGEN | 5 |
| 2.1 Unterstützte Linux-Distributionen | 5 |
| 2.2 Konfiguration von DriveLock | 5 |
| 3 INSTALLATION DES DRIVELOCK LINUX-AGENTEN | 6 |
| 3.1 Installationsschritte | 6 |
| 3.2 Installationsparameter | 7 |
| 3.3 Installation auf IGEL-Clients | 7 |
| 3.3.1 Konfiguration des UMS-Servers | 9 |
| 4 KONFIGURATIONSEINSTELLUNGEN | 13 |
| 4.1 Empfohlene Vorgehensweise | 13 |
| 4.2 Richtlinieneinstellungen für DriveLock Linux-Agenten | 14 |
| 4.2.1 Globale Einstellungen | 15 |
| 4.2.2 EDR | 15 |
| 4.2.2.1 Ereigniseinstellungen | 16 |
| 4.2.2.2 Ereignisfilter-Definitionen | 16 |
| 4.2.2.2.1 Ereignisfilter-Defintionen anlegen | 17 |
| 4.2.3 Laufwerke | 18 |
| 4.2.3.1 Laufwerkseinstellungen | 18 |
| 4.2.3.2 Laufwerks-Whitelist-Regeln | 19 |
| 4.2.4 Geräte | 20 |
| 4.2.4.1 Unterstützte Geräteklassen für Linux-Agenten | 20 |
| 4.2.4.2 Geräteeinstellungen | 20 |
| 4.2.4.2.1 Geräte-Whitelist-Regeln (USB-Schnittstelle) | 22 |
| 4.2.4.2.2 Geräte-Whitelist-Regeln (Geräte) | 23 |
| 4.2.4.2.3 Android- und Apple-Geräte | 23 |

| | |
|---|-----------|
| 4.2.4.2.4 Gerätelisten | 24 |
| 4.2.4.2.4.1 Gerätelisten anlegen | 25 |
| 4.2.5 Anwendungen | 26 |
| 4.2.5.1 Voraussetzungen für Application Control auf Linux-Agenten | 26 |
| 4.2.5.2 Scan- und Blockiermodus | 27 |
| 4.2.5.3 Datei-Eigenschaften-Regel (für Linux) | 28 |
| 4.2.5.4 Spezielle Regel (für Linux) | 29 |
| 4.3 Agenten-Fernkontrolle | 30 |
| 5 LINUX-AGENTEN IM DCC | 32 |
| 5.1 DCC: HelpDesk-Aktionen | 32 |
| 6 LINUX-AGENTEN IM DOC | 34 |
| 7 EREIGNISLISTE | 35 |
| 8 KOMMANDOZEILENPROGRAMM | 47 |
| COPYRIGHT | 49 |

1 DriveLock Linux-Agent

DriveLock unterstützt die Zuweisung von zentral gespeicherten Richtlinien auf DriveLock Agenten mit dem Betriebssystem Linux.

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

2 Systemvoraussetzungen

2.1 Unterstützte Linux-Distributionen

DriveLock unterstützt folgende Linux-Distributionen (als 64-Bit Varianten) in den genannten Versionen und höher:

- CentOS Linux 8
- Debian 7
- Fedora 31
- IGEL OS ab Version 10
- Red Hat Enterprise Linux 5
- SUSE 15.1
- Ubuntu 18.04

2.2 Konfiguration von DriveLock

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

Vollständige Installation und Konfiguration einer DriveLock Suite mit

- DriveLock Management Konsole (DMC): Version 2019.2 und neuer
- DriveLock Enterprise Service (DES): Version 2019.2 SP1 und neuer
- DriveLock Linux-Agent (auf den Linux-Clients): Version 2019.2 SP1 und neuer




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 Linux-Agenten

3.1 Installationsschritte

Gehen Sie folgendermaßen vor, um den DriveLock Linux-Agenten auf Ihren Linux-Clients zu installieren.


 Hinweis: Beachten Sie bitte, dass die Installation bei [IGEL-Clients](#) abweicht.

1. Kopieren und entpacken Sie die Datei **drivelock.tgz** auf Ihren Linux-Clients. Sie ist auf dem DriveLock-ISO-Image enthalten.
2. Die Datei enthält das Installationskript **drivelockd-install.sh**. Führen Sie dieses Skript aus (siehe auch [Installationsparameter](#)).

 Achtung: Zur Skriptausführung auf dem Linux-Client werden Administrator-Rechte benötigt (siehe Abbildung).

```
test@debian10:~$ sudo ./drivelockd-install.sh
[sudo] password for test:
Drivelock self extract installer
extracting archive...
install to path [suggest: '/opt/drivelock']:
drivelock server url [format: http(s)://<server>:<port>]: https://192.168.8.249:6067
drivelock tenant [default: root]: kav
installing drivelock linux agent to: '/opt/drivelock'
setting server to: 'https://192.168.8.249:6067'
setting tenant to: 'kav'
starting agent ...
```

3. Geben Sie dabei folgendes an:
 - Installationsverzeichnis: Als Standard wird hier `/opt/drivelock` vorgeschlagen, Sie können aber auch einen anderen Pfad angeben.
 - DES und Port: Geben Sie hier die Server-URL im Format `'https://<Server>:<Port>'` ein.
 - Mandant: Als Standard wird hier `'root'` vorgeschlagen, Sie können aber auch einen anderen Mandanten (tenant) angeben (in der Abbildung `kav`).
4. Sobald die Installation des DriveLock Linux-Agenten abgeschlossen ist, startet der DriveLock Service.
5. Sollte es zu Fehlern während der Installation kommen, wird ein Neustart des Linux-Clients empfohlen, um sicher zu stellen, dass alle DriveLock-Meldungen in der Benutzeroberfläche des Linux-Clients angezeigt werden.

 Hinweis: Auf dem Linux-Client werden nur Meldungen beim Verbinden oder Trennen von Geräten angezeigt (als Popups), eine eigene Benutzeroberfläche für den DriveLock Agenten gibt es hier nicht.

3.2 Installationsparameter

Für die Installation des DriveLock Linux-Agenten auf Ihren Linux-Clients können Sie alternativ Installationsparameter verwenden. Um sich die einzelnen Parameter anzeigen zu lassen, öffnen Sie das Installationskript mit dem Parameter `-h` (siehe Abbildung).

```

test@debian10:~$ sudo ./drivelockd-install.sh -h
Drivelock self extract installer
extracting archive...
usage: ./drivelockd-install.sh [options]

options:
-h|--help                print this help message
-c|--custom-part         create a custom partition package
-i|--install <PATH>     install into path
-s|--server <SRV>       server
-t|--tenant <TENANT>    tenant
test@debian10:~$ sudo ./drivelockd-install.sh -t kav -s https://192.168.8.207:6067

```

Folgende Installationsparameter können angegeben werden:

- `-h`: Anzeige der Installationsparameter
- `-c`: Dieser Parameter ist nur für IGEL-Clients anwendbar. Hier wird das zu erstellende 'Custom Partition Package' angegeben.
- `-i`: Geben Sie hier den Pfad zum Installationsverzeichnis für DriveLock an. Als Standard wird hier das aktuelle Arbeitsverzeichnis vorgeschlagen, Sie können aber auch einen anderen Pfad angeben.
- `-s`: Geben Sie hier den Server im Format 'https://<server>:<port>' ein. Siehe Abbildung oben.
- `-t`: Geben Sie hier den Mandanten (tenant) an, Standard ist 'root'.

3.3 Installation auf IGEL-Clients

Gehen Sie folgendermaßen vor, um den DriveLock Linux-Agenten auf Ihren IGEL-Clients zu installieren.

1. Kopieren und entpacken Sie die Datei **tar -xzf drivelock.tgz** auf Ihren Linux-Clients. Sie ist auf dem DriveLock-ISO-Image enthalten.
2. Die tar-Datei enthält das Installationskript **drivelockd-install.sh**. Führen Sie dieses Skript mit Parameter `-c` aus (siehe Abbildung).

```
test@testub:~/igel_custom_partition$ ./drivelockd-install.sh -c
Drivelock self extract installer
extracting archive...
install to path [suggest: '/home/test/igel_custom_partition']:
drivelock server url [format: http(s)://<server>:<port>]: https://192.168.8.207:6067
drivelock tenant [default: root]:
installing drivelock linux agent to: '/home/test/igel_custom_partition'
setting server to: 'https://192.168.8.207:6067'
setting tenant to: 'root'
path to save custom partition package [default: '/home/test/igel_custom_partition']:
custom partition package name [default: 'drivelock']:
```

Weitere Informationen finden Sie unter [Installationsparameter](#).

3. Geben Sie dabei folgendes an:

- Installationsverzeichnis: Als Standard wird hier das aktuelle Arbeitsverzeichnis vorgeschlagen, Sie können aber auch einen anderen Pfad angeben (in der Abbildung ist das `/home/test/igel_custom_partition`).
- DES und Port: Geben Sie hier die Server-URL im Format `'https://<Server>:<Port>'` ein.
- Mandant: Als Standard wird hier `root` vorgeschlagen, Sie können aber auch einen anderen Mandanten (tenant) angeben.
- Pfad und Name für die benutzerdefinierten IGEL OS-Partitionsdateien. Standardmäßig werden die Dateien im aktuellen Arbeitsverzeichnis erstellt.



Hinweis: Für diesen Vorgang benötigen Sie keine Root-Rechte.

4. Sobald das Skript abgeschlossen ist, werden die IGEL OS-Partitionsdateien `drivelock.inf` und `drivelock.tar.bz2` generiert und können in dem im obigen Schritt angegebenen Pfad gefunden werden.

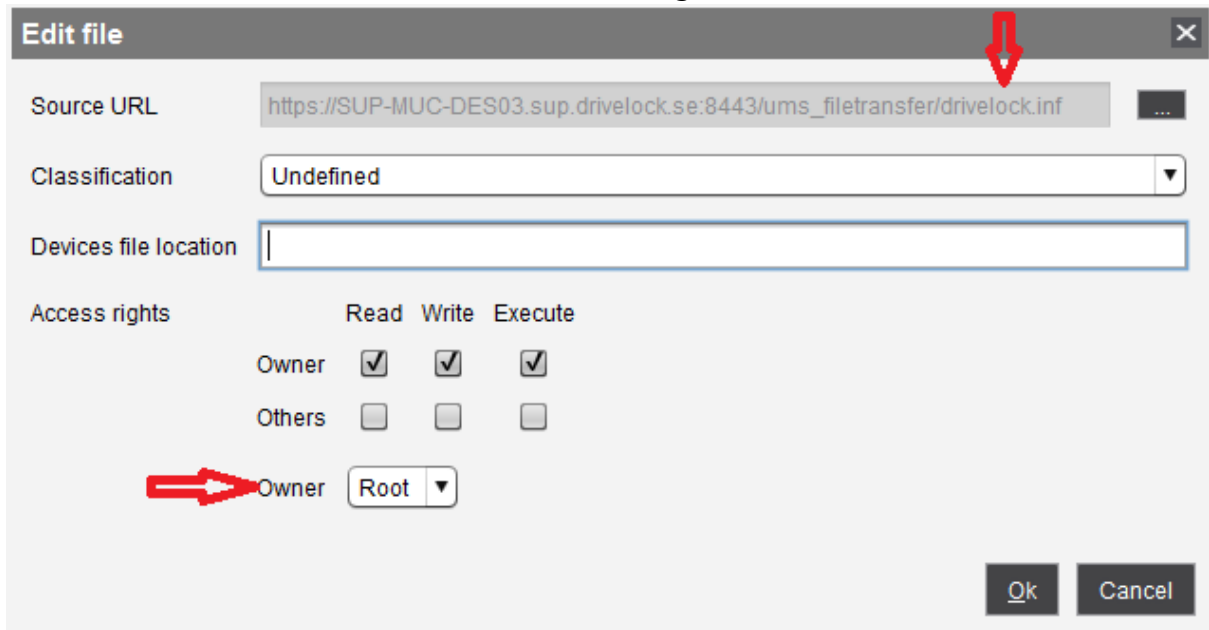
```
test@testub:~/igel_custom_partition$ ls -al
total 42224
drwxr-xr-x  3 test test    4096 Feb 19 10:02 .
drwxr-xr-x 15 test test    4096 Feb 19 10:00 ..
drwxr-xr-x  2 test test    4096 Feb 14 16:45 bin
-rwxr-xr-x  1 test test   1032 Feb  4 18:09 dl_getinfo
-rw-r--r--  1 test test  36864 Feb 19 10:02 DLSettings.db3
-rw-r--r--  1 test test  36864 Feb 19 10:02 DLSettings.db3-ini
-rwxr-xr-x  1 test test   3723 Feb  4 18:09 drivelock-ctl
-rwxr-xr-x  1 test test 14694959 Feb 14 16:45 drivelockd-install.sh
-rwxr-xr-x  1 test test    213 Jan  7 13:55 drivelockd.service
-rw-r--r--  1 test test    72 Feb 19 10:02 drivelock.inf
-rw-r--r--  1 test test 13974612 Feb 19 10:02 drivelock.tar.bz2
-rwxr-xr-x  1 test test 14451584 Feb 19 10:01 drivelock.tgz
-rwxr-xr-x  1 test test    127 Jan  7 13:55 run
```

5. Anschließend konfigurieren Sie den [UMS-Server](#).

3.3.1 Konfiguration des UMS-Servers

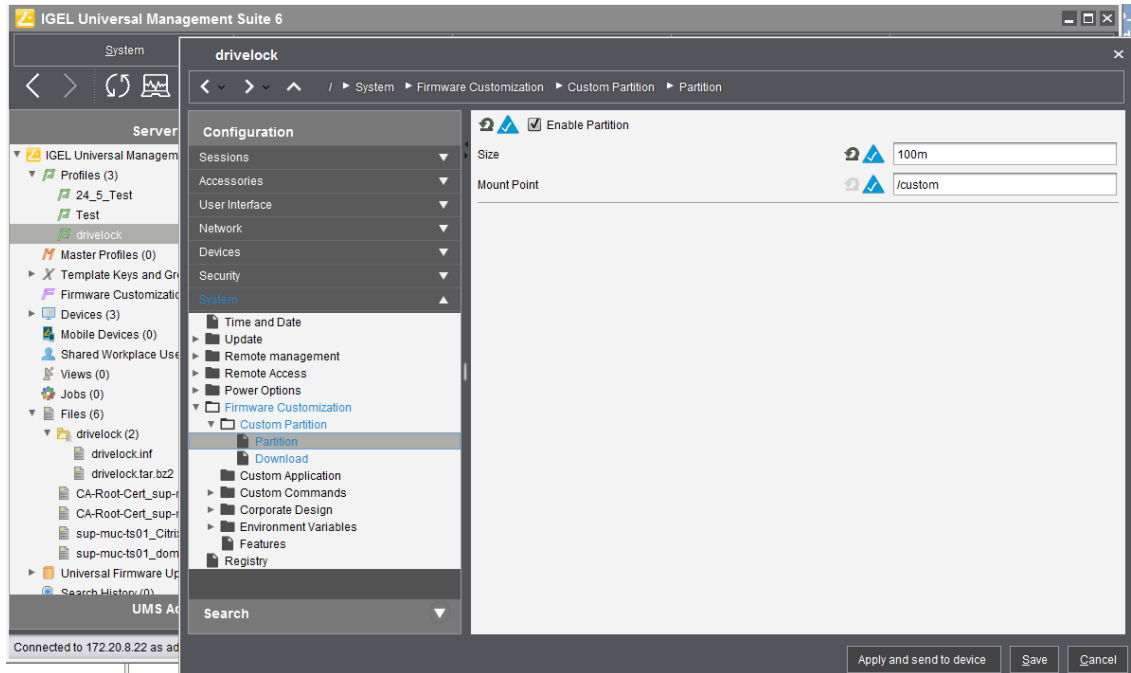
Gehen Sie folgendermaßen vor:

1. Laden Sie die Dateien **drivelock.inf** und **drivelock.tar.bz2** auf den UMS-Server hoch.
2. Öffnen Sie die UMS-Konsole.
3. Öffnen Sie in der UMS-Konsole den Menüpunkt **Files**, wählen dann **New File** und dann den Menübefehl **Upload local file to UMS server**
4. Wählen Sie **Root** als **Owner** aus (siehe Abbildung).



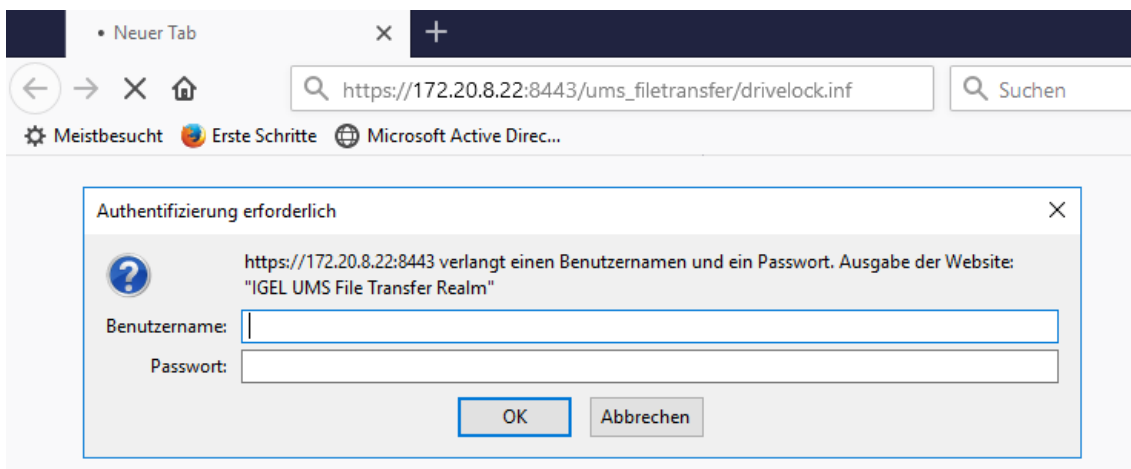
5. Wiederholen Sie das Gleiche für die Datei **drivelock.tar.bz2**.
6. Erstellen Sie im UMS-System ein neues Profil, z.B. drivelock.
7. Wählen Sie in der UMS-Konsole zuerst **Profiles**, dann **New Profile** und **Profile name**.
8. Bearbeiten Sie das erstellte Profil und aktivieren Sie die Custom Partition folgendermaßen (siehe Abbildung):
 1. Öffnen Sie **System** -> **Firmware Customization** -> **Custom Partition** -> **Partition**
 2. Geben Sie **Enable Partition** frei
 3. Setzen Sie ein Häkchen bei **Enable Partition**
 4. Legen Sie die Größe der Partition auf 150 oder 200 MB fest

5. Lassen Sie /custom als **Mount Point**.



9. Legen Sie die Download-Quelle fest.

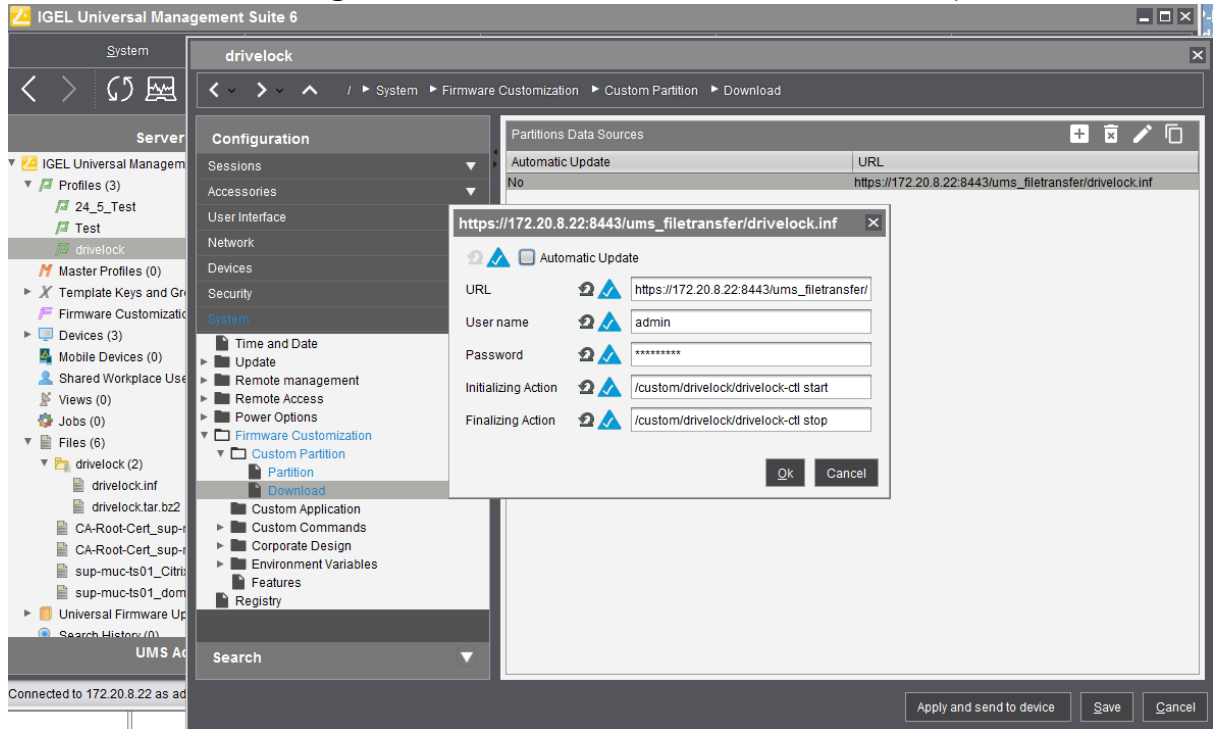
1. Öffnen Sie **System** -> **Firmware Customization** -> **Custom Partition** -> **Download**
2. Fügen Sie eine **Partition Download Source** durch Klicken von [+] hinzu.
3. Geben Sie als Download-URL folgendes ein: **http(s)://<server>:8443/ums_filetransfer/drivelock.inf**
4. Geben Sie dann den **Benutzernamen** und das **Passwort** für den Datei-Download an. Um zu überprüfen, ob der Benutzer Zugriff hat, testen Sie dies im Browser.




10. Im nächsten Schritt geben Sie folgendes an (siehe Abbildung):

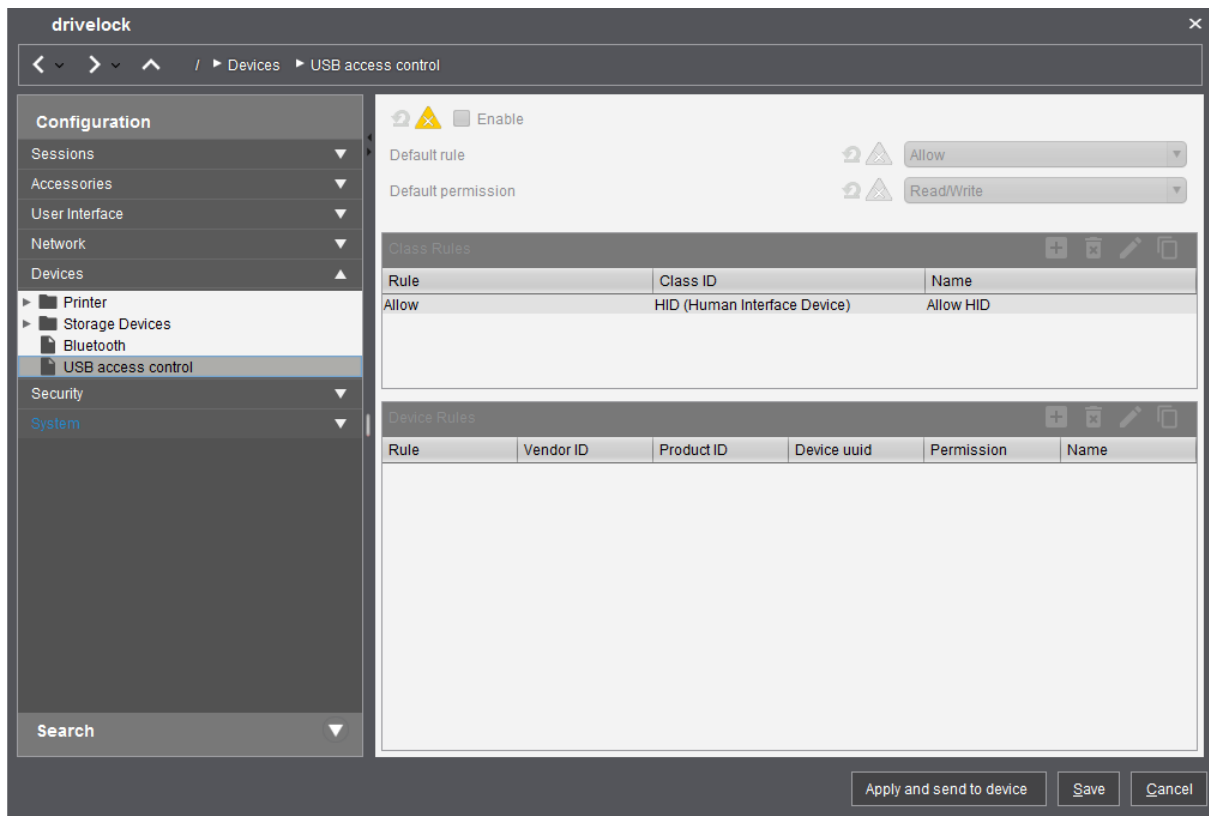
Geben Sie als **Initializing Action** /custom/drivelock/drivelock-ctl start ein.

Geben Sie als **Finalizing Action** /custom/drivelock/drivelock-ctl stop ein.



 Hinweis: Bitte beachten Sie, dass der Mount Point mit dem unter Schritt 8 konfigurierten Mount Point übereinstimmt.

11. Deaktivieren Sie **USB access control** auf Thin Clients.
Öffnen Sie dazu **Devices** -> **USB access control** -> entfernen Sie das Häkchen bei **Enable**.



12. Weisen Sie das Drivelock-Profil abschließend den Thin Clients zu.

1. Öffnen Sie hierzu **Devices->Client**. Fügen Sie mit Drag and drop das Drivelock-Profil-Symbol dem Thin Client hinzu.
2. Laut Anforderung müssen Sie **Now** oder **By next reboot** wählen, damit die Änderungen aktiviert werden.

4 Konfigurationseinstellungen

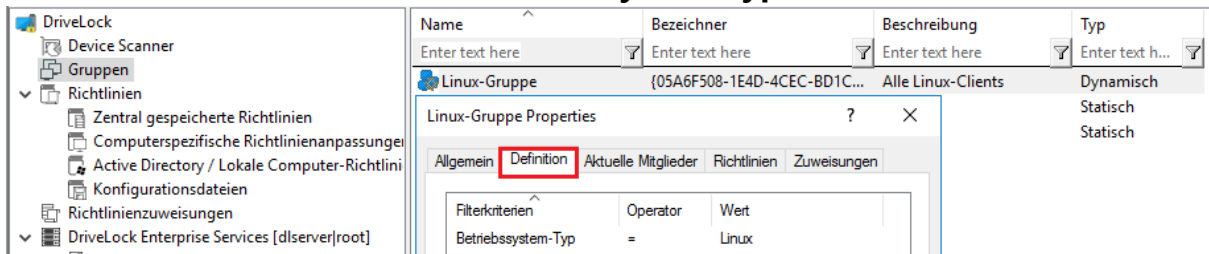
4.1 Empfohlene Vorgehensweise

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

1. Beginnen Sie mit der Erstellung einer DriveLock-Gruppe (statisch oder dynamisch), die Ihre Linux-Agenten umfasst.
Dies erleichtert das spätere Zuweisen der Richtlinie, die Sie für Ihre Linux-Agenten konfigurieren.

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

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



Weitere Informationen zum Thema DriveLock-Gruppen finden Sie im Administrationshandbuch auf [DriveLock Online Help](#).

2. Falls Sie für Ihre DriveLock Linux-Agenten einen anderen Mandanten verwenden wollen, müssen Sie diesen explizit auswählen. Weitere Informationen zur Verwendung von Mandanten finden Sie ebenfalls im Administrationshandbuch.
3. Erstellen Sie eine neue zentral gespeicherte Richtlinie für Ihre Linux-Clients, benennen Sie diese entsprechend (z.B. 'Linux-Richtlinie') und nehmen Sie zunächst [globale Einstellungen](#) vor.
4. Je nachdem, ob Sie die Verwendung von [Geräten](#), [Laufwerken](#) oder [Anwendungen](#) kontrollieren wollen, setzen Sie die entsprechenden Einstellungen.

5. Weisen Sie die 'Linux-Richtlinie' Ihrer DriveLock-Gruppe zu. Eine Zuweisung ist auch auf Alle Computer möglich, wenn Sie keine Gruppe verwenden möchten. In der Abbildung unten ist die Richtlinie 'Linux' einmal auf die DriveLock-Gruppe Linux und einmal auf Alle Computer zugewiesen.

| Reihenfolge | Objekttyp | Objektname | Mandant ... | Richtliniename | Bemerkung | Aktiv |
|-------------|------------------|-------------------------------|-------------|--------------------------------|----------------|-------|
| 1 | Alle Computer | Alle Computer | root | Default company policy | | Ja |
| 2 | Alle Computer | Default MachineConfig Assi... | root | < Computerspezifische Richt... | auto-generated | Ja |
| 3 | Computer | DLCLIENT01 | root | Security Education | | Ja |
| 4 | Computer | DLCLIENT01 | root | BitLocker To Go | | Ja |
| 5 | DriveLock-Gruppe | Linux | root | Linux | | Ja |
| 6 | Alle Computer | Alle Computer | root | Linux | | Ja |

4.2 Richtlinieneinstellungen für DriveLock Linux-Agenten

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

- **Globale Einstellungen:** Einstellungen, Server-Verbindungen, Vertrauenswürdige Zertifikate
- **EDR:** Ereignisse (Allgemeine Ereignisse, Geräte- und Laufwerks-Ereignisse), Ereignisfilter-Definitionen
- **Laufwerke:** Sperr-Einstellungen, Laufwerks-Whitelist-Regeln
- **Geräte:** Sperr-Einstellungen, Geräte-Whitelist-Regeln, Gerätelisten, Gerätelistenregeln
- **Anwendungen:** Einstellung des Scan- und Blockiermodus, Spezielle Regel und Dateieigenschaften-Regel (beide für Linux)



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

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

Zwei Beispiele für Geräte-Einstellungen, die jeweils für alle Benutzer der Linux-Clients gelten:

- Wenn Sie die Verwendung von Eingabegeräten, z.B. Tastaturen, grundsätzlich erlauben und nur bestimmte Tastaturen sperren wollen, geben Sie nur die Eingabegeräte in einer entsprechenden Geräte-Regel an, die gesperrt sein sollen (Blacklist-Modus).
- 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).



Achtung: Eine Übereinstimmung der **Geräte- bzw. Laufwerksklassen** bei Windows und Linux ist nicht immer gegeben. Als Übereinstimmungskriterium verwendet DriveLock derzeit die Hardware-ID des Gerätes oder Laufwerks, das am DriveLock Linux-Agent gesperrt (oder erlaubt) wird.

4.2.1 Globale Einstellungen

1. Im Unterknoten **Einstellungen** können folgende Einstellungen gesetzt werden:
 - **Agentenfernkontroll-Einstellungen und -Berechtigungen:** Auf dem Reiter **Zugriffsrechte** geben Sie die Benutzer an, die explizit Aktionen auf dem Linux-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.
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 Linux-Agenten und dem DES aus. Weitere Informationen zur Zertifikaten finden Sie im entsprechenden Kapitel Im Administrationshandbuch auf drivelock.help.

4.2.2 EDR

EDR (Event Detection & Response) bietet eine optimierte Darstellung der einzelnen Ereignisse verbunden mit verschiedenen Filtermöglichkeiten.

Für DriveLock Linux-Agenten sind die Ereignisse der Kategorien **Allgemeine Ereignisse**, **Applikationskontrolle**, **Geräte-** 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.

Für Linux-Agenten gibt es derzeit folgende **Einstellungen**.

4.2.2.1 Ereignisseinstellungen

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

1. Öffnen Sie im Knoten **EDR** den Unterknoten **Ereignisse**. Doppelklicken Sie unter **Laufwerks-Ereignisse** das entsprechende Ereignis. Für Linux-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.

The screenshot displays the DriveLock configuration window. On the left, a tree view shows the navigation path: **EDR** > **DriveLock-Ereignisse** > **Laufwerks-Ereignisse** > **Dynamisches Sperren von Laufwerken**. The main area shows the configuration for the event 'Laufwerk verbunden, nicht gesperrt' (ID 110). The 'Allgemein' tab is active, showing the following settings:

- Ereignis speichern mit:**
 - Windows Ereignisanzeige
 - DriveLock Enterprise Service
 - E-Mail (SMTP)
 - SNMP
- Unterdrückung von Ereignissen:**
 - Doppelte Ereignisse unterdrücken
 - innerhalb von: 10 Minuten
 - gerechnet vom:
 - erstem Auftreten des Ereignisses
 - letztem Auftreten des Ereignisses

The right side of the window shows a list of event instances, all with a severity of 'Audit erfolgreich'.

4.2.2.2 Ereignisfilter-Definitionen

Auf Linux-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.

4.2.2.2.1 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:

1. Klicken Sie mit der rechten Maustaste auf den Unterknoten **Ereignisfilter-Definitionen** im **EDR**-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**.

The screenshot shows the DriveLock configuration interface. On the left, a tree view shows the 'Ereignisfilter-Definitionen' menu item selected under the 'EDR' node. The main area displays a table of events:

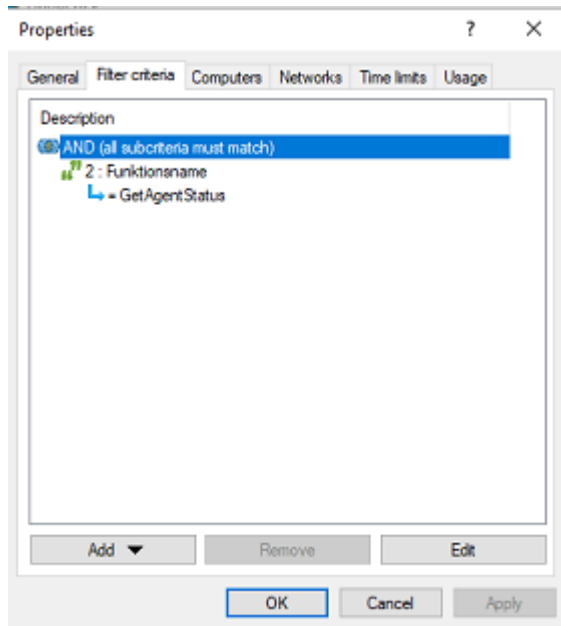
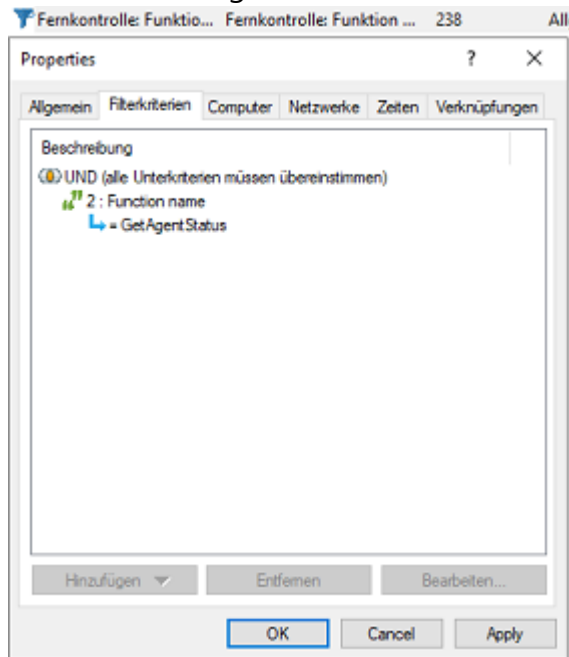
| Beschreibung | Ereignis | Ereignis-ID | Unterkategorie |
|---------------------------|---------------------------------|-------------|----------------------------------|
| DLL geladen (649) | DLL geladen | 649 | Applikationskontrolle |
| Fernkontrolle: Funktio... | Fernkontrolle: Funktion aufg... | 238 | Allgemeine Ereignisse Agent... |

The 'Properties' dialog box for event 238 is open, showing the 'Allgemein' tab. The description is 'Fernkontrolle: Funktion aufgerufen (238)'. The 'Aktiv' checkbox is checked. Under 'Ereignisse speichern mit', the checkboxes for 'Windows Ereignisanzeige' and 'DriveLock Enterprise Service' are checked, while 'E-Mail (SMTP)' and 'SNMP' are unchecked. The 'Kommentar' field is empty.

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.




4.2.3 Laufwerke

4.2.3.1 Laufwerkseinstellungen

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

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

 Hinweis: Beachten Sie, dass für Linux-Richtlinien nur die Einstellungen auf dem Reiter **Allgemein** relevant sind.

1. 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.
2. 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.

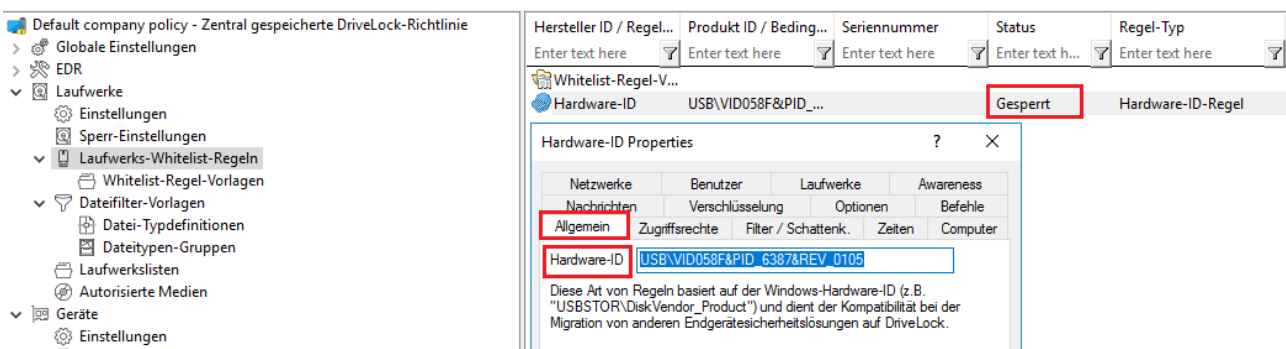
4.2.3.2 Laufwerks-Whitelist-Regeln

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 Linux-Agenten nicht möglich ist.

In der Abbildung unten ist das USB-Laufwerk mit der Hardware ID USB\VID058F&PID_6387&REV_0105 für die Verwendung gesperrt.



4.2.4 Geräte

4.2.4.1 Unterstützte Geräteklassen für Linux-Agenten

Folgende DriveLock-Geräteklassen werden derzeit für Linux unterstützt:

- **Geräte:**

- Debugging- und Software-Schutz-Geräte (WinUSB, ADB) -> entspricht Linux "Diagnostic Device class" (DC)
- Drucker -> entspricht Linux "Printers class" (07)
- Eingabegeräte (HID) -> entspricht Linux "Human Interface Devices class" (03)
- Modems, Netzwerk-Adapter -> entspricht Linux "Communications & CDC control class" (02)
- Scanner und Kameras -> entspricht Linux "Image class" (06)
- Smartcard-Lesegeräte -> entspricht Linux "Smart Card class" (0B)
- Sound-, Video- und Spiele-Controller -> entspricht Linux "Audio/Video/Audio&Video classes" (01|0e|10)

- **Adapter und Schnittstellen:**

- Bluetooth-Adapter -> entspricht Linux "Wireless Controller Class" (e0)
- USB-Controller -> entspricht Linux "Hub class" (09)

4.2.4.2 Geräteeinstellungen

Öffnen Sie im Knoten **Geräte** den Unterknoten **Sperr-Einstellungen**.


Bei den Geräteeinstellungen für Ihre Linux-Richtlinie haben Sie zwei Möglichkeiten:

1. Wählen Sie im Unterknoten **Adapter und Schnittstellen** den Menüpunkt **USB-Controller**. Durch diese Einstellung lässt sich die komplette USB-Schnittstelle des Linux-Agenten sperren oder freigeben.

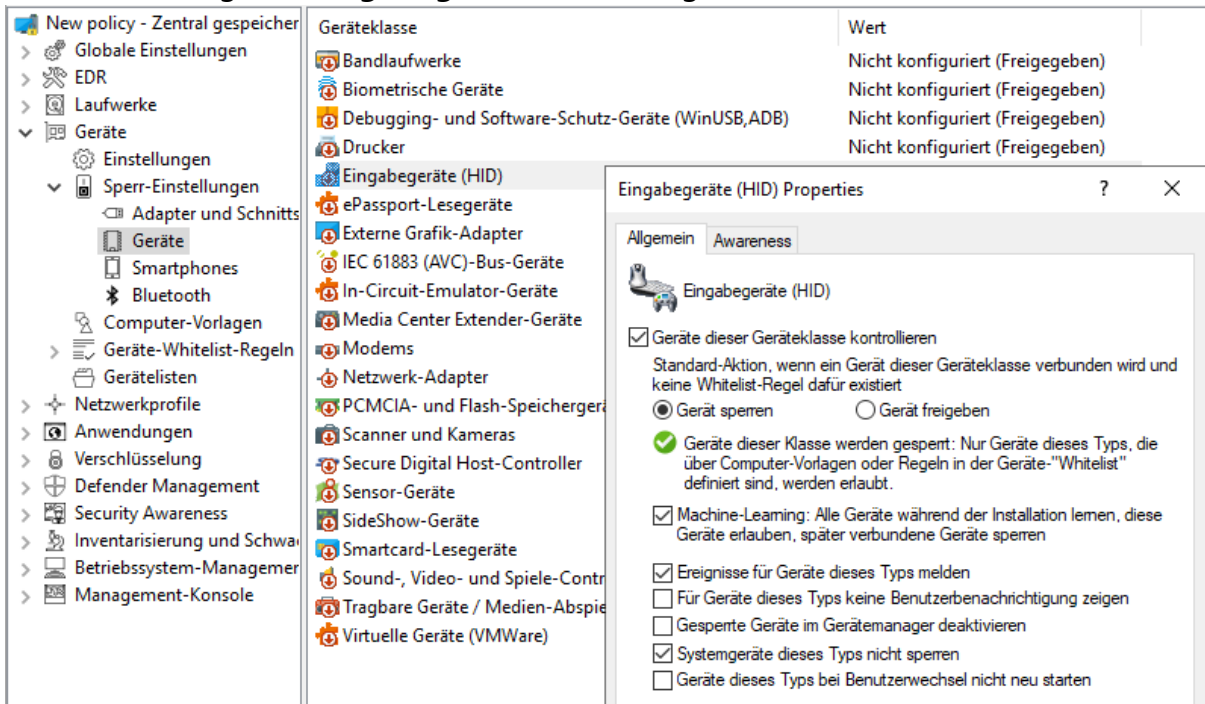
Folgende Optionen sind möglich:

- a. Sie lassen die Einstellung unkonfiguriert.
Die Option **Geräte dieser Geräteklasse kontrollieren** bleibt frei. Dies ist die Standard-Einstellung: **nicht konfiguriert (freigegeben)**.
- b. Sperren Sie die USB-Schnittstelle.
Setzen Sie ein Häkchen bei **Geräte dieser Geräteklasse kontrollieren** und wählen Sie dann **Gerät sperren** aus. In diesem Fall müssen Sie entsprechende Whitelist-Regeln für die Geräte konfigurieren, die Sie erlauben wollen.

- c. Geben Sie die USB-Schnittstelle frei.
Setzen Sie ein Häkchen bei **Geräte dieser Geräteklasse kontrollieren** und wählen Sie dann **Gerät freigeben** aus. In diesem Fall müssen Sie entsprechende Geräte-Regeln (Blacklist) für die gesperrten Geräte konfigurieren.
- d. Wenn Sie die Option **Machine-Learning** auswählen, werden alle Geräte, die bei der Installation mit dem Linux-Agenten verbunden sind, in eine lokale Whitelist eingetragen und sind somit freigegeben. Beachten Sie hierbei, dass die Geräte beim Start der Linux-Agenten auch weiterhin verbunden sein müssen. Alle anderen Geräte, die später verbunden werden, sind gesperrt.
2. Wählen Sie im Unterknoten **Geräte** den Menüpunkt **Eingabegeräte (HID)**.

 Hinweis: Bitte beachten Sie, dass nur einige der [Geräteklassen](#), die für Windows-Richtlinien verfügbar sind, eine Entsprechung auf der Linux-Seite haben.

In der Abbildung sind **Eingabegeräte (HID)** ausgewählt.



| Geräteklasse | Wert |
|--|--|
| Bandlaufwerke | Nicht konfiguriert (Freigegeben) |
| Biometrische Geräte | Nicht konfiguriert (Freigegeben) |
| Debugging- und Software-Schutz-Geräte (WinUSB,ADB) | Nicht konfiguriert (Freigegeben) |
| Drucker | Nicht konfiguriert (Freigegeben) |
| Eingabegeräte (HID) | Geräte dieser Geräteklasse kontrollieren (checked) |
| ePassport-Lesegeräte | Standard-Aktion, wenn ein Gerät dieser Geräteklasse verbunden wird und keine Whitelist-Regel dafür existiert |
| Externe Grafik-Adapter | <input checked="" type="radio"/> Gerät sperren <input type="radio"/> Gerät freigeben |
| IEC 61883 (AVC)-Bus-Geräte | <input checked="" type="checkbox"/> Geräte dieser Klasse werden gesperrt: Nur Geräte dieses Typs, die über Computer-Vorlagen oder Regeln in der Geräte-"Whitelist" definiert sind, werden erlaubt. |
| In-Circuit-Emulator-Geräte | <input checked="" type="checkbox"/> Machine-Learning: Alle Geräte während der Installation lernen, diese Geräte erlauben, später verbundene Geräte sperren |
| Media Center Extender-Geräte | <input checked="" type="checkbox"/> Ereignisse für Geräte dieses Typs melden |
| Modems | <input type="checkbox"/> Für Geräte dieses Typs keine Benutzerbenachrichtigung zeigen |
| Netzwerk-Adapter | <input type="checkbox"/> Gesperrte Geräte im Gerätemanager deaktivieren |
| PCMCIA- und Flash-Speichergeräte | <input checked="" type="checkbox"/> Systemgeräte dieses Typs nicht sperren |
| Scanner und Kameras | <input type="checkbox"/> Geräte dieses Typs bei Benutzerwechsel nicht neu starten |
| Secure Digital Host-Controller | |
| Sensor-Geräte | |
| SideShow-Geräte | |
| Smartcard-Lesegeräte | |
| Sound-, Video- und Spiele-Controller | |
| Tragbare Geräte / Medien-Abspieler | |
| Virtuelle Geräte (VMWare) | |

Bei der Kontrolle der Eingabegeräte erscheint derselbe Dialog wie oben beschrieben:

- a. Setzen Sie ein Häkchen bei **Geräte dieser Geräteklasse kontrollieren** und wählen Sie dann **Gerät sperren** aus.
Alle Eingabegeräte, die an der USB-Schnittstelle angesteckt werden, werden nach Zuweisung der Richtlinie an den DriveLock Linux-Agenten gesperrt. Sie müssen

eine entsprechende Whitelist-Regel konfigurieren, mit der erlaubte Geräte freigegeben werden.

- b. Setzen Sie ein Häkchen bei **Geräte dieser Geräteklasse kontrollieren** und wählen Sie dann **Gerät freigegeben** aus.

Alle Eingabegeräte sind somit erlaubt. In diesem Fall müssen Sie entsprechende Geräte-Regeln (Blacklist) für die gesperrten Geräte konfigurieren.

- c. Die Option **Machine-Learning** kann ebenfalls gewählt werden.
- d. Übernehmen Sie die vorausgewählten Standard-Optionen. Alle anderen Optionen sind für Linux-Agenten nicht relevant.

4.2.4.2.1 Geräte-Whitelist-Regeln (USB-Schnittstelle)

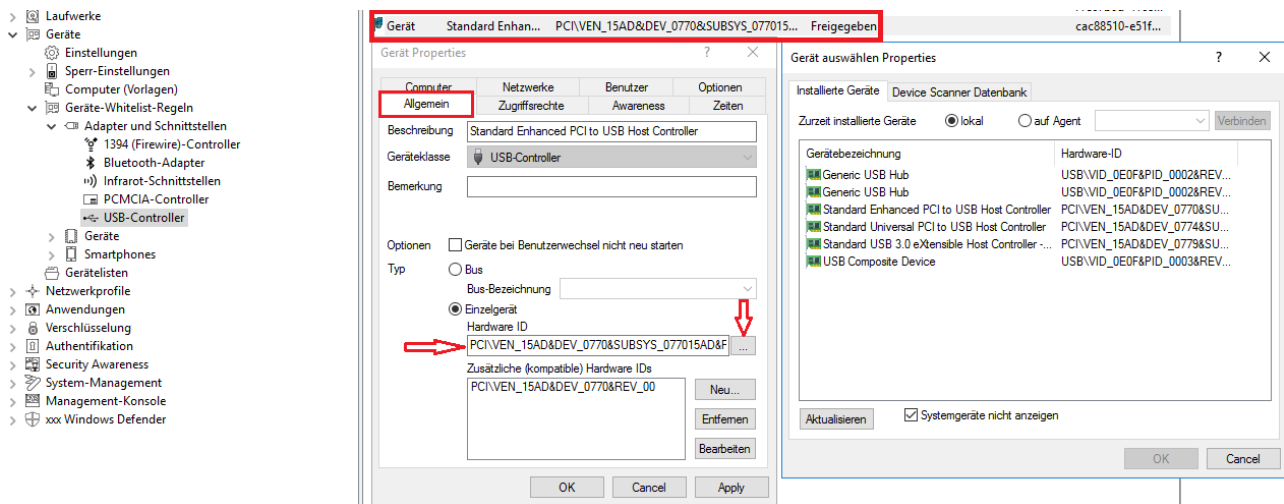
Um eine Geräte-Regel (als White- oder Blacklist) für USB-Schnittstellen zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie im Knoten **Geräte** den Unterknoten **Geräte-Whitelist-Regeln** und dann aus dem Unterknoten **Adapter und Schnittstellen** Option **USB-Controller** aus (siehe Abbildung).
2. Öffnen Sie das Kontextmenü, wählen Sie **Neu** und dann **Geräte oder Bus**. Nur diese Option ist für Linux-Agenten relevant.
3. Auf dem Reiter **Allgemein** wählen Sie die Option **Einzelgerät** aus und suchen dann über die Suchen-Schaltfläche das Gerät, das Sie sperren oder erlauben wollen (je nachdem, ob es sich um eine White- oder Blacklist-Regel handelt).
4. Im Dialog **Geräte auswählen** können Sie sich die **lokal** installierten Geräte anzeigen lassen oder die Geräte, die gerade mit dem Linux-Agenten verbunden sind (**auf Agent**). Beachten Sie, dass im zweiten Fall der DriveLock Linux-Agent online sein muss.
5. Auf dem Reiter **Zugriffsrechte** geben Sie dann die entsprechenden **Sperr-Einstellungen** an.



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

In der Abbildung unten ist der USB-Controller mit der ID **PCI\VEN_15AD&DEV_0770&SUBSYS_077015AD&REV_00** erlaubt und hat den Status **Freigegeben**.

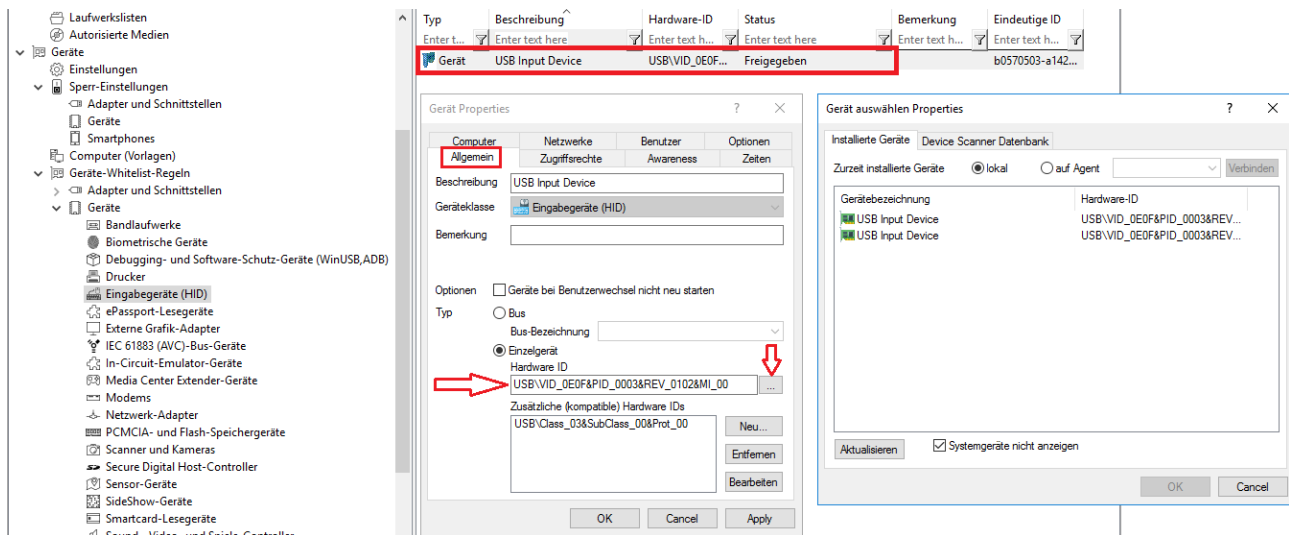


4.2.4.2.2 Geräte-Whitelist-Regeln (Geräte)

Um eine Whitelist-Regel für Geräte zu konfigurieren, gehen Sie wie unter [Geräte-Whitelist-Regeln \(Schnittstellen\)](#) beschrieben vor, mit dem Unterschied, dass Sie im Unterknoten **Geräte-Whitelist-Regeln** die Option **Eingabegeräte (HID)** auswählen.

Alle anderen Schritte sind gleich.

In der Abbildung unten hat das USB-Eingabegerät mit der Hardware ID **USB\VID_0E0F&PID_0003&REV_0102&MI_00** den Status **Freigegeben**.




4.2.4.2.3 Android- und Apple-Geräte

Es ist auch möglich, Regeln für Android- und Apple-Geräte anzulegen, wie in der Abbildung gezeigt. Wie bei anderen Gerätekategorien benötigen Sie hierfür die Hardware-ID bzw. Seriennummer des Geräts. Auf dem Reiter **Zugriffsrechte** können Sie entsprechende Sperr-Einstellungen setzen.

The screenshot shows the DriveLock configuration interface. On the left is a tree view of settings, with 'Geräte' expanded to show 'Smartphones' and 'Android-Geräte'. On the right, a table lists devices with columns for 'Typ', 'Beschreibung', 'Hardware-ID', and 'Status'. Below the table, a 'Neue Regel Properties' dialog box is open, showing fields for 'Beschreibung' (Android Device: OnePlus A5000), 'Geräteklasse' (Android-Geräte), 'Hersteller-ID', 'Produkt-ID', and 'Hardware ID' (USB\VID_2A70&PID_F003). There is also a checkbox for 'Nur definierte Seriennummern zulassen' and a table for 'Seriennummer' and 'Bemerkung'.

Der Agent erkennt ein Gerät als Android- oder Apple-Gerät, wenn es in der Liste der Geräte eingetragen ist, die mit dem Drivelock-Agenten installiert wird. Diese Liste enthält die Produkt- und Hersteller-IDs (bzw. Seriennummern) und wird beim Verbinden des jeweiligen Geräts verglichen.

Diese Liste liegt im System im Verzeichnis `/etc/udev/rules.d/` in den Dateien **51-drivelock-apple.rules** und **51-drivelock-android.rules**.

 Hinweis: Die Liste kann erweitert werden. Falls Sie hierbei Unterstützung benötigen, kontaktieren Sie bitte unseren Support.

4.2.4.2.4 Gerätelisten

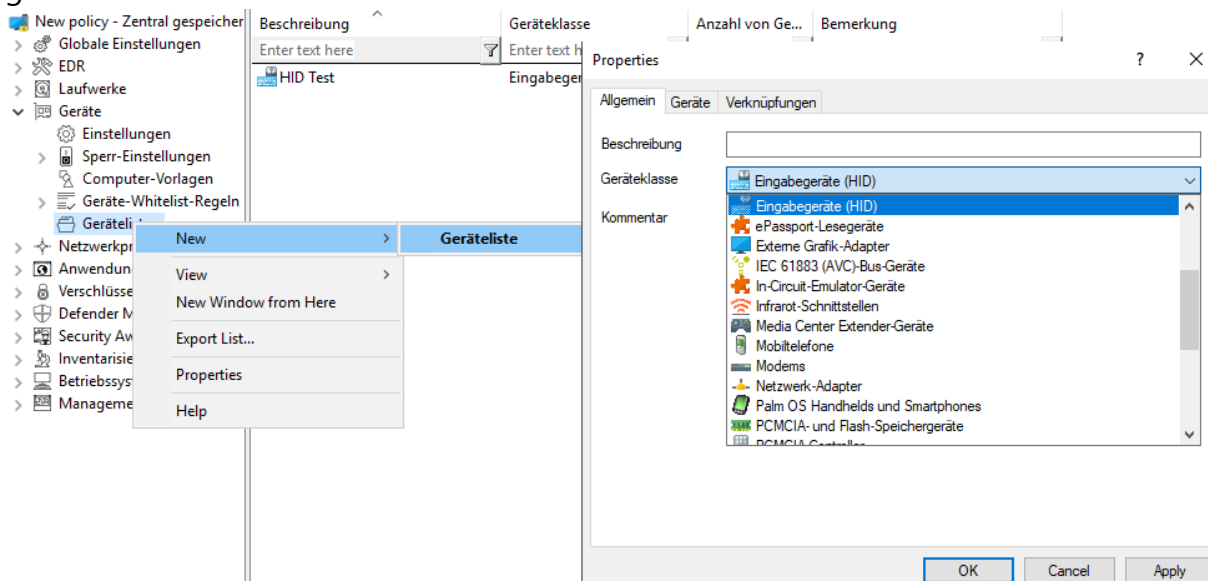
Auf Linux-Agenten können Gerätelisten verwendet werden. Sie vereinfachen die Verwaltung von Geräten des gleichen Typs, wenn dafür gleiche Einstellungen gelten sollen und reduzieren dabei die Anzahl der benötigten Whitelistregeln. Gerätelisten können mehrere gleichartige Geräte enthalten und für die Konfiguration von Whitelistregeln verwendet werden - analog zur Verwendung von einzelnen Geräten anhand deren Hardware ID.

Beachten Sie, dass die gewählten Geräteklassen auf Linux-Agenten unterstützt werden. Durch Angabe der entsprechenden Hardware-ID könnte die Klasse beim Vergleich ignoriert werden.

4.2.4.2.4.1 Gerätelisten anlegen

So erstellen Sie eine Geräteliste:

1. Gehen Sie im Knoten **Geräte** zum Unterknoten **Gerätelisten** und klicken Sie dann **Neu** aus dem Kontextmenü.
2. Im Eigenschaftendialog der Geräteliste wählen Sie auf dem Reiter **Allgemein** die gewünschte Geräteklasse aus.



3. Auf dem Reiter **Geräte** können Sie dann über die Schaltfläche **Hinzufügen** die Geräte auswählen.
4. Wählen Sie im nachfolgenden Dialog die entsprechende **Hardware-ID** des Gerätes aus. Sie können sich dabei auch auf den Linux-Agenten verbinden und dort Geräte direkt auswählen.
5. Sobald Sie eine Geräteliste angelegt haben, können Sie diese in [Gerätelisten-Regeln](#) verwenden.

4.2.5 Anwendungen

DriveLock bietet für Linux-Agenten einige Application Control-Optionen an.

1. Mit der Einstellung [Scan- und Blockiermodus](#) wird die Application Control-Funktionalität aktiviert.
2. Zwei Anwendungsregeln können für Linux eingesetzt werden: [Datei-Eigenschaften-Regel](#) und [Spezielle Regel](#).

Um Application Control für Linux verwenden zu können, müssen bestimmte [Voraussetzungen](#) hinsichtlich des Linux-Kernels erfüllt sein.


Weitere allgemeine Informationen zu Application Control finden Sie in der gleichnamigen Dokumentation auf [DriveLock Online Help](#).


4.2.5.1 Voraussetzungen für Application Control auf Linux-Agenten

Um die volle Funktionalität von Application Control mit Whitelisting unterstützen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Die fanotify-API muss im Linux-Kernel aktiv sein
- Der Linux-Kernel muss größer als 5.0 sein.
Ist dies nicht der Fall, ist nur der fanotify-Flag FAN_OPEN_PERM vorhanden und somit lediglich Blacklisting möglich.
- Das Dateisystem muss fanotify-Ereignisse unterstützen.
Aktuelle Liste der unterstützten Dateisysteme:
 - bfs
 - btrfs
 - cifs
 - ecryptfs
 - ext2
 - ext3
 - ext4
 - fuseblk
 - fuse.vmhgfs-fuse
 - iso9660
 - jfs

- minix
- msdos
- nfs
- nfs4
- nssvol
- ncpfs
- overlay
- overlayfs
- ramfs
- reiserfs
- smbfs
- squashfs
- tmpfs
- udf
- vfat
- xfs
- zfs

 Hinweis: Das Ausführen von Application Control auf Linux neben anderen fanotify-basierten Sicherheitslösungen wird nicht unterstützt. Dies kann zu unvorhersehbaren Ergebnissen führen, einschließlich des Aufhängens des Betriebssystems.

 Hinweis: Aufgrund der Einschränkungen von fanotify ist es nicht möglich, Application Control innerhalb von Containern zu verwenden.

4.2.5.2 Scan- und Blockiermodus

Diese Einstellung wird verwendet, um den Modus auszuwählen, mit dem DriveLock die Anwendungen auf dem Linux-Agenten überprüft bzw. entsprechende Aktionen einleitet.

Gehen Sie folgendermaßen vor:

Wählen Sie **Einstellen auf festen Wert** und suchen Sie dann aus der Liste eine der folgenden Optionen aus:

- **Nur Ereignisse:** es werden nur Ereignisse generiert, die Sie dann auswerten können
- **Whitelist:** es dürfen nur die Anwendungen ausgeführt werden, für die es eine entsprechende Whitelist-Regel gibt. Alle anderen Anwendungen werden geblockt.
- **Blacklist:** es werden nur die Anwendungen geblockt, für die es eine entsprechende Blacklist-Regel gibt. Alle anderen Anwendungen sind erlaubt.
- **inklusive DLLs:** dieser Zusatz prüft auch die gemeinsamen Bibliotheken
- **(simulieren):** dieser Zusatz bedeutet, dass die Auswirkungen Ihrer Regeln vorab getestet und entsprechende Ereignisse erzeugt werden.

4.2.5.3 Datei-Eigenschaften-Regel (für Linux)

Mit dieser Regel können Sie verschiedene Dateieigenschaften angeben, nach denen gefiltert werden soll. Diese Regel kann als Whitelist- oder Blacklist-Regel angelegt werden.

Gehen Sie folgendermaßen vor:

Öffnen Sie im Knoten **Anwendungen** unter **Anwendungsregeln** den Kontextmenüeintrag **Datei-Eigenschaften-Regel (für Linux)...**

1. Auf dem Reiter **Allgemein** legen Sie als erstes den Regel-Typ fest. Dann haben Sie folgenden Auswahlmöglichkeiten:
 - **Pfad:** Geben Sie einen Pfad im Linux-Format (z.B. /home/test/) an, wenn Sie Anwendungen aus einem speziellen Pfad erlauben (oder blockieren) wollen. Platzhalter sind erlaubt.
 - **Hash:** Diese Option überprüft, ob der Hashwert des Dateiinhalts mit dem angegebenen Wert übereinstimmt. Dieser wird bei der Regelerstellung gespeichert und zur Laufzeit mit dem aktuell berechneten verglichen. Stimmen beide überein, wird die Regel aktiviert. Diese Option eignet sich z.B. für eine einzelne Applikation, die per Whitelist oder Blacklist erlaubt oder gesperrt werden soll.
 - **Eigentümer:** Mit dieser Option wird der Start von Anwendungen vom Dateieigentümer abhängig gemacht, z.B. können Sie mit dieser Einstellung alle Programme, die von einem Administrator oder einem vertrauenswürdigen Installationskonto installiert wurden, erlauben. Alle Programme, die von anderen Benutzern installiert wurden, sind hingegen gesperrt. So können auch automatisch alle Programme gesperrt werden, die ohne vorherige Installation ausgeführt werden können.

Eine Kombination der Optionen ist möglich.

2. Auf dem Reiter **Zeiten** können Sie die Zeiten angeben, wann die Regel aktiv sein soll.
3. Auf dem Reiter **Computer** können Sie angeben, auf welchen Computern die Regel aktiv sein soll.

4.2.5.4 Spezielle Regel (für Linux)

Die spezielle Regel kann nur als Whitelist-Regel verwendet werden.

Gehen Sie folgendermaßen vor:

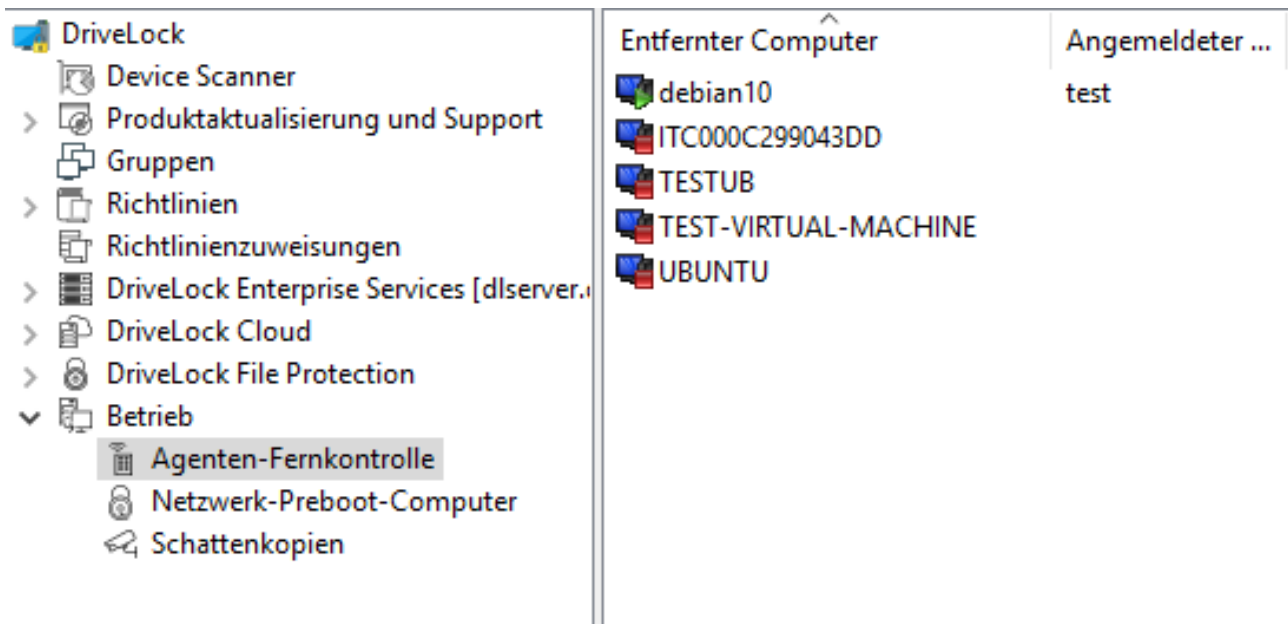
1. Öffnen Sie im Knoten **Anwendungen** unter **Anwendungsregeln** den Kontextmenüeintrag **Spezielle Regel (für Linux)**.
2. Auf dem Reiter **Allgemein** haben Sie drei Optionen zur Wahl:
 - **Anwendungen, die Teil des Betriebssystems sind:**
Mit dieser Option werden Betriebssystemprogramme aus folgenden Systemverzeichnisse automatisch zugelassen:
 - /bin, /sbin, /lib, /lib64, /usr, /etc
 - Ubuntu: /snap
 - Suse: /.snapshots
 - **Anwendungen, die Teil von DriveLock sind:**
Hier werden Binärdateien im Drivelock-Installationsordner und dem "bin"-Ordner darunter erlaubt.
Das eigene Installationsprogramm drivelockd-install.sh ist nicht enthalten, der Benutzer muss selbst eine Regel hinzufügen, um das Skript im Falle von Upgrades laufen zu lassen.
 - **Jede gestartete Anwendung:**
Hier werden alle gestarteten Anwendungen erlaubt, unabhängig vom Verzeichnis.
3. Auf dem Reiter **Zeiten** können Sie die Zeiten angeben, wann die Regel aktiv sein soll.
4. Auf dem Reiter **Computer** können Sie angeben, auf welchen Computern die Regel aktiv sein soll.

4.3 Agenten-Fernkontrolle

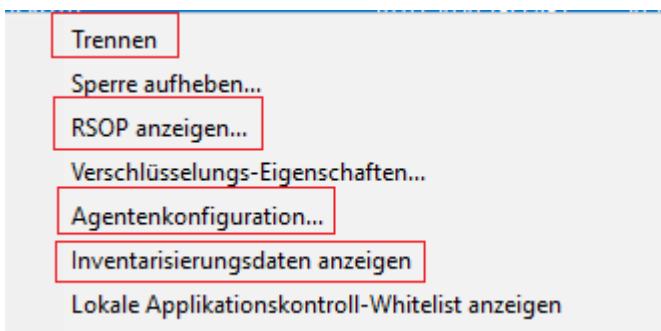
Öffnen Sie in der DriveLock Management Konsole im Knoten **Betrieb** den Unterknoten **Agenten-Fernkontrolle**. Sie sehen eine Liste der Client-Computer, auf denen der DriveLock Agent installiert ist (siehe Abbildung).

 Hinweis: Weitere Informationen zum Thema Agenten-Fernkontrolle finden Sie im Administrationshandbuch auf [drive.lock.help](https://drive.lock/help).

Klicken Sie im Kontextmenü des ausgewählten Linux-Clients auf **Verbinden**.



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



1. **Trennen** der Verbindung
2. **RSOP anzeigen...**

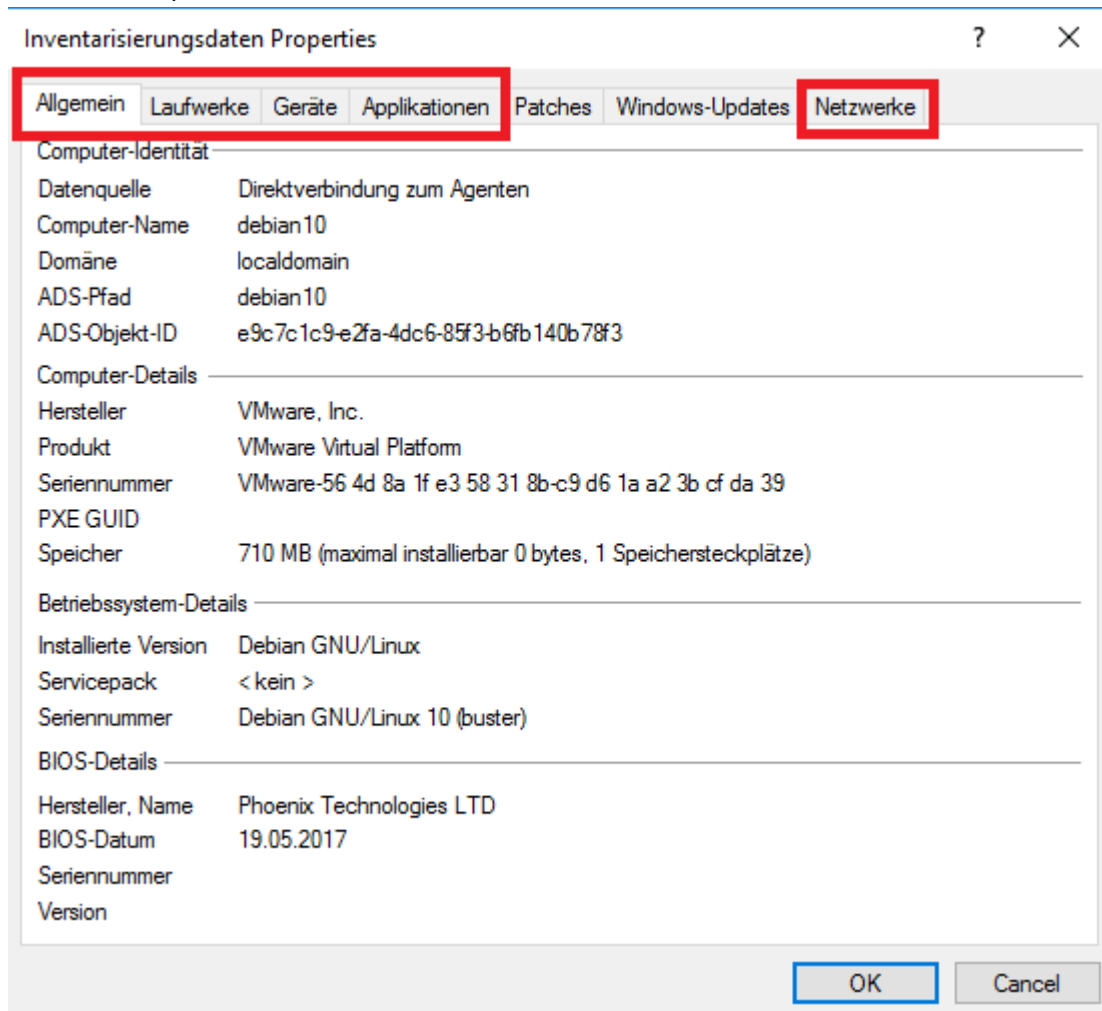
Klicken Sie diese Option, um sich eine Zusammenfassung der Richtlinie zeigen zu lassen, die auf den Linux-Agenten zugewiesen ist. Änderungen lassen sich hier nicht durchführen.

3. Agentenkonfiguration...

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

4. Inventarisierungsdaten anzeigen

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



5 Linux-Agenten im DCC

DriveLock Linux-Agenten werden wie andere DriveLock Agenten im DriveLock Control Center (DCC) angezeigt.



Hinweis: Eine detaillierte Beschreibung des DCC finden Sie im DriveLock Control Center Handbuch auf drivelock.help.

Folgende Ansichten und Funktionen sind für Linux-Agenten wichtig:

- **HelpDesk:**

In der HelpDesk-Ansicht werden Ihre Linux-Agenten mit Status und weiteren Informationen angezeigt. Eine Beschreibung der [Aktionen](#) finden sie hier.

- **Statistikreport:**

Agent alive: Hier werden Ihnen die Linux-Agenten angezeigt, die sich zuletzt am DES zurückgemeldet haben.

- **Ereignisreport:**

Hier werden alle Ereignisse aufgelistet, die vom Linux-Agenten an den DES geschickt werden. Eine Liste der Ereignisse finden Sie unter [Ereignisse](#).

- **Inventar:**

Computer: Hier sehen Sie eine Übersicht Ihrer Linux-Agenten mit Informationen zum jeweiligen Linux-Computer, Betriebssystem und DriveLock Linux-Agent.

- **DOC öffnen:**

Öffnen Sie das [DriveLock Operations Center \(DOC\)](#), um sich dort den Status der DriveLock Linux-Agenten anzeigen zu lassen.

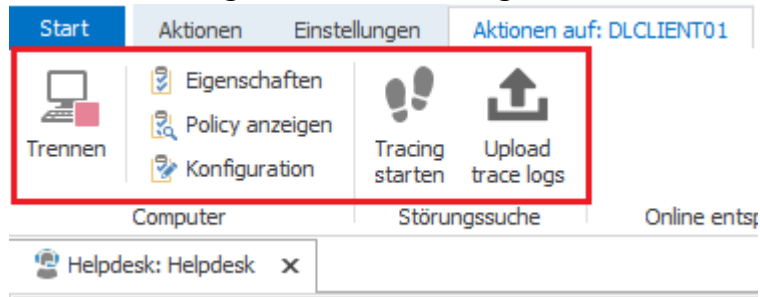
5.1 DCC: HelpDesk-Aktionen

Auf dem Reiter **Aktionen** ist die Schaltfläche **Verbinden** für DriveLock Linux-Agenten relevant.

Mit dieser Aktion starten Sie die Agenten-Fernkontrolle. Diese kann auch aus der [DriveLock Management Konsole](#) gestartet werden.

1. Verbindung herstellen: Markieren Sie einen Linux-Agenten in der Liste und klicken Sie **Verbinden** oder geben Sie den Namen des Linux-Clients in das Textfeld unter der Schaltfläche ein.
2. Sobald die Verbindung hergestellt ist, wird ein neuer Reiter **Aktionen auf: [Name des Linux-Clients]** geöffnet.

Hier können folgende Aktionen ausgewählt werden (siehe Abbildung):



3. Klicken Sie **Eigenschaften**, um detaillierte Informationen zum Status des Linux-Agenten zu erhalten.
Der Reiter **Allgemein** zeigt eine Übersicht an. Durch Klicken der Schaltfläche **Richtlinie aktualisieren** wird die Aktualisierung auf dem Agenten gestartet.
4. Klicken Sie **Policy anzeigen**, um sich den Richtlinienergebnissatz (RSOP) des Linux-Clients anzeigen zu lassen.
5. Wenn Sie **Konfiguration** klicken, öffnet sich ein Dialog mit Informationen zur Konfiguration des Linux-Agenten. Hier können Sie z.B. einen weiteren Server hinzufügen oder einen anderen Mandanten auswählen.
6. Falls Sie **Tracing** bzw. Fehlersuche für Ihre Linux-Agenten aktivieren wollen, kontaktieren Sie bitte den technischen Support von DriveLock.


6 Linux-Agenten im DOC

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



Hinweis: Eine Einführung in das DOC finden Sie im DriveLock Control Center Handbuch auf drivelock.help.

Folgende DOC-Ansichten sind für Linux-Agenten relevant:

- **Computer:** Filtern Sie z.B. nach **OS Typ** (mit  gekennzeichnet) , um Ihre Linux-Agenten anhand ihres Betriebssystems gruppieren zu lassen. Markieren Sie einen beliebigen Linux-Agenten, um sich Details anzusehen.
- **Gruppen:** Wenn Sie eine DriveLock Gruppe für Ihre Linux-Agenten definiert haben, wird diese mit Informationen zu den jeweiligen Mitgliedern und den zugewiesenen Richtlinien hier angezeigt.
- **Ereignisse:** Die Ereignisse, die ein Linux-Agent an den DES schickt, werden in dieser Ansicht aufgelistet.
- **EDR:** Die Endpoint Detection & Response Ansicht ermöglicht eine kontinuierliche Überwachung und konfigurierbare Reaktion auf sicherheitsrelevante Ereignisse.
- **Konten:** 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.

7 Ereignisliste

Folgende Tabelle enthält alle Linux-relevanten Ereignisse, die im DriveLock Control Center oder 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 [DriveLock Online Help](#).

Der DriveLock Linux-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 Benutzerkennung [gesperrt/entsperrt] sein. Geräteidentifikation: [ID] [ID] (Rev. [rev]) (Seriennummer [Nummer]) Angewendete Whitelist-Regel: [Regel] Bildschirm-Status (Tasten [Win]-[L]): [Status] |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|-------|---------------------------------|---|
| 111 | Audit | Laufwerk verbunden und gesperrt | <p>Das Laufwerk [Name] ([Kategorie]) wurde dem System hinzugefügt. Es konnte aufgrund eines Systemfehlers nicht gesperrt werden. Es handelt sich um ein [Typ]-Bus-Gerät. Das Laufwerk sollte für diese Benutzererkennung [gesperrt/entsperrt] sein.</p> <p>Geräteidentifikation: [ID] [ID] (Rev. [rev]) (Seriennummer [Nummer]) Angewendete Whitelist-Regel: [Regel] Bildschirm-Status (Tasten [Win]-[L]): [Status]</p> |
| 129 | Audit | Gerät verbunden und gesperrt | <p>Das Gerät [Name] wurde an den Computer angeschlossen. Es wurde gesperrt. Gerätetyp: [Typ] Hardware-ID: [ID] Klassen-ID: [ID] Angewendete Whitelist-Regel: [Name] Bildschirm-Status (Tasten [Win]-[L]): [Status]</p> |
| 130 | Audit | Gerät verbunden und freigegeben | <p>Das Gerät [Name] wurde an den Computer angeschlossen. Gerätetyp: [Typ] Hardware-ID: [ID] Klassen-ID: [ID] Angewendete Whi-</p> |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|---------|--|---|
| | | | telist-Regel: [Name] Bildschirm-Status (Tasten [Win]-[L]): [Status] |
| 152 | Warnung | Richtliniendateispeicher-Entpackfehler | Der Richtliniendateispeicher [Name] kann nicht entpackt werden. Einige Funktionen, welche diese Dateien benötigen, werden fehlschlagen. |
| 153 | Warnung | Konfigurationsdatei angewendet | Die Konfigurationsdatei [Name] wurde erfolgreich angewendet. |
| 154 | Fehler | Konfigurations-Datei Download-Fehler | Die Konfigurationsdatei [Name] kann nicht heruntergeladen werden. Fehler-Code: [Code] Fehler: [Fehler] |
| 158 | Fehler | Konfigurations-Datei Fehler | Die Konfigurationsdatei [Name] kann nicht gelesen werden. Fehler-Code: [Code] Fehler: [Fehler] |
| 191 | Warnung | {PrefixEnterpriseService} ausgewählt | Der {PrefixEnterpriseService} [Name] wurde von {Product} ausgewählt. Verbindungs-ID: [ID] Benutzt für: [Inventory/Recovery/Events] |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|--------------|---|---|
| 192 | Warnung | {PrefixEnterpriseService} nicht verfügbar | Es ist kein {PrefixEnterpriseService} verfügbar, weil keine gültige Verbindung konfiguriert ist. |
| 235 | Fehler | SSL: Kann nicht initialisiert werden | Das Modul für verschlüsselte Kommunikation (SSL) konnte nicht initialisiert werden. Fehler: [Fehler] |
| 236 | Fehler | Fernkontrolle: Kann Server nicht initialisieren | Die Serverkomponente für Agentenfernkontrolle konnte nicht initialisiert werden. Agentenfernkontrolle ist nicht verfügbar. Fehler: [Fehler] |
| 237 | Fehler | Fernkontrolle: Interner Fehler | Agentenfernkontrolle: Ein interner SOAP-Kommunikationsfehler ist aufgetreten. Fehler: [Fehler] |
| 238 | SuccessAudit | Fernkontrolle: Funktion aufgerufen | Eine Funktion der Agentenfernkontrolle wurde aufgerufen. Aufrufende IP-Adresse: [IP-Adresse] Aufgerufene Funktion: [Funktion] |
| 243 | Fehler | Kann Kon- | Eine Kon- |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|---------|--|--|
| | | figurationsdatenbank nicht öffnen | figurationsdatenbank konnte nicht geöffnet werden. Datenbank-Datei: [Name] Fehler-Code: [Code] Fehler: [Fehler] |
| 246 | Fehler | Kann Konfigurationsstatus nicht speichern | Der {Product}-Agent kann den Konfigurationsstatus nicht speichern, der von anderen {Product}-Komponenten benutzt wird. Fehler-Code: [Code] Fehler: [Fehler] |
| 247 | Fehler | Kann Konfigurations-Speicher nicht initialisieren | Der {Product}-Agent kann den Konfigurationsdatenbank-Speicher nicht initialisieren. |
| 249 | Fehler | Konfigurationsdatei: Alles-Sperren-Konfiguration wird angewendet | Eine Konfiguration mit Konfigurations-Dateien wurde erkannt aber es konnten keine Einstellungen aus einer Konfigurationsdatenbank gelesen werden. {Product} wird eine Konfiguration verwenden, in der alle Wechseldatenträger gesperrt sind. |
| 250 | Warnung | Konfigurationsdatei: | Die Konfigurationsdatei |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|-------------|--|--|
| | | Benutze zwischengespeicherte Kopie | [Name] konnte nicht von ihrem ursprünglichen Ort geladen werden. Eine lokal zwischengespeicherte Kopie wird benutzt. |
| 251 | Fehler | Konfigurationsdatei: Kann nicht extrahiert werden. | Eine {Product}-Konfigurationsdatei konnte nicht extrahiert werden. Einstellungen aus dieser Datei werden nicht angewendet. Datenbankdatei: [Name] Fehler-Code: [Code] Fehler: [Fehler] |
| 264 | Fehler | Kann Konfigurationsdatenbank nicht mit RSoP zusammenführen | Die Konfigurationsdatenbank [Name] kann nicht mit dem Richtlinienenergebnissatz zusammengeführt werden. |
| 287 | Fehler | Kein Server für Inventarisierung definiert | Es ist kein Server für den Upload von Hard- und Softwareinventarisierungsdaten definiert. |
| 288 | Information | Inventarisierung erfolgreich | Hard- und Softwareinventarisierungsdaten wurden erfolgreich gesammelt und hochgeladen. DES-Server: [Servername] Ver- |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|-------------|--|--|
| | | | bindungs-ID: [ID] |
| 289 | Information | Inventarisierung fehlgeschlagen | Beim Sammeln von Hard- und Softwareinventarisierungsdaten ist ein Fehler aufgetreten. DES-Server: [Servername] Verbindungs-ID: [ID] Fehler: [Fehler] |
| 294 | Fehler | Kann zentral gespeicherte Richtlinie nicht laden | Die zentral gespeicherte Richtlinie [Name] kann nicht heruntergeladen werden. Server: [Name] Fehler: [Fehler] |
| 295 | Fehler | Zentral gespeicherte Konfiguration: Kann nicht extrahiert werden. | Eine zentral gespeicherte Richtlinie konnte nicht extrahiert werden. Einstellungen aus dieser Datei werden nicht angewendet. Konfigurations-ID: [ID] Fehler: [Fehler] |
| 297 | Fehler | Zentral gespeicherte Richtlinie: Alles-Sperren-Konfiguration wird angewendet | Eine Konfiguration mit zentral gespeicherter Richtlinie wurde erkannt aber es konnten keine Einstellungen vom Server geladen werden. {Product} wird eine Konfiguration verwenden, in der |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|-------------|---|--|
| | | | alle Wechseldatenträger gesperrt sind. |
| 299 | Information | Zentral gespeicherte Richtlinie heruntergeladen | Die zentral gespeicherte Richtlinie [Name] wurde erfolgreich heruntergeladen. Konfigurations-ID: [ID] Version: [Version] |
| 443 | Fehler | Start einer Komponente fehlgeschlagen | Eine {Product}-Systemkomponente konnte auf diesem Computer nicht gestartet werden. Fehlercode: [Code] Fehler-Code: [Code] Fehler: [Fehler]] Komponenten-ID: [ID] |
| 473 | Audit | Prozess gesperrt | Die Ausführung eines Prozesses wurde verhindert. Prozess: [ProcessName] Datei Hash: [ProcessHash] Angewendete Regel: [ObjectID] Regel-Typ: [WIType] Dateibesitzer (Benutzername): [UserName] Dateibesitzer (Benutzer SID): [SID] Dateiversion: [FileVersion] Zertifikatsherausgeber: [CertIssuer] Zertifikat herausgegeben für: [CertSubject] Zer- |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|-------|-------------------|--|
| | | | tifikatsseriennummer: [CertSerNo] Zertifikatsfingerabdruck: [CertThumbprint] Beschreibung: [VerDescription] Produkt: [VerProduct] Befehlszeile: [CmdLine] Aufrufender Prozess: [ProcessName] ([ProcessGuid]) |
| 474 | Audit | Prozess gestartet | Ein Prozess wurde gestartet. Prozess: [ProcessName] Datei Hash: [ProcessHash] Angewendete Regel: [ObjectID] Regel-Typ: [WIType] Dateibesitzer (Benutzername): [UserName] Dateibesitzer (Benutzer SID): [SID] Dateiversion: [FileVersion] Zertifikatsherausgeber: [CertIssuer] Zertifikat herausgegeben für: [CertSubject] Zertifikatsseriennummer: [CertSerNo] Zertifikatsfingerabdruck: [CertThumbprint] Beschreibung: [VerDescription] Produkt: [VerProduct] Eindeutige Process ID: [ProcessGuid] Befehlszeile: [CmdLine] Aufrufender Pro- |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|---------|--|---|
| | | | zess: [ProcessName] ([ProcessGuid]) |
| 520 | Fehler | Alle {PrefixES} nicht erreichbar | Die Unternehmensrichtlinie kann nicht geladen werden. Alle konfigurierten {PrefixEnterpriseService}s sind nicht erreichbar. |
| 521 | Fehler | Kann Computer-Token nicht ermitteln | Der Computer-Token kann nicht ermittelt werden. Fehler-Code: [Code] Fehler: [Fehler] |
| 522 | Fehler | Fehler beim Laden von Richtlinienzuweisungen | Beim Laden der Richtlinienzuweisungen von Server [Name] ist ein Fehler aufgetreten. Fehler: [Fehler] |
| 523 | Fehler | Richtlinienintegritätsprüfung fehlgeschlagen | Die Integrität einer zugewiesenen Richtlinie konnte nicht überprüft werden. Richtlinien-ID: [ID] Richtlinienname: [Name] Aktueller Hashwert: [Wert] Erwarteter Hashwert: [Wert] |
| 533 | Warnung | Keine Richtlinie - wurde gelöscht | Die Unternehmensrichtlinie wurde gelöscht, da der Computer für eine zu lange Zeit offline war. |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|-------------|----------------------------|--|
| 584 | Information | Inventarisierung gestartet | Inventarisierung wurde durch den DES gestartet. |
| 639 | Fehler | Server Zertifikat Fehler | Server Zertifikatsfehler aufgetreten. Zertifikat: [Name]. Fehlermeldung: [Text] |
| 648 | Audit | DLL gesperrt | Das Laden einer DLL wurde verhindert. Prozess: [ProcessName] ([ProcessGuid]) Angewendete Regel: [ObjectID] Regel-Typ: [WType] [WType]LL Dateiname: [ProcessName] DLL Datei Hash: [ProcessHash] Dateibesitzer (Benutzername): [UserName] Dateibesitzer (Benutzer SID): [SID] Datei-version: [FileVersion] Zertifikatsherausgeber: [CertIssuer] Zertifikat herausgegeben für: [CertSubject] Zertifikatsseriennummer: [CertSerNo] Zertifikatsfingerabdruck: [CertThumbprint] Beschreibung: [VerDescription] Produkt: [VerProduct] |
| 649 | Audit | DLL geladen | Eine DLL wurde geladen. |

| Ereignis ID | Ebene | Text | Beschreibung |
|-------------|-------|------|---|
| | | | <p>Prozess: [ProcessName] ([ProcessGuid]) Ange- wendete Regel: [ObjectID] Regel-Typ: [WIType][WITy- pe]LL Dateiname: [Pro- cessName] DLL Datei Hash: [ProcessHash] Dateibesitzer (Benutzername): [UserName] Dateibesitzer (Benutzer SID): [SID] Datei- version: [FileVersion] Zer- tifikatsherausgeber: [CertIssuer] Zertifikat her- ausgegeben für: [Cer- tSubject] Zertifikatsseriennummer: [CertSerNo] Zer- tifikatsfingerabdruck: [Cer- tThumbprint] Beschreibung: [VerDescription] Produkt: [VerProduct]</p> |

8 Kommandozeilenprogramm

Mit diesem Kommandozeilentool können Sie die lokale Konfiguration eines Linux-Agenten ändern oder sich die aktuelle Konfiguration anzeigen lassen. Das Programm **drivelock-ctl** befindet sich im Installationsverzeichnis des DriveLock Linux-Agenten.

Folgende Kommandozeilenbefehle stehen zur Verfügung (siehe Abbildung):

```
test@debian10:~$ /opt/drivelock/drivelock-ctl -h
-----
Drivelock Linux Agent- Command line tool
-----
DriveLock, 19.2.5.27684

Usage: drivelock-ctl [Option]

Options:
  -enabletracing           Enable service logging
  -disabletracing         Disable service logging
  -updateconfig           Trigger a configuration update
  -showstatus             Show drivelock configuration status
  -settenant <tenantname> Set tenant name
  -setserver [http(s)://<server>:<port>] Set one or more server(DES) URLs,
                                         URLs should be delimited by ;
```

- **enabletracing**: Aktiviert das Tracing zur Datei **Drivelock.log**, die im Installationsverzeichnis im Unterordner **log** zu finden ist.
- **disabletracing**: Deaktiviert das Tracing
- **updateconfig**: Aktualisiert Ihre Konfiguration, z.B. wenn Sie Änderungen an Ihren Richtlinien gemacht haben. Der Linux Agent verbindet sich dann sofort mit dem DES und lädt die Änderungen.
- **settenant**: Gibt den Mandanten für Ihren Linux-Agenten an.
- **setserver**: Gibt den DES an, mit dem der Linux-Client kommuniziert.
- **showstatus**: Zeigt den aktuellen Status des Linux-Clients an und informiert, wann z.B. der DES zuletzt kontaktiert wurde und welche Richtlinien zugewiesen sind (siehe Abbildung unten).

```
test@debian10:~$ /opt/drivelock/drivelock-ctl -showstatus
```

```
Agent Identity:
```

```
-----
```

```
Agent version: 19.2.5.27684
```

```
Computer Name: debian10
```

```
Computer GUID: e9c7c1c9-e2fa-4dc6-85f3-b6fb140b78f3
```

```
Domain Name: localdomain
```

```
OS Name: Debian GNU/Linux
```

```
OS Version: 10 (buster)
```

```
Agent Configuration & Status:
```

```
-----
```

```
Tenant : kav
```

```
Server URL(s) : https://192.168.8.207:6067
```

```
Last server contact at : 10.02.2020 15:34:34
```

```
Last inventory at : unknown
```

```
Assigned Policies:
```

```
-----
```

```
1 CSP ID: 55f8de53-9444-4151-979b-8895c2cdc6da
```

```
ConfigName: Linux Tenant Test
```

```
Version: 7
```

```
Target: LinuxGroup
```

```
2 CSP ID: aad3f718-228f-4737-871b-e16e13fffc7a
```

```
ConfigName: TestEvtNotCfg
```

```
Version: 2
```

```
Target: LinuxGroup
```


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.

© 2021 DriveLock SE. Alle Rechte vorbehalten.