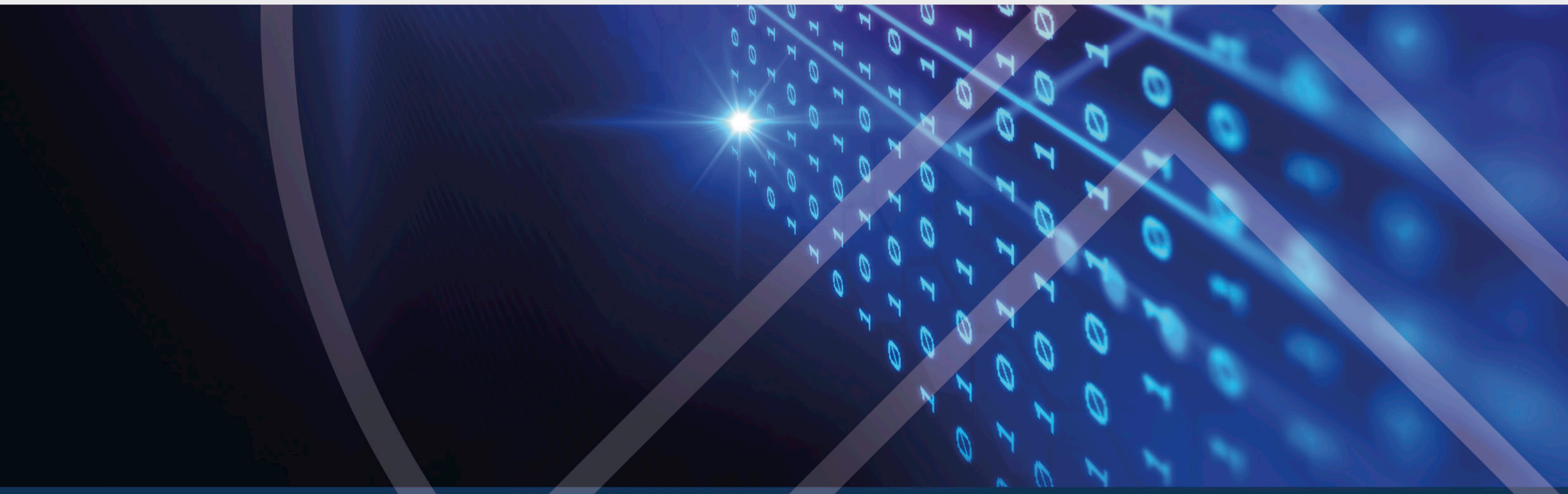
# DriveLock Linux Agent

## Manual 2020.2

DriveLock SE 2021



# Table of Contents

# 1 DriveLock Linux Agents

With release 2019.2 SP1, DriveLock supports assignment of centrally stored policies to DriveLock Agents running on Linux.

Linux support in this version is limited to blocking/allowing external devices and drives connected to the Linux clients via a USB interface. This gives DriveLock administrators the means to control the use of external devices and drives, even on DriveLock Linux Agents, so that these client computers are protected against malware attacks as well.

# 2 System Requirements

## 2.1 Supported Linux distributions

DriveLock supports the following 64-bit Linux distributions (as listed below and higher):

- CentOS Linux 8
- Debian 7
- Fedora 31
- IGEL OS starting with version 10
- Red Hat Enterprise Linux 5
- SUSE 15.1
- Ubuntu 18.04

## 2.2 DriveLock configurations

The following configuration requirements must be met to manage DriveLock Linux Agents in a DriveLock environment and control the use of their USB interfaces.

Full installation and configuration of a DriveLock Suite with

- DriveLock Management Console (DMC): Version 2019.2 and higher
- DriveLock Enterprise Service (DES): Version 2019.2 SP1 and higher
- DriveLock Linux-Agent (on Linux clients): Version 2019.2 SP1 and higher

> Note: Please ensure that the same DriveLock version (or higher) is installed on the DES and on the DriveLock Agent.

# 3 Installing the DriveLock Agent

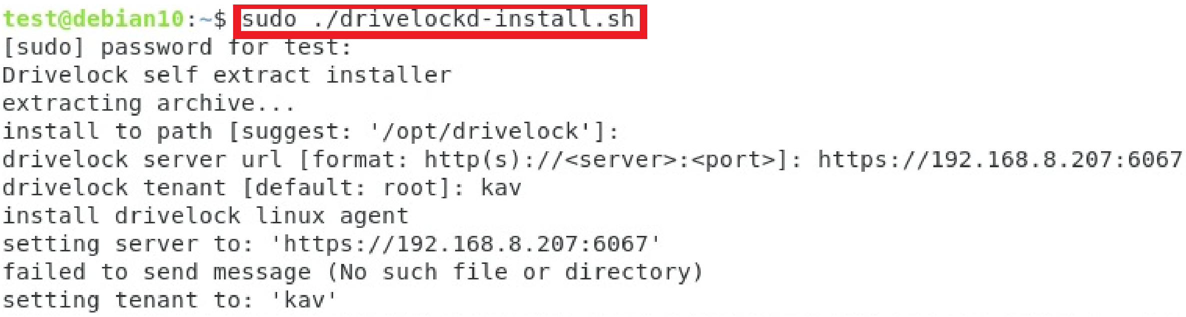
## 3.1 Installation instructions

Follow these steps to install the DriveLock Linux Agent on your Linux clients.

Note: Please note that the installation is different for IGEL clients.

1. Copy and extract the **drivelock.tgz** file on your Linux clients. It is included on the DriveLock ISO image.
2. The file contains the **drivelockd-install.sh** installation script . Run this script (see also Installation parameters).

   Warning: To run scripts on the Linux client, you must have administrator rights (see figure).



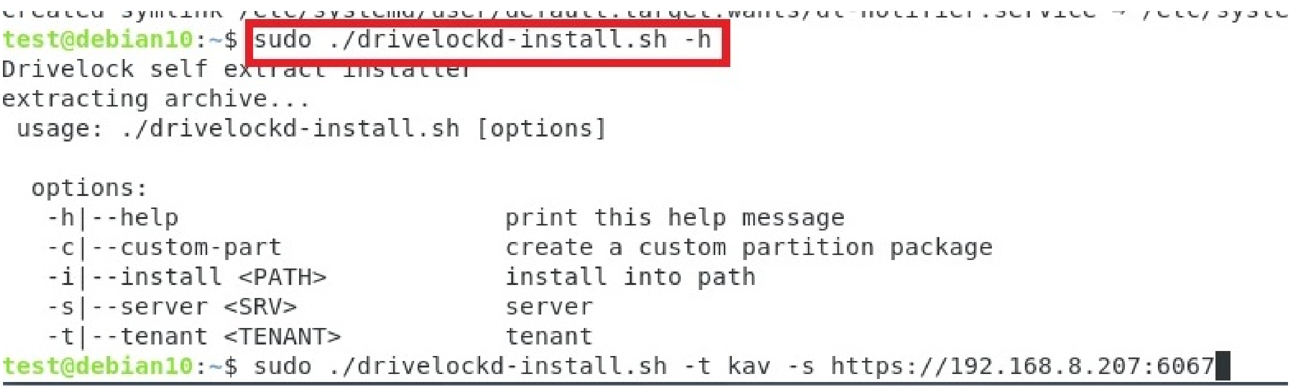
```
test@debian10:~$ sudo ./drivelockd-install.sh
[sudo] password for test:
Drivelock self extract installer
extracting archive...
install to path [suggest: '/opt/drivelock']:
drivelock server url [format: http(s)://<server>:<port>]: https://192.168.8.207:6067
drivelock tenant [default: root]: kav
install drivelock linux agent
setting server to: 'https://192.168.8.207:6067'
failed to send message (No such file or directory)
setting tenant to: 'kav'
```

3. Enter the following:
   - Installation path: The default is `/opt/drivelock`, but you can also specify a different path.
   - DES and port: Enter the server URL in the format '`https://<Server>:<Port>`' here.
   - Tenant: The default is 'root', but you can also specify a different tenant (in the figure `kav`).
4. The DriveLock Service starts as soon as the DriveLock Linux Agent has been completely installed.
5. If you experience errors during installation, we recommend restarting the Linux client to ensure that all DriveLock messages are displayed in the Linux client's user interface.

> Note: Note that the Linux client only displays a popup message when devices are connected or disconnected. There is no separate user interface for the DriveLock Agent.

## 3.2 Installation parameters

To install the DriveLock Linux Agent on your Linux clients, you can optionally use installation parameters. To display the individual parameters, open the installation script with the parameter `-h` (see figure).



```
created symlink /etc/systemd/user/default.target.wants/dl-notifier.service → /etc/syste
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
```

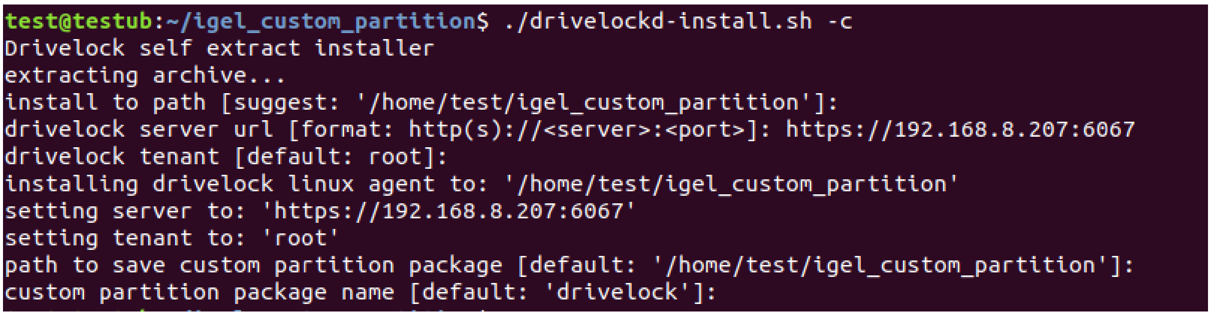
You can specify the following installation parameters:

- `-h`: Displays help for the installation parameters
- `-c`: This parameter only applies to IGEL clients. Here you enter the Custom Partition Package you want to use.
- `-i`: Enter the path to the DriveLock installation directory. The default is the current working directory, but you can also specify a different path.
- `-s`: Enter the server in the format 'https://<server>:<port>' here. See figure above.
- `-t`: Enter the tenant, the default is ‘root’.

## 3.3 Installing the DriveLock Agent on IGEL clients

Follow these steps to install the DriveLock Linux Agent on your IGEL clients.

1. Copy and extract the **tar -xzf drivelock.tgz** file on your Linux clients. It is included on the DriveLock ISO image.
2. The tar file contains the **drivelockd-install.sh** installation script.
   Run this script with the parameter `-c` (see figure).



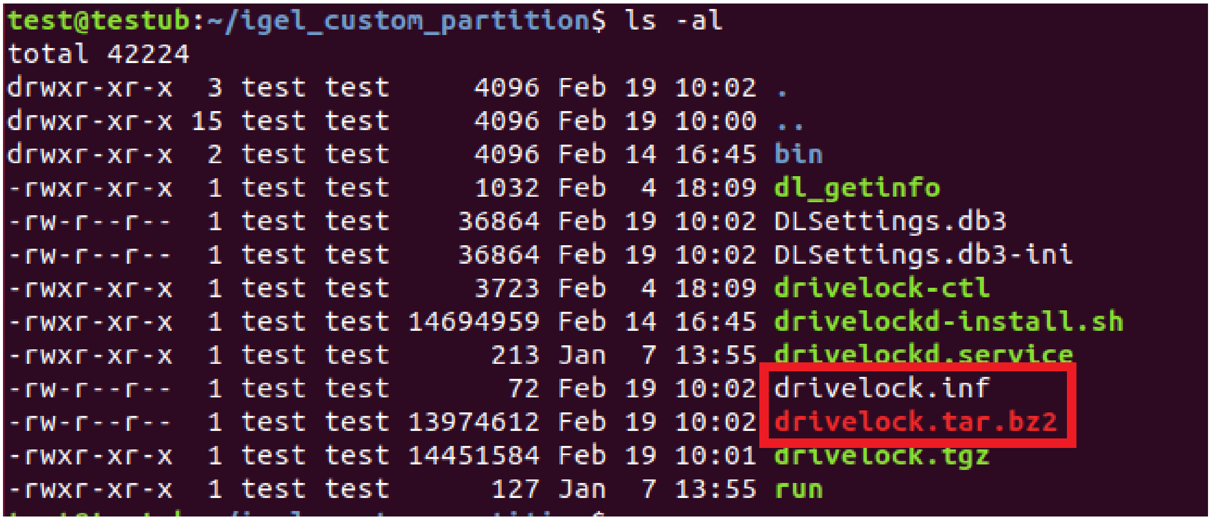
```
test@testub:~/igel_custom_partition$ ./drivelockd-install.sh -c
Drivelock self extract installer
extracting archive...
install to path [suggest: '/home/test/igel_custom_partition']:
drivelock server url [format: http(s)://<server>:<port>]: https://192.168.8.207:6067
drivelock tenant [default: root]: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

See Installation parameters for more information.

3. Enter the following:
   - Installation path: The default is the current working directory, but you can also specify a different path (in the figure `/home/test/igel_custom_partition`).
   - DES and port: Enter the server URL in the format '`https://<Server>:<Port>`' here.
   - Tenant: The default is `root`, but you can also specify a different tenant.
   - Path and name for the user-defined IGEL OS partition files. By default, these files are created in the current working directory.

Note: You do not need root rights for this process.

4. Once the script is finished, the IGEL OS partition files `drivelock.inf` und `drivelock.tar.bz2` are generated and located in the path specified in the above step.



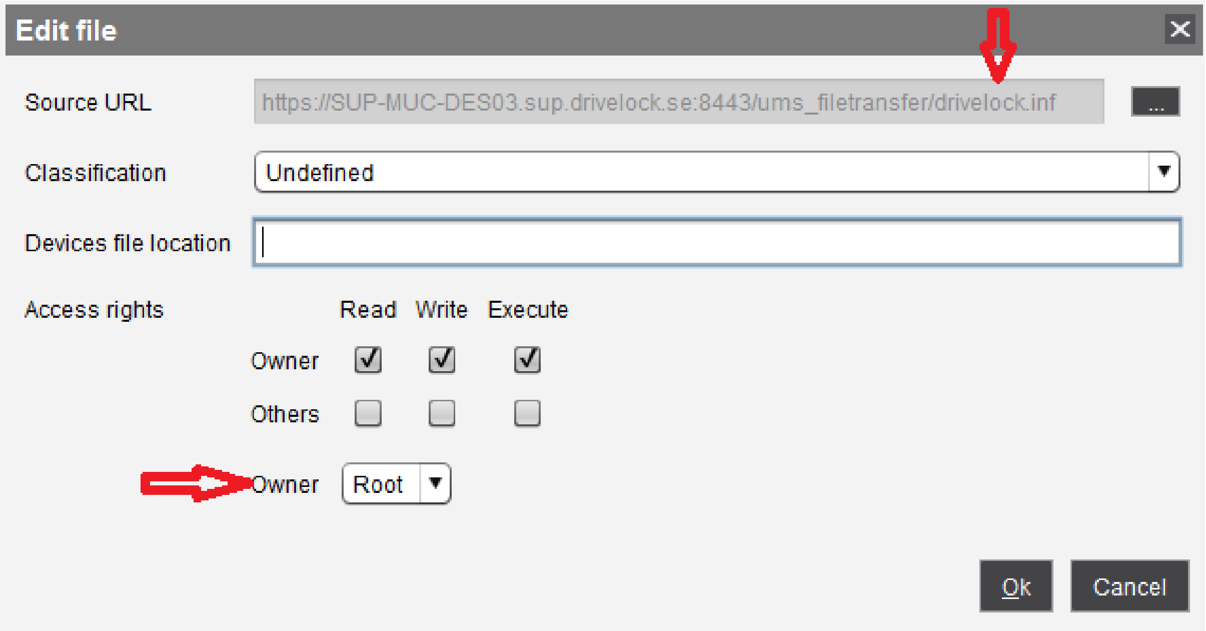
```
test@testub:~/igel_custom_partition$ ls -al
total 42224
drwxr-xr-x  3 test test     4096 Feb 19 10:02 .
drwxr-xr-x 15 test test     4096 Feb 19 10:00 ..
drwxr-xr-x  2 test test     4096 Feb 14 16:45 bin
-rwxr-xr-x  1 test test     1032 Feb  4 18:09 dl_getinfo
-rw-r--r--  1 test test    36864 Feb 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. Next, configure the UMS server.

### 3.3.1 Configuring the UMS server

Gehen Sie folgendermaßen vor:

1. Upload the **drivelock.inf** and **drivelock.tar.bz2** files to the UMS server.
2. Open the UMS Console.
3. In the UMS Console, navigate to **Files** -> **New File** -> **Upload local file to UMS server**.
4. Set **Root** as **Owner** (see figure).



Edit file

Source URL: https://SUP-MUC-DES03.sup.drivelock.se:8443/ums_filetransfer/drivelock.inf

Classification: Undefined

Devices file location:

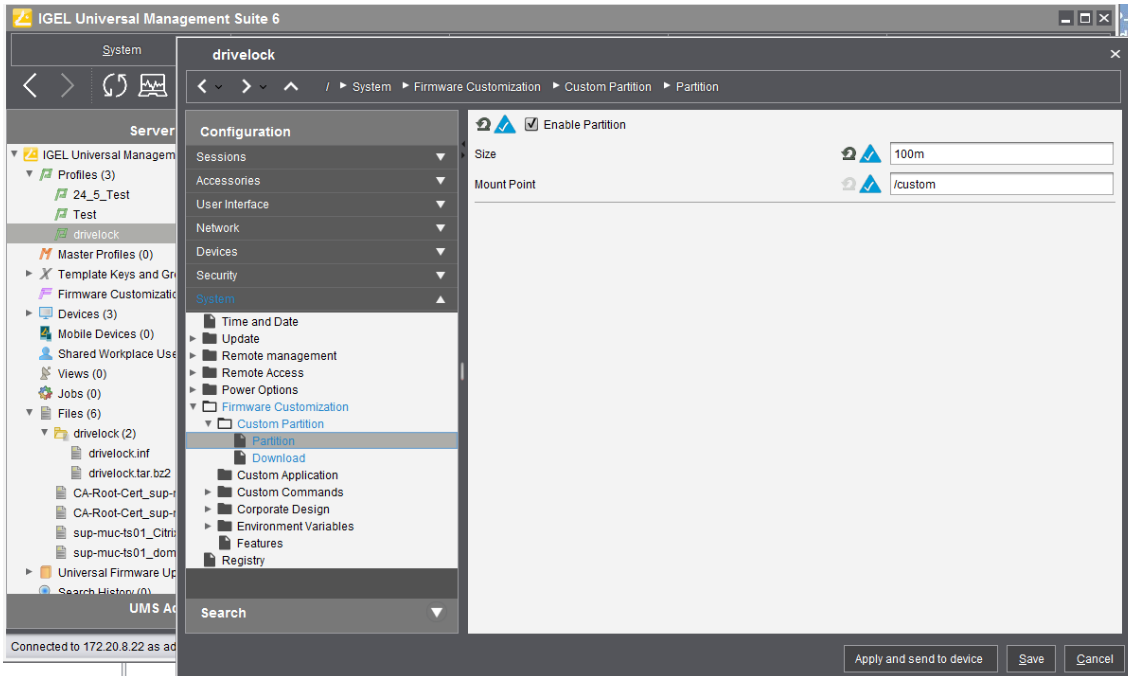
Access rights

| | Read | Write | Execute |
|---|---|---|---|
| Owner | ☑ | ☑ | ☑ |
| Others | ☐ | ☐ | ☐ |

Owner: Root

5. Repeat the same for the **drivelock.tar.bz2** file.
6. In the UMS system, create a new profile, e.g. drivelock.
7. In the UMS Console, navigate to **Profiles** -> **New Profiles** -> **Profile Name**.
8. Edit the created profile and activate the Custom Partition as follows (see figure):
    1. Navigate to **System** -> **Firmware Customization** -> **Custom Partition** -> **Partition**
    2. Unlock **Enable Partition**
    3. Check **Enable Partition**
    4. Set size of the partition to 150 or 200 MB

5. Keep /custom as **Mount Point**.

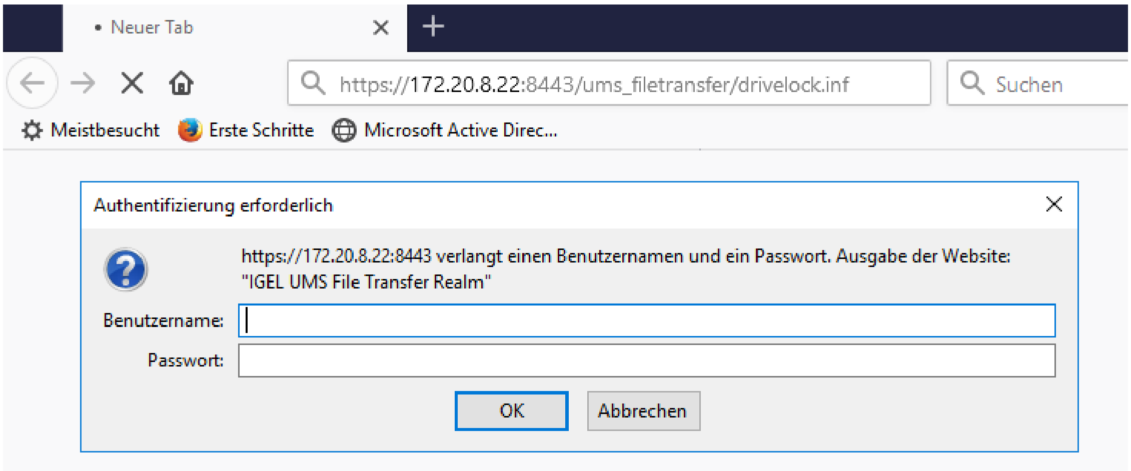


☑ Enable Partition

Size: 100m

Mount Point: /custom

9. Specify the download source.
   1. Navigate to **System** -> **Firmware Customization** -> **Custom Partition** -> **Download**
   2. Click [+] to add a **Partition Download Source**.
   3. Add the download URL **http(s)://<server>:8443/ums_filetransfer/drivelock.inf**
   4. Enter the **user name** and **password** to download the file. To confirm the user has access, test in browser.



https://172.20.8.22:8443/ums_filetransfer/drivelock.inf

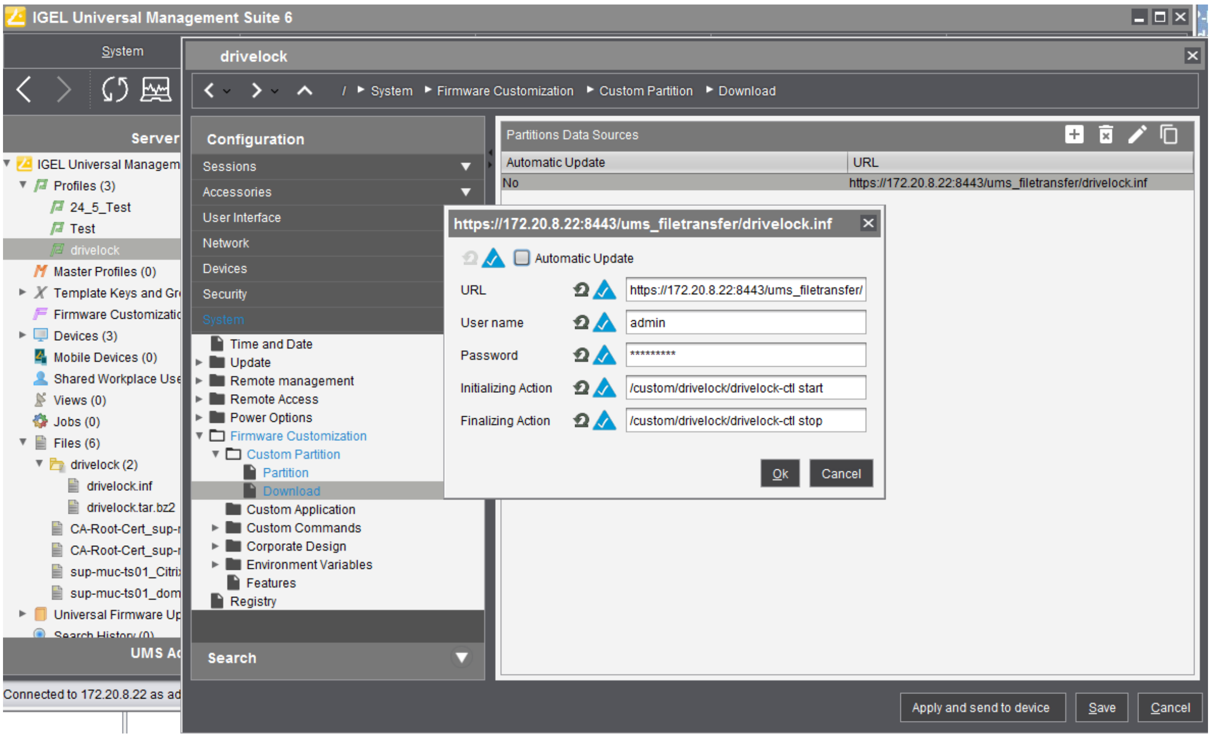
Authentifizierung erforderlich

https://172.20.8.22:8443 verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "IGEL UMS File Transfer Realm"

Benutzername:

Passwort:

10. In the next step, enter the following (see figure):
    Set **Initializing Action** to /custom/drivelock/drivelock-ctl start.
    Set **Finalizing Action** to /custom/drivelock/drivelock-ctl stop.



| Automatic Update | URL |
|---|---|
| No | https://172.20.8.22:8443/ums_filetransfer/drivelock.inf |

https://172.20.8.22:8443/ums_filetransfer/drivelock.inf

☐ Automatic Update

URL: https://172.20.8.22:8443/ums_filetransfer/

User name: admin

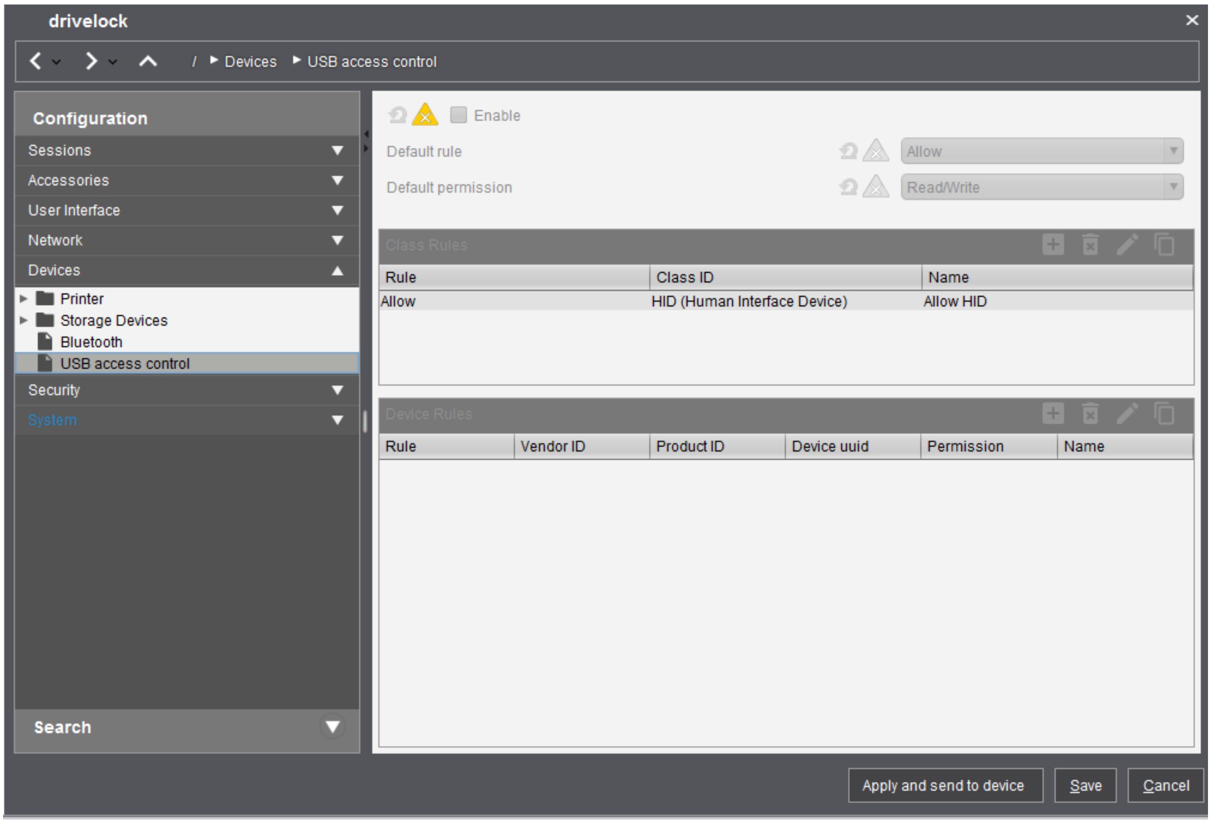
Password: *********

Initializing Action: /custom/drivelock/drivelock-ctl start

Finalizing Action: /custom/drivelock/drivelock-ctl stop

Note: Please note that the Mount Point matches the mount point configured in step 8.

11. Disable **USB access control** on Thin Clients.
    Navigate to **Devices** -> **USB access control** -> uncheck **Enable**.



Enable

Default rule: Allow

Default permission: Read/Write

Class Rules

| Rule | Class ID | Name |
|---|---|---|
| Allow | HID (Human Interface Device) | Allow HID |

Device Rules

| Rule | Vendor ID | Product ID | Device uuid | Permission | Name |
|---|---|---|---|---|---|

12. Assign the DriveLock profile to the Thin Clients.
    1. Navigate to **Devices** -> **Client**. Drag and drop the DriveLock profile icon to the Thin Client.
    2. As per requirement, select **Now** or **By next reboot** to activate the changes.

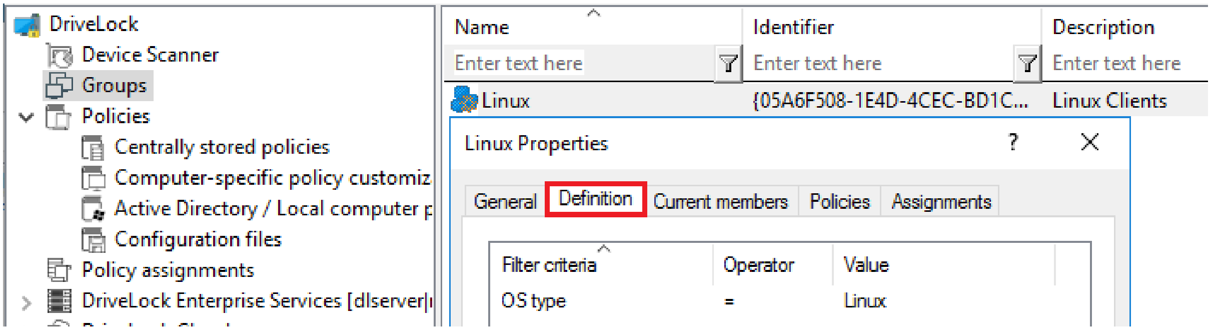
# 4 Configuration settings

## 4.1 Recommended procedure

To configure the DriveLock Linux Agent, we recommend following the procedure below:

1. Start by creating a DriveLock group (static or dynamic) that includes your Linux agents. This makes it easier to assign the policy you configure for your Linux agents later. Select the filter criteria **OS type Linux** as group definition.

   The figure below shows the dynamic **Linux** group with description **All Linux clients** and filter criterion **OS type = Linux**.

   | Name | Identifier | Description |
   |---|---|---|
   | Enter text here | Enter text here | Enter text here |
   | Linux | {05A6F508-1E4D-4CEC-BD1C... | Linux Clients |

   | Filter criteria | Operator | Value |
   |---|---|---|
   | OS type | = | Linux |

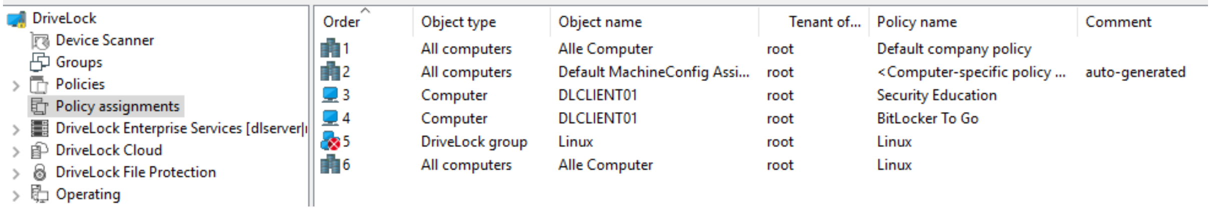
   Please refer to the DriveLock Administration Guide at drivelock.help for further information on groups.

2. To use a different tenant for your DriveLock Linux agents, select another one. For more information on using tenants, please also refer to the Administration Guide.

3. Create a new centrally stored policy for your Linux clients, name it accordingly (e.g. 'Linux policy') and start with Global settings.

4. Select the appropriate settings depending on the devices or drives you want to control.

5. Assign the 'Linux policy' to your DriveLock group. You can also assign to All Computers if you do not want to use a group.
   The figure below shows the 'Linux' policy assigned to the Linux group and to All Computers.

   | Order | Object type | Object name | Tenant of... | Policy name | Comment |
   |---|---|---|---|---|---|
   | 1 | All computers | Alle Computer | root | Default company policy | |
   | 2 | All computers | Default MachineConfig Assi... | root | <Computer-specific policy ... | auto-generated |
   | 3 | Computer | DLCLIENT01 | root | Security Education | |
   | 4 | Computer | DLCLIENT01 | root | BitLocker To Go | |
   | 5 | DriveLock group | Linux | root | Linux | |
   | 6 | All computers | Alle Computer | root | Linux | |

## 4.2 Policy settings for DriveLock Linux Agents

Use the following settings to configure the policies you want to assign to DriveLock Linux Agents:

- **Global configuration**: Settings, Server connections, Trusted certificates
- **EDR**: Events (General Agent events, Device and Drive events)
- **Drives**: Removable drive locking, Drive whitelist rules
- **Devices**: Device class locking, Device whitelist rules

❗ Warning: Please note that the settings for DriveLock Linux Agents are limited to controlling the USB interface.

The configuration of your 'Linux policy' depends on the specific requirements for your DriveLock Linux Agents.

Here are two scenarios (applicable to all users of the Linux clients):

- You want to allow the usage of Human Interface Devices, e.g. keyboards, but want to lock specific keyboards: create a device rule where you only list the devices you want to lock (blacklist mode).
- You want to block the usage of USB drives, e.g. USB flash drives, but want to allow specific USB flash drives: create a drive rule where you specify the allowed USB flash drives (whitelist mode).

❗ Warning: Note that the device and drive classes used in Windows and Linux do not always match. DriveLock currently uses the hardware ID of the device or drive that will be locked (or allowed) on the DriveLock Linux Agent as match criteria.

### 4.2.1 Global configuration

1. Open the **Settings** section to configure the following:
   - **Remote control settings and permissions**: On the **Permissions** tab you can add the users that are allowed to take action on the Linux agent, such as changing the configuration.
   - **Event message transfer settings**: Make sure to check the **Enable event forwarding to the DriveLock Enterprise Service** option on the **Server** tab. The second option, **Report agent status to server**, allows you to specify the intervals for sending agent alive messages to the DES.

- **Advanced DriveLock Agent settings**: On the **Intervals** tab you can set the intervals for loading the configuration from the server.

2. In the **Server connections** section you can add a new server, if required.
3. In the **Trusted certificates** section you select the certificates for the secure communication between the DriveLock Management Console and/or the DriveLock Linux Agents and the DES. Please refer to the DriveLock Administration Guide at drivelock.help for further information on certificates.

### 4.2.2 EDR

EDR (Event Detection & Response) provides an enhanced visualization of individual events combined with various configuration options. The EDR features can be useful, for example, to create rules that define the response to a particular event. Configurable responses (e.g. by running a specific script) allow you to react quickly to alerts.

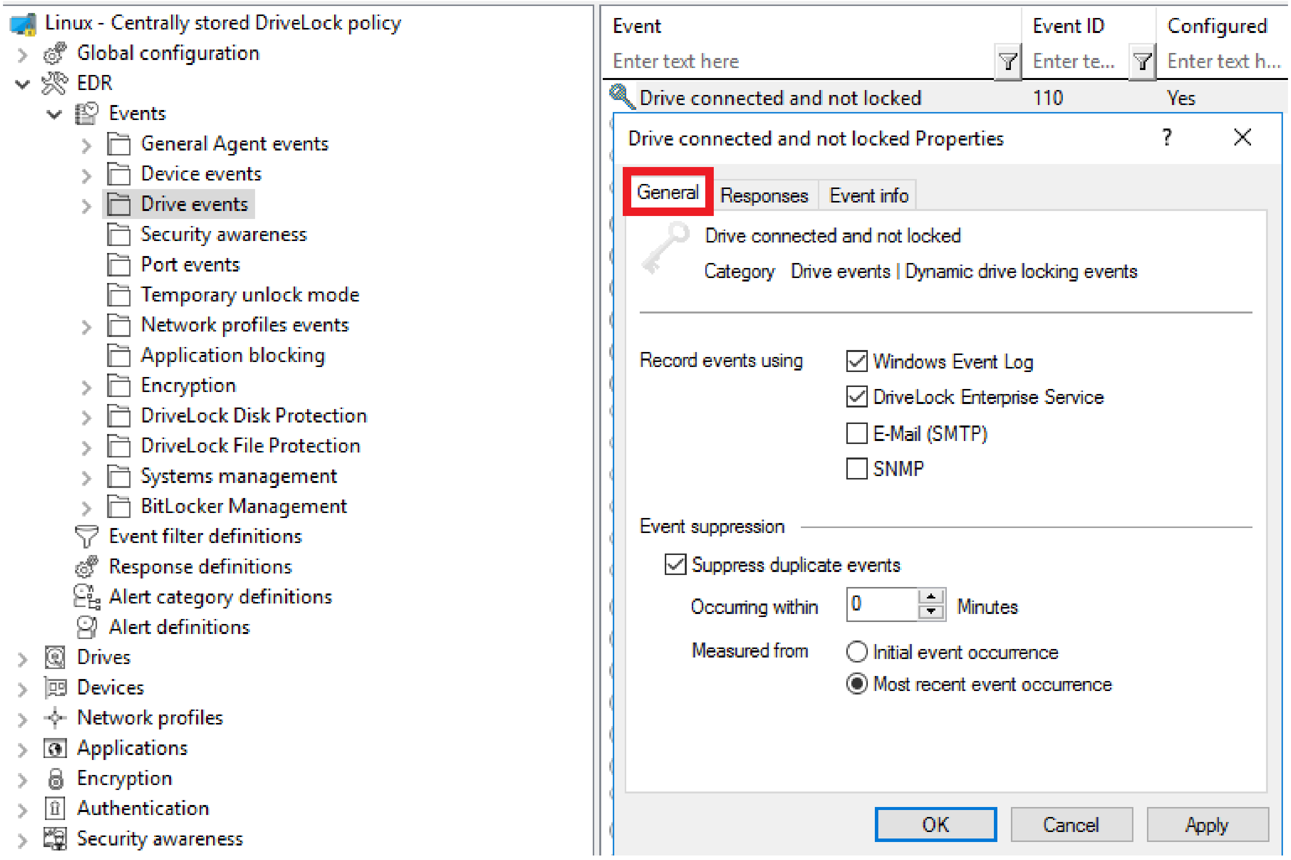
The only event categories that are important for DriveLock Linux Agents are **General Agent events**, **Device events** and **Drive events**. Refer to the list of events here.

The following settings are currently available for Linux Agents.

### 4.2.3 EDR: Event settings

Example of how to configure drive event 110, which indicates that a drive is connected to the DriveLock Linux Agent and that it is not locked.

1. In the **EDR** node, open the **Events** subnode. Doubleclick the event in the **Drive events** section. Currently only the settings on the **General** tab are available for Linux agents (see figure).
2. The System Event Log (**Windows Event Log**) option is the default, but you can also select **DriveLock Enterprise Service** to save the events in the event log on the DES.
3. If required, you can also check the **Suppress duplicate events** option.



- Linux - Centrally stored DriveLock policy
  - Global configuration
  - EDR
    - Events
      - General Agent events
      - Device events
      - Drive events
      - Security awareness
      - Port events
      - Temporary unlock mode
      - Network profiles events
      - Application blocking
      - Encryption
      - DriveLock Disk Protection
      - DriveLock File Protection
      - Systems management
      - BitLocker Management
    - Event filter definitions
    - Response definitions
    - Alert category definitions
    - Alert definitions
  - Drives
  - Devices
  - Network profiles
  - Applications
  - Encryption
  - Authentication
  - Security awareness

| Event | Event ID | Configured |
|---|---|---|
| Enter text here | Enter te... | Enter text h... |
| Drive connected and not locked | 110 | Yes |

Drive connected and not locked Properties

Drive connected and not locked

Category Drive events | Dynamic drive locking events

Record events using ☑ Windows Event Log
☑ DriveLock Enterprise Service
☐ E-Mail (SMTP)
☐ SNMP

Event suppression

☑ Suppress duplicate events

Occurring within 0 Minutes

Measured from ○ Initial event occurrence
● Most recent event occurrence

## 4.2.4 Drive settings

In the **Drives** node, select **Removable drive locking** and then doubleclick the **USB bus connected drives** option.

The Removable drive locking section provides two choices for your Linux policy:

> Note: Note that only the settings on the **General** tab apply to Linux policies.

1. Select the default option **Deny (lock) for all users (default)**:
   This setting blocks the use of all drives connected via the USB interface for all users. You will need to define a whitelist rule that allows specific drives to be used.
2. Select **Allow** (for all users):
   This option allows users to connect all drives over the USB interface. You will need to specify the drives you want to block in your drive rule.

## 4.2.5 Drive whitelist rules

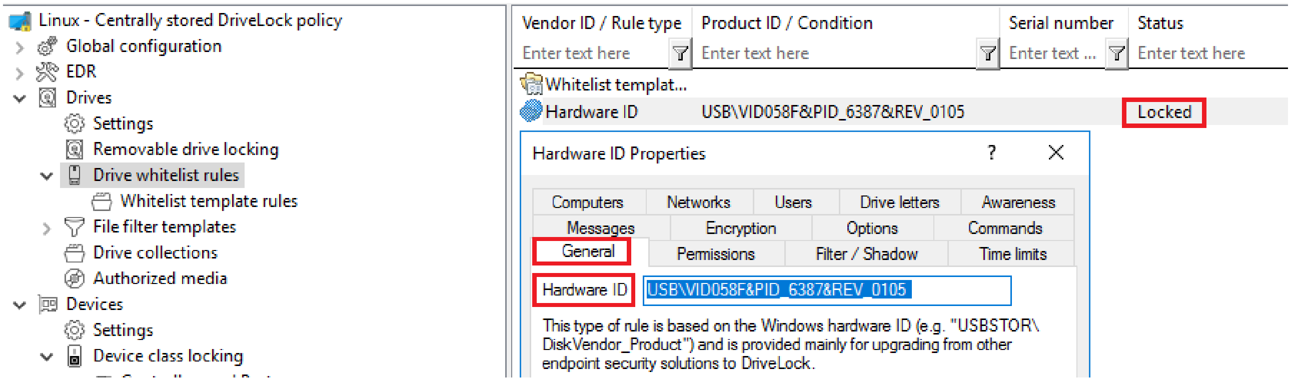
To configure a drive rule (as whitelist or blacklist), please proceed as follows:

1. In the **Drives** node, select **Drive whitelist rule**. Open the context menu, select **New** and then **Hardware ID rule**.

2. On the **General** tab, please enter the drive's hardware ID. This ID consists of the vendor ID (VID), product ID (PID) and revision number (REV).
3. On the **Permissions** tab, specify whether to deny (lock) or allow the drive (depending on your removable drive settings).

> Warning: Please note that you cannot use the option 'Deny (lock) but allow access for defined users and groups' on Linux agents.

The figure below shows that the USB drive with the hardware ID USB\VID058F&PID_6387&REV_0105 is blocked and cannot be used.



Linux - Centrally stored DriveLock policy
- Global configuration
- EDR
- Drives
  - Settings
  - Removable drive locking
  - Drive whitelist rules
    - Whitelist template rules
  - File filter templates
  - Drive collections
  - Authorized media
- Devices
  - Settings
  - Device class locking

| Vendor ID / Rule type | Product ID / Condition | Serial number | Status |
|---|---|---|---|
| Enter text here | Enter text here | Enter text ... | Enter text here |
| Whitelist templat... | | | |
| Hardware ID | USB\VID058F&PID_6387&REV_0105 | | Locked |

Hardware ID Properties

Hardware ID: USB\VID058F&PID_6387&REV_0105

This type of rule is based on the Windows hardware ID (e.g. "USBSTOR\DiskVendor_Product") and is provided mainly for upgrading from other endpoint security solutions to DriveLock.

### 4.2.6 Device settings

In the **Devices** node, select **Device class locking**.

This section provides two choices for your Linux policy:

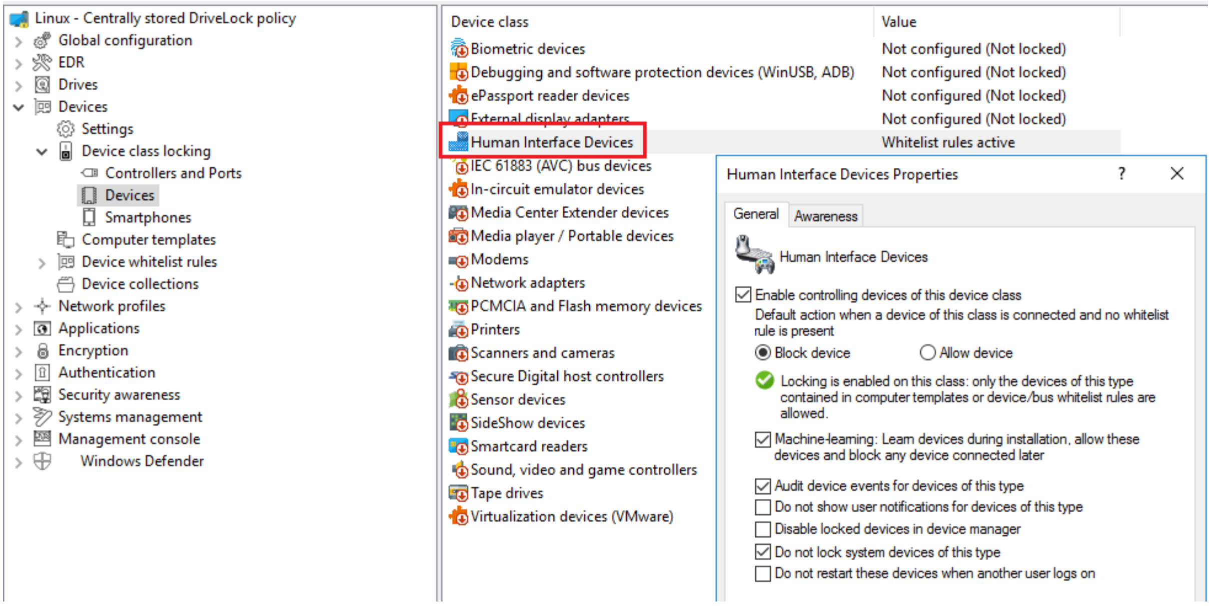
1. Open the **Controllers and Ports** section and doubleclick **USB controllers**. This setting lets you block or allow the complete USB interface of the Linux Agent.
   The following options are available:
   a. Leave the setting as it is.
      You do not check the **Enable controlling devices of this device class** option. This is the default setting: **Not configured (not locked)**.
   b. Lock the USB interface.
      Check the **Enable controlling devices of this device class** option and then select **Block device**. This means that you will need to configure appropriate whitelist rules for the devices you want to allow.
   c. Allow the USB interface.

Check the **Enable controlling devices of this device class** option and then select **Allow device**. This means that you will need to configure appropriate rules (blacklist) for the devices you want to block.

d. If you select the **Machine Learning** option, all devices that are connected to the Linux Agent during installation are entered into a local whitelist and thereby allowed. All other devices that are connected later are blocked.

2. Open the **Devices** section and doubleclick **Human Interface Devices**.

> Note: Please note that only some device classes available for the Windows policy have a Linux equivalent. This is why you can currently only block or allow Human Interface Devices (HID) (see figure).



| Device class | Value |
|---|---|
| Biometric devices | Not configured (Not locked) |
| Debugging and software protection devices (WinUSB, ADB) | Not configured (Not locked) |
| ePassport reader devices | Not configured (Not locked) |
| External display adapters | Not configured (Not locked) |
| Human Interface Devices | Whitelist rules active |
| IEC 61883 (AVC) bus devices | |
| In-circuit emulator devices | |
| Media Center Extender devices | |
| Media player / Portable devices | |
| Modems | |
| Network adapters | |
| PCMCIA and Flash memory devices | |
| Printers | |
| Scanners and cameras | |
| Secure Digital host controllers | |
| Sensor devices | |
| SideShow devices | |
| Smartcard readers | |
| Sound, video and game controllers | |
| Tape drives | |
| Virtualization devices (VMware) | |

Human Interface Devices

☑ Enable controlling devices of this device class

Default action when a device of this class is connected and no whitelist rule is present

● Block device ○ Allow device

Locking is enabled on this class: only the devices of this type contained in computer templates or device/bus whitelist rules are allowed.

☑ Machine-learning: Learn devices during installation, allow these devices and block any device connected later

☑ Audit device events for devices of this type

□ Do not show user notifications for devices of this type

□ Disable locked devices in device manager

☑ Do not lock system devices of this type

□ Do not restart these devices when another user logs on

The same dialog is displayed as described above:

a. Check the **Enable controlling devices of this device class** option and then select **Block device**.
All HID devices connected to the USB interface are blocked after the policy is assigned to the DriveLock Linux Agent. You must configure an appropriate whitelist rule for the devices you want to allow.

b. Check the **Enable controlling devices of this device class** option and then select **Allow device**.
All HID devices are allowed. This means that you will need to configure appropriate rules (blacklist) for the devices you want to block.

c. You can also select the **Machine Learning** option.

d. Keep the default options checked. None of the other options are relevant for Linux agents.

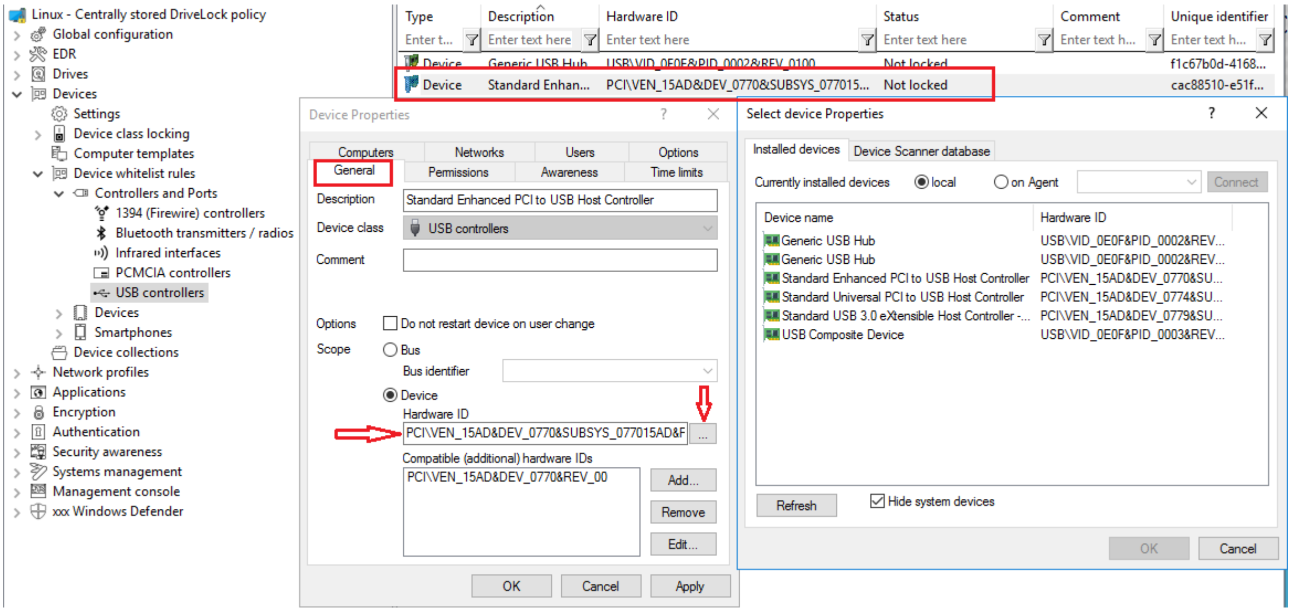
### 4.2.7 Device whitelist rules (for USB controllers)

To configure a device rule (as whitelist or blacklist) for USB controllers, please proceed as follows:

1. In the **Devices** node, open the **Device whitelist rules** subnode; select **Controllers and Ports** and then **USB controllers** (see figure).
2. Open the context menu, select **New** and then **Device or bus...**.
   None of the other options are relevant for Linux agents.
3. On the **General** tab, select the **Device** radio button and find the device you want to lock or allow (depending on whitelist or blacklist mode).
4. In the **Select devices** dialog you can display the devices that are installed **locally** or the devices that are currently connected to the DriveLock Linux Agent (**on Agent**). Note that the DriveLock Linux Agent must be online if you choose the 'on Agent' option.
5. On the **Permissions** tab, specify the appropriate **Device locking behavior**.

> Warning: Please note that you cannot use the option 'Deny (lock) but allow access for defined users and groups' on Linux agents.

In the figure below the USB controller with the ID **PCI\VEN_15AD&DEV_0770&SUBSYS_077015AD&REV_00** is allowed and has the status **not locked**.



| Type | Description | Hardware ID | Status | Comment | Unique identifier |
|---|---|---|---|---|---|
| Enter t... | Enter text here | Enter text here | Enter text here | Enter text h... | Enter text h... |
| Device | Generic USB Hub | USB\VID_0E0F&PID_0002&REV_0100 | Not locked | | f1c67b0d-4168... |
| Device | Standard Enhan... | PCI\VEN_15AD&DEV_0770&SUBSYS_077015... | Not locked | | cac88510-e51f... |

Device Properties

Description: Standard Enhanced PCI to USB Host Controller

Device class: USB controllers

Comment:

Options: □ Do not restart device on user change

Scope: ○ Bus

Bus identifier:

● Device

Hardware ID: PCI\VEN_15AD&DEV_0770&SUBSYS_077015AD&F ...

Compatible (additional) hardware IDs: PCI\VEN_15AD&DEV_0770&REV_00

Select device Properties

Currently installed devices ● local ○ on Agent

| Device name | Hardware ID |
|---|---|
| Generic USB Hub | USB\VID_0E0F&PID_0002&REV... |
| Generic USB Hub | USB\VID_0E0F&PID_0002&REV... |
| Standard Enhanced PCI to USB Host Controller | PCI\VEN_15AD&DEV_0770&SU... |
| Standard Universal PCI to USB Host Controller | PCI\VEN_15AD&DEV_0774&SU... |
| Standard USB 3.0 eXtensible Host Controller -... | PCI\VEN_15AD&DEV_0779&SU... |
| USB Composite Device | USB\VID_0E0F&PID_0003&REV... |

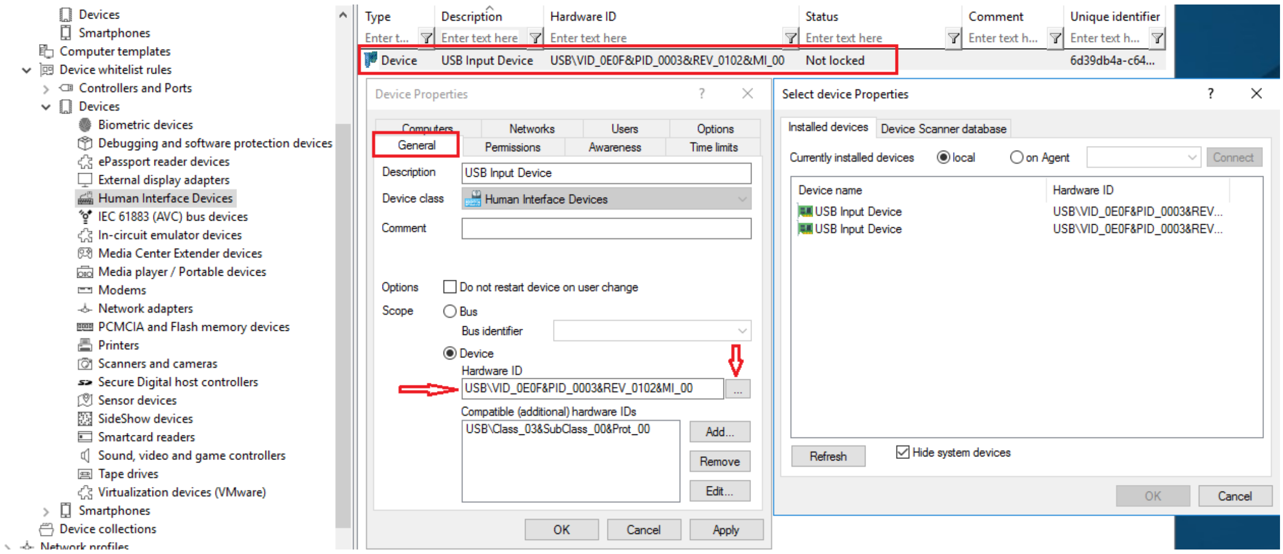
☑ Hide system devices

### 4.2.8 Device whitelist rules (for devices)

To configure a whitelist rule for devices, proceed as explained in Device whitelist rules (for USB controllers) except that you select **Input Devices (HID)** in the **Device whitelist rules** sub-node.

All other steps are identical.

In the figure below, the USB device with the hardware ID **USB\VID_0E0F&PID_0003&REV_0102&MI_00** has the status **Not locked**.


Devices
Smartphones
Computer templates
Device whitelist rules
Controllers and Ports
Devices
Biometric devices
Debugging and software protection devices
ePassport reader devices
External display adapters
Human Interface Devices
IEC 61883 (AVC) bus devices
In-circuit emulator devices
Media Center Extender devices
Media player / Portable devices
Modems
Network adapters
PCMCIA and Flash memory devices
Printers
Scanners and cameras
Secure Digital host controllers
Sensor devices
SideShow devices
Smartcard readers
Sound, video and game controllers
Tape drives
Virtualization devices (VMware)
Smartphones
Device collections
Network profiles

| Type | Description | Hardware ID | Status | Comment | Unique identifier |
|---|---|---|---|---|---|
| Enter t... | Enter text here | Enter text here | Enter text here | Enter text h... | Enter text h... |
| Device | USB Input Device | USB\VID_0E0F&PID_0003&REV_0102&MI_00 | Not locked | | 6d39db4a-c64... |

Device Properties

Description: USB Input Device

Device class: Human Interface Devices

Comment:

Options: □ Do not restart device on user change

Scope: ○ Bus

Bus identifier:

● Device

Hardware ID: USB\VID_0E0F&PID_0003&REV_0102&MI_00

Compatible (additional) hardware IDs: USB\Class_03&SubClass_00&Prot_00

Select device Properties

Currently installed devices ● local ○ on Agent

| Device name | Hardware ID |
|---|---|
| USB Input Device | USB\VID_0E0F&PID_0003&REV... |
| USB Input Device | USB\VID_0E0F&PID_0003&REV... |

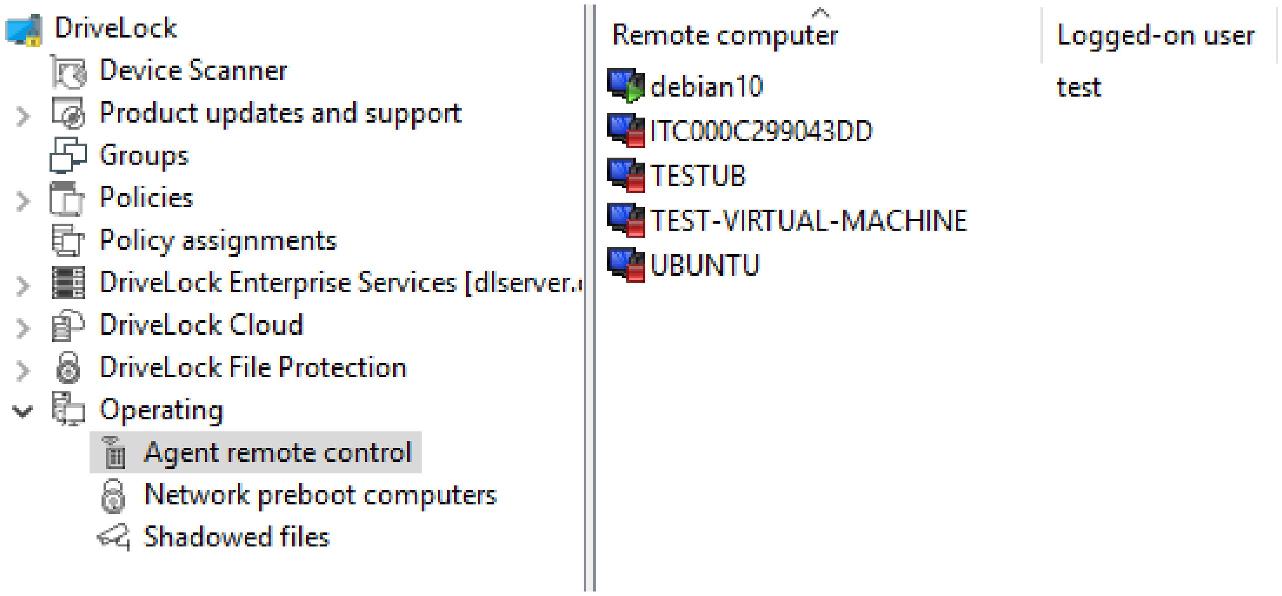
☑ Hide system devices

## 4.3 Agent remote control

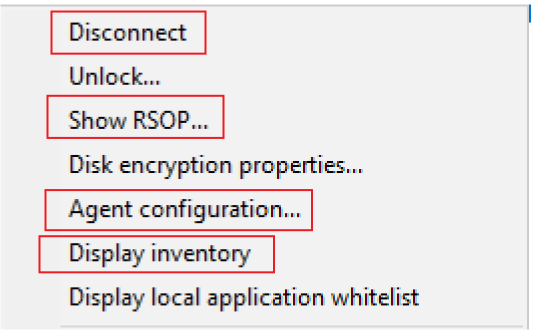
Open the **Operating** node in the DriveLock Management Console and select **Agent remote control**. You see a list of client computers where the DriveLock Agent is installed (see figure).

> Note: Please refer to the DriveLock Administration Guide at drivelock.help for further information on agent remote control.

Open the context menu of the Linux client you selected and click **Connect**.

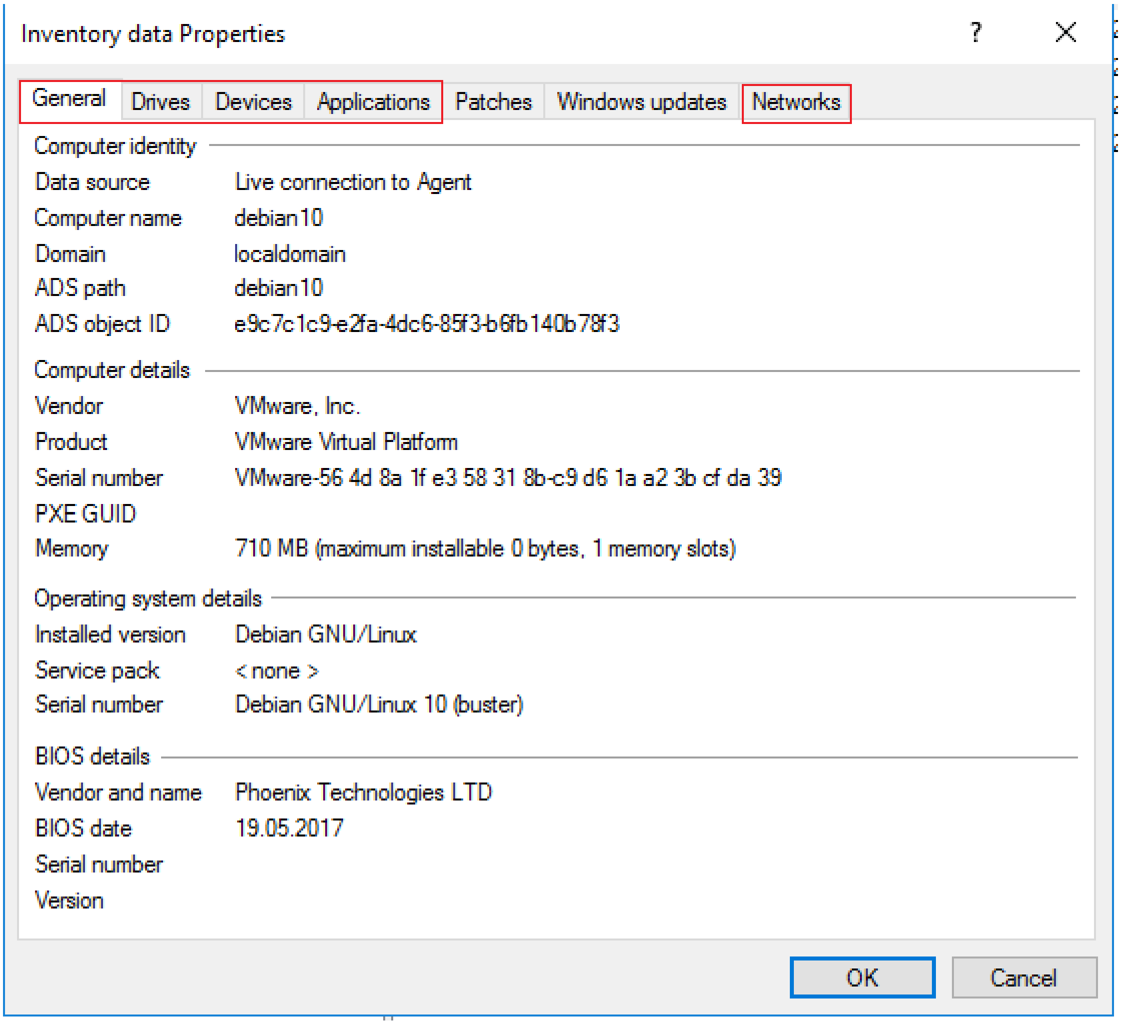


**The following agent remote control actions are relevant for Linux agents:**



1. **Disconnect** the Linux agent.
2. **Show RSOP...**
   Click this option to view a summary of the policy (Resultant Set of Policy) assigned to the Linux agent. You can not change any settings here.
3. **Agent configuration...**
   Click this option to open a dialog with information on the agent's configuration. It shows you the server your Linux agent receives the centrally stored policy from and, if necessary, you can add another server or enter another tenant on the **Options** tab.
4. **Display inventory**
   Click here to get inventory information on your Linux agent (on the **General**, **Drives**,

**Devices**, **Applications** and **Networks** tabs).



Inventory data Properties

Computer identity

|  |  |
|---|---|
| Data source | Live connection to Agent |
| Computer name | debian10 |
| Domain | localdomain |
| ADS path | debian10 |
| ADS object ID | e9c7c1c9-e2fa-4dc6-85f3-b6fb140b78f3 |

Computer details

|  |  |
|---|---|
| Vendor | VMware, Inc. |
| Product | VMware Virtual Platform |
| Serial number | VMware-56 4d 8a 1f e3 58 31 8b-c9 d6 1a a2 3b cf da 39 |
| PXE GUID |  |
| Memory | 710 MB (maximum installable 0 bytes, 1 memory slots) |

Operating system details

|  |  |
|---|---|
| Installed version | Debian GNU/Linux |
| Service pack | < none > |
| Serial number | Debian GNU/Linux 10 (buster) |

BIOS details

|  |  |
|---|---|
| Vendor and name | Phoenix Technologies LTD |
| BIOS date | 19.05.2017 |
| Serial number |  |
| Version |  |

# 5 Linux agents in the DCC

DriveLock Linux Agents are displayed in the DriveLock Control Center (DCC) like other DriveLock Agents.

Note: Refer to the DriveLock Control Center documentation for a detailed description of the DCC at drivelock.help.

The following views and features are important for Linux agents:

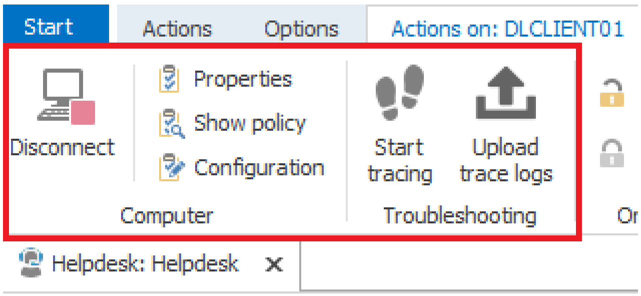
- **HelpDesk**:
  The HelpDesk view provides status and other information about your Linux agents. Find a description of the actions here.
- **Statistic report**:
  **Agent alive**: Here you can see the Linux agents that recently reported to DES.
- **Event report**:
  Shows all events the Linux agent sends to the DES. Refer to the list of events here.
- **Inventory**:
  **Computer**: Here you get an overview of your Linux agents with information about the respective Linux computer, operating system and DriveLock Linux Agent.
- **Open DOC**:
  Open the DriveLock Operations Center (DOC) in your browser to check the status of the DriveLock Linux Agents.

## 5.1 DCC: Help Desk actions

On the **Actions** tab, you can use the **Connect** button for DriveLock Linux Agents.

This action starts the agent remote control. You can also start remote control from the DriveLock Management Console.

1. Connect: Select the Linux agent on the list and click **Connect** or enter the name of the Linux client in the text box below the button.
2. Once the connection is set up, a new tab will appear, **Actions on: [Name of the Linux client]**.
   Here you can choose the following actions (see figure):



3. Click **Properties** for detailed information about the status of the Linux agent. The **General** tab provides an overview. By clicking the **Refresh policy...** button, you start the policy update on the agent.
4. Click **Show policy** to display the Resultant Set of Policy (RSOP) of the Linux agent.
5. Clicking **Configuration** opens a dialog with information about the configuration of the Linux agent. You can add another server or select another tenant here, for example.
6. Please contact DriveLock Technical Support if you want to enable **tracing** or debugging for your Linux agents.

# 6 Linux agents in the DOC

DriveLock Linux Agents are displayed in the DriveLock Operations Center (DOC) like other DriveLock Agents.

Note: Refer to the DriveLock Control Center documentation for an introduction to the DOC at drivelock.help.

The following DOC views are relevant for Linux agents:

- **Computer**: Filter by **OS Type** ( 🐧 icon), for example, to group your Linux agents by their OS type. Select any Linux agent to check details.
- **Groups**: If you have defined a DriveLock group for your Linux agents, it is displayed here with information about the respective members and the assigned policies.
- **Events**:This view lists the events that a Linux agent sends to the DES.
- **EDR**: The Endpoint Detection & Response view provides continuous monitoring and allows you to configure your response to security alerts.
- **Accounts**:This view provides a list of all user accounts that are allowed to access the DOC. It also shows information on status and roles along with name and logon details.

# 7 List of events

The table contains all events related to Linux as displayed in the DriveLock Control Center or the DriveLock  Operations Center (DOC). All events below are triggered by DriveLock:

The DriveLock Linux Agent sends the following events to the DES:

| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| 105 | Information | Service started | The [name] service was started. |
| 108 | Information | Service stopped | The service [name] was stopped. |
| 110 | Audit | Drive connected and unlocked | The drive [name] ([category]) was added to the system. It is a [type] bus device. The drive is [locked/unlocked] for this event's user account. Device Id: [ID] [ID] (Rev. [rev]) (Serial number [number]) Applied whitelist rule: [rule] Screen state (keyboard [Win]-[L]): [state] |
| 111 | Audit | Drive connected and locked | The drive [name] ([category]) was added to the system. It is controlled by {Product} because of com- |

| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| | | | pany policy. As an ACL was applied to the drive, some users may no longer be able to access it. It is a [type] bus device. The drive is [locked/unlocked] for this event's user account. Device Id: [ID] [ID] (Rev. [rev]) (Serial number [number]) Applied whitelist rule: [rule] Screen state (keyboard [Win]-[L]): [state] |
| 129 | Audit | Device connected and locked | The device [name] was connected to the computer. It was locked due to company policy. Device type: [type] Hardware ID: [ID] Class ID: [ID] Applied whitelist rule: [rule] Screen state (keyboard [Win]-[L]): [state] |
| 130 | Audit | Device connected and not locked | The device [name] was connected to the computer. Device type: [type] Hardware ID: [ID] Class ID: [ID] Applied whitelist rule: [rule] Screen state (keyboard [Win]-[L]): [state] |

| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| 152 | Warning | Policy storage extraction failed | The policy storage container [name] cannot be unpacked to the local computer. Some functions relying on files stored in this container may fail. |
| 153 | Warning | Configuration file applied | The configuration file [name] was successfully applied. |
| 154 | Error | Configuration file download error | The configuration file [name] could not be downloaded. Error code: [code] Error: [error] |
| 158 | Error | Configuration file error | The configuration file [name] could not be read. Error code: [code] Error: [error] |
| 191 | Warning | {PrefixEnterpriseService} selected | The {PrefixEnterpriseService} [name] was selected by {Product}. Connection ID: [ID] Used for: [Inventory/Recovery/Events] |
| 192 | Warning | {PrefixEnterpriseService} not available | No {PrefixEnterpriseService} is |

| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| | | | available because no valid server connection is configured. |
| 235 | Error | SSL: Cannot set up | The encrypted communications layer (SSL) could not be set up. Error: [error] |
| 236 | Error | Remote control: Cannot set up server | The remote control server component coud not be set up. Agent remote control will be unavailable. Error: [error] |
| 237 | Error | Remote control: Internal error | Agent remote control: An internal SOAP communications error occurred. Error: [error] |
| 238 | SuccessAudit | Remote control: Function called | An Agent remote control function was called. Calling IP address: [IP address] Called function: [function] |
| 243 | Error | Cannot open database | A database could not be opened. Database file: [name] Error code: [code] Error: [error] |

| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| 246 | Error | Cannot store configuration status | The Agent cannot store the configuration status used by other {Product} components. Error code: [code] Error: [error] |
| 247 | Error | Cannot initialize configuration store | {Product} Agent cannot initialize the configuration database stores. |
| 249 | Error | Configuration file: Fallback configuration applied | A configuration using configuration files was detected but no settings could be retrieved from a configuration database. {Product} will fall-back to a configuration where all removable drives are blocked. |
| 250 | Warning | Configuration file: Using cached copy | The configuration file [name] could not be loaded from its original location. A locally cached copy was used. |
| 251 | Error | Configuration file: Cannot extract | A {Product} configuration file could no be extracted.%rSettings from this file will not be applied. |

| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| | | | Database file: [name] Error code: [code] Error: [error] |
| 264 | Error | Cannot merge configuration database with RSoP | Cannot merge the configuration database [name] into the resulting set of policy. |
| 287 | Error | No server defined for inventory | No server is defined for uploading collected inventory data. |
| 288 | Information | Inventory collection successful | Hard- and software inventory data was successfully collected and uploaded. DES server: [server name] Connection ID: [ID] |
| 289 | Information | Inventory collection failed | An error occurred while collecting hard- and software inventory data.DES server: [server name] Connection ID: [ID] Error: [error] |
| 294 | Error | Cannot download centrally stored policy | The centrally stored policy [name] could not be downloaded. Server: [name] Error: [error] |

| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| 295 | Error | Centrally stored policy: Cannot extract | A centrally stored policy could no be extracted. Settings from this file will not be applied. Configuration ID: [ID] Error code: [code] Error: [error] |
| 297 | Error | Centrally stored policy: Fall-back configuration applied | A configuration using centrally stored policies was detected but no settings could be retrieved from a server. {Product} will fallback to a configuration where all removable drives are blocked. |
| 299 | Information | Centrally stored policy downloaded | The centrally stored policy [name] was successfully downloaded. Configuration ID: [ID] Version: [version] |
| 443 | Error | Component start error | A {Product} system component could not be started on this computer. Error code: [code] Error: [error] Component ID: [ID] |
| 520 | Error | All {PrefixES} not reachable | Cannot load company policy. All configured {Pre- |

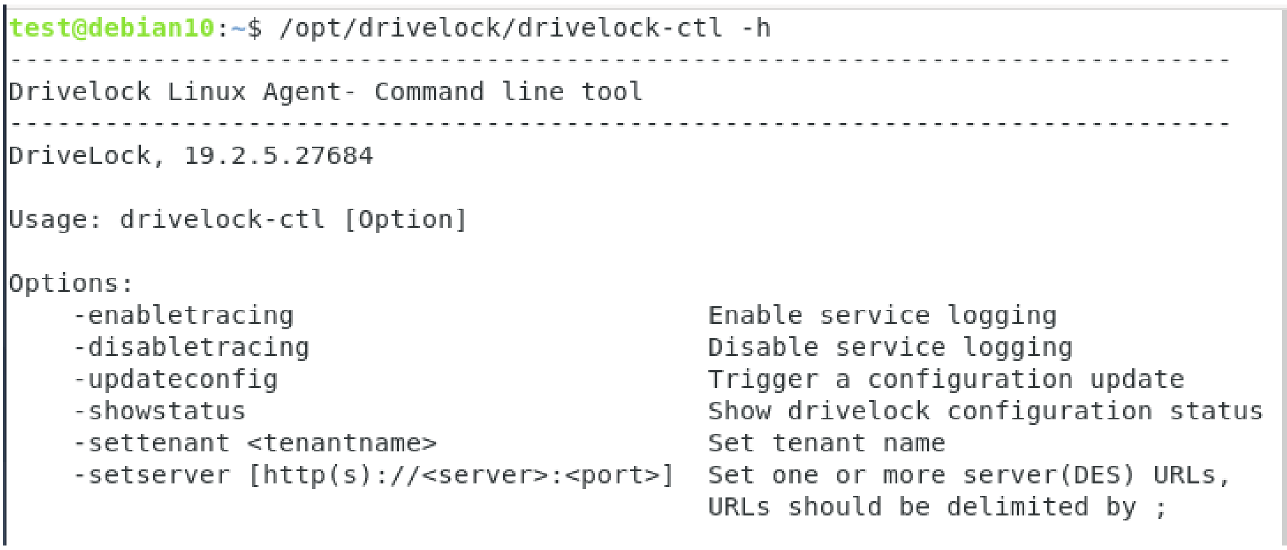
| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| | | | fixEnterpriseService}s are not reachable. |
| 521 | Error | Cannot determine computer token | Cannot determine the computer token. Error code: [code] Error: [error] |
| 522 | Error | Error loading policy assignments | An error occurred while loading policy assignments from server [name]. Error: [error] |
| 523 | Error | Policy integrity check failed | The integrity of an assigned policy could not be verified.%rPolicy ID: [ID] Policy name: [name] Actual hash: [value] Expected hash: [value] |
| 533 | Warning | No policy - wiped | No valid policy available - the company policy was wiped because the computer was offline for a long period of time. |
| 584 | Information | Inventory started | Inventory generation was triggered by DES. |
| 639 | Error | Server certificate error | Server certificate error detected. Certificate: |

| Event ID | Event level (Information, Warning, Error) | Event text | Description |
|---|---|---|---|
| | | | [name]. Error message: [text] |

# 8 Command line tool

Use this command line tool to change the local configuration of a Linux Agent or to display the current configuration. You will find the **drivelock-ctl** tool in the installation directory of the DriveLock Linux Agent.

The following commands are available (see figure):

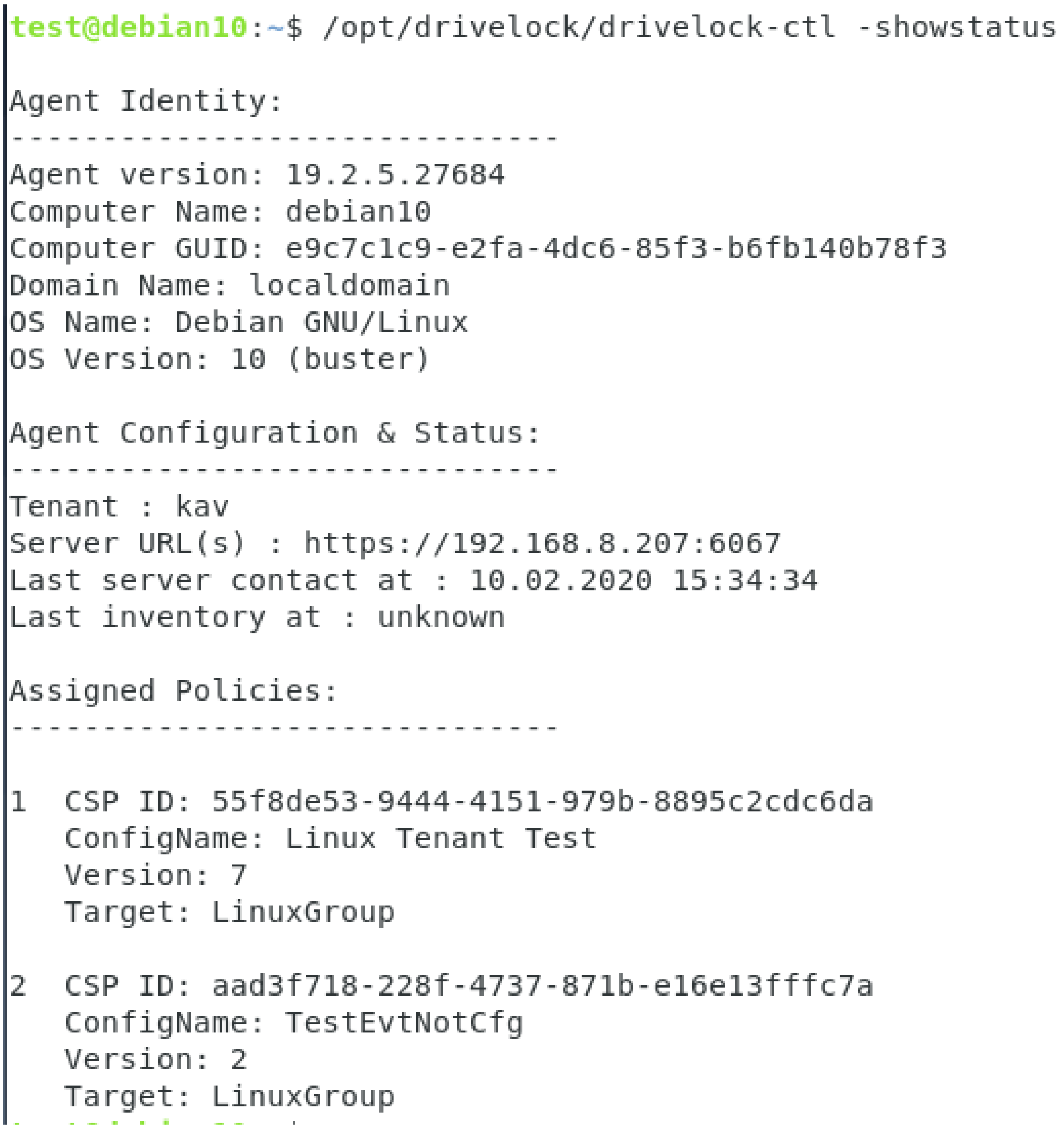


```
test@debian10:~$ /opt/drivelock/drivelock-ctl -h
-----------------------------------------------------------------------------
Drivelock Linux Agent- Command line tool
-----------------------------------------------------------------------------
DriveLock, 19.2.5.27684

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`: Enables tracing to the **Drivelock.log** file residing in the installation directory in the **log** child directory.
- `disabletracing`: Disables tracing
- `updateconfig`: Updates the configuration, for example after modifying the policies. The Linux agent connects to the DES immediately and uploads the modifications.
- `settenant`: Specifies the tenant for your Linux agent
- `setserver`: Specifies the DES that communicates with the Linux agent
- `showstatus`: Shows the current status of the Linux agent and provides information such as the last time the DES was contacted and the policies assigned (see figure below)



```
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