DriveLock MacOS Agent

Documentation 2023.1

DriveLock SE 2023

Table of Contents

1 DriveLock macOS support

DriveLock supports assigning centrally stored policies to DriveLock Agents running Catalina (10.15) OS and above on Intel and ARM architectures.

> Note: DriveLock on-premise customers can find the macOS Agent (DriveLock Agent.dmg) on the DriveLock ISO file. Managed services customers can download the macOS Agent package from the installation area in the DriveLock Operations Center (DOC).

DriveLock macOS support is currently limited to selective blocking of external drives that end users connect to their macOS clients via a USB interface. This feature lets administrators control the usage of external drives thus making sure that the DriveLock macOS Agents are reliably protected against malware attacks. In addition, admins can check the related DriveLock events and create event filter definitions.

Starting with version 2023.1, command line parameters can also be used to specify a proxy server used for downloads and DES communication.

> Note: The DriveLock Agent comes as a system extension and as such supports the Apple Endpoint Security Framework. For more information on system extensions and Endpoint Security, click here and here.

2 System requirements

2.1 Supported macOS versions

DriveLock supports macOS starting with version Catalina (10.15) with Intel (x86_64) and Apple Silicon (arm64) architectures.

2.2 DriveLock configurations

To be able to manage macOS Agents in a DriveLock environment, the configuration and installation of the following DriveLock management components is required. The macOS support starts with DriveLock version 2022.2.4.

- DriveLock Management Console (DMC) and Policy Editor or DriveLock Operations Center (DOC) with DOC Companion
- DriveLock Enterprise Service (DES)
- DriveLock macOS Agent (on macOS clients)

Note: Please make sure that the DES is always running the same DriveLock version or higher as the DriveLock Agent.

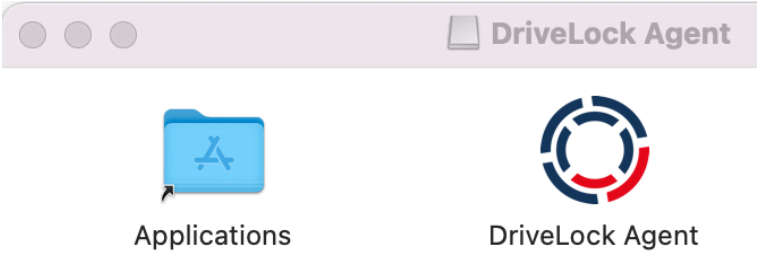
3 Installing the DriveLock macOS Agent

3.1 Installation instructions

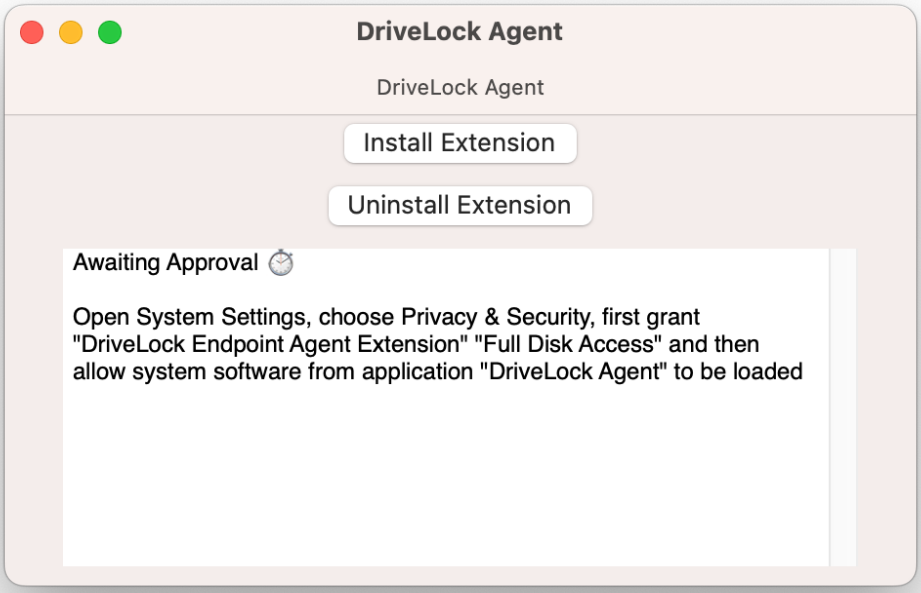
Follow these steps to install the DriveLock macOS Agent on macOS clients.

Note: First, copy the DriveLock Agent app to the /Applications folder and then activate the DriveLock Agent system extension.

1. Double-click the **DriveLock Agent.dmg** disk image file.
2. Drag and drop the **DriveLock Agent** app into the **Applications** folder.

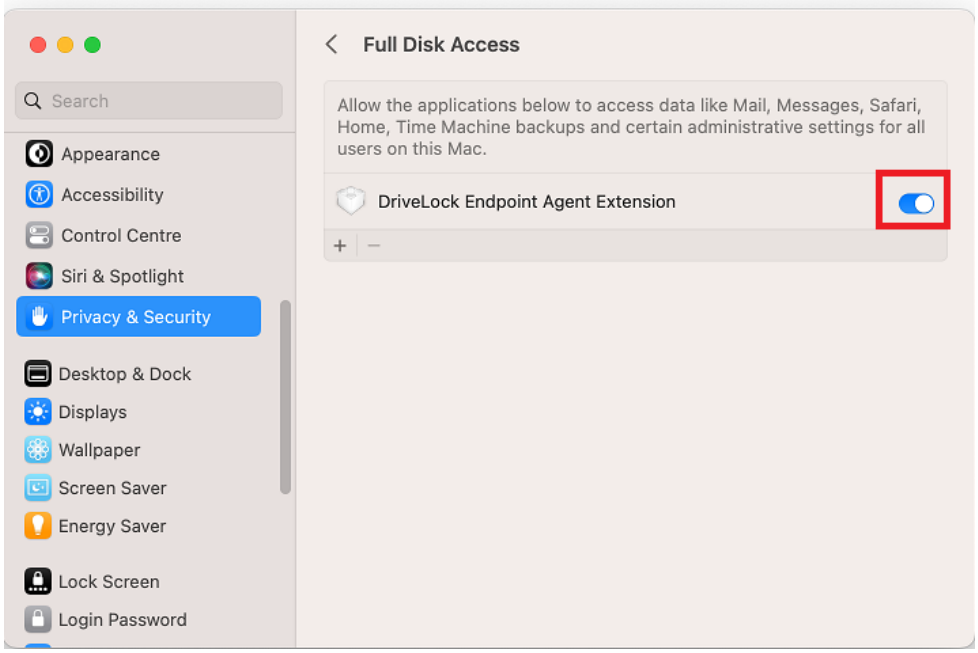


3. Now, configure the DriveLock Agent by running the following command line:
   `% sudo /Applications/DriveLock\ Agent.app/Contents/MacOS/dlconfig -t tenant_name -s DES_server_url -d debug_level`
   Example:`% sudo /Applications/DriveLock\ Agent.app/Contents/MacOS/dlconfig -t root -s https://DES_HOSTNAME:6067 -d 3`
4. Start the DriveLock Agent system extension activation process from the DriveLock Agent app.
   1. Open the **DriveLock Agent** app in the **Applications** folder.
   2. Click the **Install extension** button.

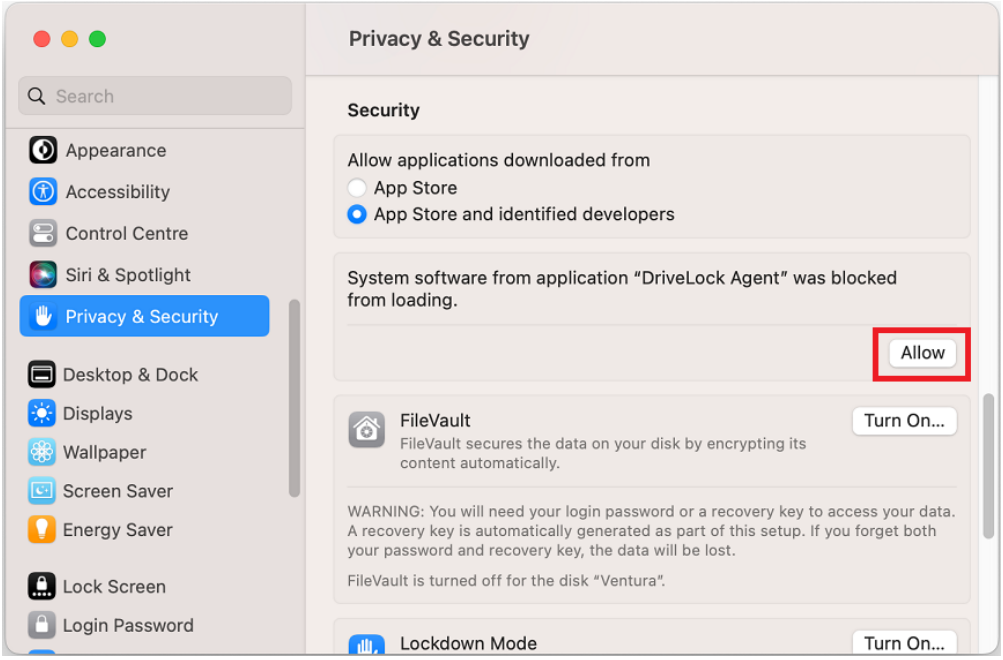


Note: Alternatively, you can enable the system extension from the command line by entering the following command: `% /Applications/DriveLock\ Agent.app/Contents/MacOS/DriveLock\ Agent -a`

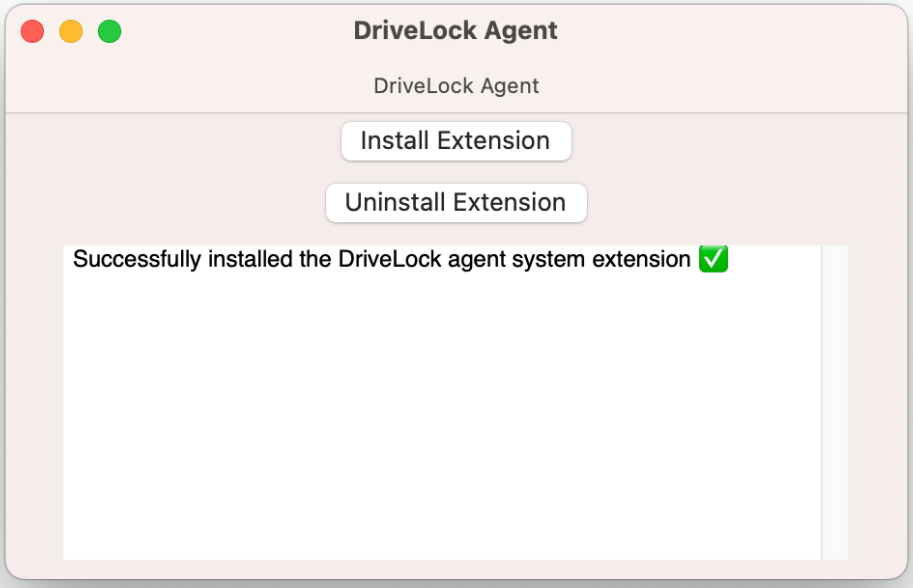
5. Then, in the **System Preferences/Settings** -> **Privacy & Security** section, enable **Full Disk Access** for **DriveLock Endpoint Agent Extension**.



6. Next, allow the system software to load.



7. The installation is completed successfully as soon as the following message appears:



8. If necessary, you can check the process status of the DriveLock Agent in the activity display.

3.1.1 Use join token

The functionality to securely add agents by means of a join token can also be used for macOS Agents. After installation, this is done by setting an accession token with the `--jointoken` option.

```
#sudo ./dlconfig -t tenant_name -s DES_server_url --jointoken join-token
```

Example:`#sudo ./dlconfig -t root -s https://192.168.8.75:6067 --join-token fa173c1e-6403-439d-8850-f0a71a2fbea7`

You can find the join token of a macOS client in the computer details in the DOC.

3.2 Update

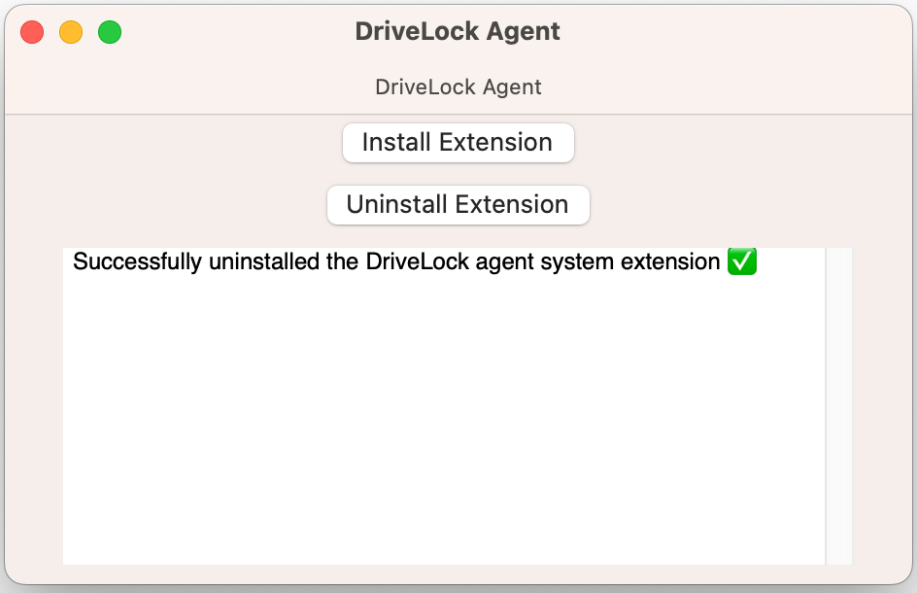
The steps for updating a running DriveLock Agent are the same as the installation steps described, except that the system settings (steps 5 and 6) are omitted.

> Note: It is not necessary to uninstall before updating.

3.3 Uninstall

Before removing DriveLock Agent app from the applications, the installed DriveLock Agent system extension hosted by this app must be disabled in the system. There are several ways to uninstall the DriveLock Agent app and the hosted system extension.

- **Uninstalling with the DriveLock Agent app**
  1. Open the app under **Programs**.
  2. Click the **Uninstall extension** button.
  3. Enter your password to delete the system extension.
  4. After the message **Successfully uninstalled the extension** appears in the app's dialog box, quit the DriveLock Agent app and delete it from the **Applications** folder.



Note: Alternatively, you can disable the system extension from the command line by entering the following command:

```
% /Applications/DriveLock\ Agent.app/Contents/MacOS/DriveLock\ Agent -d
```

- **Delete DriveLock Agent app directly from Programs.**
  1. Enter your password to delete the DriveLock Agent system extension.
  2. If the DriveLock Agent program is not completely removed the first time, you may have to delete it twice.

Warning: For complete removal, the computer must be rebooted and the /DriveLock/ directory under /opt/ must be removed. To reinstall the DriveLock Agent app, all installation steps including configuration steps must be performed.

4 Settings in the DriveLock Policy Editor

The following settings are used to configure policies that will be assigned to DriveLock macOS Agents:

- **Global configuration**: Settings, Server connections, Trusted certificates
- **Events and alerts**: events (general events, device and drive events), event filter definitions
- **Drives**: Removable drive locking, Drive whitelist rules
  Example: If you want to generally block the usage of USB drives, but allow specific USB flash drives, you will set the appropriate blocking settings first and then create a drive rule for the allowed USB flash drives (whitelist mode).

> Warning: Please note that the settings for drives for DriveLock macOS Agents are limited to controlling the USB interface.

4.1 Global configuration

1. Open the **Settings** section to configure the following:
   - **License**: Add here the licenses you have purchased for your macOS Agents.
   - **Remote control settings and permissions**: On the **Permissions** tab, you specify the users who are explicitly allowed to perform actions on the macOS Agent, such as making changes to 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.
   - Settings for logging: **Logging level**, **Maximum log file size in MB** and **Time until automatic deletion of old log files**.
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 macOS Agents and the DES.

Note: For more information on all settings, see the corresponding chapter under DriveLock Administration auf DriveLock Online Help.

4.2 Drives

4.2.1 Drive settings

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

You have two options for the drive settings for your macOS policy:

Note: Note that only the settings on the **General** tab are relevant for macOS 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.

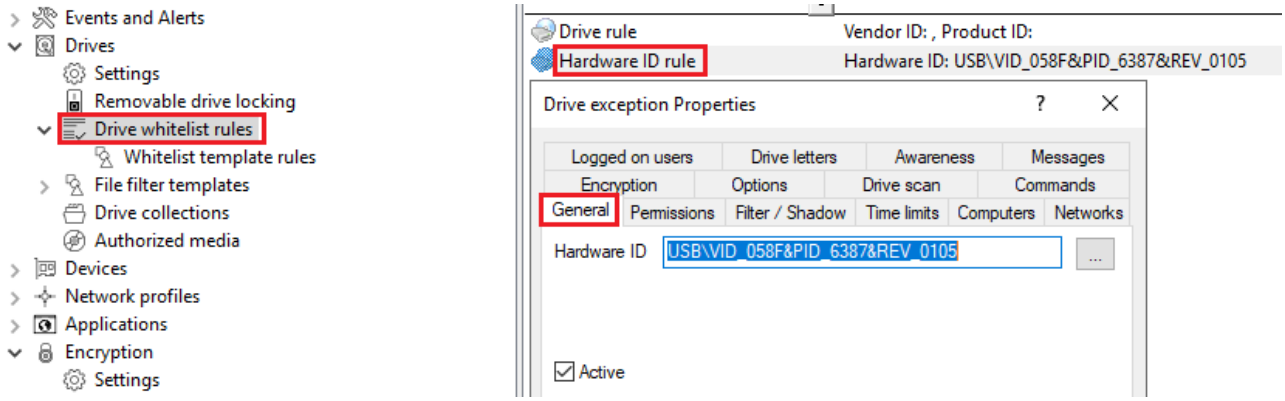
4.2.2 Drive whitelist rules

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: Note that locking with access for defined users/groups is not possible on macOS Agents.

In the figure below, the USB drive with hardware ID USB\VID_058F&PID_6387&REV_0105 is locked for use.



4.3 Agent remote control

In the DriveLock Management Console, open the **Operating** node and select **Agent remote control**. You will see a list of client computers on which DriveLock Agent is installed.

> Note: For more information on agent remote control, see DriveLock Administration at drivelock.help.

Click **Connect** on the context menu of the selected macOS client.

The following remote control features are relevant to DriveLock macOS Agents:

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

4.3.1 Temporary unlock

Use the temporary unlocking feature to quickly and temporarily allow a connected DriveLock macOS Agent to access blocked drives via agent remote control in the DriveLock

Management Console (DMC). This can also be done from the DriveLock Operations Center (DOC).

Please do the following:

1. From the macOS Agent context menu, choose the menu command **Unlock computer online...**
2. Specify the drive types you want the unlock to apply to.
3. Then, specify the time period and reason for unlocking the drive.

5 macOS Agents in the DOC

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

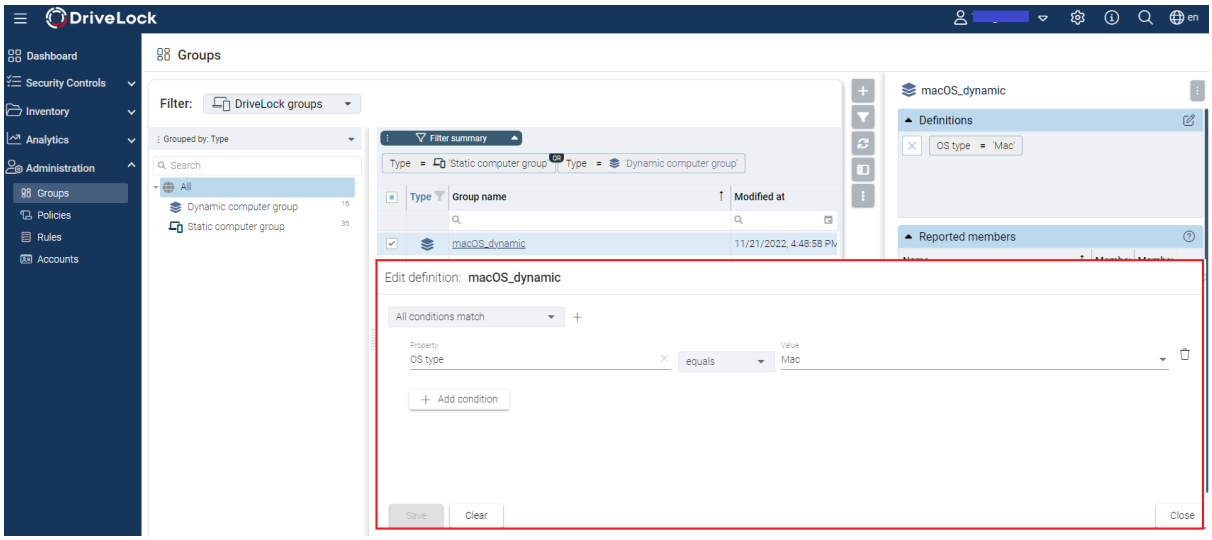
The following DOC views are relevant for macOS Agents:

- **Inventory/Computers**: Filter by **OS type**, for example, to have your macOS Agents grouped by their operating system. Select any macOS Agent to view its details.
- **Inventory/User**: In this view you can see a listing 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.
- **Administration/Groups**: If you have defined a DriveLock group for your macOS Agents, it will be displayed here with information about the respective members and the assigned policies.
- **Analysis/Events**: The events that a macOS Agent sends to the DES are listed in this view.
- **Analysis/Threats**: The **Alerts** tab provides ongoing monitoring and configurable response to safety-related events.

5.1 Creating a DriveLock group in the DOC

We recommend the following approach when working with DriveLock macOS Agents:

1. In DriveLock Operations Center (DOC), start by creating a DriveLock group (static or dynamic) that includes your macOS Agents.
   This makes it easier to assign policies for your macOS Agents at a later stage.
   As a definition, specify 'Mac' as the filter criterion for **Operating system type**.
   In the figure below, the **macOS_dynamic** group is defined with description **All macOS clients** and filter criterion **Operating system type = macOS**.

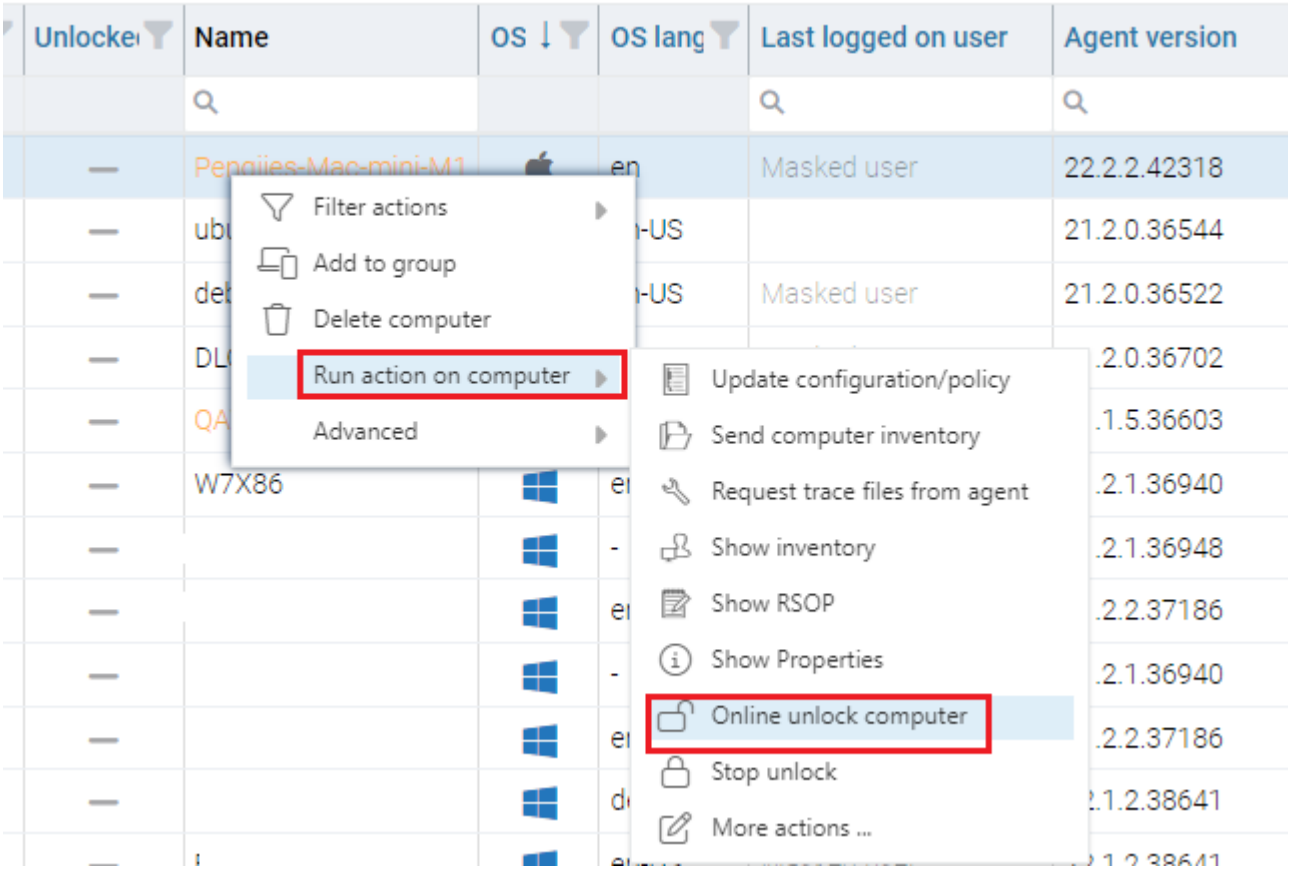


2. For more information about DriveLock groups, see DriveLock Administration auf DriveLock Online Help.
3. If you want to use a different tenant for your DriveLock macOS Agents, you must explicitly select it. You can also find out more about using tenants in DriveLock Administration.
4. Create a new centrally stored policy for your macOS clients, name it accordingly (for example 'macOSpolicy') and start with Global configuration settings.
5. Assign the 'macOS policy' to your DriveLock group. You can also assign to All Computers if you do not want to use a group.

5.2 Temporary unlock from the DOC

It is possible to temporarily unlock macOS Agent drives from DriveLock Operations Center (DOC) using the **Online unlock computer** action.

See the example below.



The temporary unlock ends after the configured time limit. If you specify an absolute time, the temporary unlock will be upheld even if a restart is performed.

The temporary unlock can be stopped with the **Stop unlock** option.

All USB drives can be unlocked at once.

5.3 Display license status in DOC

The macOS Agent supports policy-configured Drivelock licenses for drive control.

The agent activates the components according to the license and reports the correct license status to DriveLock Enterprise Service (DES). You can check this in the computer's details in the DOC.

6 Events

DriveLock events can be viewed in the DriveLock Operations Center (DOC) and the DriveLock Policy Editor. Various filter options are available for the events.

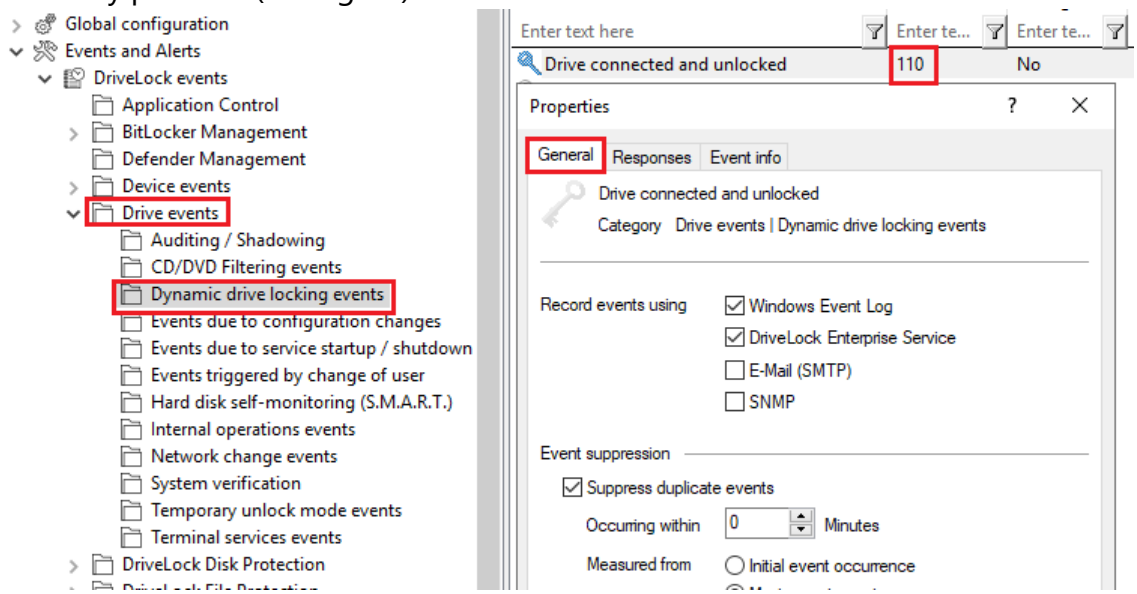
The events important for DriveLock macOs Agents are in the **General events** and **Drive events** categories. See Events for a detailed list.

You can log events in the Windows Event Viewer or on the DriveLock Enterprise Service, but not in SNMP or SMTP.

6.1 Event settings

You can configure events in the Policy Editor. As an example, configure drive event 110, which indicates that a drive is connected to the DriveLock macOS Agent and is not locked.

1. In the **Events and Alerts** node, open the **Events** sub-node. Doubleclick the event in the **Drive events** section. For macOS Agents, only the settings on the **General** tab are currently possible (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.

6.1.1 Event filter definitions

For macOS Agents, you can use event filter definitions for the macOS events that are available.

You can filter

- by filter criteria,
- by computers (with computer names or Drivelock groups)
- and by time range.

Event filter definitions can be used to reduce the number of events in the DOC event view, making it easier to find relevant events.

6.1.1.1 Create event filter definitions

Example: Event 238 (remote control access) - generates a large number of events during a session. To reduce the number and restrict only to certain ones, specify filter criteria with certain parameters.

Please do the following:

1. Right-click the **Event Filter Definitions** sub-node in the **Events and Alerts node** and select **New.**.. from the menu. A list of available events is displayed. Select the event 238.
2. On the **General** tab, check the **Windows Event Log** and **DriveLock Enterprise Service** options.
3. On the **Filter criteria** tab, select the parameters to filter by. By clicking the **Add** button you can select the appropriate criteria and the operators.
   In the example above, one criterion would be the **function name** GetAgentStatus.
   Then the DriveLock Agent will send only the relevant events.

6.2 List of events

The following table contains all events related to macOS that are displayed in the DriveLock Operations Center (DOC). All events below are triggered by DriveLock:

You can find a list of all events DriveLock processes in the Events documentation auf DriveLock Online Help..

The DriveLock macOS Agent reports 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 company 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.

Event ID	Event level (Information, Warning, Error)	Event text	Description
			Device Id: [ID] [ID] (Rev. [rev]) (Serial number [number]) Applied whitelist rule: [rule] Screen state (keyboard [Win]-[L]): [state]
131	Audit	Temporarily unlocked	{Product} Agent was temporarily unlocked by an administrator. Administrator computer: [ComputerName] (unique ID [ComputerGuid]). Administrator account: [UserName] (domain [Domain], SID [SID])
132	Audit	Temporary unlocked cancelled	The temporary unlock mode of the {Product} Agent was canceled by an administrator. Administrator computer: [ComputerName] (unique ID [ComputerGuid]). Administrator account: [UserName] (domain [Domain], SID [SID]
139	Warning	Temporary unlock ended	The temporary unlock mode of the {Product}

Event ID	Event level (Information, Warning, Error)	Event text	Description
			Agent ended because the unlock time elapsed.
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: [Invent-

Event ID	Event level (Information, Warning, Error)	Event text	Description
			ory/Recovery/Events]
192	Warning	{Pre-fixEnterpriseService} not available	No {Pre-fixEnterpriseService} is available because no valid server connection is configured.
199	Warning	Drive temporarily unlocked	Drive types temporarily unlocked by administrative intervention are [DriveType1] [DriveType2] [DriveType3] [DriveType4] [DriveType5] [DriveType6] [DriveType7] [DriveType8] [DriveType9] [DriveType10]
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:	Agent remote control: An

Event ID	Event level (Information, Warning, Error)	Event text	Description
		Internal error	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]
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.

Event ID	Event level (Information, Warning, Error)	Event text	Description
			{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. 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

Event ID	Event level (Information, Warning, Error)	Event text	Description
			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]
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

Event ID	Event level (Information, Warning, Error)	Event text	Description
			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 {PrefixEnterpriseService}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	The integrity of an assigned

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

7 DriveLock configuration tool

The following parameters are available in the command line for the **dlconfig** configuration tool:

```
Usage: ./dlconfig [OPTIONS]
Options:
  -c, --config_cert path    config cert path
  -s, --server serverurl    server url
  -t, --tenant tenantname   tenant name
  -j, --jointoken token     tenant join token
  -p, --setproxy <type>;<proxy>
        Set proxy server to use for downloads and DES communication.
        <type> can be system, none, named or pac with the following meaning:
           system               = use system proxy settings
           none                 = no proxy
           named;<proxy>:<port> = explicit proxy
           pac;<pac url>        = use proxy configuration script
  -x, --setproxyaccount <proxyuser>;<proxypassword>
        Set proxy server credentials.
  -m, --removeproxy         clear all proxy settings
  -d, --debug  off|<0-7>    activate/deactivate logging
  -u, --update              update the configuration
  -a, --status              show status
  -r, --recreatebootdevices re-create boot devices
      --rescanapps          re-create local whitelist hashdb
  -v, --verbose             verbose output
  -V, --version             show version
  -S, --getserver           show server
  -T, --gettenant           show tenant
      --regget value        get registry value
      --regget SOFTWARE/CenterTools/DLStatus/KeepInventoryFiles:dword
      --regset value        set registry value
      --regset SOFTWARE/CenterTools/DLStatus/KeepInventoryFiles:dword=1
      --regdel value        delete registry key or value
      --regcreate value     create registry key
  -h, --help                print this help and exit
```

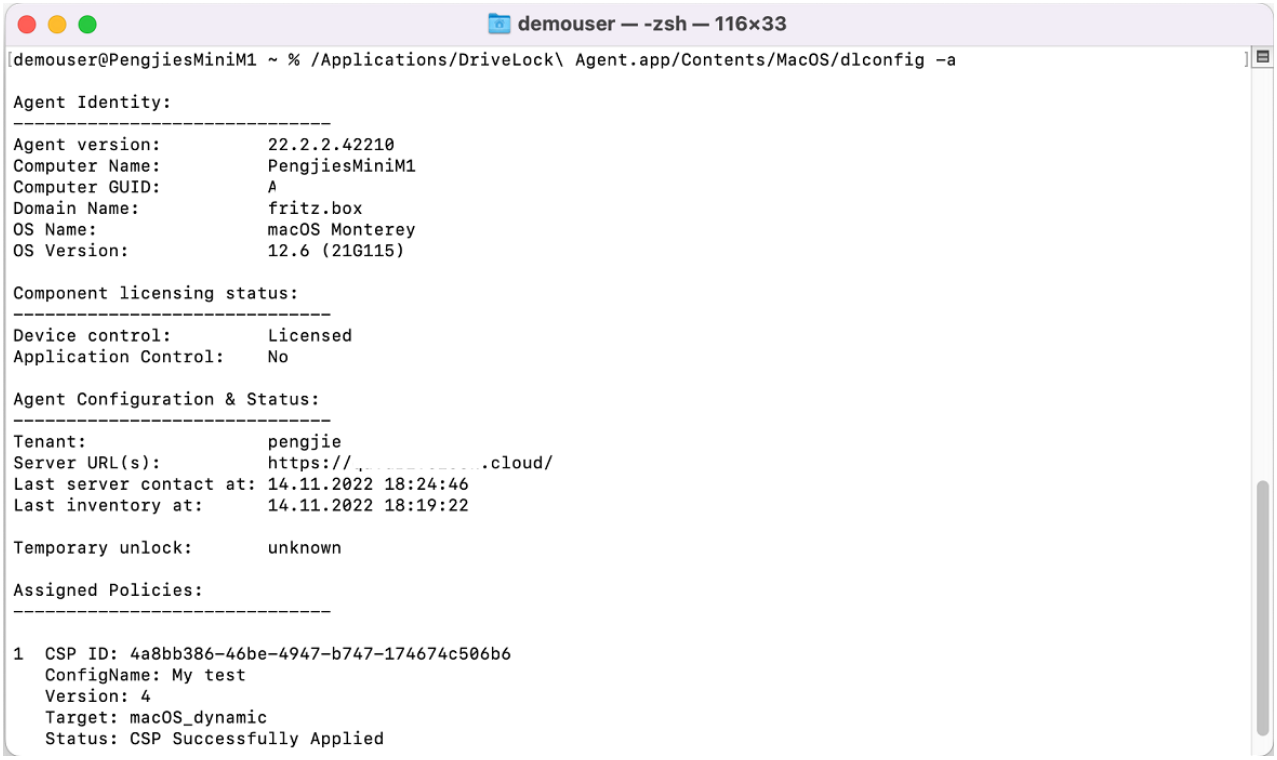
Parameter details:

Parameter	Description
`-s, --server serverurl`	Specifies the DES the macOS client communicates with
`-t, --tenant tenantname`	Specifies the tenant for your macOS Agent
`-j, --jointoken token`	Specifies the join token set during installation

Parameter	Description
`-p, --set-proxy<type>;<proxy>`	Specifies the proxy server to be used for downloads and DES communication. `<type>` can be system, none, named or pac with the following meaning: • `system` = use system proxy settings • `none` = no proxy • `named;<proxy>:<port>` = explicit proxy • `pac;<pac url>` = use proxy configuration script Example: `% sudo ./dlconfig -p "pac;https://www.company.com/proxy.pac"`
`-x, --setproxyaccount <proxy-user>;<proxypassword>`	Sets the credentials for the proxy server.
`-m, --removeproxy`	Deletes all proxy settings.
`-d, --debug off|<0-7>`	Enables or disables tracing to log files located in the installation directory in the log subfolder. (Larger number means more detailed tracing. Standard is 4 - info. The value 0 or off disables tracing).
`-u, --update`	Updates your configuration, e.g. if you have made changes to your policies The macOS Agent then connects to the DES immediately and loads the changes

Parameter	Description
`-a, --status`	Shows the current status of the macOS client and informs when, for example, the DES was last contacted, which policies are assigned or which DriveLock modules are licensed (see figure below)
`-r, --recreatebootdevices`	Creates a new list of currently connected USB devices that should always be allowed at boot time

To view the status of the macOS Agent, use the `-a` option. Here is an example:



8 macOS tools

The following command line tools are available for macOS.

1. To check the status of the process:
   `% sudo launchctl list 6GZR4TWXD2.com.drivelock.agent.extension`: Allows you to view the details of the DriveLock agent system extension history.
2. To display all system extensions:
   `% sudo systemextensionsctl list`: Displays all system extensions that are installed on the corresponding client.

Copyright