DriveLock Administration

Documentation 2022.2

DriveLock SE 2023

Table of Contents

1 Important note on this documentation

This documentation replaces the former DriveLock Admin Guide. You can find an introduction to the DriveLock Operations Center (DOC), and information on working with the DriveLock Policy Editor and the DriveLock Management Console (DMC) here.

We also offer stand-alone documentation for the following modules:

- Application Control,
- DriveLock Encryption (includes Disk Protection, File Protection, BitLocker Management, BitLocker To Go, Encryption 2-Go and DriveLock PBA),
- Defender Management,
- DOC Companion,
- DriveLock Events,
- Linux Agents,
- macOS Agents,
- Security Awareness and
- Vulnerability Management.

Furthermore, there is an installation manual for DriveLock 'On-Premise'.

We are continuously revising, restructuring and updating all of our documentation, possibly independently of our product releases.

Note: For customers of the DriveLock Managed Security Services, please note that there is a different set of information available, for example on installing DriveLock.

2 Working with DriveLock

DriveLock is a modern security platform designed to keep you safeguarded against all kinds of cyber attacks and loss of valuable data. The DriveLock Managed Security Services provide cloud hosting for your entire DriveLock solution, managed by our security experts. No need for your own infrastructure or third-party software. As an alternative, you can manage your own infrastructure on premises. You will find important information about the different options here.

You can manage your own security infrastructure with the help of the following consoles:

- DriveLock Operations Center (DOC)
- DriveLock Management Console (DMC)
- DriveLock Policy Editor

Note: Please be aware that you will still need the DMC (Policy Editor) for some functionalities, whereas others are fully available in the DOC.

2.1 Licensing

DriveLock offers various licensing models with different subscription periods. A basic subscription always includes the respective licensed main module with various basic modules that are required to operate DriveLock. These include the DriveLock Operations Center (DOC), DriveLock Agent (which is distributed to client computers), DriveLock Enterprise Service (DES) with associated databases, and inventory and event viewing capabilities. Combination modules can be added to some main modules (for example Encryption 2-Go to Device Control, see table below).

The following modules are currently available:

Main module	Combination module	Functionality
Device Control		Drive and Device Control
Device Control	Encryption-2-Go	Control and encryption of external media

Main module	Combination module	Functionality
Device Control	BitLocker To Go	Control and encrypt external media with BitLocker To Go
BitLocker Management		Management of Microsoft BitLocker functionality
BitLocker Management	DriveLock PBA for BitLocker	Pre-boot authentication management
Application Control		Control of applications with the help of whitelists or blacklists
Application Control	Application Behavior Control	Control of application behavior (included in the Application Control module, but separately configurable)
Disk Protection		Hard disk encryption
File Protection		Encryption of files and folders
Security Awareness		Integration of security awareness campaigns with interactive training, learning content and videos
Defender Management		Integration and management of Microsoft Defender functionality
Vulnerability Management		Risk-based identification of vulnerabilities

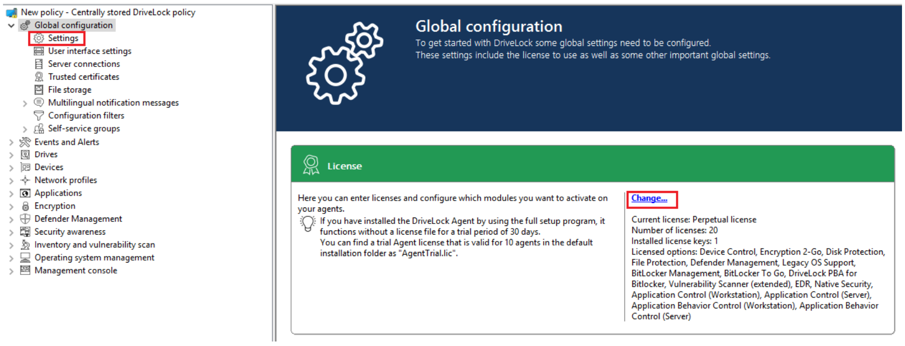
Main module	Combination module	Functionality
Security Configuration Management		Security management using the native security settings

Note: Formerly available as an individual license, the Risk & Compliance (EDR) module has been part of DriveLock's base functionality since version 2022.2. It is only needed individually if you want to work with MITRE Attack rules and Application Control. In this case, please contact the DriveLock Support Team.

Once you have performed the basic DriveLock installation, DriveLock policies distribute the licenses to the agents and DES verifies them. The license status is displayed in the DriveLock Operations Center (DOC).

2.1.1 Enter licenses in policies

If you have installed a DriveLock Enterprise Service (DES), you should transfer the license information directly to it. Certain server functions, for example downloading the Security Awareness Content AddOn, can only be activated if a valid license is present on the DES.



Global configuration

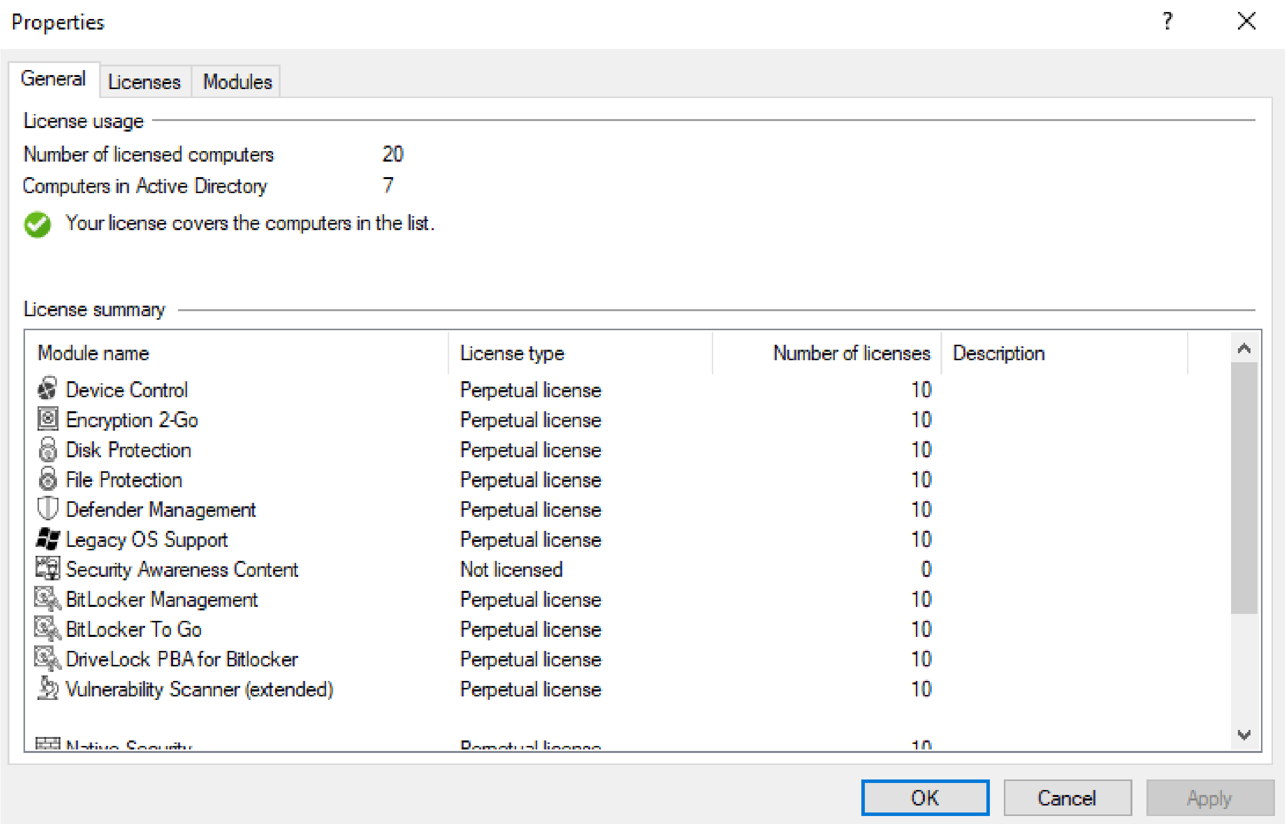
To get started with DriveLock some global settings need to be configured.
These settings include the license to use as well as some other important global settings.

Here you can enter licenses and configure which modules you want to activate on your agents.

If you have installed the DriveLock Agent by using the full setup program, it functions without a license file for a trial period of 30 days.
You can find a trial Agent license that is valid for 10 agents in the default installation folder as "AgentTrial.lic".

Current license: Perpetual license
Number of licenses: 20
Installed license keys: 1
Licensed options: Device Control, Encryption 2-Go, Disk Protection, File Protection, Defender Management, Legacy OS Support, BitLocker Management, BitLocker To Go, DriveLock PBA for Bitlocker, Vulnerability Scanner (extended), EDR, Native Security, Application Control (Workstation), Application Control (Server), Application Behavior Control (Workstation), Application Behavior Control (Server)

Click **Change...** to open the license dialog.



License usage

Number of licensed computers 20
Computers in Active Directory 7

✓ Your license covers the computers in the list.

License summary

Module name	License type	Number of licenses	Description
Device Control	Perpetual license	10	
Encryption 2-Go	Perpetual license	10	
Disk Protection	Perpetual license	10	
File Protection	Perpetual license	10	
Defender Management	Perpetual license	10	
Legacy OS Support	Perpetual license	10	
Security Awareness Content	Not licensed	0	
BitLocker Management	Perpetual license	10	
BitLocker To Go	Perpetual license	10	
DriveLock PBA for Bitlocker	Perpetual license	10	
Vulnerability Scanner (extended)	Perpetual license	10	
Native Security	Perpetual license	10	

The **General** tab displays the license status of each module.

On the **Licenses** tab, you can add your license file or license key, or remove expired or trial licenses if necessary.

Follow the license activation steps in the wizard.

The DriveLock license can be activated either online or manually by calling the DriveLock Activation Center. For online activation, select **Online** . If specifying a proxy server is necessary for your Internet connection, click **Proxy** and enter the server name, a user and the appropriate password.

The license is activated by connecting to the DriveLock activation server. This usually takes only a few seconds.

Instructions for telephone activation:

1. To avoid discrepancies, please make sure that the computer you use for activation has a current time and the correct time zone.
2. The activation code is valid only for a certain period of time. You must enter the activation code within one hour, otherwise you will have to request a new activation code. If this happens, click Cancel and start the Activation Wizard again.

Note: After successful activation, we recommend transferring the licenses to DriveLock Enterprise Service. At this point, specify the server name where your DriveLock Enterprise Service is installed. If you do not specify a name, the transfer process will be skipped.

To view the contents of a license, highlight the desired license and click **Properties...** .

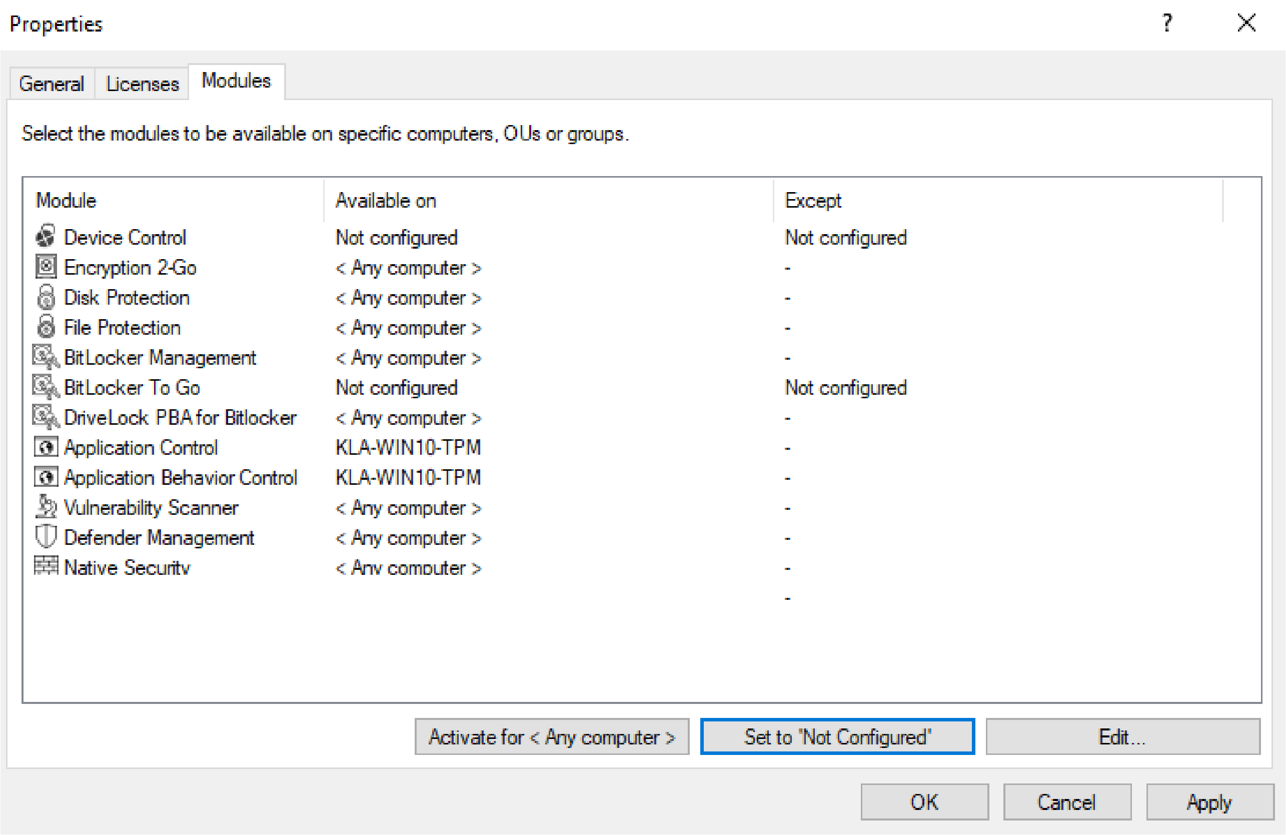
On the **Modules** tab you can configure which module should be active on which agents.

Based on this information you can...

- avoid using a specific module on too many DriveLock agents (only active modules "consume" a license)
- avoid initializing modules on an agent that are not needed there.

If you set modules to the value not configured, the settings from another policy are used. This means that you can configure different modules in different policies than just the policy where you enter the license.

Note: The total number of licenses required is determined based on agent feedback. You will be alerted if you do not have enough licenses. On terminal servers, user licenses are counted separately. In Security Awareness, the number of licenses is determined by the users running campaigns.



Select the modules to be available on specific computers, OUs or groups.

Module	Available on	Except
Device Control	Not configured	Not configured
Encryption 2-Go	< Any computer >	-
Disk Protection	< Any computer >	-
File Protection	< Any computer >	-
BitLocker Management	< Any computer >	-
BitLocker To Go	Not configured	Not configured
DriveLock PBA for Bitlocker	< Any computer >	-
Application Control	KLA-WIN10-TPM	-
Application Behavior Control	KLA-WIN10-TPM	-
Vulnerability Scanner	< Any computer >	-
Defender Management	< Any computer >	-
Native Security	< Any computer >	-
		-

2.1.2 Licenses in the DriveLock Operations Center (DOC)

The **Licenses in use** tab shows a summary of how your licenses are assigned and used. Please note that computer and user licenses are displayed separately. This is primarily important when using terminal servers.

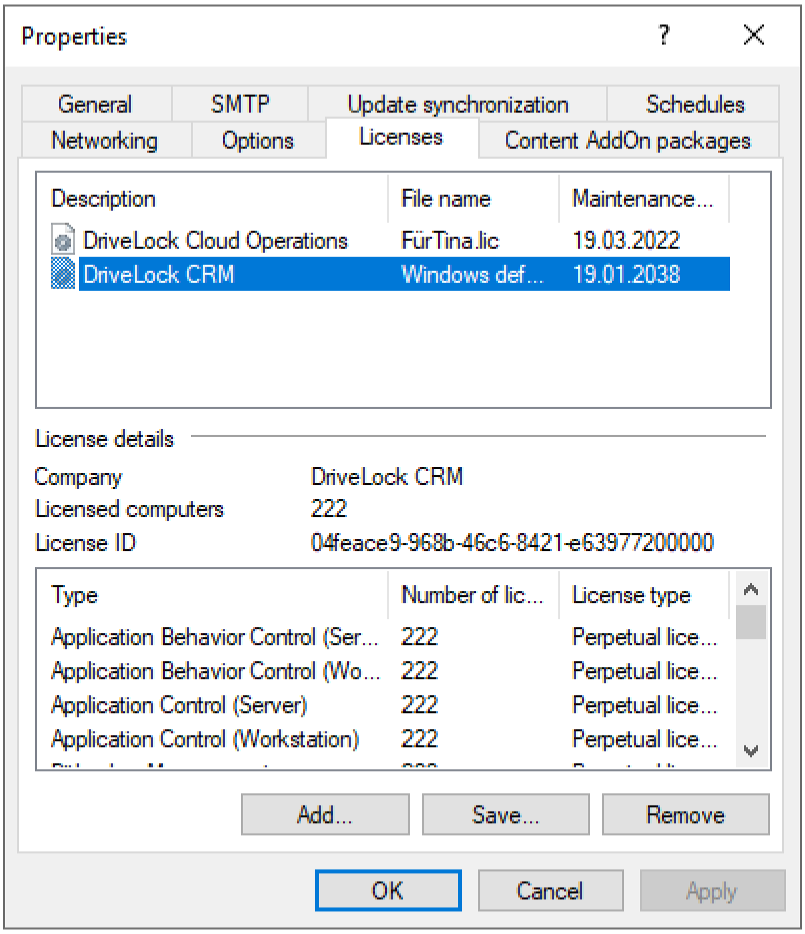
The **Licenses** tab shows you which DriveLock modules are licensed, what type of license is involved, and when the maintenance expires.

If you have any questions about licenses, please contact your DriveLock sales representative or the DriveLock Managed Services team.

2.1.3 Licenses in the DriveLock Enterprise Service properties

When you create a new DriveLock configuration and import a license file, you can transfer it to your DriveLock Enterprise Service. This activates additional functions for various areas (e.g. Security Awareness Content AddOn, hard disk encryption) in the DriveLock Enterprise Service.

In the DriveLock Enterprise Service Properties window, you can view the saved licenses and delete licenses that are no longer needed. To do this, select the **Licenses** tab:



Description	File name	Maintenance...
DriveLock Cloud Operations	FürTina.lic	19.03.2022
DriveLock CRM	Windows def...	19.01.2038

License details

Company	DriveLock CRM
Licensed computers	222
License ID	04feace9-968b-46c6-8421-e63977200000

Type	Number of lic...	License type
Application Behavior Control (Ser...	222	Perpetual lice...
Application Behavior Control (Wo...	222	Perpetual lice...
Application Control (Server)	222	Perpetual lice...
Application Control (Workstation)	222	Perpetual lice...

Once you select a license in the upper pane, the license details are displayed below.

Select a license and click Remove to delete the selected license from the DriveLock database.

3 DriveLock Operations Center (DOC)

The DOC is a modern browser based user interface for the DriveLock Zero Trust Platform. It can be used by DriveLock Managed Security Services customers who have chosen our cloud-based security solution, and by customers who use and manage DriveLock 'on-premise'. Here are some of the differences between the two.

The DOC gives you an overview of the current status of all computers in your company being managed with DriveLock. The languages we support are English and German, you can switch languages by clicking the language of your choice.

All the features that were previously available in the DriveLock Control Center (DCC) are now available in the DOC: inventory, creating event and statistics reports and forensic analysis, performing maintenance tasks or installing DriveLock Agents.

The DOC Companion can be used to access the policy editor (until version 2021.2, this was only available via the installed DriveLock Management Console). This allows you to edit and create policies, and access settings that are not yet available in DOC.

3.1 General notes

DriveLock Managed Security Services and DriveLock 'On-Prem' are using a nearly identical DOC user interface.

However, there are some functional differences:

1. Login to DOC
    - Managed Services: Login via e-mail activation or via SAML
    - On-Prem: Login as AD user or via membership in an AD group

    > Note: The first logged-in user becomes an administrator, all others become users.

2. Deploy the DriveLock Agent
    - Managed Services: Download via WebInstaller / Agent
    - On-Prem: Run push installation
3. Configure the DriveLock Agent
    - Managed Services: The agent cannot be configured remotely
    - On-Prem: The agent can be configured (client, policy, etc.)

3.2 DriveLock Operations Center 'on-premise'

3.2.1 Signing in to the DOC

There are two ways to open the DOC:

The **DriveLock Operations Center web link** in the Start menu opens the DOC web-based user interface right away with the correct URL in your browser. However, you can also open the DOC directly from your browser by manually entering the URL **https://DES-SERVER:4568** in the browser.

Warning: The DOC can only be opened in a current version of Google Chrome, Microsoft Edge, Mozilla Firefox or Safari. Older web browsers are not supported!

Note: Please also note the instructions on the use of certificates for the individual browsers.

3.2.2 Notes on using SSL certificates

DriveLock uses SSL certificates for communication with the DriveLock Operations Center (DOC). You can specify them when installing DriveLock Enterprise Service (DES) or, alternatively, create a self-signed certificate. For more information about certificates, see the Installation Guide on Drivelock Online Help.

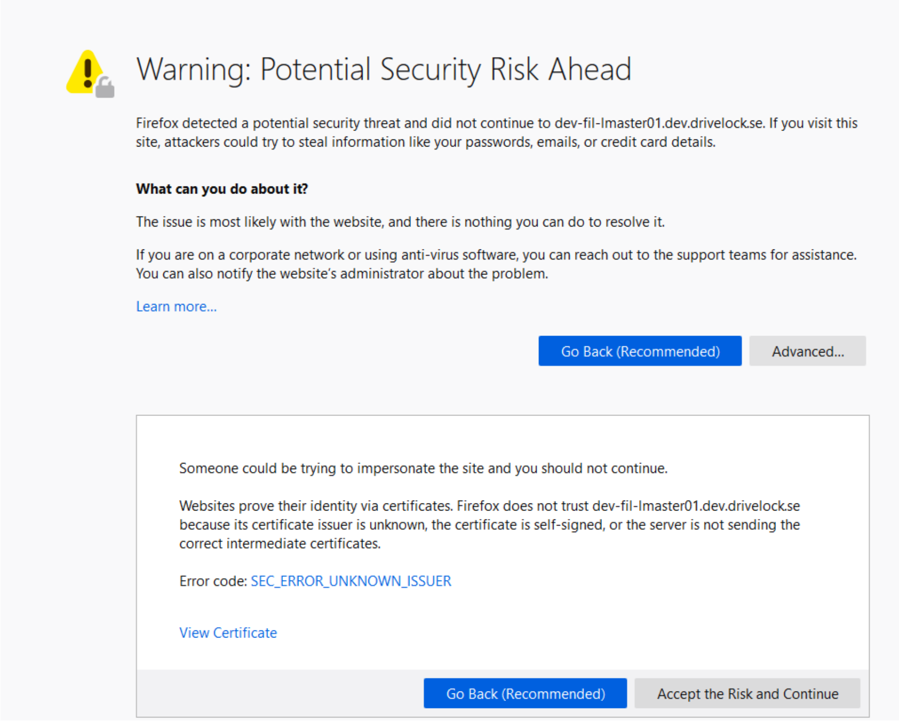
Note: We recommend that you get a certificate for the DES from a recognized certificate authority (CA)!

If you are using a self-signed certificate, different warnings will appear when opening the DOC, depending on the browser, because from the browser's perspective the certificate is not trusted.

In the examples below the name of the DES is dlserver.dlse.local.

If you are using Mozilla Firefox, the following applies:

Click **Accept the Risk and Continue** to accept the certificate. There is no need to show the certificate details or to import the certificate. Firefox adds only one security exception for this web page. Nothing else needs to be done.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to dev-fil-lmaster01.dev.drivelock.se. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Someone could be trying to impersonate the site and you should not continue.

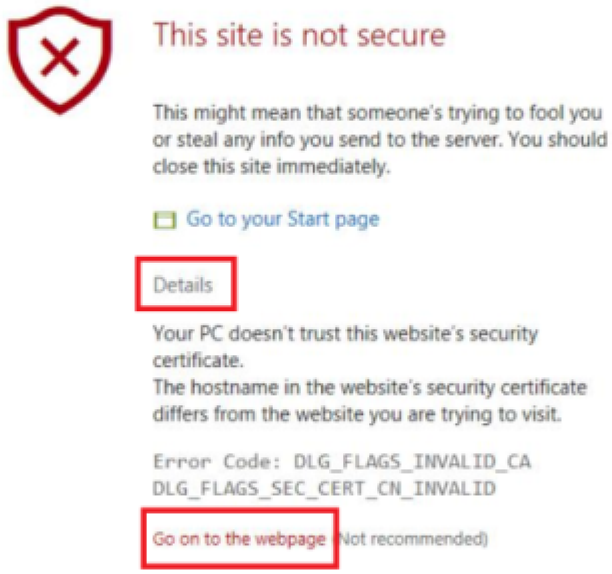
Websites prove their identity via certificates. Firefox does not trust dev-fil-lmaster01.dev.drivelock.se because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

For Google Chrome and Microsoft Edge, the following applies:

With both browsers, you need to add the certificate to the certificate store so that you don't get a warning every time you launch the DOC.

- Microsoft Edge:



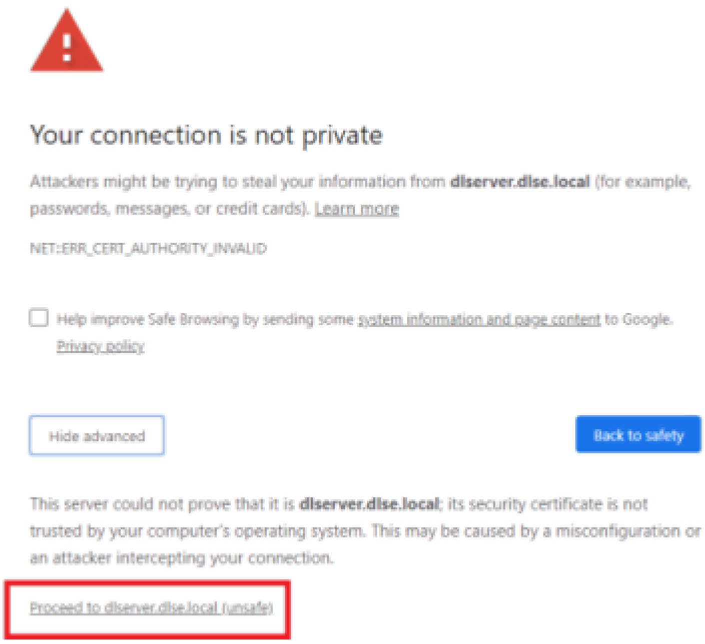
This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

- Google Chrome



Your connection is not private

Attackers might be trying to steal your information from **dlserver.dlse.local** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

☐ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

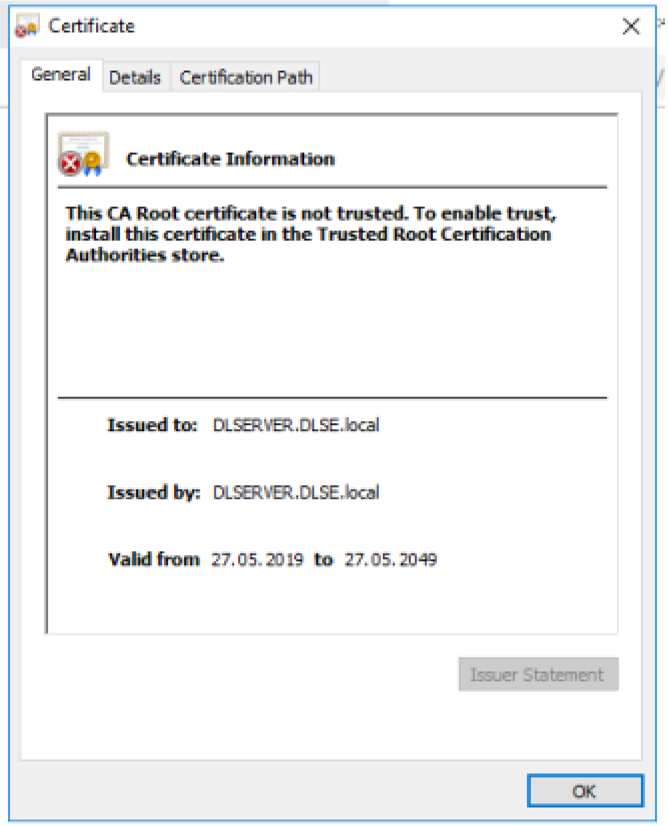
This server could not prove that it is **dlserver.dlse.local**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to dlserver.dlse.local (unsafe)

3.2.2.1 Importing certificates

Please do the following:

1. For both browsers, accept the warning and open the certificate.
2. You can view the certificate details and import the certificate to the local certificate store using the Certificate Import Wizard.



Certificate

General | Details | Certification Path

Certificate Information

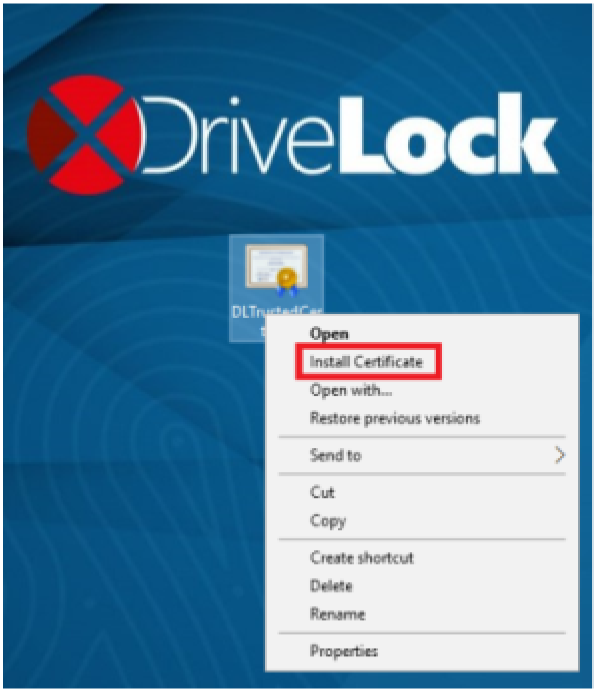
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: DLSERVER.DLSE.local

Issued by: DLSERVER.DLSE.local

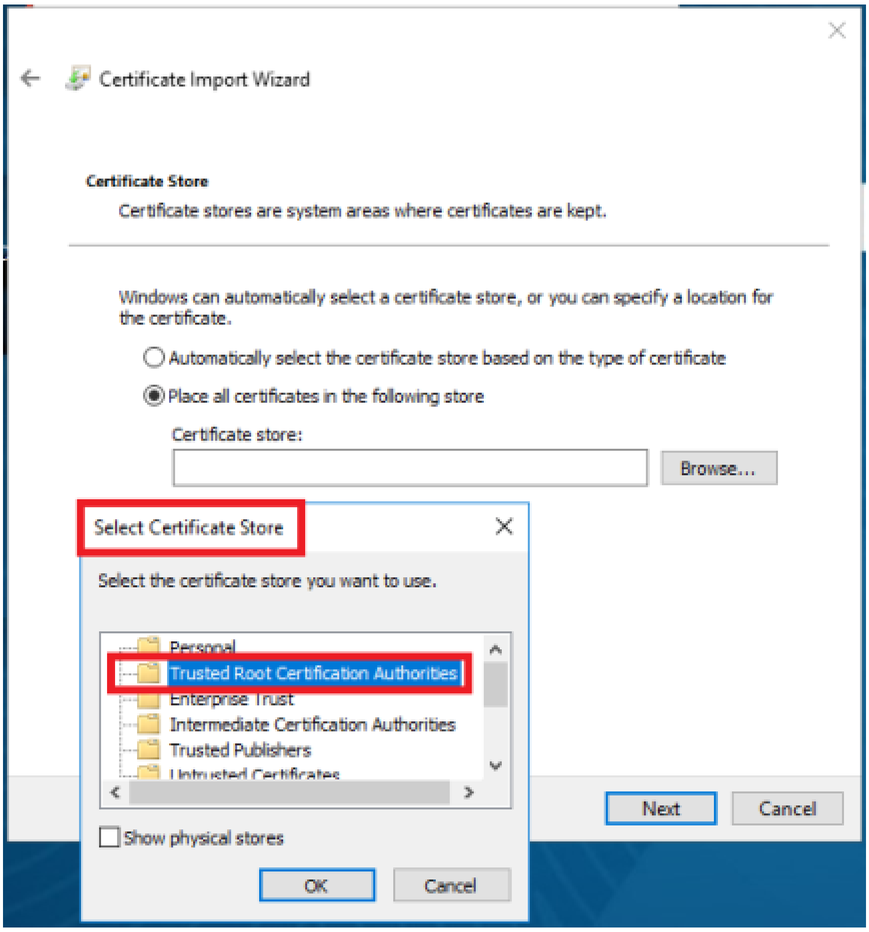
Valid from 27.05.2019 to 27.05.2049

3. Store the certificate in a directory on your computer.
4. Open the certificate's context menu and click **Install Certificate**.



5. The Certificate Import Wizard opens. On the first page, keep the default X.509.
6. On the next page, select Local computer.

7. On the third page, select **Trusted Root Certification Authority** as the certificate store:



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

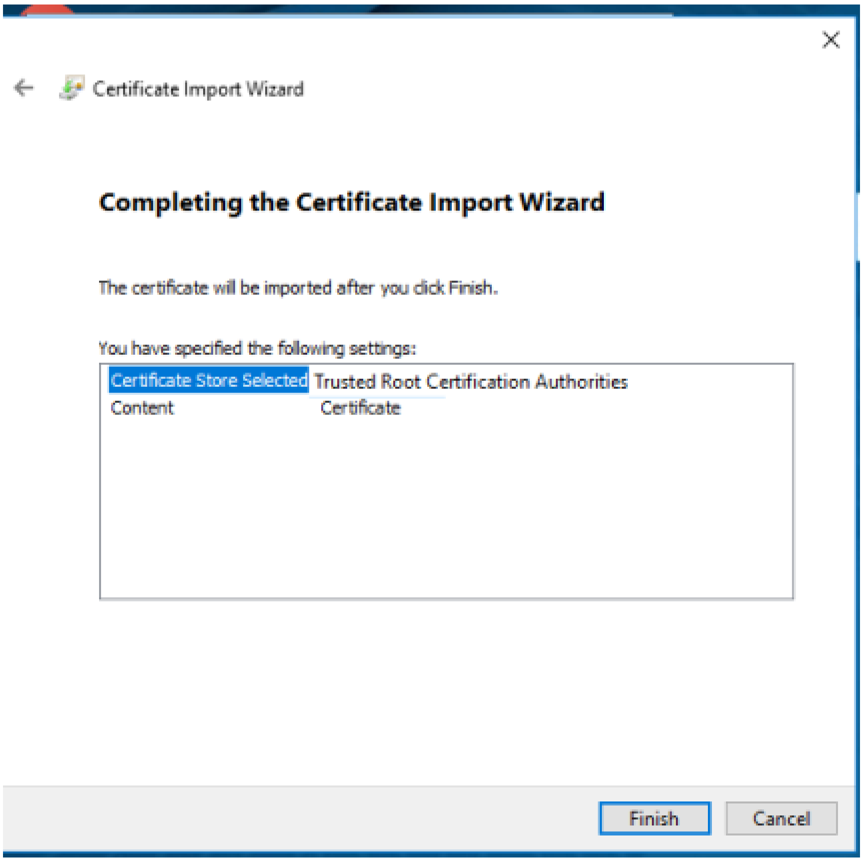
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

8. In the next dialog, click **Finish**.



Certificate Import Wizard

Completing the Certificate Import Wizard

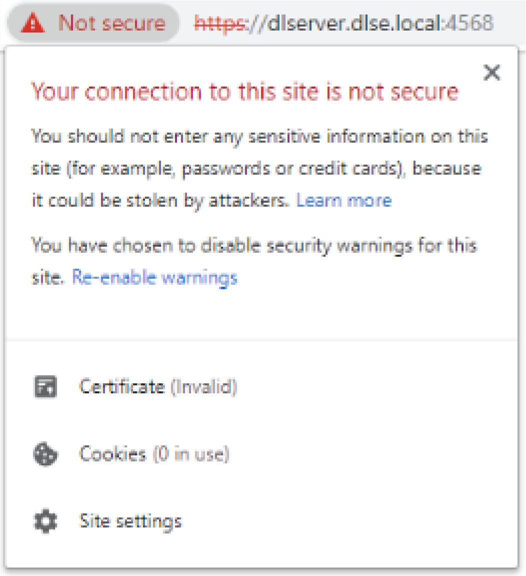
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Trusted Root Certification Authorities
Content	Certificate

9. Now the certificate is registered and the next time you open the DOC, you will be taken directly to the logon screen without any error message.

Warning: Note, however, that even then the certificate will be considered not secure by the browser and the following warning will still appear (in the example below for Google Chrome):



Not secure ~~https~~://dlserver.dlse.local:4568

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

3.3 Security settings in DOC

The DriveLock Enterprise Service generates a unique join token for each tenant, which must be specified during the installation of an agent so that the agent can be added to the tenant.

Note: Existing agents do not need this join token, only new agent installations will be checked.

The join token is automatically passed to the MSI when the agent is installed from the DOC.

f you run the DriveLock Agent setup manually, the join token must be passed to the MSI as a parameter:

`USEJOINTOKEN=1 JOINTOKEN=<Join Token>`, for example.

```
msiexec /I "d:\DriveLock Agent X64.msi" /qb USESERVERCONFIG=1
CONFIGSERVER=https://dlserver.dlse.local:6067 USEJOINTOKEN=1
JOINTOKEN=c93a2959-0c10-444b-b700-6f8ec3630ad2
```

If the token is missing on the agent or an incorrect one is specified, the DriveLock Agent can be installed, but it will be rejected by the DriveLock Enterprise Service. In this case, you can use the `driveLock -SetJoinToken <Join Token>` command to set the join token afterwards. Then you need to restart the DriveLock service or call the `driveLock -updateconfig` command.

If the registration fails, an error message will be displayed in the tray icon on the agent. DriveLock Enterprise Service generates a corresponding event with the reason for rejecting the agent.

ID	Type	Meaning
2105	Success audit	An agent successfully registered
2106	Failure audit	The agent tried to register with the invalid join token '%1'.
2107	Failure audit	The agent tried to update its agent ID to the new value '%1'. This is not permitted. Please reset the agent registration via DOC if this change is intended

2108	Failure audit	Rejected access to DES for agent. The agent sent the not existing agent ID '%1'.
2109	Failure audit	Rejected access to DES for agent. The agent sent the agent ID '%1' which does not belong to it. The conflicting data (name/ID) is: %2

3.3.1 Adding new agents securely

In the **Deployment** view of the **Configuration** menu in the DOC, on the **Security settings** tab, you can specify that a DriveLock Agent can only be added to a tenant if it has a join token (Join ID).

You can enable or disable the option **Agents must present a join token to be added to the list of managed computers** for each tenant. By default, the option is disabled.

The DriveLock Enterprise Service (DES) can identify each individual agent and thus ensure that the data coming from an agent was actually sent by that agent and not another computer. To make sure this check is performed, you must enable the **Verify agent identity** security setting in the DOC.

Note: All DriveLock Agents must be at least version 2021.2 to be able to use this option. If older agents are still present, the setting will remain grayed out and you can view a list of computers that have not yet been updated.

You can also reset the agent identity by selecting the **Advanced** menu item in the context menus of a managed computer and then by clicking **Reset agent identity**. This may be required related to the reinstallation of a golden image.

3.3.1.1 Scenarios for using join tokens

- **Reinstalling an existing computer**

  A computer is reinstalled from scratch. Note that the computer object already exists in the DriveLock Enterprise Service (DES). The DriveLock Agent gets installed after installing the operating system while specifying the join token. Here, you have to manually reset the join token in the DOC. To do so, open the context menu of the computer. If you do not reset the join token, all SOAP calls from the agent will fail, because the new installation of the MSI generates a new join token, which cannot be registered since a join token is already known. An error message indicating that the connection to the DES cannot be established now appears on the agent.

- **Reinstalling the agent**

  If you only reinstall the DriveLock Agent without deleting the DriveLock entries from the registry, no further action is required. If the registry entries have also been deleted, you can proceed in the same way as explained in the section "Reinstalling an existing computer" above.

- **Renaming a computer**

  In this case, there is nothing to consider either, because the DriveLock Agent recognizes that the computer has been renamed and notifies the DriveLock Enterprise Service accordingly. The DriveLock Service may temporarily stop communicating with the agent until it learns that the computer has been renamed.

- **Updating an agent from an older version**

  Again, no need to do anything here. A join token is not required because the computer object already exists.

3.3.2 DriveLock in virtualization environments

If you have a VDI (Virtual Disk Image) environment in your company or are working with disk images where a DriveLock Agent is pre-installed, the clone images (also referred to as golden images) will need to be introduced to the DriveLock Enterprise Service (DES) as such.

Please do the following:

In the DOC, open the **Computer** view. Select your golden image there and open the configuration of this computer.

Enable the **Computer is used as an image for other computers** setting. This will allow DriveLock to identify the computers that are repeatedly recreated with the same name, and the entire history will be saved.

In the computer overview, you can show the columns **Image for other computers** and **Created from** to get an overview of all the clone images that exist and the computers that were created from them.

Note: In case you have to completely reinstall a golden image and the **Verify agent identity** option is enabled in the DOC security settings, make sure to reset the agent identity of this computer in the DOC first. This is important so that the cloned images can connect to the DES on the first boot.

3.4 Azure AD integration

Organizations managing their infrastructure and user permissions centrally through the Microsoft Azure cloud platform and Azure Active Directory can synchronize the groups they have there into DriveLock and use them for access permissions and assignment of DriveLock policies in the same manner as they could previously do with a local Active Directory.

DriveLock treats computer groups from AAD like static groups, except that they are automatically maintained through synchronization rather than manually by the user.

It helps you achieve the following goals:

1. **Assign policies to computer groups**

   Computer groups connected to an AAD are used as the target of policy assignments. They are available as static computer groups in DriveLock. These groups need to be readable by DOC and DriveLock Management Console (DMC).

2. **Use computer groups in policies**

   Within policies, you can use AAD groups in the same way as you use static groups. Rules for individual computers need to be created using the computer name.

3. **Use users and user groups in policies**

   The AAD account name is used for users instead of the SID as before. This is an address such as "user@mydomain.onmicrosoft.com".
   AAD user groups may also be selected within the DMC as a DriveLock user group. The available user groups and their members are entered in the same way as computer groups by means of a synchronization mechanism.

4. **Log in on a role and permission basis using Azure AD user groups**

   You can select an AAD user group for role assignments. When a user logs in to the DOC via SAML, the DES determines the AAD user groups that the user is a member of. The remaining logic is no different from standard AD.

5. **Self-service groups**

   Azure AD user and computer groups can be used as self-service groups.

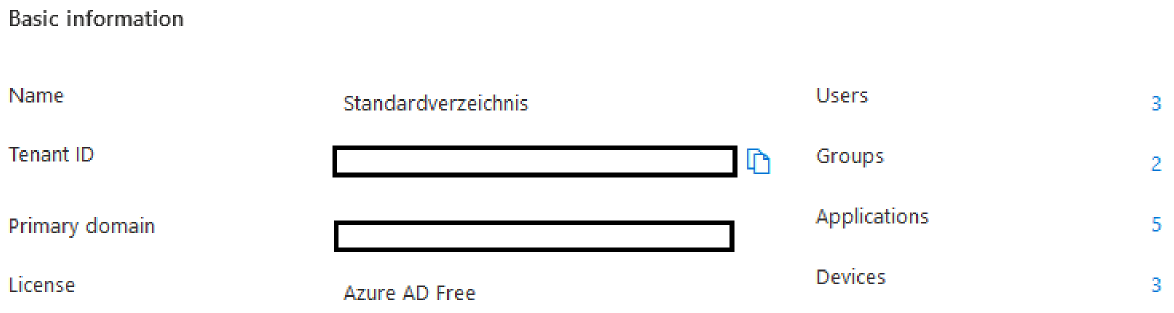
3.4.1 Settings for Azure AD

By integrating with Azure AD, groups and their members are synchronized from Azure AD to DriveLock. The first step to make this work is to complete some configuration steps in

Azure AD, and then paste the resulting data into the appropriate text fields in DriveLock Operations Center (DOC).

1. **Settings in "Overview"**

   You need the following data from the Azure AD Overview for synchronization: Tenant ID and Primary domain.



Basic information

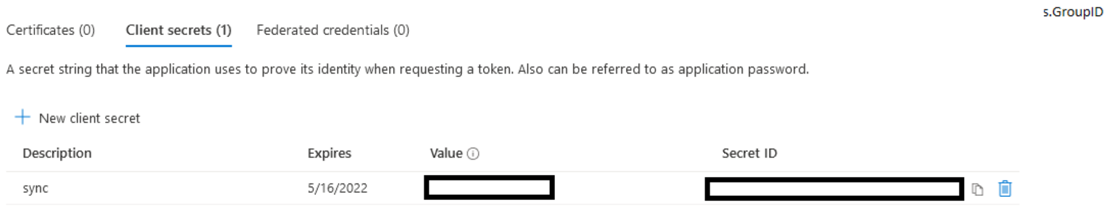
Name	Standardverzeichnis	Users	3
Tenant ID	[redacted]	Groups	2
Primary domain	[redacted]	Applications	5
License	Azure AD Free	Devices	3

2. **Registering and configuring the application**

   Create a new application in the "App registrations" section and note the "Application ID (Client ID)" from the overview page.

   - **Generating a client secret**

     Create a new client secret in the Certificates & Client secrets section. You need the complete content from the "Value" column.



s.GroupID

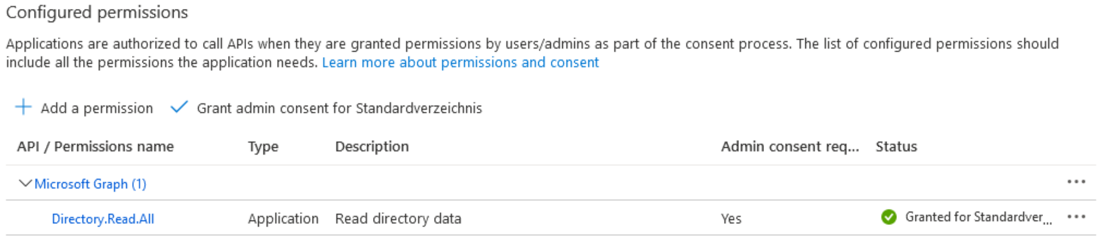
Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID
sync	5/16/2022	[redacted]	[redacted]

   - **Setting permissions**

     In the "API permissions" section, assign the permissions as shown in the figure:



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
∨ Microsoft Graph (1)				···
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Standardver... ···

SAML configuration

You can optionally link a SAML configuration to the Azure AD configuration. This enables logging in with Azure AD users who have been assigned permissions because they belong to an Azure AD group.

3.5 DriveLock in Active Directory, Azure AD or workgroups

DriveLock is basically designed to use Active Directory, as it follows the AD permissions concept and structure. For example, drives can be shared with specific user groups or policies can be assigned to OUs.

DriveLock without Active Directory

If you want to use DriveLock without Active Directory, you can still use DriveLock groups and Azure AD integration is also available. You can use DriveLock computer groups or Azure AD computer groups wherever you can use AD computer groups or OUs.

DriveLock and Azure AD user groups, on the other hand, cannot be used everywhere.

Please note the following:

- A DriveLock on-premises installation uses the local users of the computer where the DES is installed for managing the environment.
- If you are a DriveLock Managed Services user, you can use an Azure AD integration for logging in to the DOC or you can create your own users. Here, you can also assign permissions to Azure-AD groups.
- If the MQTT connection between the agent and DES is disabled, you need to have name resolution (NETBIOS/FQDN Name) working in order to access the clients for helpdesk activities.

3.6 Groups

3.6.1 Creating DriveLock groups

There are two different DriveLock groups:

Static computer groups are defined by manually adding computers, groups, or organizational units from Active Directory (AD), from individual computers (which are added individually by name), or even from existing DriveLock groups (also Azure AD groups).

Dynamic computer groups are defined from the results of queries (filter criteria), for example, queries based on operating system version, IP range, Windows version, and more. A group membership of a DriveLock Agent is determined in the following way: First, the filter criteria are stored in a database. The criteria are then transmitted to the agent computers, where they are evaluated, and then feedback is provided on the respective group membership. After updating the configuration, the individual members are displayed in the properties of the dynamic group (Current members tab).

You can create DriveLock groups by selecting the **Groups** item in the **Configuration** menu in the **DriveLock Operations Center**. The **+** icon allows you to add either static and dynamic DriveLock groups. You can also create a copy of an already existing group.

Azure AD groups are synchronized to DriveLock when the Azure AD integration is triggered. Click here to learn more about the settings you need for this.

3.6.2 Static computer group

To create a static computer group, proceed as follows:

1. Click **+ Add group** and select **Create static group**.
2. Specify a name for the group and optionally add a description.
3. Your group appears in the list. Click on the name to edit the group.
4. Under **Definitions** you now have the option to add static group members. Click **+ Add group member**.
   Here you have the following choices:
   - AD Computer / AD Group: Select individual computers or groups directly from AD and add them to your static group.
   - OU container: select the computers from an AD organizational unit (OU).
   - Computer name: add individual computers by name to the group.
   - DriveLock group: You can also add a previously created DriveLock group (dynamic or static).
   - Azure AD group: If you have already integrated Azure AD groups into DriveLock, you can also select them here.

   Note: Please note that you cannot use wildcards with static group definitions.

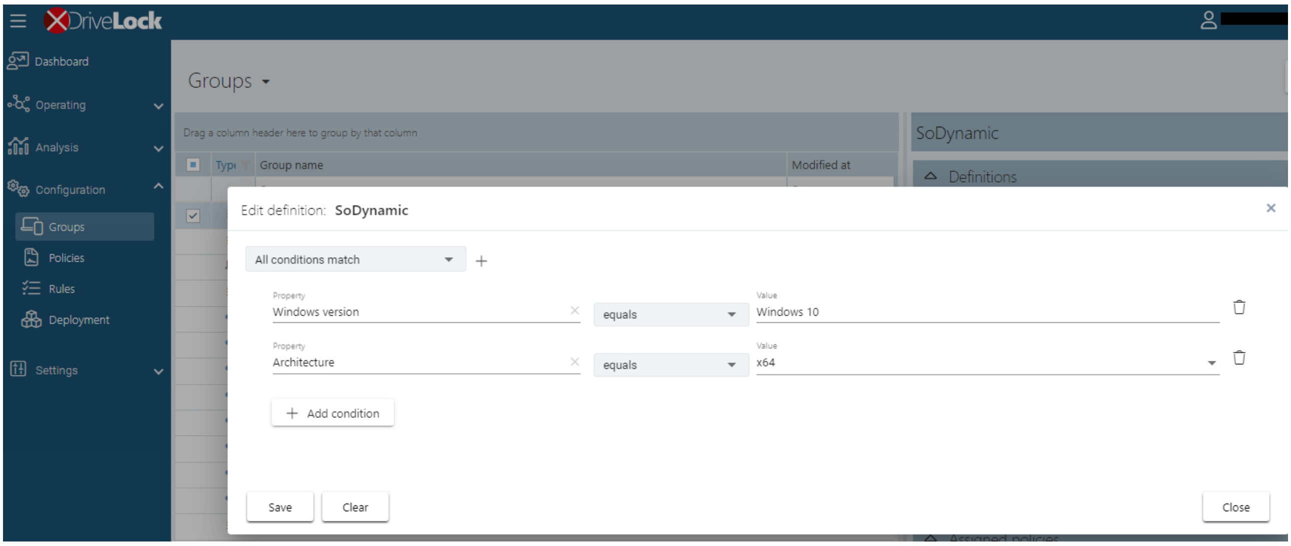
5. After you update the configuration, a list of computers that belong to your static group now appears on the **Current members** tab. In the example these are the computers DLCLIENT01 and DLCLIENT04. In the **Identified by** column you can see how the group membership was determined. If the groups were added via the DriveLock Management Console, Server is entered in the column.
   As soon as the client reports its group membership back to the DES, the column entry is Client.

   See Using groups in policies for information on the **Policies** and **Assignments** tabs.

3.6.3 Dynamic computer group

To create a dynamic computer group, proceed as follows:

1. Click **+ Add group** and select **Create dynamic group**.
2. Specify a name for the group and optionally add a description.
3. The **Edit definition** dialog opens. Here you select the filter criteria you want to apply to your group. For example, you can select the Windows version (Windows 10 as value) and then the architecture. The operator selected is "equal" in this example. However, in other cases you can select from a list of different operators.



Edit definition: SoDynamic

All conditions match

Property: Windows version | equals | Value: Windows 10

Property: Architecture | equals | Value: x64

Now you can use the created dynamic group in policy configuration and assignment.

3.6.3.1 Filter criteria for dynamic groups (DOC)

Below please find a description of the filter criteria (properties) that you can use to define dynamic groups.

Filter criterion	Available from DriveLock version	Type	Value, name, example
AD computer properties	2022.1	unknown, integer	You can find the possible attributes or values in the Attribute Editor in the Domain Controller section Active Directory Users and Computers

Filter criterion	Available from DriveLock version	Type	Value, name, example
			All computers from a specific department (Department attribute from AD).
Architecture	2019.1	Enum	x86, x64
OS build	2022.1	String	21H2
OS name	2019.1	String	Windows 10 Pro
OS type	2019.2	Enum	available operating systems (Linux, Windows)
BIOS vendor	2022.1	String	
BIOS version	2022.1	String	
BIOS timestamp	2022.1	Date / Time	
Computer name	2019.1	String	
Defender Service version	2022.1	String	
Defender	2022.1	Enum	Active, Inactive, Partially active

Filter criterion	Available from DriveLock version	Type	Value, name, example
state			
Distinguished name	2022.1	String	CN=PC01,C-CN=Computers,DC=DLSE,DC=local
Domain name	2022.1	String	
DriveLock version	2019.1	Version	
IP4 range	2019.1	IP address list	Enter the corresponding IP4 ranges
Is server	2019.1	Boolean	Yes, No
Is staging	2019.1	Boolean	Yes, No
Open vulnerability	2022.1	Stringlist	Enter the name of the vulnerability
Registry	2019.1	unknown, integer	Enter the registry key and name
SMBIOS ver-	2022.1	String	

Filter criterion	Available from DriveLock version	Type	Value, name, example
sion			
TPM version	2022.1	Version	
TPM exists	2022.1	Boolean	Yes, No
Windows version	2019.1	Version	

Examples of how to use the operators in combination with the appropriate type:

Operator	Type	Example
equals / not equals	all types except lists	Architecture equals to x64
matches	Strings (wildcards possible)	Computer name matches PC*
greater than / greater or equals / less than / less than or equals	Integer, versions	DriveLock version greater than 21.2.5
contains value	For lists only	Open vulnerability contains value CVE-2022-123
within range	IP address lists, dates	IP range within range 192.168.0.0 to 192.168.255.255

3.6.4 Using groups in policies

You can use static and dynamic groups in all whitelist rules (drive and device whitelist rules), application rules, file filter templates, and configuration filters. Also, you can use groups to define rules for Security Awareness.

Note: You must first define static and dynamic DriveLock groups before you can use them in policies. We do not provide any default DriveLock groups which you can use out of the box.

Once the DriveLock group has been defined, the respective usage is displayed in the group properties in the **Used in policies** menu.

Warning: Please note that it is absolutely necessary to be connected to a DES to be able to implement DriveLock's group concept.
Clients that are temporarily disconnected from the DES will be updated with the current policies (and group settings) the next time they connect. Until this update is done, the clients are displayed in the list of group members with an incorrect status, which means that either they are displayed although they are no longer members or they are not displayed although they should already be members.

3.6.5 Update group members in DOC

Warning: Please note that a connection to a DriveLock Enterprise Service (DES) is mandatory to implement the group principle.

Clients that are temporarily disconnected from the DES will be updated with the current policies (and group settings) the next time they connect. Until this update is done, the clients are displayed in the list of group members with an incorrect status, which means that either they are displayed although they are no longer members or they are not displayed although they should already be members.

3.7 Rules in the DOC

To enable quick unlocking, you can create drive or application rules from the following views in the DOC:

Drive rules

1. In the **Analysis** menu in the **Events** view:
   Events that provide drive data can be used as a source for a drive rule. Select the **Drive events** option in the vertical split of the window to display the corresponding

events. The associated drives are displayed in the **Related objects** section. Select **Drives**, and then open the drive's context menu. Click the **Add to rule** menu item to add the drive to an existing rule. Click the **Create rule** menu item to create a new rule that already contains the data of the respective drive.

2. In the **Analysis** menu in the **Inventory** view on the **Drives** tab:
   All drives are listed on this tab along with the corresponding information. The detail view shows a list of all policies and rules that already apply to the selected drive. Again, you can add drives to an existing rule or create a new rule by clicking the appropriate menu items.
3. All drive rules that have already been created are listed in the **Configuration** menu in the **Rules** view. Click the **Create drive rule** button to create a new rule. You will have to enter all the data manually if you choose this option.

Application rules

Application Control must be licensed in order to create application rules and the following events must also be configured so that the DriveLock Agent will send them to the DES.

- 473: Process blocked
- 474: Process started
- 648: DLL blocked
- 649: DLL loaded

1. In the **Analysis** menu in the **Events** view:
   Events that report back information about applications can be used as a source for an application rule. You can view the events for application control by selecting the **Application Control** option in the vertical split of the window. Select an event, open the context menu and click **Create application rule**. This allows you to create a new rule with the application data (path, hash, version, etc.) already entered. Please make sure that you select at least one of the displayed file properties.
2. In the **Analysis** menu in the **Inventory** view under Installed software or Binaries:
   Processes that can be used in application rules are listed here.
3. The Application rules tab in the **Configuration** menu in the **Rules** view lists all the application rules that have already been created. Here you can create a new rule by clicking the **Create application rule** button. You will have to enter all the data manually if you choose this option.

Note: For more information on application rules, especially the file properties rule, see the separate Application Control documentation at DriveLock Online Help.

3.7.1 Creating rules for drives

Please do the following:

1. After you select the **Create drive rule** option, a wizard will open.
2. On the **Properties** tab, enter a rule name and select the rule type. It determines the basic behavior of the rule:
   - **Allow for specific users or computers**: this unlocks the drives for selected users on selected computers.
   - **Allow for all**: This will unlock the drives for all users on all computers.
   - **Deny for all**: This locks the drives for all users on all computers.
3. The drives for the new rule are listed on the **List of drives** tab. A warning appears if there are already rules for the drives. If you add only one drive to the rule, you can edit the drive's properties and enter a comment. The drive properties support wildcards (*, ?), so you can specify a range of serial numbers, for example.
4. On the **Permissions** tab, you can choose users and groups from the AD inventory and add them to the rule. Permissions for reading, writing and executing can also be configured here. When you select computers, you can include computers and groups from the AD inventory and DriveLock groups.
5. On the Options tab, you can configure the following options:
   - **User must accept usage policy**: A drive may not be accessed until the user confirms reading a usage policy.
   - **Require drive to be encrypted**
   - **Automatically encrypt unencrypted drives**

   Note: Please note that encryption and recovery must be configured in a different policy for enforced encryption. For more information on encryption, see the Encryption documentation at DriveLock Online Help.

3.7.2 Creating rules for applications

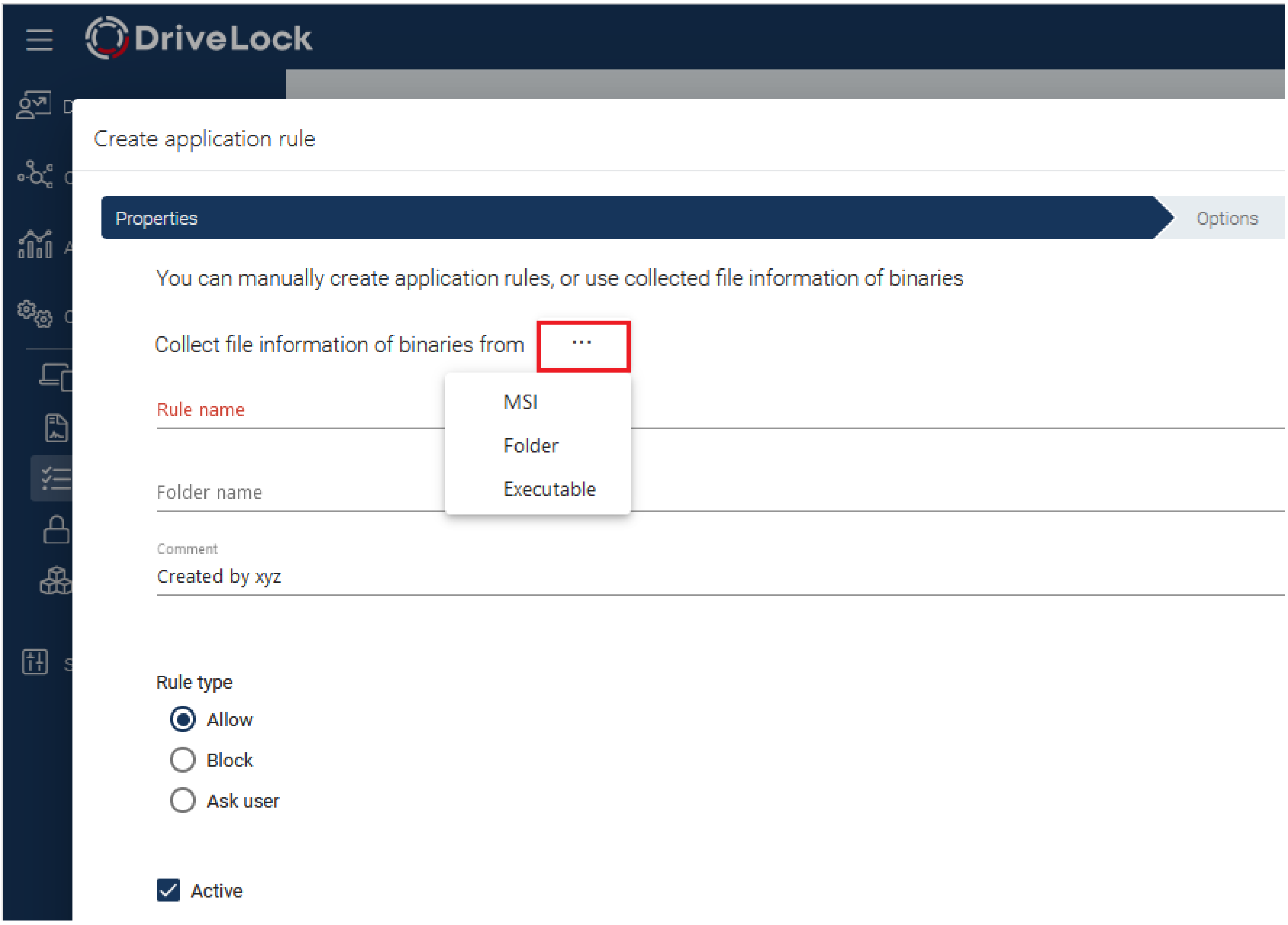
Note: For more information on application rules, see the separate Application Control documentation at DriveLock Online Help.

To create an application rule in the DOC, proceed as follows:

1. After you select the **Create application rule** option, a wizard will open.
2. On the **Properties** tab, choose whether you want to create an application rule manually or whether you want to collect file information from binaries to create it.
   In case you create it manually, enter a rule name and select the rule type. It determines the basic behavior of the rule:
   - **Do not block**: This setting corresponds to the Whitelist rule type, the selected application is allowed and may be executed.
   - **Block**: This setting corresponds to the Blacklist rule type, the selected application is forbidden and may not be executed.
   - **Ask user**: With this rule type, an application is allowed (whitelist), but the user must confirm its start.
   - **Active**: This option is set by default. If you want to create the rule but do not want to activate it right away, you can uncheck it.
3. On the **Options** tab, you specify the criteria (file properties) that determines whether to allow or block an application.

3.7.2.1 Using file information from binaries

Using the **MSI**, **Folder** or **Executable** options, it is possible to have multiple application rules created at the same time.



Create application rule

Properties | Options

You can manually create application rules, or use collected file information of binaries

Collect file information of binaries from ...

Rule name

Folder name

Comment
Created by xyz

Rule type

● Allow
○ Block
○ Ask user

☑ Active

For example, when you select an MSI, DriveLock unpacks the selected MSI in the background and then creates suggested rules with the appropriate rule criteria. A set of standard criteria (information) found is grouped within the rules.

You can accept or reject the suggestions (by removing the checkmarks from the checkboxes) and use only the criteria that you find useful.

Note: Please always consider the safety aspect when choosing your criteria.

The rules are grouped and saved using the specified name and are then displayed in the Application rules section. Here you can edit, activate, deactivate or delete the individual rules.

Note: For more information on application rules, see the Application Control documentation at DriveLock Online Help.

3.7.2.2 Creating application rules via executables

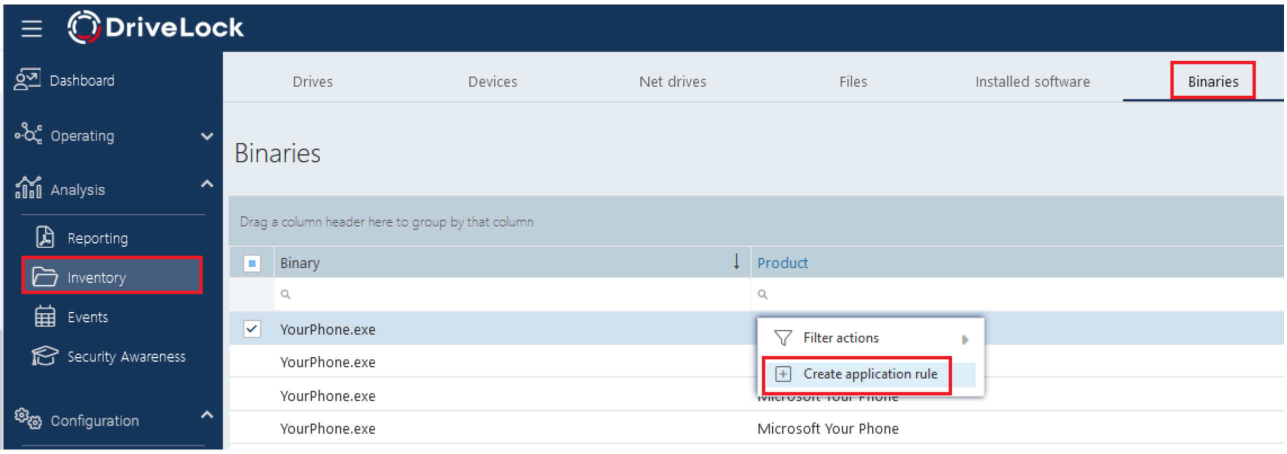
The list shows only the executable files that are already stored in the application hash database and for which the DriveLock Agent has already sent events.

To create a rule for single or multiple executable files, do the following:

Select the required file(s), open the context menu and then click the **Create application rule** option. The rule creation wizard opens and automatically creates rules with the appropriate **properties**.

The **Options** tab lists the rule criteria.

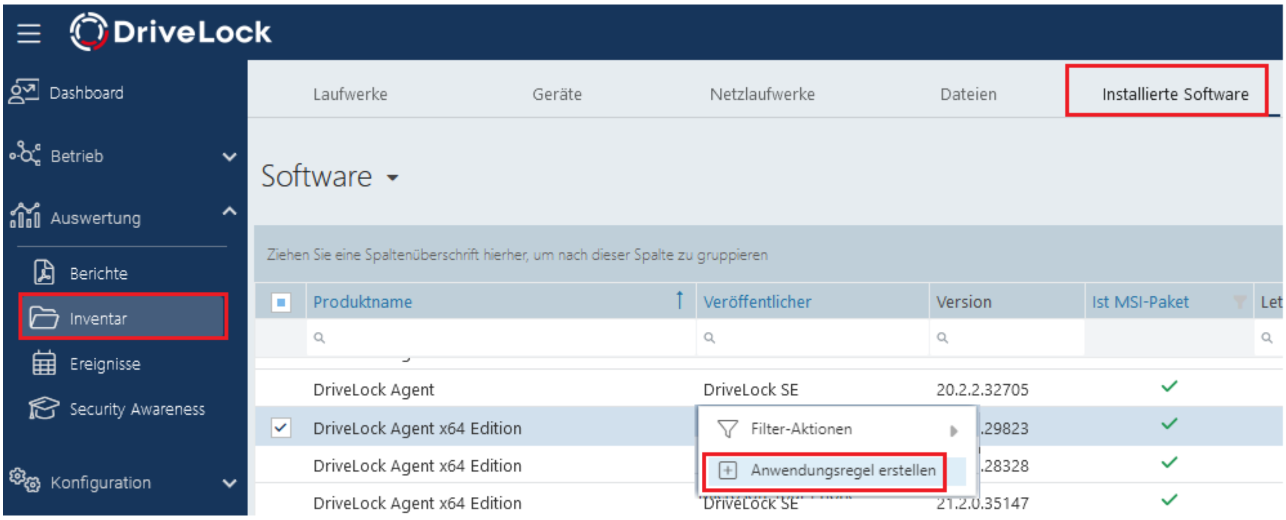
On the **Review** tab, you can review your rule settings again before clicking **Finish** to create the rules.



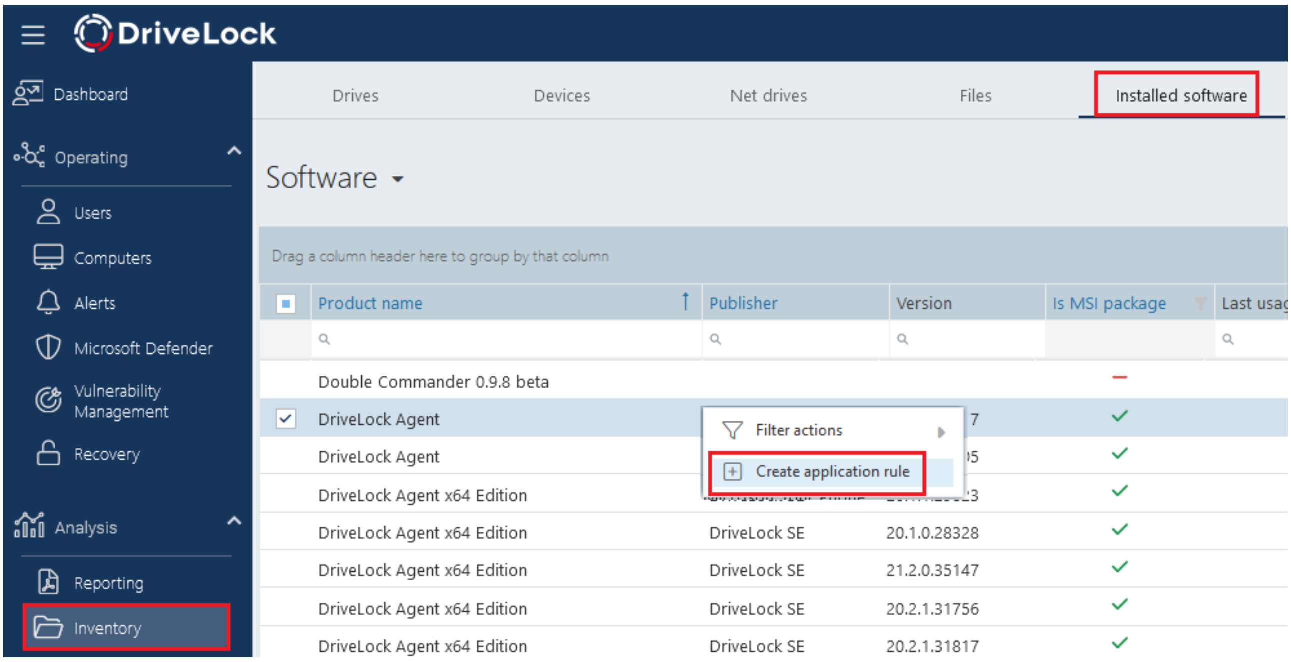
3.7.2.3 Creating application rules via installed software

If there are executables for an application in the application database, you can also create application rules via the installed software. Mapping the executable files to the corresponding installed software is achieved based on events sent by the DriveLock Agent to the DriveLock Enterprise Service (DES).

Proceed exactly the same way here as you would when creating application rules via executable files.



	Produktname	Veröffentlicher	Version	Ist MSI-Paket	Let
	DriveLock Agent	DriveLock SE	20.2.2.32705	✓	
☑	DriveLock Agent x64 Edition		.29823	✓	
	DriveLock Agent x64 Edition		.28328	✓	
	DriveLock Agent x64 Edition	DriveLock SE	21.2.0.35147	✓	



	Product name	Publisher	Version	Is MSI package	Last usag
	Double Commander 0.9.8 beta			—	
☑	DriveLock Agent		7	✓	
	DriveLock Agent		5	✓	
	DriveLock Agent x64 Edition		3	✓	
	DriveLock Agent x64 Edition	DriveLock SE	20.1.0.28328	✓	
	DriveLock Agent x64 Edition	DriveLock SE	21.2.0.35147	✓	
	DriveLock Agent x64 Edition	DriveLock SE	20.2.1.31756	✓	
	DriveLock Agent x64 Edition	DriveLock SE	20.2.1.31817	✓	

3.8 Permissions in the DOC

You can configure the DriveLock permissions settings only in the DriveLock Operations Center (DOC). These settings in the DOC also apply to the DriveLock Management Console (DMC).

To define user accounts and permissions, go to the **Permissions** view in the **Settings** menu.

Accounts

An account contains a user's security-related data and provides access to DriveLock functionality. Each account has roles assigned to it (role assignments), which include various rights (role permissions) to perform actions.

- Accounts in the cloud environment
  Role assignments are evaluated directly for email accounts
- Active Directory accounts
  Accounts can be created for both individual users and groups in Active Directory. When a user logs in, their Active Directory groups are resolved and the user's role assignments are completed with the role assignments for any group accounts found.
- Azure Active Directory accounts
  The groups and memberships of an Azure Active Directory (AAD) can be synchronized. In combination with SAML login, the user's group memberships are queried by Azure Active Directory. This enables role assignments to the Azure AD groups the user is a member of, similar to the Active Directory.

Roles and role permissions

- Different permissions are combined in a role. DriveLock checks whether the required permissions are assigned when actions are performed.
- DriveLock provides several built-in roles (e.g. Supervisor, Administrator). But you can also define and use your own roles.

Role assignments

- A role assignment links an account to a role and optionally a context that restricts how the role and its permissions are applied to specific objects.
- Available contexts for role assignments:
  - **Global**: the role applies globally with no restrictions on objects.
  - **OU**: the role applies only to computers included in the selected Active Directory OU
  - **Group**: the role applies only to computers that are members of the specified DriveLock group
  - **Policy collection**: the role applies only to policies that are included in a policy collection

> Note: In the computer context (OU or group), it is only possible to have permissions on computers, even if the role originally includes permissions to other areas.
> In the policy collections context, permissions only apply to policies, but not to other objects.

- Examples:

- In the Global context, a user with the Helpdesk role is allowed to see all computers and events, the entire inventory, etc., and also to open policies (but not save them).
- In the Active Directory OU context, a user with the Helpdesk role is allowed to see only computers, events, etc. that are contained in the specified Active Directory OU. However, this user is not allowed to open policies because the role assignment to OUs applies only to computers, but not to policies. You can add an additional role assignment to allow that.

3.9 Policy collections (DOC)

In the DOC, you can group policies into policy collections. These collections can then be used in role assignments to restrict access to specific policies for a given role.

3.10 Data masking

By enabling data masking, you can easily hide sensitive user or computer data as required by the General Data Protection Regulation (GDPR). Instead of showing the user or computer name, a substitute is displayed. This prevents the analysis of user behavior and, if configured accordingly, can help to make it impossible to draw conclusions about specific computer users.

To enable or disable masking, you need to have a special permission (role).

In the **Show unmasked data** section, you can specify the conditions for temporarily unmasking the data for the current browser view. The data will still be displayed masked in all other views. This may be necessary, for example, to fix urgent issues that affect the system or to detect any unusual behavior on the user's part.

You also need special permissions to unmask the data. The following options are available here:

- **With role permission**: The appropriate permission must be assigned.
- **With code**: It is only possible to undo the masking when entering a code. The code must be requested separately and is valid for a certain period of time. This option is used if no one has access to the DOC, but it is mandatory to request data, for example, due to operational reasons. The code must be handled like a password, kept secret and entered on site.
- **Approved by**: If you use this option, you need to provide a contact person to authorize the unmasking. In the text field below, you can enter the appropriate information (for example, name, phone number, e-mail address). This is also done in the DOC. This

is where the request will be sent to and a response will be given accordingly (approval or rejection).

In the **Level of data masking** section, you specify which data to mask.

- **Full**: all user and computer data gets masked. Neither related entities, nor information in events, alerts or in security awareness sessions are displayed. It is not possible to draw any conclusions about the computer or the user. While this option provides the highest level of privacy, it also makes troubleshooting difficult.
- **Only user names**: This option is useful when several users are working on the same computer. You will see only the computer names, the user names are masked. For troubleshooting, this is a good option to use.
- **Individual**: Click **Configure** to specify the context and the events where user or computer data gets masked. These settings allow you to precisely configure data masking and, for example, limit it to different events.

On the **General** tab you can select the following options:

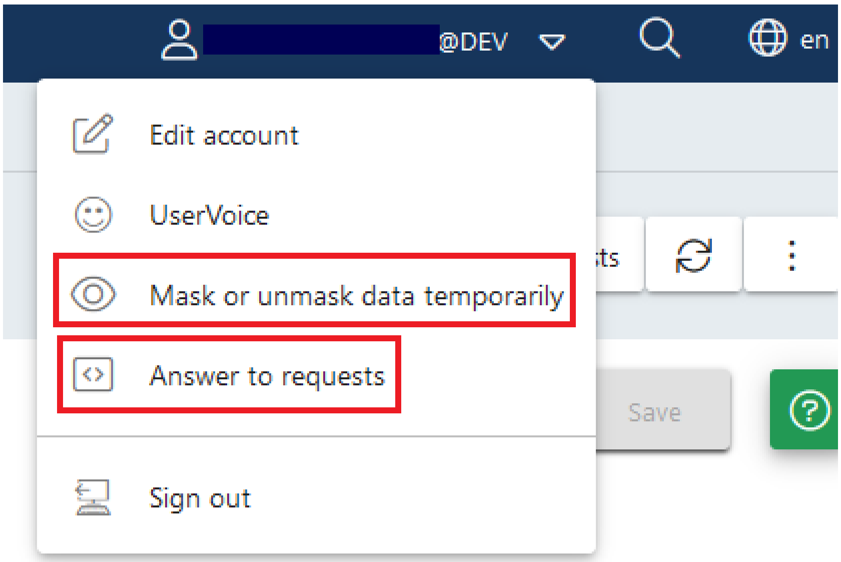
- **Show user's computers**: If you enable this option, the computers of a masked user will be displayed in the **Related entities** section in the **Users** view**(End users on managed computers**). Note that this may allow tracing the user through the particular computer.
- **Show 'Last logged in user' in plain text**: In the **Computers** view, the name of the user who was last logged on to this computer is displayed in the **Last logged on user** column.
- **Show 'built-in user' in plain text**: You also see the operating system accounts in all views when this option is enabled, for example NT-AUTHORITY\SYSTEM. This option is selected by default.
- In addition, you can select the **context** to apply the data masking, e.g. for security awareness sessions.

On the **Events** tab, you can select individual or multiple events where you want to mask data.

Other data masking options (see figure):

Use the **Answer to requests** button to approve or deny requests to unmask data.

You can also select this option from the user's context menu (see figure). The option to temporarily "reverse" the data masking is also available here. If data is already masked, a request to temporarily display the data in plain text, or in the reverse case, a request to temporarily mask the data quickly (for computer and/or user data respectively) can be made here.



Applying data masking with the "User name" filter set

If the **User name** filter is set in a widget and data masking is enabled at the same time, no data will be displayed. The system user is an exception. It is set with the help of the `Ist Systembenutzer` property.

3.11 Windows authentication in the DOC

To enable Windows authentication, NTLM pass-through must be provided. This involves different steps depending on the security mechanisms of the different browsers.

Mozilla Firefox:

1. Enter **about:config** as the URL.
2. Confirm the security prompt by clicking **Accept risk and continue.**
3. Search for **NTLM**.
4. Edit the **network.automatic-ntlm-auth.trusted-uris** value by entering the host name of your DES and save.

Microsoft Edge and Chrome:

1. Open Internet Explorer
2. From the Tools menu, select **Internet Options** , and then click the **Security** tab.
3. Select the **Local Intranet** icon and then click **Custom Level**.

4. In the **Security Settings** - **Local Intranet Zone** dialog box, go to **User Authentication** and select **Automatic logon to Intranet Zone only**.
5. Add the URL of your DES to the local intranet zone.

3.12 SAML authentication in the DOC

SAML is an open standard for authentication that can be used to implement a Single Sign On (SSO). With SAML, you can log in to an Azure AD and authenticate yourself as a user, and the DriveLock Operations Center (DOC) will use this login, making an additional login via email and password no longer necessary. SAML refers to identity providers and service providers. In the example, Azure AD is the Identity Provider. The Service Provider is always DriveLock. To be able to log in to the DOC via SAML, you must ensure that the e-mail account you use to log in to the Identity Provider is also available as an account in the DOC.

In case of Azure AD in particular, DriveLock also supports logging in via group membership to an Azure AD group. In this case, you first need to set up Azure AD synchronization and create a role assignment to an Azure AD group in the DOC. Once logged in via SAML, an account is automatically created for the Azure AD user within DOC. This requires configuring SAML authentication in DOC first. Then configure the Azure AD integration and reference the SAML configuration there.

Configuration

To enable SAML SSO logon functionality in the DOC, you need to configure both the DOC and your Identity Provider.

In your identity provider configuration, identify an entry option for the Redirect URL or **callback URL** and set it to the value that the DOC shows you in the **Identity provider** section.

Make sure that the identity provider contains the e-mail address listed in the **Claims** section. Here DriveLock searches for the default claim ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress") by default. If your identity provider returns the email address under a different claim, you can also specify that in the DOC in the **Identity Provider** section.

This completes the configuration of the Identity Provider. Now look in the Identity Provider for a way to download the configuration as a "Federation metadata document". This is an XML document that starts with "<EntityDescriptor...".

Paste the XML in the DOC in the **Identity provider metadata** section.

If your Identity Provider insists on a specific **entity ID**, you can enter it in the DOC in the **Service Provider** section. For example, with Azure AD, this value must be set to the **Application (Client) ID**. Other providers such as Auth0 work with the pre-entered value.

Troubleshooting

Sometimes you may not be able to configure SAML authentication successfully. To get more information about a possible misconfiguration, select **Enable debug mode [...]** in the DOC in the **General** section.

This option lists possible causes in the event of an error below the DOC login screen. This is where you can find out if the e-mail address, for example, is not available in the credentials (claims) or with the expected name. The DOC shows the submitted claims and allows you to analyze them.

3.13 Certificates

In the **Certificates** view you can store certificates in the server database. This allows administrators to select a certificate file and assign a purpose to the certificate.

In the DOC you can select different certificates. For the following DriveLock modules, there are standard certificates that you can use directly. Please ensure secure storage of the appropriate private key and passwords.

Default certificate name	Intended use	Private key	More information
DLBlDataRecovery.cer	Data recovery with BitLocker	DLBlDataRecovery.pfx	BitLocker certificates
DLBlEmergencyLogon.cer	Emergency login with BitLocker	DLBlEmergencyLogon.pfx	BitLocker certificates
DLFDERecovery.cer	Data recovery with Disk Protection	DLFDERecovery.pfx	Disk Protection certificates

Default certificate name	Intended use	Private key	More information
DLFDEMaster.cer	Emergency logon with Disk Protection	DLFDEMaster.pfx	Disk Protection certificates
DLFfeRecovery.cer	Recovery with File Protection	DLFfeRecovery.pfx	File Protection Certificates
DLBl2GoRecovery.cer	Recovery with BitLocker To Go	DLBl2GoRecovery.pfx	Certificate-based recovery
DLDlvRecovery.cer	Recovery with Encryption 2-Go	DLDlvRecovery.pfx	Certificate-based container recovery
Certificate is generated individually; certificate name e.g. TempUnlockCert.p7b	Temporary offline release	*Matching private key*	more information

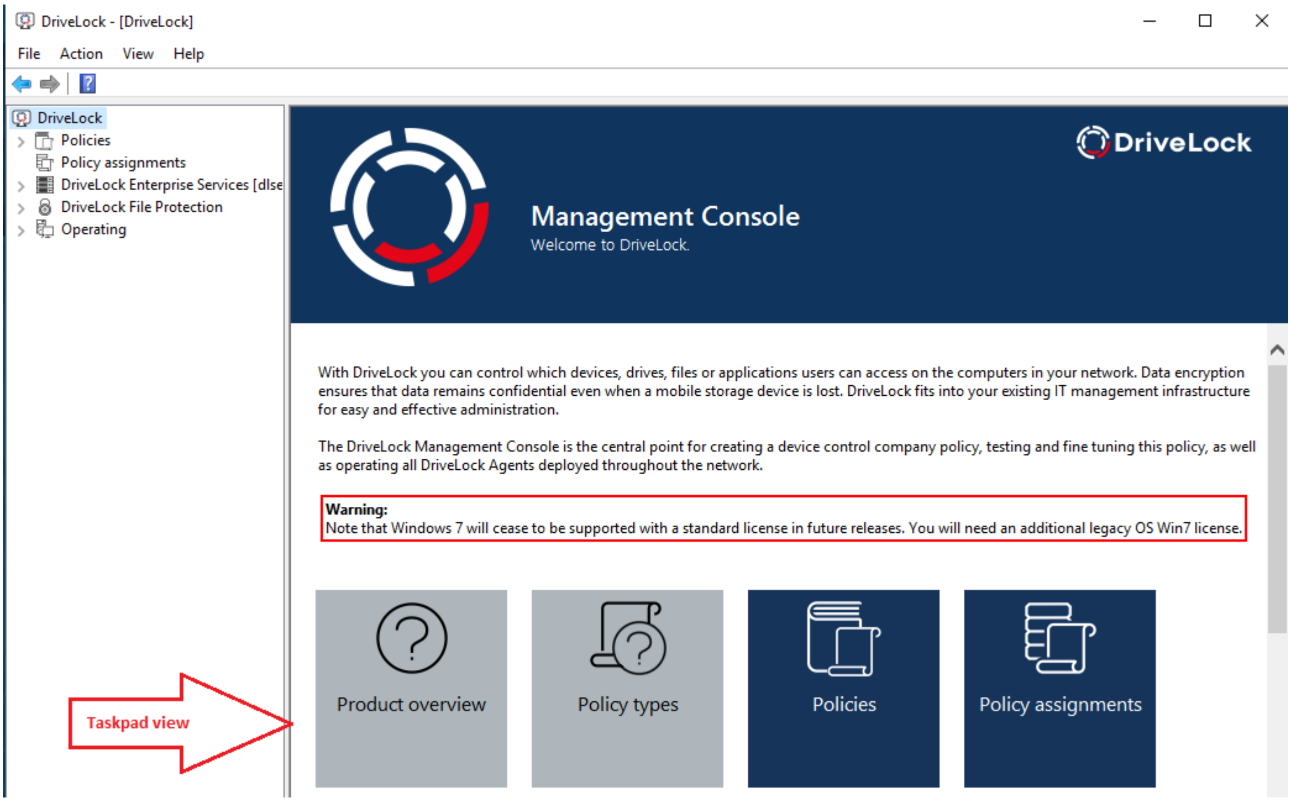
4 DriveLock Management Console

The DriveLock Management Console (DMC) acts as a MMC snap-in and can be used as a stand-alone console or as an additional part of an existing administrative set-up in a Microsoft Management Console (MMC).

In the DMC, you perform important configuration tasks for DriveLock 'On-Prem'. These are:

- Create policies,
- Assign policies,
- Configure DriveLock Enterprise Services,
- Configure DriveLock File Protection and
- Control the DriveLock Agents in operation.

Once you have installed the DriveLock Management Console, you can start it from the Windows Start menu by selecting **All Programs / DriveLock / DriveLock Management Console**:



With DriveLock you can control which devices, drives, files or applications users can access on the computers in your network. Data encryption ensures that data remains confidential even when a mobile storage device is lost. DriveLock fits into your existing IT management infrastructure for easy and effective administration.

The DriveLock Management Console is the central point for creating a device control company policy, testing and fine tuning this policy, as well as operating all DriveLock Agents deployed throughout the network.

Warning:
Note that Windows 7 will cease to be supported with a standard license in future releases. You will need an additional legacy OS Win7 license.

The menu bar at the top contains the standard menu of an MMC, along with the buttons for accessing certain functions.

On the left side of the navigation area you can access the different functions of the DriveLock Management Console. The tree structure contains individual nodes with their sub-functions.

The taskpad view on the right shows the menu items available within a node. You can also switch this view to a detailed view (**List view**) showing items inside a list. This is largely the same as the classic view of an MMC.

Almost every node in the navigation pane and every element of a detail view has a context menu with corresponding functions, accessed by right-clicking.

In some places of the DriveLock Management Console or in the policy editor, you can switch from the taskpad view to the **list view**. Select the **context menu / View / Taskpad view** to switch back.

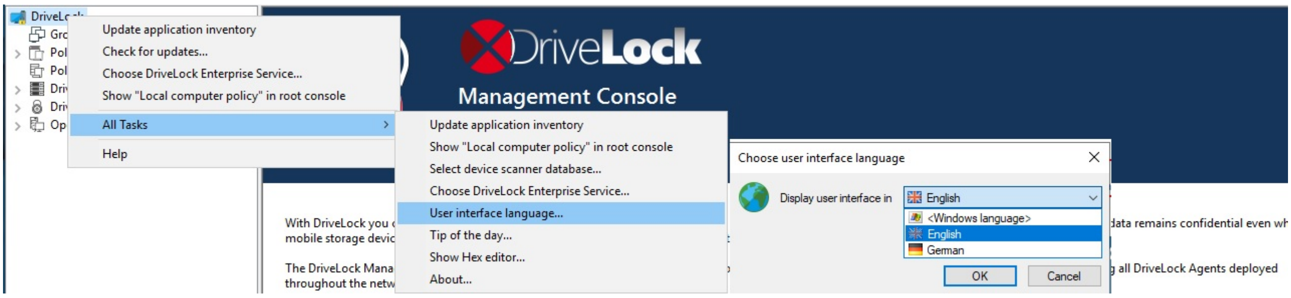
4.1 General notes

4.1.1 Changing the language of the user interface

Right-click DriveLock and select **All Tasks-> User interface language**.

Note: Depending on your operating system language settings, some default buttons and menu items may be displayed in that language rather than the one you select as the user interface language in DriveLock.

How to choose your language:


Update application inventory
Check for updates...
Choose DriveLock Enterprise Service...
Show "Local computer policy" in root console
All Tasks
Help
DriveLock
Management Console
Update application inventory
Show "Local computer policy" in root console
Select device scanner database...
Choose DriveLock Enterprise Service...
User interface language...
Tip of the day...
Show Hex editor...
About...
Choose user interface language
<Windows language>
English
German
OK
Cancel

Display user interface in: English

4.2 Policies

4.2.1 Deploying DriveLock configuration settings

There are several ways to distribute configuration settings to clients. The steps to configure settings are identical in all types of policies. You can configure the same parameters, whitelist rules, or network settings.

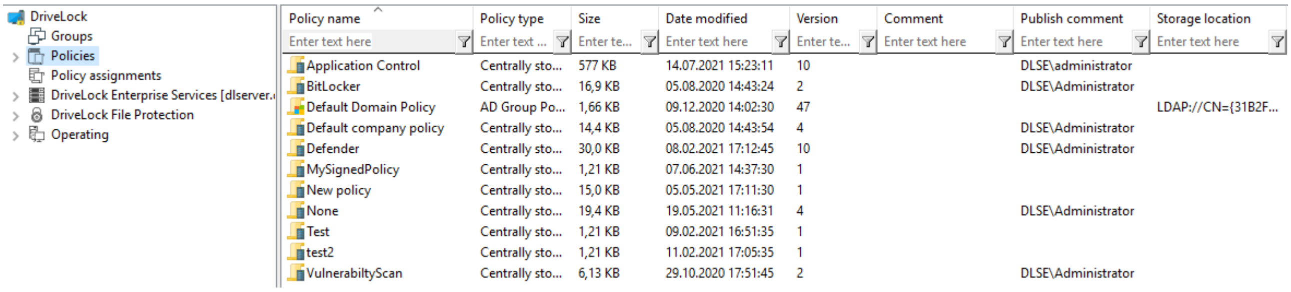
The following configuration matrix helps you to get an overview of which configuration types are possible.

Note: Generally, we recommend that you only work with centrally stored policies.

	Central configuration	Requires DES	Uses existing infrastructure	History / Versioning	Flexibility
Centrally stored policy (CSP)	Yes	Yes	No	Yes	Very good
Group Policy	Yes	No	Yes (AD)	No	Acceptable
Configuration file	Yes	No	Yes (UNC, http, ftp)	No	No
Local policy	No	No	No	No	No

Warning: Before distributing settings to multiple clients on the network, we recommend that you first test them on one or more test clients.

Configuration settings are managed in the DriveLock Management Console in the Policies node:

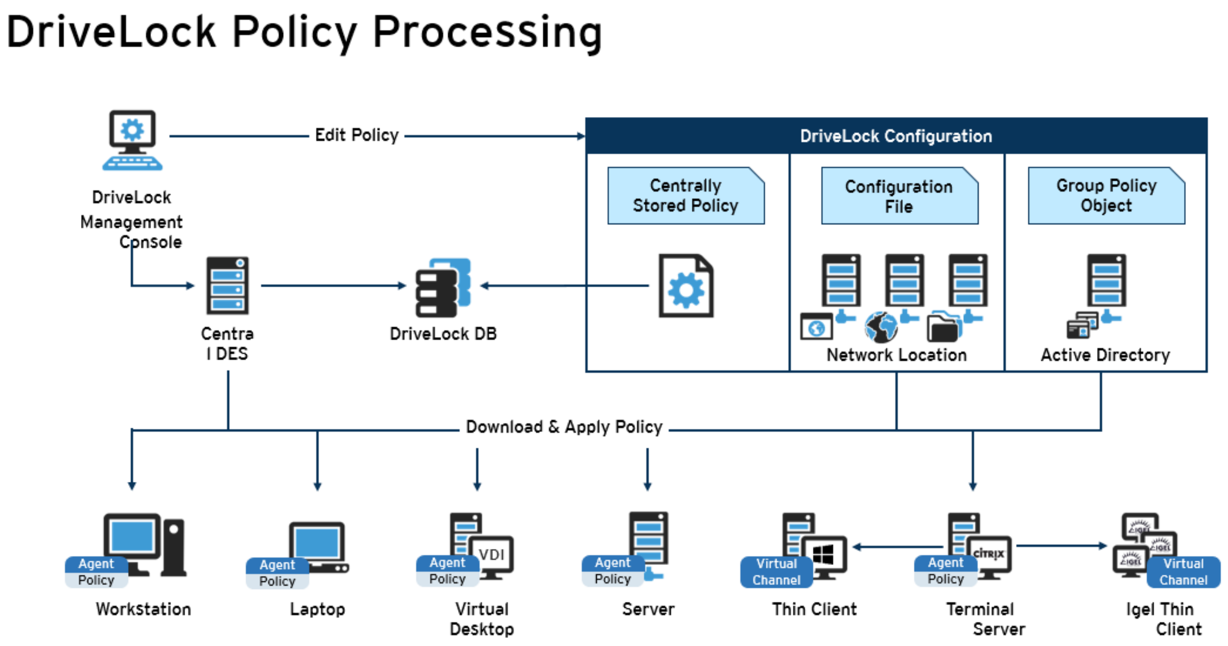


DriveLock
Groups
Policies
Policy assignments
DriveLock Enterprise Services [dlserver.
DriveLock File Protection
Operating

Policy name	Policy type	Size	Date modified	Version	Comment	Publish comment	Storage location
Enter text here	Enter text ...	Enter te...	Enter text here	Enter te...	Enter text here	Enter text here	Enter text here
Application Control	Centrally sto...	577 KB	14.07.2021 15:23:11	10		DLSE\administrator	
BitLocker	Centrally sto...	16,9 KB	05.08.2020 14:43:24	2		DLSE\Administrator	
Default Domain Policy	AD Group Po...	1,66 KB	09.12.2020 14:02:30	47			LDAP://CN={31B2F...
Default company policy	Centrally sto...	14,4 KB	05.08.2020 14:43:54	4		DLSE\Administrator	
Defender	Centrally sto...	30,0 KB	08.02.2021 17:12:45	10		DLSE\Administrator	
MySignedPolicy	Centrally sto...	1,21 KB	07.06.2021 14:37:30	1			
New policy	Centrally sto...	15,0 KB	05.05.2021 17:11:30	1			
None	Centrally sto...	19,4 KB	19.05.2021 11:16:31	4		DLSE\Administrator	
Test	Centrally sto...	1,21 KB	09.02.2021 16:51:35	1			
test2	Centrally sto...	1,21 KB	11.02.2021 17:05:35	1			
VulnerabiltyScan	Centrally sto...	6,13 KB	29.10.2020 17:51:45	2		DLSE\Administrator	

Architecture

The following figure provides an overview of the available deployment methods.



Warning: If using Microsoft Group Policy, we recommend that you also use the Group Policy permissions concept to ensure that only authorized administrators can view or modify the DriveLock configuration policy. If you are using configuration files, use Windows file access permissions for this. For centrally stored policies, access control to the DriveLock Enterprise Service provides appropriate security.

4.2.2 Centrally stored policies

Centrally stored policies (CSP) are stored in the DriveLock database and are distributed to the agents via the DriveLock Enterprise Server (DES).

CSPs are ideal for most use cases because:

- CSPs support versioning and change tracking and can be edited or published separately by the administrator.
- Several CSPs can be assigned to one agent (which is not the case with configuration files, for example).
- CSPs can be used in almost any network environment, including Active Directory, Workgroups and Novell Directory Service.

For Managed Security Service Providers (MSSP), CSPs are the best choice for keeping policies of different tenants separate.

Warning: A DriveLock Enterprise Service (DES) is required if you want to use centrally stored policies.

You can assign one or several CSPs to computers, DriveLock groups, AD groups, OUs or even to All computers. The CSPs can belong to the default tenant (root) or any other tenant. The agent knows the DES servers it can get CSPs from. This allows CSPs with different settings to be combined, for example, one CSP contains only basic settings that are then distributed to all clients, and another contains special settings that are assigned only to clients in a specific department. So for example you can create a CSP that contains the USB sticks of the marketing department, and this CSP will only be applied to the marketing clients.

Example:

Order, policy name	Assigned to	Description
1. License policy	All computers	Contains license information for all computers
2. Default_all	All computers	Default settings for all computers
3. USB sticks marketing	Marketing clients	Unlocked USB sticks for marketing
4. Disk Protection laptops	Laptops	Disk Protection
5. Application Control Servers	Servers	Allowed applications for servers

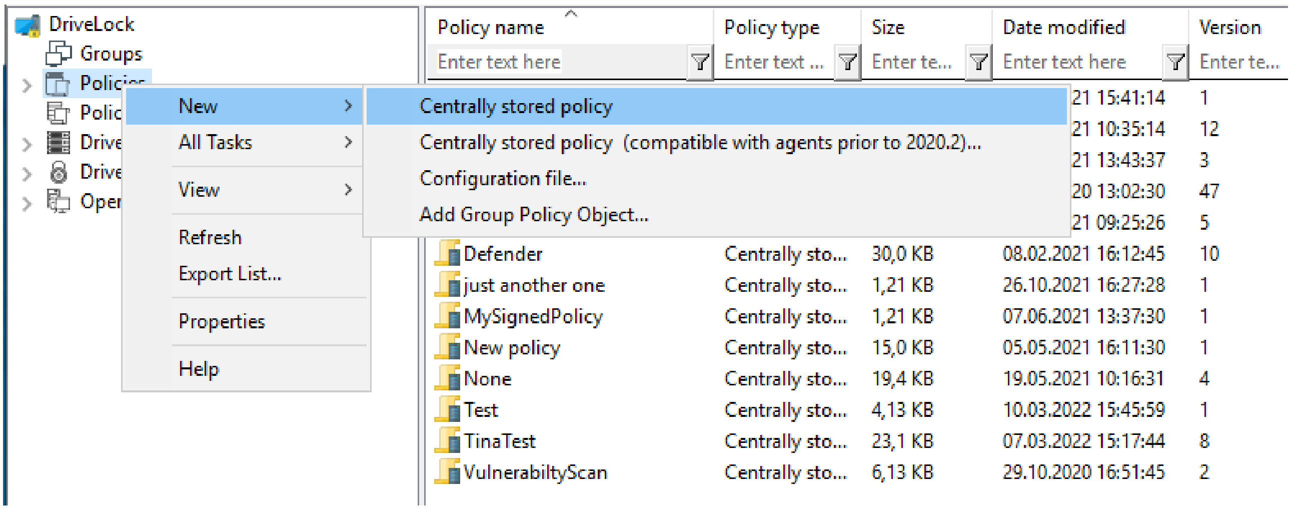
4.2.2.1 Creating and editing policies (DMC and DOC)

In the DriveLock Management Console (DMC)

To create a new centrally stored policy for the root tenant or other tenants, right-click **Policies**, select **New** and then **Centrally stored policy...**.

Note: If you are working with DriveLock Agents that have older DriveLock versions than 2020.2 installed, please select the option **Centrally stored policy (com-**

patible with agents prior to 2020.2).... These agents cannot yet handle the new policy format.



Policy name	Policy type	Size	Date modified	Version
Enter text here	Enter text ...	Enter te...	Enter text here	Enter te...
			21 15:41:14	1
			21 10:35:14	12
			21 13:43:37	3
			20 13:02:30	47
			21 09:25:26	5
Defender	Centrally sto...	30,0 KB	08.02.2021 16:12:45	10
just another one	Centrally sto...	1,21 KB	26.10.2021 16:27:28	1
MySignedPolicy	Centrally sto...	1,21 KB	07.06.2021 13:37:30	1
New policy	Centrally sto...	15,0 KB	05.05.2021 16:11:30	1
None	Centrally sto...	19,4 KB	19.05.2021 10:16:31	4
Test	Centrally sto...	4,13 KB	10.03.2022 15:45:59	1
TinaTest	Centrally sto...	23,1 KB	07.03.2022 15:17:44	8
VulnerabiltyScan	Centrally sto...	6,13 KB	29.10.2020 16:51:45	2

Assign a name, select a tenant, and enter a brief description of the policy.

Optionally, check **Use existing policy as template** and select a policy you want to create a copy of.

Click **OK** to save the new policy.

The DriveLock Policy Editor will then open, allowing you to edit the new policy.

If you want to edit an existing policy, right-click the policy and select **Edit**.

Warning: Remember to specify the license information in the global settings.

Note: Using the Import and Export functions, settings can be exchanged between a centrally stored policy and a local policy.

In the DriveLock Operations Center (DOC)

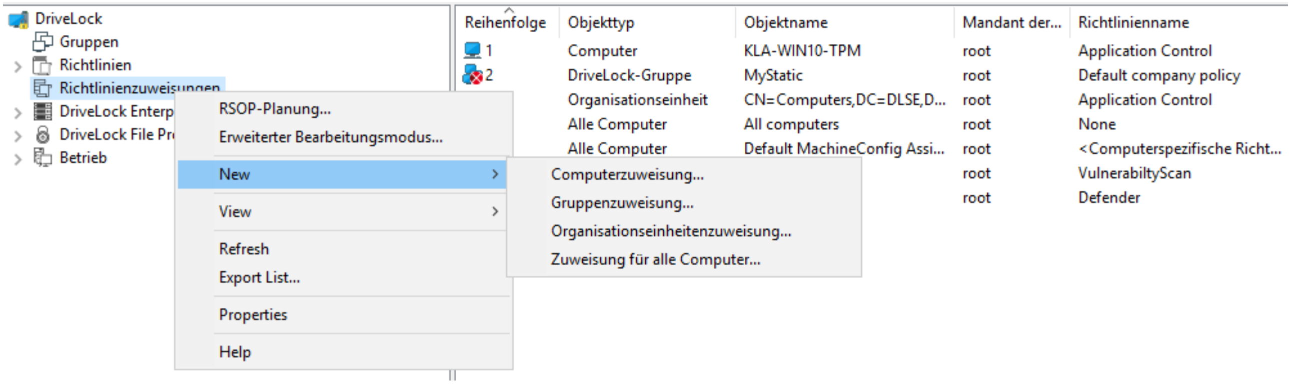
In the **Configuration** menu, open the **Policies** view. Click the **Create policy** button. Then the DOC Companion starts, if it is not already running. Then the Policy Editor opens and you can edit, save, publish, and then assign the policy directly in the DOC. For more information, see the separate DOC Companion documentation at DriveLock Online Help.

4.2.2.2 Assigning policies (DMC and DOC)

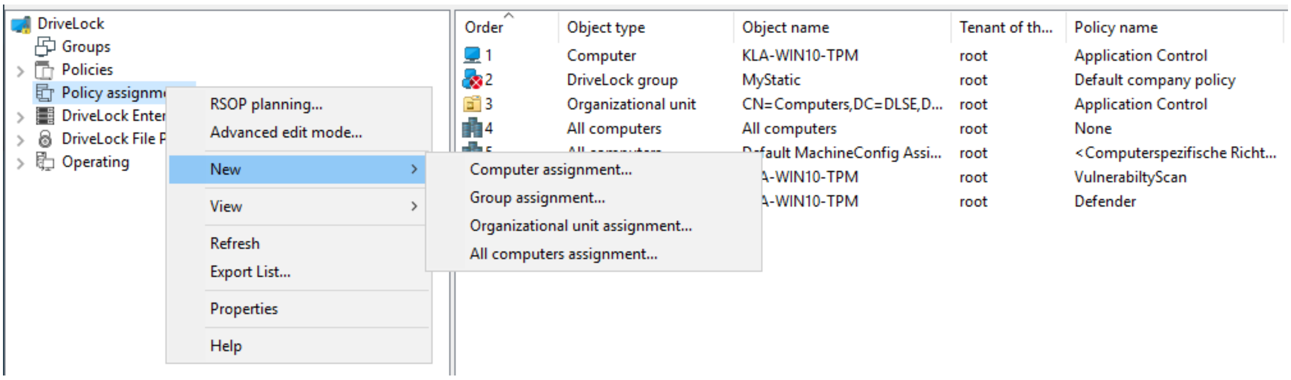
In the DriveLock Management Console (DMC)

Once you have created and configured a centrally stored policy, you will assign it to specific or all computers, groups, DriveLock groups, or organizational units (OUs) where you want it to take effect.

> Note: Before using static and dynamic DriveLock groups in policy assignments, you need to have defined them first. When the DriveLock group has been successfully applied to a policy, it appears on the Policy assignments tab of the group properties.



Reihenfolge	Objekttyp	Objektname	Mandant der...	Richtlinienname
1	Computer	KLA-WIN10-TPM	root	Application Control
2	DriveLock-Gruppe	MyStatic	root	Default company policy
	Organisationseinheit	CN=Computers,DC=DLSE,D...	root	Application Control
	Alle Computer	All computers	root	None
	Alle Computer	Default MachineConfig Assi...	root	<Computerspezifische Richt...
			root	VulnerabiltyScan
			root	Defender

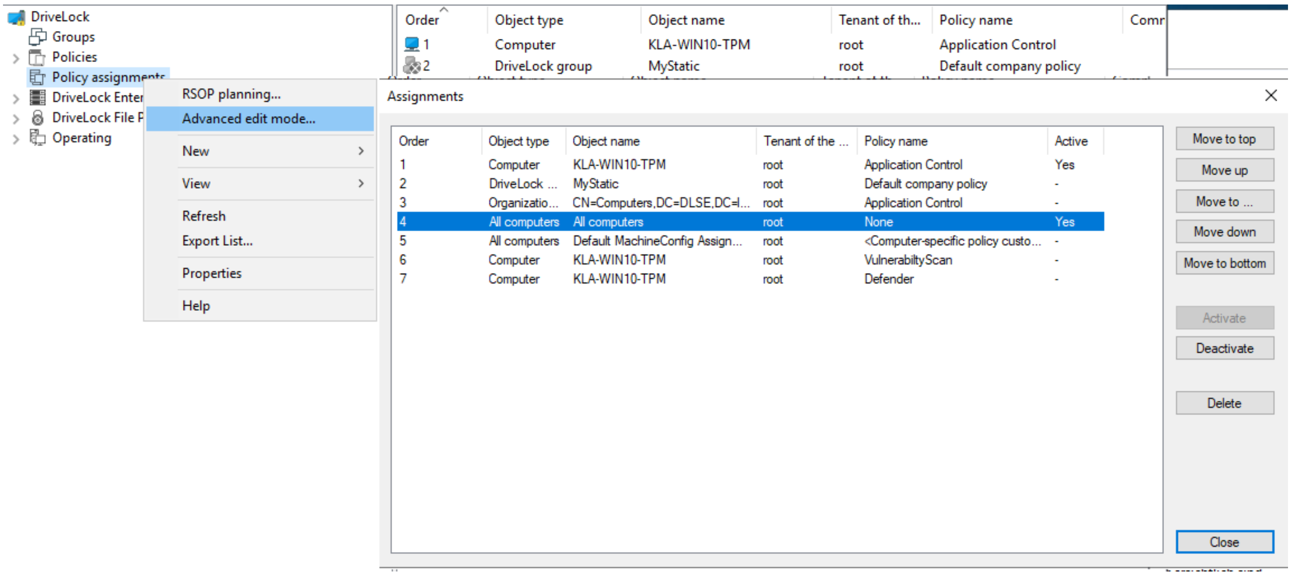


Order	Object type	Object name	Tenant of th...	Policy name
1	Computer	KLA-WIN10-TPM	root	Application Control
2	DriveLock group	MyStatic	root	Default company policy
3	Organizational unit	CN=Computers,DC=DLSE,D...	root	Application Control
4	All computers	All computers	root	None
		Default MachineConfig Assi...	root	<Computerspezifische Richt...
		A-WIN10-TPM	root	VulnerabiltyScan
		A-WIN10-TPM	root	Defender

In the assignment dialog, you specify the computers, groups or OUs, select a tenant and the appropriate policy. Policies stored for the root tenant can be used with any tenant, while policies stored for a specific tenant can only be assigned to that tenant.

To change the order, simply right-click an entry and move it.

If you want to move or edit more than one policy at a time, click **Advanced edit mode...** and move the policy to where you want to place it. Here you can also disable or delete the policies.



Order	Object type	Object name	Tenant of th...	Policy name	Comr
1	Computer	KLA-WIN10-TPM	root	Application Control	
2	DriveLock group	MyStatic	root	Default company policy	

Assignments

Order	Object type	Object name	Tenant of the ...	Policy name	Active
1	Computer	KLA-WIN10-TPM	root	Application Control	Yes
2	DriveLock ...	MyStatic	root	Default company policy	-
3	Organizatio...	CN=Computers,DC=DLSE,DC=l...	root	Application Control	-
4	All computers	All computers	root	None	Yes
5	All computers	Default MachineConfig Assign...	root	<Computer-specific policy custo...	-
6	Computer	KLA-WIN10-TPM	root	VulnerabiltyScan	-
7	Computer	KLA-WIN10-TPM	root	Defender	-

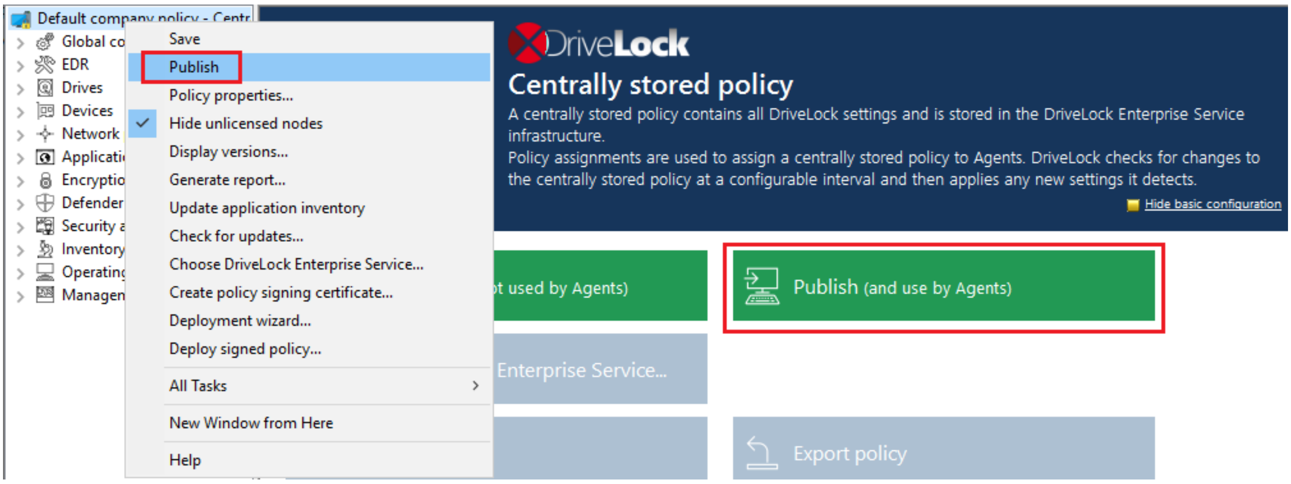
In the DriveLock Operations Center (DOC)

On the **Policy assignments** tab (in the **Configuration** menu, **Policies** view), you can create, edit, drag and drop to the desired location, and enable or disable policy assignments in the same way as in the DMC.

Also in DOC, you have the option to assign a policy to all computers (this option is enabled by default) or to specific targets (AD computers, DriveLock groups, Azure AD groups, AD groups or OU containers).

4.2.2.3 Publishing policies

To have a policy take effect on the DriveLock Agent, you need to publish the modified policy first. To do so, select either the context menu command or the button in the Taskpad view:

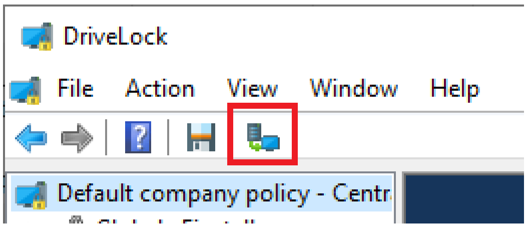


Centrally stored policy

A centrally stored policy contains all DriveLock settings and is stored in the DriveLock Enterprise Service infrastructure.

Policy assignments are used to assign a centrally stored policy to Agents. DriveLock checks for changes to the centrally stored policy at a configurable interval and then applies any new settings it detects.

Or simply in the menu bar by clicking the following icon:



Optionally enter a **publish comment** in the dialog and confirm with OK.

If you save the policy **in the new format**, only agents installed with a DriveLock Agent version 2020.2 or higher will be able to interpret it. The new policy format provides better performance (faster policy processing, less traffic between DES and agents).

Note: If necessary, you can also sign the policy and select the appropriate signing certificate in the dialog.

4.2.3 Group policy object

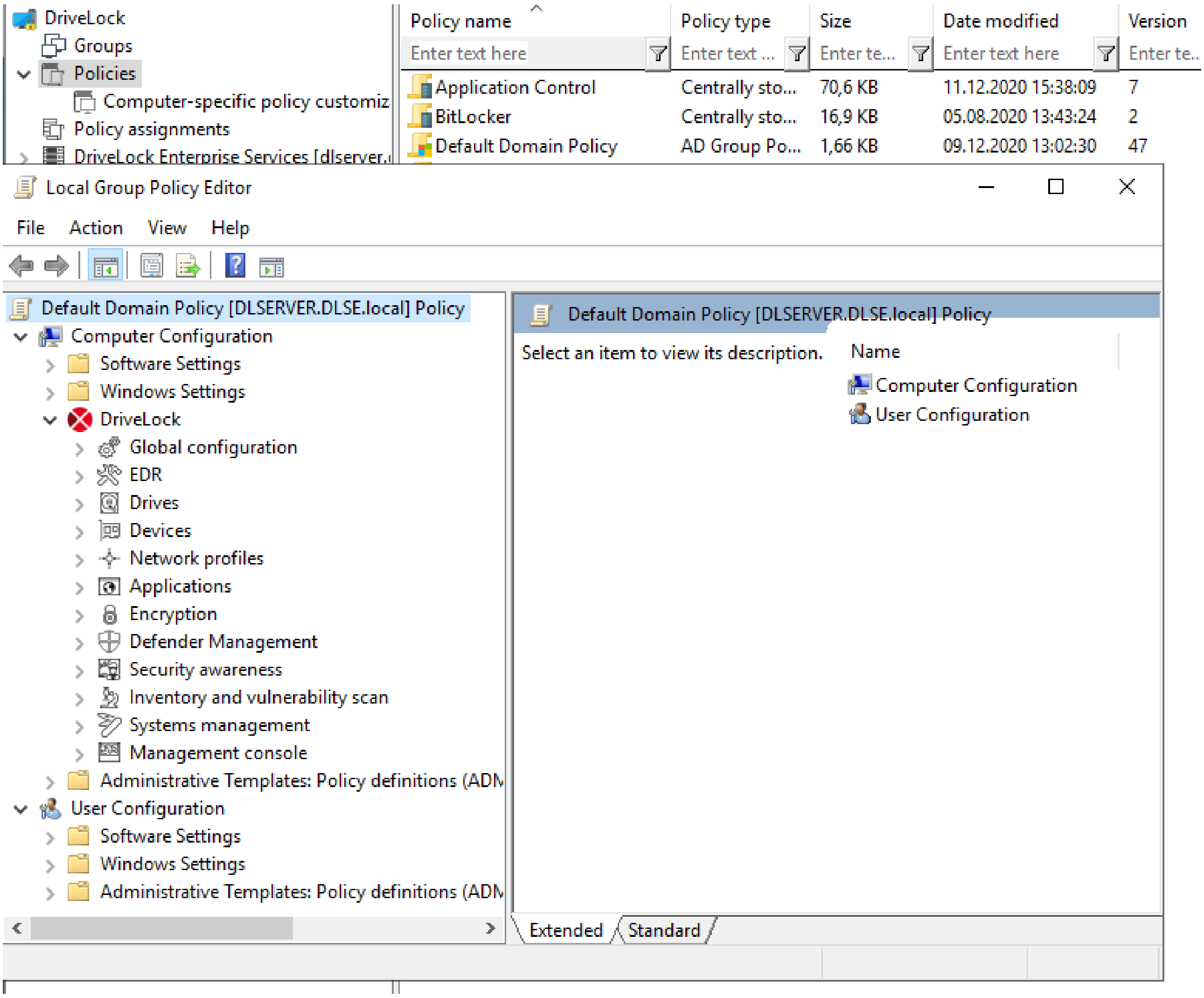
Another way of configuring the DriveLock Agent on multiple computers in a network is by using an Active Directory Group Policy. DriveLock can be configured by using the Group Policy Object Editor in conjunction with the DriveLock Management Console (MMC) snap-in. This snap-in is automatically installed as part of the DriveLock installation.

DriveLock can use Group Policy to deploy settings to computers that belong to an Active Directory domain. The DriveLock Agent running on these computers automatically applies all settings that are contained in the Group Policy Object.

In an Active Directory environment, computers are organized into organizational units (OUs) to implement common identical settings; it is therefore common practice to assign group policies - which include DriveLock settings - to OUs. Another reason for using OUs is the ability to delegate administrative tasks. Assigning GPOs to an OU instead of an entire domain or Active Directory site is a recommended practice because it allows you to maintain the appropriate protection level for each department or business unit.

To add existing or new Group Policies containing DriveLock settings, right-click Policies -> New -> Add Group Policy Object... to add the Group Policy to the MMC.

After that, select the appropriate GPO and click Edit. This opens a new window with the Microsoft GPO Editor where you can edit the settings.



Policy name	Policy type	Size	Date modified	Version
Enter text here	Enter text ...	Enter te...	Enter text here	Enter te..
Application Control	Centrally sto...	70,6 KB	11.12.2020 15:38:09	7
BitLocker	Centrally sto...	16,9 KB	05.08.2020 13:43:24	2
Default Domain Policy	AD Group Po...	1,66 KB	09.12.2020 13:02:30	47

The DriveLock snap-in shows the same objects in the console as in a local configuration.

Configuration changes are detected by the DriveLock Agent immediately after Windows applies the group policies. This can take up to 30 minutes after the policy is created. To apply policy changes immediately, a group policy update can be initiated. This is done by executing one of the following commands at the command line level (which can also be activated via agent remote control): `gpupdate /force`

4.2.4 Configuration files

Rather than using group policies or centrally stored policies, it is also possible to configure DriveLock centrally in non-Windows operating system environments (e.g. Novell NetWare).

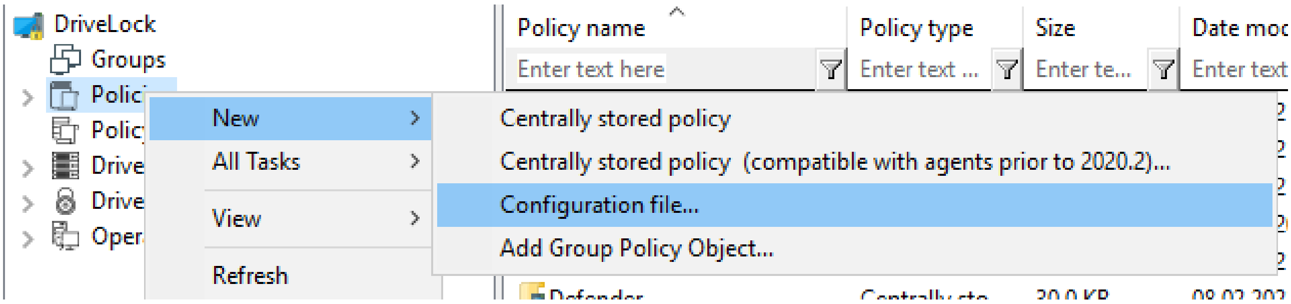
In system environments without Active Directory or a DriveLock Enterprise Service, DriveLock settings can be distributed using a configuration file. This file can be accessed on a central network drive using a UNC path or via HTTP/FTP.

Using configuration files is very similar to using group policies. However, user-specific configuration options are limited when Active Directory is not available as the central user database. You can still use local users or groups in your configuration settings. Also, you can use Novell eDirectory, if available.

You will need to configure the DriveLock Agent so that it gets its configuration settings from a configuration file. DriveLock includes a software distribution wizard that can create a customized MSI or MST file to do so.

For more information about using DriveLock in a Novell network, see the white paper "WP - DriveLock in Novell Environments.pdf" (available on request).

Right-click **Policies**, select **New** , and then **Configuration file...**.



DriveLock prompts you to provide the name and location of the new configuration file and then opens a new window, displaying the policy. You can configure policy settings in this window.

You can also export or import settings.

Warning: Remember to specify the license information in the global settings.

Note: You can transfer settings between a configuration file and other policy types by using the Import configuration and Export configuration commands.

To open an existing configuration file, right-click **Policies**, then select **All Tasks** and then **Open Configuration File....**. The configuration file appears on the right side.

Select the file and click Edit to open a new DriveLock Management console window.

Note: DriveLock Management console window automatically saves configuration changes when the window is closed

Once the settings are complete, you can make the configuration available by copying the configuration file to the central network share from which the clients obtain the settings.

The DriveLock Agent can access configuration files as follows:

- UNC: e.g. \\myserver\share$\drivelock\dlconfig.cfg
- FTP: e.g. myserver/pub/drivelock/dlconfig.cfg
- HTTP: e.g. http://myserver/drivelock/dlconfig.cfg

In environments without Active Directory (such as Novell NetWare), the location of the configuration file must be specified during agent installation.

> Note: You should create an initial configuration file before deploying the agents and specify the path of this file during the installation using command line or customized installation file.

DriveLock Agent reads the configuration file during installation and starts implementing the settings it contains.

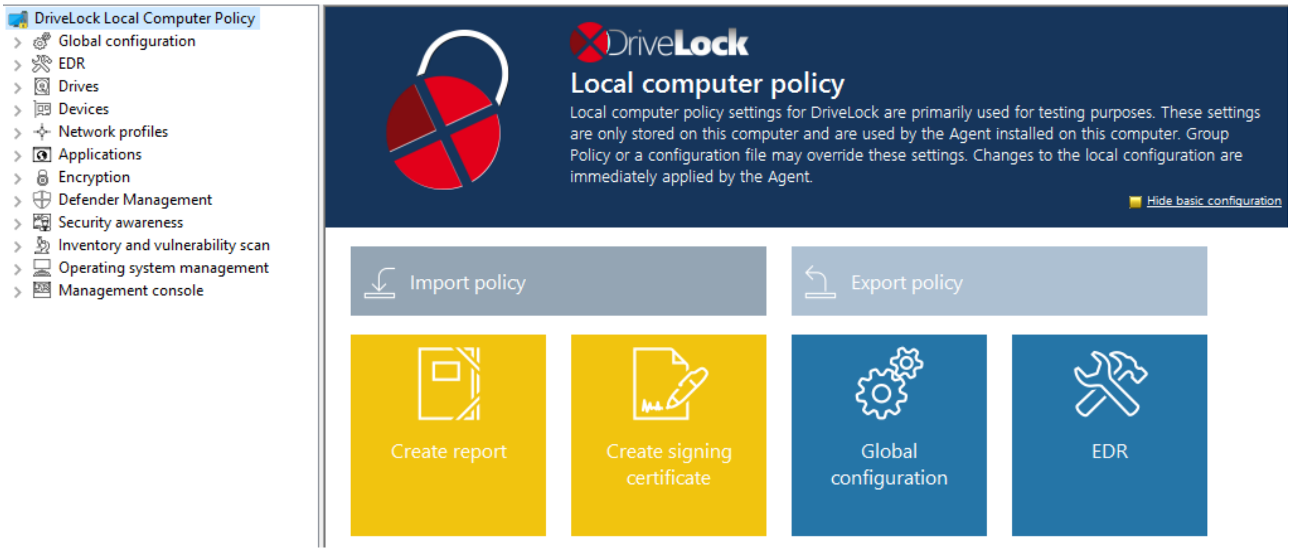
> Warning: When using configuration files, the agent checks them for changes only at startup and at specified intervals that can be defined.

When installing the DriveLock Agent, you must include the information from where the agent should load its configuration. The easiest way to accomplish this is by using the Deployment wizard. Open this wizard by right-clicking **Policies**, then **All Tasks** and then **Deploy configuration file...**.

4.2.5 Local configuration

A local configuration is applied only on the computer where the DriveLock Management Console is installed. Use it to test specific policy settings on a single computer with DriveLock Agent installed before deploying additional policies to more agents on your network.

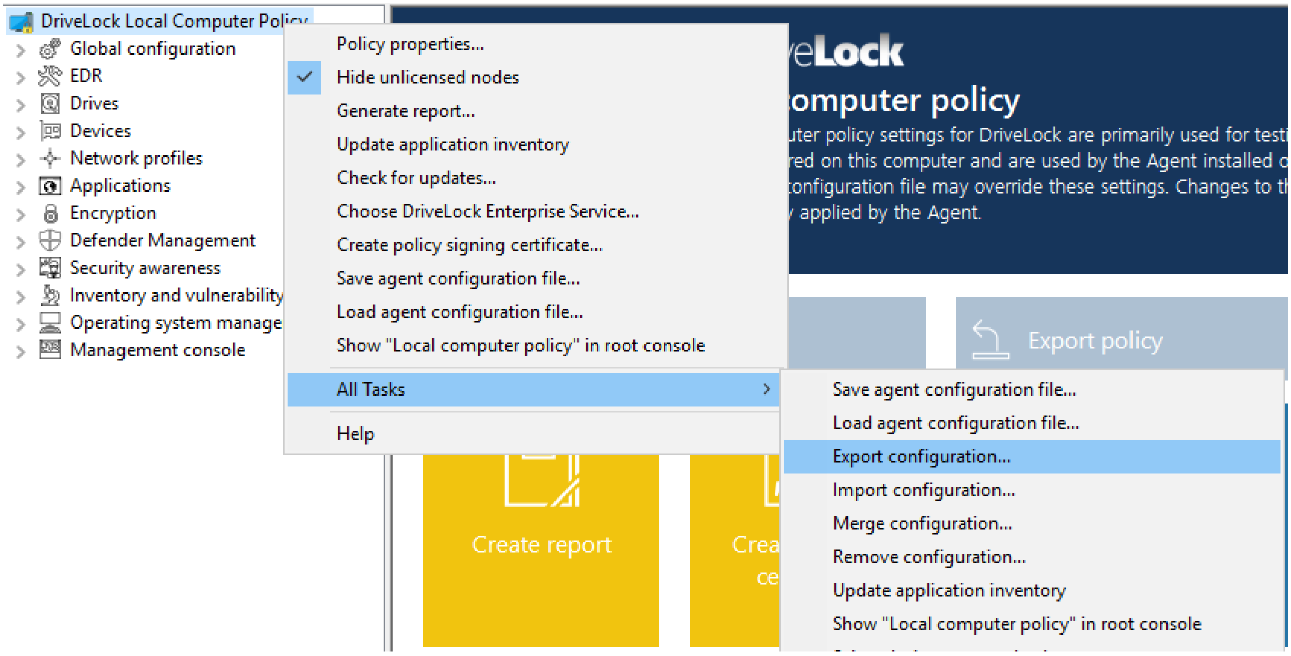
To configure the local settings, open the **Start menu** -> **All Programs** -> **DriveLock** and then select **DriveLock Local Policy**. The policy editor opens.



Local computer policy

Local computer policy settings for DriveLock are primarily used for testing purposes. These settings are only stored on this computer and are used by the Agent installed on this computer. Group Policy or a configuration file may override these settings. Changes to the local configuration are immediately applied by the Agent.

If you want to use the local configuration in another policy or back it up, it must first be exported to a file. Open the context menu of the topmost node and then select the **Export configuration...** menu command under **All Tasks**. Then specify a directory and file name and save the local configuration file. This has the extension .dlr.


DriveLock Local Computer Policy
Global configuration
EDR
Drives
Devices
Network profiles
Applications
Encryption
Defender Management
Security awareness
Inventory and vulnerability
Operating system manage
Management console
Policy properties...
Hide unlicensed nodes
Generate report...
Update application inventory
Check for updates...
Choose DriveLock Enterprise Service...
Create policy signing certificate...
Save agent configuration file...
Load agent configuration file...
Show "Local computer policy" in root console
All Tasks
Help
Save agent configuration file...
Load agent configuration file...
Export configuration...
Import configuration...
Merge configuration...
Remove configuration...
Update application inventory
Show "Local computer policy" in root console
eLock
omputer policy
Export policy
Create report

uter policy settings for DriveLock are primarily used for testi
red on this computer and are used by the Agent installed o
configuration file may override these settings. Changes to th
applied by the Agent.

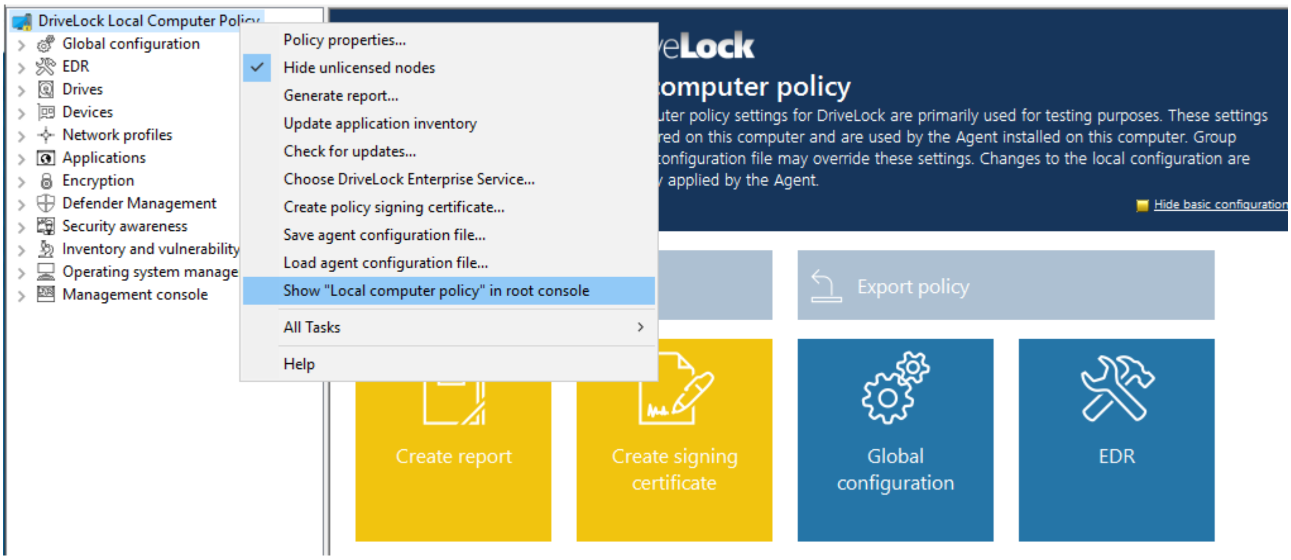
Note: You can also import a local configuration if, for example, you have previously exported a policy from a group policy and then imported it into a local DriveLock configuration.

Other options:

Save agent configuration file: This command creates an agent configuration file (.cfg). The file can be used to distribute a DriveLock configuration without group policies or deployed on a network that does not have Active Directory.

Remove configuration: Use this command to delete an existing DriveLock configuration (local or in group policies).

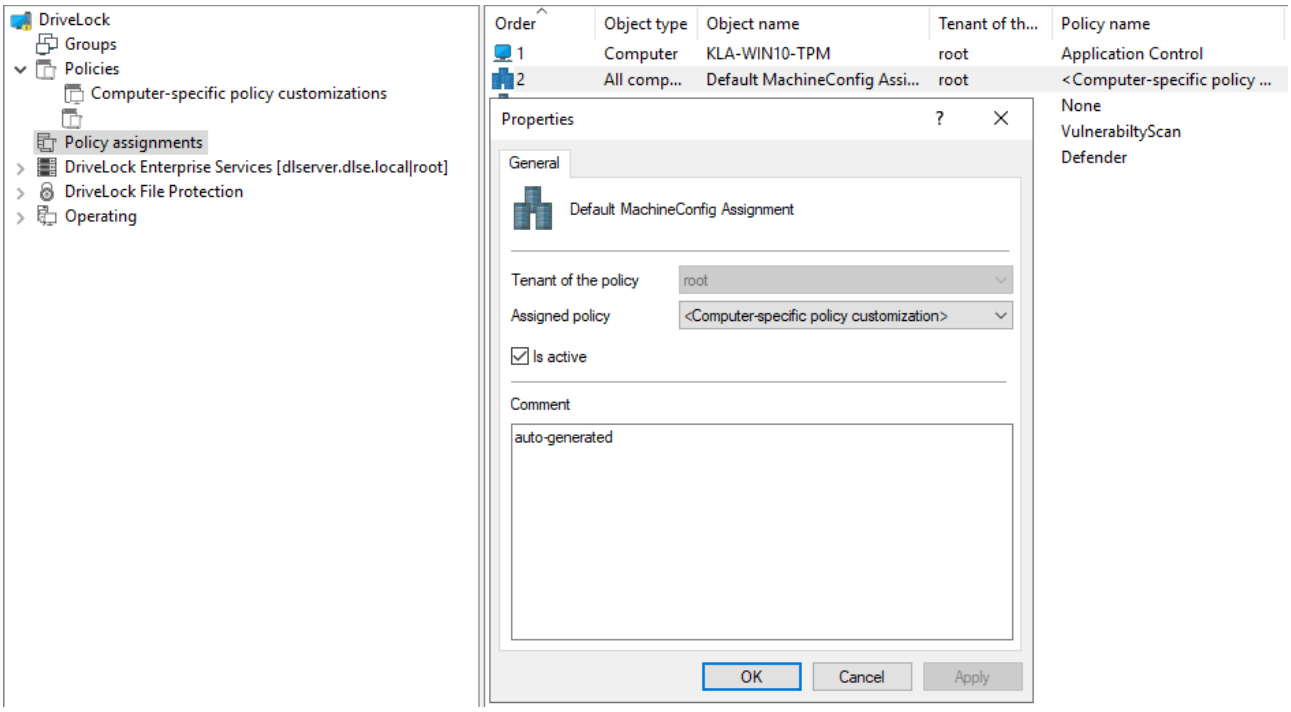
Show "Local computer policy" in root console: Select this option if you also want to display the settings of a local policy as a separate node in the DriveLock Management Console policy editor. This command is also available at the top level in the DMC in the context menu of DriveLock.



uter policy settings for DriveLock are primarily used for testing purposes. These settings red on this computer and are used by the Agent installed on this computer. Group configuration file may override these settings. Changes to the local configuration are applied by the Agent.

4.2.6 Computer-specific policy customizations

A Computer Specific Policy Adaptation (CPA) is technically a centrally stored policy that only contains settings for a single computer. However, unlike normal centrally stored policies, they are not assigned individually, but through a single policy assignment, the computer specific policy customization.



- DriveLock
  - Groups
  - Policies
    - Computer-specific policy customizations
  - Policy assignments
- DriveLock Enterprise Services [dlserver.dlse.local|root]
- DriveLock File Protection
- Operating

Order	Object type	Object name	Tenant of th...	Policy name
1	Computer	KLA-WIN10-TPM	root	Application Control
2	All comp...	Default MachineConfig Assi...	root	<Computer-specific policy ...
				None
				VulnerabiltyScan
				Defender

Properties

General

Default MachineConfig Assignment

Tenant of the policy: root

Assigned policy: <Computer-specific policy customization>

☑ Is active

Comment

auto-generated

- By default, this type of assignment is created with the name Default MachineConfig Assignment. It provides the CPA associated with each computer.
- CPAs are used, for example, for computer-specific BitLocker password settings. A CPA is automatically created as needed.
- CPAs are managed/displayed separately from other policies in their own node.
- CPAs also work if the DriveLock Agent is not configured to use centrally stored policies. In this case, the agent requires a configured server connection.

4.2.7 Permanent unlock policy

With this special type of centrally stored policy, you can quickly and easily unlock drives or block applications on DriveLock Agents from within the DriveLock Operations Center (DOC). This involves creating drive or application rules for various types of behavior and configuring them in the DOC.

In the DriveLock Management Console (DMC), the permanent unlock policy is displayed in the **Policies** node.

Properties

- A permanent unlock policy is automatically generated by the server when you create the first rule.
- Any change to rules creates a new version of the policy. It is automatically published.

- The server automatically generates a policy assignment for a permanent unlock policy when it is created. It is assigned to all computers, but may be changed if necessary.
- Make sure the priority of the assignment is higher than that of the applied policy.
- A permanent unlock policy applies only to the particular tenant. So there is only one policy per tenant.
- You can set the following permissions:
  - Manage rules: Create, modify and delete rules
  - Manage objects in rules: Add or delete managed objects in rules.
  - Read rules: Display the rule

Restrictions

- We recommend editing the rules in the DOC only. You can open the permanent unlock policy from the DMC as well. If you do so, please note that you will not be able to make any changes to the rules in the DOC.
- The rules can only be evaluated by DriveLock Agents running version 2020.2 or higher.
- When working with rules for users and computers, we recommend using groups.
- We recommend that you prepare a clear set of rules so that you can efficiently assign drives or applications to existing rules during operation.

4.3 Policy assignment

In the Policy assignments node, you specify the order in which your policies are assigned and the object they are assigned to. For more information, please visit here.

4.3.1 RSoP planning

The agent merges all policies assigned to it into a final policy (Resulting Set of Policies, RSOP) in the specified order.

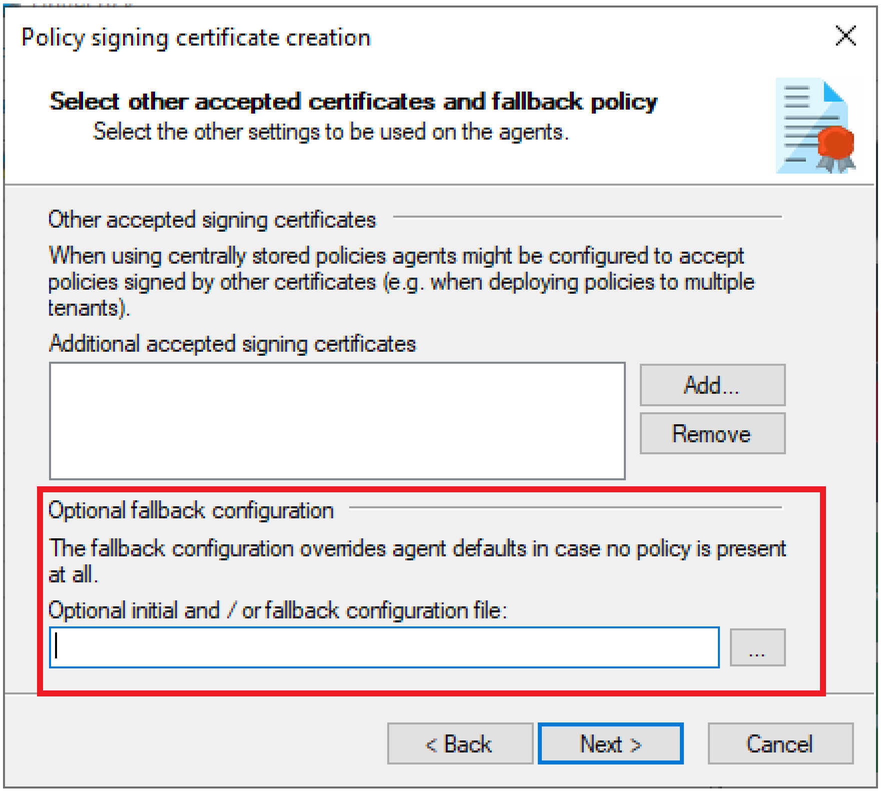
In the DriveLock Management Console (DMC)

If you want to evaluate an RSoP from the DMC as it is, open the **Policy assignment** node, then right-click and select **RSOP planning**. Specify a computer from your AD to display the RSoP.

Depending on the agent configuration, one of the following combinations is used for this (order of evaluation:)

1. Fixed policy (setting under Agent configuration, General tab, option Ignore policy assignments, use fixed policy) + computer specific policy assignment (CPA)

2. Policy assignments
3. Configuration file + computer specific policy assignment (CPA)
4. Local configuration + group policy object + computer specific policy assignment (CPA)
5. Fallback configuration file (special configuration file on an agent), setting during policy signing certificate creation, see figure:



Policy signing certificate creation

Select other accepted certificates and fallback policy

Select the other settings to be used on the agents.

Other accepted signing certificates

When using centrally stored policies agents might be configured to accept policies signed by other certificates (e.g. when deploying policies to multiple tenants).

Additional accepted signing certificates

Optional fallback configuration

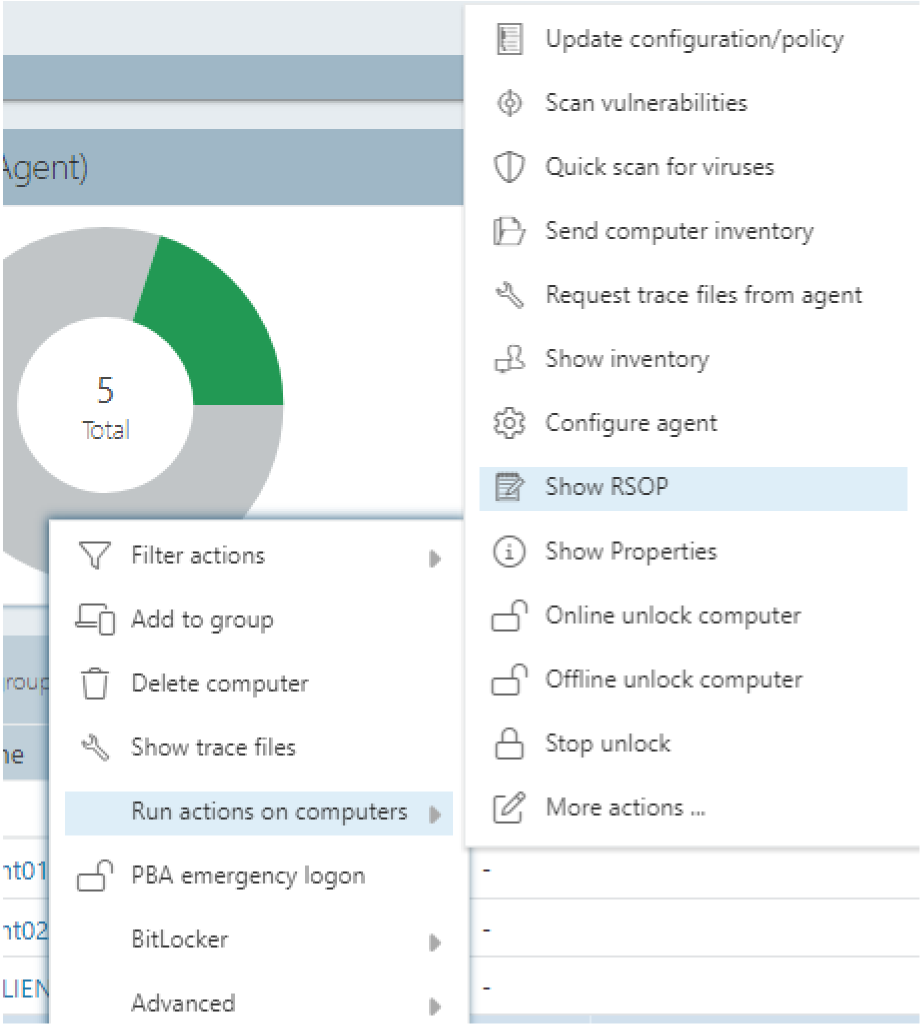
The fallback configuration overrides agent defaults in case no policy is present at all.

Optional initial and / or fallback configuration file:

You can view the RSoP via Agent remote control to see the policies that the agent has been using.

In the DriveLock Operations Center (DOC)

If you want to view an RSoP from the DOC, open the **Computers** view in the **Operations** menu and select a computer. Proceed as shown in the figure:



4.4 DriveLock Enterprise Services (DES)

4.4.1 Servers

DriveLock Enterprise Service is the central server component of a DriveLock installation. It is responsible for processing the events, which means that it accepts the DriveLock events created by the agents, adds them to the central database and links the events to each other using various boundary parameters. At the same time, it serves all DriveLock Agents and the DriveLock Management Console as an interface for database queries and for saving and loading important files (e.g. recovery keys).

For an overview of the DriveLock components and information on installation, refer to the DriveLock Installation documentation at DriveLock Online Help.

4.4.1.1 DES operating mode

You can operate the DriveLock Enterprise Service in different ways:

- as a central DriveLock Enterprise Service or
- as a linked DriveLock Enterprise Service (also referred to as Linked DES)

Typically, you will only install a single central DriveLock Enterprise Service in your system environment. Linked DriveLock Enterprise Services are only common in larger system environments (e.g. with multiple sites) or when installed by a Security Service Provider (SecaaS).

4.4.1.1.1 Central server

The first DriveLock Enterprise Service of an infrastructure is always a central server, with direct database connection. Each additional one is a linked DriveLock Enterprise Service that can only access the database via the central DriveLock Enterprise Service or forward events and data to it.

Since it takes some time to process the events, in this mode they are first written to a local cache and then to the database with a time delay. In this way, peak loads can be better absorbed. At the same time, this ensures that there are no bottlenecks in the processing of events, even in larger system environments (>20,000 clients).

The cache is set to 100,000 events by default. If the cache is filled, all further events are rejected by Agents. The Agent gets an appropriate feedback and tries again later to drop the events. Meanwhile, DriveLock Enterprise Service continues to write events to the database.

In the properties dialog of the server you can adjust the cache settings on the **Options** tab.

Note: When DriveLock Enterprise Service is stopped, the cache is written to the file`%PROGRAMDATA%\CenterTools DriveLock\SavedCache.db3` by default.

4.4.1.1.2 Linked servers

Linked servers are suitable especially for sites with poor Internet connections. They are directly connected to the central DES and can handle a large number of events. To save bandwidth, the events are transmitted to the DES

- in a compressed form and
- only at scheduled times.

A linked DriveLock Enterprise Service is also employed when installing and maintaining DriveLock by a Security Service Provider.

A linked server can perform the following tasks:

- Process events (all): forwarded to the central DriveLock Enterprise Service by schedule.
- Send agent alive status: forwarded to the central DriveLock Enterprise Service by schedule.
- Upload recovery data: data is immediately forwarded to the central DriveLock Enterprise Service
- Process inventory data from DriveLock agents: immediately forwarded to the central DriveLock Enterprise Service
- Get installation packages from central DriveLock Enterprise Service and deploy to agents
- Retrieve centrally stored policies from the central DriveLock Enterprise Service and deploy them to the agent
- Upload Active Directory group and user inventory data to the central DriveLock Enterprise service (see also Active Directory object inventory of a client)
- Receive agent remote connection requests from the central DriveLock Enterprise Service and forward them to the correct agent (agent remote proxy)

> Note: Processing inventory data from agents with an older DriveLock version is not possible.

You can specify how often the upload from the linked to the central DriveLock Enterprise Service should take place on the **General** tab in the properties dialog of the linked DES. By default, the upload occurs every hour.

On the **Options** tab (Number of events per batch upload (for linked servers) option), specify how many events you want to cache on the linked server before uploading to the central DriveLock Enterprise service. If this value is too high, it may take a long time for events to arrive at the central DriveLock Enterprise Service and become visible in the reporting. This means that if you only have a small remote office that receives a maximum of 10,000 events per day and you want to run a daily report, you will have to change this value from 20,000 to 10,000 or even 5,000.

> Note: Once the defined cache size has been reached, the cache is written by default in compressed form to the `%PROGRAMDATA%\CenterTools DriveLock\Storage` directory.

Note: By default, the central (receiving) DriveLock Enterprise Service stores the cache in the `%PROGRAMDATA%\CenterTools DriveLock\ReceivedStorage` directory.

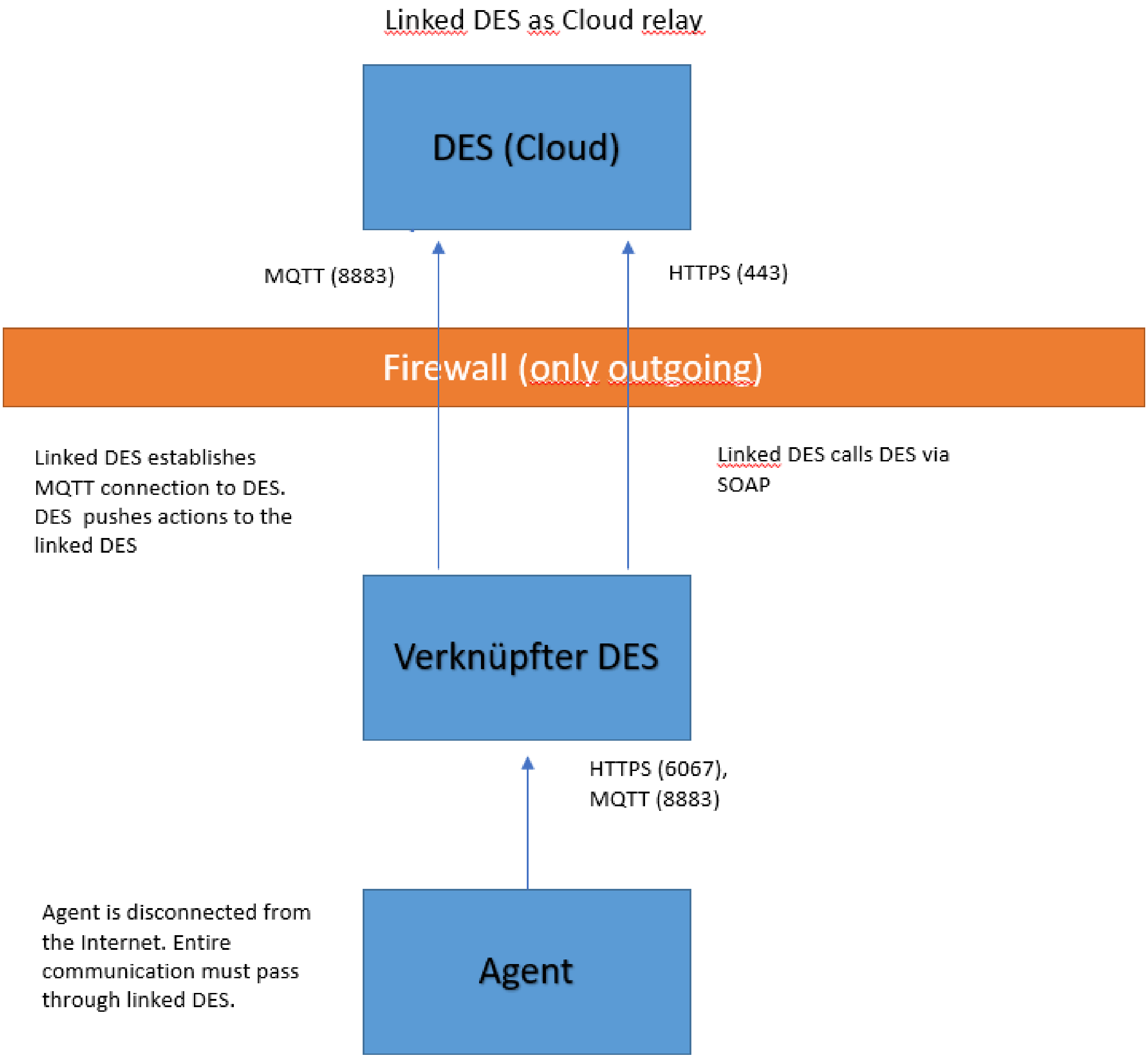
4.4.1.1.2.1 Linked DES for connection to the DriveLock Cloud

The linked DES in cloud mode acts as an intermediary to connect agents to the DriveLock Cloud when there is no internet connection.

It accomplishes three tasks in the process:

1. It forwards requests from the agents to the cloud
2. It caches data from the central DES
3. It provides an MQTT broker
    - Allows agents to be controlled remotely via agent control
    - Allows the central DES in the cloud to reach the linked DES

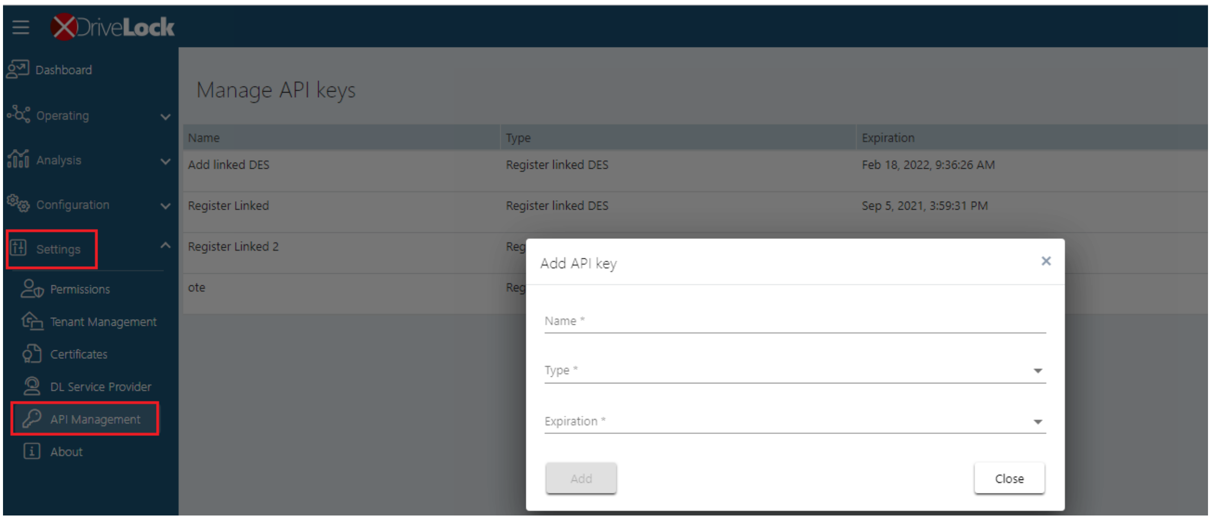
Network diagram:


Linked DES as Cloud relay
DES (Cloud)
MQTT (8883)
HTTPS (443)
Firewall (only outgoing)
Linked DES establishes MQTT connection to DES. DES pushes actions to the linked DES
Linked DES calls DES via SOAP
Verknüpfter DES
HTTPS (6067), MQTT (8883)
Agent is disconnected from the Internet. Entire communication must pass through linked DES.
Agent

4.4.1.1.2.2 Register linked DES as cloud relay

Follow these steps to register a linked DES:

1. Create an API key that allows the linked DES to be registered in the cloud tenant.
2. Open the **Settings** view in the DOC and then open **API Management**, as illustrated in the figure:



Manage API keys

Name	Type	Expiration
Add linked DES	Register linked DES	Feb 18, 2022, 9:36:26 AM
Register Linked	Register linked DES	Sep 5, 2021, 3:59:31 PM
Register Linked 2	Reg	
ote	Reg	

Add API key ×

Name *

Type *

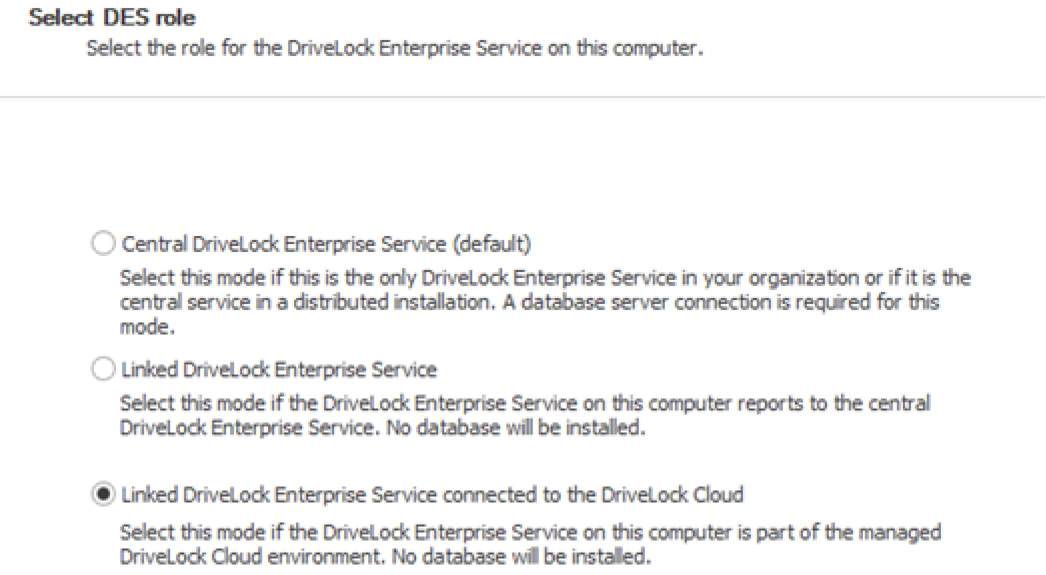
Expiration *

Add   Close

3. Create a new key of the type **Register linked DES.**.
4. The result is a long string (API key) that is used for authorization. The key must now be transferred to the linked DES in a secure way. Which method you choose is up to you.

> Note: Note that the key has an expiration date. This only means that you will no longer be able to register a linked DES with the cloud using the key when the expiration date is reached, but not that the linked DES will then no longer work. After use, keys can therefore also be deleted without hesitation.

5. Register the linked DES in the cloud in the database installation wizard.
6. To do this, open the Database Installation Wizard and select the **Linked DriveLock Enterprise Service** option there **to connect to the DriveLock Cloud**.



Select DES role

Select the role for the DriveLock Enterprise Service on this computer.

○ Central DriveLock Enterprise Service (default)

Select this mode if this is the only DriveLock Enterprise Service in your organization or if it is the central service in a distributed installation. A database server connection is required for this mode.

○ Linked DriveLock Enterprise Service

Select this mode if the DriveLock Enterprise Service on this computer reports to the central DriveLock Enterprise Service. No database will be installed.

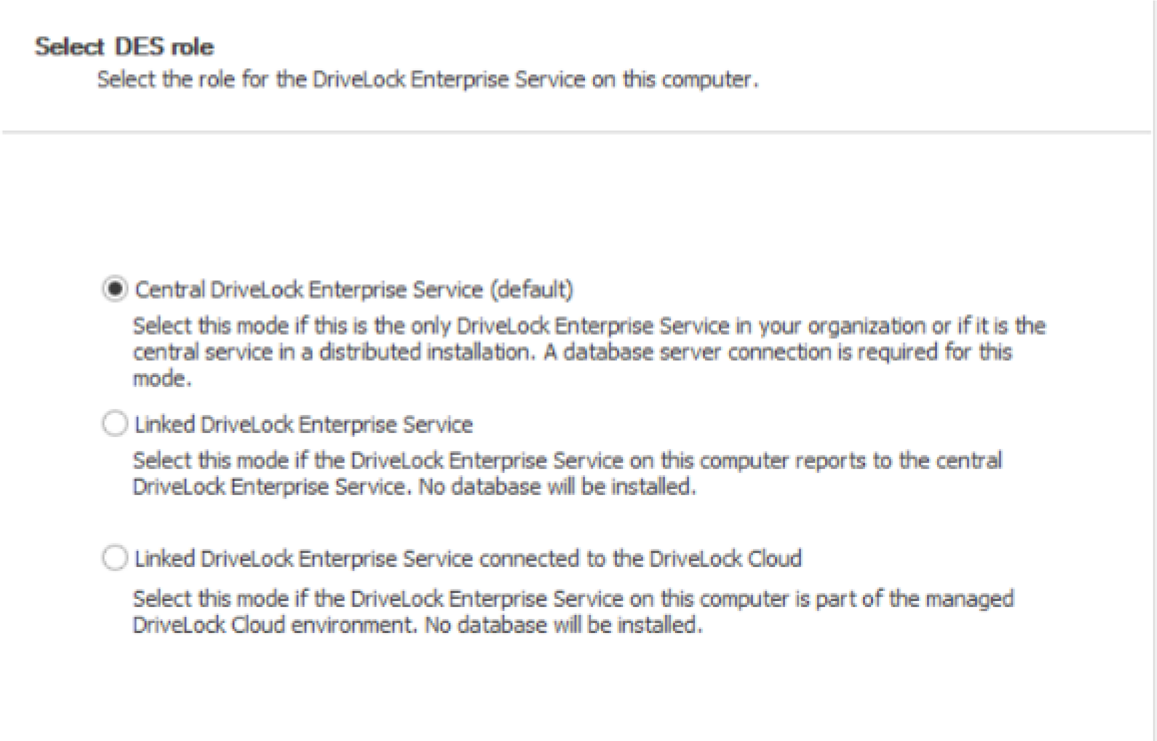
● Linked DriveLock Enterprise Service connected to the DriveLock Cloud

Select this mode if the DriveLock Enterprise Service on this computer is part of the managed DriveLock Cloud environment. No database will be installed.

7. In the next dialog, copy the API key into the text box.
8. Click **Register server**.

4.4.1.1.3 Changing the operating mode after installation

The operating mode is set up immediately after installing DriveLock Enterprise Service with the Database Installation Wizard. If you want to change the operating mode after installation, this wizard must be opened again:



Select DES role
Select the role for the DriveLock Enterprise Service on this computer.

● Central DriveLock Enterprise Service (default)
Select this mode if this is the only DriveLock Enterprise Service in your organization or if it is the central service in a distributed installation. A database server connection is required for this mode.

○ Linked DriveLock Enterprise Service
Select this mode if the DriveLock Enterprise Service on this computer reports to the central DriveLock Enterprise Service. No database will be installed.

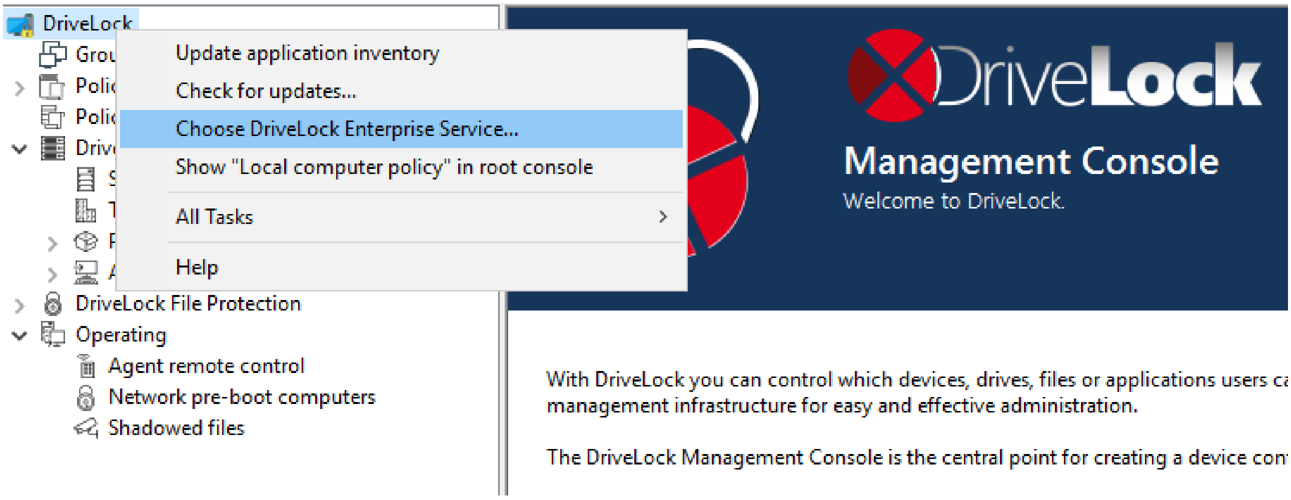
○ Linked DriveLock Enterprise Service connected to the DriveLock Cloud
Select this mode if the DriveLock Enterprise Service on this computer is part of the managed DriveLock Cloud environment. No database will be installed.

For example, select the second option **Linked DriveLock Enterprise Service** here. For more information on installing the DriveLock Enterprise Service, see the DriveLock Installation Guide at DriveLock Online Help.

4.4.1.2 Connecting to the DES

The DriveLock Management Console connects to the DriveLock Enterprise Service at various points to store information there (e.g. license data or centrally stored policies) or to retrieve data from the DriveLock Enterprise Service. First, you have to configure a connection to the DriveLock Enterprise Service in the DriveLock Management Console.

Either right-click **DriveLock** and select **Choose DriveLock Enterprise Service...** from the context menu.

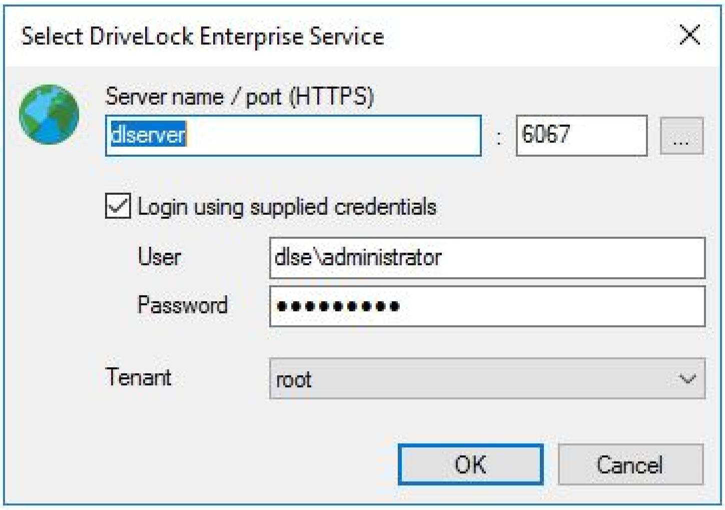

DriveLock
Grou
Polic
Polic
Driv
DriveLock File Protection
Operating
Agent remote control
Network pre-boot computers
Shadowed files
Update application inventory
Check for updates...
Choose DriveLock Enterprise Service...
Show "Local computer policy" in root console
All Tasks
Help
DriveLock
Management Console
Welcome to DriveLock.

With DriveLock you can control which devices, drives, files or applications users ca
management infrastructure for easy and effective administration.

The DriveLock Management Console is the central point for creating a device con

Or right-click **DriveLock Enterprise Services** and select **Choose DriveLock Enterprise Service...** from the context menu.

Next, enter the server name, tenant and your connection details.



Server name / port (HTTPS) dlserver : 6067

☑ Login using supplied credentials

User dlse\administrator

Password •••••••••

Tenant root

Note: When the DriveLock Management Console connects to the DES for the first time, it checks the DES certificate. For more information, see the Certificates chapter.

If the DriveLock Management Console has already found the DriveLock Enterprise Service via DNS-SD when it is started for the first time, then it is automatically listed. If not, enter the server name here. If you changed the default port when installing DriveLock Enterprise Service, you will also need to enter the new port here.

If you want to use an account other than your current one, you can enter a different account and password that the DriveLock Management Console will use to connect to DriveLock Enterprise Service.

> ❗ Warning: The user account used to connect to DriveLock Enterprise Service must also have the appropriate permissions. You can specify an authorized account/group either during the installation of DriveLock Enterprise Service (see DriveLock Installation Guide), or you can set it up later using the DriveLock Enterprise Service settings.

You can also specify which tenant data this connection connects to (this is only important if you are running a multi-tenant DriveLock environment).

4.4.1.2.1 Connection settings for proxy server

The DriveLock Management Console uses system proxy settings. An explicit proxy can be specified for some actions. For more information, please visit here.

4.4.1.2.1.1 Proxy settings on the DriveLock Agent

You can also set the proxy server settings directly on the agent. The two command line commands are used for this purpose:

- `drivelock -setproxy <proxytype>;<proxy>`
  - `<proxytype>` specifies the proxy type and can be named, pac, none or netsh
  - `<proxy>` contains either the proxy or the URL for the proxy auto-configuration file
- `drivelock -setproxyaccount <authscheme>;<proxyuser>;>proxypassword>`

Examples of use:

```
drivelock -setproxy name;myproxy:myport

drivelock -setproxy pac;//myhttpserver/myproxy.pac

drivelock -setproxy none

drivelock -setproxy netsh
```

If the proxy requires authentication, you can set the user and password with the `drivelock -setproxyaccount <authscheme>;<proxyuser>;>proxypassword>`

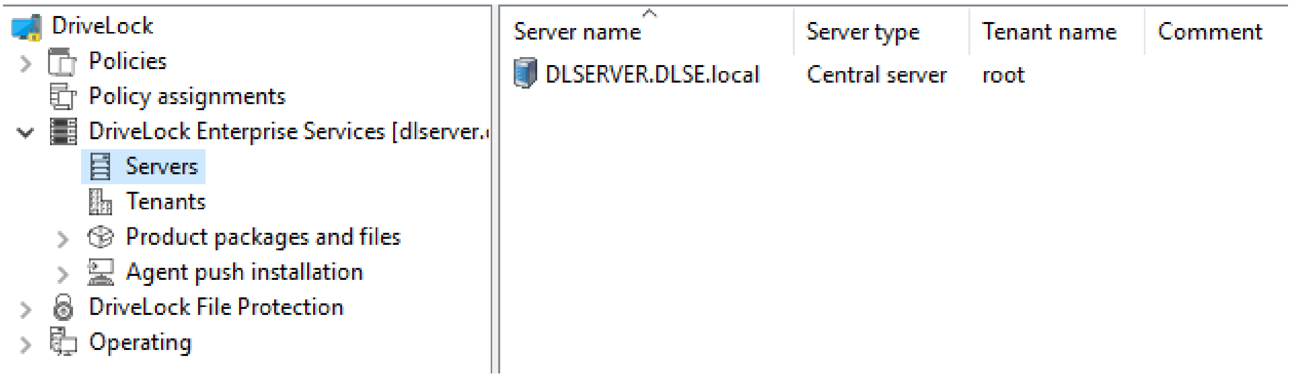
command. Here, `<authscheme>` is used to specify the authentication scheme (`basic, ntlm, passport, digest und negotiate`).

These settings are stored in the registry under the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriveLock\Parameters`. They are evaluated with priority, i.e. if a proxy has been set with the `drivelock -setproxy` command, all other settings are ignored.

Warning: Proxy settings that were specified when running the MSI (see the Installation Guide) or set with the `drivelock -setproxy` command can be deleted with `drivelock -removeproxy`.

4.4.1.3 Settings for the DES

In the **Servers** node, all registered DriveLock Enterprise Services are displayed:

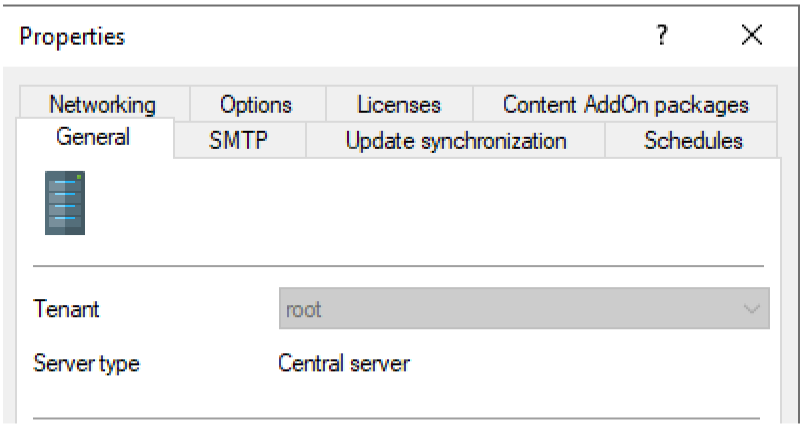

DriveLock
Policies
Policy assignments
DriveLock Enterprise Services [dlserver.
Servers
Tenants
Product packages and files
Agent push installation
DriveLock File Protection
Operating

Server name	Server type	Tenant name	Comment
DLSERVER.DLSE.local	Central server	root	

The **Server type** column shows which operating mode the server is running. Depending on its operating mode, you can configure different settings in the server's properties dialog.

Note: In this dialog you manage all settings related to the DriveLock Enterprise Service. The name of the DriveLock Enterprise Service corresponds to the server's computer name.

You can open the properties dialog by double-clicking the server name. See the following for information on the individual tabs.



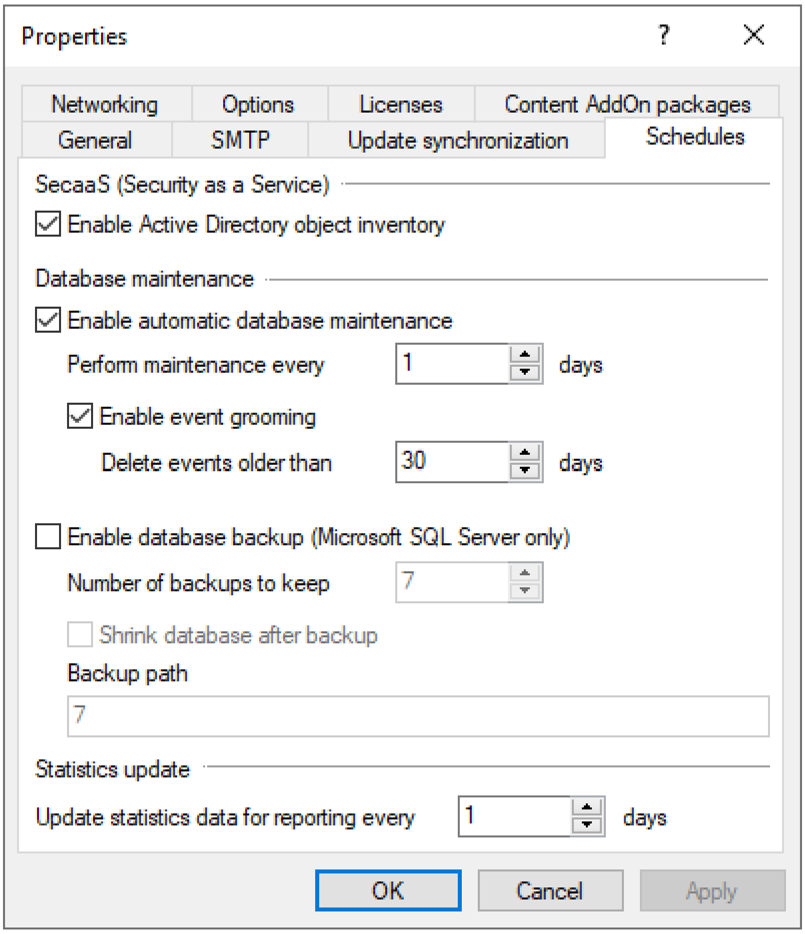
Tenant: root

Server type: Central server

4.4.1.3.1 Planned tasks

Database maintenance is used to limit data growth and maintain indexes on table columns to ensure best possible performance even with large data volumes.

Note: We recommend that you configure the database maintenance options in DriveLock Enterprise Service only if you are using SQL Server Express version (e.g. MSDE 2000, SQL2005 Express, SQL2008 Express). When using the full version of SQL Server, we recommend that you set database maintenance manually on the server. For more information, please contact our support or refer to the Database Guide under Technical Articles at DriveLock Online Help.



SecaaS (Security as a Service)

☑ Enable Active Directory object inventory

Database maintenance

☑ Enable automatic database maintenance

Perform maintenance every 1 days

☑ Enable event grooming

Delete events older than 30 days

□ Enable database backup (Microsoft SQL Server only)

Number of backups to keep 7

□ Shrink database after backup

Backup path

7

Statistics update

Update statistics data for reporting every 1 days

To limit SQL database growth, DriveLock Enterprise Service may automatically delete old events. Note to set database cleanup if you do not need to run reports or forensic analysis on old data, or if you archive your SQL data with a third-party tool.

To enable database cleanup, click **Enable automatic database maintenance** and select the maximum age of events. This option must be disabled if you have manually set up a maintenance job on the SQL server.

By default, all events older than 30 days are automatically deleted on a daily basis.

he maintenance of the indexes on the table columns is also turned on using the **Enable automatic database maintenance** option. This optimizes the search. Note to disable this option if you have manually set up a maintenance job on the SQL server.

By default, database maintenance is performed automatically on a daily basis.

The **Enable Active Directory object inventory** option is described here.

4.4.1.3.1.1 Collecting Active Directory object inventory

A DriveLock Enterprise Service is capable of reading all users, computers, groups and OU information from the current Active Directory (that is, the same domain the DriveLock Enterprise Service user account belongs to) as an AD object inventory and storing it in the DriveLock database so that it can be used within a DriveLock configuration.

Use this option especially when you want to create a DriveLock configuration for DriveLock Agents with permissions for users or groups from another domain.

If you start the DriveLock Management Console from a computer located in the same domain as the one you are creating the configuration for, it is not necessary to read the users and groups from the Active Directory, as the DriveLock Management Console can access this data directly. However, even in this case, the AD object inventory can be used for configuration and can lead to a performance advantage over direct access, especially in larger AD environments.

To allow a DriveLock Enterprise Service to create an Active Directory object inventory, you must first enable this option in the DriveLock Enterprise Service settings.

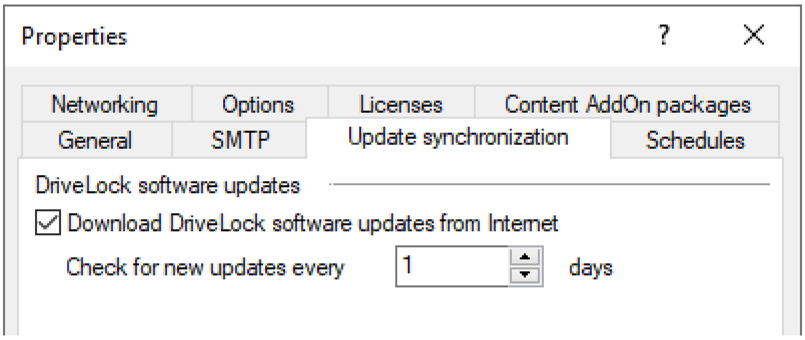
Since the **Enable Active Directory object inventory** option is enabled by default, DriveLock Enterprise Service automatically determines all users and groups in the current domain once every 24 hours and synchronizes them with the data stored in its database. The data is also stored separately for each tenant, if you have created more than one tenant.

Once an AD object inventory is available, it can be used during configuration within the DriveLock Management Console.

Here you can activate the option to automatically load the AD object inventory. If you want this process to take place automatically once a day, activate the corresponding option here as well. The time of the last successful upload process is also displayed.

4.4.1.3.2 Update synchronization

You can use the synchronization settings to determine whether and how often the DriveLock Enterprise Service checks for new DriveLock software packages via an Internet connection.



DriveLock software updates

☑ Download DriveLock software updates from Internet

Check for new updates every 1 days

4.4.1.3.3 Networking

You can configure network settings for the central DES and for linked DriveLock Enterprise Services. They can be viewed and changed on the **Networking** tab.

One of the basic DriveLock Enterprise Service settings is the port used by the service for receiving data or queries.

Note: This port can also be configured in other places in the DMC. The certificate for the DES is also associated with the port!

The **External URL** refers to the address that is given to the client as the server address, for example, during push installation. It must be the same as the server address in the policy.

By default, events are transmitted between DriveLock Agent and DriveLock Enterprise Service encrypted. For this reason, the **Enforce HTTPS** option is set by default.

This setting has to be configured consistently and should be set to the same value for all DriveLock Enterprise Services.

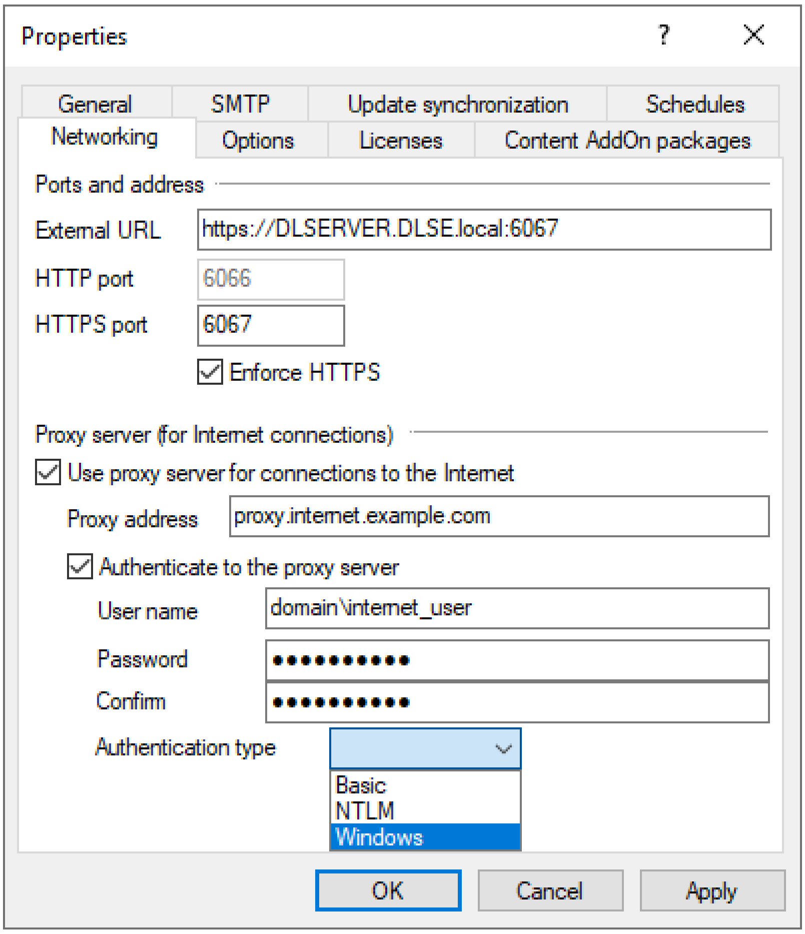
Warning: When you change the default ports, you also need to change them in the DriveLock policy for the agents, at: Advanced Configuration - Global Settings - Server Connections.

Continue to proxy server settings.

4.4.1.3.3.1 Using proxy servers

An Internet connection is required for the automatic update. If access to the Internet is only possible via a proxy server, this has to be configured for each DriveLock Enterprise Service.

The following options are available:



Properties

General | SMTP | Update synchronization | Schedules
Networking | Options | Licenses | Content AddOn packages

Ports and address

External URL: https://DLSERVER.DLSE.local:6067

HTTP port: 6066

HTTPS port: 6067

☑ Enforce HTTPS

Proxy server (for Internet connections)

☑ Use proxy server for connections to the Internet

Proxy address: proxy.internet.example.com

☑ Authenticate to the proxy server

User name: domain\internet_user

Password: ●●●●●●●●●●

Confirm: ●●●●●●●●●●

Authentication type: Basic / NTLM / Windows

- **Use proxy server for connections to the Internet**: The proxy server specified here will be used to access the Internet. It may be necessary to specify a port separated by ":", e.g.: proxy.internal.example.com:8080
- **Authenticate to the proxy server**: Must only be specified if anonymous access via the proxy is not possible.
- **User name**: A user who is allowed to access the Internet through the proxy. If necessary, the domain must also be specified, e.g.: domain\internet_user
- **Password**: The password that matches the user.
- **Authentication type**: Different authentication types are provided for authentication to the proxy server. The proxy server must support the option selected here:
  - **Basic**: User and password are transmitted in plain text
  - **NTLM**: The user specified there is used for Internet access. The password is transmitted encrypted.
  - **Windows**: Windows integrated login, the service account from DriveLock Enterprise Service is used for Internet access (and not the user specified in the dialog).

4.4.1.3.4 SMTP

The e-mail server settings are used for sending reports. For this purpose, the corresponding server is specified in the **SMTP server** text box. The default port is 25.

In case the SMTP server demands a login for sending internal emails, the data required for this can be specified in the User name and Password section.

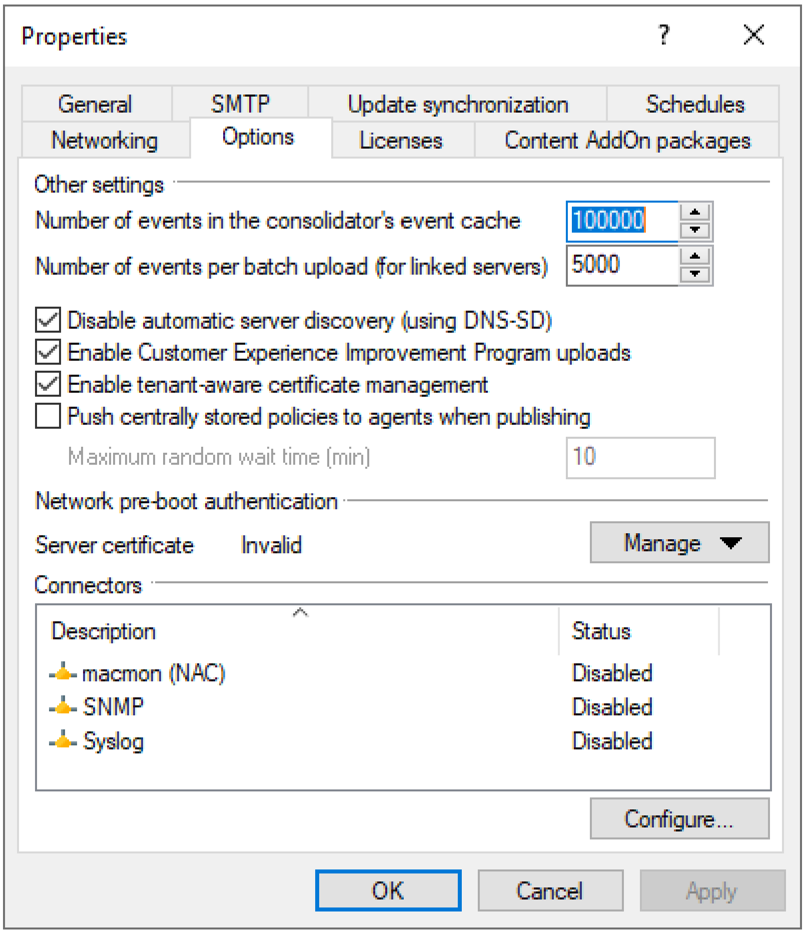
You can also specify the sender name and the sender email address. Usually an internal email address must be used as email address.

4.4.1.3.5 Content AddOn packages

On this tab you can specify whether and how often the DriveLock Enterprise Service checks for new Security Awareness Content Addon packages when connected to the Internet.

4.4.1.3.6 Options

On the **Options** tab, we recommend that you use the default settings.



Other settings

Number of events in the consolidator's event cache: 100000

Number of events per batch upload (for linked servers): 5000

☑ Disable automatic server discovery (using DNS-SD)
☑ Enable Customer Experience Improvement Program uploads
☑ Enable tenant-aware certificate management
☐ Push centrally stored policies to agents when publishing

Maximum random wait time (min): 10

Network pre-boot authentication

Server certificate: Invalid

Connectors

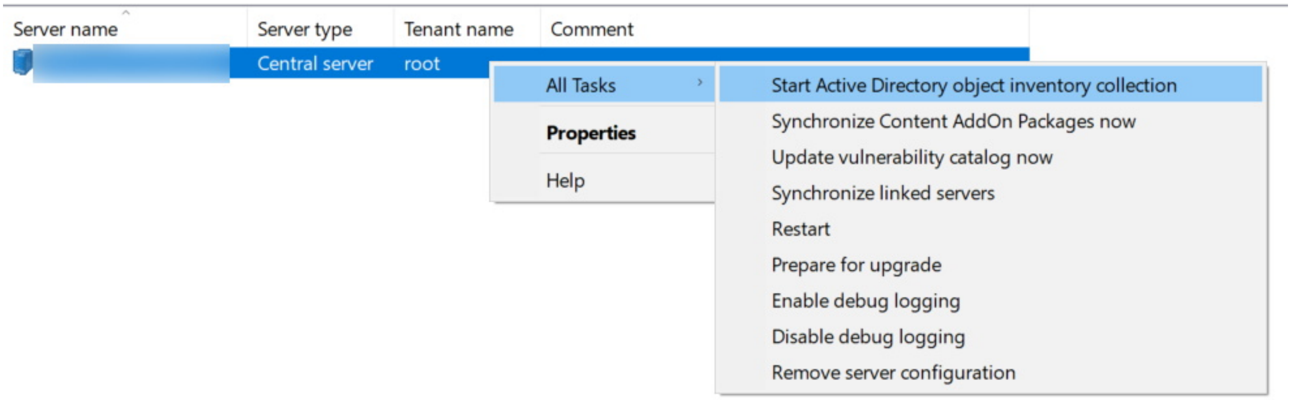
Description	Status
macmon (NAC)	Disabled
SNMP	Disabled
Syslog	Disabled

Options in detail:

- If you enable **Customer Experience Improvement Program**, statistical data about the speed and frequency of used features will be collected, anonymized and uploaded to DriveLock. This helps to further improve the product. No personal or personally identifiable information is stored or transmitted. You can uncheck the option if you do not want to participate in the program or do not want any data uploaded to DriveLock.
- Agents update their policies every 30 minutes by default. Enabling the **Push centrally stored policy to agents when publishing** option will perform a faster policy update on the agent.

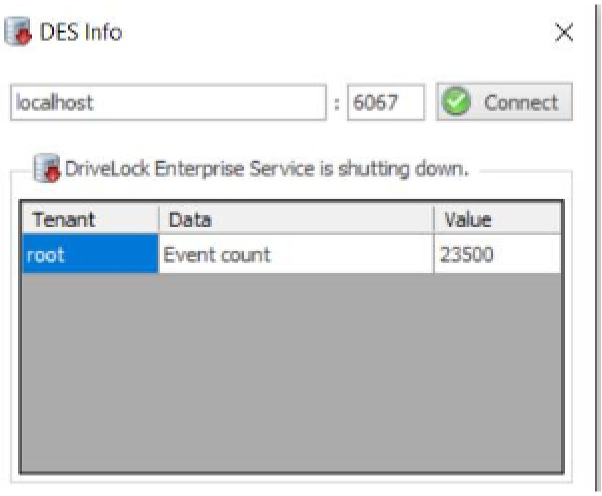
4.4.1.4 Starting manual actions for the DES

Open the DES context menu and select **All Tasks**. This provides you with the following options:


Server name
Server type
Tenant name
Comment
[redacted]
Central server
root
All Tasks
Properties
Help
Start Active Directory object inventory collection
Synchronize Content AddOn Packages now
Update vulnerability catalog now
Synchronize linked servers
Restart
Prepare for upgrade
Enable debug logging
Disable debug logging
Remove server configuration

1. **Start Active Directory object inventory collection**: The DriveLock Enterprise Service automatically determines all users and groups in the current domain once every 24 hours and synchronizes them with the data stored in its database.
2. **Synchronize Content AddOn packages now**: If you are using Security Awareness, you can use this command to update the data on purchased AddOn packages and then download them to the DES. For more information, see the Security Awareness documentation at DriveLock Online Help.
3. **Update vulnerability catalog now**: If you are using DriveLock Vulnerability Scanner, you can use this command to have the vulnerability catalogs updated. For more information, see the Vulnerability Scanner documentation at DriveLock Online Help.

4. **Synchronize linked servers**: Select this command if you want to synchronize miscellaneous data (policies, security awareness packages, and agent installation packages) on all linked DES to the central DES.
5. **Restart**: The DES will be restarted. If you are using linked DES, you can restart them without direct access.
6. **Prepare for upgrade**: The DES will stop communicating with the DriveLock agents and will not accept any more data. First, the events are processed and the DES is stopped and restarted. We recommend this procedure in large environments. You can get an overview via the taskbar icon:



localhost : 6067

DriveLock Enterprise Service is shutting down.

Tenant	Data	Value
root	Event count	23500

7. **Enable** or **disable** debug logging: Use this command to enable or disable detailed debug information in the log files. The change is active immediately and does not require restarting the service.
8. **Remove server configuration**: This command deletes the complete server configuration. his is useful, for example, if you want to remove servers that are not in use.

4.4.1.5 DES status

You can monitor and check the availability of the DriveLock Enterprise service via the DES taskbar icon. If the service is not available, it will be displayed in red. During service startup, it may take a few minutes for the status to change to green.

Double-click on the icon to open the detailed view.

You can see different connection information like the address, database server, database type, database name or its version.

Right-clicking on the icon opens a context menu that allows you to quickly restart the DriveLock Enterprise Service or perform actions useful for support.

4.4.2 Tenants

DriveLock and the DriveLock Enterprise Service support using multiple tenants. A tenant is a completely separate database containing all data belonging to that tenant. Multi-tenancy is this logical and physical separation of several different tenants. A DriveLock Agent can be associated with one tenant at a time.

This is based on the following concept: A central DriveLock Enterprise Service is operated by a system provider who manages several small customer installations. Each customer has a linked DriveLock Enterprise Service installed and is connected to the central DriveLock Enterprise Service of the system provider. Each customer installation runs its own tenant. This keeps the data separate and ensures different access rights so that no customer can see another customer's reports.

In order to associate events to a particular tenant, you can set up a dedicated linked DriveLock Enterprise Service for each tenant:

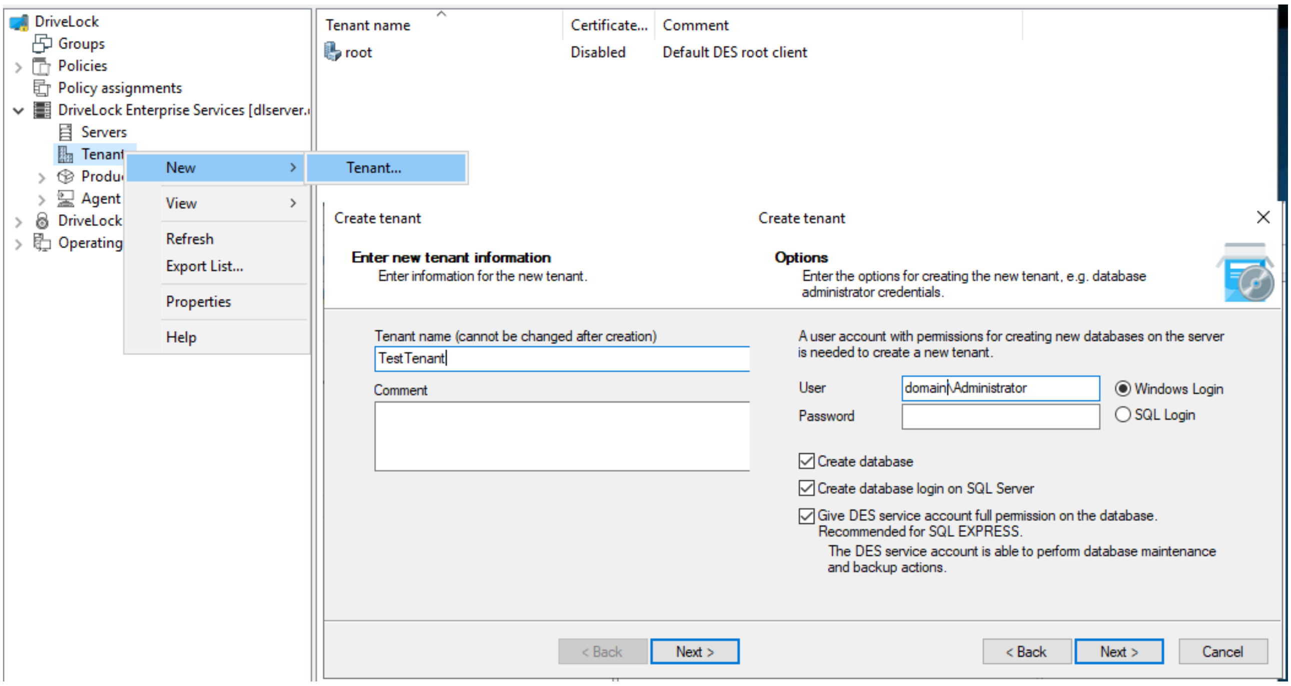
- Server1 (central DES, default tenant "root")
- Server2 (linked DES to Server1, default tenant "B")
- DriveLock Agents (server link to Server2, tenant "B").

The default tenant of a server can be assigned via the DriveLock Management Console - DriveLock Enterprise Services - Server - <select server> - right-click Properties - Tenant.

4.4.2.1 Creating or deleting a tenant

The default root client is created automatically once you have completed the installation of the DES and the databases.

To create another tenant, right-click on Tenants in the DriveLock Enterprise Services node and select New and then Tenant.



Create tenant

Enter new tenant information
Enter information for the new tenant.

Tenant name (cannot be changed after creation): TestTenant

Comment

Create tenant

Options
Enter the options for creating the new tenant, e.g. database administrator credentials.

A user account with permissions for creating new databases on the server is needed to create a new tenant.

User: domain\Administrator

● Windows Login
○ SQL Login

Password

☑ Create database

☑ Create database login on SQL Server

☑ Give DES service account full permission on the database. Recommended for SQL EXPRESS.
The DES service account is able to perform database maintenance and backup actions.

Specify a name for the new tenant. It must not contain any special characters or umlauts. The maximum length of the name is limited to 50 characters.

You can configure the installation settings here in a similar way to the installation of the DriveLock database.

Select the users or groups that have already been configured to access the DriveLock Enterprise Service and choose the ones that need to have access to the tenant data stored in the DriveLock Management Console.

The new database is now created on the database sever directly.

Note: Once you are finished creating the tenant, a new database <root name>_<tenant name> is created, where the <root name> is the database name that was specified when installing the DriveLock Enterprise Service. By default, this is DRIVELOCK.

Deleting a tenant

To delete a tenant, right-click the tenant in the DriveLock Enterprise Services node - Tenants, and then click **Delete tenant**.

Note: This will not delete the tenant's database. Make sure to delete it manually.

4.4.2.2 Assigning DriveLock Agents to a tenant

By default, a DriveLock Agent is assigned to the default tenant **root**. If you want to use a different tenant, be sure to specify this during installation. For more information, refer to the Installation instructions at DriveLock Online Help.

You can also change the assignment of an agent to a tenant later through Agent remote control or command line commands.

4.4.3 Product packages and files

4.4.3.1 Product update

You can access the DriveLock installation packages that are managed locally or available online in the DriveLock Management Console (DMC) in the **Software packages** subnode located in the **DriveLock Enterprise Services**, **Product packages and files** node.

Updates to DriveLock components are managed on the DES. The DES can download DriveLock packages when an Internet connection is available. Alternatively, in offline environments, the packages can be deployed manually.

Cloud sourced packages have been published by DriveLock and can be added to the local management. You will be notified about new packages when starting the DMC. Packages with source DES are available locally and can be managed and published.

You can save the installation package locally for further use by right-clicking and selecting Download or you can display more details about it by selecting Properties.

> Note: To ensure that updates run as smoothly as possible, we recommend that you update the servers and management components first and then the agents.

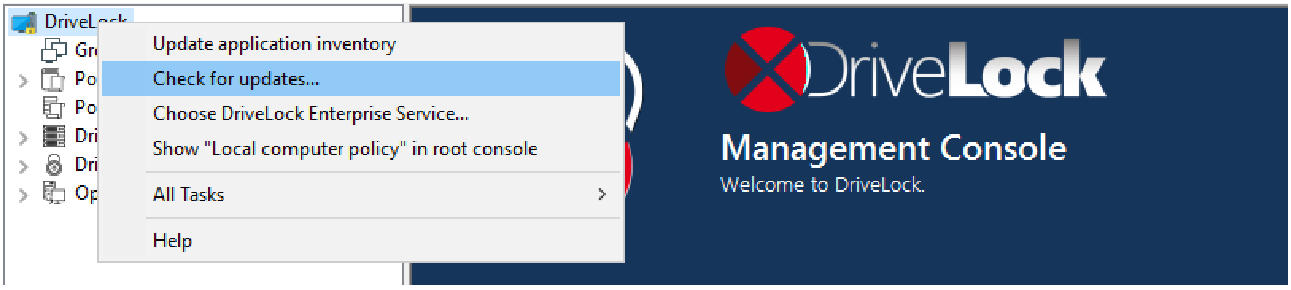
Using the context menu **Download to DES** for a package that has the source **Cloud**, you can add new packages to your configuration.

Using the context menu on the **Software packages** subnode, you can show or hide the packages from the cloud and manually upload packages to the DES to include them in the configuration. This is required for offline systems, for example.

Each package is provided with a publication status, so that an update is only possible from newer package versions.

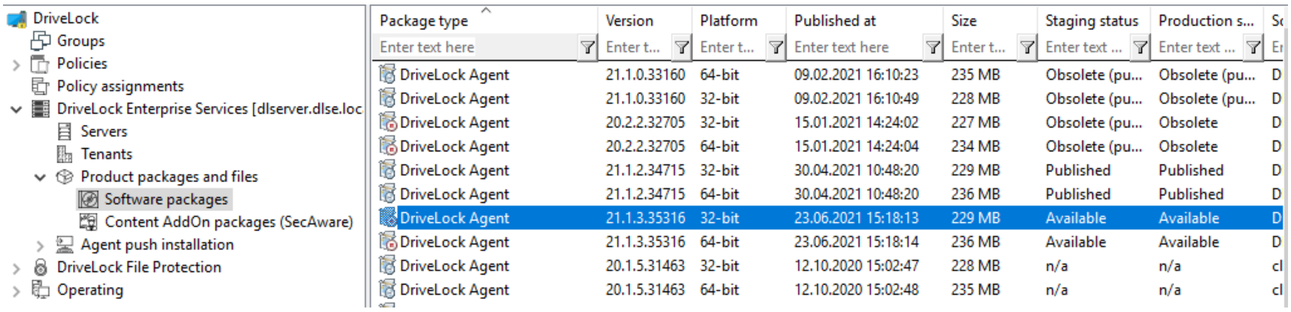
4.4.3.2 Check for updates

Right-click **DriveLock** and select **Check for updates....**.


DriveLock
Gr
Po
Po
Dri
Dri
Op
Update application inventory
Check for updates...
Choose DriveLock Enterprise Service...
Show "Local computer policy" in root console
All Tasks
Help
DriveLock
Management Console
Welcome to DriveLock.

The application will now connect to the DriveLock website and check for a new version. If available, a corresponding message and information about the new version will be displayed. You can also specify here how often to automatically check for updates.

Another way to check the latest published version is in the navigation pane in the **DriveLock Enterprise Services** node under **Product packages and files** in the **Software packages** subnode:


DriveLock
Groups
Policies
Policy assignments
DriveLock Enterprise Services [dlserver.dlse.loc
Servers
Tenants
Product packages and files
Software packages
Content AddOn packages (SecAware)
Agent push installation
DriveLock File Protection
Operating

Package type	Version	Platform	Published at	Size	Staging status	Production s...	Sc
Enter text here	Enter t...	Enter t...	Enter text here	Enter t...	Enter text ...	Enter text ...	Er
DriveLock Agent	21.1.0.33160	64-bit	09.02.2021 16:10:23	235 MB	Obsolete (pu...	Obsolete (pu...	D
DriveLock Agent	21.1.0.33160	32-bit	09.02.2021 16:10:49	228 MB	Obsolete (pu...	Obsolete (pu...	D
DriveLock Agent	20.2.2.32705	32-bit	15.01.2021 14:24:02	227 MB	Obsolete (pu...	Obsolete	D
DriveLock Agent	20.2.2.32705	64-bit	15.01.2021 14:24:04	234 MB	Obsolete (pu...	Obsolete	D
DriveLock Agent	21.1.2.34715	32-bit	30.04.2021 10:48:20	229 MB	Published	Published	D
DriveLock Agent	21.1.2.34715	64-bit	30.04.2021 10:48:20	236 MB	Published	Published	D
DriveLock Agent	21.1.3.35316	32-bit	23.06.2021 15:18:13	229 MB	Available	Available	D
DriveLock Agent	21.1.3.35316	64-bit	23.06.2021 15:18:14	236 MB	Available	Available	D
DriveLock Agent	20.1.5.31463	32-bit	12.10.2020 15:02:47	228 MB	n/a	n/a	cl
DriveLock Agent	20.1.5.31463	64-bit	12.10.2020 15:02:48	235 MB	n/a	n/a	cl

Here you can see the most recent DriveLock installation packages available at the moment and download them immediately and individually from the context menu of an item.

You can also see the latest Security Awareness packages that can be downloaded via the DriveLock Enterprise Service (DES) in the **Content AddOn Packages (SecAware)** subnode. If you have a license for the Security Awareness Content AddOn, you will see all modules, if not, you will see the modules that you can use for demo purposes. For more information, see the Security Awareness documentation at DriveLock Online Help.

4.4.3.3 Staging and production environment

All DriveLock Agents are assigned to the production environment by default. Individual agents can be assigned to a staging environment to update and test new product versions independently of the production environment.

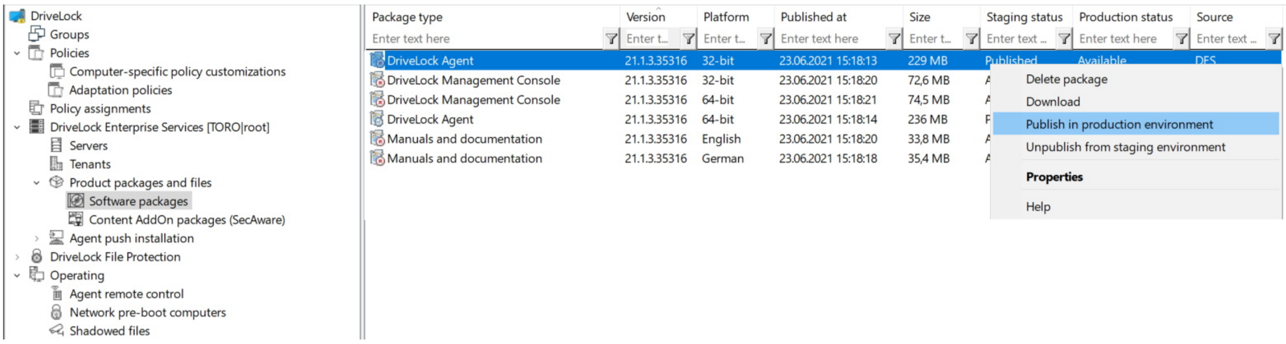
In the software packages overview, you can publish the packages in the staging or production environment.

You can configure the environment (staging or production) for the agent as follows:

- Via an option in the agent remote control
- By applying a command line command directly on the agent
- `drivelock.exe -setstaging`: Assigns the client to the staging environment
- `drivelock.exe -setproduction`: Assigns the client to the production environment (default)

The publishing status affects the version of DriveLock to be deployed or installed.

A change takes effect on all DES servers. Publishing is carried out for each product, version and platform.


DriveLock
Groups
Policies
Computer-specific policy customizations
Adaptation policies
Policy assignments
DriveLock Enterprise Services [TORO|root]
Servers
Tenants
Product packages and files
Software packages
Content AddOn packages (SecAware)
Agent push installation
DriveLock File Protection
Operating
Agent remote control
Network pre-boot computers
Shadowed files
Delete package
Download
Publish in production environment
Unpublish from staging environment
Properties
Help

Package type	Version	Platform	Published at	Size	Staging status	Production status	Source
Enter text here	Enter t...	Enter t...	Enter text here	Enter t...	Enter text ...	Enter text here	Enter text ...
DriveLock Agent	21.1.3.35316	32-bit	23.06.2021 15:18:13	229 MB	Published	Available	DES
DriveLock Management Console	21.1.3.35316	32-bit	23.06.2021 15:18:20	72,6 MB	A		
DriveLock Management Console	21.1.3.35316	64-bit	23.06.2021 15:18:21	74,5 MB	A		
DriveLock Agent	21.1.3.35316	64-bit	23.06.2021 15:18:14	236 MB	P		
Manuals and documentation	21.1.3.35316	English	23.06.2021 15:18:20	33,8 MB	A		
Manuals and documentation	21.1.3.35316	German	23.06.2021 15:18:18	35,4 MB	A		

The staging and production status can be one of the following:

- Published: Clients will download the package and install the update.
- Downloaded: Package has been downloaded to the DriveLock Enterprise Service but is not available to clients.
- Obsolete (downloaded): Package has been downloaded to the DES but is superseded by a newer package. The package is not available to clients.
- Obsolete (published): Package has been downloaded to the DES but is superseded by a newer package. The package is still available to clients until the newer version is published.

Right-click on a package to start one of the following actions or to publish or unpublish:

- Delete package: Remove the package from the DES. You can only delete packages that are not currently published.
- Download: Download the package to the DES. Once the package has been downloaded, you need to publish it to make it available to clients.
- Publish in staging / production: Make the package available to the staging or production environment.

- Unpublish from staging / production: Make the package unavailable to clients in the staging or production environment.

4.4.4 Agent push installation

Use the DriveLock push installation to manually or automatically install the DriveLock Agent on end users' client computers (target computers).

To perform push installation, the DriveLock Enterprise Service (DES) periodically checks that all computers from the configured AD groups / OUs have a DriveLock Agent installed. On computers where DriveLock is not installed yet, the administrator can go to the DriveLock Operations Center (DOC), select Configuration and then Deployment and start the installation manually.

When using automatic push installation, you can configure the DriveLock Agent installation to work for configured AD groups and OUs. The DES determines the associated computers from the AD and triggers the push installation for computers that do not yet have DriveLock.

The administrator can also trigger the manual push installation from the DOC for individual computers independently of AD groups / OUs.

To do a push installation, the DriveLock Update Service (DlUpdSvc) is copied to the computer via administrative access, then it is installed and started. Next, the DlUpdSvc retrieves the currently released installation package via the DES and performs the agent installation.

Note: The push installation will only start if both 32-bit and 64-bit versions of the DriveLock Agent are available in the software packages published in the test and production environment.

4.4.4.1 Requirements for the push installation

The following conditions must all be met for the push installation to work:

- The agent installation packages for 32-bit and 64-bit operating systems must be available on the DES and published in the correct environment (production/staging).
- The target computer must be accessible on the network, DNS must be working.
- The admin$ share of the target computer must be accessible.
- File and print sharing must be enabled on the target computer.
- The account used for push installation must have administrator privileges on the target computer.

Note: Note that the push installation will only work if the server running the DES also supports the correct version of SMB. This may not be enabled on current Windows Server versions and must be installed later if required.

4.4.4.2 Global settings per server

The global settings for push installation are configured independently for each DES. This allows you to easily keep the settings separate for different organizational units within a company.

The following settings are available on the General tab:

- **Enable synchronization with Active Directory**: the DES will determine the associated computers via the configured AD groups. Computers without DriveLock Agent can be selected and installed in the DriveLock Operations Center (DOC).
- **Enable automatic push deployment**: computers that are detected without a DriveLock Agent will be installed automatically.

By default, both settings are enabled.

- **Account for installation**: the account must have administrative privileges on the local computer.
- **Install in staging environment**: if enabled, the computers being installed will be assigned to the staging environment.
- **Force reboot after installation**: if enabled, the computers will be rebooted after the installation of the agent without further prompt.
- **Configuration type**: select the type of policy the computers are configured with.

4.4.4.3 Automatic push groups / OUs

You can select the computer groups or OUs from the AD where you want to use the automated or automatic push installation here.

Open the subnode's context menu, select **New** and then **Group...** or **Organizational unit...**, depending on what you want to create.

4.4.4.4 Performing a push installation (DOC)

You can start a new (manual) push installation in the DriveLock Operations Center (DOC) by opening the **Configuration** view and selecting the **Agent installation** tab in the **Deployment** menu.

Computer selection: Here you can specify multiple computers for manual push installation.

Options: This is where the agent installation packages currently used for the push installation and their versions for the staging and production environment are listed. They are managed in the DMC as software packages in the DriveLock Enterprise Service node under Product packages and files.

You can specify the following additional options:

User account for installation: the user must have administrative privileges on the local computer.

Force reboot after installation: if enabled, the computer will be rebooted after the installation of the agent without prompting.

Force removal of installed DriveLock Agents: only use this option after consulting DriveLock Support, if a previous DriveLock installation failed and the agent can no longer be uninstalled properly.

Agent configuration: Here you can configure a proxy that will be used by the update service to download the installation package from the DES. This is also used for the agent configuration.

Configuration type: Select the type of policy used to configure the computers here.

4.4.4.5 Automatic update

The automatic update also needs to be configured for the DriveLock Agent in a policy.

In your policy, open **Global configuration**, then the **Settings** subnode and select **Automatic updates**.

4.5 Operating

4.5.1 Agent remote control

DriveLock allows you to connect to a remote computer that already has a DriveLock Agent installed and running. This is useful, for example, if you want to allow temporary access to a drive class on a remote computer or to check the current status of your agents. You can also display inventory data that has been previously collected, for example, or start a hardware and software inventory manually.

DriveLock uses HTTPS protocol by default to connect to remote computers. To connect to a remote computer, DriveLock must be installed on the remote computer. To connect to a computer, incoming connections from TCP port 6065 and the "DriveLock" program must be allowed in the firewall settings. The HTTP protocol with port 6064 is not recommended.

Using the quick configuration via DNS-SD, the MMC lists all neighboring DriveLock Agents under the remote agent control. By default, all DriveLock Agents are directly provided by the DriveLock Enterprise Service.

Warning: You must define permissions in order to perform remote control actions on DriveLock Agents. These are defined in the Agent remote control settings and permissions.

Agent remote control is not available when you use the Group Policy Editor to edit a DriveLock group policy. With a locally installed DriveLock Management Console, you can use agent remote control and connect to DriveLock agents configured via group policy, for example.

4.5.1.1 Agent remote control properties

To view the Agent remote control properties, right-click the **Agent remote control** node and then select **Properties**.

The **Retrieve agent computer list from DriveLock Enterprise Service** option is set by default.

If the **Retrieve agent list using DNS-SD** option is selected, the list is determined dynamically and only contains clients that are online.

You can use the **Display as offline when last contact was more than ... minutes ago** option to define the time interval after which a DriveLock Agent is marked as offline. Default is 15 minutes.

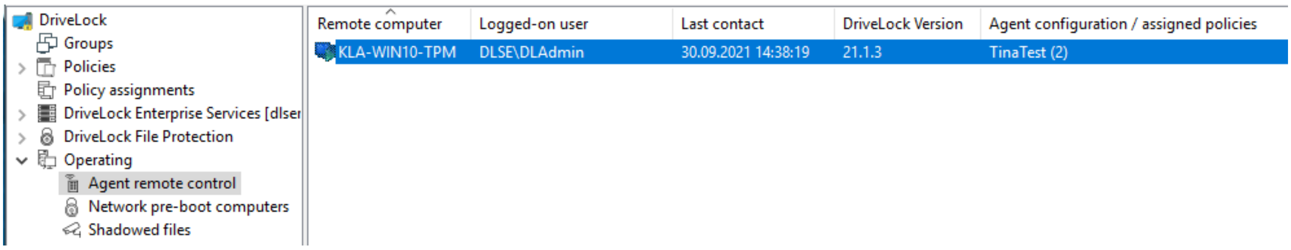
The **Use remote control trough DriveLock Enterprise Service (proxy)...** options control the behavior of the DriveLock Management Console when connecting to a DriveLock Agent via remote agent control:

- **Always** : DriveLock Management Console connects exclusively through DriveLock Enterprise Service.
- **Never**: DriveLock Management Console only connects directly without going through DriveLock Enterprise Service.
- **On demand**: The DriveLock Management Console first tries to reach the DriveLock Agent directly. If this attempt fails, a connection via the DriveLock Enterprise Service is tried.

A connection via a DriveLock Enterprise Service as a proxy is only relevant if the DriveLock Agents are not located in the same corporate network and are connected to the central DriveLock Enterprise Service via a linked DriveLock Enterprise Service (as is the case with a Security Service Provider - SecaaS).

4.5.1.2 Show active DriveLock Agents

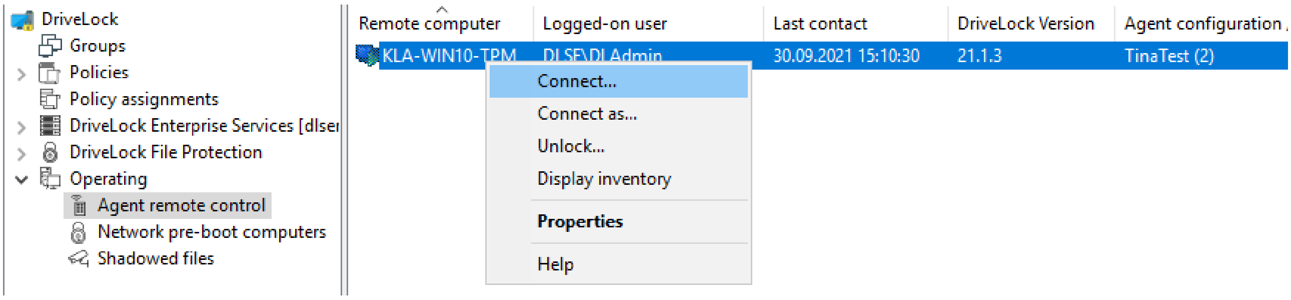
By default, the DriveLock Management Console displays all client computers it could find in the environment in the**Agent remote control** section of the **Operating** node. This works with the help of DNS-SD.


DriveLock
Groups
Policies
Policy assignments
DriveLock Enterprise Services [dlser
DriveLock File Protection
Operating
Agent remote control
Network pre-boot computers
Shadowed files

Remote computer	Logged-on user	Last contact	DriveLock Version	Agent configuration / assigned policies
KLA-WIN10-TPM	DLSE\DLAdmin	30.09.2021 14:38:19	21.1.3	TinaTest (2)

4.5.1.3 Connect to a DriveLock Agent

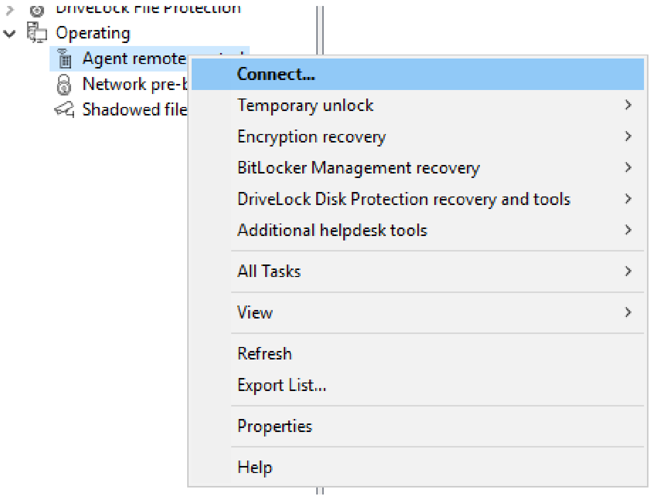
Before you can execute any tasks on a DriveLock Agent, you must first connect to it. The easiest way to do this is to select the agent, then right-click and choose **Connect** from the context menu:

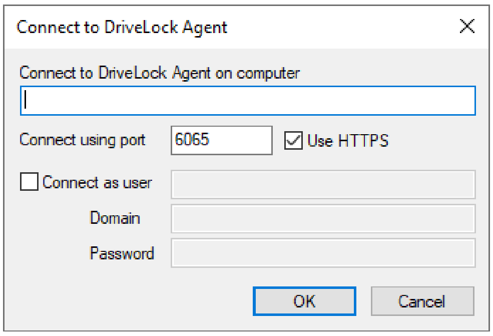


Remote computer	Logged-on user	Last contact	DriveLock Version	Agent configuration ,
KLA-WIN10-TPM	DLSE\DLAdmin	30.09.2021 15:10:30	21.1.3	TinaTest (2)

This option automatically uses port 6065 and HTTPS.

Alternatively, right-click on the **Agent remote control** node to select **Connect** and then enter the computer name or IP address.




Connect to DriveLock Agent

Connect to DriveLock Agent on computer

Connect using port: 6065 ☑ Use HTTPS

☐ Connect as user

Domain

Password

Note: To connect to a remote computer, you must allow incoming connections from TCP port 6064 and 6065 (default) and the DriveLock program in the firewall settings.

After a connection is established, you can read out the current configuration and control the DriveLock Agent.

Context menu entry: Connect as...

To use a different port for communication between the DriveLock agent and DES, select the **Connect as**... menu command in the context menu of the Drivelock Agent.

To ensure that the connection with the agent is encrypted, the **Use HTTPS** option is set by default. If necessary, enter the required user data in the dialog.

4.5.1.4 Show properties of the DriveLock Agent

You can display all DriveLock Agent properties, for example the connected drives and devices, temporary unlock, encryption or application control status by double-clicking the client computer.

Note: In the Properties dialog, different tabs are displayed depending on the licenses that are valid for the agent. For example, the **Application Control** tab is only visible if you have also licensed this DriveLock module.

On the **Drives** tab you can see all the drives currently connected to the computer and their current state. Select a drive and click the **Details** button to view more information, such as the whitelist rules applied, or the file filters currently active on the drive.

On the **General** tab you can update the agent configuration by clicking the **Refresh policy...** button. Clicking the **Unlock temporarily...** button will open the Unlock Wizard. For more information on how to unlock, click here.

On the **Encryption** tab, you will find a detailed list of the (licensed) encryption modules you are using and their properties. You will also see a listing of the encrypted drives with their respective encryption status.

For more information on the respective tabs, please refer to the corresponding chapters in this manual or the respective documentation at DriveLock Online Help.

4.5.1.5 Read out the client configuration (RSoP)

To view the current configuration (RSOP = Resultant Set of Policy) of a remote agent, right-click the remote computer and select **Show RSOP...** from the context menu.

After that, an extra console window will open, which looks like the DriveLock Policy Editor in terms of its structure. To check which settings work on the agent, expand the corresponding node and select the setting.

> Note: The settings can only be read but not changed.The settings can only be read but not changed.

Click **Generate report** to generate a report that displays all settings similar to a report from GPMC. With CTRL + F you can search in the HTML view.

4.5.1.6 Display inventory data

To view the current inventory data of a computer, right-click the computer and select **Display inventory** from the context menu. You will then see all of the computer's software and hardware data.

The data source indicates whether the information was read directly from the computer (if you are connected to it directly via the remote agent control), or whether the data was read from the DriveLock database via the DriveLock Enterprise Service.

Click the required tab to display the associated information, for example, information about the installed applications or the Windows updates that have been installed.

4.5.1.7 Show encryption properties

Similar to the Encryption tab in the agent's properties dialog, the status of the encryption option used is displayed here.

On the **General** tab you have the following options:

Click the **Details** button if you want to view information about the TPM used (if available).

Click **Reconfigure agent** if you want to make changes to the agent's encryption or pre-boot authentication settings. You can configure computer-specific settings in the dialog that opens, which may be different from the ones in the central policy. However, the selected settings apply only to the currently connected computer. For more information, see the DriveLock Encryption documentation at DriveLock Online Help.

Click **Re-upload recovery key** if there is no recovery data for the agent on the DriveLock Enterprise service. This option manually uploads the local data to the server.

On the **Users** tab, you can see which users can log in to the client computer using pre-boot authentication (if PBA is available there). Click **Add** to add other users.

4.5.1.8 Show local application control whitelist

If you have purchased a license for Application Control, you can use this command to display the contents of the application database containing the applications released for this DriveLock agent with the corresponding hash values. Likewise, you can see the certificates used. The information can be copied, if necessary.

4.5.1.9 Enabling debug tracing

You can activate detailed logging on the DriveLock Agent to help you troubleshoot any issues. This process is called tracing. Tracing allows DriveLock technical support to determine the cause of an issue, for example, in the event that settings are not being applied as expected. It is best to enable tracing only for troubleshooting purposes and disable it again once you have collected the data.

Right-click the target computer, then select **All Tasks** and then **Debug tracing** to enable tracing for the selected computer. A message pops up confirming that tracing has been successfully enabled and indicating the path where the trace files are stored.

4.5.1.10 Unlocking DriveLock Agents temporarily

Using temporary unlocking, you can quickly and temporarily allow a connected DriveLock Agent to access locked drives, devices or applications and/or disable Microsoft Defender control.

This also works for multiple DriveLock Agents.

Example: you have locked all USB drives by default, but an end user needs immediate access to their USB drive so they can show their presentation. Using agent remote control, the user gets access to their USB drive within minutes.

Please do the following:

1. Either click the **Unlock temporarily** button in the agent's properties dialog or the menu command **Unlock temporarily...** from the context menu. If you want to unlock multiple agents, open the menu command **Unlock multiple agents...** in the context menu of the **Agent remote control** node using the **Temporary unlock...** menu command.
2. The Temporarily unlock agent wizard opens. In the first dialog, select the drives or devices to unlock so that only the ones you authorize are unlocked.
   Example: If you want to temporarily unlock an USB flash drive, check the **Drives connected via USB** box.
3. Now specify the options for drive control. Extended access can be given temporarily by setting the following options for drives:
   - **Disable file filtering during the unlock period**: Allow access to files or file types that are otherwise blocked by a file filter.
   - **Disable enforced encryption**: Allow access to drives where enforced encryption has been enabled. For more information on enforced encryption, see the DriveLock Encryption documentation at DriveLock Online Help..
   - **Force accepting usage policy before drive can be accessed**: The user must agree to a configured usage policy before the drive is unlocked.
   - **Disable drive scan**: If a drive scan has been configured (in the drive whitelist rules), you can disable it here.
4. If you are using application control, you can configure settings in the next dialog to disable it during unlocking as well. In addition, you can specify whether application files are added to the local hash database during this unlock period, and if so, which ones.
   The option **Require user approval for all files after unlock period ends** provides a manual check of all previously "learned" applications before they are finally added to the local application database and therefore unlocked.
5. If you want to **Disable Microsoft Defender control**, you can specify this in the next dialog. For more information about Microsoft Defender Management, see the corresponding documentation at DriveLock Online Help.

> Note: Please note that this does not disable Microsoft Defender, only DriveLock's management of Defender settings.

6. Lastly, configure the unlock period, either in minutes or until a specific date and time. Additionally, you can enter a text (e.g. the reason for the unlock) at this point. This text is also stored in the event and can be evaluated via reporting.
7. The unlocking starts immediately after you clicked Finish. If you have configured a user notification, it will be displayed on the agent.

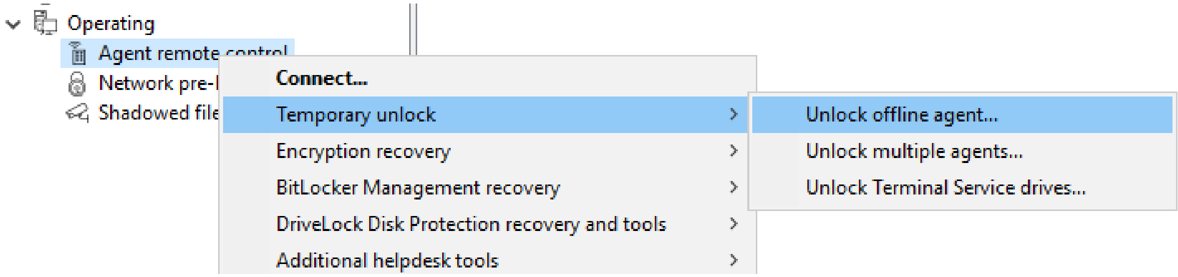
You can also terminate the unlock prematurely by clicking **Finish unlock**. If applicable, a confirmation will be displayed also.

Temporarily unlocking offline agents

To unlock agents that are not connected to your network, you need to follow the steps outlined below. This process involves the end user and the administrator, both have different tasks to perform.

Please do the following:

1. Right-click **Agent remote control**, then select **Temporary unlock**, then **Unlock offline agent** from the context menu.


Operating
Agent remote control
Network pre-l
Shadowed file
Connect...
Temporary unlock
Encryption recovery
BitLocker Management recovery
DriveLock Disk Protection recovery and tools
Additional helpdesk tools
Unlock offline agent...
Unlock multiple agents...
Unlock Terminal Service drives...

2. Depending on what you have specified in your policy in the offline unlock setting, you will now enter the offline unlock password or select a certificate. You can import a certificate from a file or from the Windows certificate store on the local computer. To import a certificate from a file, click Import from File and select the certificate file. To import a certificate from the local certificate store, click Import from Store.
3. Enter the computer name and request code provided by the user. DriveLock verifies the data. If the request code was created over an hour ago, this is shown in the Code age box.
4. The code provided by the user to unlock the DriveLock Agent is only valid for one hour. If this time is exceeded, you will need to run the Temporarily Unlock Computer

wizard again.

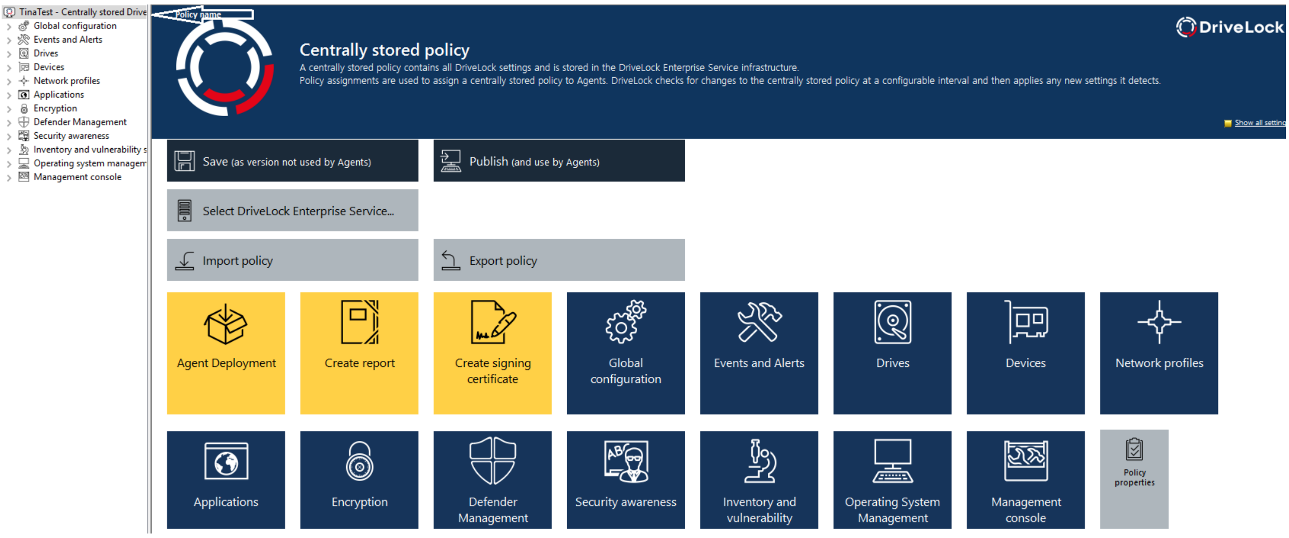
5. Select the permissions and the time period the unlock is valid for.
6. The response code is displayed. The returned response code must be entered by the user in the appropriate spaces.

4.5.1.11 Updating the configuration

You can manually force updating group policies or reloading a configuration file using the DriveLock Management Console and the remote agent control. To do so, you need to connect to the agent.

5 DriveLock Policy Editor

The DriveLock Policy Editor is a management console where you can configure all settings for your DriveLock policy.



Centrally stored policy

A centrally stored policy contains all DriveLock settings and is stored in the DriveLock Enterprise Service infrastructure.
Policy assignments are used to assign a centrally stored policy to Agents. DriveLock checks for changes to the centrally stored policy at a configurable interval and then applies any new settings it detects.

This documentation contains information about the following Policy Editor nodes:

- Global configuration
- Events and alerts
- Drives
- Devices
- Network profiles
- Operating system management
- Management Console

The following nodes have stand-alone documentation:

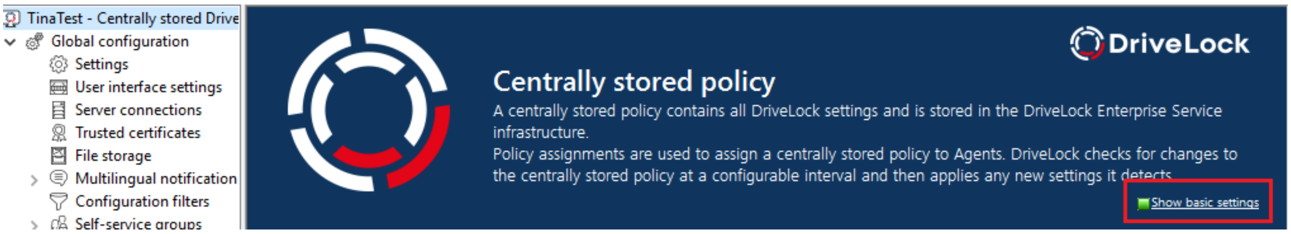
- Application Control
- Encryption (DriveLock Encryption with BitLocker Management, DriveLock PBA, Disk Protection, File Protection, BitLocker To Go and Encryption 2-Go)
- Defender Management
- Security Awareness
- Inventory and vulnerability scanner

Note: You can find all our documentationat DriveLock Online Help.

5.1 General notes

5.1.1 Show basic settings

In the top node of a policy, you can select which settings you want to work with and which taskpads are displayed (to you) on the right side of the editor. The selection affects all nodes in a policy and can be changed at any time.



Centrally stored policy

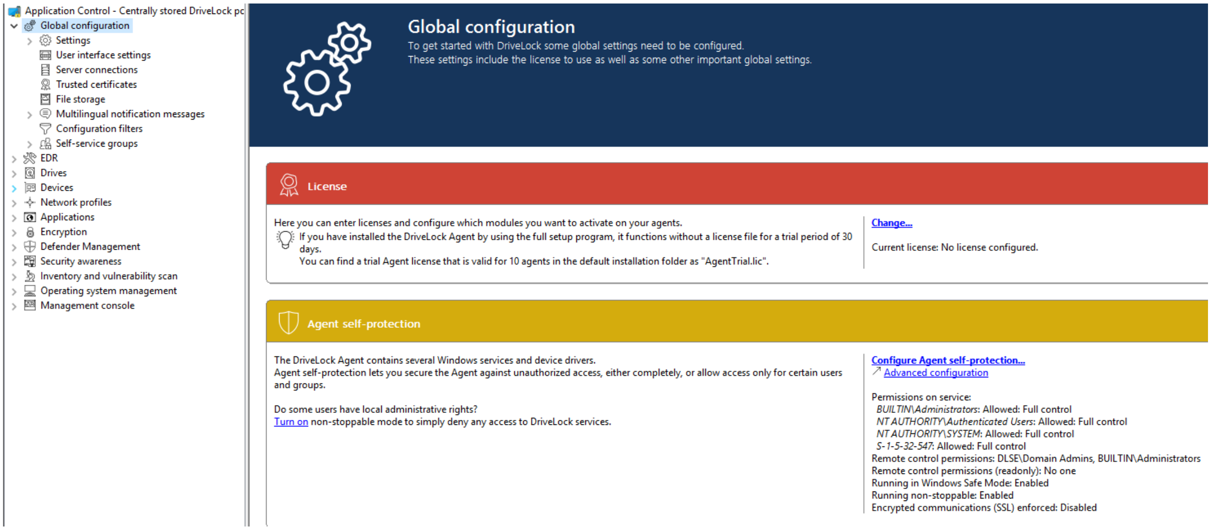
A centrally stored policy contains all DriveLock settings and is stored in the DriveLock Enterprise Service infrastructure.
Policy assignments are used to assign a centrally stored policy to Agents. DriveLock checks for changes to the centrally stored policy at a configurable interval and then applies any new settings it detects.

There are two top-level options: **Show basic settings** or **Show all settings** Depending on the selection you make, you will see different views of the nodes (see example below for the **Global Settings** node)

With the basic settings you can achieve a quick (basic) configuration of the most important parameters. When this view is active, the taskpads of the topmost nodes are divided into different sections, which indicate by their color whether important settings still need to be configured (red), whether the basic settings have been configured but more useful ones should be configured (yellow), or whether all settings for safe operation have already been made (green).

Tip: From this view you can ↗ Advanced configuration quickly access all available settings via the link.

- View with basic settings enabled:



Global configuration

To get started with DriveLock some global settings need to be configured.
These settings include the license to use as well as some other important global settings.

License

Here you can enter licenses and configure which modules you want to activate on your agents.
If you have installed the DriveLock Agent by using the full setup program, it functions without a license file for a trial period of 30 days.
You can find a trial Agent license that is valid for 10 agents in the default installation folder as "AgentTrial.lic".

Current license: No license configured.

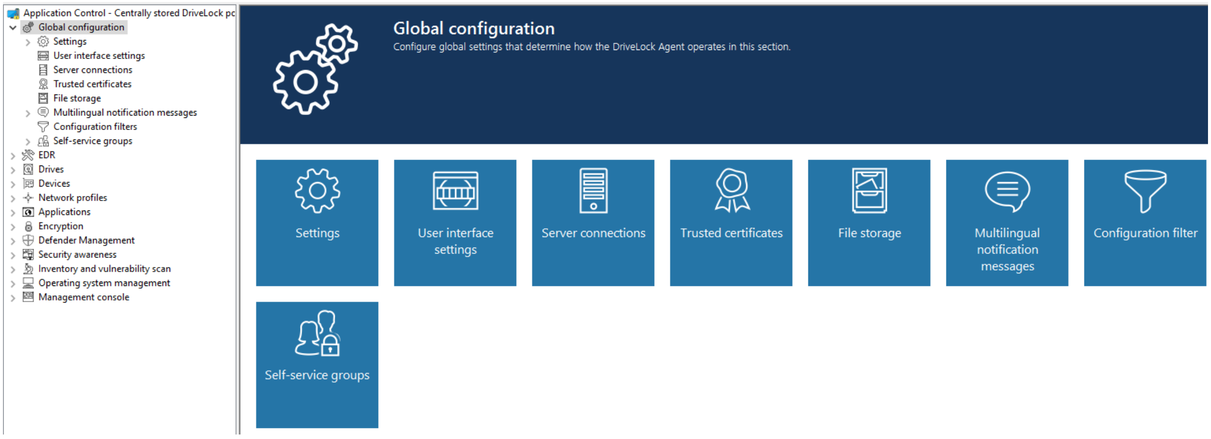
Agent self-protection

The DriveLock Agent contains several Windows services and device drivers.
Agent self-protection lets you secure the Agent against unauthorized access, either completely, or allow access only for certain users and groups.

Do some users have local administrative rights?
Turn on non-stoppable mode to simply deny any access to DriveLock services.

Permissions on service:
BUILTIN\Administrators: Allowed: Full control
NT AUTHORITY\Authenticated Users: Allowed: Full control
NT AUTHORITY\SYSTEM: Allowed: Full control
S-1-5-32-547: Allowed: Full control
Remote control permissions: DLSE\Domain Admins, BUILTIN\Administrators
Remote control permissions (readonly): No one
Running in Windows Safe Mode: Enabled
Running non-stoppable: Enabled
Encrypted communications (SSL) enforced: Disabled

- View with all settings:

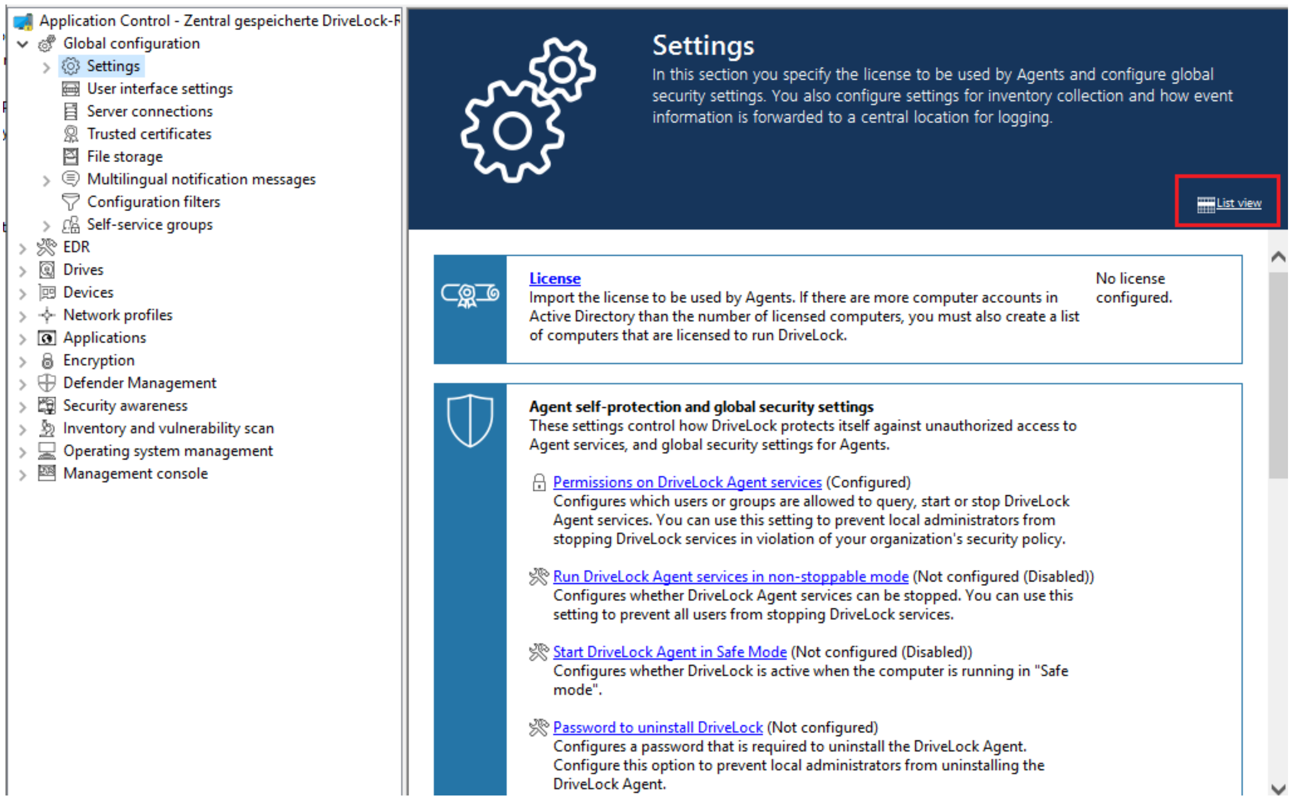


Global configuration

Configure global settings that determine how the DriveLock Agent operates in this section.

For some nodes in the Management Console or Policy Editor, you also still have the option to switch from a user-friendly and structured **taskpad view** to a simple **list view**.

Here is the taskpad view using the **Settings** node as an example :



Settings

In this section you specify the license to be used by Agents and configure global security settings. You also configure settings for inventory collection and how event information is forwarded to a central location for logging.

License
Import the license to be used by Agents. If there are more computer accounts in Active Directory than the number of licensed computers, you must also create a list of computers that are licensed to run DriveLock.

No license configured.

Agent self-protection and global security settings
These settings control how DriveLock protects itself against unauthorized access to Agent services, and global security settings for Agents.

Permissions on DriveLock Agent services (Configured)
Configures which users or groups are allowed to query, start or stop DriveLock Agent services. You can use this setting to prevent local administrators from stopping DriveLock services in violation of your organization's security policy.

Run DriveLock Agent services in non-stoppable mode (Not configured (Disabled))
Configures whether DriveLock Agent services can be stopped. You can use this setting to prevent all users from stopping DriveLock services.

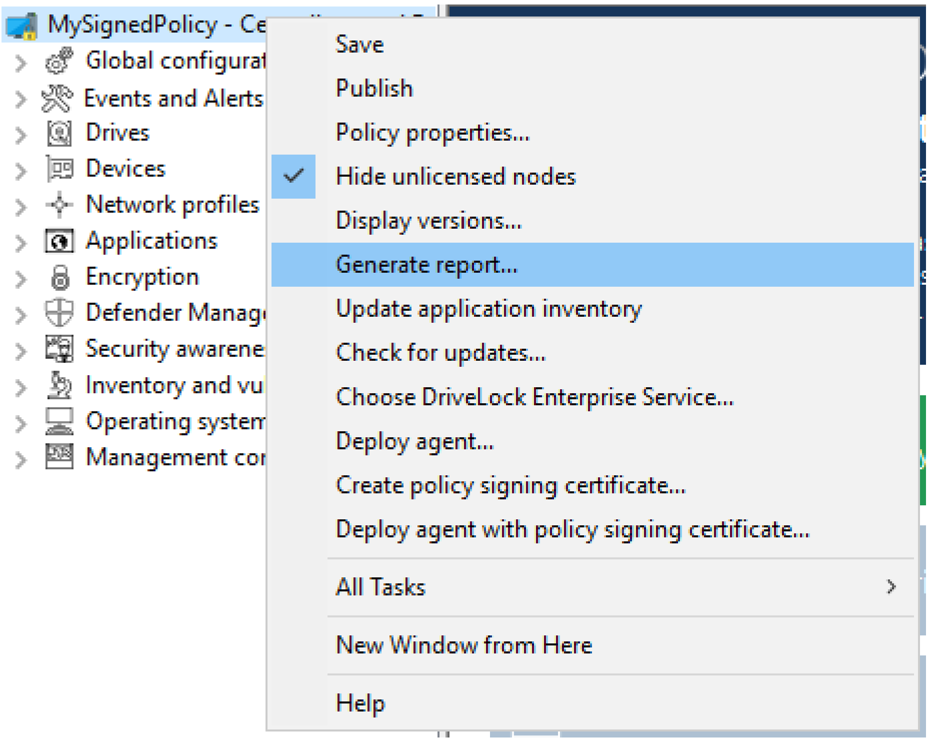
Start DriveLock Agent in Safe Mode (Not configured (Disabled))
Configures whether DriveLock is active when the computer is running in "Safe mode".

Password to uninstall DriveLock (Not configured)
Configures a password that is required to uninstall the DriveLock Agent. Configure this option to prevent local administrators from uninstalling the DriveLock Agent.

5.1.2 Generate configuration report

DriveLock can generate an XML-based report containing all configuration settings similar to a Group Policy report. You can view, save or print the report.

Click **Generate report...** to generate a configuration report.



Use the scroll bar and the "+" and "-" icons to navigate through the report.

Click Save Report to save it as a "*.html" file. For example, you can use Internet Explorer to view it.

Click Print to print the report. This opens a new Internet Explorer window and the print menu opens. Select a printer and click Print.

5.1.3 Policy signing certificate

You can sign centrally stored policies with a certificate to further secure policy distribution to DriveLock Agents. By using signing certificates, you can ensure that a DriveLock Agent receives only the signed policies assigned to it and that they are not modified in transit from the DriveLock Enterprise Service (DES) to the Agent. Some security certifications require signature certificates.

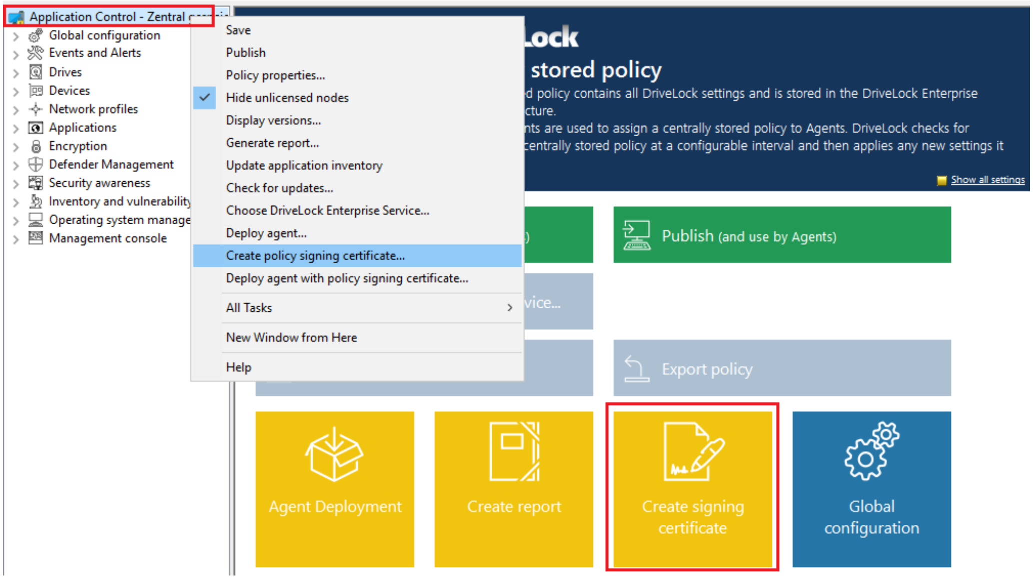
Please note the following:

- A DriveLock Agent that has not yet been configured can use unsigned and signed policies
- Once an agent is configured to use only signed policies, unsigned policies are ignored
- The complete agent configuration is stored in the signing certificate
  - DES server
  - Tenant

  - Policy type
  - Additional certificates
  - Emergency policy
- This configuration can only be changed with a new, different signing certificate
- An agent configured to use signed policies ignores manual reconfiguration via DOC

5.1.3.1 Creating a signature certificate

A certificate is generated within the DriveLock policy editor. To do so, select the menu command **Generate Policy signing certificate...** in the top navigation node.

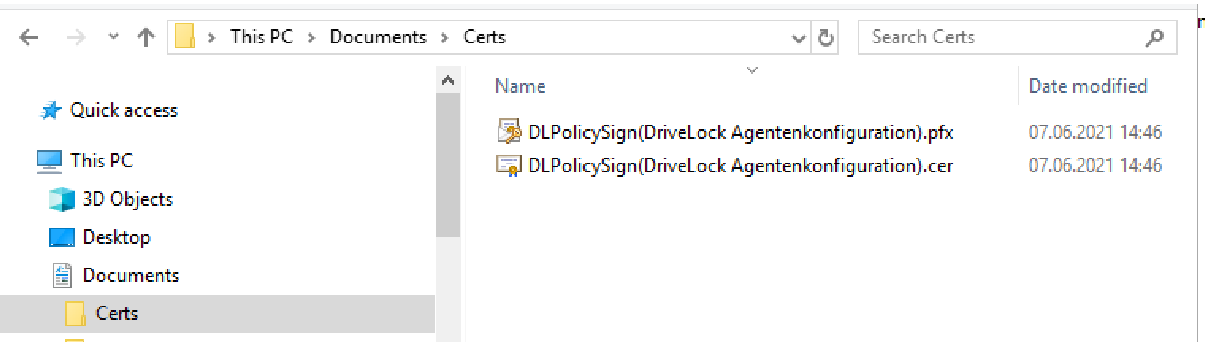


d policy contains all DriveLock settings and is stored in the DriveLock Enterprise cture.
nts are used to assign a centrally stored policy to Agents. DriveLock checks for centrally stored policy at a configurable interval and then applies any new settings it

A wizard will start to guide you through the steps of creating them.

1. Select the storage location for the generated certificate. Optionally, you can also save the certificate on a smart card.
2. You will need a password later to access the certificate and/or the private key. Specify it.
3. In the next step you can configure one or more server connections and a tenant, provided you are working with multiple tenants. Similarly, you can specify that a DriveLock Agent installed with this certificate will always use a very specific policy, regardless of what assignment you have made to the policies in DriveLock Management Console.
4. The final step is to specify whether the agent installed with this certificate will accept other policies signed with the other certificates you specify here.

5. Also, you can add a configuration from a configuration file that the Agent uses as long as it does not receive a policy through a DES or group policy.
6. Exit the wizard. The following certificate/key files are located in the given location:



Name	Date modified
DLPolicySign(DriveLock Agentenkonfiguration).pfx	07.06.2021 14:46
DLPolicySign(DriveLock Agentenkonfiguration).cer	07.06.2021 14:46

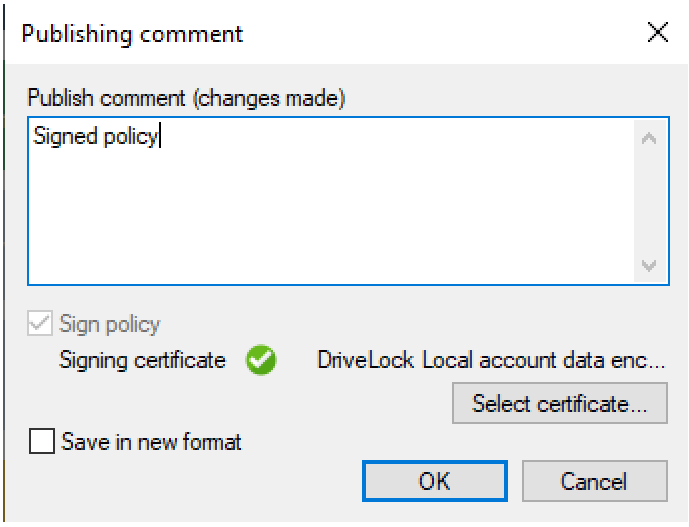
5.1.3.2 Signing a policy

Please do the following:

1. First you need to publish the policy you want to sign.
2. In the publish dialog, enter an appropriate comment, enable **sign policy** and click **selected certificate**

> Warning: Please note that a policy must be signed each time you want to publish it.

3. Select the previously generated certificate or its private key file, enter the matching password and click OK.
4. An icon indicates the successful signature. Click OK to publish the signed policy.



Publishing comment

Publish comment (changes made)

Signed policy

☑ Sign policy

Signing certificate ✓ DriveLock Local account data enc...

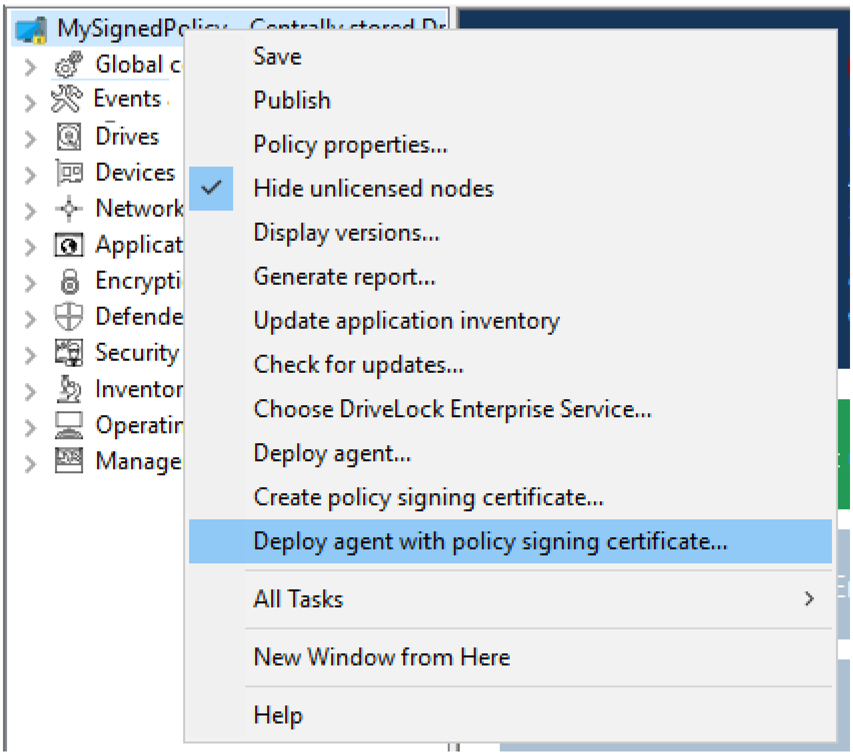
□ Save in new format

5.1.3.3 Deploying signed policies

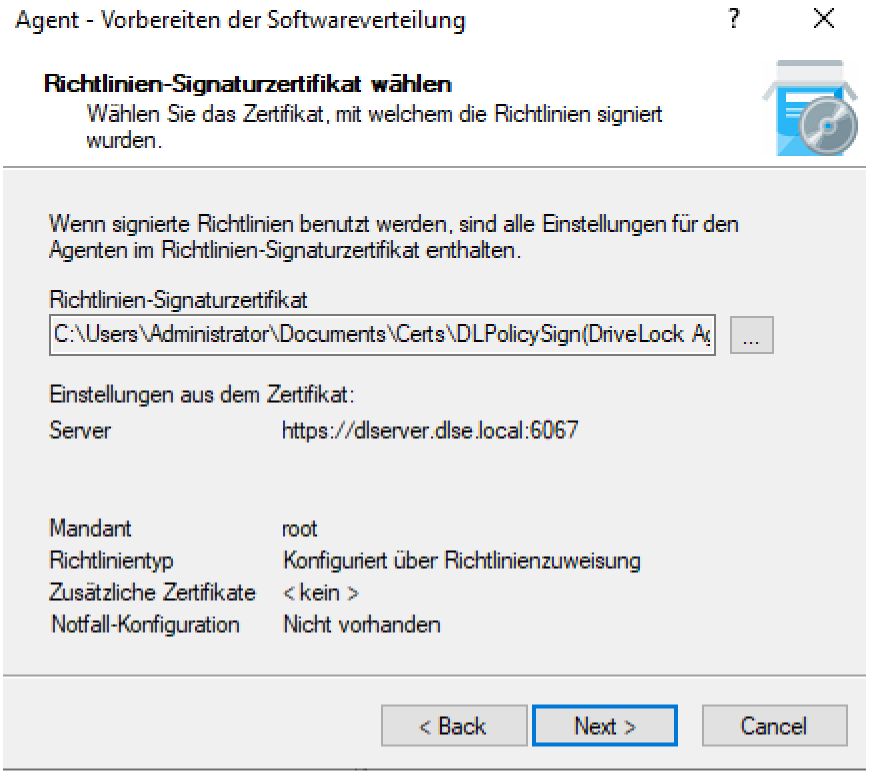
After you have generated at least one certificate, signed it, and then published the signed policy, the following steps must be completed to install the DriveLock Agent with the policy signing certificate.

For detailed information on installing the DriveLock Agents, please refer to the Installation Guide at DriveLock Online Help.

1. Open the policy context menu in the DriveLock Management Console and select **Deploy agent with policy signing certificate** to launch the agent distribution wizard.



2. Using this wizard, you will create a prepared installation package, which you can then use to install the DriveLock Agents on your network.
3. In the next dialog, select the policy signing certificate used to sign the DriveLock policy. Once selected, you will be shown the information stored in the certificate.



Agent - Vorbereiten der Softwareverteilung

Richtlinien-Signaturzertifikat wählen

Wählen Sie das Zertifikat, mit welchem die Richtlinien signiert wurden.

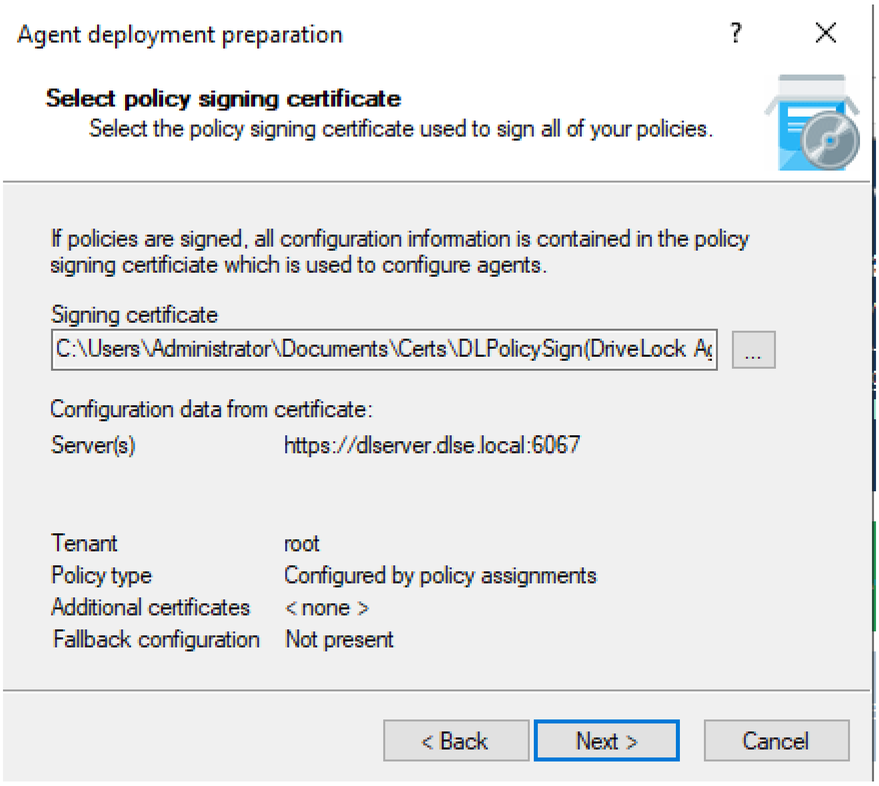
Wenn signierte Richtlinien benutzt werden, sind alle Einstellungen für den Agenten im Richtlinien-Signaturzertifikat enthalten.

Richtlinien-Signaturzertifikat

C:\Users\Administrator\Documents\Certs\DLPolicySign(DriveLock Ag

Einstellungen aus dem Zertifikat:

Server	https://dlserver.dlse.local:6067
Mandant	root
Richtlinientyp	Konfiguriert über Richtlinienzuweisung
Zusätzliche Zertifikate	< kein >
Notfall-Konfiguration	Nicht vorhanden



Agent deployment preparation

Select policy signing certificate

Select the policy signing certificate used to sign all of your policies.

If policies are signed, all configuration information is contained in the policy signing certificiate which is used to configure agents.

Signing certificate

C:\Users\Administrator\Documents\Certs\DLPolicySign(DriveLock Ag

Configuration data from certificate:

Server(s)	https://dlserver.dlse.local:6067
Tenant	root
Policy type	Configured by policy assignments
Additional certificates	< none >
Fallback configuration	Not present

4. Choose the type of installation package.
   - Windows Installer Package (MSI): Creates a new Microsoft Installer package that contains the previously specified settings.

- Windows Installer Transform (MST): Creates a Microsoft Installer Transform (MST) file with the chosen settings. You can use a MST file together with the original MSI package that is included in the DriveLock installation.
- Command line: Displays the command line syntax with the selected settings for the Microsoft Installer.

5. Specify source and destination for the package.
6. You can now distribute the generated installation package, using your company's software distribution, for example.

Manual agent configuration via the command line.

Alternatively, you can install the DriveLock Agent (with an unmodified MSI package) from the command line and specify the necessary parameters for using the policy signing certificate:

```
msiexec /I <DriveLockAgent.msi> /qb USESIGNCERT=1 POLSIGNCERT-
T="<PATHTOCERTIFICATE>\<PolicySigningCertificate>.cer"
```

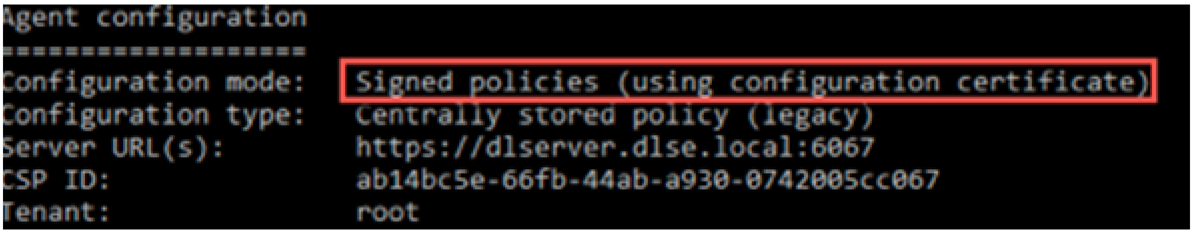
If you want to reconfigure an already installed agent to accept only policies signed with a specific certificate, you can do so with the following command line command:

```
drivelock -setconfigcert "<PATHTOCERTIFICATE>\<Poli-
cySigningCertificate>.cer"
```

> Warning: Please note that once an agent has been installed along with a signing certificate or switched to signed policies via command line command, it will no longer accept non-signed policies! For security reasons, deactivation of this verification is no longer possible!

You can check the status of the current agent configuration using the following command line command:

```
drivelock -showstatus
```



```
Agent configuration
===================
Configuration mode:   Signed policies (using configuration certificate)
Configuration type:   Centrally stored policy (legacy)
Server URL(s):        https://dlserver.dlse.local:6067
CSP ID:               ab14bc5e-66fb-44ab-a930-0742005cc067
Tenant:               root
```

5.2 Global configuration

You can define module-independent settings in the **Global configuration** node.

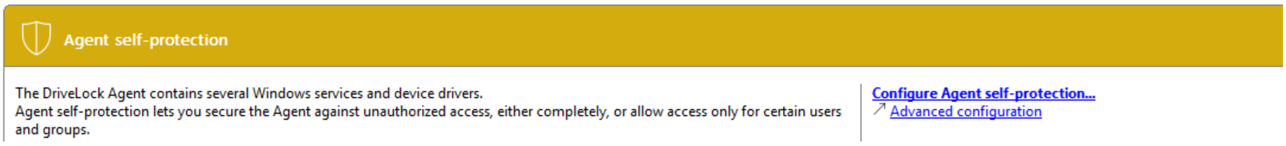
They take effect for all agents using this configuration, regardless of whether they were specified via GPO, centrally stored policy, or configuration file.

5.2.1 Settings

5.2.1.1 Agent self-protection and global security settings

Agent self-protection mechanisms protect against users being able to bypass DriveLock's configured security settings.

You can either quickly perform basic configuration steps via the Agent Self-Protection Wizard by clicking on **Configure Agent Self-Protection....** click:



Agent self-protection

The DriveLock Agent contains several Windows services and device drivers.
Agent self-protection lets you secure the Agent against unauthorized access, either completely, or allow access only for certain users and groups.

Alternatively, you can set the following settings separately via **Advanced configuration**:

Permissions on DriveLock Agent service

Run DriveLock Agent in unstoppable mode

Start DriveLock Agent in Safe mode

Password to uninstall DriveLock

Agent remote control settings and permissions

5.2.1.1.1 Permissions on DriveLock Agent services

This option allows you to set DriveLock service permissions individually and specifically, for example, to deny certain users access to the service or to control the DriveLock (agent) service (e.g. deny the "Power Users" group the ability to stop the service).

To set which users are allowed to stop the DriveLock service on the client machines, you can configure the appropriate permissions here. For example, you should remove the right to stop DriveLock service from the main users.

You can allow (or deny) the following actions for users and groups:

- Read service information: Displays the properties of the service.
- Start / stop service
- Full access

Warning: You cannot revoke rights from the "Local System" (SYSTEM)" account. DriveLock will automatically restore the appropriate permissions. It is mandatory that the system account has the appropriate rights to the DriveLock service.

5.2.1.1.2 Run DriveLock Agent in unstoppable mode

If you do not want to assign individual permissions and instead want to completely secure the DriveLock Agent service, use this option.

Warning: This setting results in the fact that the agent service can no longer be terminated by any user, regardless of the settings you have made in the individual permission configuration. Please note that it is not possible to uninstall the agent when the unstoppable mode is enabled.

5.2.1.1.3 Start DriveLock Agent in Safe mode

Click Start DriveLock Agent in Safe Mode to specify whether DriveLock should also run in Windows Safe Mode.

Warning: When this option is enabled, it is no longer possible to return to a previous DriveLock configuration setting in Windows Safe Mode.

5.2.1.1.4 Password to uninstall DriveLock

To prevent a DriveLock Agent from being uninstalled on a computer without permission, you can assign an uninstall password here for protection.

If the **Not configured** option is set, no password is required to uninstall agents.

If you want to uninstall a DriveLock Agent with password, you need to run the following command:

```
msiexec /x DriveLockAgent.msi UNINSTPWD= your password
```

Warning: The password for the installation is only applicable for DriveLock Agents. The complete installation of DriveLock cannot be protected with this password.

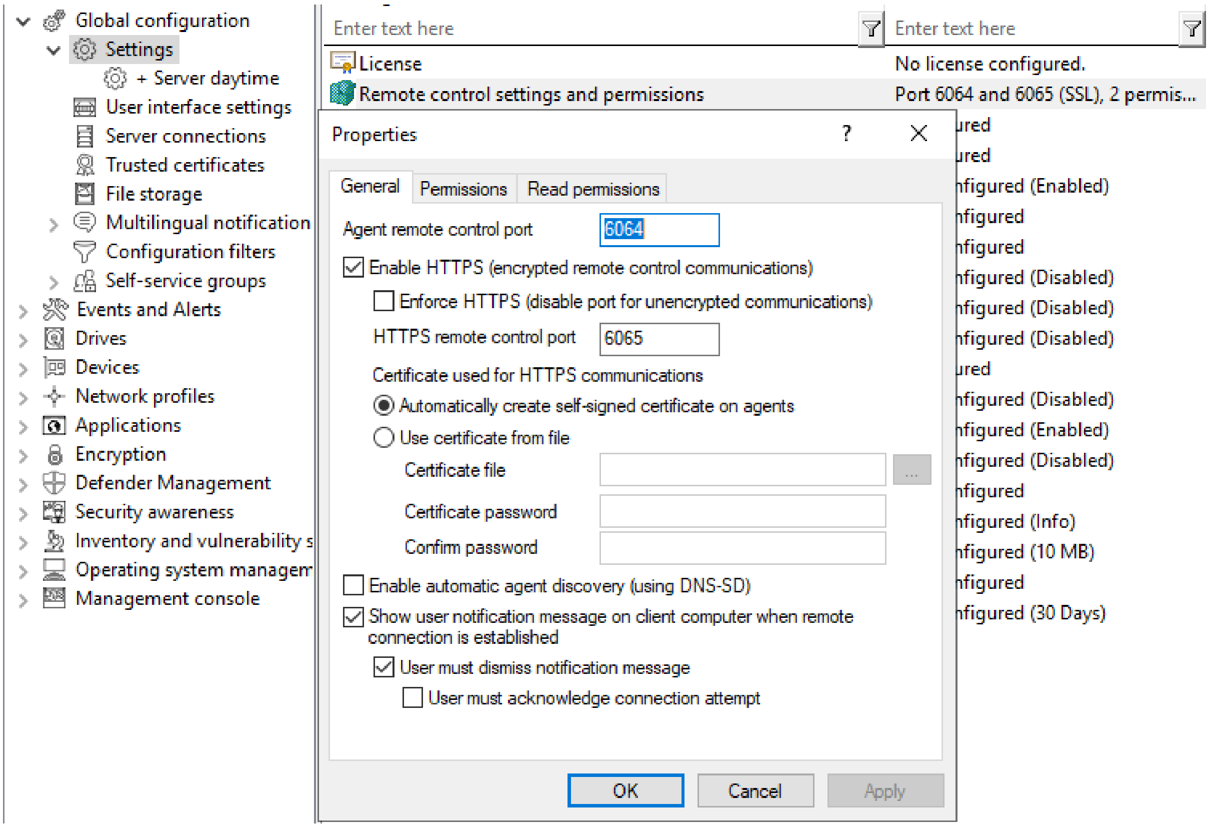
Warning: It is recommended to keep the default **Not configured** setting if you want to update DriveLock agents on your network.

5.2.1.1.5 Agent remote control settings and permissions

> Warning: In order to perform remote control actions on DriveLock agents, it is mandatory to define permissions.

Under **Remote control settings and permissions**, different permissions can be set for users (see figure) to control DriveLock agents remotely. In addition, you define further connection settings here.

- **Read permissions** tab: here you specify users or groups that are exclusively allowed to query information from DriveLock agents during remote connection actions.
- **Access rights** tab: here you specify users or groups that can explicitly perform actions on the agent, for example, temporarily release an agent or make changes to the configuration.
- **General** tab :



Global configuration
Settings
+ Server daytime
User interface settings
Server connections
Trusted certificates
File storage
Multilingual notification
Configuration filters
Self-service groups
Events and Alerts
Drives
Devices
Network profiles
Applications
Encryption
Defender Management
Security awareness
Inventory and vulnerability s
Operating system managem
Management console

Enter text here	Enter text here
License	No license configured.
Remote control settings and permissions	Port 6064 and 6065 (SSL), 2 permis...
	ured
	ured
	nfigured (Enabled)
	nfigured
	nfigured
	nfigured (Disabled)
	nfigured (Disabled)
	nfigured (Disabled)
	ured
	nfigured (Disabled)
	nfigured (Enabled)
	nfigured (Disabled)
	nfigured
	nfigured (Info)
	nfigured (10 MB)
	nfigured
	nfigured (30 Days)

Properties

General | Permissions | Read permissions

Agent remote control port: 6064
☑ Enable HTTPS (encrypted remote control communications)
☐ Enforce HTTPS (disable port for unencrypted communications)
HTTPS remote control port: 6065
Certificate used for HTTPS communications
● Automatically create self-signed certificate on agents
○ Use certificate from file
Certificate file:
Certificate password:
Confirm password:
☐ Enable automatic agent discovery (using DNS-SD)
☑ Show user notification message on client computer when remote connection is established
☑ User must dismiss notification message
☐ User must acknowledge connection attempt

- The remote control port 6064 is set for unencrypted and 6065 for encrypted connections. You can change these ports if necessary. The **Enable HTTPS (encrypted remote control communication)** setting is the default.

Note: For safety reasons, we strongly recommend using this setting. DriveLock agents thus refuse unencrypted connections.

- Normally DriveLock uses an automatically generated and self-signed certificate for the HTTPS connection. Select the **Use certificate from file** option to use a different certificate, which you can then select using the ... button. If the private key of the certificate is protected by a password, enter it twice.
- If you have selected the **Show user notification message on client computer when remote connection is established** option, the currently logged-in user on the target computer will receive a notification about the remote control access that has taken place.

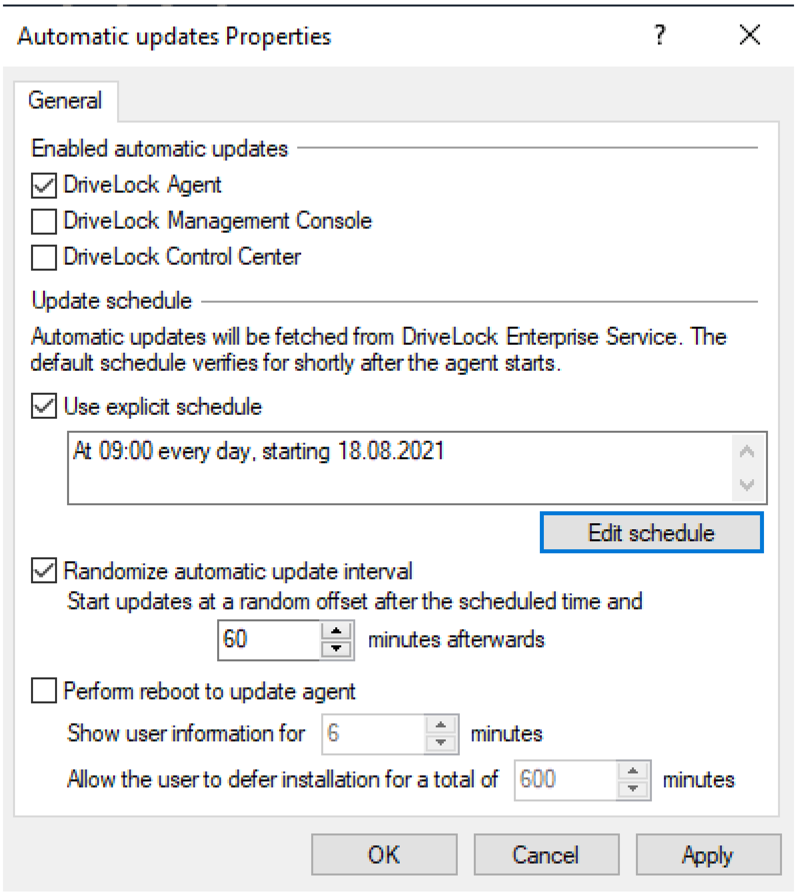
5.2.1.2 Event message transfer settings

Click here to find Information about event transfer in the events and alerts topic.

5.2.1.3 Automatic updates

DriveLock Agents can automatically update themselves and other components to a newer version.

Under **Enabled automatic updates**, select the components that you want to update automatically.


Automatic updates Properties

General

Enabled automatic updates

☑ DriveLock Agent

□ DriveLock Management Console

□ DriveLock Control Center

Update schedule

Automatic updates will be fetched from DriveLock Enterprise Service. The default schedule verifies for shortly after the agent starts.

☑ Use explicit schedule

At 09:00 every day, starting 18.08.2021

☑ Randomize automatic update interval

Start updates at a random offset after the scheduled time and 60 minutes afterwards

□ Perform reboot to update agent

Show user information for 6 minutes

Allow the user to defer installation for a total of 600 minutes

By default, the agent then randomly checks for newer versions on the DES within 60 minutes of system startup and continues to do so every 60 minutes thereafter. If so, the DES will download and install it immediately. The random timing ensures that not all computers in a company start updating or downloading the installation package at the same time.

You can also set your own schedules and add your own random time period to the set update time.

During the update DriveLock is inactive for a short time. If you want to ensure that the system is not in use during the update, check **Perform reboot to update agent**. The user can then delay the update by a maximum of N minutes. If a user agrees beforehand or the time has expired, they will be logged out and the update will be performed before the restart.

5.2.1.4 Set DriveLock simulation mode

DriveLock simulation mode allows you to install DriveLock and deploy the configuration without user disruption by locking drives, devices or applications.

Typically, simulation mode is used by creating and distributing a simple DriveLock policy with simulation mode enabled. After this has been applied, you can examine the relevant

DriveLock events or consult with users to identify settings that should be adjusted. Once you are sure that your policy is working as needed, you can disable simulation mode.

When the simulation mode is active, DriveLock responds as follows:

- DriveLock does not lock external drives, devices, applications and network connections.
- The file filter is disabled.
- Event messages are generated and forwarded according to the configuration.
- User notifications are generated as configured.
- Forced encryption is enabled, unencrypted drives are encrypted as configured.
- All other functions respond normally.

Note: By default, the simulation mode is disabled.

5.2.1.5 Advanced settings

These are special settings for communication with the DriveLock agent.

5.2.1.5.1 Allowing remote access in the Windows firewall

This option is enabled by default.

TCP ports 6064 (HTTP) and 6065 (HTTPS - default port) must be enabled in the firewall to allow remote agent control.

Warning: If you set this setting to Disabled later, the ports will still remain enabled.

5.2.1.5.2 Text messaging (SMS) configuration settings

This setting configures the SMS gateway that DriveLock agents should use to send text messages. It is set if you want to use Encryption 2-Go and use sending passwords for newly created encrypted containers.

Note: You need to know your gateway, provider, authentication details and the appropriate API parameters and enter them as required. These values are independent of DriveLock.

The **Gateway URL** is configurable within the company and must be specified accordingly.

Specify whether you are using **GET** or **POST**. If necessary, test the connection.

5.2.1.5.3 When impersonating users: Use 'network logon' instead of 'interactive logon'

This setting specifies how the login with username and password is performed when uploading data to network shares (shadow copies, recovery data for Bitlocker and Disk Protection).

For user accounts from other domains or those that have minimal rights to access the network share, interactive logon is not possible. Only network logon works here.

It therefore makes sense to use the **Enable** setting.

5.2.1.5.4 Update configuration only after all protective mechanisms are active on the agent

If you enable this setting, the DriveLock Agent starts with the last known configuration from the cache. This is recommended if neither Active Directory nor DriveLock Enterprise Service (DES) are accessible.

With this setting you can

- ensure that a DriveLock Agent updates the configuration only after all protection measures (e.g. drive and application control) have been activated and
- increase the starting speed of the agent.

> Note: This setting prevents the agent from starting with the current policy.

5.2.1.5.5 Enable access to agents outside the corporate network (MQTT)

Remote control of agents is always possible with direct network access. Additionally, by using the MQTT protocol, agents can be accessed behind firewalls or outside the corporate network. MQTT is enabled by default, but requires CPU and RAM resources on the DES. Therefore, if there are a large number of agents, it is advisable not to activate MQTT across the board for all agents, but only for those that cannot be reached via direct network access. Load balancing can take place through the use of Linked DES servers.

5.2.1.6 Logging settings

These settings allow you to specify additional levels and contexts for logging. They provide a much simpler and faster analysis of errors.

5.2.1.6.1 Log level

This setting allows you to specify a fixed value for the level of detail of the log files. There are 4 levels to choose from:

- **Error** : Only errors are logged (e.g. driver could not be started)
- **Info (default)**: Only the most important details are logged. Allows a 'rough' tracing
- **Detailed**: This level provides the most important information
- **Debug**: This level provides a very accurate error analysis and is rather rarely necessary. Note that this can make the log file very large.

5.2.1.6.2 Maximum log file size in MB

This setting allows you to specify a maximum value for the log file size. Once the maximum size is reached, a new log file is started. The old log file then gets the name suffix 'old', for example Drivelock.log becomes Drivelock.old.log

The value depends on the logging level.

5.2.1.6.3 Logging context

With this setting you can specify which processes create log files.

Values:

Locally logged in user (default) and **Remote Desktop Connection**: By default, only the processes for the locally logged on user are logged here.

> Note: For example, if you want to log all processes on terminal servers, especially within user sessions, you must expect that the number of log files can increase enormously. Therefore, by default, log files are not written for users in remote sessions.

Normal user , **Administrator with elevated privileges(default)** and **Administrator without elevated privileges**: Allows you to specify for which user groups logging is performed. By default, the administrator with elevated privileges is always set here so that administrative activities (e.g. for troubleshooting) are always logged.

Process: mmc.exe (default): All DriveLock Management Console processes are logged by default.

5.2.1.6.4 Time until old log files are automatically deleted

With this setting you can define the time after which old log files will be deleted automatically and regularly.

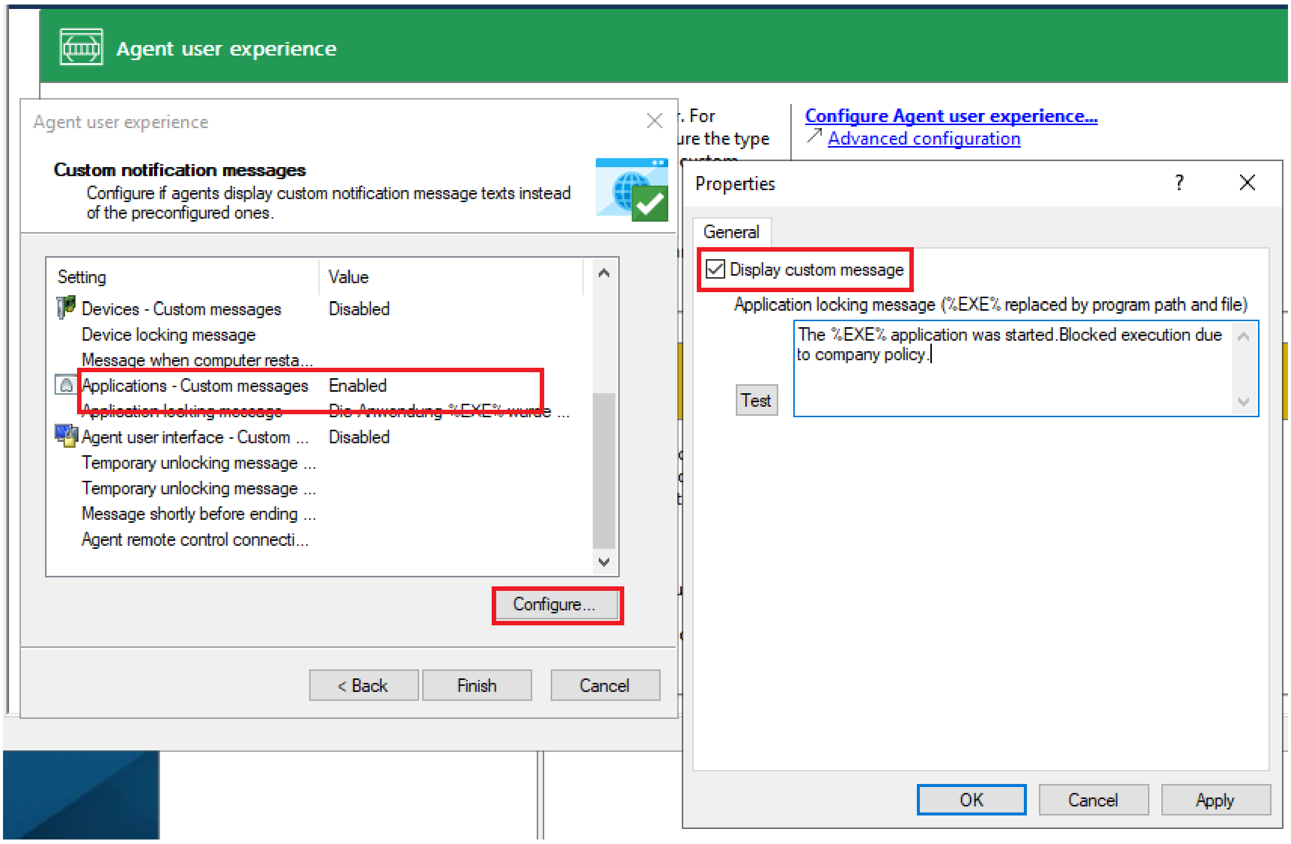
5.2.2 Agent user interface settings

You can configure the way notifications are displayed to the end user. Once you have enabled the basic settings, you can configure the agent notifications in a wizard, otherwise the settings can also be made individually via the advanced configuration.

In the wizard, first specify the notification type (corresponds to the setting for the Taskbar information area). Next are some settings for offline unlock. To finish, you can define customized notification texts, if necessary. At this point you can centrally specify texts that will be displayed to the end user in various situations. If you enter your own text, DriveLock will display it instead of the already built-in message.

Texts can be created for the following areas:

- Drive texts are displayed when DriveLock controls access to external drives or access to files, for example.
- Device texts are displayed when DriveLock blocks connected devices.
- Application texts are displayed when DriveLock prevents the launch of unauthorized applications.
  In the screenshot, you can see that a custom message is displayed notifying the end user that an application has been blocked:



Agent user experience

Custom notification messages

Configure if agents display custom notification message texts instead of the preconfigured ones.

Setting	Value
Devices - Custom messages	Disabled
Device locking message	
Message when computer resta...	
Applications - Custom messages	Enabled
Application locking message	Die Anwendung %EXE% wurde ...
Agent user interface - Custom ...	Disabled
Temporary unlocking message ...	
Temporary unlocking message ...	
Message shortly before ending ...	
Agent remote control connecti...	

Properties

General

☑ Display custom message

Application locking message (%EXE% replaced by program path and file)

The %EXE% application was started.Blocked execution due to company policy.

5.2.2.1 Agent user interface settings

Use these settings to specify which features are available to the end user in the agent user interface.

On the **General** tab, select the different categories, and on the **Start menu** tab, select the location in the Start menu where DriveLock is displayed. Here you also specify whether a shortcut to the self-service sharing wizard or the security awareness library is displayed in the end user's Start menu.

You can find information about self-service unlock here, about security awareness in the corresponding documentation at DriveLock Online Help.

5.2.2.2 Taskbar notification area settings

DriveLock can be configured to display an icon in the taskbar notification area and show notifications to the user.

On the **General** tab you can choose whether user notifications should be displayed to the user as pop-up dialog windows or balloon tips.

- If you select **Display popup window**, configurable messages are displayed. You also have the possibility to define your own custom messages including HTML instructions.

- If you select **Display balloon messages**, the corresponding message from Windows will be displayed as a balloon. To select this, the option **Display notification are icon** must also be set.
- The DriveLock icon is needed in the information area to display bubble tips. You can configure the icon to be visible only during a message. To do so, select the option **Display icon only when a message is displayed**.
- The **Display messages for...** duration bar defines how long the message is visible.
- To enable the DriveLock sound that plays when messages are displayed, check the **Play sound when a message is displayed** option.

On the **Options** tab, you configure the way DriveLock functions are displayed to the end user in the context menu of the taskbar icon.

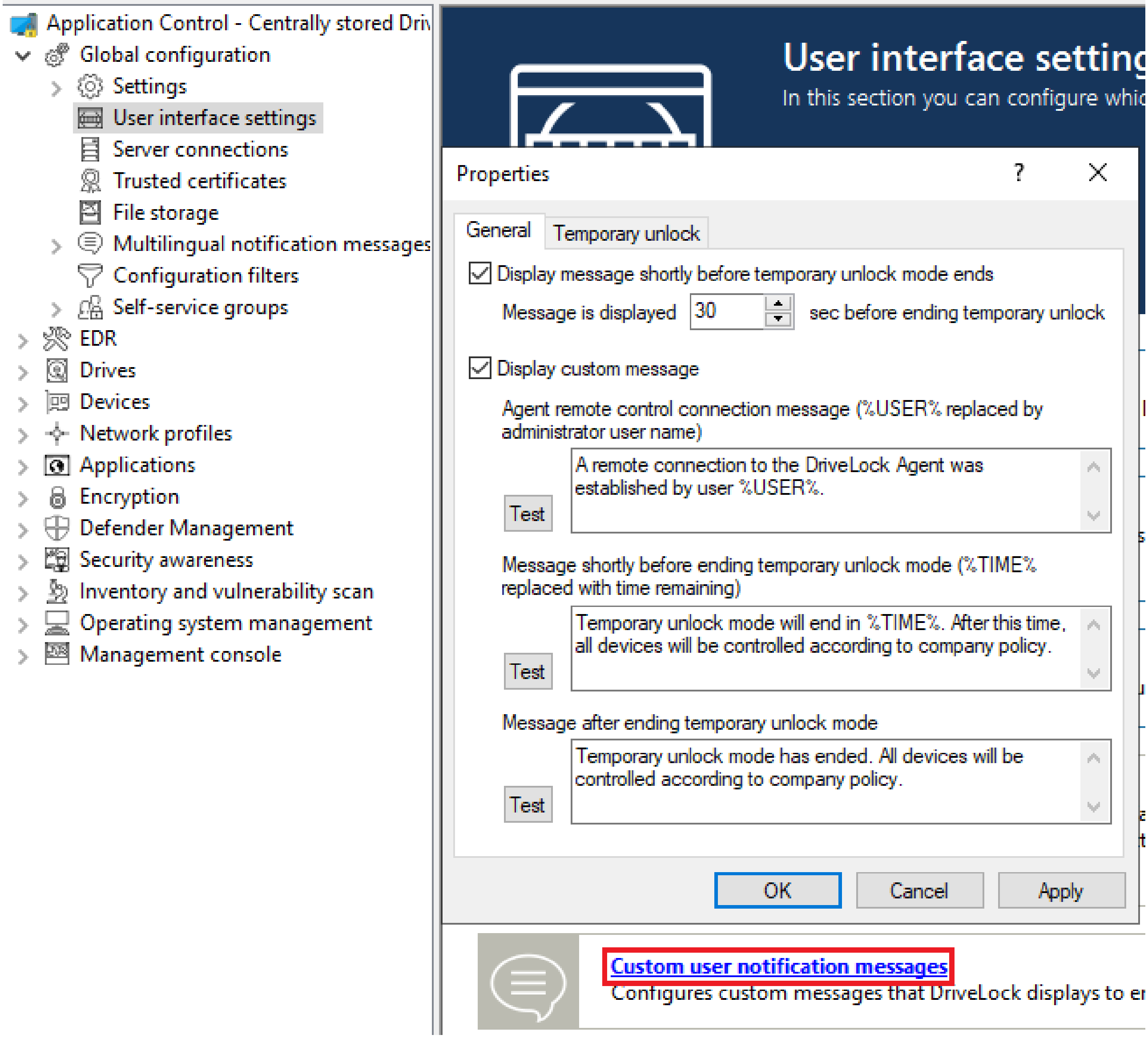
- To change the order of the elements, select the desired element and click **Move Up** or **Move Down** . Click **Remove** to delete the selected item. To add elements that are currently not visible, such as a separator line, click **Add** .
- To restore the default settings, click **Reset** .

5.2.2.3 Custom notifications

DriveLock displays user notifications to the end user to inform them of changes, such as device or drive locks or shares. You can use predefined notifications (from DriveLock) or customize the texts based on your preferences. In the following places in the DMC these notifications can be customized:

- On the final page of the wizard where you configure the agent user interface.
- In this node for the temporary unlock of the DriveLock agent (see figure).
- In the **Multilingual notification messages** node under **Languages / Standard messages**. For more information, please visit here.
- In the **Settings** for **Drives**, **Devices** and **Applications** as specific user notifications for these three areas.

On tab **General** you can select the following options for temporary unlock:



☑ Display message shortly before temporary unlock mode ends

Message is displayed 30 sec before ending temporary unlock

☑ Display custom message

Agent remote control connection message (%USER% replaced by administrator user name)

A remote connection to the DriveLock Agent was established by user %USER%.

Message shortly before ending temporary unlock mode (%TIME% replaced with time remaining)

Temporary unlock mode will end in %TIME%. After this time, all devices will be controlled according to company policy.

Message after ending temporary unlock mode

Temporary unlock mode has ended. All devices will be controlled according to company policy.

- **Display message shortly before temporary unlock mode ends** : This option is enabled by default. If necessary, you can set the time here for the notification to appear.
- **Use custom message**: Enable this option if you want to specify your own texts. The following variables are used:
  - `%USER%`: will be replaced by the administrator's user name when displayed.
  - `%TIME%`:is replaced by the time of release when displaying. You can configure different messages depending on the time in minutes or a time period used for the release.

You can use **Test** to display the message.

The options on **Temporary Share** are active only when you use custom messages. Here you can adjust messages for the duration of the short-term release.

Note: If you have already specified a language in the **Languages / Standard Messages** sub-node of the **Multilingual notification messages** node and defined texts there, you can no longer make any entries here.

5.2.2.4 Offline unlock settings

DriveLock can temporarily unlock locked removable media even if the computer is offline.

The associated wizard can be enabled or disabled with this setting.

The following options are available on the **General** tab:

- If you select **Disable offline unlock requests**, the end user will no longer be able to launch the wizard from the taskbar icon context menu and thus request offline sharing.
- The **Use short (weak) request / response codes** option allows you to reduce the complexity of challenge-response codes to fewer characters when releasing offline.

  Warning: Reducing the complexity also significantly reduces the security of this process.

- To completely disable the use of the wizard, you must also disable the **Show offline unlocking in context menu of notification area icon**.
- You can specify a message text for the end user.

On the **Security** tab, you can specify if an authentication by entering a password is required when accessing the offline unlock or if DriveLock allows access to this functionality by means of a user certificate from the local Windows certificate store.

- Select **Use password** if authentication is to be performed using a password. Enter and confirm the appropriate password.
- Select **Use certificate** if you want to authenticate using a certificate. It can be either imported from a file or read from the local certificate store. If you click the **Import from store** button, you will be prompted to select one of the displayed certificates. If you are using a certificate, you must enter the password to access the certificate's private key when approving the share.

> Note: You can also import the certificates via the DOC. Open the **Certificates** view and add the appropriate certificate. Thus, the offline unlock can be done conveniently via this certificate. A password is no longer required, only the user's permissions are relevant (that is, the roles needed for certificate management and for offline unlocking must be assigned).

5.2.2.5 User interface language on agents

Here you set the language of the DriveLock Agents.

If you select **Not configured**, the installation will take place in the language of the Windows installation or the language setting of the current user.

5.2.3 Server connections

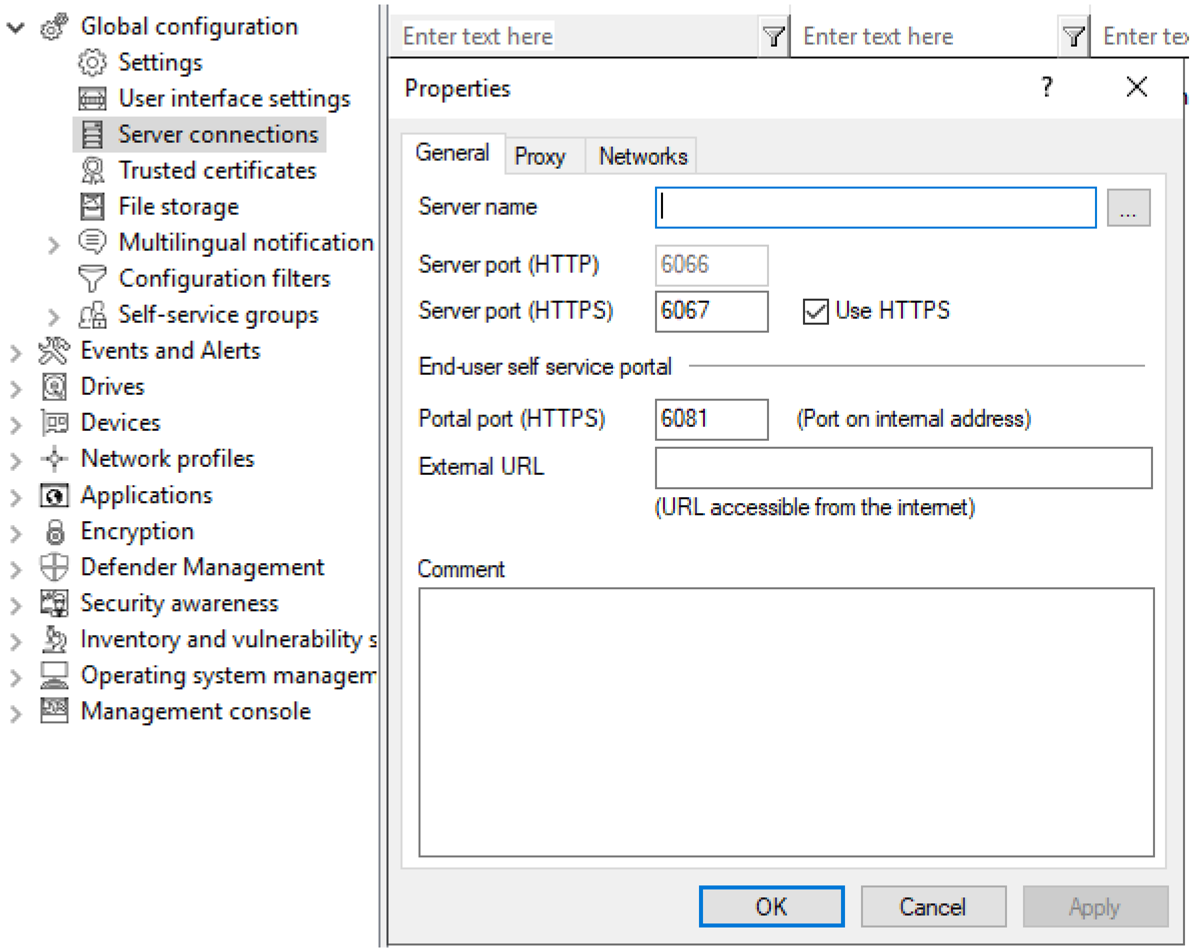
DriveLock Enterprise Service (DES) is the DriveLock component that performs all centralized tasks and functions. DriveLock can manage multiple server connections to a DriveLock Enterprise Service. Various connections are typically used in larger system environments or in environments with remote locations.

You can install DES on one or more computers in your network, but there can be only one central DriveLock database.

Under **Server connections**, you will initially only see the DES that you configured during installation. To add a Proxy server, do the same.

5.2.3.1 Configure server connections

To add a new connection, right-click **Server connections**, and then select **New** and **Server connection**.



Server name

Server port (HTTP) 6066

Server port (HTTPS) 6067 ☑ Use HTTPS

End-user self service portal

Portal port (HTTPS) 6081 (Port on internal address)

External URL

(URL accessible from the internet)

Comment

On the **General** tab, specify the **Server name**. If you have changed the default ports during its installation, change them here accordingly. By default, DriveLock Enterprise Service uses ports 6066 and 6067 to receive events from agents.

- The **Use HTTPS** option is selected by default. DriveLock automatically creates an appropriate certificate which is used for the SSL connection.
- If you want to use the Self-Service Portal (SSP), specify an **External URL** that end users can use to reach the SSP. For more information on configuring the SSP, refer to the corresponding documentation at DriveLock Online Help.

On the **Networks** tab, you can specify for which network connection this server connection should be used.

- The **All networks** option is set by default and causes the specified server connections to be used regardless of the currently detected network connection.
- To specify a previously defined network connection, activate **Selected network location** and select an entry from the list.

- If you want the server connection to be used when the computer is at a specific Active Directory location, select **Selected Active Directory location** and add a location. This is the easiest way to configure different server connections for different locations.
- If the server connection is to be used when the computer is located in an undefined network, enable the option **Locations where no other connection is configured** .

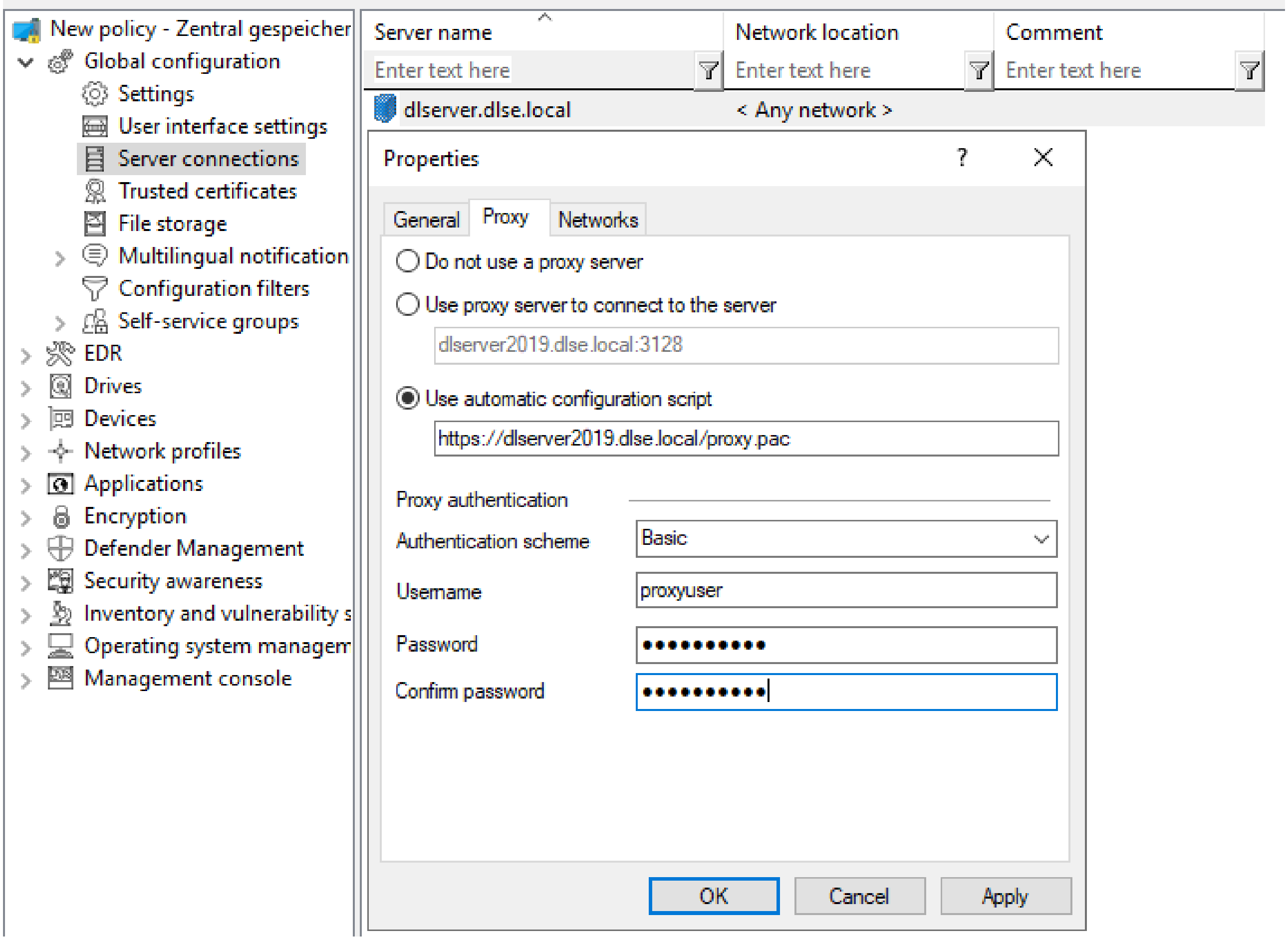
The **Proxy** tab is described here.

5.2.3.2 Proxy-Server

You can specify a proxy server in the DES connection settings. It is possible to specify a different proxy per server.

On the **Proxy** tab select the **Use proxy server option to connect to the server** option and specify the appropriate server.

Alternatively, you can **use an automatic configuration script** (*.pac file). To do this, specify the URL accordingly. If necessary, enter the authentication scheme, a user name and password.



○ Do not use a proxy server

○ Use proxy server to connect to the server

dlserver2019.dlse.local:3128

● Use automatic configuration script

https://dlserver2019.dlse.local/proxy.pac

Proxy authentication

Authentication scheme: Basic

Username: proxyuser

Password: ••••••••••

Confirm password: ••••••••••

Warning: Once you specify a proxy server in the policy, any settings set during installation are no longer used.

For information on proxy settings on the DriveLock Agent, click here .

5.2.4 Trusted certificates

DriveLock uses trusted certificates for secure communication between the DriveLock Management Console or DriveLock Agents and the DES. You can specify these certificates in the Global Settings of a policy.

Note: The **ChangeDesCert.exe** tool is located in the DriveLock Enterprise Services (DES) program directory under C:\Program Files\CenterTools\DriveLock Enterprise Service\ChangeDesCert.exe.
Note that if you want to exchange an existing DES server certificate using ChangeDesCert.exe, you must import the new certificate into the computer's Certificate Store and configure the private key as exportable.

Important information:

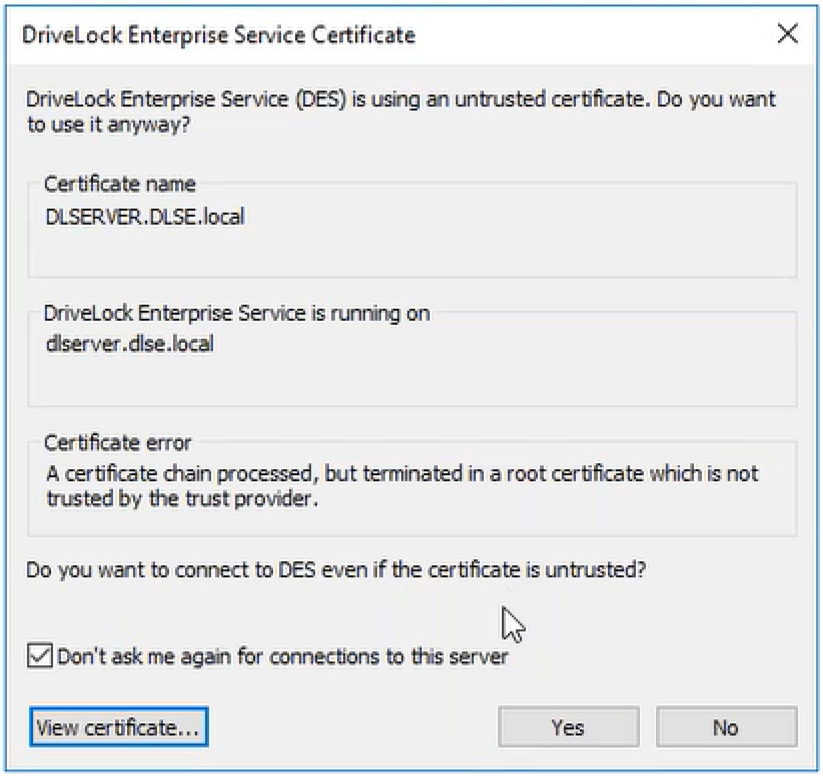
- Make sure your certificates are always up to date. If you need to replace the DES certificate or have additional linked DES installed, please enter the new certificates in the list in a timely manner and ensure that DriveLock agents are assigned this policy before communicating with the DES (or new linked DES).
- As long as a DriveLock Agent has not yet managed to find the DES certificate in the list of trusted certificates, it will accept connections to any DES. Once the certificate is successfully verified, from that moment on the agent communicates only with the DES whose hash values are entered in the list of trusted certificates.
- If you remove all certificates from this list, the agents will communicate with all DES again.

Note: If a DriveLock Agent receives an invalid certificate, an error message will be displayed on the agent and there will be no more communication between DES and the Agent! In this case, the only solution is making manual changes in the Agent's local registry. Please contact DriveLock Support for more information.

5.2.4.1 Verify trusted certificates in the DMC

Each time a DriveLock Enterprise Service function is called, the DriveLock Management Console (DMC) verifies the certificate that the server is using.

If Windows classifies the certificate as untrusted or the certificate is invalid, the following message appears first (see figure).



DriveLock Enterprise Service Certificate

DriveLock Enterprise Service (DES) is using an untrusted certificate. Do you want to use it anyway?

Certificate name
DLSERVER.DLSE.local

DriveLock Enterprise Service is running on
dlserver.dlse.local

Certificate error
A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

Do you want to connect to DES even if the certificate is untrusted?

☑ Don't ask me again for connections to this server

Warning: Please note that self-signed certificates are initially classified as untrusted by Windows because the root certificate cannot be verified.

You can look at the certificate and verify that it is indeed the certificate that the DES is using before you agree to use it. In this case, a corresponding entry is made in the registry under `HKEY_CURRENT_USER/SOFTWARE/CenterTools/DriveLock/MMC`. The message will no longer appear because the certificate has been entered.

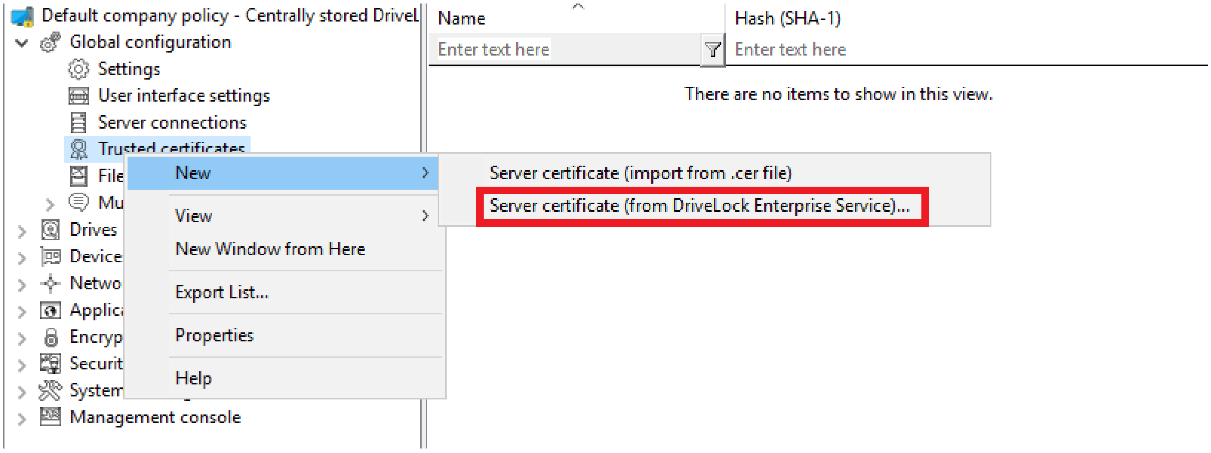
5.2.4.2 Select trusted certificates

Note: We recommend using this setting to increase the security requirements for communication between DriveLock Agent and DriveLock Enterprise Service. If you do not specify certificates, DriveLock cannot ensure that the agent communicates with the correct DES.

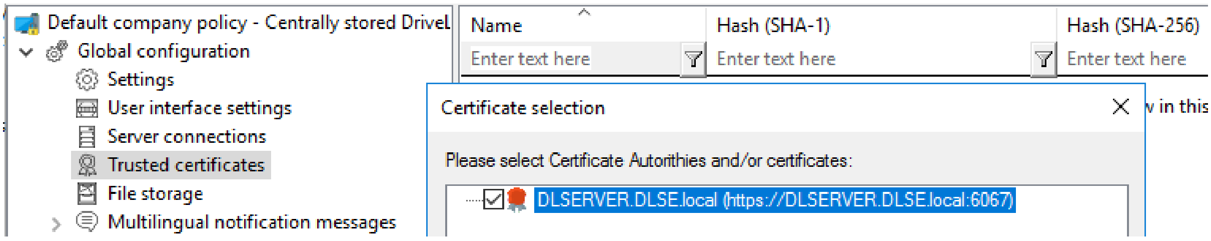
For more information about certificates, see the Installation Guide at DriveLock Online Help.. If you use self-signed certificates, be sure to specify them. Certificates issued by a certificate authority (CA) can be verified by Windows.

There are two options when selecting trusted certificates:

1. If you are using the server certificate that you selected during the DES installation with the **Create self-signed certificate** option, select **New** in the context menu and then **Server certificate (from DriveLock Enterprise Service)** .
   You can directly select the certificate used by the DES (or linked DES) (see figure).



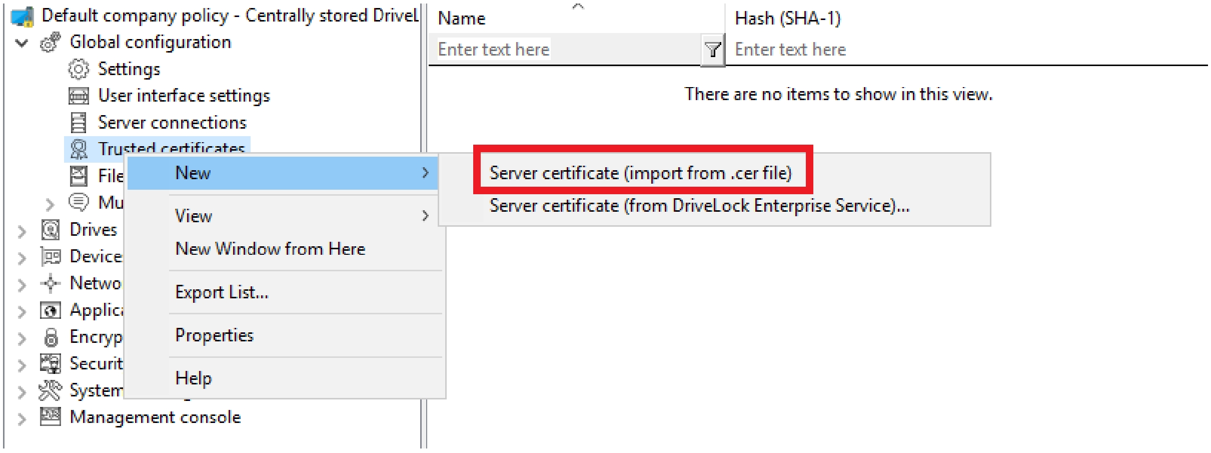
   After that, place a check mark next to those DES (or linked DES) certificates with which the agent communicates (in the example below DLSERVER.DLSE.local...):



Please select Certificate Autorithies and/or certificates:

☑ DLSERVER.DLSE.local (https://DLSERVER.DLSE.local:6067)

2. If you have specified your own server certificate for communication, you can select it here and use it in your policy:



   In the next step, select the appropriate certificate in the directory structure.
   You can also import the root CA certificate with this option. This will make DriveLock agents trust all certificates with this root CA. If your DES certificates have the same root CA, you no longer need to list them individually.

The list of trusted certificates now displays the corresponding information about the certificate (for example, name and hash values SHA-1 and SHA-256).

Note: Note: The SHA-1 hash value is now only used for XP.

The DriveLock Agents to which you then assign your policy will trust the server certificate and communicate only with the appropriate trusted servers.

5.2.5 File storage

The DriveLock policy file storage is a protected storage area within a DriveLock policy. For example, it is used to store files to be executed via a command line command within a DriveLock whitelist rule. The policy file store thus simplifies the distribution of scripts or programs used by the DriveLock Agent on client computers. After you import files into the policy file storage, they are automatically distributed to the agents along with the other settings. You can use the policy file storage in a local policy as well as within a configuration file or a group policy.

Warning: Importing large files into the policy file storage can increase network traffic and increase user logon times because the computer receives these files when Group Policy is applied to a computer and the store either has not yet been loaded or has changed.

Select File storage to see a list of all the files contained in the policy file storage.

Right-click **File Storage**, and then select **New**, and then **File...** to import a file into the policy file storage. Select the desired file using the file selection dialog.

Right-click a file and choose from the following options:

- **Extract file**: Save a copy of the file in any folder.
- **Delete**: Delete the selected file from the policy file storage
- **Properties**: Display details about the selected file.

Right-click **File storage** and select the **Display system files** option to also see the files that DriveLock stores internally within the policy file storage (such as the recovery certificates or application hash databases).

Note: System files cannot be deleted from the policy file storage.

Right-click **File Storage** and select **Properties** to get more information about the policy file storage.

To create a new policy file storage, click the **Reset storage...** button.

Warning: Resetting the policy file storage has the effect of deleting all the files it contains, including the system files. Make absolutely sure that you have a copy of the files before you delete the policy file store, especially if you are using DriveLock Disk Protection.

5.2.6 Multilingual notification messages

You can create individual text messages in different languages within DriveLock that can be used with different user notifications.

Before you can use individual text messages in whitelist rules, you must first specify the languages that should be available.

5.2.6.1 Languages / Standard messages

Right-click **Languages / Standard messages**, then **New** and first select the **language** on the **General** tab. The list contains all currently available Windows languages. Optionally, you can also add a description.

Notifications can be defined for the following areas:

Select the **Drive control** tab and enter the default messages that DriveLock should use when locking drives.

- The variable `%DRV%` is replaced by the drive letter when the message is displayed.
- Click **Test** to verify that the message is displayed correctly. DriveLock briefly displays the message as a user will see it.

Select the **Drive access** tab to configure messages for accessing files or locking CD/DVD recorders, for example.

- The following variables are available and will be replaced accordingly:

- `%DRV%` is replaced by the drive letter.
- `%PATH%` is replaced by the file path.
- `%NAME%` is replaced by the file name.
- `%EXT%` is replaced by the file extension.
- `%REASON%` is replaced by the reason why a file was blocked.

Select the **Devices** tab to set the default messages for devices. The variable `%DEV%` is replaced by the current device name when displayed.

On the **Applications** tab, you can define the messages for Application Control.

- The variable `%EXE%` is replaced by the current application when it is displayed.
- The variable `%PARENT%` is replaced for the program start.

On the **Temporary unlock** tab, the messages for temporarily unlocking drives or devices can be configured by an administrator.

- The variable `%TIME%` is replaced by the time of release when displayed.
- You can configure different messages depending on the time in minutes or a time period used for the release.
- You should configure an information text that will be displayed on the first page of the Share Wizard.

On the **Usage policy** tab, you define the texts for usage policies.

- Usage policies are used to inform the user of security-related behavioral measures or corporate policies before actually accessing a drive or device. Only after the user has read and comprehensibly accepted a hint message (usage policy), the drive or device is released.
- Both a heading, the texts for the two buttons, and the text itself can be freely defined via this configuration item.
- Either type the message text directly into the input field, or select an RTF-formatted file from the local disk or policy store. A file from the policy store is marked with an "*".

> ! Warning: When you select a file, you must make sure that it is located in the specified path on the local hard disk of the client computer and can be loaded from there. You can use the policy store to distribute this file along with the DriveLock configuration. For more information on policy storage, see File storage.

- An AVI video can also be played within the usage guideline, which can also be configured via this dialog.

On the **Agent** tab you can configure the message for remote control access.

- You can configure an information text that is displayed to the logged-in user as soon as an administrator establishes a remote control connection.
- The variable `%USER%` will be replaced with the user name of the administrator who started the remote control access when it is displayed.

On the **Awareness** tab, you define the default texts for the display window of the security awareness campaigns

On the **Encryption** tab, specify a contact (e.g. the Administrator or HelpDesk) that the end user can contact to perform the recovery process.

5.2.6.2 Notification messages

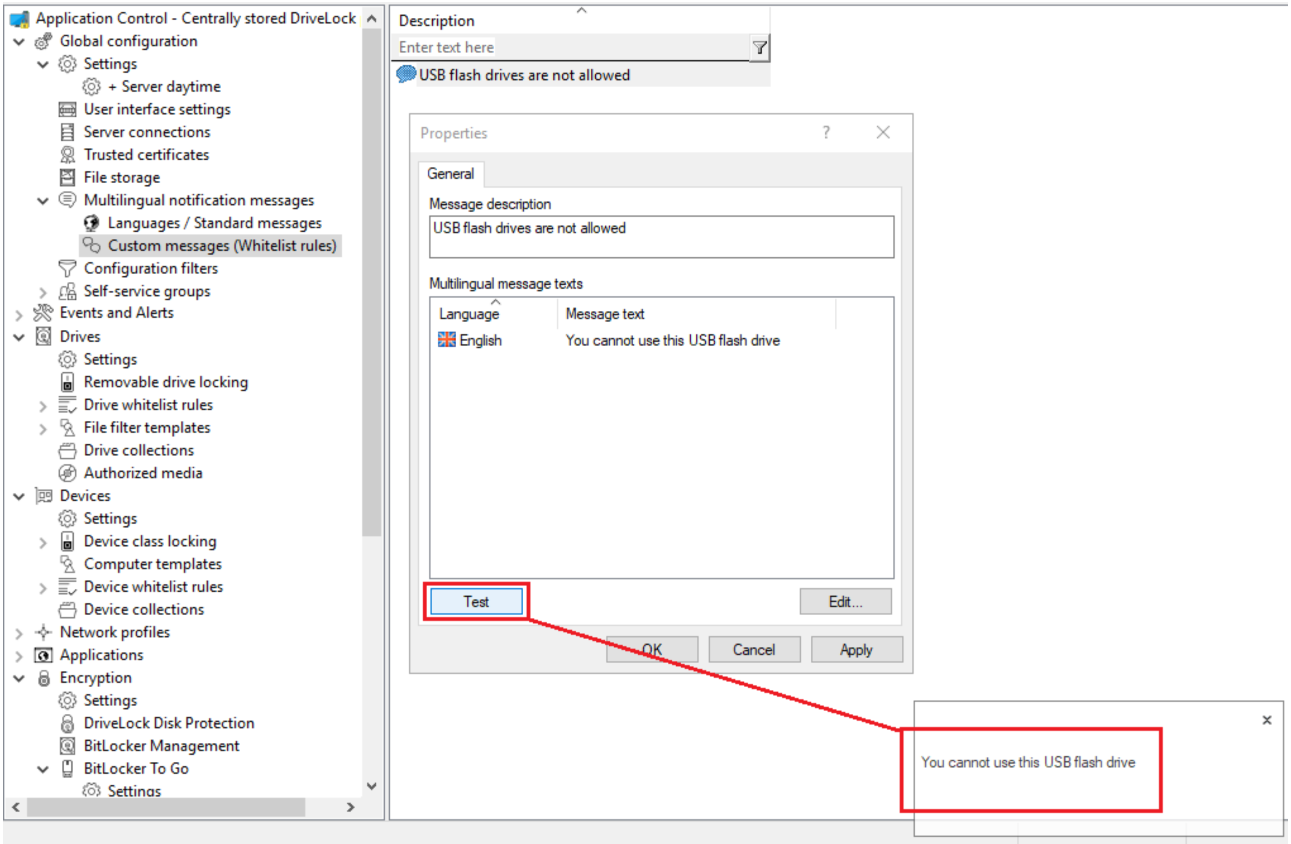
Here you can create individual user messages for different languages. In addition to the default notifications, other user notifications can be defined and used within whitelist rules. But before that - as described in the previous section - the available languages have to be configured.

Right-click **Custom messages (Whitelist rules)**, then New and **Custom message**.

Enter a descriptive text. This is also displayed in the list from which you can select a specific notification within whitelist rules.

All available languages are displayed. To compose a message in one of these languages, select the language and click **Edit** .

After entering the text, use the **Test** button to check if the message is displayed correctly. Click OK to accept the entered text.



Message description: USB flash drives are not allowed

Multilingual message texts

Language	Message text
English	You cannot use this USB flash drive

You cannot use this USB flash drive

Repeat these steps to enter the respective text for all languages.

Note: The use of multilingual messages is defined within the respective whitelist rules.

5.2.7 Configuration filter

Basics:

In general, a setting applies wherever the corresponding policy also applies: A specific setting is configured in a specific policy. This means that if you want to configure individual settings differently, you have to create another policy.

Configuration filters for different computers, users, or times within a single policy eliminate the need to create another policy and the hassle of maintaining a large set of policies with individual settings.

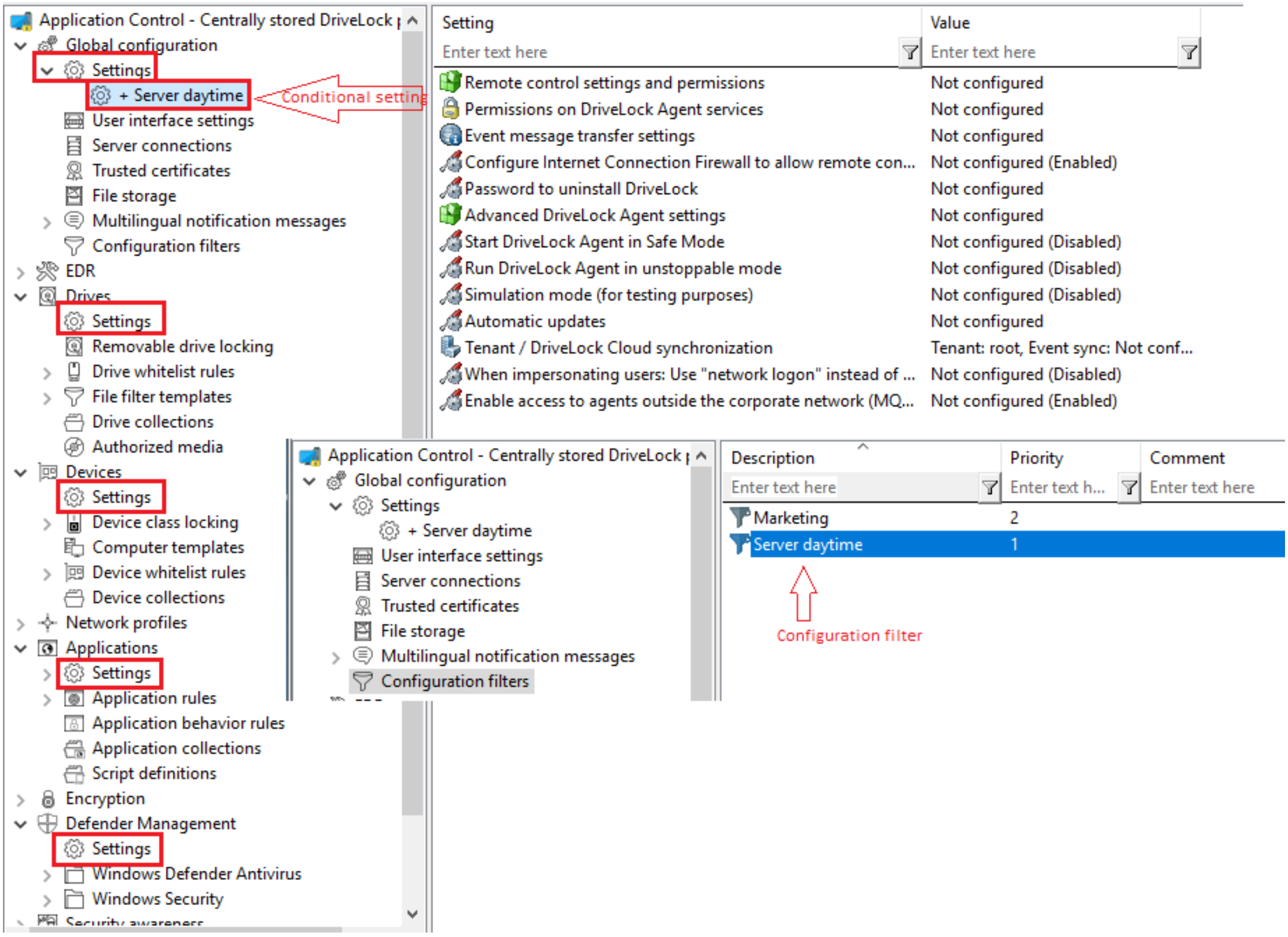
Effect:

Configuration filters allow you to combine conditions (i.e. "conditional settings") for specific computers, users, or times into a single policy. The configuration filter itself has no functionality, but is used as a criterion for conditional settings. It can be used in all setting nodes of the DriveLock Management Console.

Here you can see how to create a configuration filter and use it as a conditional setting.

Using the configuration filter in conditional settings:

Duplicates of the respective node are created below the various settings nodes, which are linked to a configuration filter.



Conditional setting

Setting	Value
Enter text here	Enter text here
Remote control settings and permissions	Not configured
Permissions on DriveLock Agent services	Not configured
Event message transfer settings	Not configured
Configure Internet Connection Firewall to allow remote con...	Not configured (Enabled)
Password to uninstall DriveLock	Not configured
Advanced DriveLock Agent settings	Not configured
Start DriveLock Agent in Safe Mode	Not configured (Disabled)
Run DriveLock Agent in unstoppable mode	Not configured (Disabled)
Simulation mode (for testing purposes)	Not configured (Disabled)
Automatic updates	Not configured
Tenant / DriveLock Cloud synchronization	Tenant: root, Event sync: Not conf...
When impersonating users: Use "network logon" instead of ...	Not configured (Disabled)
Enable access to agents outside the corporate network (MQ...	Not configured (Enabled)

Description	Priority	Comment
Enter text here	Enter text h...	Enter text here
Marketing	2	
Server daytime	1	

Configuration filter

Settings set in this node will take effect only if the filter on the Computer, Users or Times tabs is fulfilled.

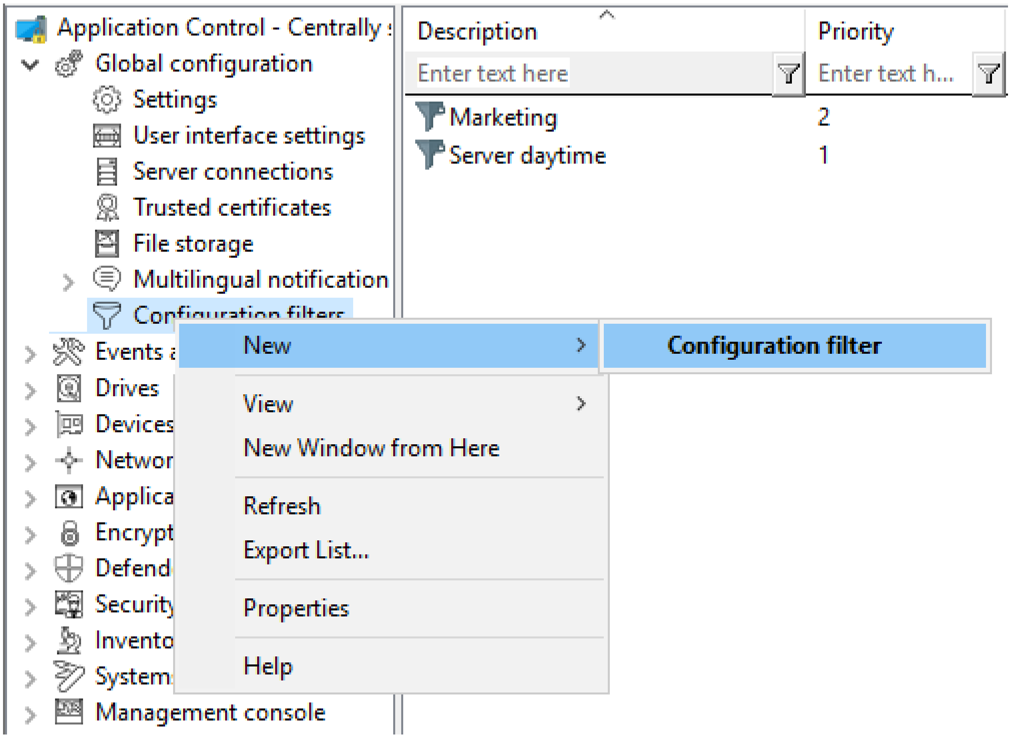
Advantages of conditional settings:

- More setting options are available than in a normal policy (because you can set active times for the conditions, for example)
- You avoid the creation of many policies and their assignments
- Individual settings can be overwritten more easily
- You can track your settings more easily because everything is included in a single policy
- Configuration filters also apply offline

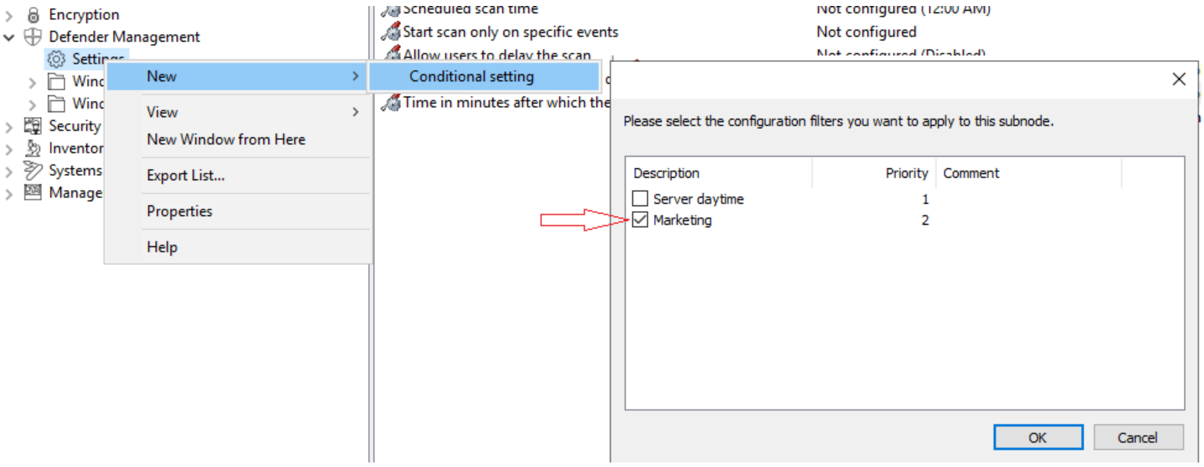
5.2.7.1 Creating configuration filters and specifying conditional settings

Set up configuration filters as follows:

1. In the **Configuration filter** node, click **New** and then **Configuration filter** (s. figure).



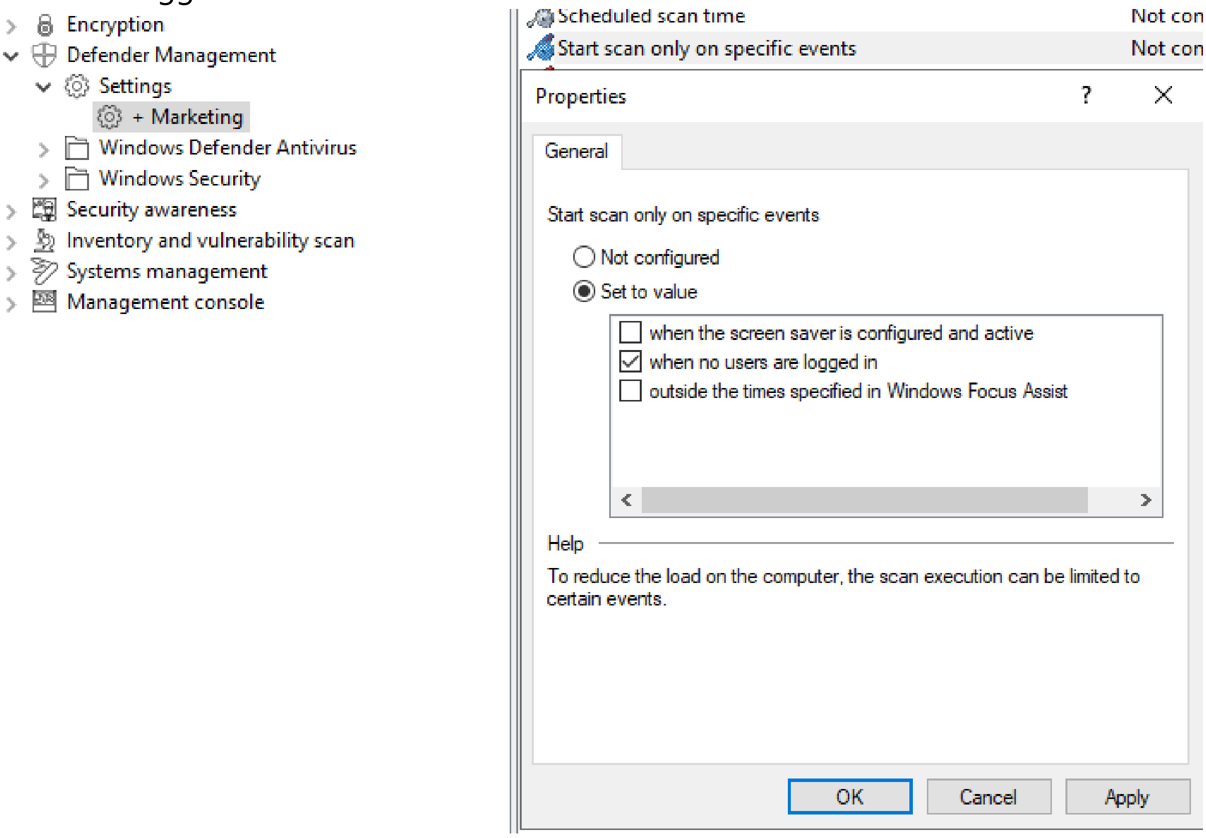
2. In the configuration filter properties, enter a description and, if necessary, a comment. In the example below, the configuration filter is called **Marketing** .
3. Depending on the conditions you want to set (specific **times** , **computers** or **logged in users**), specify the required settings in the corresponding tabs. You will find an example here.
4. Save the configuration filter.
5. Next, set the configuration filter as a conditional setting in any settings node of the DriveLock Management Console.
   Example:
   If you want to associate Defender Management settings with a condition for specific client computers (in the example, the computers of the Marketing department), proceed as shown in the figure:



Please select the configuration filters you want to apply to this subnode.

Description	Priority	Comment
□ Server daytime	1	
☑ Marketing	2	

6. Then select the setting that should explicitly apply to the marketing computers. In the example, Defender Scan should be started on the marketing computers only when no users are logged in:



Start scan only on specific events

○ Not configured
● Set to value

☐ when the screen saver is configured and active
☑ when no users are logged in
☐ outside the times specified in Windows Focus Assist

Help

To reduce the load on the computer, the scan execution can be limited to certain events.

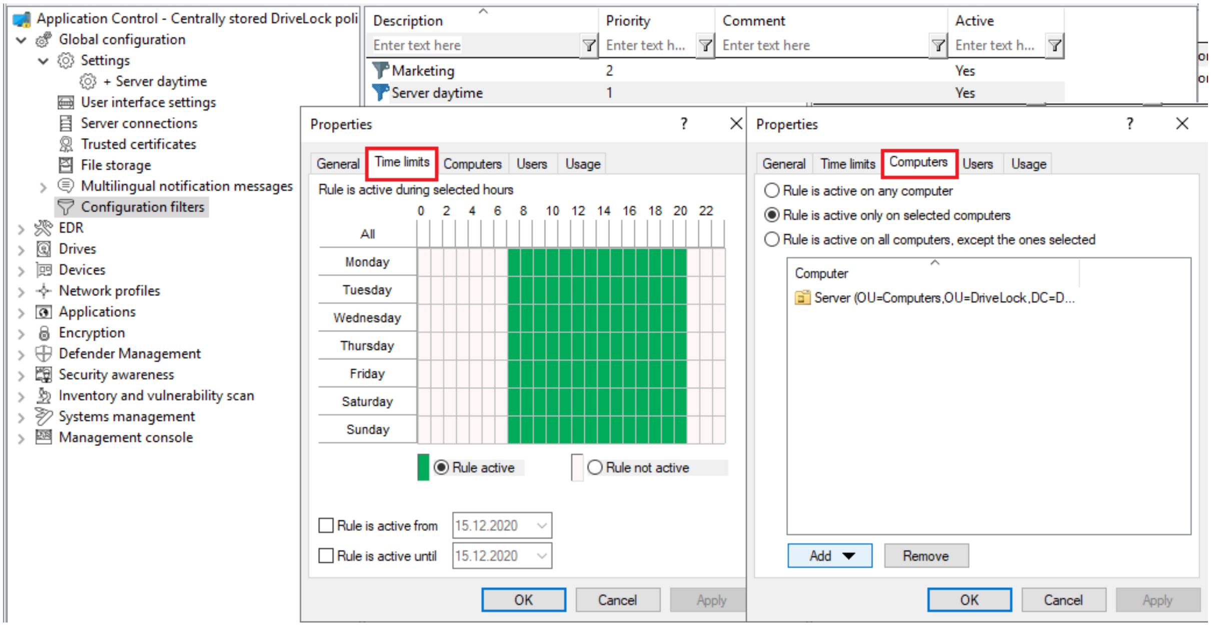
7. Save your setting and then assign the policy.

5.2.7.2 Configuration filter use case

Goal: You want to disable automatic updating during the day for certain DriveLock agents (servers).

Please do the following:

1. Create a new configuration filter.
2. Enter a **description** (example Server Tag) and a **comment** in the dialog. The check mark at **Is active** is set by default.
3. On the **Time limits** tab, select when the rule should be active (during the day).
4. On the **Computers** tab select the **Rule is active only on selected computers** option and under **Add** add the server(s) of your choice.



Description	Priority	Comment	Active
Enter text here	Enter text h...	Enter text here	Enter text h...
Marketing	2		Yes
Server daytime	1		Yes

Rule is active during selected hours

● Rule active ○ Rule not active

□ Rule is active from 15.12.2020

□ Rule is active until 15.12.2020

○ Rule is active on any computer

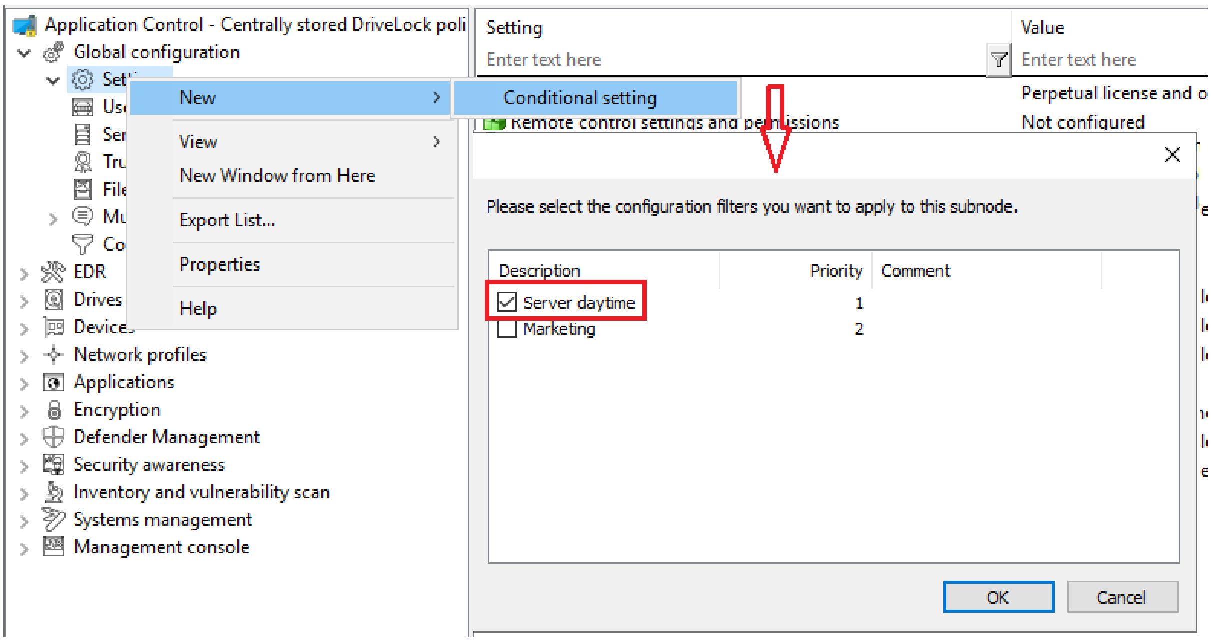
● Rule is active only on selected computers

○ Rule is active on all computers, except the ones selected

Computer

Server (OU=Computers,OU=DriveLock,DC=D...

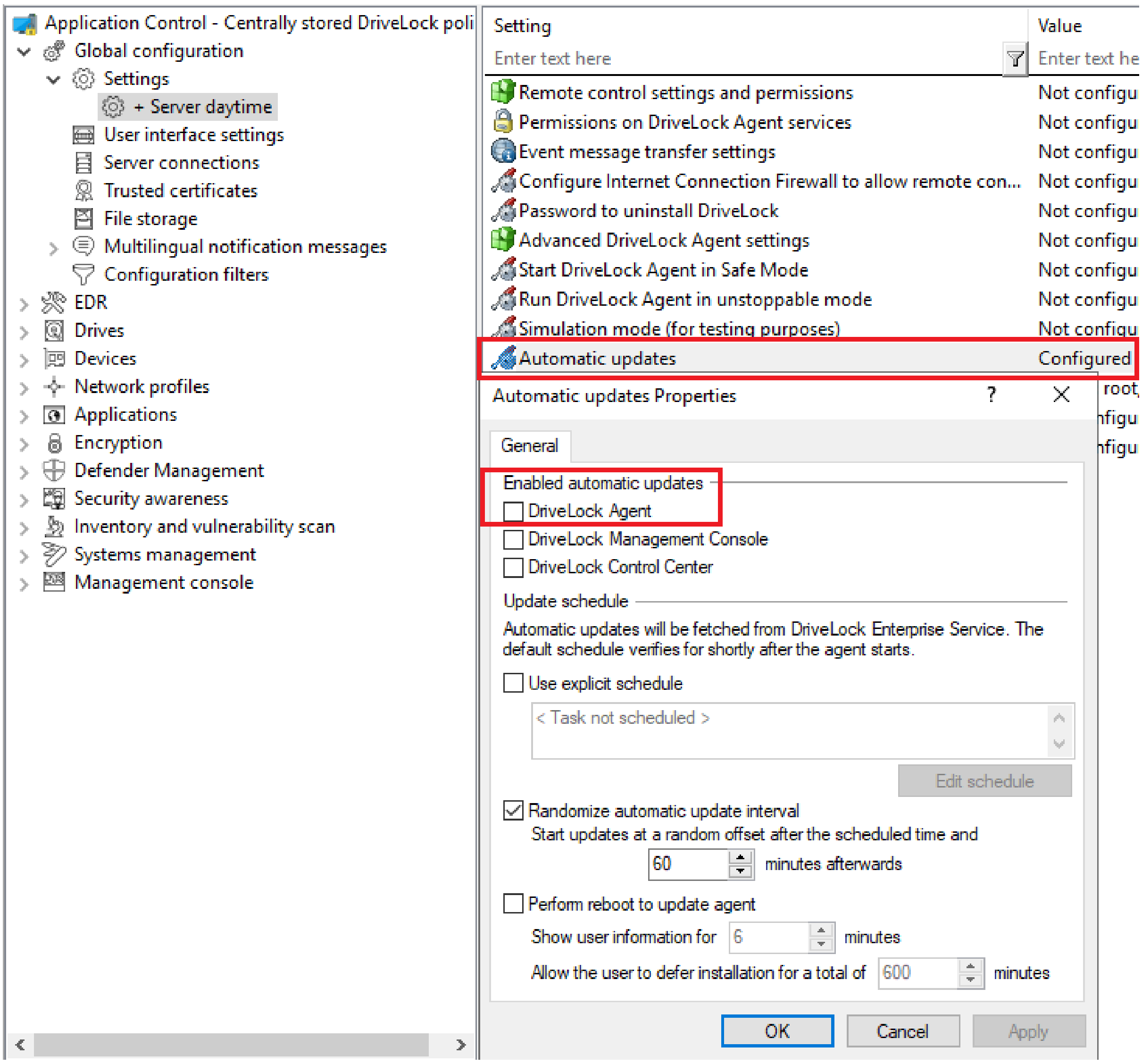
5. Save the configuration filter.
6. The created configuration filter now appears in the node with the same name and can be used as a conditional setting.
7. To do this, select the **Settings** sub-node under **Global configuration**, open the context menu and select **New** and as a Conditional setting your configuration filter **Server daytime** .



Please select the configuration filters you want to apply to this subnode.

Description	Priority	Comment
☑ Server daytime	1	
□ Marketing	2	

8. Then, in this conditional setting, open the **Automatic updates** option and uncheck **DriveLock Agent** which is checked by default .



Setting	Value
Enter text here	Enter text he
Remote control settings and permissions	Not configu
Permissions on DriveLock Agent services	Not configu
Event message transfer settings	Not configu
Configure Internet Connection Firewall to allow remote con...	Not configu
Password to uninstall DriveLock	Not configu
Advanced DriveLock Agent settings	Not configu
Start DriveLock Agent in Safe Mode	Not configu
Run DriveLock Agent in unstoppable mode	Not configu
Simulation mode (for testing purposes)	Not configu
Automatic updates	Configured

Automatic updates Properties

General

Enabled automatic updates

□ DriveLock Agent

□ DriveLock Management Console

□ DriveLock Control Center

Update schedule

Automatic updates will be fetched from DriveLock Enterprise Service. The default schedule verifies for shortly after the agent starts.

□ Use explicit schedule

< Task not scheduled >

Edit schedule

☑ Randomize automatic update interval

Start updates at a random offset after the scheduled time and 60 minutes afterwards

□ Perform reboot to update agent

Show user information for 6 minutes

Allow the user to defer installation for a total of 600 minutes

OK Cancel Apply

9. Save your configuration.

Conclusion:

The rule with the conditional setting 'Automatic update' is thus disabled on the defined servers during the day, but active on all other DriveLock agents (as set in the normal settings).

Explanation:

Conditional settings overwrite the normal settings

> Note: If there are multiple conditional settings, it depends on the priority of the configuration filters when they are applied. You can adjust the priority.

5.2.8 Self service groups

Using self-service groups, you can allow authorized users to unlock DriveLock Agents on their own, without having to use the DriveLock Management Console (MMC) or DriveLock Operations Center (DOC).

How to unlock agents is explained here.

5.2.8.1 Settings

The three settings for self-service are used to allow end users to use this functionality even if their computers are either in no domain or in a different domain.

In these cases, you can specify an account (or even an alternate account) so that Active Directory queries can be performed.

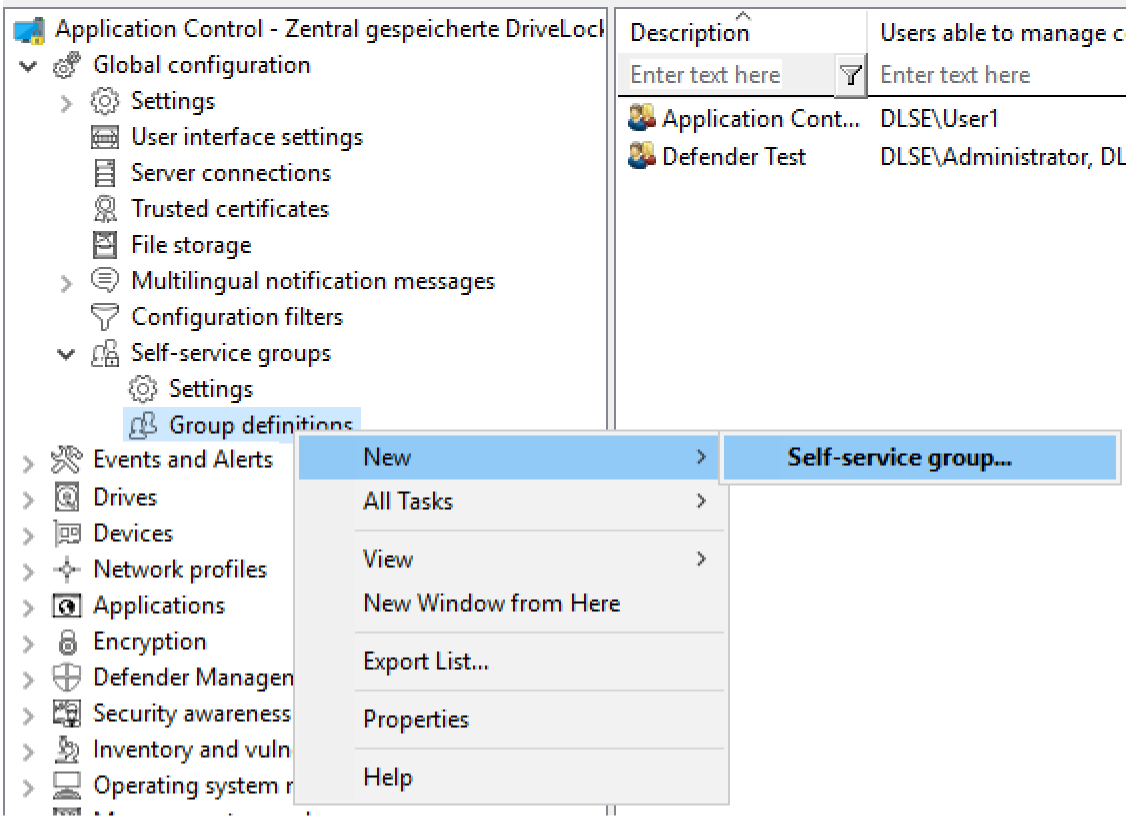
With the help of the setting **Show "run as" page at the beginning of the self service wizard**, the user gets the possibility to use another account for login at the beginning of the self-service wizard.

5.2.8.2 Definitions of groups

In order for users to be allowed to use self-service, they must be included in a self-service group. Here you specify the modules you want to allow for self-service (e.g. only drives or only applications).

Please do the following:

1. Create a new self-service group.



2. On the **General** tab, provide a short description and comment to identify this self-service group. Use the **End user information** field for an explanation of when and for what the user should use this rule. This text is then displayed in the wizard if more than one group is configured and selectable.

3. On the **Self-service** tab, select the device types and modules to be unlocked and the time for unlocking.
   If you select **Use simplified module selection page on unlock wizard**, the user is offered only these exact options and no advanced options. Activate the option **Hide advanced options page on unlock wizard**, then the user does not have to select an option.

4. For example, on the **Options** tab, you specify whether end users must accept usage policies before they are allowed to launch the share. You can also specify here that self-service will be terminated as soon as the end user logs off.

5. On the **Users** and **Computers** tabs, add the Windows users who are allowed to use the Self-service wizard and the computers where these users are allowed to use the wizard. If you select the **Only allow unlocking the local computer** option, an end user can share any computer to which this policy applies and where they can launch the Self-service wizard locally. You can also add DriveLock groups, computer names or

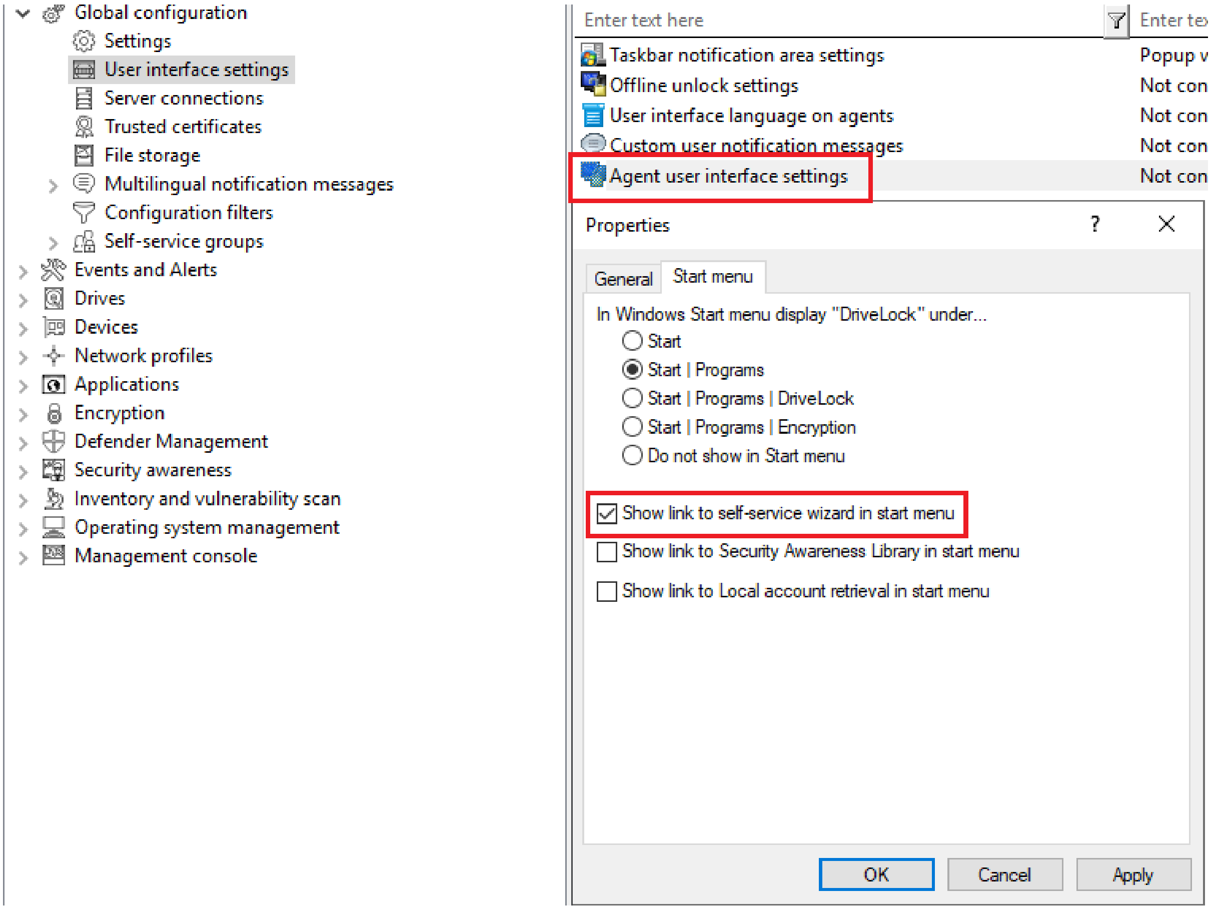
Active Directory computers, groups or OUs.

You can find a use case for self-service here .

5.2.8.3 Starting the self-service wizard

The self-service wizard is not offered to the end user by default. You can enable this option in a policy at the following locations:

1. In the **Agent user interface settings** on the **Start menu** tab: **Show link to the self service wizard in start menu**

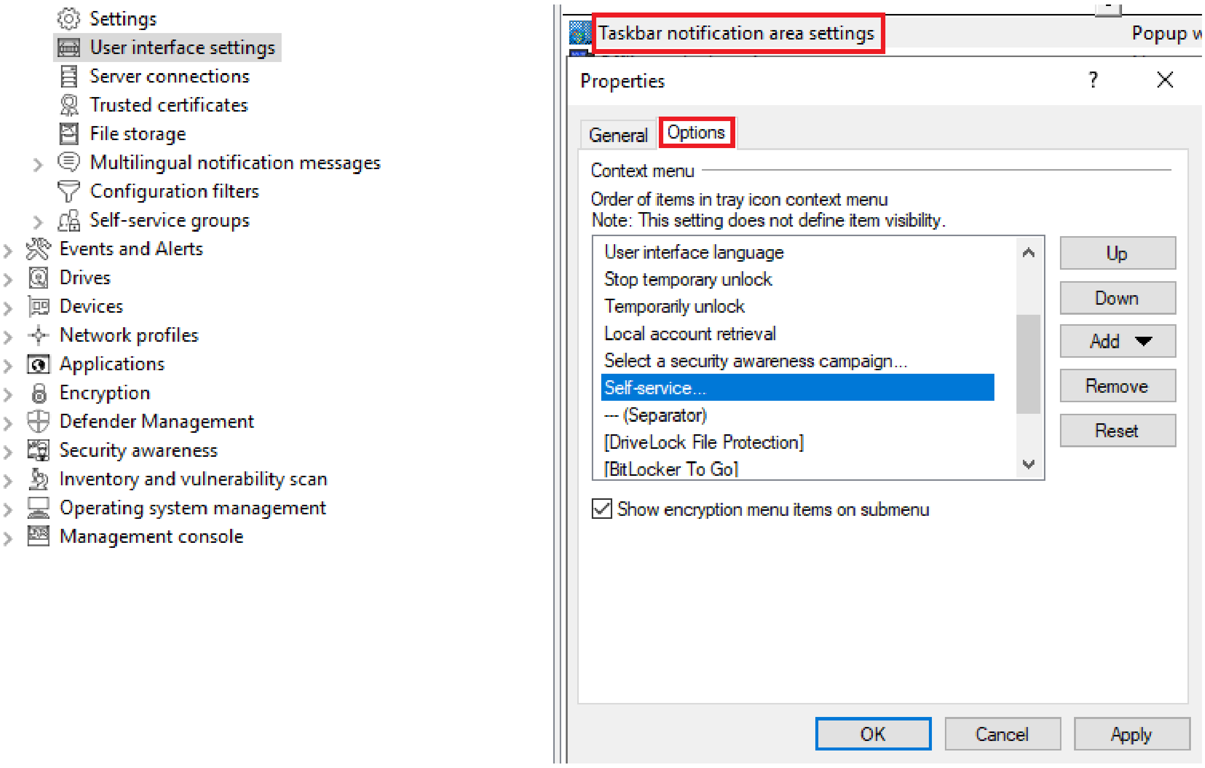


In Windows Start menu display "DriveLock" under...

○ Start
● Start | Programs
○ Start | Programs | DriveLock
○ Start | Programs | Encryption
○ Do not show in Start menu

☑ Show link to self-service wizard in start menu
□ Show link to Security Awareness Library in start menu
□ Show link to Local account retrieval in start menu

2. In the **Taskbar notification area settings** on the Options tab. Add Self-service... and set the entry to the desired position.



Context menu

Order of items in tray icon context menu
Note: This setting does not define item visibility.

User interface language
Stop temporary unlock
Temporarily unlock
Local account retrieval
Select a security awareness campaign...
Self-service...
--- (Separator)
[DriveLock File Protection]
[BitLocker To Go]

☑ Show encryption menu items on submenu

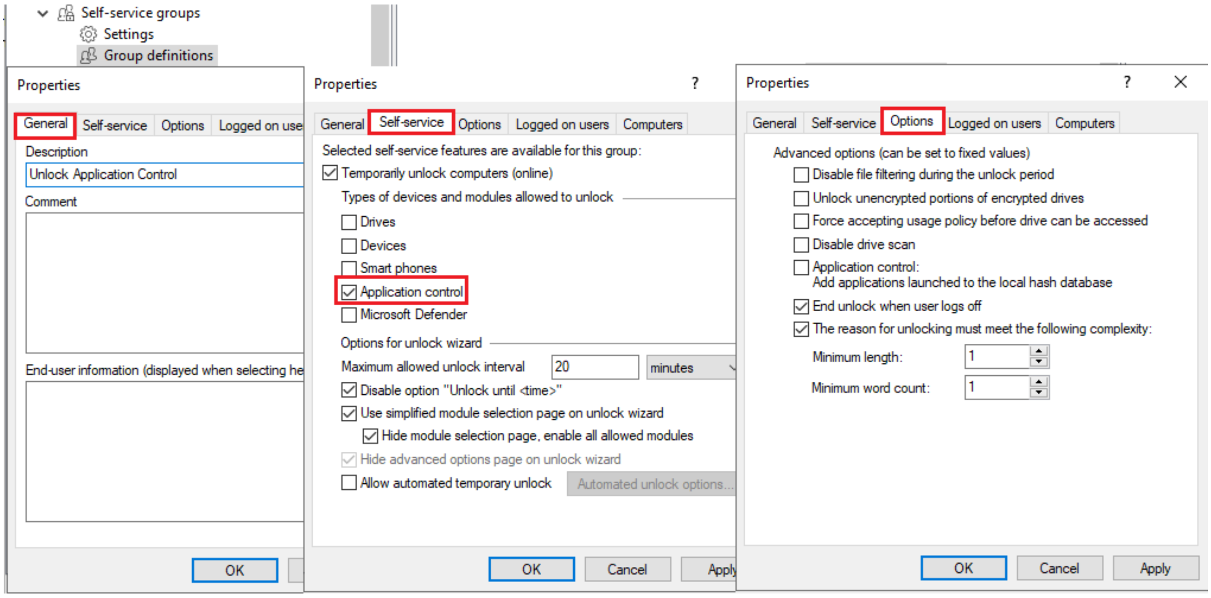
3. You can also set up the Self-service wizard to start as soon as a usage policy is applied. You can find out more here.

5.2.8.4 Use case for self-service with Application Control

Goal : Simple self-service to achieve that specific users may run applications that are not whitelisted during emergencies or maintenance. In this case, Application Control is temporarily deactivated with the help of self-service. The local whitelist is neither changed nor extended.

Please do the following:

1. Create a new self-service group. You can find details here .
2. Assign a description on the **General** tab and set the options on the **Self-service** and **Options** tabs as shown in the figure:



Self-service groups
Settings
Group definitions

Properties

General | Self-service | Options | Logged on use

Description: Unlock Application Control

Comment

End-user information (displayed when selecting he

Properties ?

General | Self-service | Options | Logged on users | Computers

Selected self-service features are available for this group:

☑ Temporarily unlock computers (online)

Types of devices and modules allowed to unlock

☐ Drives
☐ Devices
☐ Smart phones
☑ Application control
☐ Microsoft Defender

Options for unlock wizard

Maximum allowed unlock interval 20 minutes

☑ Disable option "Unlock until <time>"
☑ Use simplified module selection page on unlock wizard
☑ Hide module selection page, enable all allowed modules
☑ Hide advanced options page on unlock wizard
☐ Allow automated temporary unlock   Automated unlock options...

Properties ? ×

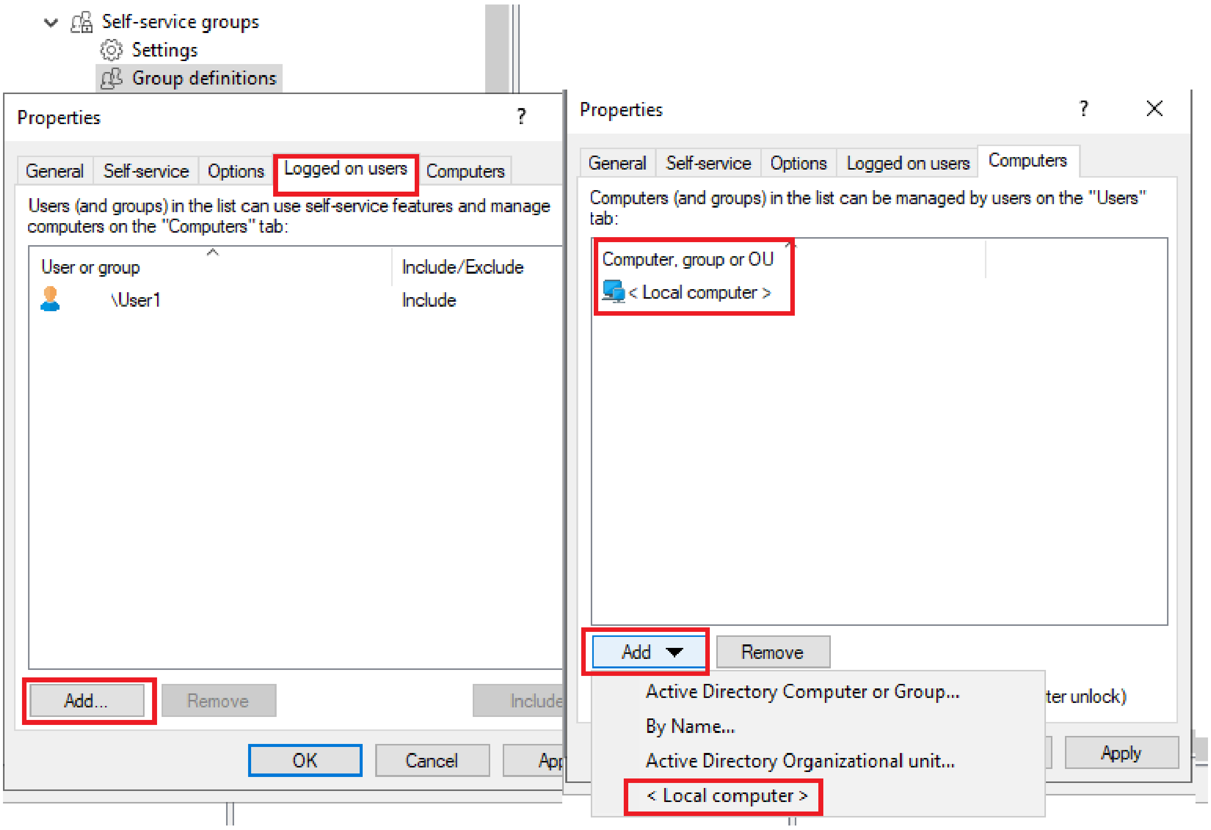
General | Self-service | Options | Logged on users | Computers

Advanced options (can be set to fixed values)

☐ Disable file filtering during the unlock period
☐ Unlock unencrypted portions of encrypted drives
☐ Force accepting usage policy before drive can be accessed
☐ Disable drive scan
☐ Application control:
Add applications launched to the local hash database
☑ End unlock when user logs off
☑ The reason for unlocking must meet the following complexity:

Minimum length: 1
Minimum word count: 1

3. On the **Logged on users** and **Computers** tabs, select the users and computers you want to enable self-service for. Use the Add button for this purpose. See example below:



Self-service groups
Settings
Group definitions

Properties ?

General | Self-service | Options | Logged on users | Computers

Users (and groups) in the list can use self-service features and manage computers on the "Computers" tab:

User or group	Include/Exclude
\User1	Include

Properties ? ×

General | Self-service | Options | Logged on users | Computers

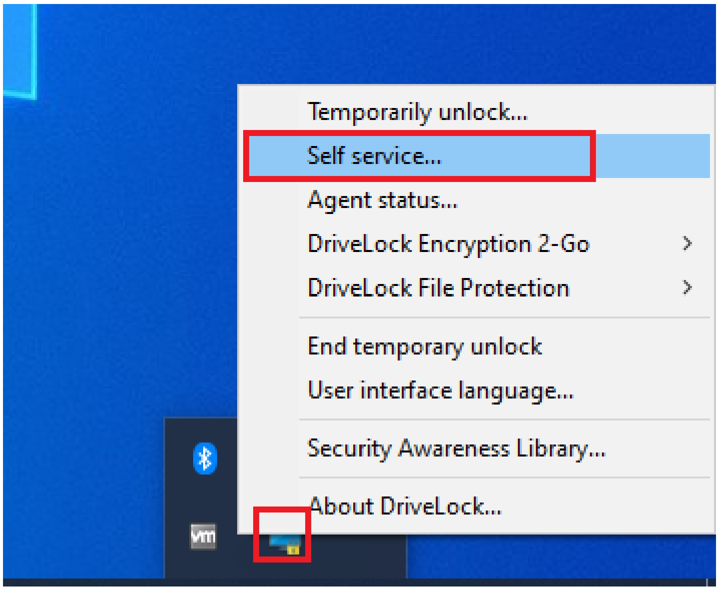
Computers (and groups) in the list can be managed by users on the "Users" tab:

Computer, group or OU
< Local computer >

4. Set the appropriate settings for the self-service in **Global configuration**, as shown here (explained under 1. and 2.).

5. Publish and assign the policy.

6. On the DriveLock Agent, the end user can now launch the Self-service wizard from the taskbar icon and then work with the required application in the set time.


Temporarily unlock...
Self service...
Agent status...
DriveLock Encryption 2-Go
DriveLock File Protection
End temporary unlock
User interface language...
Security Awareness Library...
About DriveLock...

5.3 Events and Alerts (Analytics)

You can monitor and configure all events that occur with DriveLock and its modules.

In addition to transmitting DriveLock events, the basic functionality also includes the ability to react to such events.

Risk & Compliance (EDR) provides additional functionality:

- Monitoring events from third-party providers,
- Defining and using filters, alerts and responses,
- Applying parts of the Application Behavior Control functionality,
- Using parts of the MITRE Attack Framework, which is supplied in an importable form of DriveLock rules.

For more information about MITRE Attack and Application Control, please check the documentation at DriveLock Online Help.

5.3.1 Event transmission

Before DriveLock actions can be logged, please specify that the DriveLock events have to be sent. Events can be sent to the Windows Event Viewer, SNMP, SMTP (email) or written to the central DriveLock database.

There are two event sources that are configured together:

- DriveLock Agent events (Source: "DriveLock")
- DriveLock Management Console events (Source: "DriveLockMMC")

To analyze DriveLock events, we recommend using the DriveLock Operations Center.

5.3.1.1 Configuring the event transmission

You can configure the way DriveLock event messages are logged and where they are stored. If you configure a remote destination and the computer is not connected to the network, all messages are temporarily stored on the local computer.

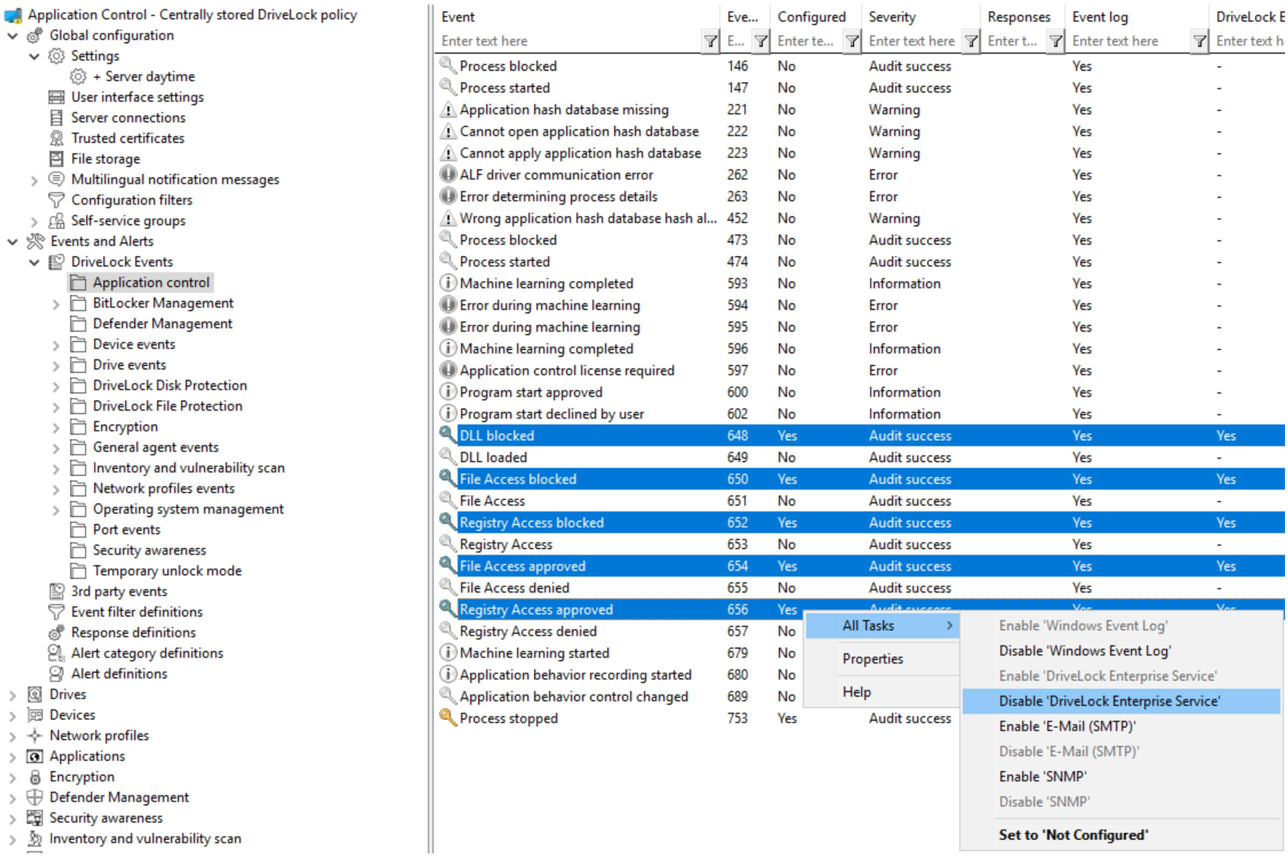
In the DriveLock Management Console, open the **Events and alerts** node in the console structure on the left, and then open the **DriveLock Events** subnode. In this subnode, all events are grouped by the components that create them. When you select a node, a list of available events is displayed in the right part of the window.

To change the settings for a specific event, double-click it to open its properties dialog. On the **General** tab, you can specify where this event should be sent (multiple destinations are possible) and whether multiple occurrences should be suppressed in a short time interval to take up less storage space in the log file(s).

Specified targets must be further configured.

On **Responses** tab, a specific action can be triggered when this event occurs. The action must be described beforehand as a response definition. The **Event Info** tab shows the event text and parameters in detail. This information is useful when creating event filters.

To quickly route multiple events to a target, select them in the right pane (using Shift and Ctrl), then right-click the selection. The context menu that opens contains a submenu **All Tasks**, which contains options to enable or disable each available event target for all selected events.



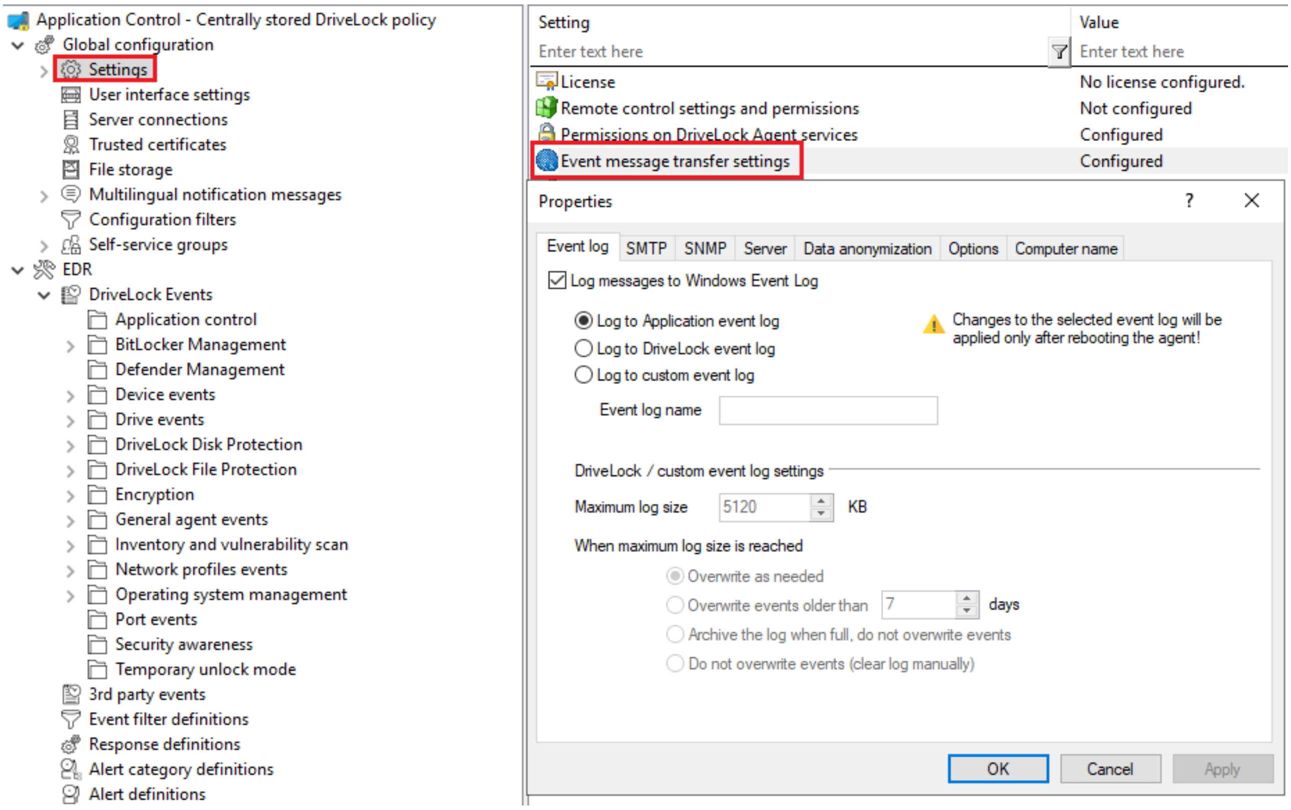
- Application Control - Centrally stored DriveLock policy
  - Global configuration
    - Settings
      - + Server daytime
    - User interface settings
    - Server connections
    - Trusted certificates
    - File storage
    - Multilingual notification messages
    - Configuration filters
    - Self-service groups
  - Events and Alerts
    - DriveLock Events
      - Application control
      - BitLocker Management
      - Defender Management
      - Device events
      - Drive events
      - DriveLock Disk Protection
      - DriveLock File Protection
      - Encryption
      - General agent events
      - Inventory and vulnerability scan
      - Network profiles events
      - Operating system management
      - Port events
      - Security awareness
      - Temporary unlock mode
    - 3rd party events
    - Event filter definitions
    - Response definitions
    - Alert category definitions
    - Alert definitions
  - Drives
  - Devices
  - Network profiles
  - Applications
  - Encryption
  - Defender Management
  - Security awareness
  - Inventory and vulnerability scan

Event	Eve...	Configured	Severity	Responses	Event log	DriveLock E
Enter text here	E...	Enter te...	Enter text here	Enter t...	Enter text here	Enter text h
Process blocked	146	No	Audit success		Yes	-
Process started	147	No	Audit success		Yes	-
Application hash database missing	221	No	Warning		Yes	-
Cannot open application hash database	222	No	Warning		Yes	-
Cannot apply application hash database	223	No	Warning		Yes	-
ALF driver communication error	262	No	Error		Yes	-
Error determining process details	263	No	Error		Yes	-
Wrong application hash database hash al...	452	No	Warning		Yes	-
Process blocked	473	No	Audit success		Yes	-
Process started	474	No	Audit success		Yes	-
Machine learning completed	593	No	Information		Yes	-
Error during machine learning	594	No	Error		Yes	-
Error during machine learning	595	No	Error		Yes	-
Machine learning completed	596	No	Information		Yes	-
Application control license required	597	No	Error		Yes	-
Program start approved	600	No	Information		Yes	-
Program start declined by user	602	No	Information		Yes	-
DLL blocked	648	Yes	Audit success		Yes	Yes
DLL loaded	649	No	Audit success		Yes	-
File Access blocked	650	Yes	Audit success		Yes	Yes
File Access	651	No	Audit success		Yes	-
Registry Access blocked	652	Yes	Audit success		Yes	Yes
Registry Access	653	No	Audit success		Yes	-
File Access approved	654	Yes	Audit success		Yes	Yes
File Access denied	655	No	Audit success		Yes	-
Registry Access approved	656	Yes	Audit success		Yes	Yes
Registry Access denied	657	No				
Machine learning started	679	No				
Application behavior recording started	680	No				
Application behavior control changed	689	No				
Process stopped	753	Yes	Audit success			

All Tasks >
Properties
Help
Enable 'Windows Event Log'
Disable 'Windows Event Log'
Enable 'DriveLock Enterprise Service'
Disable 'DriveLock Enterprise Service'
Enable 'E-Mail (SMTP)'
Disable 'E-Mail (SMTP)'
Enable 'SNMP'
Disable 'SNMP'
Set to 'Not Configured'

5.3.1.2 Targets for event transfer

Each of the possible targets to which events can be sent require different settings. To configure the targets events are sent to, open the **Global configuration** node in the console tree on the left and select **Settings**. Then click **Event message transfer settings** in the right pane to open the settings dialog. The individual tabs of this dialog box are described below.



Setting	Value
License	No license configured.
Remote control settings and permissions	Not configured
Permissions on DriveLock Agent services	Configured
Event message transfer settings	Configured

Properties

☑ Log messages to Windows Event Log

● Log to Application event log
○ Log to DriveLock event log
○ Log to custom event log

Changes to the selected event log will be applied only after rebooting the agent!

Event log name

DriveLock / custom event log settings

Maximum log size 5120 KB

When maximum log size is reached

● Overwrite as needed
○ Overwrite events older than 7 days
○ Archive the log when full, do not overwrite events
○ Do not overwrite events (clear log manually)

5.3.1.2.1 Event log

On the **Event log** tab, configure which event log DriveLock uses to store events locally. This setting determines whether the events of the agent are written to the Windows Application Event Viewer or to another event log. If you are not using the Windows Application Event Viewer, set the size and behavior when the log memory becomes full.

5.3.1.2.2 SMTP

Select the **SMTP** tab to configure SMTP settings for sending event messages by e-mail.

Select **Enable sending event messages using SMTP** to enable event log message transfer. Enter the required server properties and make sure that messages are accepted by your e-mail system. If your mail server requires authentication, you must also provide authentication credentials.

Click the **Message text** button to configure the actual email. The two > buttons on the right can be used to insert predefined wildcards into the text, which will be filled with current values at the time of execution. An e-mail can be sent both as text and as HTML e-mail.

Click **Test** to send a test email to the configured recipients. You will then see a corresponding message informing you whether all parameters have been configured correctly.

5.3.1.2.3 SNMP

On the **SNMP** tab, check Enable message transmission via SNMP traps option to transmit the events via SNMP and specify the required server properties.

5.3.1.2.4 Server

Click the **Server** tab to configure the transfer settings for DriveLock Enterprise Service.

Select **Enable event forwarding to DriveLock Enterprise Service** to enable event transmission to the central DriveLock database.

Select **Report agent status to server** if you want to specify the time interval of the transmission. By default, DriveLock Agent will send its events to DriveLock Enterprise Service every 300 seconds.

> Note: Note that the server connection must be configured under Global Settings / Server Connections.

5.3.1.2.5 Data anonymization

Data anonymization functionality is no longer configurable in this location. This is now only possible in the DriveLock Operations Center. See Data masking for more information.

5.3.1.2.6 Options

On the **Options** tab, you can specify how DriveLock processes DriveLock Enterprise Service messages when the client is offline. Event messages can be cached locally if DriveLock Agent cannot deliver them to the configured destination.

Select **Queue events when offline (...)** to enable temporary storage of messages. DriveLock agents always use an internal memory-based queue to temporarily store events when they are generated faster than they can be processed. In addition, you can configure the agent to store events in a disk-based queue when the agent is offline and cannot contact DriveLock Enterprise Service. Events are automatically deleted from both queues once they have been processed. You can configure the maximum number of messages that these queues can hold. If one of the two queues exceeds the limit you have configured, additional events are no longer forwarded to the DriveLock Enterprise Service and are only written to the local event log.

In general, each agent transmits event data in real time to the destinations you configure. In system environments where available network bandwidth is limited, DriveLock Agent can collect events and send multiple events together in packets. To enable this setting, select the **Send events in batches** check box and configure a packet size and interval appropriate for your network environment.

5.3.1.2.7 Computer name

If you do not want the default Windows computer name to be reported as the source of an event, the **Computer name** tab provides several options for customizing the name used. The computer name can be retrieved from a registry key, an INI file, or even from a custom DLL that returns the name. Select the appropriate radio button and enter the information required for the selected option.

5.3.1.3 Response to events (Response)

The DriveLock Agent can not only simply send event messages to various destinations, but also initiate a local response to the event ('Response') when the event occurs. Such a reaction can be the execution of a program or script, or taking a photo with a webcam connected to the system. Responses can be used with individual events (see here) and alerts (see here) once they have been defined and named.

To create a new **response definition**, right-click Response definitions, and then select **New...** in the context menu. The following response types are available:

- **PowerShell script**: Executes a named PowerShell script with optional parameters from the event to which the response refers.
- **Batch script** : Runs a batch script with the command processor, optionally with parameters.
- **Command line execution** : Starts any executable file, optionally with parameters.
- **Show awareness campaign**: Displays a defined awareness campaign when the event occurs.
- **Take picture using webcam**: Creates a recording when the event occurs and transmits it along with the event. This option should be used with caution, as it can quickly consume a lot of memory if the event is triggered too frequently.

Responses are defined via a dialog box with the following tabs.

On the **General** tab, a name and an optional comment can be entered.

Using the **Script** or **Command Line** tabs, the command or script to be executed is created including all parameters. The command line can be simply typed into the text field or created by selecting an executable file/script and all required parameters. However, to use the **Insert parameter** option, the parameters must first be defined on the Parameters tab.

For all response types, various options are available to define conditions for their use: The tabs **Computer** , **Networks** and **Times** can be used to activate or deactivate the response if certain conditions are met. This could, for example, trigger the response only on certain computers while they are connected to the corporate network and the event takes place outside regular office hours.

Click **OK** once all settings are complete to save the response definition. It will be added to the list of response definitions on the right. This list can then be used to select responses to events and alerts.

5.3.1.4 Event filter definitions

Event filters can be used to select specific instances of an event based on the event parameters. Besides the event number and the message, events often contain additional information. This information can be used to distinguish relevant from less relevant events. By defining event filters separately, they can be quickly reused in rules that require event selection.

To create an event filter, right-click **Event filter definition** sub-node and select **New...** from the menu. A list of available events is displayed. Select the event to which this filter should be applied and click **OK** .

A dialog box with tabs will be displayed. On the **General** tab, a name for the filter can be entered in **Description** - this is the name that will be displayed in the event filter list once the definition is saved.

The **Filter criteria** tab is used to define how the different instances of the event should be filtered. Using **Add** , criteria and logical operators can be added to the filter specification. The available criteria vary by event type, depending on the additional information logged with the event. Logical operators can be used to combine multiple conditions for event selection.

For describing a condition, start by adding an operator. Following operators are available:

- **AND**: All criteria associated with this operator must match
- **OR**: At least one of the criteria associated with this operator must match

- **N**: At least n criteria of the listed (more than n) associated with this operator must match The number n is selected when the operator is added.

To link a criterion to an operator, select the operator in the list, click Add and select Criterion. Select one from the displayed list of event parameters. The next dialog box is where you complete the criterion by selecting a comparison or match operator and one or more value(s) to compare. To add the criterion to the filter description, click OK.

You can change operators and conditions by selecting them and clicking **Edit** .

The **Computers**, **Networks** and **Times** tabs can be used to enable or disable the use of the filter on specific computers connected to specific networks during specific time periods.

Save the new filter definition. It will be added to the Alert definitions list on the right.

5.3.1.5 Alerts

Alerts are a method of generating a meta event, for example, when certain combinations of events occur within a short period of time. Instead of looking for patterns in event logs, it is possible to use an alert definition to detect and immediately report such a pattern. Besides reporting the detection, an alert can also trigger a corresponding response.

> Note: Please note that if Event Encryption is configured, the content of the alert events will be displayed unencrypted in the DriveLock Operations Center (DOC) and in the possibly defined response in order to be able to report business-critical events (e.g. data theft) instantaneously and with useful content.

To create an alert definition, right-click **Alert definition** subnode and select **New...** A dialog with multiple tabs will be displayed.

On the tab **General** a name for the alert can be entered in **Description** - this is the name that will be displayed in the list of alert definitions once the definition has been saved. In addition, **severity** and **alert category** can be set in order to organize the alert reports in the DOC. Alert categories must be defined in "Alert category definitions" in "Events and alerts" and are managed on the server.

On the **Conditions** tab, you can define the criteria for triggering the alert. Click **Add** to add logical operators and criteria that describe the condition(s) for the alert.

The simplest condition that can be used for an alert is matching a single Event filter. To do this, simply click **Add, Criterion**, and select the suitable event filter from the list.

It is also possible to combine several event filters: First add one of the logical operators **AND**, **OR** or**N**. Then select the operator in the conditions list and click **Add** once again to start adding criteria to which the operator will apply. Selecting the criterion opens the **list of event filters** for selecting a filter to be used in the condition. Continue adding a criterion until all required event filters are listed below the selected operator. Be sure to select an appropriate time window in **Events for this condition must occur within ... seconds**, to prevent the condition from encountering unrelated events that trigger false alerts.

On the **Responses** tab an immediate response can be set up in addition to the alert message. In the **response to execute** drop-down list, select a response from the response definitions list. The parameter definitions for this response are displayed in the **Parameter mapping** list. Select a parameter and click the **Edit** button to customize the parameter value to be used in this alert if the value in the response definition is not suitable.

The tabs **Computers**, **Networks** and **Times** can be used to enable or disable the use of the filter on specific computers connected to specific networks during specific time periods.

Save the new filter definition. It will be added to the Alert definitions list on the right.

5.3.2 Data masking in events

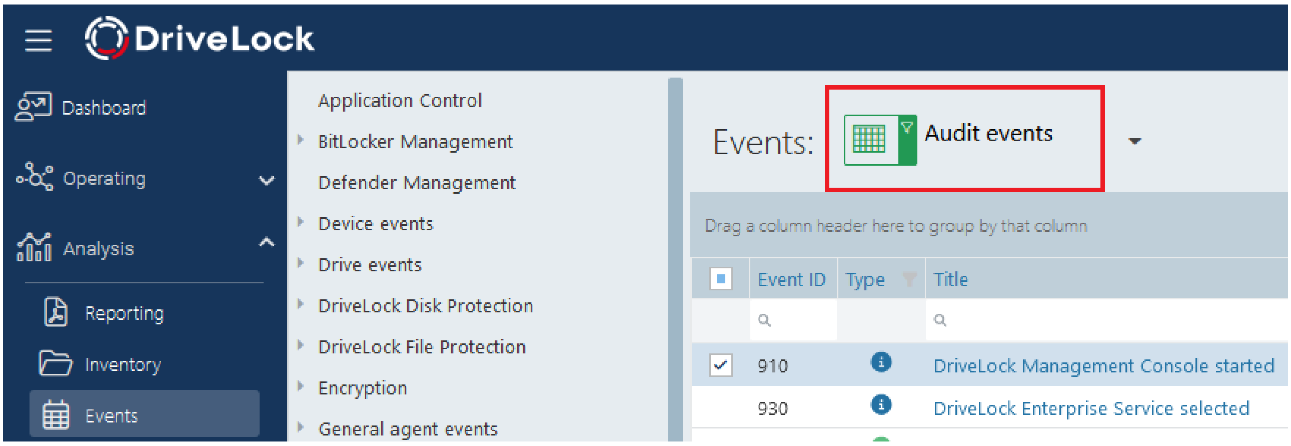
Please note that names are not displayed in plain text in the DOC if data masking is enabled and filtering is set to user and computer names. System user names are always displayed by default, but by deactivating the option **Show 'Integrated user' in plain text.**but they can also be masked. You can filter them by using the Is system user filter **Is system user** property.

5.3.3 Audit events

Audit events are events used to track administrative and security actions triggered by DriveLock accounts in the DOC and MMC; they are issued, for example, whenever policies or permissions are changed.

Audit events can be processed like other events. In the database they are marked with a flag.

To display audit events, you can select the **Audit events** filter in the **Events** view in the DOC (see figure).



For a list of all events and audit events, refer to the DriveLock Events documentation at DriveLock Online Help.

5.4 Drives and Devices (Device Control)

With DriveLock Device Control you are able to control all removable and external devices and drives. Using rules (whitelist or blacklist), you define which actions are allowed.

Device Control offers the following functionalities, among others:

- Control of all externally connected media: you define who is allowed to use which drives at which time.
- Integrated data flow control through data type checking: You define who is allowed to read or copy which data.
- Audit of file operations: You control who copied which file to which media at what time.
- Security for network shares or WebDAV-based drives: You define who is allowed to use which drives and when.
- Shadow copy creation and forced encryption
- Data volume control: You define how high the data volume may be that is transferred between the removable storage device and the end device,

5.4.1 Drives

DriveLock operates with whitelist rules. This means that after you enable basic drive locking for a specific type of drive, this drive type is initially locked. Exceptions have to be configured separately by means of a whitelist rule. That is, you create a rule for every drive (or group of similar drives) you want to use. If a drive is not listed in a corresponding rule, DriveLock automatically blocks access to it and it cannot be used. This will ensure that your environment's security level remains intact, even if new or unfamiliar devices are introduced and accessed by your end users at some point in the future.

You can find an overview on how drive control interacts here.

To configure drive locking, we recommend creating the required drive whitelist rules first and then activating the general removable drive locking settings.

> ❗ Warning: For security reasons, USB flash drives, for example, are locked by default without any previous configuration. This is the default configuration when you install a DriveLock Agent on a computer without previously configuring and deploying a policy. This way, your environment is protected in situations where an agent is unable to get or process policies.

DriveLock provides functionality for defining drive rules for various scopes (beginning with the broadest scope):

- Drive classes (for example all USB drives)
- Drive size (for example, all drives with a capacity larger than 128 MB)
- Manufacturer (for example SanDisk)
- Product ID (for example Ultra II 1 GB Compact Flash)
- Serial number

In addition to the scope, you can also configure how and when whitelist rules are applied.

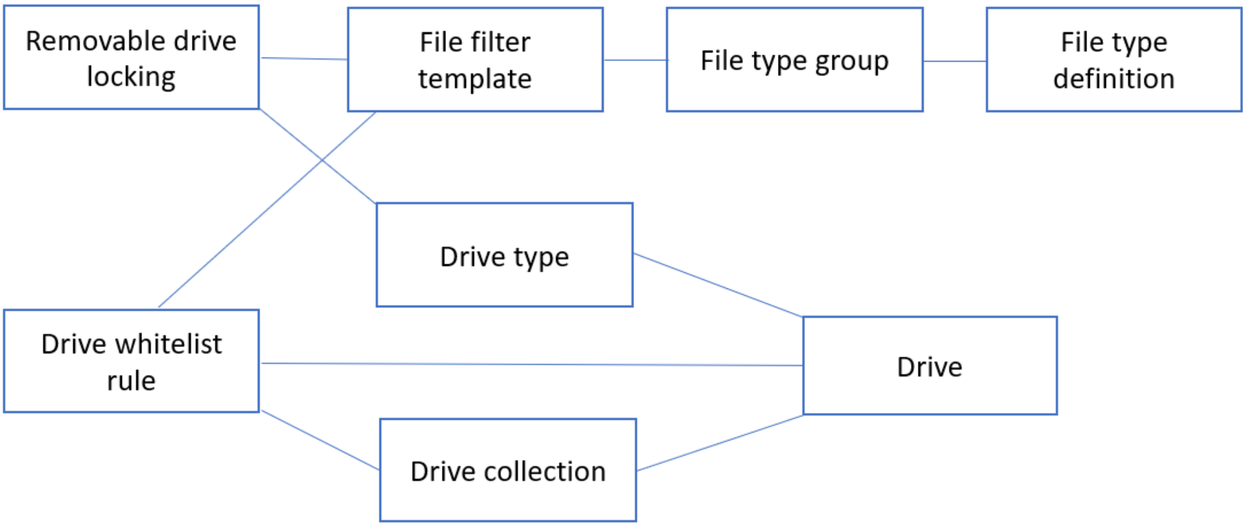
- Select the computers (all or only some) you want the rule to apply to.
- Which active network connections do you want the rules to apply to?
- During which time (e.g. Monday to Friday between 09:00 and 18:00)?
- Do you want the rules to apply to all users, or is a specific group member allowed to use a drive (or device) while it is locked for all other logged-on users?
- Does the logged-on user have to agree to a company policy before being granted access?
- Is an attached USB stick encrypted?
- Is a virus scanner service active?
- Does a USB stick possibly contain malware?

Considering these scopes and questions in your planning helps to reduce the number of rules needed in your configuration and thereby your administrative workload.

Warning: When you evaluate DriveLock, we recommend that you enable removable drive locking first before configuring individual rules. Our Managed Services environment provides predefined policies that are already available and which you can evaluate.
In a production environment, make sure that you first create all the necessary rules before enabling locking completely.

5.4.1.1 Drive control overview

The following figure shows how the different elements are related to each other.



The removable drive locking settings are used to specify the type of drive you want to lock at a general level. Here, you can use file filter templates, file type definitions or file type groups that you have created earlier. In this case, proceed as follows: first define the file type, then specify a file type group, then create the file filter template, and finally specify the removable drive locking setting.

By means of the drive whitelist rules you can define specific criteria that will apply to particular drives. You can use the file filters you created earlier (see above) and drive collections. Note that each drive rule may have different criteria for defining drives, for example, by vendor ID, by drive letter, or by being a network drive.

Note: General rules have a lower priority than special rules. That is, a drive whitelist rule has a higher priority than a general removable drive locking setting.

The drive rules you can create in the DriveLock Operations Center (DOC) are different.

5.4.1.2 Settings

When configuring drive lock/share settings, you can specify the following settings.

- Global security settings
- Customized user notifications
- Settings of the file hash generation
- Drive identification file settings
- Shadow copy settings
- Hard disk self-monitoring (SMART) settings
- Advanced settings

5.4.1.2.1 Global security settings

Setting	Functionality
Always allow access to administrators	You have the ability to share access to drives with all members of the Administrators group, regardless of which whitelist rules or settings are enabled.
Format and eject removable media	You can also specify which users are allowed to eject or format removable media. Via Add you can add users or groups to the list, via Remove you can delete them.

5.4.1.2.2 Custom user notification messages

If you enable user notification, DriveLock displays a notification message when a drive is connected to the computer and locked. Configure this setting to customize your own messages. You can also use some of the HTML tags for formatting your message (for example `<b>Text</b>`).

Note: If you have configured multilingual user messages, DriveLock displays the default messages in your current language.

5.4.1.2.3 Configuring file digest (hash) generation

Each time a file is read from or written to an external disk, DriveLock generates a hash value (digest) of the file name. This hash value can be used for more detailed investigation of file transfer and tracking of files in your organization.

You can specify the hash algorithm you want to use and whether you want to generate another hash value (the content hash value) by selecting a hash algorithm from the list. Due to company policies, it may be necessary to use a specific hash algorithm.

To enable the generation of content hash values, select the **Generate digest from file contents** option and set whether they will be generated synchronously or delayed. For larger files, generating these hash values can take some time.

5.4.1.2.4 Volume identification file settings

In most cases, storage media are uniquely identifiable via a hardware ID (manufacturer ID, product ID, serial number). There are also storage media, such as SD cards or NoName USB sticks without hardware ID and cases where the hardware ID cannot be accessed. For example, when the storage media are connected via thin clients (without DriveLock Virtual Channel) or SD cards via USB SD card readers.

You can create volume identification files with a drive ID on this type of storage media. By doing so, DriveLock will be able to identify them.

If you select Use volume identification files (if present), the ID from the file overwrites the hardware ID of the storage medium.

Security and compatibility mode:

- **High secure**: the drive ID must match the volume serial number of the partition. If a drive identification file is copied to another partition, it is invalid. Some ICA-based thin clients do not transmit the volume serial number to Windows. DriveLock then cannot verify the drive ID.
- **Medium secure**: the drive ID must match the size of the partition. If a drive identification file is copied to another partition, it is invalid.
- **Low secure**: a drive identification file can be copied to another partition. DriveLock accepts a drive ID regardless of the volume serial number or the size of the partition. Use this option only if your thin client does not transmit a volume serial number and size.

The drive identification file contains all three security modes. Always start with Very secure and reduce only if necessary. Existing drive identification files remain valid even if the security mode is changed.

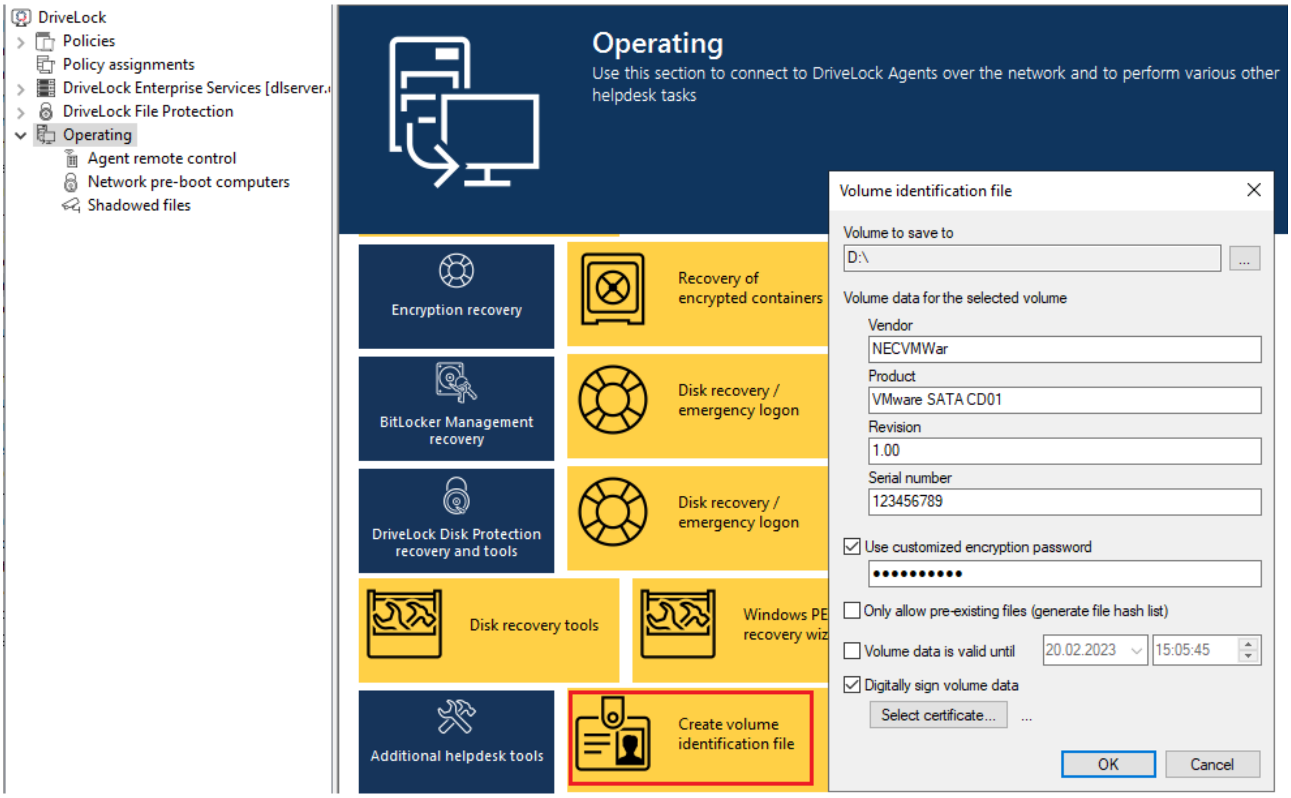
If you enable the **Automatically create volume identification file [...]** option, this type of file is automatically created with the hardware ID values as soon as a storage medium on a FAT client (not thin client) is connected to DriveLock.

Volume identification files are encrypted either with a preset key or, if set, with the key generated from the customer-specific password. If you change the password all existing drive identification files are invalid.

> Note: Volume identification files are not visible for normal users (attributes Hidden, System)

5.4.1.2.4.1 Create volume identification files manually

In the DriveLock Management Console, in the **Operating** node, open the **Create Volume identification file** option and enter the required data to create volume identification files, for example, on SD cards.


DriveLock
Policies
Policy assignments
DriveLock Enterprise Services [dlserver.
DriveLock File Protection
Operating
Agent remote control
Network pre-boot computers
Shadowed files
Operating
Use this section to connect to DriveLock Agents over the network and to perform various other helpdesk tasks
Encryption recovery
Recovery of encrypted containers
BitLocker Management recovery
Disk recovery / emergency logon
DriveLock Disk Protection recovery and tools
Disk recovery / emergency logon
Disk recovery tools
Windows PE recovery wiz
Additional helpdesk tools
Create volume identification file

Volume identification file

Volume to save to: D:\

Volume data for the selected volume

Vendor: NECVMWar

Product: VMware SATA CD01

Revision: 1.00

Serial number: 123456789

☑ Use customized encryption password: ••••••••••

☐ Only allow pre-existing files (generate file hash list)

☐ Volume data is valid until 20.02.2023 15:05:45

☑ Digitally sign volume data

Select certificate... ...

OK Cancel

5.4.1.2.5 Shadow copies

Shadowing creates copies of files transferred to or from removable media to allow administrators to review what data users accessed. DriveLock can store these shadow copies on client computers and a server. You can define which files DriveLock shadows.

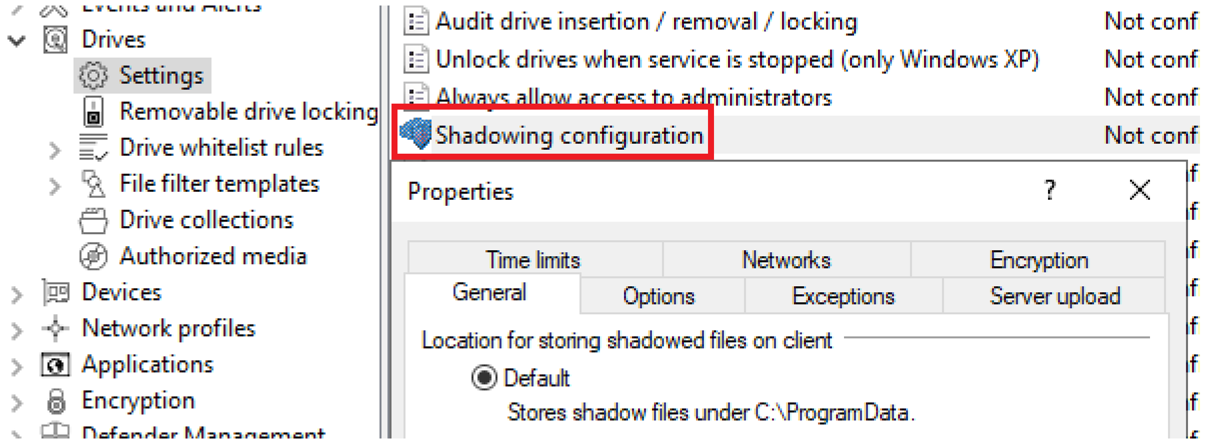
Example: If you enable shadow copies for USB drives, DriveLock will create an ISO image of each USB drive and save this file to the location you configure.

There is a special setting for creating shadow copies. To enable shadow copies, a file filter template must first be created, which can then be used for individual whitelist rules as well as for drive classes (settings on the Filter / Shadow Copy tab).

Shadow copies can be viewed using the DriveLock Management Console. For this purpose, the **Shadowed files** option is available in the **Operating** node. Open the context menu of the respective shadow copy and select **Choose folder / agent...**. After a successful connection, the shadow copies are listed in the Management Console. Double-click to display the properties of the respective file; use the Extract shadowed files command to store the shadow copy in a different location. If you have set up a password or certificates to protect the shadow copies, you must now authenticate with the appropriate keys.

5.4.1.2.5.1 Shadowing configuration

You can configure settings for shadow copies as follows.



Audit drive insertion / removal / locking Not conf
Unlock drives when service is stopped (only Windows XP) Not conf
Always allow access to administrators Not conf
Shadowing configuration Not conf

Location for storing shadowed files on client
● Default
Stores shadow files under C:\ProgramData.

1. On the **General** tab, specify:
   - **Location for storing shadowed files on client**: The shadow copies are stored in the `C:\ProgramData\CenterTools DriveLock\ShadowFiles` folder by default. However, it is also possible to specify a different storage location. To do so, select "Fixed location" and specify where to store the files. By default, only

the administrator and domain administrators can fully access this path.

- **Storage limitations**: Specify a maximum file size or the maximum storage space occupied by shadow copies. By default, only files up to 5 MB in size are copied and no more than 100 MB of disk space is used. Optionally, you can define how much data (KB) of each source file should be copied. If this option is enabled, it is no longer possible to open the copied files with the original application; a hex editor can then be used to view the contents.
- **Local storage cleanup settings**: Specify which files are deleted first when the selected maximum storage capacity for shadow copies is reached and how often you want to perform this task. Alternatively, the files can be deleted automatically at a specified time. These settings only affect the cleanup on clients. No cleanups take place on a central repository (on a server). By default, cleanup takes place every 5 minutes.

2. On the **Options** tab, specify:
    - **Create a local shared folder on clients**: If you select this option, DriveLock will automatically create a network share with the defined name. This network share can then be used to access the locally stored shadow copies. Local administrators and domain administrators are granted full access to this share.
    - **Do not delete local files after uploading to central location**: If shadow copies are uploaded to a central network server, by default they are deleted from the clients after upload. This can be prevented via this option. However, the shadow copies are still subject to the cleanup settings in this case.
3. On the **Exceptions** tab, you specify:
    - **Exclude selected processes (or users) from shadowing and auditing**: It is possible to exclude certain processes, users or groups from creating shadow copies. If a file is read or written by a process, user or group defined in this way, no shadow copy is created in this case. This option is primarily intended to exclude certain frequently accessed processes - such as virus scanners - from creating shadow copies.
      Click Add or Remove to define processes or users/groups.
4. On the **Server upload** tab, specify:
    - **Upload shadowed files to central server**: DriveLock offers the possibility to store shadow copies centrally. For this purpose, the path of a network share can be specified. DriveLock uses the user account, which also needs to be defined, to

access the network share and store the shadow copies there. This process takes place at a configurable time interval (default 15 min).

5. The tabs **Time limits** and **Networks** are cross-module settings and described here.
6. On the **Encryption** tab, specify:
   You can protect the shadow copies from unauthorized access. DriveLock encrypts the shadow copies with an internal key before uploading. You can additionally secure this key with a password or with the public key of one or more certificates (multi-eye principle). In that case, every time you open the shadow copy store, you need the appropriate password or private keys to access the shadow copies.

> Warning: If you lose these keys, you will no longer be able to view the contents of the shadow copies.

5.4.1.2.6 Hard drive self-monitoring (SMART) configuration

With the help of S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology), you can monitor the operating status of internal hard drives. This helps you detect errors early and avoid long downtimes of clients due to defective hard drives. The status can then be read out via reporting or remote agent control. To enable monitoring, click Hard drive self-monitoring (S.M.A.R.T.) configuration and check **Enable monitoring hard disks [...]** and specify the time period, for example, 60 minutes.

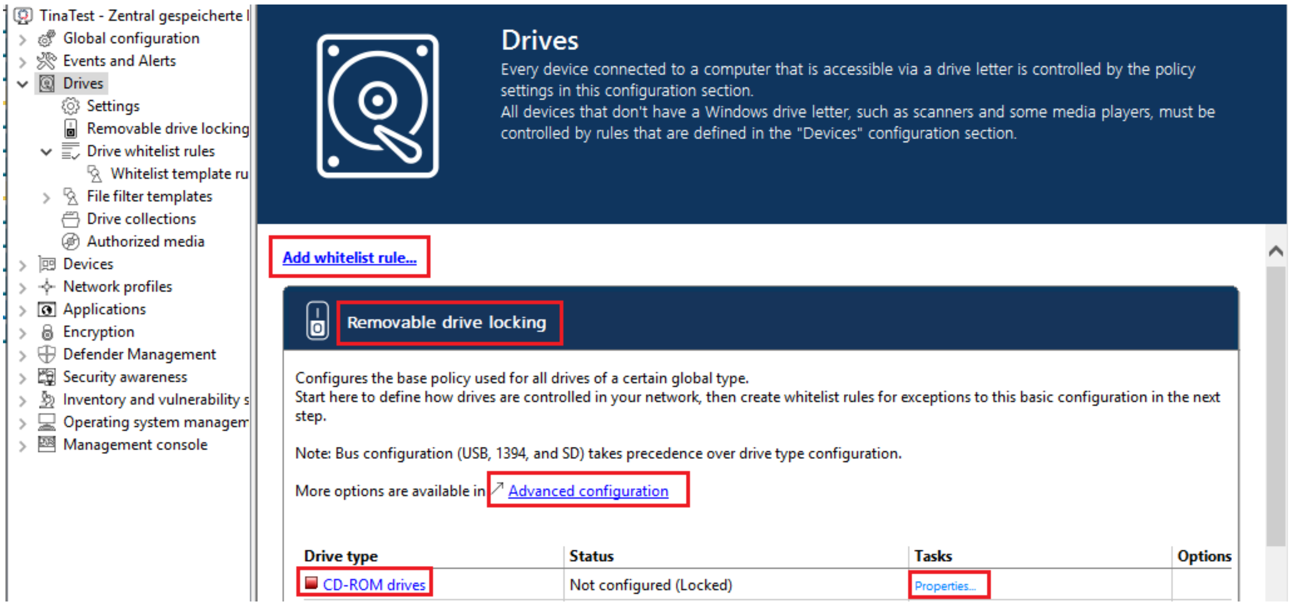
5.4.1.2.7 Advanced settings

Setting	Functionality
Audit device insertion / removal / lock	If activated, corresponding monitoring events are generated for the three events.
Unlock drives when service is stopped (only Windows XP)	Enable this feature to unlock all drives when the DriveLock service is stopped. (This setting is valid for Windows XP only)

5.4.1.3 Removable drive locking

The basic configuration allows you to easily enable or disable basic blocking settings and to add basic whitelist rules. To specify detailed settings for controlling drives, click **Advanced**

configuration in the various sections. Here you can find additional configuration options.



Drives

Every device connected to a computer that is accessible via a drive letter is controlled by the policy settings in this configuration section.
All devices that don't have a Windows drive letter, such as scanners and some media players, must be controlled by rules that are defined in the "Devices" configuration section.

Removable drive locking

Configures the base policy used for all drives of a certain global type.
Start here to define how drives are controlled in your network, then create whitelist rules for exceptions to this basic configuration in the next step.

Note: Bus configuration (USB, 1394, and SD) takes precedence over drive type configuration.

More options are available in Advanced configuration

Drive type	Status	Tasks	Options
CD-ROM drives	Not configured (Locked)	Properties...	

With DriveLock, you can control all drives that Windows detects as either removable or fixed. This includes the following classes in particular:

- Floppy drives: All internal floppy drives
- CD-ROM drives: Internal CD-ROM / DVD / BD drives (incl. burner).
- USB-connected drives: All drives that are connected via USB, e.g. USB sticks, USB hard disks, USB CD-ROM drives, USB card reader devices.
- Drives connected via Firewire (1394): All drives connected via Firewire, e.g. Firewire hard disks.
- SD card drives (SD bus): Especially in notebooks, there are pure SD card readers that are handled via this drive class
- Other removable media: All drives that do not fall into any other category, e.g. ZIP drives.
- Hard disks (eSATA hard disks, not exchangeable, no system included): All internal and external drives that are accessed via IDE, ATAPI, SCSI, RAID, SATA, or eSATA.
- Encrypted drives: special DriveLock proprietary drive class for drives encrypted by DriveLock. For more information, see the Encryption 2-Go chapter in the DriveLock Encryption documentation at DriveLock Online Help..
- Network drives and shares: Windows network drives
- WebDAV network drives: drives connected via WebDAV protocol and http/https

- Windows Terminal Services (RDP) client drive mappings
- Citrix XenApp (ICA) Client Drive Mappings

Warning: Boot partitions and partitions containing the page file are never blocked by DriveLock.

If a drive is connected via another interface, DriveLock treats it like "other removable media".

To change the settings for a drive type (e.g. other removable media, see the figure), click the corresponding link or Properties.

In the basic configuration, options are available on two tabs:

On the **General** tab:

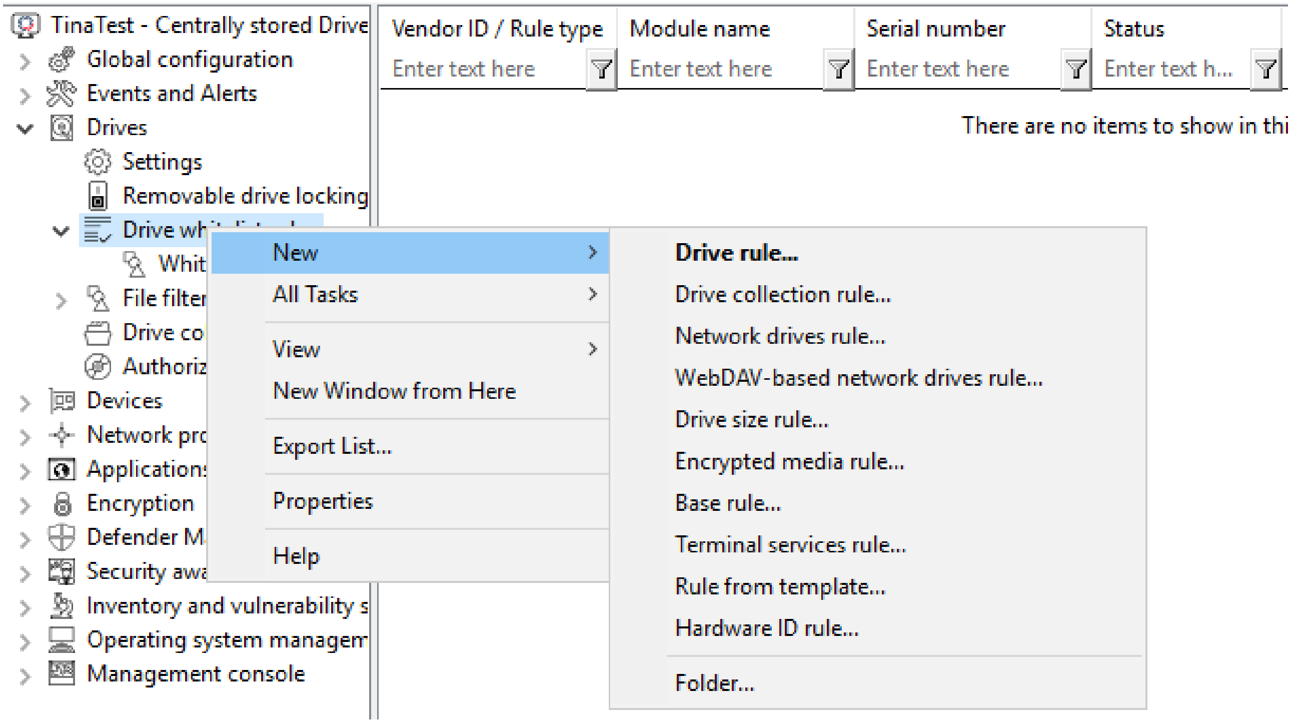
- **Allow**: Any authenticated user can use this drive
- **Deny (lock) for all users (default)**: Access to this drive is locked for all users.
- **Deny (lock), but allow access for defined users and groups**: The drive is locked, but access is possible for the specified user(s) or group(s), either read only or also write.
- To include another group or user in the list, click **Add**. Click **Remove** to delete the previously selected entry. Specify for the user or group whether they can copy data to the drive or whether read-only access is allowed.

On the **Options** tab you can select **Filter files read from or written to drives of this type...** or **Audit and shadow files [...]** to activate file filtering and the selected templates. Select one of the provided file filter templates from the list, available in the basic configuration.

- With the**Enforced encryption** option, you specify that the devices will be unlocked only if they have been encrypted earlier. In addition, you can specify that unencrypted drives are automatically encrypted.
- To force a user to confirm the usage policy first, enable the **User must accept usage policy before rule will be applied** option.
- To configure a custom message for a rule, enable the **Display custom message in user notification** option. Then enter a text which will be displayed regardless of the currently set system language.

5.4.1.4 Drive whitelist rules

Different types of whitelist rules are available and can be used to define drives according to specific criteria:



- **Drive rule**: Use this rule to define a particular drive in detail, for example, based on its serial number.
- **Drive collection rule**: The settings in this rule apply to a collection of drives you defined previously.
- **Network drives rule**: You can create this rule for directories being shared in the network (network share).
- **WebDAV-based network drives rule**: This rule applies to web drives which are connected via a URL and the WebDAV protocol.
- **Drive size rule**: In this rule, the drive/device is defined based on its size. If you activate the rule for ATA/SCSI it also applies to local hard drives. If you lock a local hard drive by mistake, you must start the computer in Safe Mode and reverse the configuration setting. This requires that the DriveLock Agent is not configured to start in Safe Mode.
- **Encrypted media rule**: This rule is applied when you want to allow or block only encrypted removable media (USB sticks or similar). This rule is only valid in connection with Encryption 2-Go, File Protection or BitLocker To Go.

- **Base rule**: Use a base rule to define exceptions for all drives of the same type. You can use this rule to define exceptions for a certain class of drives or to create time restrictions or computer-related rules.
- **Terminal services rule**: The settings in this rule are configured for a specific drive letter within a Terminal Server connection.
- **Rule from template**: Apply the whitelist rule templates you already created in this rule.
- **Hardware ID rule**: The settings in this rule apply to a specific hardware ID.
- **Folder**: You can store your whitelist rules in a directory structure (with child directories), just like you generally manage your files in folders. To create a new whitelist rule right away in a specific folder, right-click the folder and then select the desired rule type.

Rules are prioritized as follows:

1. Drive rule (a rule with a serial number has a higher priority than a rule without).
2. Device collection rule
3. Base rule
4. General removable drive locking settings

Note: A general rule has a lower priority than a special rule.

5.4.1.5 Whitelist template rules

A whitelist template is a whitelist rule that can be used as a template for other whitelist rules. Templates cannot be used directly as whitelist rules to control drives, but you can use them to create new whitelist rules.

If you need to create several rules where some settings stay the same (for example, for the same type of USB drives) and only a few settings change, you can save a lot of time with the help of a whitelist template. Instead of creating each rule step-by-step and selecting the same settings over and over again, a single whitelist rule template is convenient.

5.4.1.6 File filter templates

Using file filters, you can define your own write and/or read permissions for configured removable media and/or individual whitelist rules.

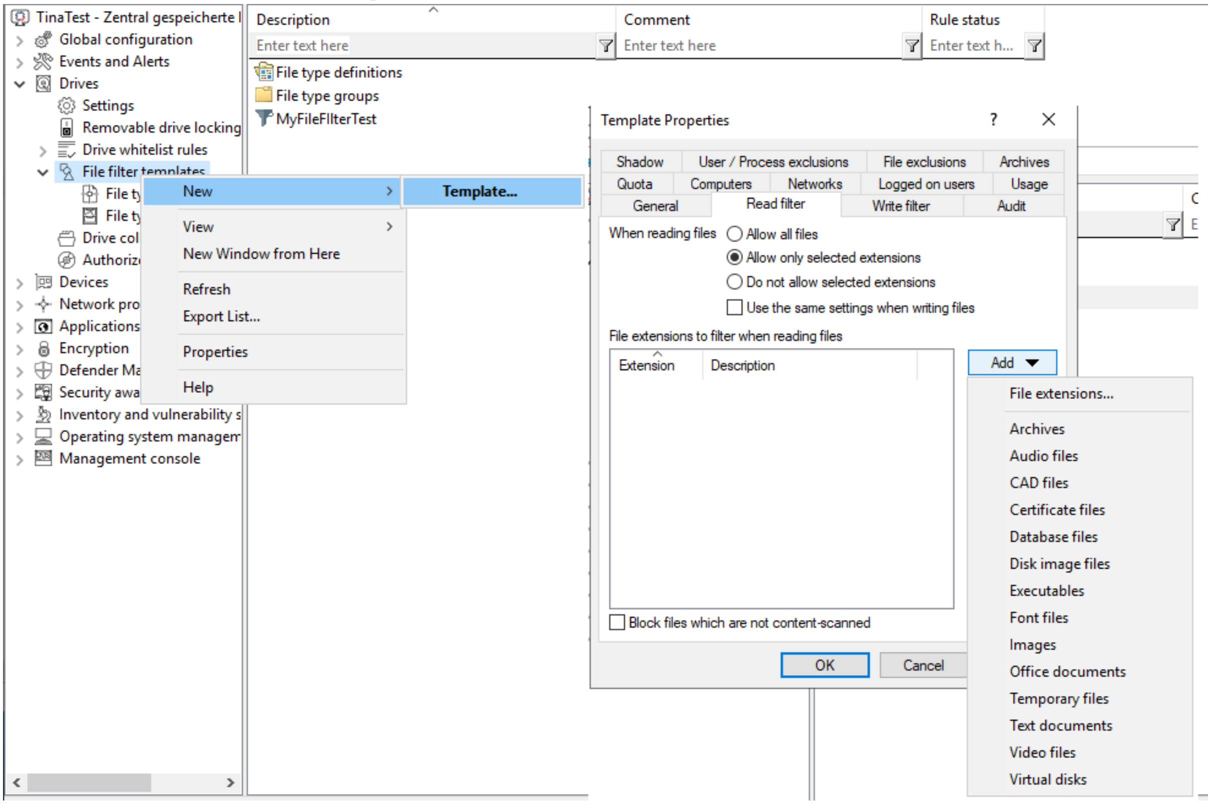
These filters can differ between read or write access and also check the file type. For example, it is possible to create a file filter that includes read permission for graphic files and write permission for Word documents. Filter templates can be used to create several of these rules according to your requirements.

DriveLock also includes a file header check, which means that DriveLock checks whether a file with a certain extension (e.g. *.docx) is actually a Word document and not a renamed MP3 file. Note that some file formats have the same header (e.g. Microsoft Office documents), while others have no specific or even a random file header. Once you have created a file filter template, it can be used as part of a drive type configuration or within a drive whitelist rule.

5.4.1.6.1 Creating a new file filter template

Follow these steps to create a new File filter template:

1. Select **New** and then **Template**.



2. On the **General** tab, enter a name in the **Template description** field and optionally a comment.

3. Next, open the **Read filter** tab. All file extensions specified here are checked each time a file is read or copied from a specific drive (e.g. a removable hard disk). You can either allow or block an extension. Enable **Allow all files** if you do not want to set up a

read filter. To allow only certain file types, select **Allow only selected extensions**. If you want to forbid certain files, check **Do not allow selected extensions**. Unless content checking has been explicitly disabled for a particular file type, DriveLock also checks whether the content and the file extension match. If this is not the case, access to this file is blocked. Click **Add** to add more file extensions to the list. You can also choose from the existing file type groups. Select the required extensions (or enter the required extension) and click **OK** to add the selection to the list.

4. Then open the **Write filter** tab and proceed as described for the read filters. All file extensions configured here are checked each time a file is copied to a specific drive (e.g. a removable hard disk) (or when a write access occurs).
5. Next, open the **Audit** tab. These monitoring settings determine which monitoring events are generated. Customize them according to your company policy or requirements.
   Monitoring events are sent either to the Windows Event Viewer or - if available and configured - to the DriveLock Enterprise Service.

   > Note: Please note that monitoring file operations may affect the performance of your systems. Furthermore, a user activity may generate more than one event (e.g. opening a Word document results in three different entries because Word first opens the file, then writes information - Last Access - and then opens it again.

6. On the **Shadow** tab, you specify the files you want to create shadow copies from. You can therefore set whether no shadow copies or shadow copies of all files are created, or only of files that are read or written. Furthermore, it is possible to specify a list of file extensions for which shadow copies are created (**Create shadow copy for selected file types only**) or not (**Do not create shadow copy for selected file types**).

   > Note: It is possible to create a File filter template for shadow copies only.

   A filter template created in this way can be used for individual whitelist rules and for drive classes.
   To do so, open the **Shadow** tab for the relevant drive class (e.g. USB) or for device-specific whitelist rules.
7. On the **User/Process exclusions** tab you can exclude users or processes from a shadow copy and logging,same as you can exclude folders and files on the **File exclusions** tab.

8. On the **Quota** tab, you can select one of the two options **When reading, deny access to files larger than ... KB** or **When writing, deny access to files larger than ... KB** to prevent read or write access to files that are too large. Enter an appropriate number. You can also limit the amount of data.
9. On the **Archives** tab, two options, each for read and write accesses separately, are available so that DriveLock applies this file filter also within archive files (ZIP and RAR). If you want DriveLock to search within these archives for the files defined in this template, enable one or both of the options **[...] Scan archive files**.
   To generally block archives that contain archive files, activate the **Block nested archives** option.
   To block archives that are password-protected and cannot be checked for that reason, activate the **Bock password-protected archives** option.

   > Note: Please note that for technical reasons, archive scanning is currently not yet possible for network and WebDAV drives.

5.4.1.6.2 Creating file type definitions

With DriveLock, you can define your own file types with specific file extensions and content.

You can use definitions that are already built in to save you time and effort. Before you can use the built-in types, they must first be created by right-clicking on **File type definitions** and then **All tasks** -> **Create built-in type definitions**.

If you want to create individual file types, right-click **File type definitions** and then select **New** -> **File type definition**.

On the **Type definition** tab you specify how to detect the file type. A file can be verified either by checking its contents or by calling a custom DLL - which you can create yourself.

A content check uses an offset (a value in hexadecimal notation) and a byte sequence, either in text form or also represented as a hexadecimal byte sequence. The length is entered automatically.

Specify whether all or only one of the specified checks must be successful for verification.

If you use your own DLL, specify the full path and name of the included function.

> Note: The specified DLL must exist locally on the hard disk of the workstation. It is not possible to specify a UNC path or use the policy store.

If you want DriveLock to check only the file extension and not the file content, enable the **Do not check any header for this file type**.

5.4.1.6.3 Creating file type groups

To use two or more file type definitions in a single step within a file filter template, you can combine file type definitions into **File type groups**.

You can create your own groups, in addition to the most common file type groups already provided by DriveLock, such as the group of all audio and video files.

Before the built-in groups can be used, they must first be created by right-clicking **File Type Groups** and then **All Tasks** -> **Create built-in file type groups**. To change an existing file type group, double-click the group you want to change.

To create a new file type group, right-click **File type groups** and select **New**. You can also add several file types at once by holding down the CTRL key and clicking on the necessary file types.

5.4.1.6.4 File filter template for encrypted drives

To apply a file filter template to encrypted drives, you need to perform an additional step. In this case, it is not enough to have a file filter active on USB-attached drives, as this is the unencrypted partition that is ideally locked to the user anyway. The encrypted container (stored on the USB-attached drive) is loaded as an extra drive and is a separate drive class from DriveLock's point of view - an encrypted container. For a file filter to be active in an encrypted container, you need to create a whitelist rule in the **Encrypted volumes** section under **Drives** -> **Removable drive locking**. Open the **Filter / Shadow** tab. Check the **Filter files...** option and/or **Audit and shadow files...** and select a template.

5.4.1.7 Drive collections

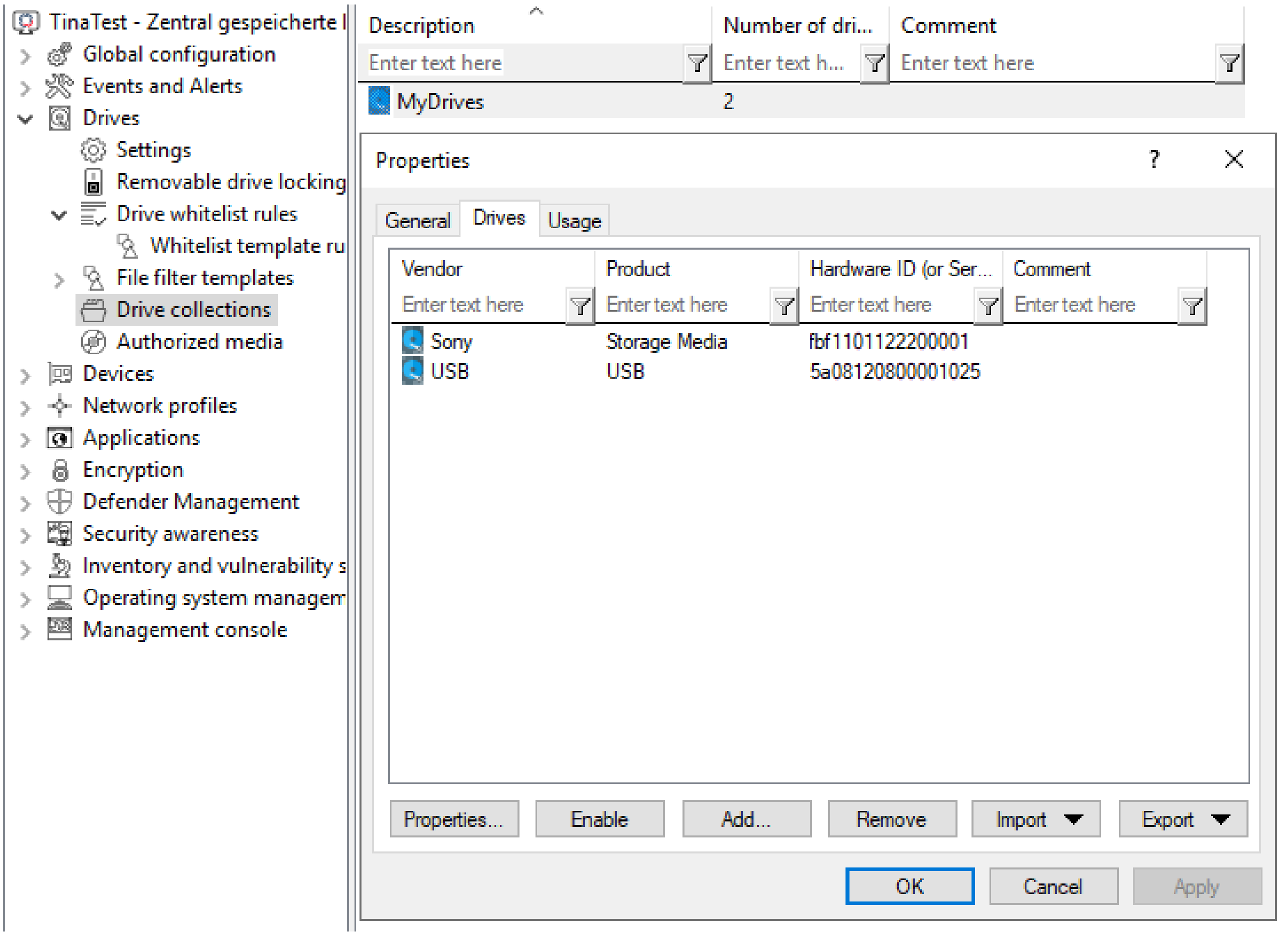
Drive collections can simplify the configuration of settings and rules and reduce the number of whitelist rules needed. Start by grouping all drives with the same settings in a drive collection and then create a drive collection rule for this list containing all settings.

5.4.1.7.1 Creating drive collections

To create a new drive collection, right-click **Drive collections** and select **New**.

On the **General** tab, enter a description and, if necessary, a comment.

On the **Drives** tab you can view, disable, edit and delete existing entries. New entries can be added as well.



Description	Number of dri...	Comment
Enter text here	Enter text h...	Enter text here
MyDrives	2	

Vendor	Product	Hardware ID (or Ser...	Comment
Enter text here	Enter text here	Enter text here	Enter text here
Sony	Storage Media	fbf1101122200001	
USB	USB	5a08120800001025	

If you want to add new entries, click **Add** and, if necessary, select whether you want to add a device based on its product or manufacturer ID or using the hardware ID (only for drives that have this information - otherwise only the hardware ID is queried). Enter the corresponding information in the subsequent dialog or select it in the usual way via the **...** button. from the currently connected drives. The **Import** button allows you to import multiple drives, either in the form of a CSV file or an INI file.

If you do not want to delete existing drives completely, but only remove them from the collection for a certain time, select the desired drive and then click **Deactivate**. An extra icon now indicates that the entry in the list is currently not activated and considered for unlocking. Deactivated collection items can be reactivated.

Click **Export** to save the current list in the form of a CSV or INI file.

Note: Tip: If you have previously created some entries individually and then exported them as a file, you can use this file as the basis for an import, since it already has the correct structure or the necessary columns.

The **Usage** tab shows you in which **drive collection rules** this collection is already used.

Note: You cannot delete the collection as long as a drive collection is used in a rule.

5.4.1.8 Authorized media

Media authorization allows you to unlock certain predefined media (such as update CDs or special program CDs) even if the CD/DVD drive is locked by default. Thus, you are able to selectively configure CD drive locking. When you create a new media rule, DriveLock creates a hash value of the CD. This is required for unlocking. We do not recommend applying a rule of this kind to writable removable media, because in this case the checked value will no longer correspond to the stored value if files have been modified in the meantime. We recommend that you use a media rule only for media that cannot be modified (such as CDs or DVDs).

There are two different types of media: audio CDs and video CDs/DVDs. You can also create your own media by selecting Specific media and reading in the media information.

5.4.2 Devices

DriveLock operates with whitelist rules. This basic concept implies that all devices are generally locked as soon as locking is enabled. Individual whitelist rules are then created to allow usage of only the permitted devices (or groups of devices or device collections). This means that you need to create a separate rule for each device (or group of devices or device list) you want to use. If a device is not defined via a corresponding rule, DriveLock automatically blocks access to it and it cannot be used. This ensures that your security policy remains intact.

To configure DriveLock, we recommend that you first create the whitelist rules you need, and then enable device locking.

It is possible to combine rules for different ranges of validity at different levels:

- Device class (e.g. all Bluetooth transmitters)
- Device bus (e.g. all PCI network cards)

- Hardware ID (e.g. a special smartcard reader)
- Device collection based on hardware ID

You can also configure how and when whitelist rules are applied:

- specify the computers,
- the network connections,
- the logged on users where they apply, and
- the time when they apply.

5.4.2.1 Settings

The following general and advanced settings can be configured to control devices:

- **Custom user notification messages**

  As soon as a removable device is locked by DriveLock using a whitelist rule, DriveLock can display a message to the current user if the corresponding option for dialog windows has been enabled. Use this setting to define your own messages.
  If you have already configured multilingual user notification messages in the global settings, DriveLock displays the default messages in the current language.
  Check **Display custom message** to enable the messages you set here. The variable `%DEV%` is replaced at runtime with the current name of the locked device.
  Click **Test** to preview the message you entered.
  You can also use some of the HTML tags for formatting your message (for example `<b>Text</b>`).

- **Restart managed devices if logged-on user changes**

  If this function is activated, all devices are automatically restarted as soon as a user change takes place.

- **Audit device restarts**

  DriveLock generates monitoring events on device reboot if this feature is enabled.

5.4.2.2 Device class locking

DriveLock distinguishes between different types of devices. By default, DriveLock does not initially lock any devices (or device classes). When you lock a device class, all devices that belong to that class (or are connected via the same controller or interface) are also locked. Exceptions to this are again defined via whitelist rules.

To enable device locking, open the **Lock Settings** sub-node in the **Devices** node in the Policy Editor .

You can set up locking for the following **adapters and interfaces**:

- Serial (COM) and parallel (LPT) interface
- Bluetooth adapter
- Infrared interface
- USB controller
- Firewire (1394) controller
- PCMCIA controller

The following is a list of **devices** that DriveLock can control and lock:

- Tape drives
- Biometric devices
- Debugging and software protection devices (WinUSB,ADB)
- Printers
- Input devices (HID)
- ePassport readers
- External graphic adapters
- IEC 61883 (AVC) bus devices
- In-circuit emulator devices
- Media Center Extender Devices
- Modems
- Network adapter
- PCMCIA and flash memory devices
- Scanners and cameras
- Secure Digital Host controller
- SideShow devices
- Sensor devices
- Smartcard reader

- Sound, video and game controllers
- Portable devices / media players
- Virtual devices (VM Ware)

The following different **smartphones** can be locked separately:

- Android devices
- Apple devices
- Black Berry devices
- iTunes software restrictions
- Cell phones
- Palm OS handhelds and smartphones
- Windows CE handhelds and smartphones

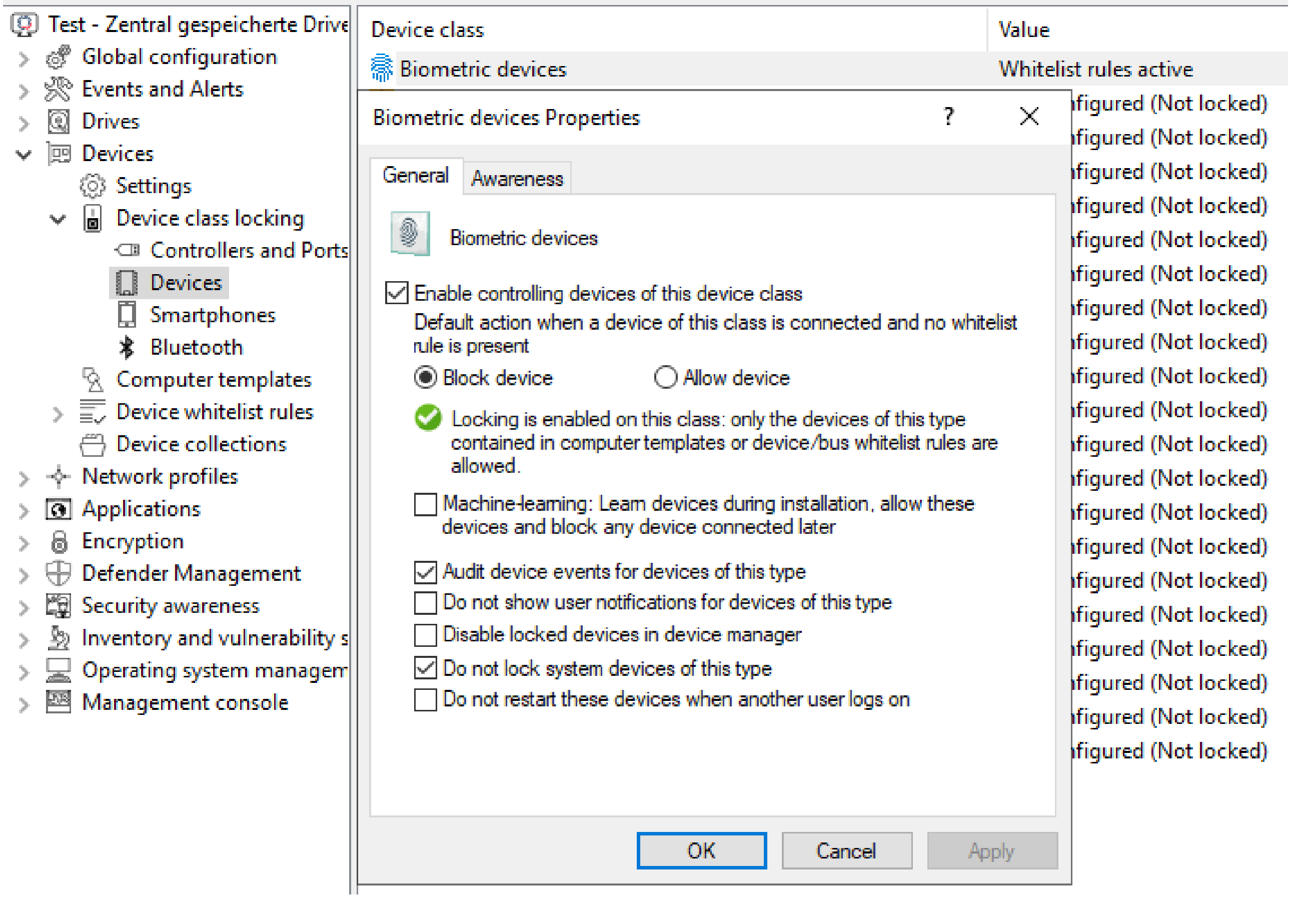
In addition, **Bluetooth** options can be set.

To configure the default settings, click on the corresponding device. The configuration is identical for all device classes except interfaces and Apple and Android devices (treated as drives).

5.4.2.2.1 Basic configuration options for locking devices

The following basic configuration options are available This example shows the settings for biometric devices.

On the General tab:



Biometric 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

- **Enable controlling devices of this device class**: Enable blocking or allowing the selected device class. Select the appropriate option.
- **Machine-learning**: For many types of devices you can activate machine learning. If this rule is applied for the first time, devices connected at the time of installation are learned in a local whitelist and are enabled in the future during the boot phase. Devices of this type that are connected later remain blocked. To relearn the local whitelist, run `drivelock -recreatebootdevs` at the command line and restart the computer.
- **Audit device events for devices of this type**: In addition, you can specify whether the associated monitoring events are generated. If this function is enabled, the events are transmitted to the configured locations (for example, Windows Event Viewer, DriveLock Enterprise Service).
- **Do not show user notifications for devices of this type**: Users do not receive information about the corresponding devices.
- **Disable locked devices in device manager**: If devices are locked, they are disabled in the Device Manager.

- **Do not lock system devices of this type**: For example, a system device is a network miniport driver or a UBS root hub. To avoid having to define separate whitelist rules for these "software" devices, this option is initially activated in principle. If you disable it, separate rules must be created for all those system devices.
- **Do not restart these devices when another user logs on**

Click here for more information about the **Awareness** tab.

5.4.2.2.2 Blocking interfaces

The configuration of the two interfaces COM and LPT is limited to blocking or allowing for some or all users. Instead of being controlled like other devices or interfaces, these are treated like removable media.

The following options are available:

- **Allow**: Any authenticated user can use this interface
- **Deny (lock) for all users**: Access to this interface is locked for all users.
- **Deny (lock), but allow access for defined users and groups**: Interface is locked, but access is possible for the specified user(s) or group(s).
  To include another group or user in the list, click **Add**. Click **Remove** to delete the previously selected entry.

> Warning: PalmOS devices or Windows CE devices, which are connected to the computer via the serial interface, can only be locked via the option "Serial interfaces (COM)". It is not possible to control these devices via the device classes "Windows CE Handhelds and Smartphones" or "Palm OS Handhelds and Smartphones", because Windows does not allow hardware detection at the serial ports (COM).

5.4.2.2.3 Blocking Apple devices

To generally control access to Apple devices, there is a special device class **Apple devices**.

Unlike other devices, which can either be locked or unlocked only, the Apple device class provides a detailed distinction by access rights. Thus, they are treated like drives. This allows all iPods, iPads and iPhones to be controlled very precisely and the data transfer to be tracked.

The following options can be configured:

The General tab

- **Allow** : Any authenticated user can use Apple devices
- **Deny (lock) for all users** : Access to Apple devices is blocked for all users.
- **Deny (lock), but allow access for defined users and groups** : Apple devices are locked, but access is possible for the specified user(s) or group(s).
  To include another group or user in the list, click **Add**. Click **Remove** to delete the previously selected entry.

The Filter / Shadow tab

- **Filter files, [...]** : Using the file filter, accesses can be restricted and logged based on the file types (PDF, DOCX, etc.). However, the file filter must have been created beforehand. The file filter can be used and assigned in all rules.
- **Audit and shadow files...**: Operations (read, write) are logged and can be evaluated later with the DOC.
- **... using the following filters** : Select the existing file filters here and insert them accordingly.
- **Allow access as configured only to selected subfolders**: Here you can **configure the folders** by clicking on the button.

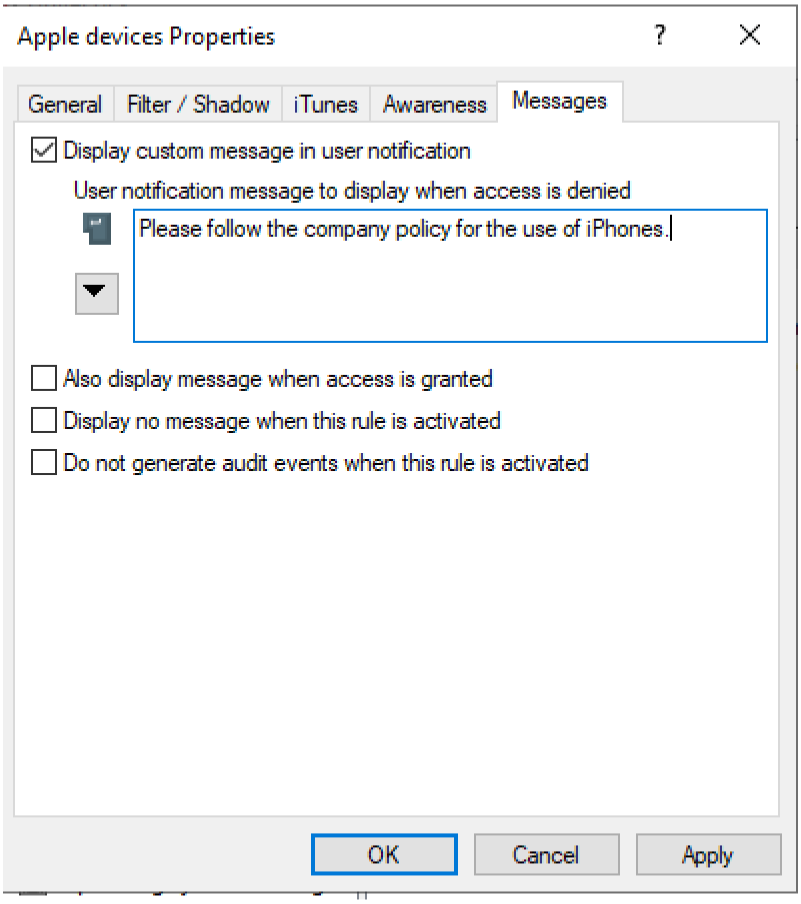
iTunes tab:

- Independently of the devices, you can also restrict the range of functions, for example the blocked iTunes functions. This way you can disable the synchronization of special data types.
- **Audit all transferred files and data** : This is equivalent to file logging in the file filter, i.e. all data exchange is logged.

Information about the **Awareness** tab can be found here.

Messages tab:

- **Display custom message in user notification**: Enable this option to configure a custom message for a rule. Enter a text that will be displayed regardless of the currently set system language. This language-independent message is represented by a key symbol at the upper left corner of the input field. If you have defined multilingual user messages, you can also select one of these messages. To do so, click the arrow and select Multilingual messaging from the list.



☑ Display custom message in user notification

User notification message to display when access is denied

Please follow the company policy for the use of iPhones.

□ Also display message when access is granted

□ Display no message when this rule is activated

□ Do not generate audit events when this rule is activated

- If you want the message to be displayed even if access by the user is possible, enable the corresponding option.
- To disable the display of notifications in general (including the display of standard notifications), enable **Do not display notification**.
- If you want to suppress the generation of monitoring events for this whitelist rule, check **Do not generate audit events when this rule is activated**.

5.4.2.2.4 Bluetooth

Using the settings for connecting devices via Bluetooth, you can, for example, prevent pairings with new devices or configure restrictions to desired Bluetooth services from DriveLock version 2021.1.

Use case: You want to control the use of some Bluetooth devices (e.g. mouse, keyboard or Microsoft Surface Pen). The use of these devices should be allowed, but all other Bluetooth devices (including their functions such as file transfer) should be blocked.

In the DriveLock Management Console, open the Devices node and select the Bluetooth sub-node in the Lock Settings.

The following settings are available here: By default, they are disabled.

- **Block Bluetooth advertising**

  Select this option if you want the device to be the source of Bluetooth announcements and be discoverable by other devices.

- **Block Bluetooth discoverability**

  Use this setting to specify whether the device should be detectable by other Bluetooth devices, e.g. a headset.

- **Block Bluetooth pre-pairing**

  Select this option if you want certain bundled Bluetooth peripherals to automatically pair with the host device.

- **Block Bluetooth proximal connections**

  This option prevents users from using fast pairing and other short-range technologies.

- **Allowed Bluetooth services**

  This setting lets you enter allowed Bluetooth services and profiles in a list (using strings in hexadecimal format).

Warning: It is recommended when making changes in this area to first apply the changed policy to the agent and then restart the machine. This is especially true if the list of allowed Bluetooth services has been edited.

5.4.2.3 Computer templates

Computer templates are used to allow or deny acces to devices for specific types of computers with the same built-in hardware. These devices, which are within the template, are automatically enabled by DriveLock, the creation of additional device rules is no longer necessary.

Right-click Devices whitelist rules and select the **Show template rules** option to display all the devices that have been defined within a template instead of via a whitelist rule. An icon shows the difference between the two types.

Note: Alternatively, templates can also be created based on device classes. It is possible, for example, to create a scanner pool and to allow access to it or to block it.

5.4.2.3.1 Creating a computer template

To create a new computer template, right-click **Computer templates** and select **New**.

First, select the source for your new computer template.

- **Local computer**: All devices on the local computer are listed.
- **Agent on remote computer**: Enter the name of the DriveLock agent to get a list of devices on this agent.

  Note: For this option, DriveLock Agent must have been installed and started on the named computer.

- **Create empty template**: Use this option if you want to select the devices manually. Here you can have devices imported into the list from various sources (from the local computer, from an agent or from a file)

In the next dialog, configure your template.

- On the **General** tab, enter a name for the template (for example, the product name) and, if necessary, a comment. Once you have set the **Enable template (allow access to devices in this template)** option, the use of all included devices will be allowed according to the assigned permissions.
- On the **Devices** tab, all devices found are listed with the corresponding hardware ID. Click **Import** and select between the different sources to insert device information into the existing computer template.

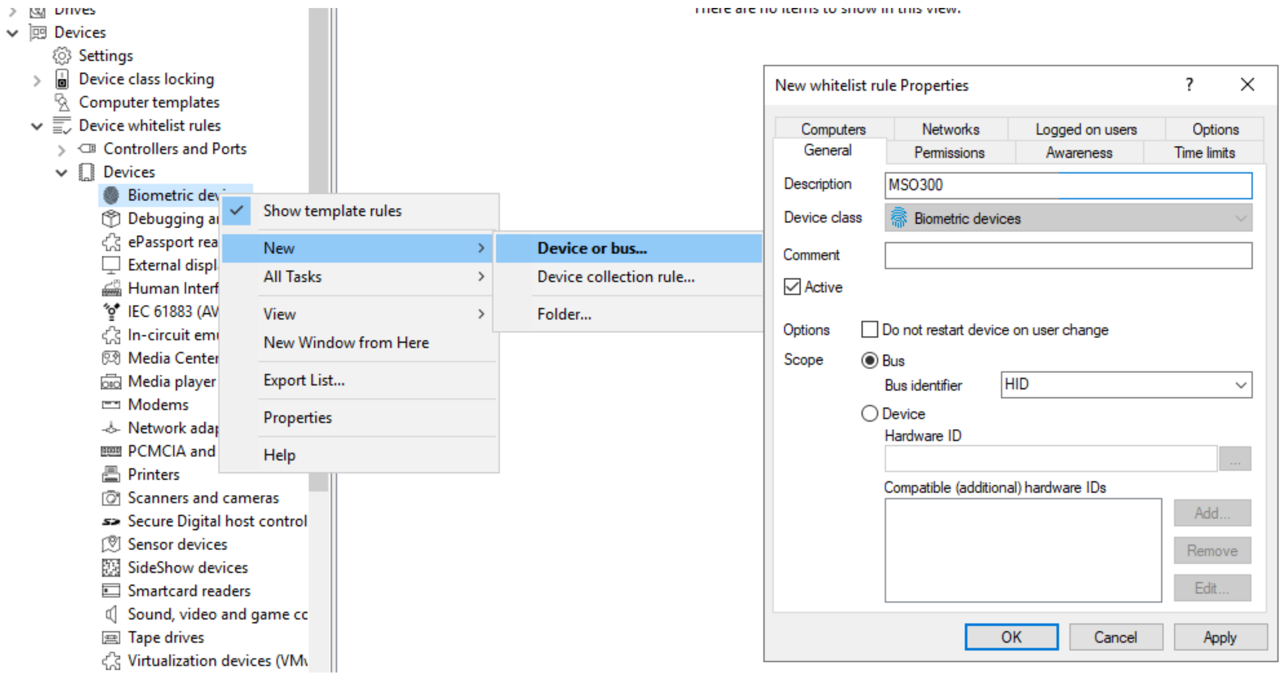
  Warning: If **(Info only)** is displayed as type in the device list, it means that DriveLock recognizes this device but cannot lock it in the current version.

  You can select devices from the list and change their **properties** (designation, device class or type (bus or single device)) by double-clicking them. Click **Deactivate** to deactivate a previously selected item from the list without deleting it from the list. Thus, it will still be locked if you use the template for sharing. The **Export** button can be used to export the device list to an INF file.

- On the **Access Rights** tab you can restrict access to the devices for a certain group of users by activating **Lock but allow access for defined users and groups**. You then simply add the appropriate users.

5.4.2.4 Device whitelist rules

Whitelist rules for devices are created in the same way as drive rules are. The following example shows the creation of a rule for a biometric device.



Description: MSO300

Device class: Biometric devices

Comment:

☑ Active

Options: ☐ Do not restart device on user change

Scope: ● Bus

Bus identifier: HID

○ Device

Hardware ID:

Compatible (additional) hardware IDs:

In the **Description** field enter a name, in this case it is the MSO300 series biometric device. You can additionally add a comment.

Narrow the scope further by providing additional information. You can either select a bus or enter a hardware ID. In this case, **HID** is used as the bus.

Thus, this rule is only applied if the device belongs to the same device class (here Biometric devices) and is connected via the configured bus.

If the bus you need is not present in the list, you can specify it subsequently by entering the appropriate name in the field.

If there are any whitelist rules that affect each other, DriveLock will use them as follows:

- Bus locked and device enabled -> Device enabled
- Bus locked and device locked -> Device locked
- Bus enabled and device blocked -> Device locked
- Bus enabled and device enabled -> Device enabled

Set up computer templates have no special prioritization regarding the manually created whitelist rules.

If a device or bus is allowed in one rule but blocked in another, the device or bus is enabled.

To distinguish devices from each other even more precisely, hardware IDs and their so-called Compatible IDs are used. Each device has its unique hardware ID. In addition, Windows maintains a list of compatible devices (Compatible ID). The Hardware ID or Compatible ID is used to find the appropriate driver. Additionally, the hardware IDs may also contain a revision number assigned by the manufacturer (which is, however, irrelevant for the choice of driver). In this case, Windows uses one of the Compatible IDs that does not contain this revision number.

Enter the correct hardware ID in the appropriate field to specify the desired device. The hardware ID can be read out either from the event display or the registration database. The list appears on the **Installed devices** tab.

The **Hide system devices** option hides all Windows system devices that are enabled by default via the **Do not lock system devices of this type** function in the device class lock settings.

Additional devices can be selected by connecting to another agent remotely and selecting a device present there. To do this, select **on Agent** and enter the name of the computer you want to connect to. This requires the DriveLock Agent to be installed on the target computer.

An explanation of the options on the other tabs can be found here.

5.4.2.5 Device collections

Device collections make it easier to manage devices of the same type if the same settings are to apply to them, while reducing the number of whitelist rules required. They may contain several similar devices and can be used as a device collection rule when configuring whitelist rules - similar to using individual devices based on their hardware ID.

When creating a new collections, you also select the device class from the list of available classes. This device class determines which types of devices you can include in the collection; it cannot be changed after saving the collection the first time.

In this way, managing the collections and the configuration of device security and blocking settings are kept separate.

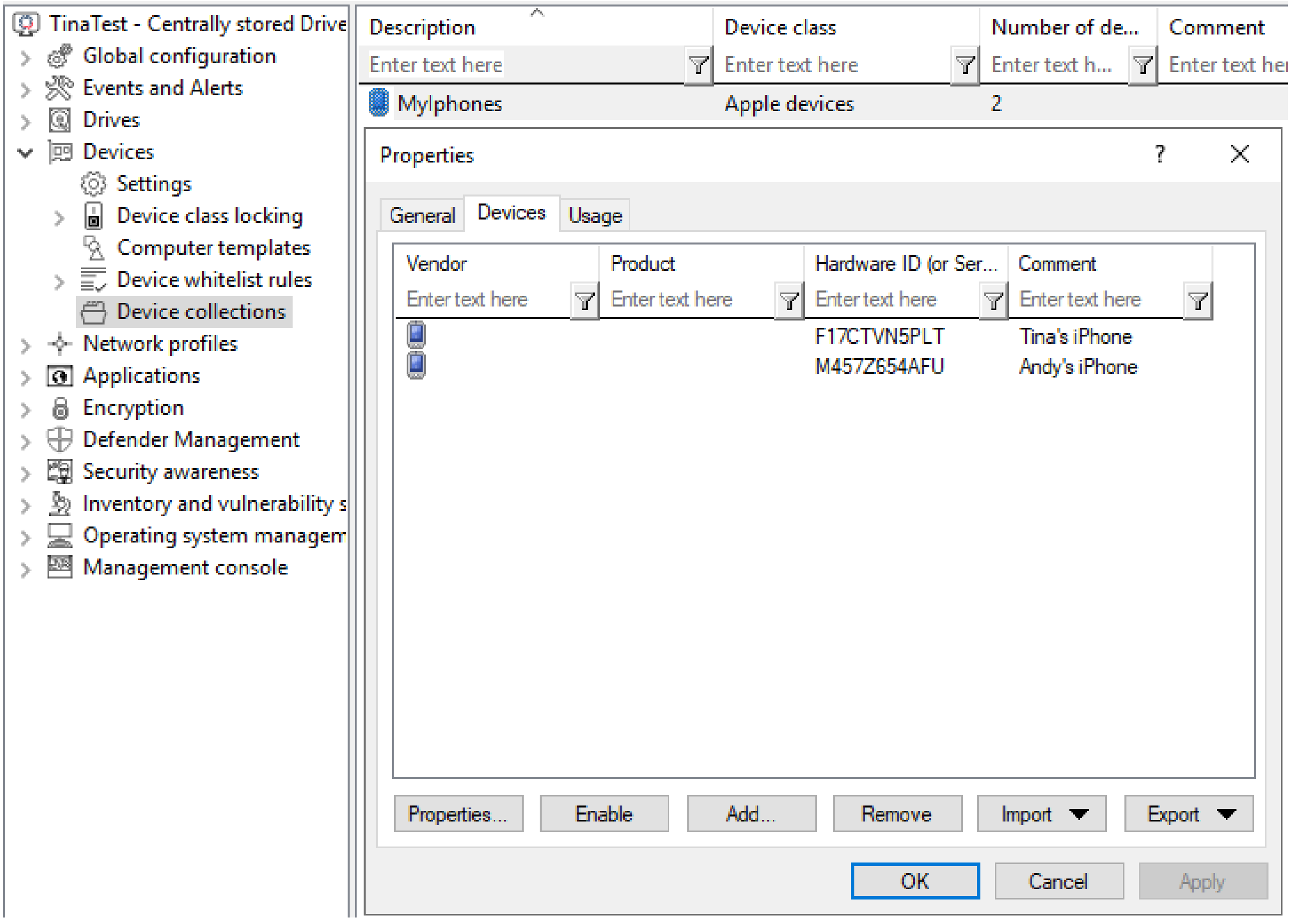
5.4.2.5.1 Creating device collections

To create a new list, right-click **Device collections**and then select **New**.

You can add a description to the collection and a comment.

Note: The selection of the device class later determines for which class this list can be used for configuration and which technical options are available to you for controlling these devices.

Open the **Devices** tab to manage the devices included in this collection.



Description	Device class	Number of de...	Comment
Enter text here	Enter text here	Enter text h...	Enter text her
MyIphones	Apple devices	2	

Vendor	Product	Hardware ID (or Ser...	Comment
Enter text here	Enter text here	Enter text here	Enter text here
		F17CTVN5PLT	Tina's iPhone
		M457Z654AFU	Andy's iPhone

Here you can display, deactivate, edit and delete existing entries. New entries can be added as well.

If you want to add new entries, click **Add** and, if necessary, select whether you want to add a device based on its product or manufacturer ID or using the hardware ID (only for devices that have this information - otherwise only the hardware ID is queried). Enter the corresponding information in the dialog or select it via the **...** button from the currently connected devices. The **Import** button allows you to import multiple devices, either in the form of a CSV file or an INI file.

If you do not want to delete existing devices completely, but only remove them from the collection for a certain time, select the desired device and then click **Deactivate**. An icon now indicates that the entry in the collection is currently not activated and considered for shares. Deactivated collection items can be reactivated.

Click **Export** to save the current list in the form of a CSV or INI file.

> Note: Tip: If you have previously created some entries individually and then exported them as a file, you can use this file as the basis for an import, since it already has the correct structure or the necessary columns.

The **Usage** tab shows you in which **device collection rules** this collection is already used.

> Note: You cannot delete the collection as long as a device collection is used in a rule.

5.4.2.6 Using Device Control to control Bluetooth devices

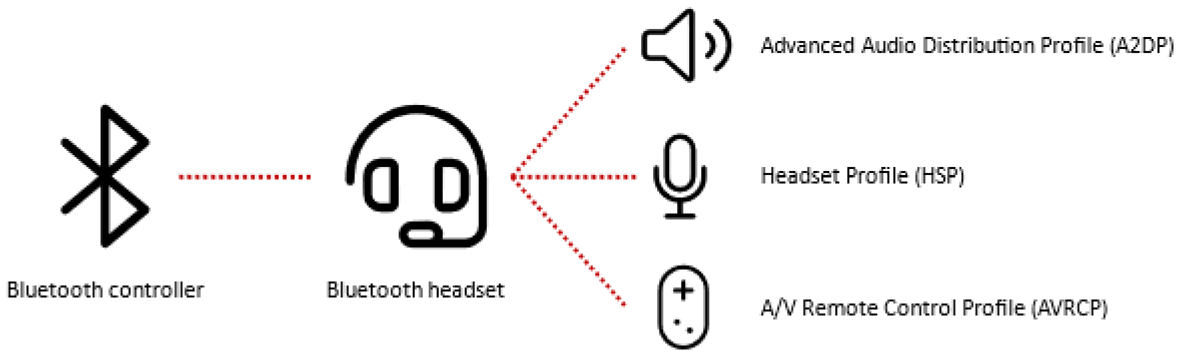
General information: The Bluetooth specification breaks down devices into Major and Minor classes. Depending on the class of device (the combination of major and minor class IDs), the Bluetooth protocol loads profiles that determine how it communicates. There are 11 major service classes, 32 major class combinations, and 64 different minor classes. Each major class and each minor class have its own class identifier in either binary or in hex.

There are two different ways to control Bluetooth devices with DriveLock. One is more restrictive and affects the individual Bluetooth devices, the other limits the services that a Bluetooth device can use.

Controlling Bluetooth controllers, devices, and services

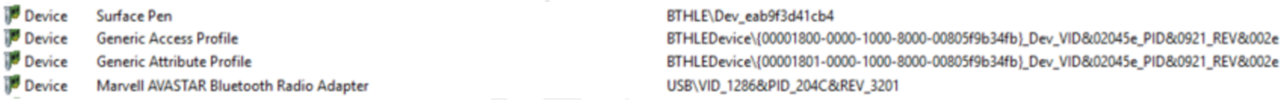
Here, the individual Bluetooth controllers ("Bluetooth cards") are controlled first. Next, the actual Bluetooth devices that connect to the host. And finally, the device-specific services.

Here's an example:


Advanced Audio Distribution Profile (A2DP)
Bluetooth controller
Bluetooth headset
Headset Profile (HSP)
A/V Remote Control Profile (AVRCP)

In this case, five whitelist rules must be created. One for the Bluetooth controller itself, one for the headset and one for each used service.

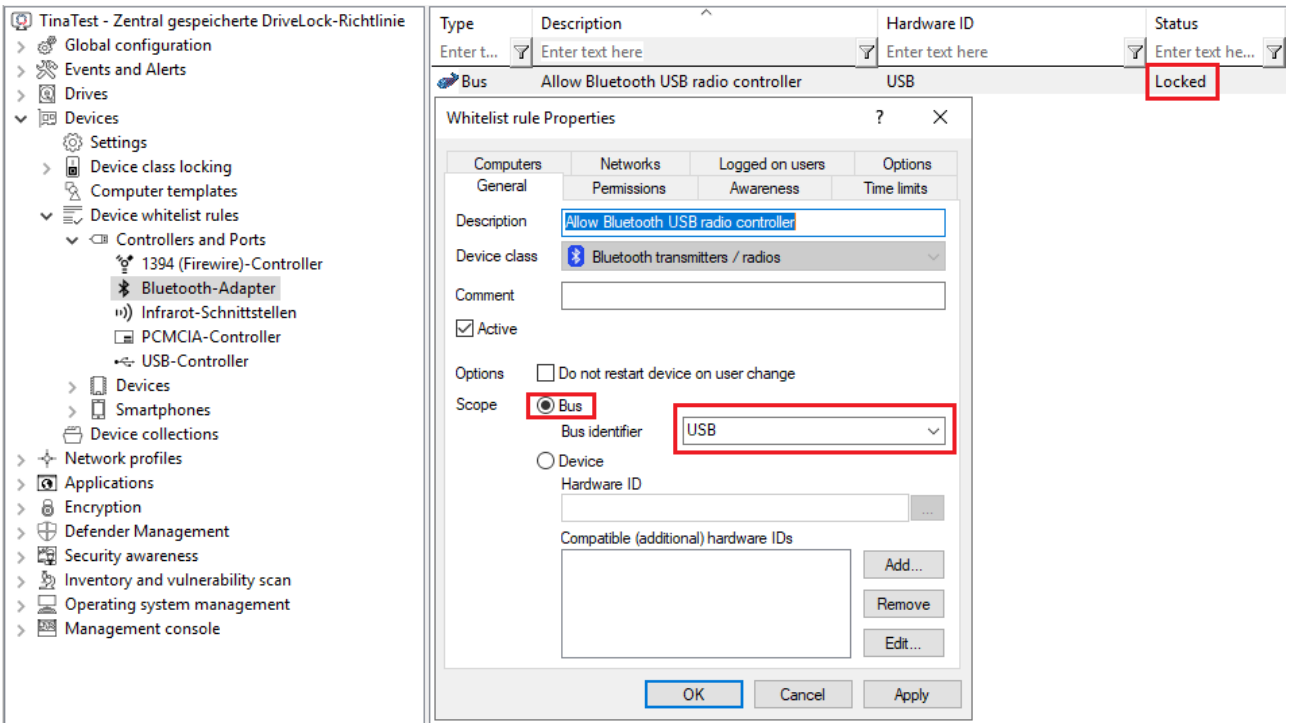
Using the example of a Microsoft Surface Pen on a Microsoft Surface Tablet, it could look like this:



Device	Surface Pen	BTHLE\Dev_eab9f3d41cb4
Device	Generic Access Profile	BTHLEDevice\{00001800-0000-1000-8000-00805f9b34fb}_Dev_VID&02045e_PID&0921_REV&002e
Device	Generic Attribute Profile	BTHLEDevice\{00001801-0000-1000-8000-00805f9b34fb}_Dev_VID&02045e_PID&0921_REV&002e
Device	Marvell AVASTAR Bluetooth Radio Adapter	USB\VID_1286&PID_204C&REV_3201

Bluetooth adapters

If you do not want to control specific Bluetooth adapters, you can also create a whitelist rule based on the bus. Internal Bluetooth radio controls are usually connected via USB. So you can create a whitelist rule that applies to all of them, see the following figure:



Type	Description	Hardware ID	Status
Enter t...	Enter text here	Enter text here	Enter text he...
Bus	Allow Bluetooth USB radio controller	USB	Locked

Whitelist rule Properties

Description: Allow Bluetooth USB radio controller

Device class: Bluetooth transmitters / radios

Comment:

☑ Active

Options: □ Do not restart device on user change

Scope: ● Bus

Bus identifier: USB

○ Device

Hardware ID:

Compatible (additional) hardware IDs

Bluetooth devices

The actual Bluetooth device is whitelisted with its Bluetooth associated terminal address ("MAC address"). This makes whitelisting of Bluetooth devices much more accurate, but also much more complex than, for example, wired USB input devices or headsets, since each individual device must be approved.

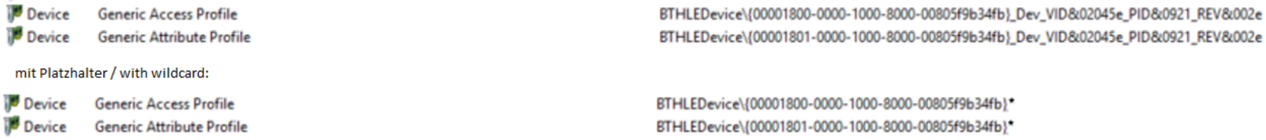
The bus may differ depending on the Bluetooth device. A Surface Pen is a Bluetooth LE device, so that the BTHLE bus is used. Apple Airpods Pro, on the other hand, is a classic Bluetooth device that uses the BTHENUM bus.   Note that each device has a unique endpoint address associated with Bluetooth, for example

- Microsoft Surface Pen: BTHLE\Dev_**FA6B8712ACFF**
- Apple Airpods Pro: BTHENUM\Dev_**EA9F6CDA1258**

Bluetooth services

Every Bluetooth device uses one or more Bluetooth services. Basically, the services Hardware ID contains a suffix for the device itself with vendor and product ID. So you need to whitelist each service for each device.

If you want to simplify this, you can use wildcards. Then you can whitelist the needed service independently from a device.



Device	Generic Access Profile	BTHLEDevice\{00001800-0000-1000-8000-00805f9b34fb}_Dev_VID&02045e_PID&0921_REV&002e
Device	Generic Attribute Profile	BTHLEDevice\{00001801-0000-1000-8000-00805f9b34fb}_Dev_VID&02045e_PID&0921_REV&002e

mit Platzhalter / with wildcard:

Device	Generic Access Profile	BTHLEDevice\{00001800-0000-1000-8000-00805f9b34fb}*
Device	Generic Attribute Profile	BTHLEDevice\{00001801-0000-1000-8000-00805f9b34fb}*

As a result, the two services are no longer tied to a specific device, but can be shared with any Bluetooth device. However, this requires that the other device has been enabled with a corresponding whitelist rule.

In general, Bluetooth services are standardized. Some devices may use vendor-specific services. Each service has a unique ID. You can find all common service GUIDs here: https://www.bluetooth.com/specifications/assigned-numbers/

Note: There are also Windows-specific Bluetooth services that have to be enabled with corresponding whitelist rules.

Controlling Bluetooth services

The second way to get control over Bluetooth is to restrict the services that can be used by any device. The main issue here is to prevent data transmission and allow devices that are needed for daily work, such as headsets or input devices, to access the Bluetooth services required for this.

The **Allowed Bluetooth services** option in the Bluetooth class locking is enabled for these purposes.

Control of authorized services is not as restrictive, but the administrative effort is very low.

Note: For example, you can identify the services in use by pairing the device with a computer and then using remote agent control to detect the services.

5.4.3 Cross-module settings in whitelist rules

The following settings (tabs) are cross-module and available in most DriveLock rules:

Logged on users

Awareness

Commands

Computer

Filter / Shadow

Drive letters

Drive scan

Messages

Networks

Options

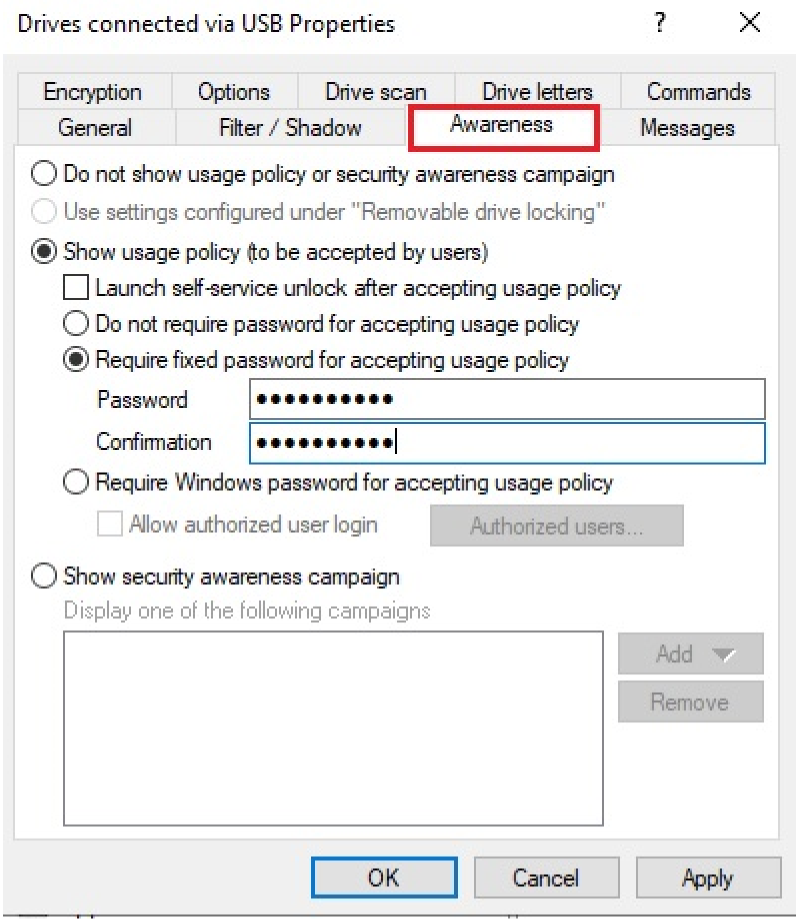
Encryption

Time limits

Permissions for users and groups

5.4.3.1 Awareness

On the **Awareness** tab, you can create a usage policy globally for the entire policy. You can then activate it similar to a security awareness campaign within a drive rule



Drives connected via USB Properties

○ Do not show usage policy or security awareness campaign

○ Use settings configured under "Removable drive locking"

● Show usage policy (to be accepted by users)

□ Launch self-service unlock after accepting usage policy

○ Do not require password for accepting usage policy

● Require fixed password for accepting usage policy

Password ●●●●●●●●●●

Confirmation ●●●●●●●●●●

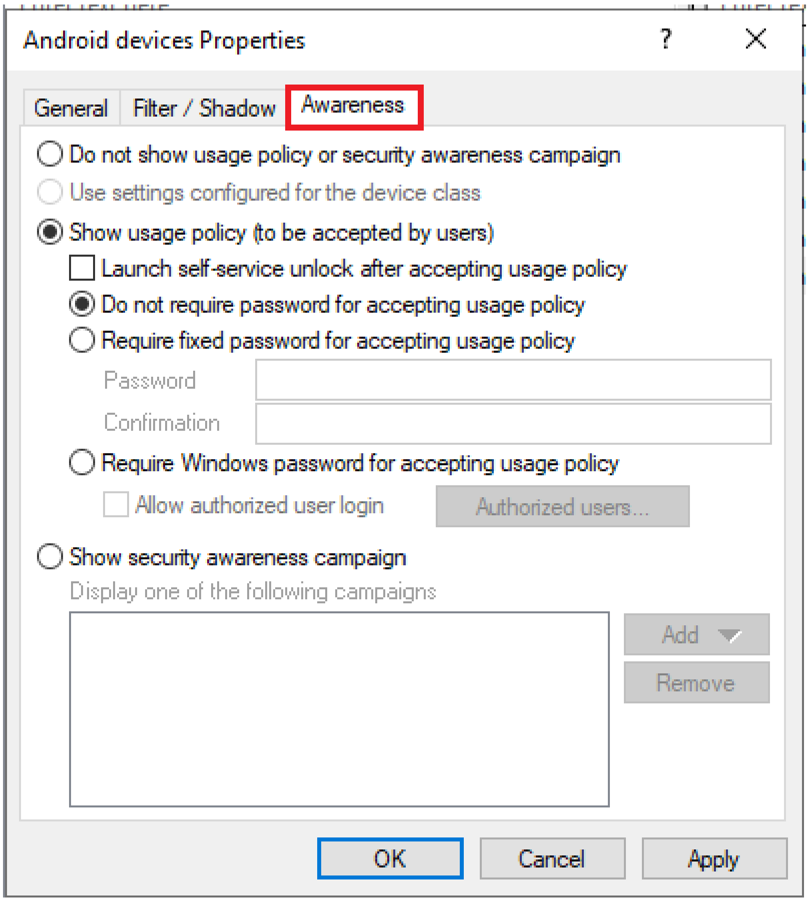
○ Require Windows password for accepting usage policy

□ Allow authorized user login

○ Show security awareness campaign

Display one of the following campaigns

or a device rule:



Android devices Properties

General | Filter / Shadow | Awareness

○ Do not show usage policy or security awareness campaign

○ Use settings configured for the device class

● Show usage policy (to be accepted by users)

□ Launch self-service unlock after accepting usage policy

● Do not require password for accepting usage policy

○ Require fixed password for accepting usage policy

Password

Confirmation

○ Require Windows password for accepting usage policy

□ Allow authorized user login

○ Show security awareness campaign

Display one of the following campaigns

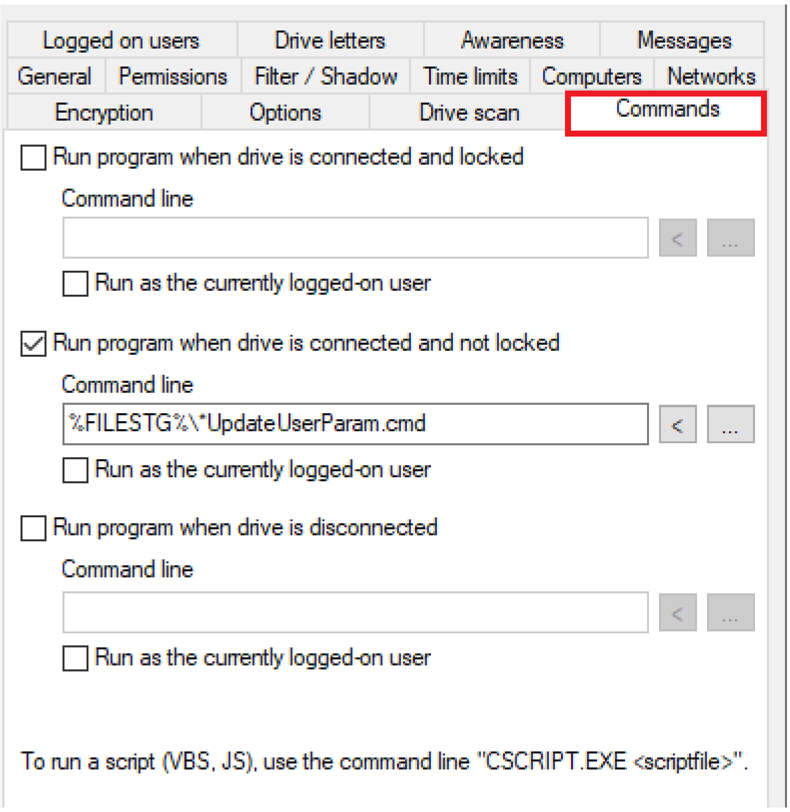
To do so, select the **Show usage policy option (to be accepted by users)**.

The following options are also available:

- **Launch self-service unlock after accepting usage policy**: Once the user confirms the usage policy, the self-service unlock wizard is automatically started.
- **Require fixed password for accepting usage policy**: Provide a password that the user must enter before unlock
- **Require Windows password for accepting usage policy**: If this option is active, the logged-in user must enter their Windows password for confirmation
    - **Allow authorized user login**: This option allows unlocking by a user other than the logged-in user, in which they enter theirs user name and the appropriate password. Optionally, you can specify the users authorized for this via the Authorized users... button.
- Show security awareness campaign: For information on the use of awareness campaigns, see the corresponding documentation at DriveLock Online Help.

5.4.3.2 Commands

On the **Commands** tab you can configure the execution of command lines (see illustration with example command).



□ Run program when drive is connected and locked

Command line

□ Run as the currently logged-on user

☑ Run program when drive is connected and not locked

Command line

%FILESTG%*UpdateUserParam.cmd

□ Run as the currently logged-on user

□ Run program when drive is disconnected

Command line

□ Run as the currently logged-on user

To run a script (VBS, JS), use the command line "CSCRIPT.EXE <scriptfile>".

- A drive was connected and locked by DriveLock.
- A drive was connected and not locked by DriveLock
- A drive was disconnected

The command line can contain any command executable from the command line. Thus, for example, you can run a program (*.exe), a Visual Basic script (*.vbs) or scripts for the new Windows PowerShell.

In this way it is possible to react to these events in many different ways. For example, you can start a backup process when a certain external hard disk is plugged in. Or, for example, you can use a PowerShell script to copy images from a camera to a predefined network share completely automatically.

To run a VB script, you must specify the full path to the script file (e.g. `cscript c:\-programing\scripts\meinscript.vbs`).

There are some variables that can be used within the command line and are replaced by the agent with the current values before execution:

`%LTR%`	Assigned drive letter
`%NAME%`	Drive name
`%SIZE%`	Drive size
`%USER%`	Name of the user currently logged in
`%SERNO%`	Drive serial number
`%HWID%`	Hardware ID of the device
`%PRODUCT%`	Drive product ID
`%VENDOR%`	Drive manufacturer
`%FILESTG%`	Path to a file within the policy file store

To do this, click **<** and select one of these variables so that it is inserted at the current cursor position.

Click the **...** button to insert a file name at the current cursor position. You can choose between two options:

- File system: the file exists on the computer's local hard drive
- Policy file store: Use the file from DriveLock's policy file store

The policy file store is a file container that is stored as part of a local policy, group policy, or configuration file. It can contain any files (such as scripts or applications) that are automatically distributed with a DriveLock configuration.

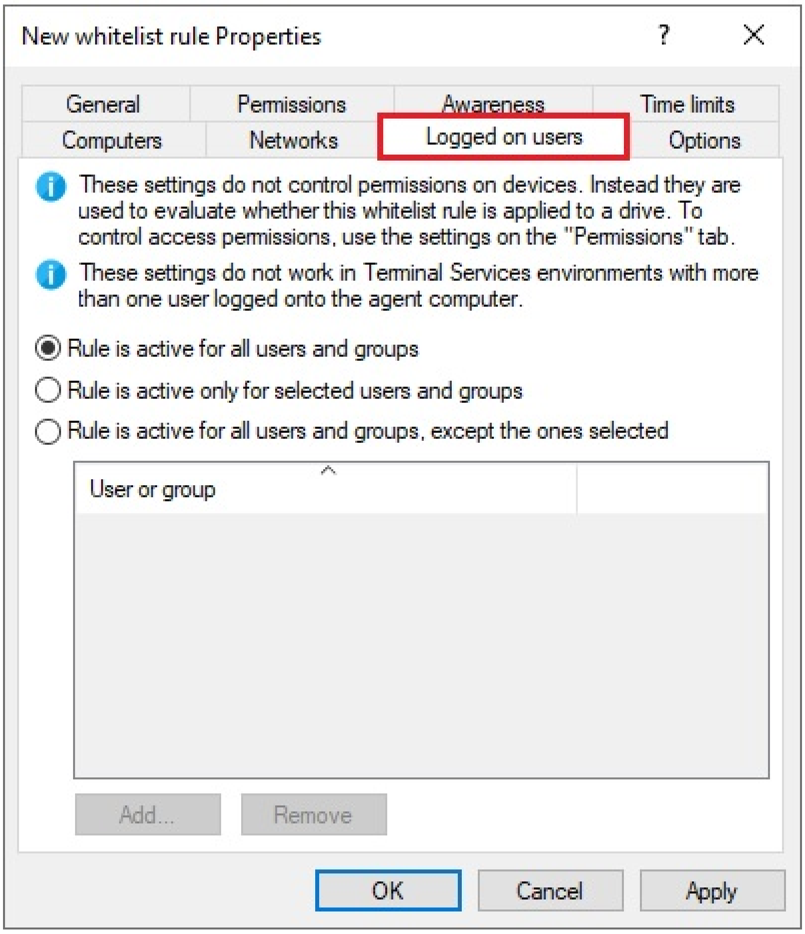
A file loaded from the policy file store is indicated by a "*". If you use a file from the policy file store, you must also use the variable `%FILESTG%` as the relative path.

In addition, you can specify whether the new process should run with the same permission that the agent has or whether it should run in the user context (i.e. under the identifier of the currently logged-in user).

5.4.3.3 Logged on users

The **Logged on users** tab allows you to specify the users or user groups the rule is applied to.

Note that these are not the same permissions as the ones configured on the **Permissions** tab. This check only determines whether this rule is even considered for the currently logged in user. Access will only be allowed or denied according to the set permissions in this case.



New whitelist rule Properties

These settings do not control permissions on devices. Instead they are used to evaluate whether this whitelist rule is applied to a drive. To control access permissions, use the settings on the "Permissions" tab.

These settings do not work in Terminal Services environments with more than one user logged onto the agent computer.

● Rule is active for all users and groups

○ Rule is active only for selected users and groups

○ Rule is active for all users and groups, except the ones selected

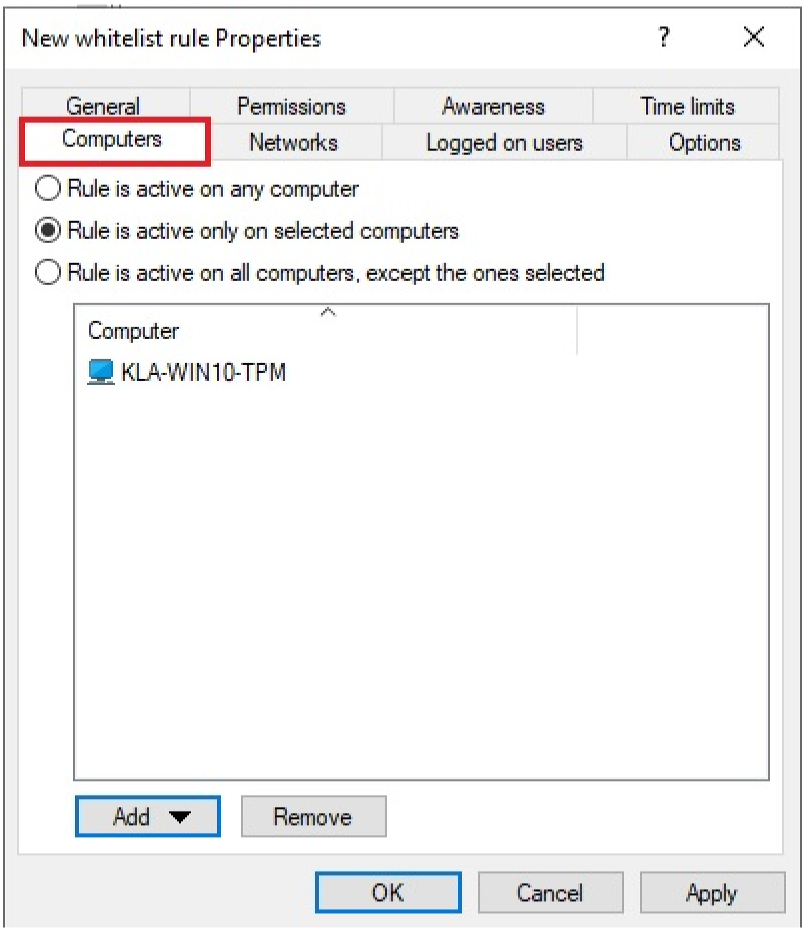
Choose one of the following options:

- Rule is active for all users
- Rule is active only for selected users and groups
- rule is active for all users and groups, except the ones selected

Click Add to add more users or groups to the list. Remove deletes previously selected users or groups from the list.

5.4.3.4 Computer

Use the **Computers** tab to specify on which computers the whitelist rule should be valid.



○ Rule is active on any computer

● Rule is active only on selected computers

○ Rule is active on all computers, except the ones selected

Computer
KLA-WIN10-TPM

Choose one of the following options:

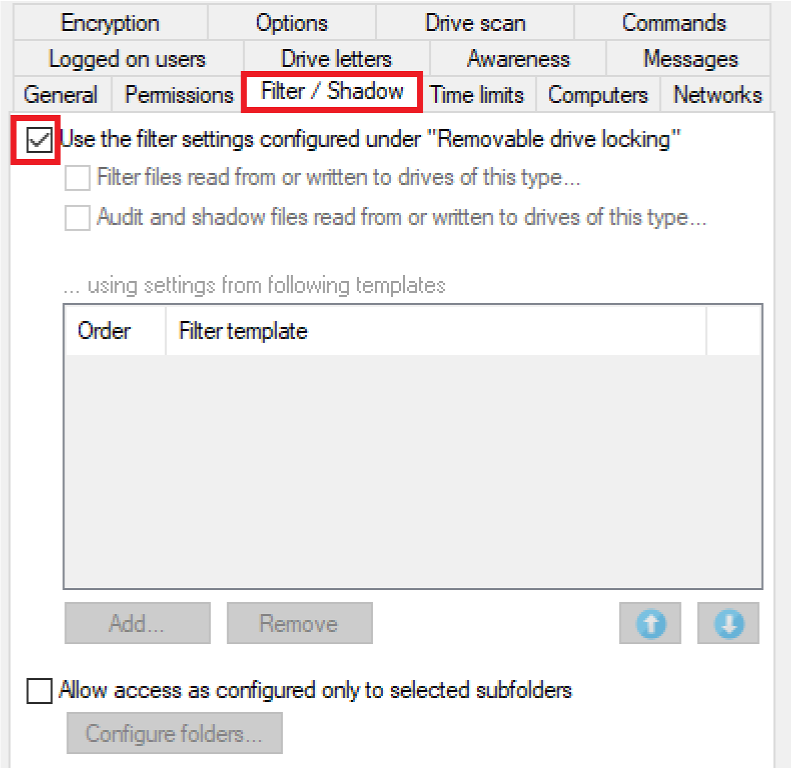
- The rule applies to all computers
- The rule applies only to the listed computers
- The rule applies to all but the listed computers

Click **Add** to add more computers to the list. You can use computers, groups or organizational units from Active Directory or enter the name of the computer directly.

Remove will delete previously selected computers from the list.

5.4.3.5 Filter / Shadow

On the **Filter / Shadow** tab the **Use the filter settings configured under "Removable drive locking"** option is enabled by default, which means that the set filter for the associated drive type will be used.



☑ Use the filter settings configured under "Removable drive locking"

□ Filter files read from or written to drives of this type...

□ Audit and shadow files read from or written to drives of this type...

... using settings from following templates

□ Allow access as configured only to selected subfolders

If you want to specify your own filter, deselect this option and use the **Filter files read from or written to drives of this type...** option instead or **Audit and shadow files read from or written to drives of this type** to turn on file filtering and selected templates for a specific drive.

You can **add** an existing file filter template to the list. Click **Remove** to delete a list entry. Use the two arrow icons to change the order of the file filter templates.

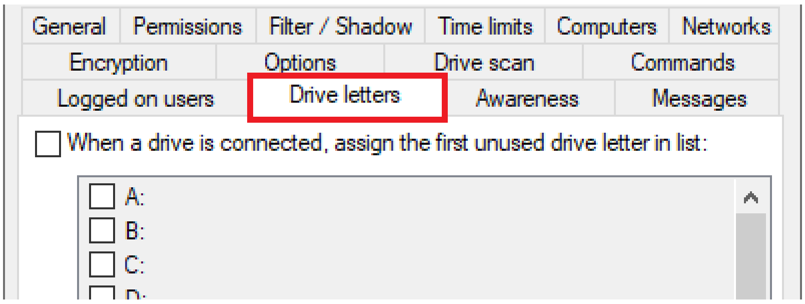
When DriveLock enables a whitelist rule, all file filter templates in the list are evaluated from top to bottom. The first template where the criteria configured in it (e.g. file size, exceptions, users and groups, computers or network connections) completely match is applied. All following templates will be ignored.

Here's an example:

You have created two templates: the first template applies only to administrators and does not filter files, the second template applies to all users and blocks access to executable files. Now when an administrator wants to access the application file, the first template is applied and access is allowed. If a standard user tries to do the same, the first template is ignored and the second one is applied to block access.

5.4.3.6 Drive letters

On this tab you can specify which drive letters will be used when a certain removable disk is connected to the computer.



☐ When a drive is connected, assign the first unused drive letter in list:

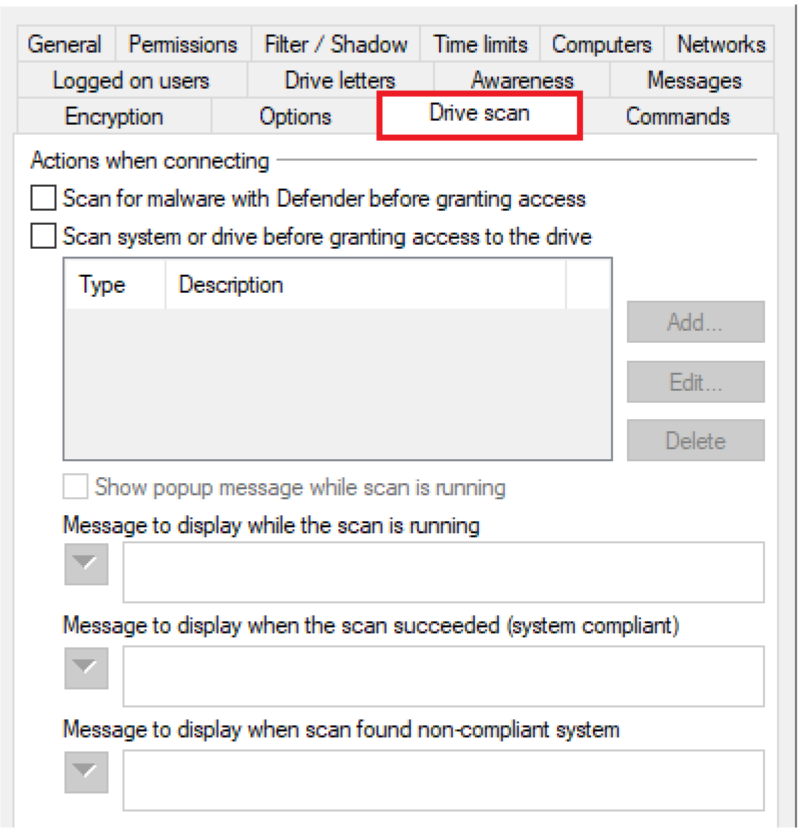
☐ A:
☐ B:
☐ C:
☐ D:

If you enable more than one letter, DriveLock Agent will automatically assign the first free letter to the drive.

Note: Please be sure not to conflict with drive letters already assigned (e.g. for network shares or user home directories).

5.4.3.7 Drive scan

You can configure the policy to start a virus scan automatically when an external drive is connected to a computer. This way, users can only access the drive when the scan is complete and no malware has been found.



Actions when connecting

□ Scan for malware with Defender before granting access

□ Scan system or drive before granting access to the drive

Type	Description

□ Show popup message while scan is running

Message to display while the scan is running

Message to display when the scan succeeded (system compliant)

Message to display when scan found non-compliant system

Check the option **Scan for malware with Microsoft Defender before granting access**.

> Note: If the drive is encrypted, DriveLock starts the scan as soon as the drive is connected and decrypted.

On the DriveLock Agent, a message appears in the system tray icon.

If Microsoft Defender finds a threat on the drive, it will noticeably increase the scanning time. Microsoft Defender then attempts to eliminate the threats. If that fails, the drive must be disconnected and reconnected so that Microsoft Defender can finish removing the threat.

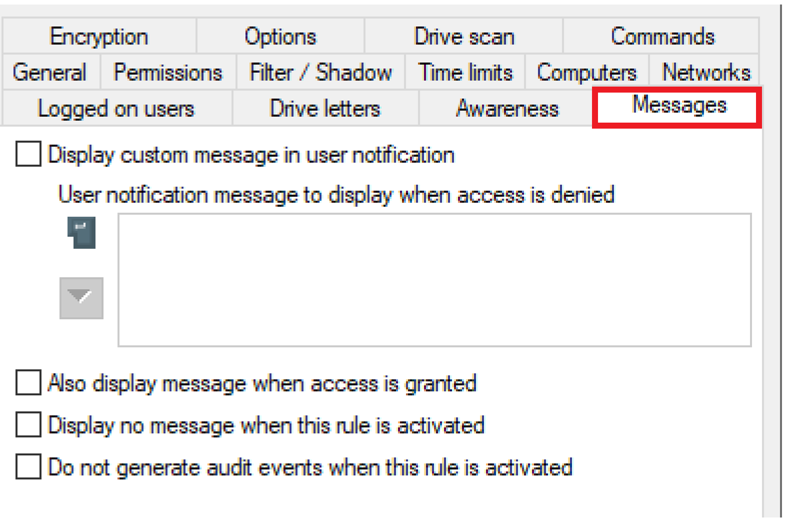
A message will inform the user whether the removal was successful and whether the drive can be accessed. The messages can be configured according to your specifications.

> Note: If Microsoft Defender cannot eliminate the threat, the only remaining option is to access the drive by temporarily unlocking it.

For more information on Defender Management, see the DriveLock Defender Management documentationat DriveLock Online Help..

5.4.3.8 Messages

On this tab you can configure user notifications. You can configure a separate user message for each rule. Unless otherwise set, this message is shown to users when access to a drive is denied.



☐ Display custom message in user notification

User notification message to display when access is denied

☐ Also display message when access is granted

☐ Display no message when this rule is activated

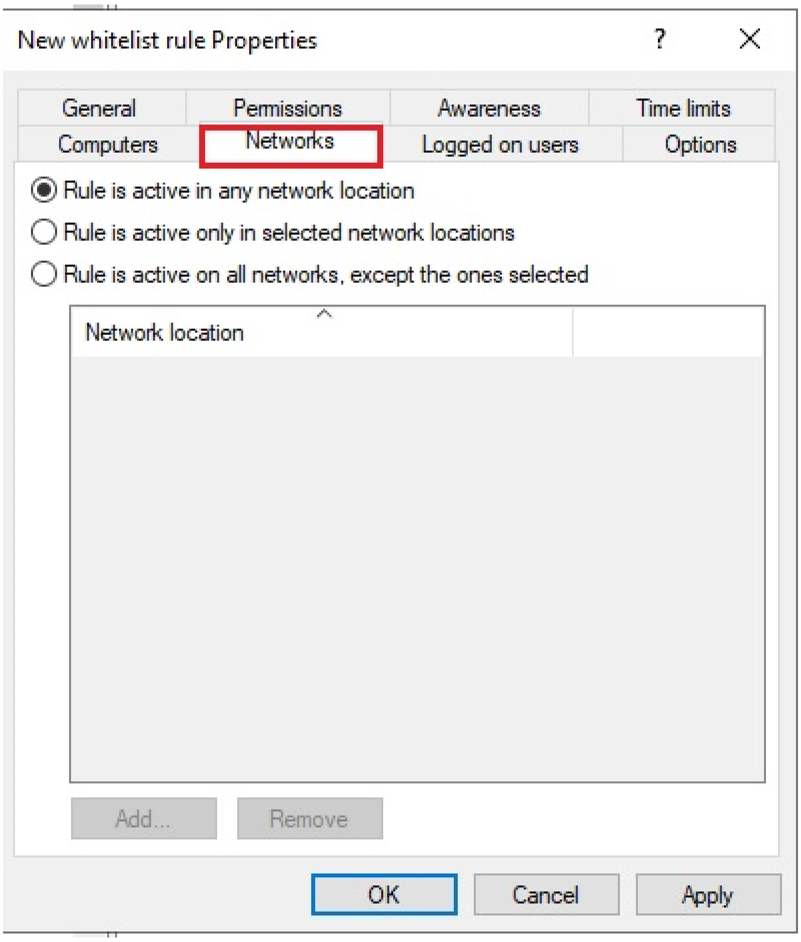
☐ Do not generate audit events when this rule is activated

To configure a custom message for a rule, enable the **Display custom message in user notification** option. Then enter a text which will be displayed regardless of the currently set system language. This language-independent message is represented by a key symbol at the upper left corner of the input field.

If you have defined multilingual notification messages, you can also select one of these messages. To do so, click the arrow and select Multilingual messaging from the list.

5.4.3.9 Networks

On the **Networks** tab you can specify the active network connections the rule will apply to.


New whitelist rule Properties

● Rule is active in any network location

○ Rule is active only in selected network locations

○ Rule is active on all networks, except the ones selected

Choose one of the following options:

- The rule applies to all network connections
- The rule applies only to the listed network connections
- The rule applies to all but the listed network connections

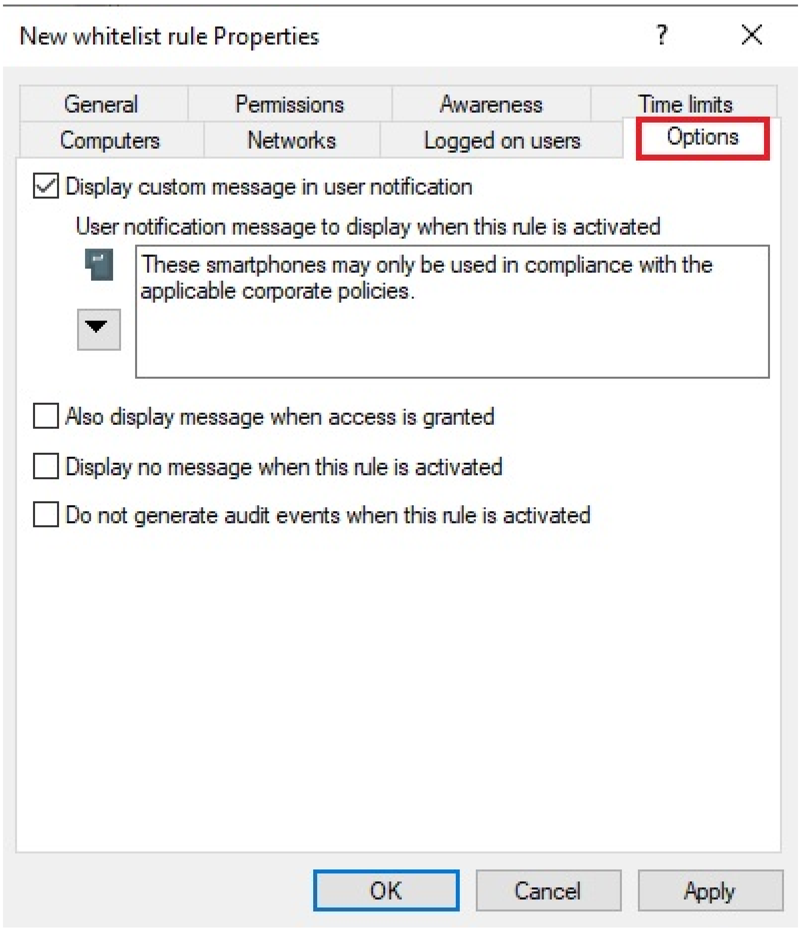
Click Add to add more network connections to the list. Remove deletes previously selected network connections from the list.

For more information on creating network profiles, click here.

5.4.3.10 Options

For each rule you can configure a separate user message on the **Options** tab. Unless otherwise set, this message is shown to users when access to a device is denied.

Note: This tab has the same options as the **Messages** tab that appears when you configure whitelist rules for drives.



☑ Display custom message in user notification

User notification message to display when this rule is activated

These smartphones may only be used in compliance with the applicable corporate policies.

□ Also display message when access is granted

□ Display no message when this rule is activated

□ Do not generate audit events when this rule is activated

To configure a custom message for a rule, enable the **Display custom message in user notification** option. Then enter a text which will be displayed regardless of the currently set system language. This language-independent message is represented by a key symbol at the upper left corner of the input field.

If you have defined multilingual user messages, you can also select one of those messages. To do so, click the arrow and select **Multilingual messaging** from the list.

Multilingual messages contain different texts for different languages for one message. Before you can use multilingual user messages, they must be defined in the Global configuration section of the policy. If you use such a message, DriveLock displays the text configured for the current system language of the logged-in user.

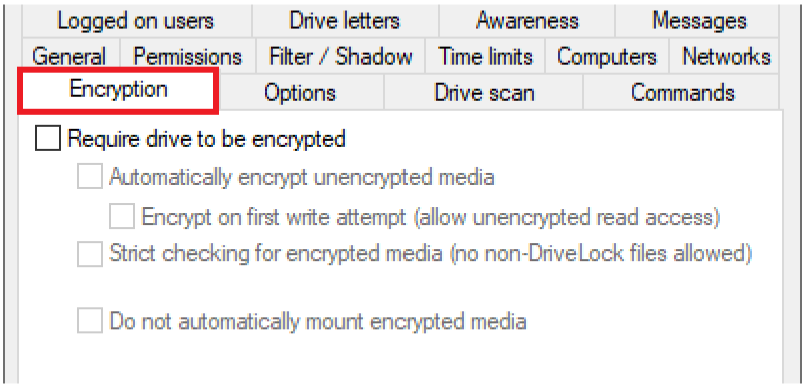
This language-dependent message is represented by a speech bubble icon at the upper left corner of the input field.

If you want the message to be displayed even if access by the user is possible, enable the corresponding option. You can also specify that no messages at all (not even standard messages) should be displayed to the user.

If you want to suppress generating audit events for this whitelist rule, please check **Do not generate audit events when this rule is activated**.

5.4.3.11 Encryption

The **Encryption** tab has nothing selected by default.



□ Require drive to be encrypted
□ Automatically encrypt unencrypted media
□ Encrypt on first write attempt (allow unencrypted read access)
□ Strict checking for encrypted media (no non-DriveLock files allowed)
□ Do not automatically mount encrypted media

Checking **Require drive to be encrypted** ensures that a mounted drive must be encrypted so that it can be used. In addition, you can specify that unencrypted drives are automatically encrypted.

> Note: This option may have the effect that the access rights are adapted to allow the requested behavior.

If you select the “Strict checking for encrypted media” checkbox, DriveLock treats a removable drive as being encrypted only if it contains no files other than the following three:

- Autorun.inf: This file specifies that the Mobile Encryption application is started automatically when the removable disk is inserted on a computer without DriveLock.
- DLMobile.exe: This is the executable program file of DriveLock Mobile Encryption Application.
- *.DLV: This is an encrypted DriveLock container file. For encryption, exactly one container file with the file extension *.DLV must exist.

If you check **Automatically encrypt unencrypted media**, encryption will start when an unencrypted drive is inserted. A wizard opens on the DriveLock Agent to guide the user through the encryption process.

The Option **Encrypt on first write attempt (allow unencrypted read access)** causes the automatic encryption wizard to start only when a write access to the drive occurs for the first time after the connection.

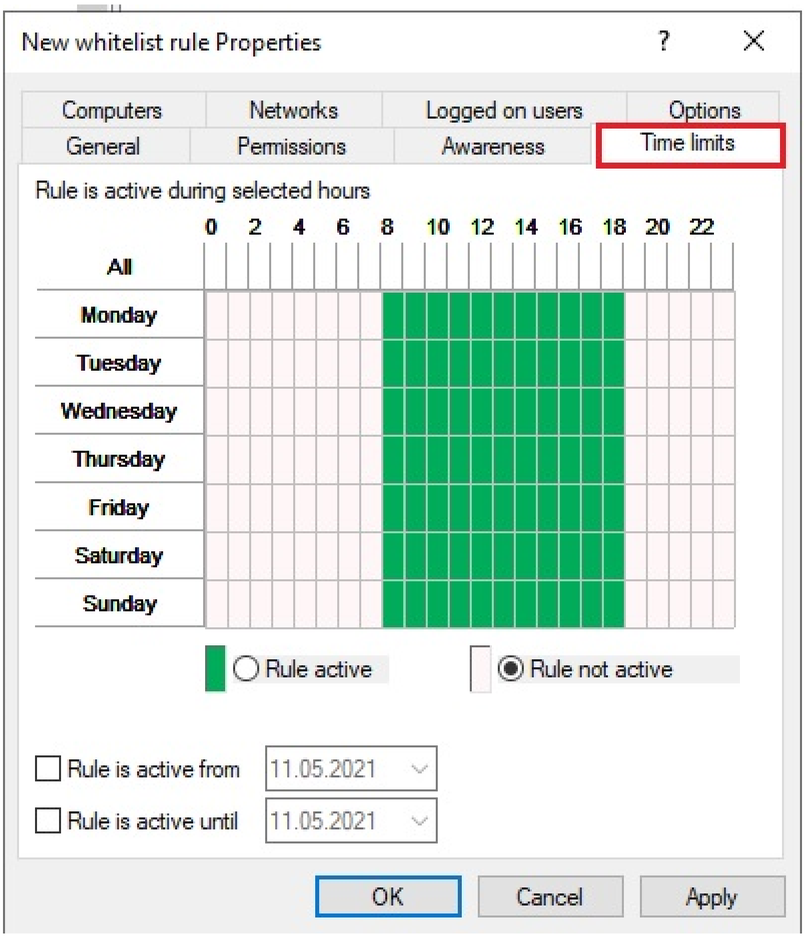
If you enable the **Strict checking for encrypted media (no non-DriveLock files allowed)** option, there must be no other files on the drive for DriveLock to recognize it as "encrypted".

You can additionally specify that already encrypted media should not be connected automatically. In this case, the user can start this process manually.

For more information on encryption, see the Encryption documentation at DriveLock Online Help.

5.4.3.12 Time limits

To ensure that a rule only applies to a very specific time period, you can specify an individual time frame on the **Time limits** tab (e.g. only from 08:00 to 19:00 on weekdays). It is also possible to specify a date for the start and end of the validity period.



Rule is active during selected hours

	0		2		4		6		8		10		12		14		16		18		20		22	
All																								
Monday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩					
Tuesday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩					
Wednesday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩					
Thursday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩					
Friday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩					
Saturday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩					
Sunday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩					

🟩 ○ Rule active   □ ● Rule not active

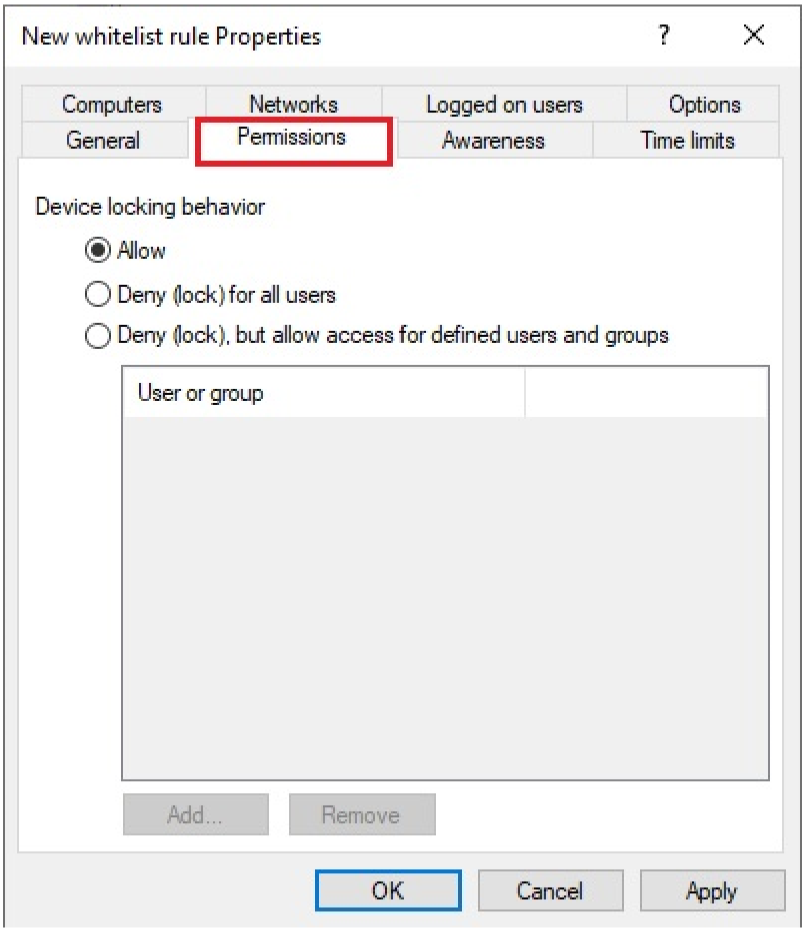
☐ Rule is active from 11.05.2021

☐ Rule is active until 11.05.2021

Highlight the required period by either activating a single field or by clicking on a weekday on the left or a time at the top. In addition, check either **Rule active** or **Rule not active** for the times you selected.

5.4.3.13 Permissions for users and groups

Select the **Permissions** tab to specify which users or groups will have access to the drive.



Device locking behavior

- ● Allow
- ○ Deny (lock) for all users
- ○ Deny (lock), but allow access for defined users and groups

The following options are available:

- Allow: Any authenticated user can use this drive
- Deny (lock) for all users: Access to this drive is locked for all users.
- Deny (lock), but allow access for defined users and groups: The drive is locked, but access is possible for the specified user(s) or group(s), either read-only or also write.

To include another group or user in the list, click **Add**. Click **Remove** to delete the previously selected entry. Specify for the user or group whether they can copy data to the drive or whether read-only access is allowed.

5.5 Network profiles

DriveLock allows you to configure various settings depending on the current network connection. This functionality can be used with portable computers where users work in different locations, for example, in the office, home office, or at customer sites.

Whitelist rules can be configured to apply to specific networks. For example, it is possible that all network devices are disabled as soon as a notebook is connected to a network other than its own. Not only rules can be activated dynamically, but certain settings regarding the network connection can be changed. These settings include the Internet Explorer proxy configuration or the current default printer.

Network profiles can also be used in conjunction with Application Control. This way you can allow or disallow the execution of certain programs depending on the current

Note: Please note that for technical reasons a reboot must be performed if the network connection (cable) is disconnected during hibernation / power saving mode and the computer does not make a new network connection afterwards before DriveLock can detect that the computer is "offline".

For more information on setting network connections, click here.

5.5.1 Settings

The following settings can be configured for network profiles:

- **Taskbar notification area settings**

  This setting allows you to configure the visibility of profiles and their appearance to the user. If you do not want network profiles to be displayed, uncheck the "Display notification area icon" option. If it is enabled, the icon defined for a network connection is displayed in the taskbar. You can also choose whether the icon is visible only during a message or all the time.

- **Disable WiFi connections when computer is connected to LAN**

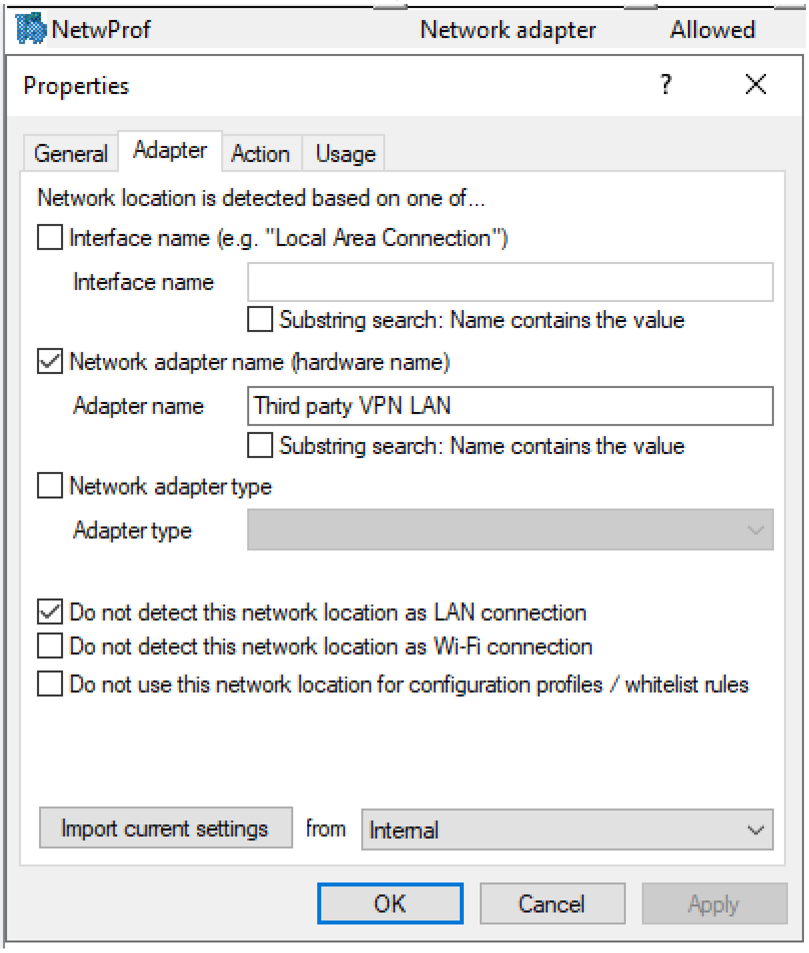
  DriveLock provides the ability to disable wireless network adapters (if any) when the computer is connected to a LAN. This can prevent cross-network links, which can usually pose a security risk to your infrastructure. WiFi connections are blocked during this time.
  Use case: Deploying third-party VPN clients
  WiFi connections should not be allowed if there is a network connection. On notebooks, a third-party VPN client (no Windows-integrated VPN connection) is used to connect mobile users to the corporate network. The third-party VPN client installs a virtual network card. Use case: A client is connected via WiFi and establishes a connection via VPN: If the option Disable WiFi connections when computer is connected to LAN is enabled, the WiFi connection will be disconnected because DriveLock thinks it is connected to a physical network.

To allow the VPN connection via WiFi outlined in the example, you need to exclude the VPN client's virtual network card in DriveLock. To do so, click **Network profiles** -> **Locations / Sites** - right click **New** -> **Network adapter** - **Adapter** tab (see figure below).

There, select a method to uniquely and reliably identify the VPN client's virtual network card. Once the VPN client is installed locally, you can import information on the network card selection and settings as criteria directly:

- **Interface name**: Name of the network connection. This name may vary.
- **Network adapter name**: Name of the adapter This name is usually identical.
- **Adapter type**: Type of network adapter. The reported value may differ per network adapter.

To exclude the adapter in this scenario, select the **Do not detect this network location as LAN connection** option:



NetwProf | Network adapter | Allowed

Properties

Network location is detected based on one of...

□ Interface name (e.g. "Local Area Connection")

Interface name:

□ Substring search: Name contains the value

☑ Network adapter name (hardware name)

Adapter name: Third party VPN LAN

□ Substring search: Name contains the value

□ Network adapter type

Adapter type:

☑ Do not detect this network location as LAN connection

□ Do not detect this network location as Wi-Fi connection

□ Do not use this network location for configuration profiles / whitelist rules

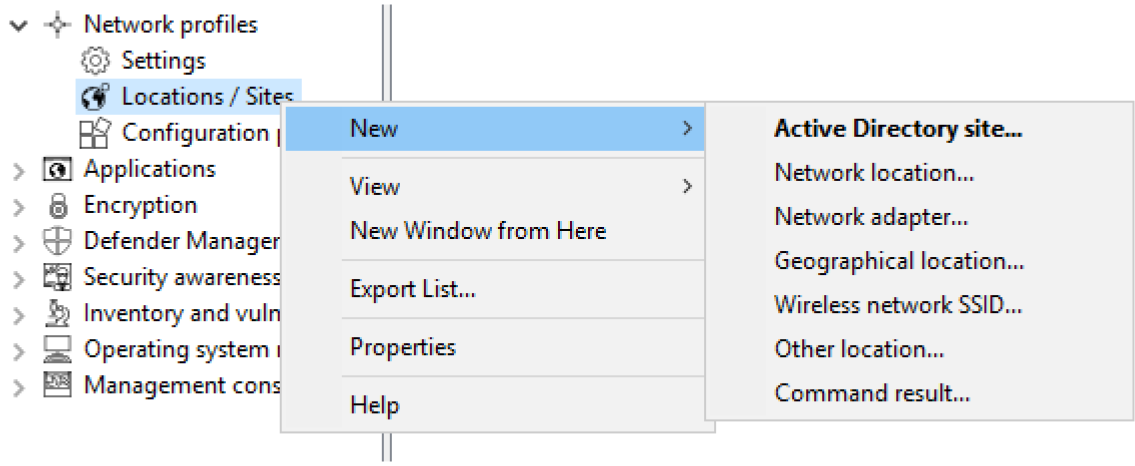
Internal

- **Allow users to configure personal networking profiles (compatible with agents prior to version 2022.2)**: This setting can only be used for agents with older versions (before 2022.2). This feature is no longer available for new agents.

5.5.2 Locations / Sites

To configure settings and assign whitelist rules based on a network connection, you must define how DriveLock identifies networks.

Right-click **Locations / Sites**, select **New** and then the required type from the context menu. For each type, you can later also select the required configuration profile from a list.



The following types of sites are available:

- **Active Directory site**

  If you select an Active Directory site, the connection is determined based on the current name of the site
  You can apply the currently valid settings by clicking the respective button. DriveLock reads this information directly from Active Directory and automatically fills in the **AD Site Name** and **Domain GUID** input fields. Alternatively, you can enter the name yourself or select an existing location in Active Directory by clicking the "..." button.

- **Network location**

  If it is necessary to define the connection using IP information (such as an IP address space), select Network Connection from the context menu. Enter a name and select an icon for display. Then configure the IP information on the **IP Settings** tab. You have the option of reading out the current settings from one of the existing network connections or entering them manually. To do so, activate the respective criteria and enter the necessary information (such as IP address space, gateway or DHCP server).

- **Network adapter**

  A network can be detected by the network card used, for example in connection with third-party VPN clients.

- **Geographical location**

  A site can also be assigned based on the public IP address. DriveLock tries to determine the public IP address of the client and compares it with the local GEO-IP database. Select one or more countries that you want to use as one site in additional DriveLock rules. You can also use it to generally block the network connection for a specific country (via the **Reaction** tab).
  Example: You have mobile employees who work and travel exclusively in the D-A-CH region. You want to make sure that generally no network connection is possible when a notebook is detected outside the countries Germany, Austria, Switzerland.

  > Note: An active internet connection is required to detect the geographical position.

- **Wireless network SSID**

  If you want your network connection to be detected by a WLAN SSID, select Wireless LAN SSID in the context menu.

- **Other location**

  A special connection can be used for two reasons:

  - You need to adjust settings automatically when the computer is not connected to any network (offline)
  - You want to configure settings (or set an action) if the computer is connected to a network that could not be detected

- **Command result**

  In some situations, it might not be acceptable for security reasons to detect a network based only on the Active Directory domain GUID or IP address. However, since there are many ways to scan your own network for identity features, you can use a self-written program or script for this purpose. If this returns the value `1`, the test is assumed to pass. This makes it possible to check for the presence of certain computers with certain names, services or settings, for example. Or you can ensure that a computer meets predefined security policies before allowing it to connect to a network.
  A command prompt is an executable command-line interface program. For example, you can execute a program (*.exe) or a Visual Basic script (*.vbs), or even a script of the new Windows PowerShell.

Note: To run a VB script, you must specify the full path to the script file (e.g. "cscript c:\programing\scripts\meinscript.vbs").

5.5.3 Configuration profiles

By using a configuration profile along with a network connection, DriveLock is able to automatically adjust certain computer settings after detecting the connection. The profile defines where to make changes:

- Internet Explorer proxy settings
- Standard printer

In addition, the DriveLock Agent can enforce the update of group policies for the computer and/or the user when the network connection changes, or running a script or program.

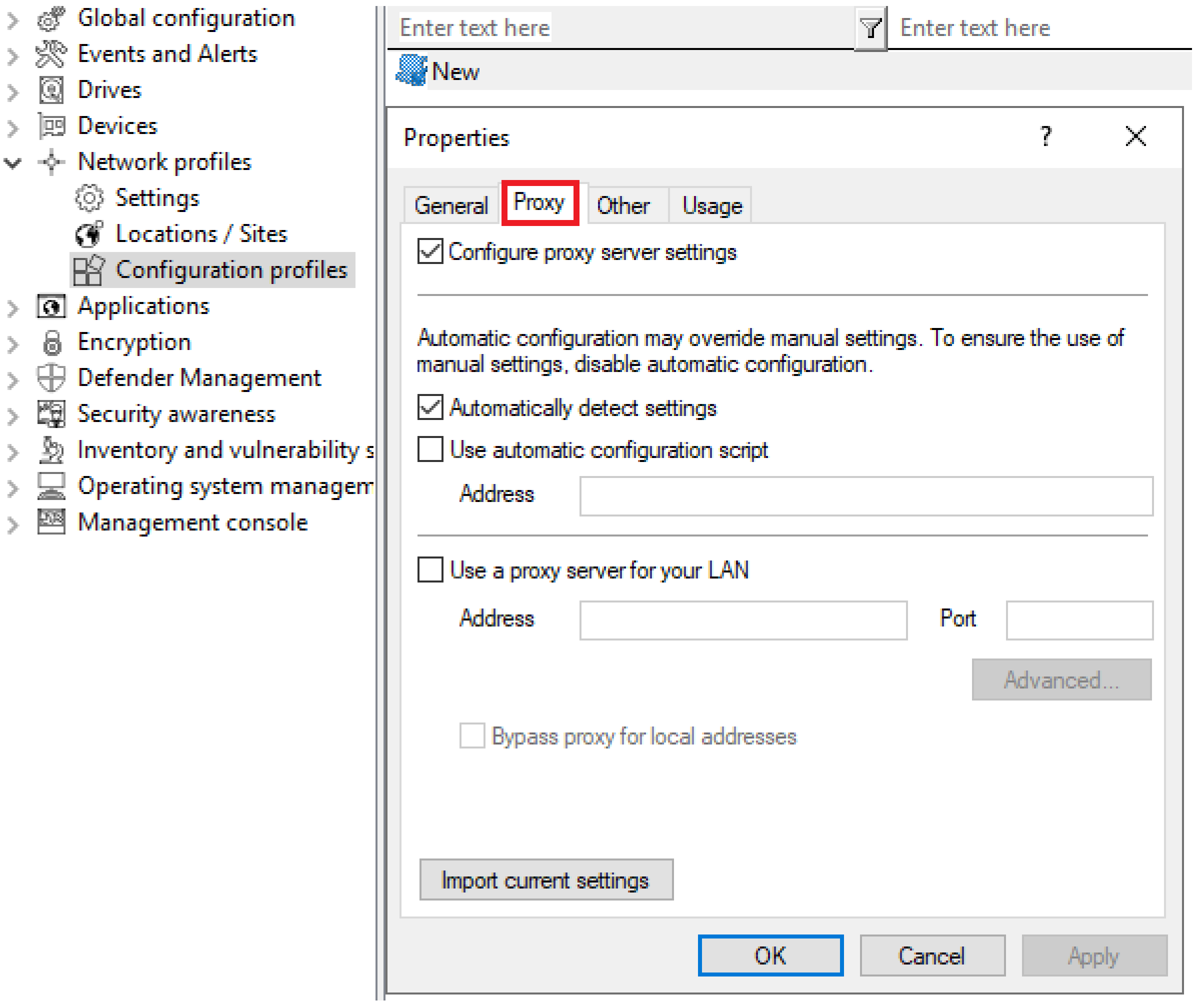
Please do the following:

Select the **Configuration profiles** sub-node and then **New** - **Configuration profile...** from the context menu.

First, enter a name for this profile and a comment.

Internet Explorer Proxy Settings

After you have created a new profile, open the **Proxy** tab .



☑ Configure proxy server settings

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

□ Use a proxy server for your LAN

Address Port

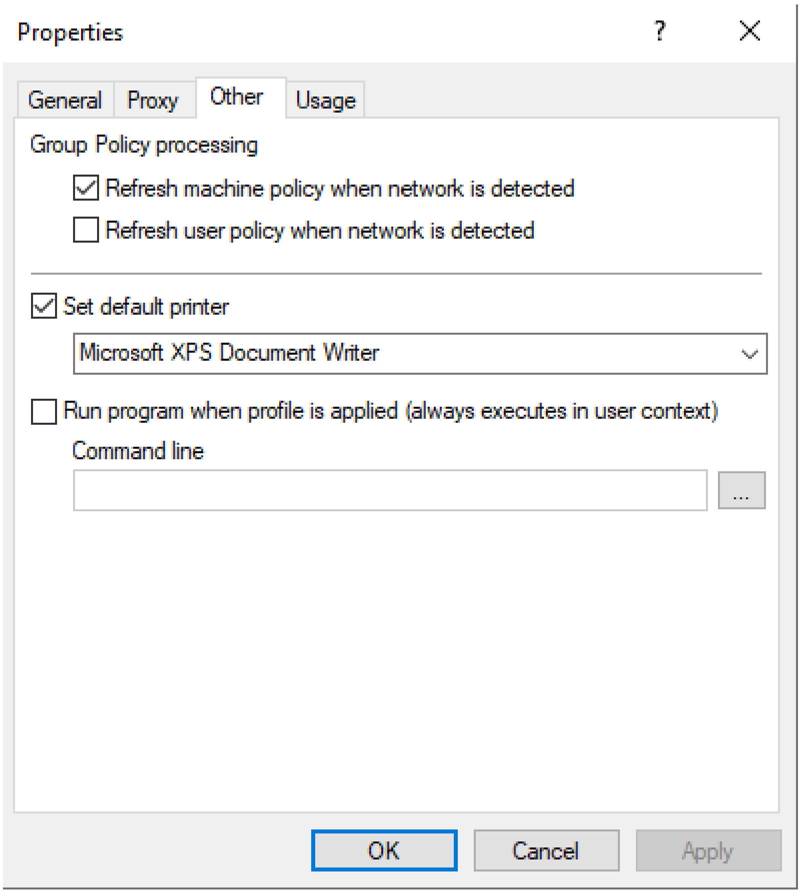
□ Bypass proxy for local addresses

To enable that Internet Explorer settings are automatically adjusted, enable "Configure proxy server settings". Then you can read out the currently valid settings from the local configuration of IE by clicking the Import current settings button. For more on the settings and their effects, please refer to the corresponding documentation for Internet Explorer.

Note: These settings apply only to the current user and are not used by the DriveLock service.

Further actions when networks are detected

Open the **Other** tab.



Group Policy processing

☑ Refresh machine policy when network is detected

☐ Refresh user policy when network is detected

☑ Set default printer

Microsoft XPS Document Writer

☐ Run program when profile is applied (always executes in user context)

Command line

Select a printer from the drop-down list if you want to change the current default printer.

If you enable one or both of the Group Policy options, DriveLock Agent will ensure that the appropriate Group Policies are reloaded when the network connection is changed.

The command line can contain any command executable from the command line. Thus, for example, you can run a program (*.exe), a Visual Basic script (*.vbs) or scripts for the new Windows PowerShell.

In this way it is possible to react to a detected new network connection differently.

Note: To run a VB script, you must specify the full path to the script file (e.g. "cscript c:\programing\scripts\meinscript.vbs").

You can choose between two options:

- File system: the file exists on the computer's local hard drive
- Policy file store: Use the file from DriveLock's policy file store

Note: The policy file store is a file container that is stored as part of a local policy, group policy, or configuration file. It can contain any files (such as scripts or applications) that are automatically distributed with a DriveLock configuration. A file loaded from the policy file store is indicated by a "*".

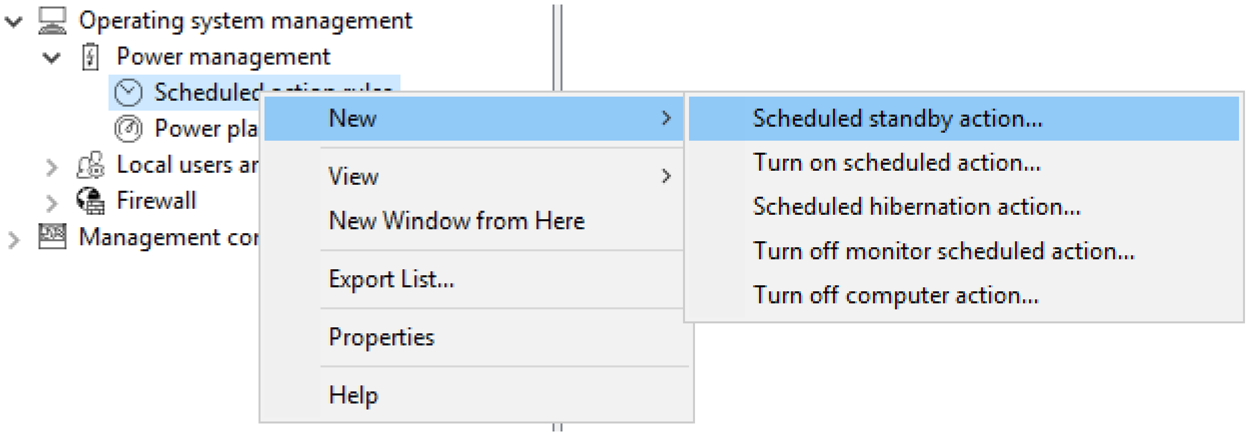
5.6 Operating system management

In this section, you configure settings for DriveLock Agent operation and system management.

5.6.1 Power management

In a DriveLock policy, you can schedule actions when computers should be in standby mode, pause or power off or on, or when which Windows power plan should apply.

Select the desired action or the appropriate plan.


Operating system management
Power management
Scheduled action rules
Power pla
Local users ar
Firewall
Management cor
New
View
New Window from Here
Export List...
Properties
Help
Scheduled standby action...
Turn on scheduled action...
Scheduled hibernation action...
Turn off monitor scheduled action...
Turn off computer action...

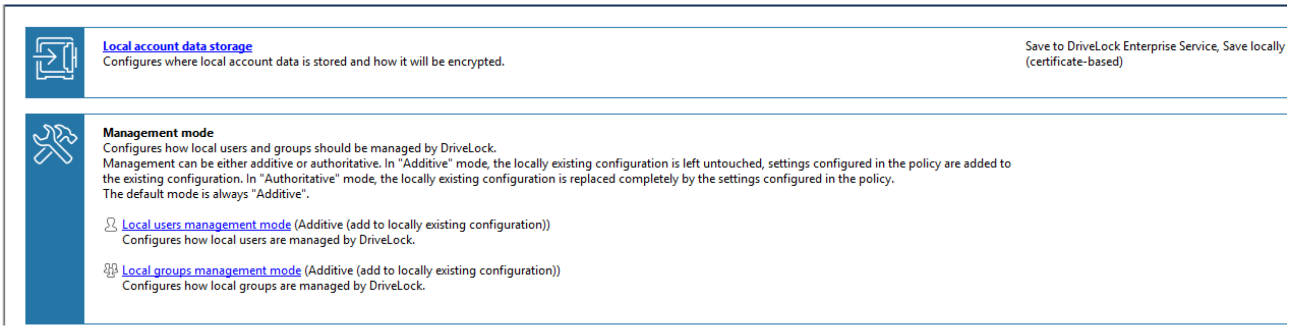
5.6.2 Local users and groups

This DriveLock functionality allows you to restrict important access rights for specific users and groups, making it easier to implement your zero-trust strategy.

For example, certain users can be added to the local administrators group, thus having different local administrators for a certain group of computers. You can then specify the systems specific users get local admin rights for.

5.6.2.1 Settings

The following settings are available:



Local account data storage
Configures where local account data is stored and how it will be encrypted.

Save to DriveLock Enterprise Service, Save locally (certificate-based)

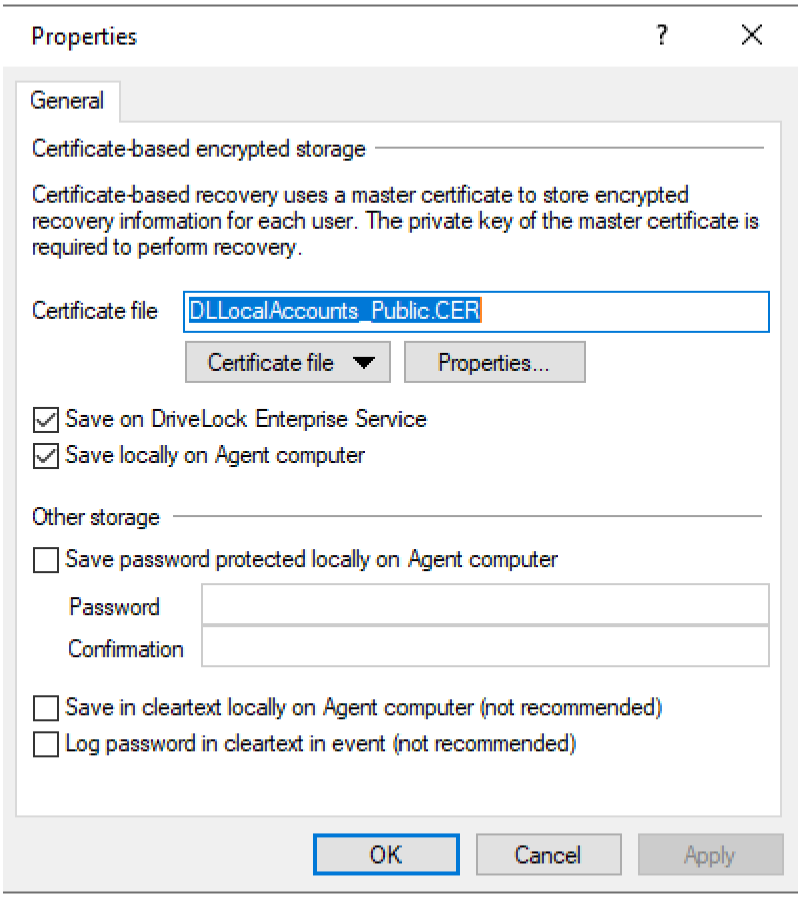
Management mode
Configures how local users and groups should be managed by DriveLock.
Management can be either additive or authoritative. In "Additive" mode, the locally existing configuration is left untouched, settings configured in the policy are added to the existing configuration. In "Authoritative" mode, the locally existing configuration is replaced completely by the settings configured in the policy.
The default mode is always "Additive".

Local users management mode (Additive (add to locally existing configuration))
Configures how local users are managed by DriveLock.

Local groups management mode (Additive (add to locally existing configuration))
Configures how local groups are managed by DriveLock.

Local account data storage

This setting allows you to specify where user names and passwords are stored - certificate based locally or on the DES.



Certificate-based encrypted storage

Certificate-based recovery uses a master certificate to store encrypted recovery information for each user. The private key of the master certificate is required to perform recovery.

Certificate file: DLLocalAccounts_Public.CER

☑ Save on DriveLock Enterprise Service
☑ Save locally on Agent computer

Other storage

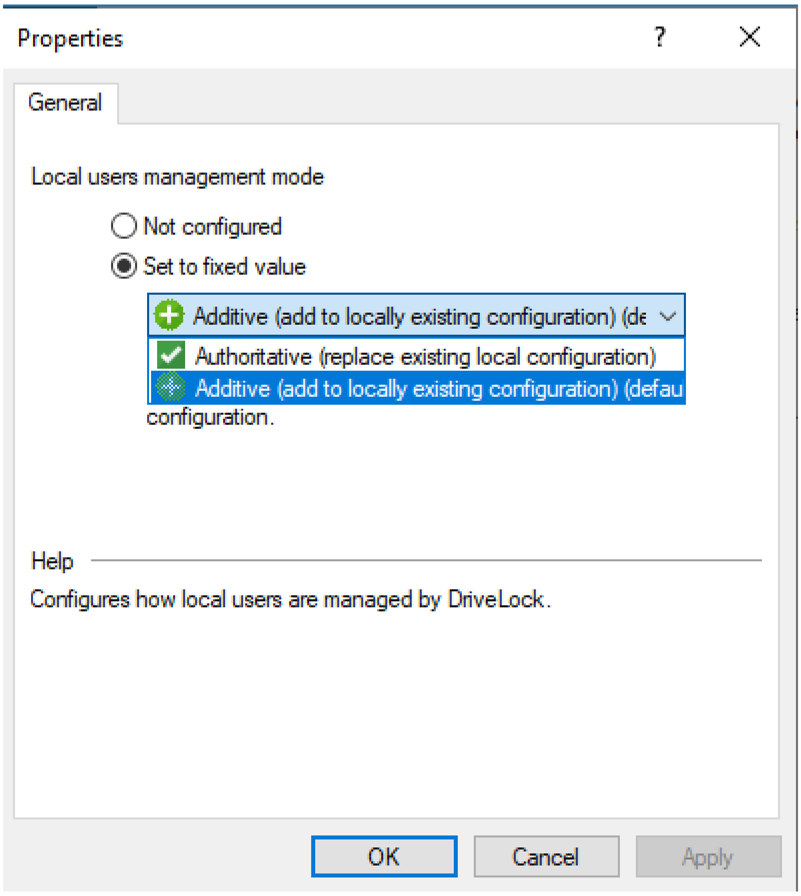
□ Save password protected locally on Agent computer

Password:
Confirmation:

□ Save in cleartext locally on Agent computer (not recommended)
□ Log password in cleartext in event (not recommended)

Management mode settings

Local user administration mode:



Local users management mode

○ Not configured

● Set to fixed value

Additive (add to locally existing configuration) (de

Authoritative (replace existing local configuration)

Additive (add to locally existing configuration) (defau

configuration.

Help

Configures how local users are managed by DriveLock.

The **user and group management mode** can be used to define how users and groups are managed by DriveLock.

- In additive mode (default), the existing local users are not modified, except for the users defined in the policy. So, for example, if a user already exists in the policy, this user will be added in addition to all other local users.
- in the authoritative mode, the existing local users/groups are all deleted and only the users/groups defined in the policy are created.

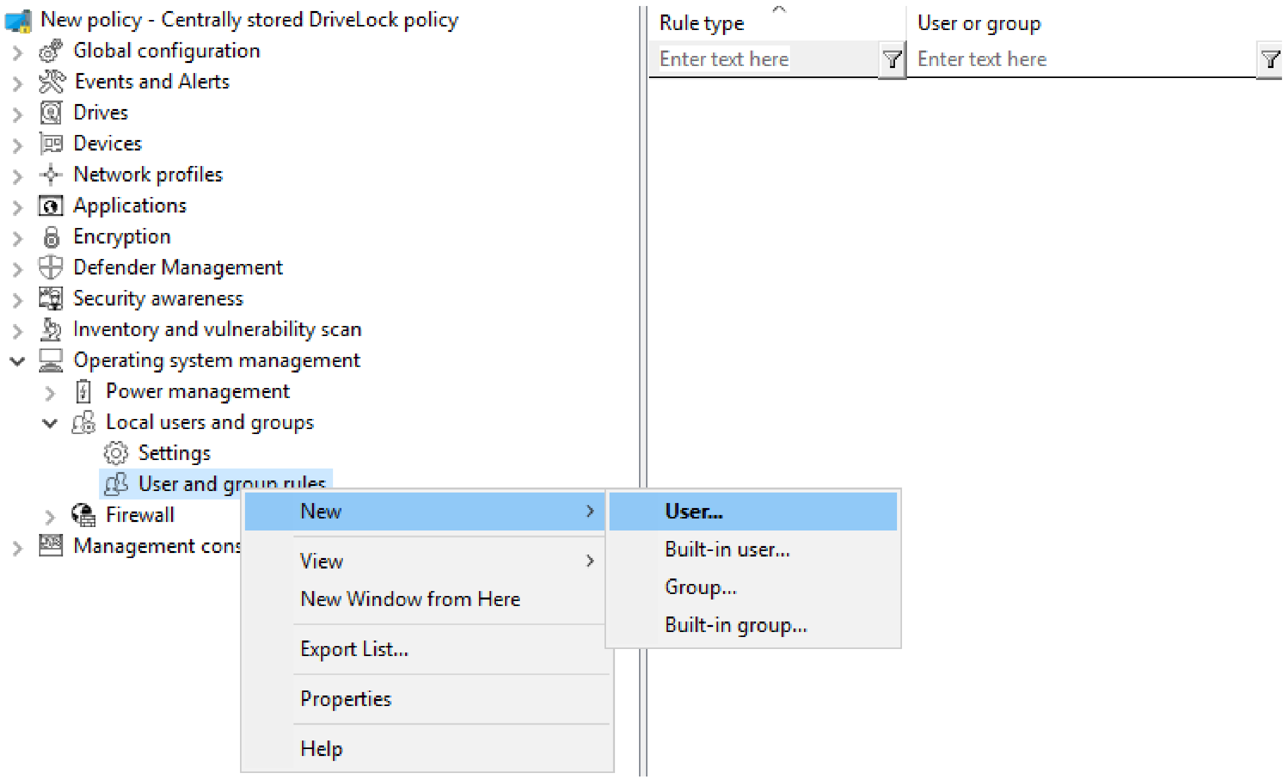
5.6.2.2 User and group rules

Set user and group rules to manage local users and groups. Depending on the management mode, users and groups defined in DriveLock can be added to the local user database or they can completely replace the users and groups in the local user database.

User rules

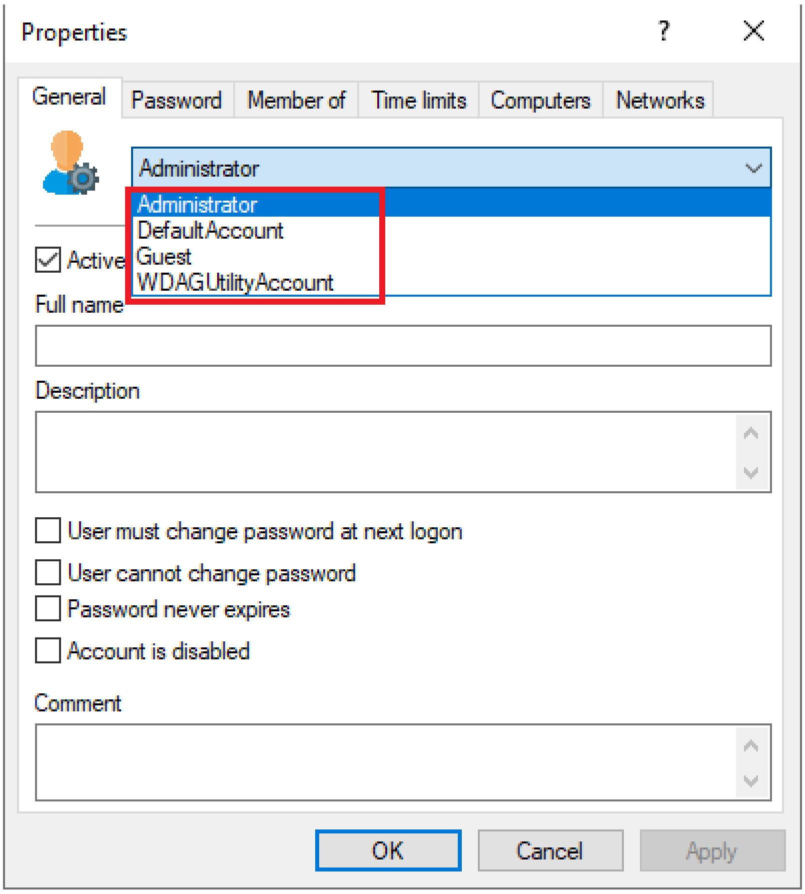
A rule can be created for every user.

Proceed as shown in the figure:



The difference between built-in and custom accounts is the username.

The built-in accounts are the four accounts created during Windows installation (most importantly, the "Administrator" account). These cannot be deleted, but can usually be renamed.



Administrator

Administrator
DefaultAccount
Guest
WDAGUtilityAccount

☑ Active

Full name

Description

☐ User must change password at next logon

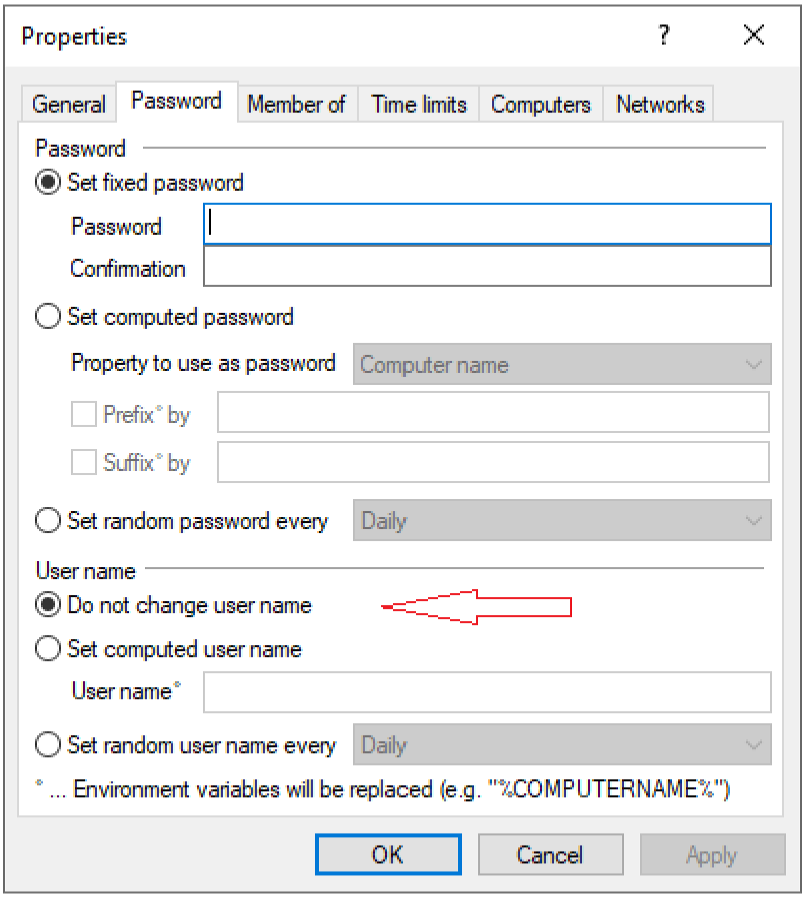
☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Comment

On the **Password** tab you specify whether a fixed, a calculated or a random password should be used for the account. Also, for built-in users, you can specify whether to change the fixed user name:



Password

● Set fixed password

Password

Confirmation

○ Set computed password

Property to use as password: Computer name

□ Prefix* by

□ Suffix* by

○ Set random password every: Daily

User name

● Do not change user name

○ Set computed user name

User name*

○ Set random user name every: Daily

* ... Environment variables will be replaced (e.g. "%COMPUTERNAME%")

Group rules

Again, the built-in groups are the predefined Windows groups. The rules define the membership.

Other users or AD users/groups can be added (using the **Include** button) or removed from the group (using the **Exclude** button). So, for example, if you want to remove a specific AD group from the Administrators group, create a rule for the built-in group and add an "Exclude" to the rule.

5.6.2.2.1 Retrieve local user accounts

Passwords can be retrieved using a local wizard available via the **Retrieve local user accounts...** menu on the DriveLock Agent tray icon menu and/or Start menu.

The wizard will ask you for the user name (or built-in user whose name can be changed) and credentials, and display the password and user name. Only the available options are displayed, so if data is uploaded to DES only, the Password option is grayed out.

In the Taskbar notification area settings, you can specify that the **Retrieve local user accounts...** menu item is displayed in the agent's Start menu.

5.6.2.2.2 Local users and groups in agent remote control

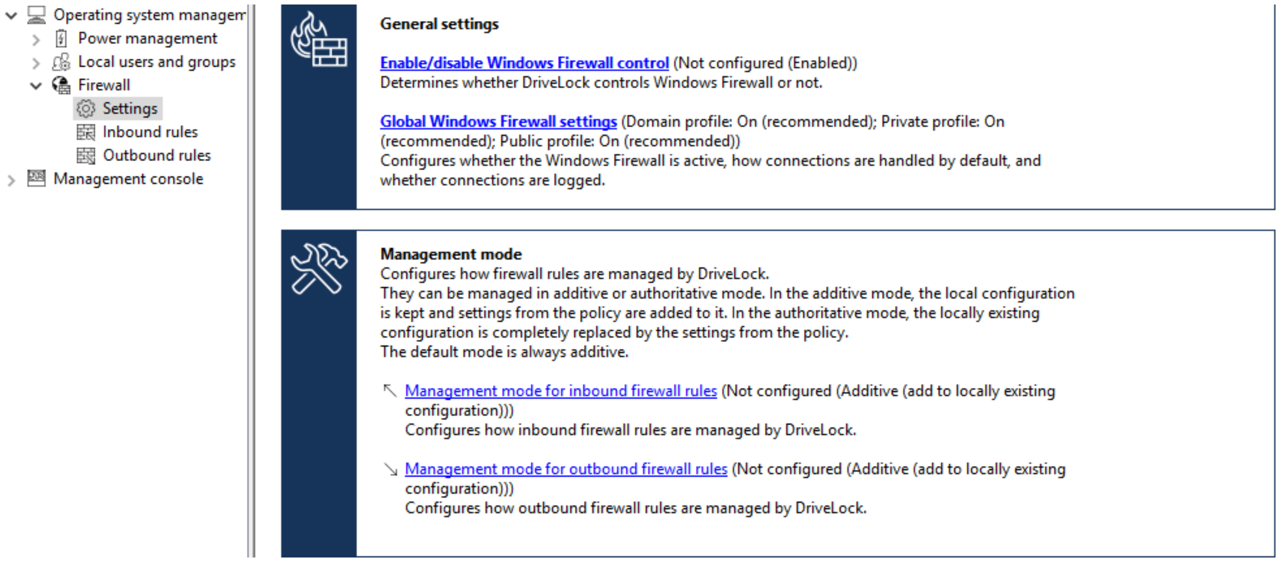
In the remote agent control, a page has been added to the agent properties dialog that displays the local **users and groups**. The users/groups managed by DriveLock are displayed with a colored icon, while other users/groups are displayed in grayscale. Clicking Details displays detailed information about the user/group.

5.6.3 Firewall

These options can be used to manage the firewall settings for DriveLock Agents. This allows rules to be configured for a specific group of computers. DriveLock extends the built-in functionality of Windows Firewall by dynamically adding and removing rules based on conditional settings.

5.6.3.1 Settings

You can configure the following options:



General settings

Enable/disable Windows Firewall control (Not configured (Enabled))
Determines whether DriveLock controls Windows Firewall or not.

Global Windows Firewall settings (Domain profile: On (recommended); Private profile: On (recommended); Public profile: On (recommended))
Configures whether the Windows Firewall is active, how connections are handled by default, and whether connections are logged.

Management mode
Configures how firewall rules are managed by DriveLock.
They can be managed in additive or authoritative mode. In the additive mode, the local configuration is kept and settings from the policy are added to it. In the authoritative mode, the locally existing configuration is completely replaced by the settings from the policy.
The default mode is always additive.

Management mode for inbound firewall rules (Not configured (Additive (add to locally existing configuration)))
Configures how inbound firewall rules are managed by DriveLock.

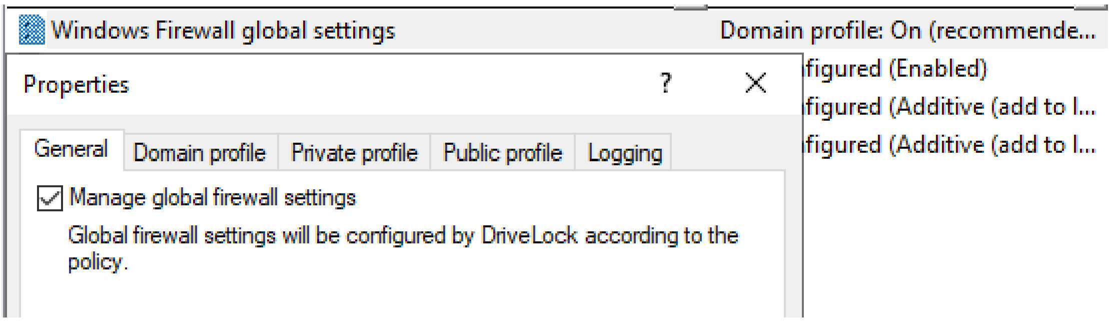
Management mode for outbound firewall rules (Not configured (Additive (add to locally existing configuration)))
Configures how outbound firewall rules are managed by DriveLock.

Enable/disable Windows Firewall control:

The setting has to be active to enable Windows Firewall control on DriveLock Agents. It is enabled by default. DriveLock will then be able to configure firewall settings, manage rules, and generate events related to the firewall.

Global Windows Firewall settings:

The global settings allow you to determine whether DriveLock manages the general Windows Firewall settings. You can also specify firewall settings for each network type and you can configure logging.



Windows Firewall global settings   Domain profile: On (recommende...

figured (Enabled)

figured (Additive (add to l...

figured (Additive (add to l...

Properties

☑ Manage global firewall settings

Global firewall settings will be configured by DriveLock according to the policy.

- **General** tab: If you want DriveLock to configure the Windows Firewall according to the settings in this dialog, check **Manage global firewall settings**. This setting does not affect the actual firewall rules. The rules are managed according to the policy, even if this setting is disabled.
- **Domain profile**, **Private profile** and **Public profile** tabs: You can configure the firewall for each of the network types separately or configure it for the domain profile only and check the **Use these settings for all profiles** setting if you want all profiles to be configured the same.
  The following options are available:
  - **Firewall state**: Select whether the firewall is on or off for the selected network type.
  - **Inbound connections**: Select whether to allow or block inbound connections for the selected network type. By default, inbound connections are blocked if none of the defined rules apply.
  - **Outbound connections**: Select whether to allow or block outbound connections for the selected network type. By default, outbound connections are allowed if none of the defined rules apply.
  - **Display notifications to the user when a program is blocked from receiving inbound connections**: Enable this setting if you want the user to receive a notification when the firewall blocks a connection for which no rule exists yet. By default, notifications are enabled.
  - **Allow unicast responses to multicast or broadcast network traffic**: Enable this setting if you want to allow unicast responses to multicast or broadcast requests within 3 seconds. We recommend that you disable this setting to avoid possible "denial of service" attacks. This setting does not affect DHCP. DHCP unicast responses are always allowed by the firewall. By default, this setting is enabled.

- **Logging** tab: Here you can customize the logging settings. Select the connections you want to log.
  The following options are available:
  - **Log network connections**: Check this option to log network connections. The default path for the log is `%windir%\system32\logfiles\firewall\pfirewall.log`
  - **Log successful connections**: Activate this setting to log successful connections.
  - **Log dropped packets**: Enable this setting to log dropped connections.
  - **Ignore multicast packets while logging**: Enable this setting to exclude multicast packets from logging.
  - **Ignore connections using the following ports**: Specify the ports to be excluded from logging.

Management mode for inbound or outbound connections:

The management mode determines how DriveLock manages firewall rules. Management can be either additive or authoritative.

- In **Additive mode**, rules that exist locally are kept. The rules from the policy are only added. If the policy contains built-in firewall rules that also exist on the agent, these rules are modified according to the policy.
- In **Authoritative mode**, existing rules on the agent are deleted and replaced with the rules in the policy. Existing built-in rules on the agent are only disabled by DriveLock and not deleted if they are not present in the policy.

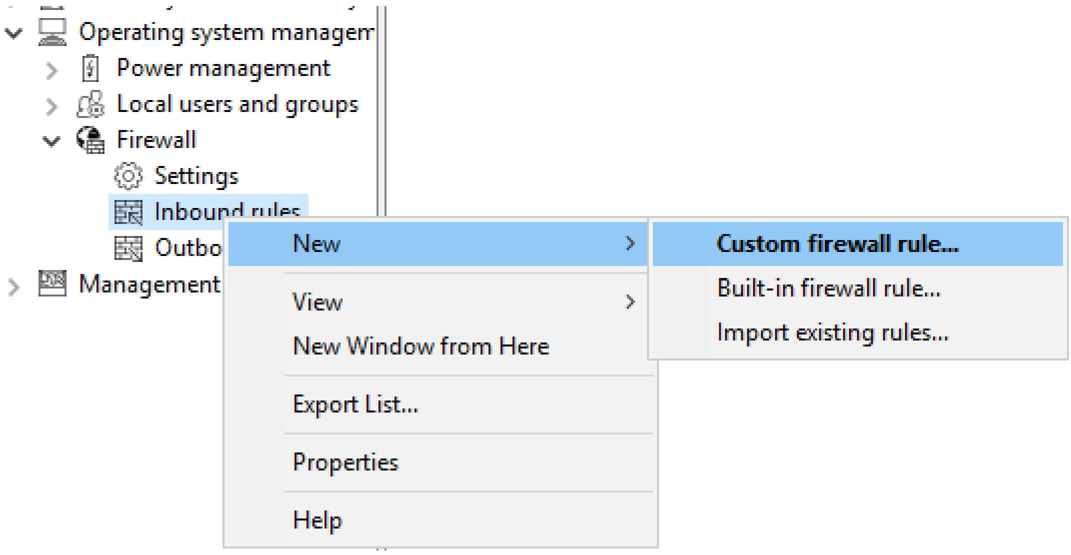
Rules created via the group policy will remain in place. DriveLock neither modifies nor deletes them.

Rules that DriveLock creates for product functionality are not managed by DriveLock. They are always created and remain in the authoritative mode.

The default setting is additive.

5.6.3.2 Inbound and outbound rules

You can define inbound and outbound rules in the policy. To do so, select **Inbound rules** or **Outbound rules** and open the context menu.



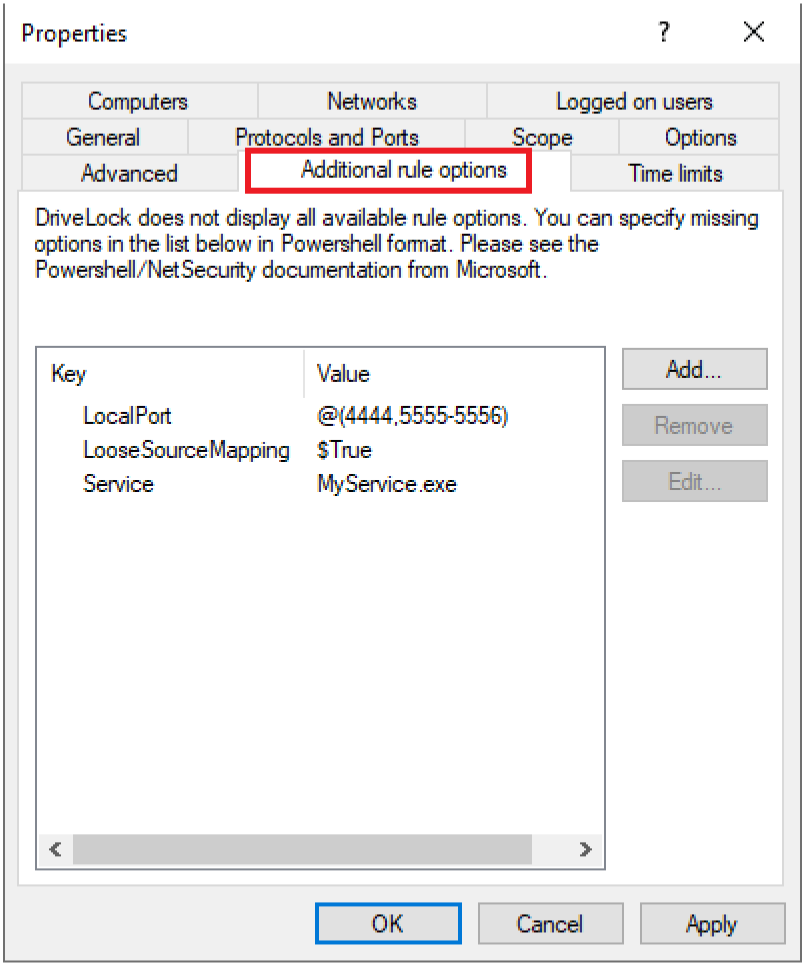
The following configuration options are available:

- **Custom firewall rule**:
  1. Specify the name of the rule and enter a description.
  2. Choose whether to allow or block the connection in the action.
  3. Select if the rule will be active in the DriveLock policy. If you uncheck this option, the rule will be treated as if it does not exist in the policy.
  4. Select if the rule will be created as active or deactivated in the Windows Firewall.
  5. You can set these two settings later in the context menu of the rule without having to open the properties dialog again.
  6. After that, define the rest of the rule options.

  In case you require an option that is not provided in the dialog, you may add it on the **Additional rule options** tab. To do so, use Powershell format. Refer to Microsoft's Powershell/NetSecurity documentation via the commands `New-NetFirewallRule` and `Set-NetFirewallRule` for a list of possible options.
  Please note the following syntax rules:
  - The name of the option is specified as the key name.
  - The value can be a string, a boolean value or a list.
  - For string type options, simply enter the value.
  - For Boolean type options the values `$True` or `$False` can be used.
  - For options that expect a list of strings, specify the values in parentheses pre-

ceded by a `$`. This is also true if the list is to contain only one value, e.g. `$(Wert1, Wert2)`.

In the example, you can use the **Service** option to specify the service to which the rule should apply (see the figure):



DriveLock does not display all available rule options. You can specify missing options in the list below in Powershell format. Please see the Powershell/NetSecurity documentation from Microsoft.

Key	Value
LocalPort	@(4444,5555-5556)
LooseSourceMapping	$True
Service	MyService.exe

Note: Note that these options only work with Windows 8.1 or later. Older operating systems will ignore these options.

- **Built-in firewall rule**:
  Built-in firewall rules are predefined firewall rules that are integrated into the operating system. Creating a built-in firewall rule in the policy involves modifying the corresponding rule on the agent. In case the rule does not exist on the agent yet, it will be created.
  You can choose the rule from your local list of rules or you can display the list of rules from an agent.

Note: Note that not every rule exists on every operating system.

Proceed as you did when creating the custom rules.

- **Import existing rules**:
  You can import all existing firewall rules at once. Again, you can choose to use the locally available rules, i.e. the rules of the computer where the policy editor is currently running, or the rules from an agent.
  Sometimes the rules you want to import contain options that DriveLock cannot import or rules with the same name already exist in the policy. If this happens, DriveLock issues a notice in the import dialog and creates a file in the `%temp%` directory that contains a list of these rules.
  1. Click **Show details** to navigate to the directory.
  2. Open the `LocalFirewallImportReport.txt` file for local rules or `RemoteFirewallImportReport.txt` for rules of the selected agent.
  3. Select whether the imported rules should be added to or replace the existing rules in the policy.
  4. Click **Import to** import the rules. This process may take a few minutes. After the import, the **Comment** column contains the date and the name of the computer the rules were imported on / from.
  5. After importing, you can edit rules as usual.

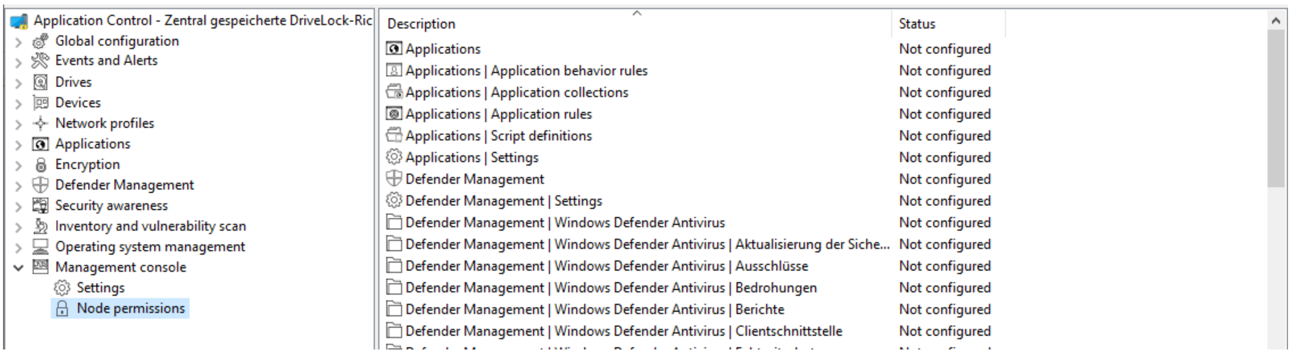
Note: Note that with the built-in firewall rules, some options are read-only and cannot be changed.

5.7 Management console

In this section you can specify management console settings, especially permissions for using the console.

5.7.1 Node permissions

The DMC can be configured to allow certain users or groups to perform only certain functions. It is possible to assign permissions to users for almost every item in the navigation console.



- Application Control - Zentral gespeicherte DriveLock-Ric
  - Global configuration
  - Events and Alerts
  - Drives
  - Devices
  - Network profiles
  - Applications
  - Encryption
  - Defender Management
  - Security awareness
  - Inventory and vulnerability scan
  - Operating system management
  - Management console
    - Settings
    - Node permissions

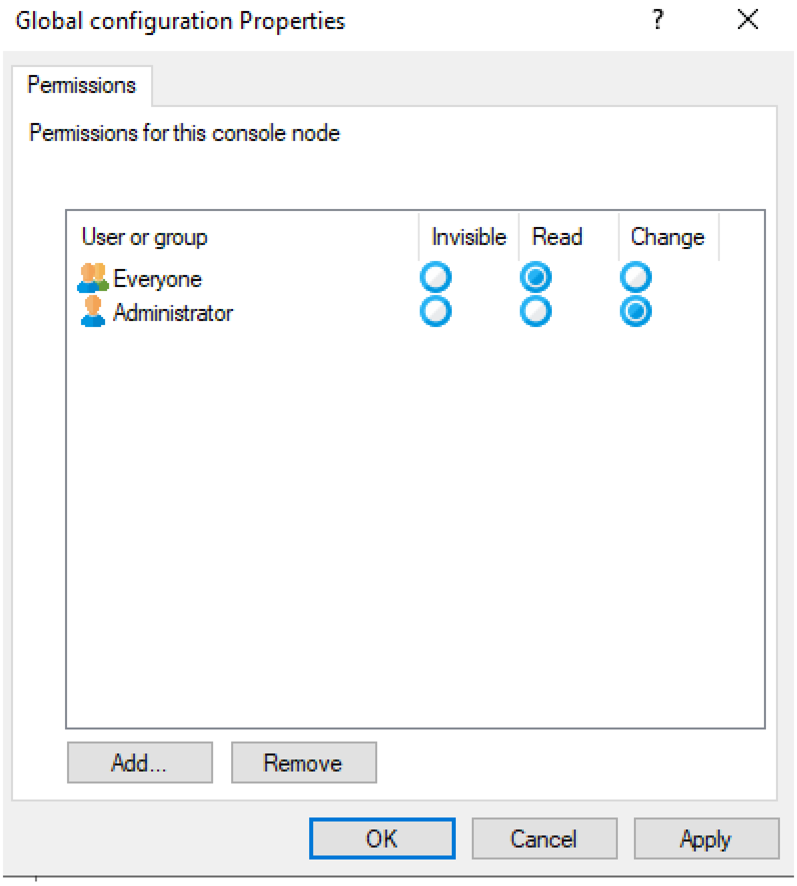
Description	Status
Applications	Not configured
Applications | Application behavior rules	Not configured
Applications | Application collections	Not configured
Applications | Application rules	Not configured
Applications | Script definitions	Not configured
Applications | Settings	Not configured
Defender Management	Not configured
Defender Management | Settings	Not configured
Defender Management | Windows Defender Antivirus	Not configured
Defender Management | Windows Defender Antivirus | Aktualisierung der Siche...	Not configured
Defender Management | Windows Defender Antivirus | Ausschlüsse	Not configured
Defender Management | Windows Defender Antivirus | Bedrohungen	Not configured
Defender Management | Windows Defender Antivirus | Berichte	Not configured
Defender Management | Windows Defender Antivirus | Clientschnittstelle	Not configured

Permissions are configured within a DriveLock policy as a setting for the DriveLock Agent, not for a DriveLock Management Console itself. This ensures that a user cannot install a DriveLock Management Console on his computer in the company and work with it without authorization.

The section "Distributing DriveLock configuration settings" describes the options and how to use DriveLock policies.

Within the DriveLock policy, click the Management Console -> Node Permissions item to view all current node permissions. After installation, all items remain in the "Not configured" state until a setting is changed. By default, the "Everyone" group has full access to all points.

Double-click an object to view its detailed settings.



Global configuration Properties

Permissions

Permissions for this console node

User or group	Invisible	Read	Change
Everyone	○	●	○
Administrator	○	○	●

Click Add to assign a new user or group to this node. Select a group or user and click Remove to remove the selected account from the list.

There are the following node permissions:

- Invisible: The node is not visible (and therefore not accessible) to the user.
- Read: The user can use the node to view all current settings, but cannot change anything
- Change: The user can change all settings within this node.

If you assign different permissions for more than one group and a user is in more than one of these groups, the higher priority permission will be applied. For example, if a user has both the "Read" permission and the "Modify" permission, the "Modify" permission will be applied (analogous to the permissions in Windows).

Warning: It is not possible to configure any node without at least one user or group having change rights. In this case, a warning is displayed.

6 Other

6.1 DriveLock on Terminal Servers

DriveLock can be used on terminal servers, this applies in particular to the Device Control and Application Control modules. There are various connection options between a client and the terminal server, some with restrictions, some with full support.

Note: For more information about **DriveLock in Citrix environments**, please see the corresponding technical article at DriveLock Online Help.

6.1.1 Connection types

Supported functions depending on the connection type (drive connections only):

Function	FAT Clients	Windows Embedded Client	Virtual Clients	Thin Clients
Authorizations based on users / groups	Yes	Yes	Yes	Yes
Sharing based on the connected drive letter	Yes	Yes	Yes	Yes
Approvals based on hardware data incl. serial number	Yes	Yes	Yes	No
File system filter	Yes	Yes	Yes	Yes
File system filter incl. header check	Yes	Yes	Yes	Yes

Function	FAT Clients	Windows Embedded Client	Virtual Clients	Thin Clients
File logging	Yes	Yes	Yes	Yes
Shadow copy	Yes	Yes	Yes	Yes
Requires DriveLock Agent locally	Yes	Yes	Yes	No
Requires DriveLock Agent on the TS	No	No	The virtual client is used instead of the terminal server.	Yes

If you want to use application control on the terminal server, the DriveLock Agent is always required on the terminal server, regardless of the above chart.

FAT clients / desktop clients

A FAT client or desktop client is a normal computer running Windows. The FAT client connects to the terminal server. The DriveLock Agent is already installed on the FAT client, so control occurs right where a device is connected. The user may only use the devices in his terminal server session that are also enabled locally by the DriveLock Agent.

If the FAT clients are in the same domain, the configuration can be done via group policy. Otherwise, we recommend using centrally stored policies.

Windows Embedded Clients

A Windows Embedded client is a special computer running Windows XP Embedded or above. The Windows Embedded client connects to the terminal server. The DriveLock agent is already installed on the embedded client or integrated into the image. Thus, control takes place exactly where a device is connected. The user may only use the devices in his terminal server session that are also enabled locally by the DriveLock Agent.

If the Windows Embedded clients are located in a domain, the configuration can be done via group policy. Otherwise, we recommend using centrally stored policies.

Virtual Desktop Infrastructure (VDI)

Ein Virtual-Client ist ein virtueller Computer mit Windows. A client connects to the virtual desktop. The DriveLock agent is installed on the virtual client. A USB mapping driver is used to connect all locally connected USB devices into the virtual computer. The user may only use the devices in his virtual client that are also released there by the DriveLock Agent.

If the virtual clients are located in the same domain, the configuration can be done via group policy. Otherwise, we recommend using centrally stored policies.

Thin Clients

A thin client is a specially stripped-down computer with a proprietary operating system. A thin client connects to the terminal server. The DriveLock agent is installed on the terminal server. The user may only use the devices in his terminal server session that are also released there by the DriveLock Agent.

If the terminal servers are located in the same domain, the configuration can be done via group policy. Otherwise, we recommend using centrally stored policies.

6.1.2 Licenses required for terminal server users

Users working on terminal servers require licenses for the Application Control, Device Control, Encryption 2-Go and File Protection modules, as long as they are active on the terminal server.

This applies to users who have been logged on to a terminal server in the last 30 days. A user always needs only one license, regardless of whether he or she was logged on to one or more terminal servers.

Computer and user licenses are displayed separately in the DOC.

6.1.3 Terminal server rules

Depending on the connection type, the configuration takes place on the client or server side. It is important to set up an authorization concept by asking some questions: What do you want to block and which exceptions are required? How much detail do you need to go into? Do you need to unlock based on users/groups, on connected drive letters, on hardware data, or a combination of these?

Another distinction applies to the whitelist rules. At a minimum, permissions can be assigned based on the connected drive letter on the terminal server. Assigning permissions based on individual drives using the hardware data (e.g. USB stick Kingston DataTraveler) only works under certain conditions.

We recommended splitting the configuration of terminal servers and clients, for example, by employing a separate configuration.

Global configuration

The easiest case is to assign permissions to all connected drives of a client. It does not matter what kind of drive is connected, for example a hard disk or a USB stick. Permissions are implemented for all these connected drives based on users or groups. A distinction is made here according to the connection protocol: (**Advanced Configuration** ->) **Drives** -> **Removable drive locking**

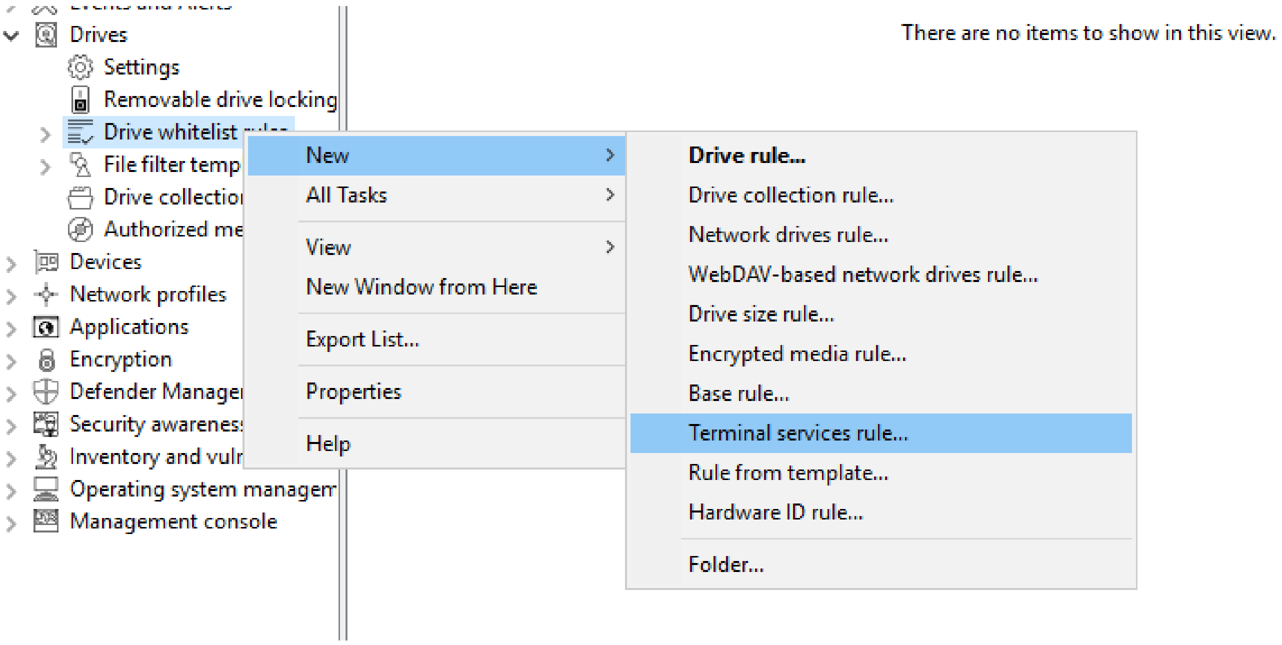
- **Windows Terminal Services (RDP) client drive mappings**: All connections via RDP, Windows default.
- **Citrix XenApp (ICA) client drive mappings**: All connections via ICA, Citrix standard. Requires Citrix Presentation Server 4.5 (64-bit) or XEN 5 or above.

Based on the connected drive letters

To block drives, you need to configure the Terminal Server environment to use predefined drive letters for certain drive types (e.g. USB removable drives). This can be set on thin client side. Then you can create a Terminal Services rule to set permissions or time restrictions on this drive letter.

Example: A user connects to a terminal server. The client is a thin client. All thin clients are configured by the administrator to always mount USB drives as drive U: within the terminal server session. The administrator creates a Terminal Services rule in DriveLock for the U: drive and assigns permissions to a group on it. In this way, access to USB drives can be controlled via the group.

To create an exception based on the connected drive letters, navigate to **Drives**: **Drive whitelist rules**, then right-click on it to **New** -> **Terminal services rule...**.



Next, select a letter from the drop-down menu and activate the appropriate protocol that is used in your environment. Permissions are assigned on the Permissions tab:

Based on the hardware data

If you want to create a whitelist rule based on the hardware data, the connection type allows it, you can create a rule as usual: **Drives** -> **Drive whitelist rules** -> **Drive rule....** and then connect to the client or terminal server, depending on the connection type, and select the drive to be shared. Then, assign the permissions on the Permissions tab.

File filter

The file filter can be used to restrict and log accesses based on file types (PDF, DOCX, etc.). However, the file filter must have been created beforehand.

The file filter can be used and assigned in all rules. In general, the client-side file filter is more powerful than server-side. Restrictions due to the connection types can be found in the overview table in chapter Connection types.

A file filter can be applied to all types of rules.

In the following example, we use a file filter template (which locks executable files), and apply it server-side to connections made using the ICA protocol: **Drives** -> **Lock Settings** -> **Citrix XenApp (ICA) Client Drive Mappings** -> **Filter /Shadow** tab.

After that, there are the following options:

- **Filter files [...]**: file types are allowed/blocked based on the selected file filter template.

- **Audit and shadow files [...]**: Operations (read, write) are logged and can be evaluated later with the DOC.
- **Allow access as configured only to selected subfolders**: Here you can **configure folders** by clicking this button.

6.1.4 Application Control on terminal servers

Application Control can also be used with terminal servers. This allows you to prevent users from accessing specific programs. System programs, such as cmd.exe, wscript.exe, cscript.exe, mmc.exe can also be blocked for basic users. Administrators are still allowed to run the program.

The configuration here is identical to the client configuration.

Note: For more information, see the Application Control documentation at DriveLock Online Help.

6.2 Troubleshooting

As part of the complete DriveLock installation, you can use a command line-based diagnostic tool. This tool allows you to diagnose any storage devices on a computer.

The command line utility "dlcmd.exe" is installed in the DriveLock installation directory. DlCmd.exe can display various types of diagnostic information.

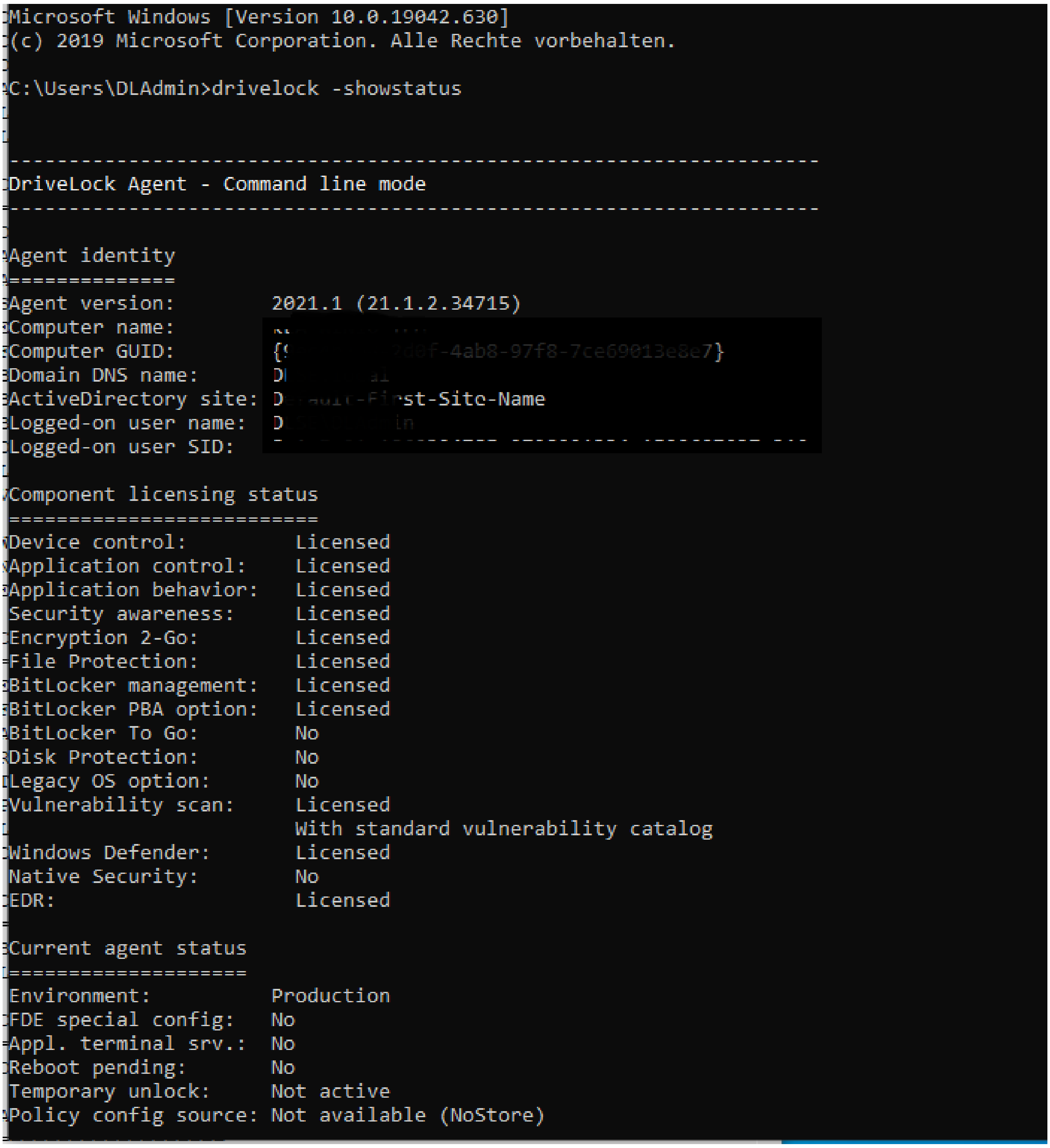
Note: For more information on troubleshooting, see Knowledge Base articles KBA00106: Collecting and Submitting Diagnostic Data from DriveLock Agent - Trace (DriveLock Support Companion) and KBA00422: Collecting Diagnostic Information. If you need more information, please contact DriveLock Support.

6.2.1 Checking the agent status

There are two ways how you can get information about the current status of the agent and its configuration as an administrator or even as an end user on the computer running the DriveLock Agent:

1. **Command line command**

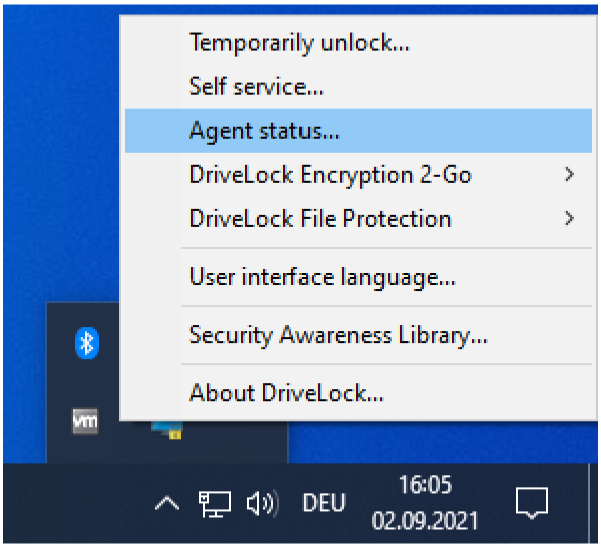
   Open a command line window and type `drivelock -showstatus`:



```
Microsoft Windows [Version 10.0.19042.630]
(c) 2019 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\DLAdmin>drivelock -showstatus



--------------------------------------------------------------------
DriveLock Agent - Command line mode
--------------------------------------------------------------------

Agent identity
==============
Agent version:         2021.1 (21.1.2.34715)
Computer name:         [redacted]
Computer GUID:
Domain DNS name:
ActiveDirectory site:
Logged-on user name:
Logged-on user SID:

Component licensing status
==========================
Device control:          Licensed
Application control:     Licensed
Application behavior:    Licensed
Security awareness:      Licensed
Encryption 2-Go:         Licensed
File Protection:         Licensed
BitLocker management:    Licensed
BitLocker PBA option:    Licensed
BitLocker To Go:         No
Disk Protection:         No
Legacy OS option:        No
Vulnerability scan:      Licensed
                         With standard vulnerability catalog
Windows Defender:        Licensed
Native Security:         No
EDR:                     Licensed

Current agent status
====================
Environment:           Production
FDE special config:    No
Appl. terminal srv.:   No
Reboot pending:        No
Temporary unlock:      Not active
Policy config source: Not available (NoStore)
```

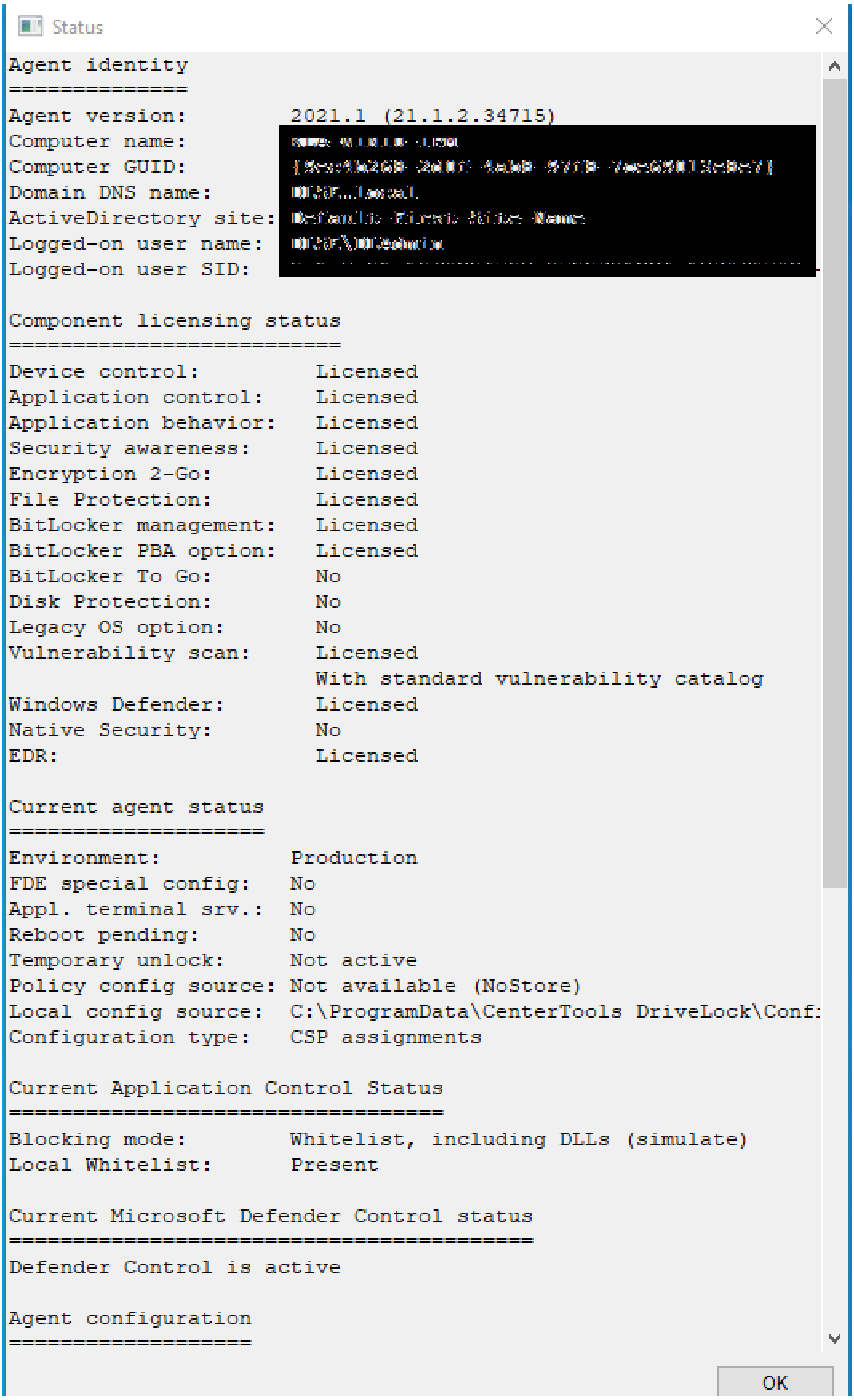
You will receive detailed information about the licenses, configuration and status of the individual components.

2. Via the tray icon on the DriveLock Agent:


Temporarily unlock...
Self service...
Agent status...
DriveLock Encryption 2-Go
DriveLock File Protection
User interface language...
Security Awareness Library...
About DriveLock...
DEU
16:05
02.09.2021

Select **Agent status**....

This opens a new window, where you can also see detailed information in the same way:



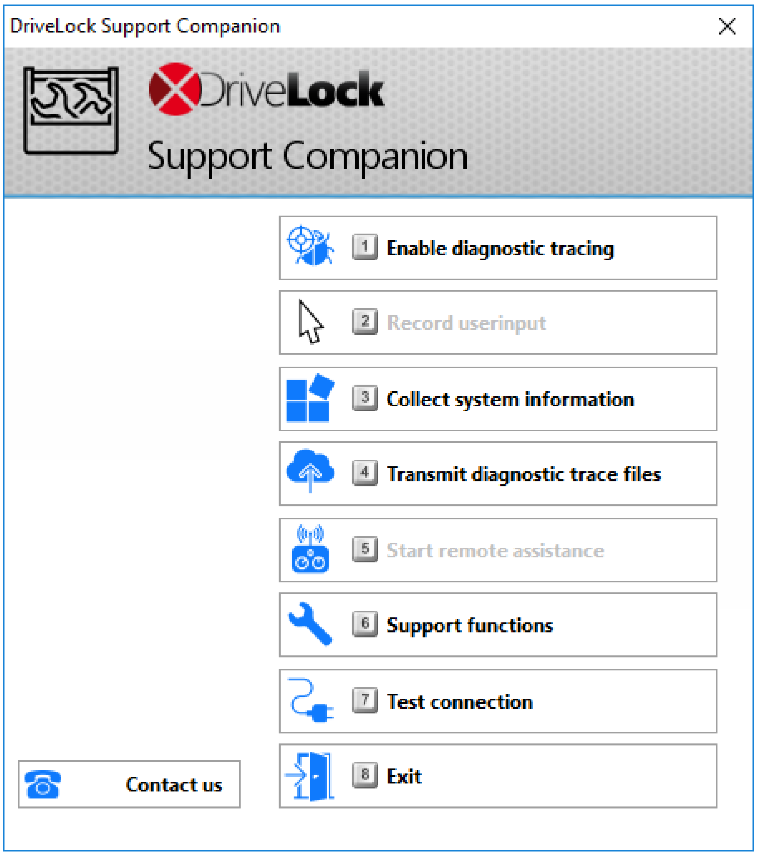
```
Agent identity
==============
Agent version:         2021.1 (21.1.2.34715)
Computer name:         [redacted]
Computer GUID:
Domain DNS name:
ActiveDirectory site:
Logged-on user name:
Logged-on user SID:

Component licensing status
==========================
Device control:          Licensed
Application control:     Licensed
Application behavior:    Licensed
Security awareness:      Licensed
Encryption 2-Go:         Licensed
File Protection:         Licensed
BitLocker management:    Licensed
BitLocker PBA option:    Licensed
BitLocker To Go:         No
Disk Protection:         No
Legacy OS option:        No
Vulnerability scan:      Licensed
                         With standard vulnerability catalog
Windows Defender:        Licensed
Native Security:         No
EDR:                     Licensed

Current agent status
====================
Environment:           Production
FDE special config:    No
Appl. terminal srv.:   No
Reboot pending:        No
Temporary unlock:      Not active
Policy config source: Not available (NoStore)
Local config source:   C:\ProgramData\CenterTools DriveLock\Conf:
Configuration type:    CSP assignments

Current Application Control Status
==================================
Blocking mode:         Whitelist, including DLLs (simulate)
Local Whitelist:       Present

Current Microsoft Defender Control status
=========================================
Defender Control is active

Agent configuration
===================
```

You can select this text and use it via copy & paste.

6.2.2 DriveLock Support Companion

The easiest way to create a trace file is directly at the client by calling one of the following files

- Dlsupport.exe: Installed with the DMC. Includes Teamviewer as a remote maintenance program.
- Dlsupportagent.exe: Installed with the DriveLock Agent. Does not include a remote maintenance program. As a rule, use this file.


DriveLock Support Companion
DriveLock
Support Companion
1 Enable diagnostic tracing
2 Record userinput
3 Collect system information
4 Transmit diagnostic trace files
5 Start remote assistance
6 Support functions
7 Test connection
8 Exit
Contact us

If you select the **Test connection** option, you can check the connection from the DriveLock Agent to the DriveLock Enterprise Service (DES). The DriveLock Connectivity Analyzer analyzes the connection and generates a listing of all important connection parameters (Connectivity Report), for example, the TCP and MQTT connections, remote agent settings or certificate verification. Furthermore, the correct registration and identity of the agent at the DES is verified, provided that the agent has been reinstalled with a jointoken from the DOC.

Copyright