DriveLock Administration

Documentation 2022.1

DriveLock SE 2022

Table of Contents

1 Note on this documentation

As we are in the process of revising and restructuring our entire documentation, you will find a brief introduction to the DriveLock Operations Center (DOC) and information on working with the DriveLock Management Console (DMC) in this document. The Policy Editor chapter is still under revision.

In the (old) DriveLock Administration Guide you can still find chapters on the following topics: Policy settings, Drive and Device Control, Network Profiles, File Protection and information on using DriveLock with Terminal Servers.

We also offer standalone documentation for several topics: Application Control, DriveLock Encryption (includes Disk Protection, BitLocker Management, BitLocker To Go, Encryption 2-Go and DriveLock PBA), Defender Management, DOC Companion, DriveLock Events, Linux Agents, Security Awareness, Self-Service Portal and Vulnerability Scanner.

Furthermore, there is an installation manual and end user documentation.

You can find the complete product documentation at DriveLock Online Help.

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.

3 DriveLock Operations Center (DOC)

The DOC represents a powerful browser-based user interface for the DriveLock Security 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.

With the help of the DOC Companion you can access the Policy Editor, which was only available via the installed DriveLock Management Console prior to version 2021.2. This allows you to edit and create policies, and access settings that are not yet available in DOC.

> Note: For more information, see the separate **DriveLock DOC Companion** documentation at DriveLock Online Help.

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-Prem'

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 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.

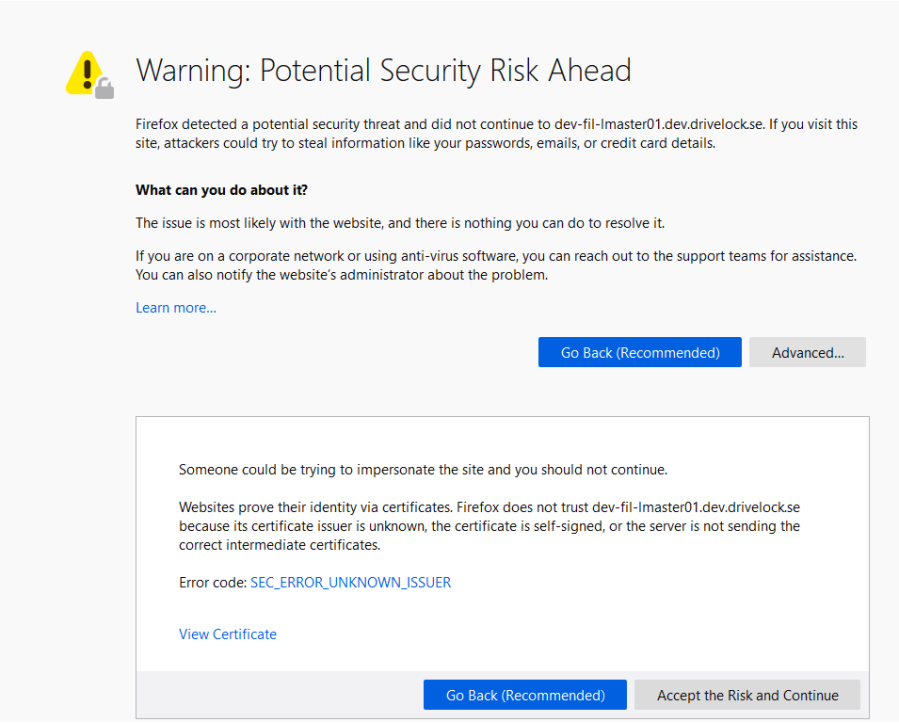
Note: We recommend that you get a certificate for the DES from a recognized certificate authority (CA)!

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:

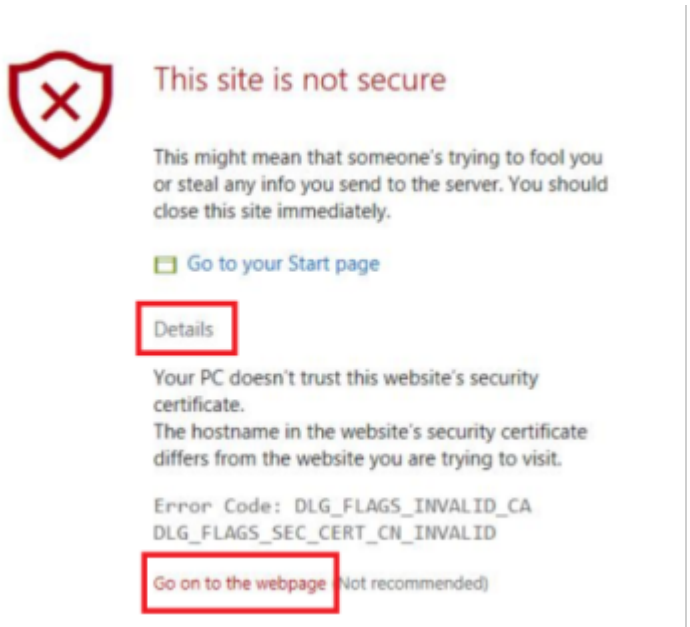
Click **Accept the Risk and Continue** to accept the certificate. There is no need to show the certificate details or to import the certificate. Firefox adds only one security exception for this web page. Nothing else needs to be done.



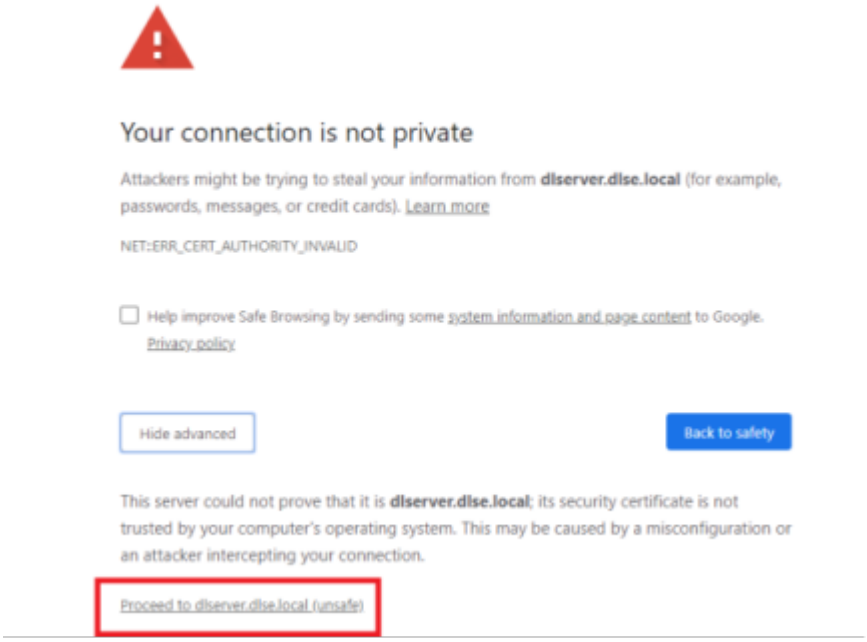
For Google Chrome and Microsoft Edge, the following applies:

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:



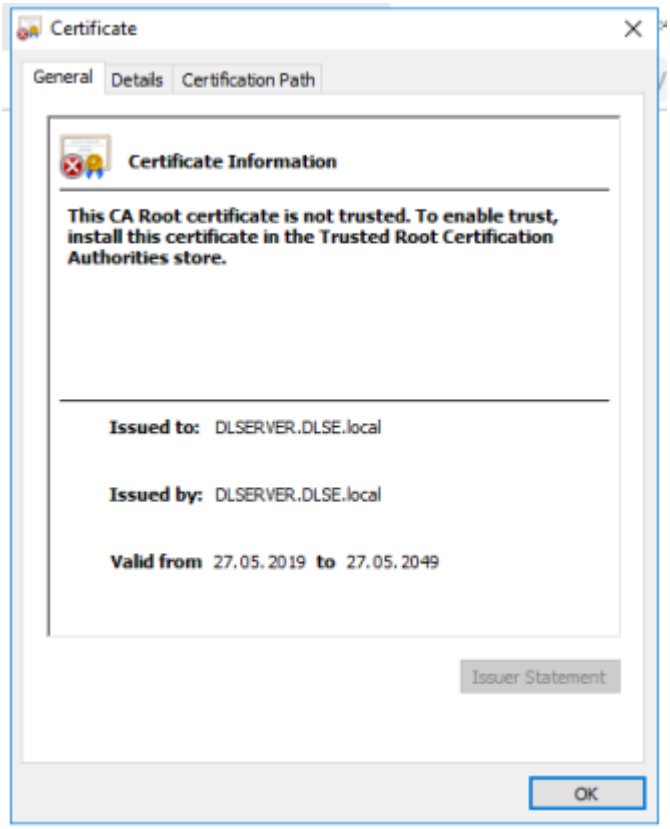
- Google Chrome



3.2.2.1 Importing certificates

Please do the following:

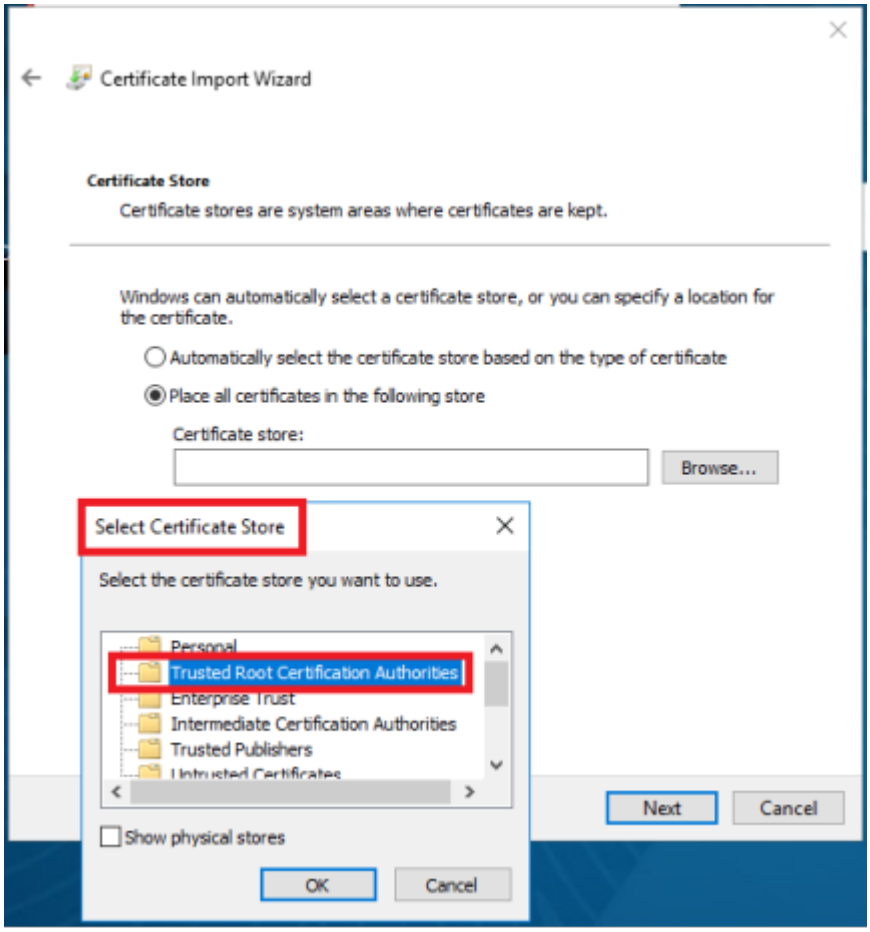
1. For both browsers, accept the warning and open the certificate.
2. You can view the certificate details and import the certificate to the local certificate store using the Certificate Import Wizard.



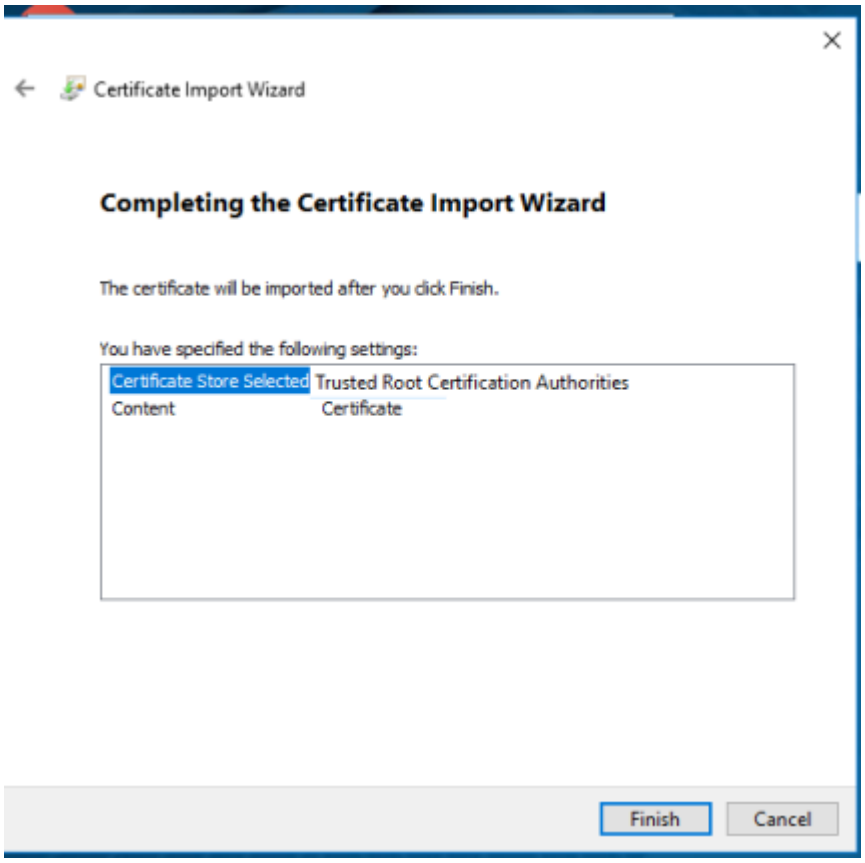
3. Store the certificate in a directory on your computer.
4. Open the certificate's context menu and click **Install Certificate**.

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:

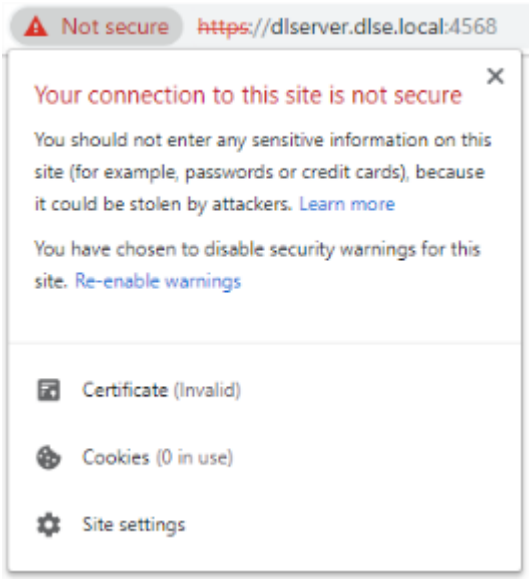


8. In the next dialog, click **Finish**.



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):



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

The Microsoft Azure Active Directory (AAD) integration allows you to access groups and their members, providing a unified management experience via centralized configuration within Azure AD. 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**

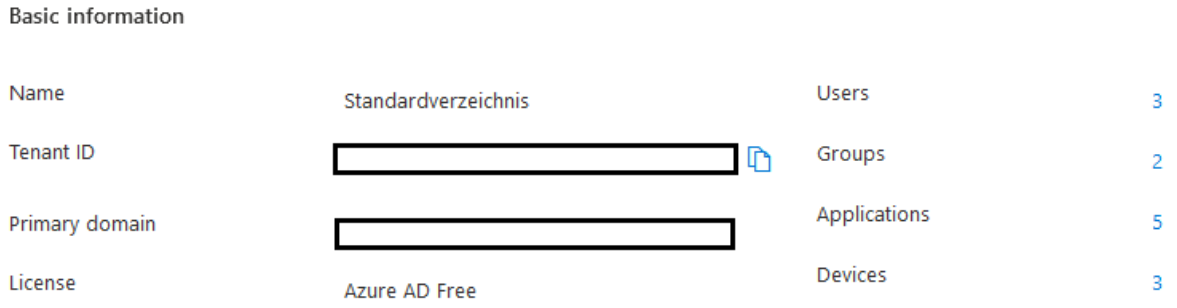
   Azure AD user and computer groups can be used as self-service groups.

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.

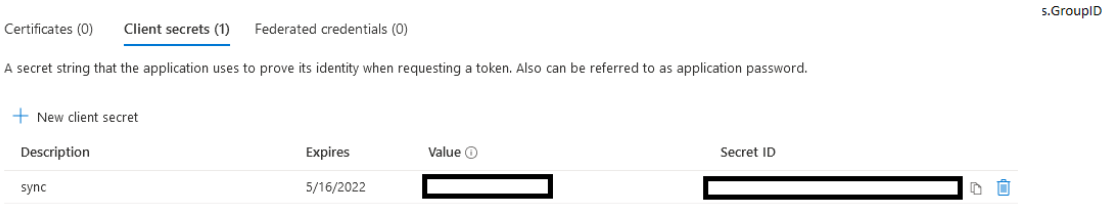


2. **Registering and configuring the application**

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

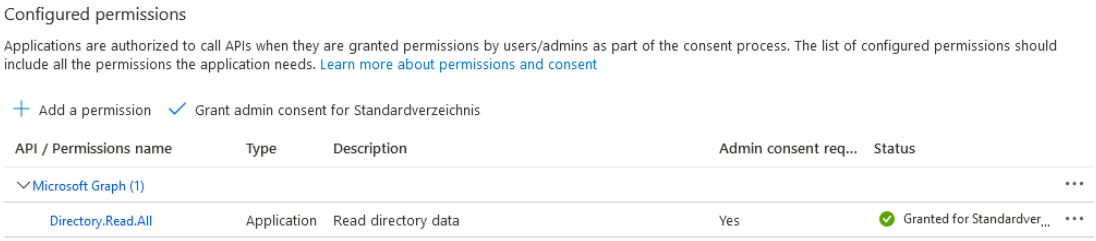
   - **Generating a client secret**

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



   - **Setting permissions**

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



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 Drive and application rules in 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

1. In the **Analysis** menu in the **Events** view:
   Events that provide data about applications can be used as a source for an application rule. Select the **Application control** option in the vertical split of the window to display the events for application control. Select an event and click the **Create rule** menu item. 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 on the **Processes** tab:
   This tab lists processes that can be used in application rules. Select the appropriate process you want to create a rule for (for example, to block it on agents) and click the **Create rule** menu item.
3. All application rules that have already been created are listed in the **Configuration** menu in the **Rules** view. Here you can create a new rule by clicking the **Create applic-**

ation 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 Application Control documentation at DriveLock Online Help.

3.5.1 Creating rules for drives

Please do the following:

1. Once you have selected the **Create rule** option, a wizard appears.
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.

3.5.2 Creating rules for applications

Please do the following:

1. Once you have selected the **Create rule** option, a wizard appears.
2. On the **Properties** tab, 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.

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

3.6 Permissions in 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.

3.7 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.

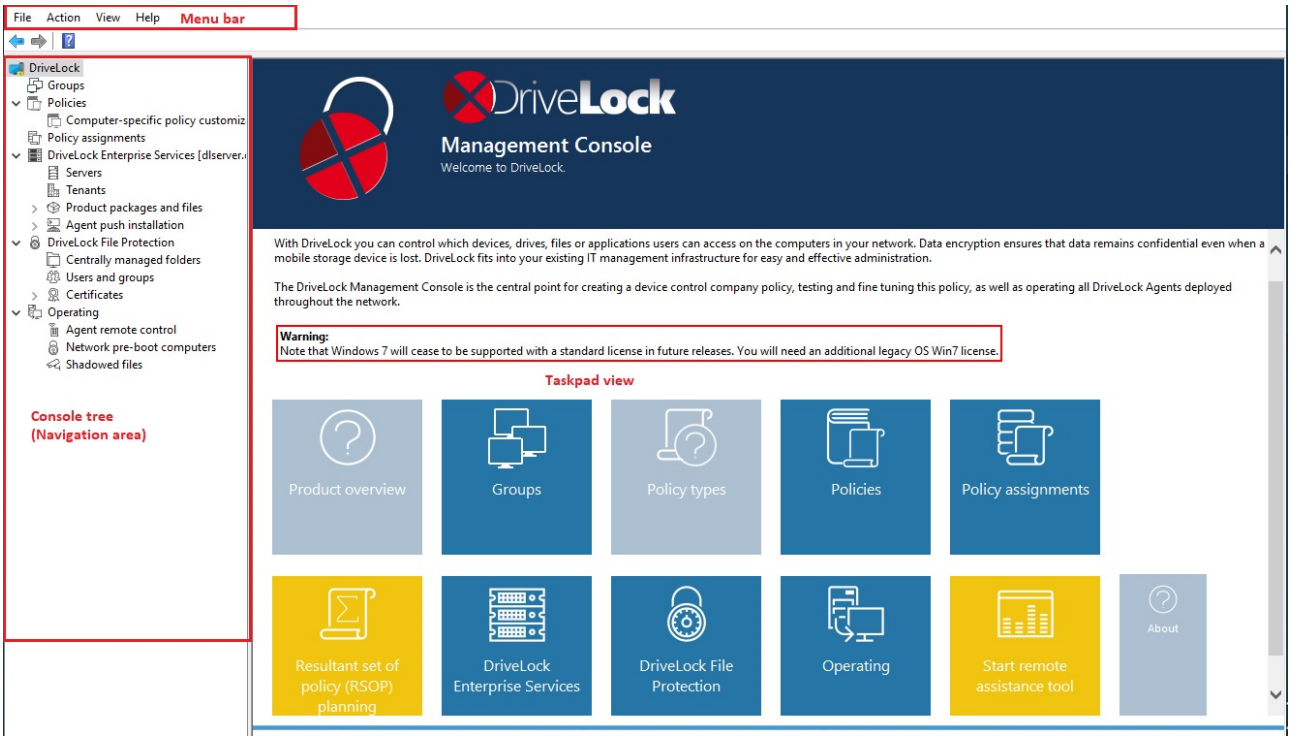
4 DriveLock Management Console

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).

You can perform the major configuration tasks in the DriveLock Management Console (DMC). These are:

- Create DriveLock groups,
- 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**:



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.

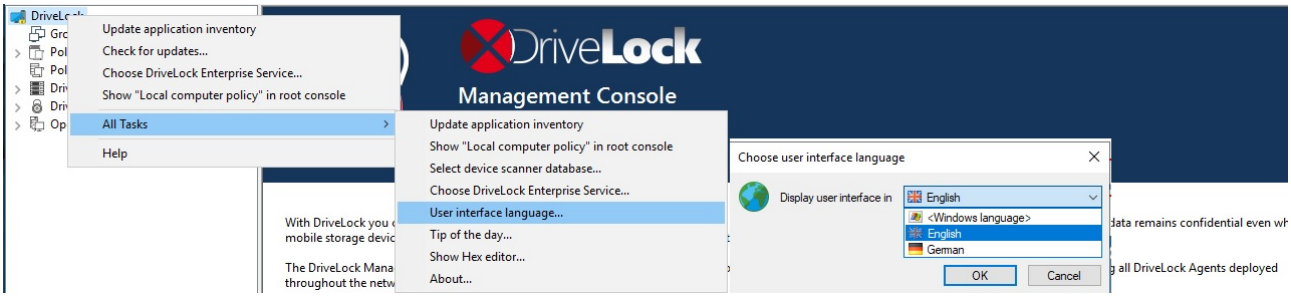
4.1 General notes

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:



4.2 Groups (DMC and DOC)

4.2.1 Creating DriveLock groups

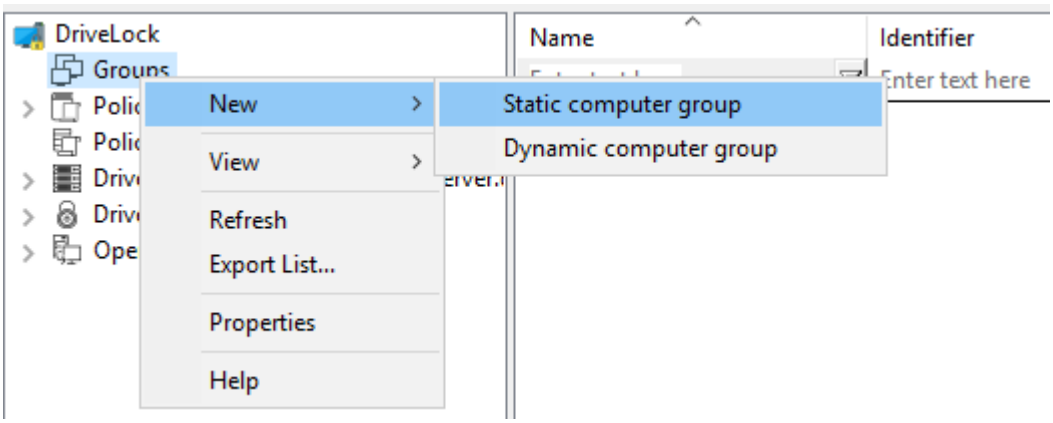
There are two different DriveLock groups:

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).

> Note: To ensure that the group membership is evaluated and reported correctly, please note that DriveLock version 2019.1 and higher (DMC, DES and all DriveLock Agents) is required.

You can create DriveLock groups centrally in the **DriveLock Management Console** from the **Groups** node (see figure):



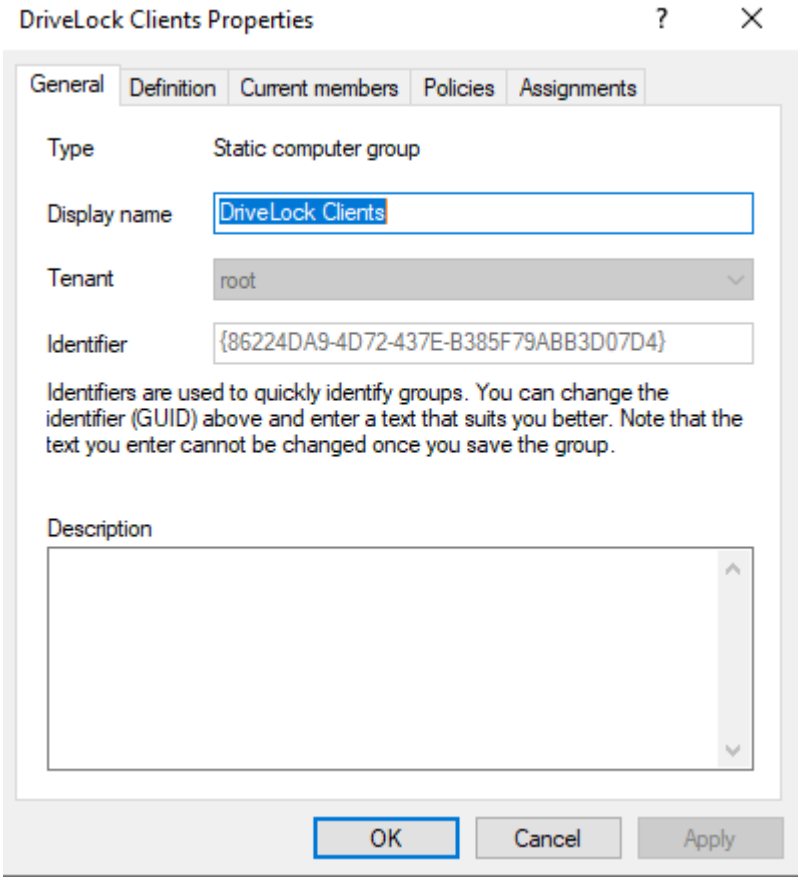
Of course, you can also create and work with static and dynamic DriveLock and Azure AD groups in the **DriveLock Operations Center (DOC)**. Go to the **Groups** view in the **Configuration** menu to create groups by clicking **Add Group**. You can also create a copy of an existing group.

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.

4.2.2 Static computer group

Here's how to create a static computer group in the DMC:

1. In the DriveLock Management Console, open the **Groups** node and select **Static computer group**.
2. On the **General** tab, enter a descriptive name for the group, select the appropriate client, and also add a comment if necessary. In the example below, the static computer group will consist of certain DriveLock clients.

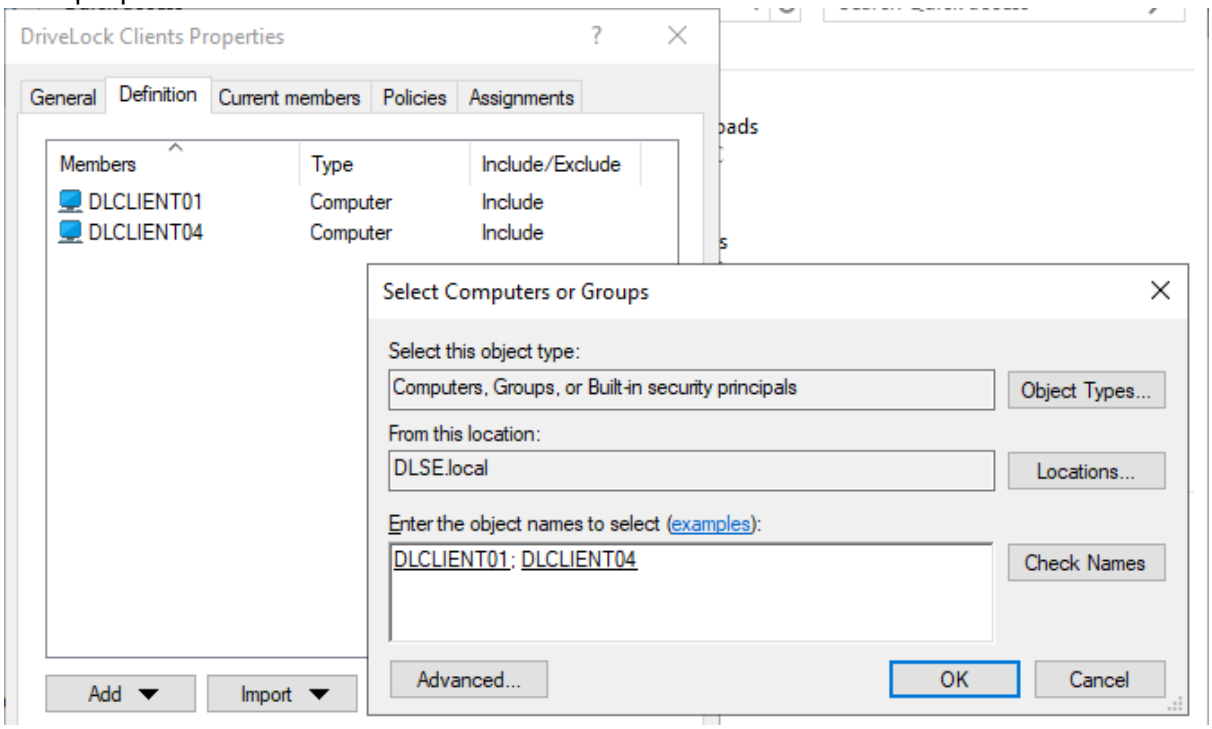


The **Identifier** is automatically inserted as a unique ID. You can rename this when creating the group, this makes it easier to find the group (e.g. in log files).

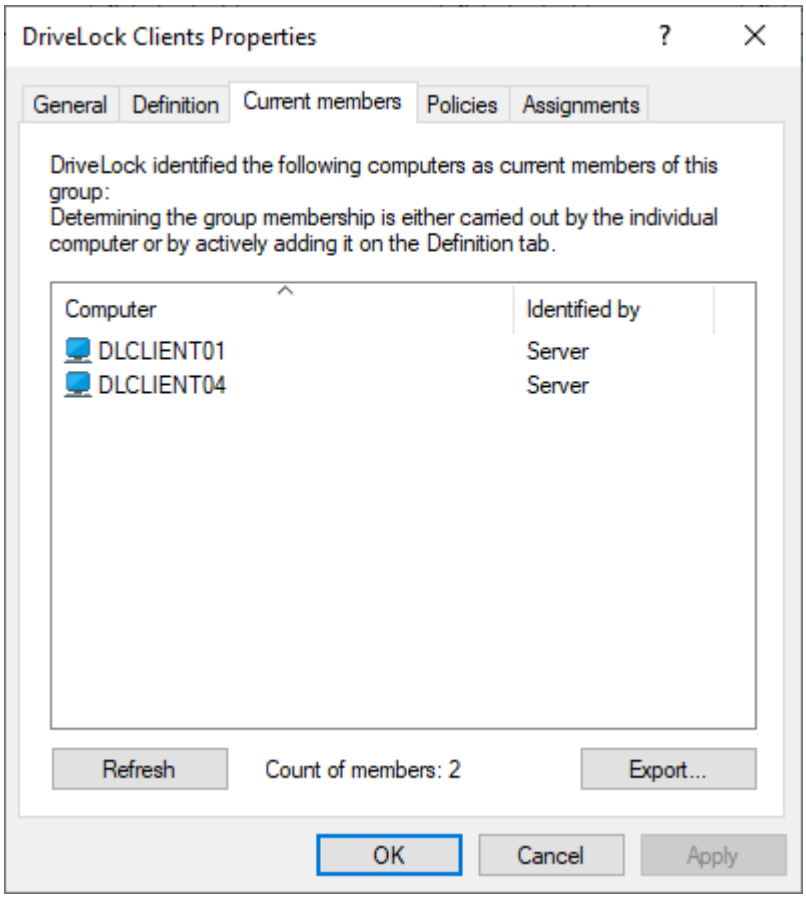
Note: Note that the identifier cannot be changed later!

3. Once you have created the group, it will appear in the DMC. When they open the group again, you will see three new tabs.
4. On the **Definition** tab, you now have the option to add or import computers using the corresponding buttons. In the example, two computers DLCLIENT01 and DLCLIENT04 were added to the static group with the Active Directory Computer or

Group option. You can also work with the Remove and Include or Exclude buttons.



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.

4.2.2.1 Adding static groups

On the **Definition** tab, click the **Add** button.

Here you have the following choices:

- **Active Directory computer or group**: select individual computers or groups directly from AD and add them to your static group.
- **Active Directory Organizational Unit**: Select the computers from an AD OU.
- **Computers by name**: add individual computers by name to the group.
- **DriveLock group**: You can also add a previously created DriveLock group (dynamic or static).

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

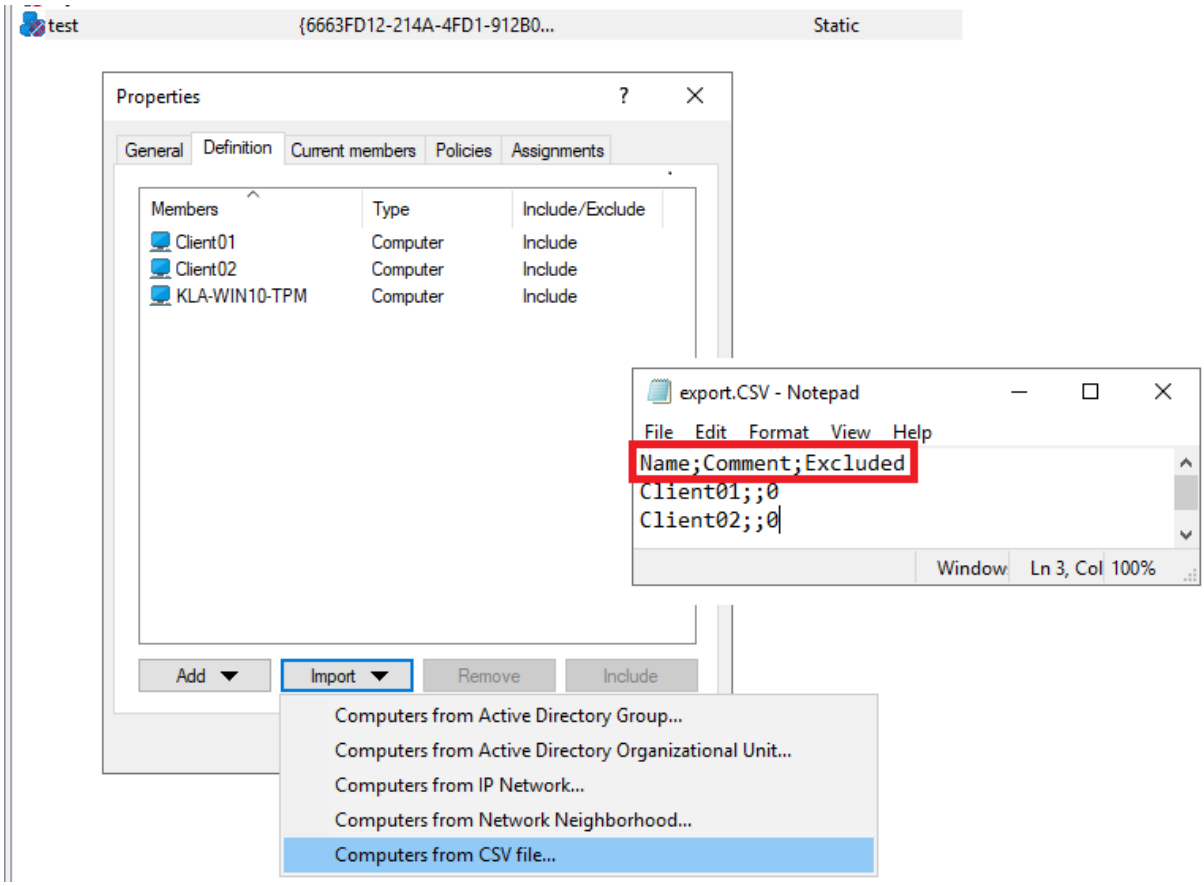
4.2.2.2 Importing static groups

On the **Definition** tab, click the **Import** button.

Here you have the following choices to import individual computers from different sources into your static group:

- **Computers from Active Directory group**: import the computers from the selected AD group directly into your static group.
- **Computers from Active Directory Organizational Unit**: select the corresponding AD OU from which you want to import the computers.
- **Computers from IP network**: Specify here a particular IP range where the computers you want to import are located.
- **Computers from Network Neighborhood**: Select the computers from the direct network neighborhood as members.
- **Computers from CSV file**: Select here the CSV file in which the computers to be added to the static group are listed.

Note: Note here that the CSV file has the format `Name;Comment;Excluded`, see the figure.

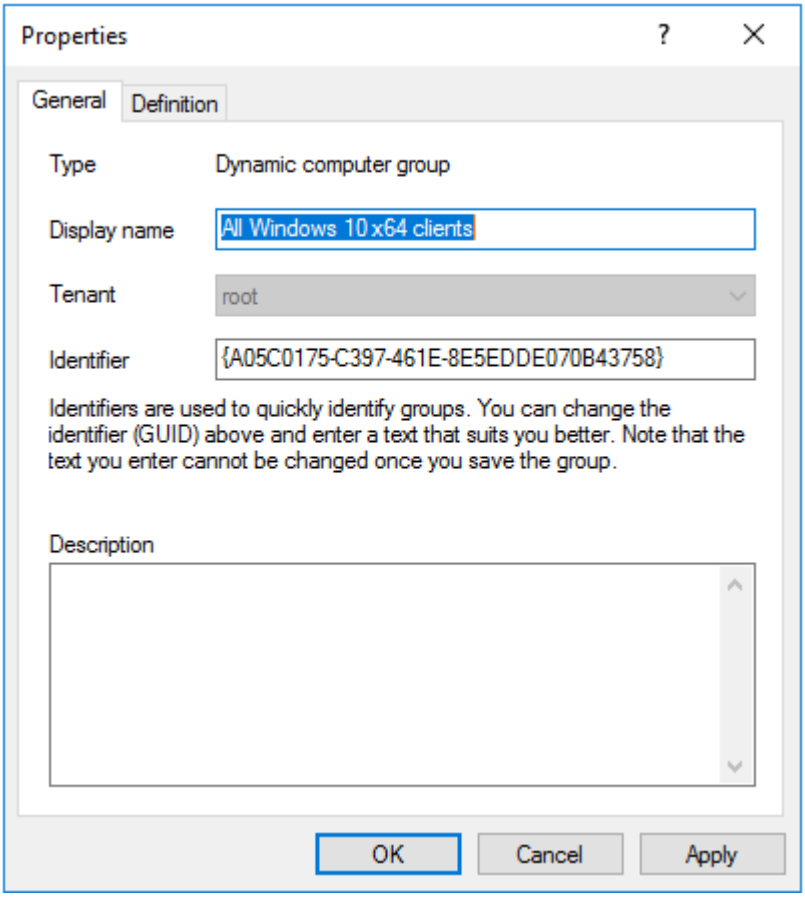


The members of static groups can also be exported to a CSV file. On the **Current members** tab, click the **Export**... button and then save the CSV file.

4.2.3 Dynamic computer group

Here's how to create a dynamic computer group in the DMC:

1. Select **Dynamic computer group**.
2. On the **General** tab, enter a descriptive name for the group, select the appropriate client, and also add a comment if necessary.
   The example below shows that the group is supposed to include client computers with Windows version 10 operating system and x64 architecture.



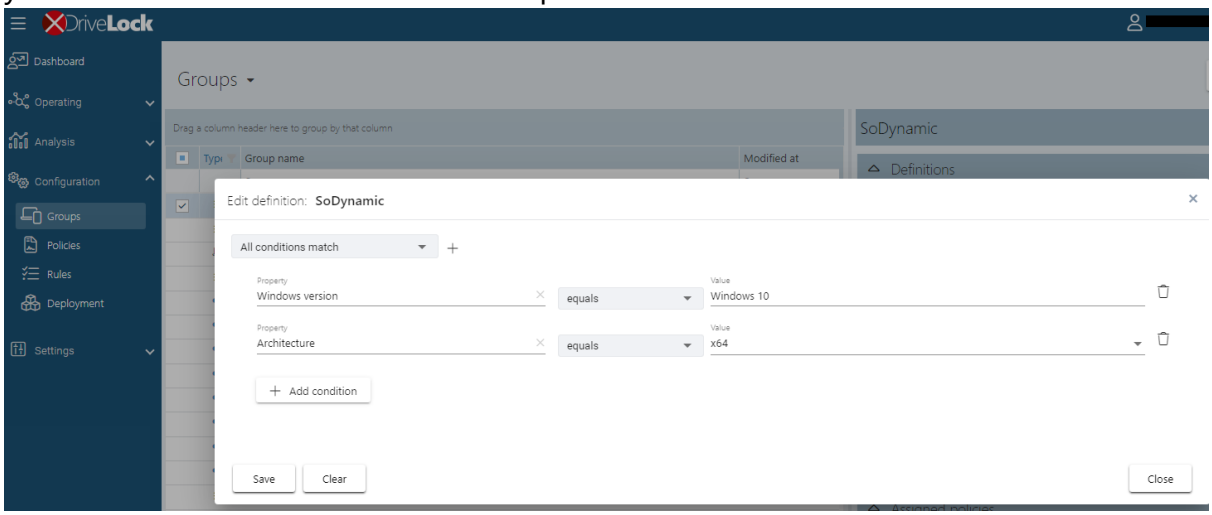
   The **Identifier** is automatically inserted as a unique ID. You can rename this when creating the group, this makes it easier to find the group (e.g. in log files).

> Note: Note that the identifier cannot be changed later!

3. You can no longer specify any details on the **Definition** tab.

   Please configure these settings in the **DriveLock Operations Center (DOC)**.

To do so, open the **Groups** view in the **Configuration** menu. Use the **Edit definition** menu command to select appropriate filter criteria for your dynamic 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.



4. Click OK to create your dynamic group. Now you can use the created dynamic group in policy configuration and assignment.
5. The properties of the dynamic group now also include the Current members, Policies and Assignments tabs.

4.2.3.1 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 All computers from a specific depart-

Filter criterion	Available from DriveLock version	Type	Value, name, example
			ment (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 state	2022.1	Enum	Active, Inactive, Partially active

Filter criterion	Available from DriveLock version	Type	Value, name, example
Distinguished name	2022.1	String	CN=PC01,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 version	2022.1	String	

Filter criterion	Available from DriveLock version	Type	Value, name, example
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

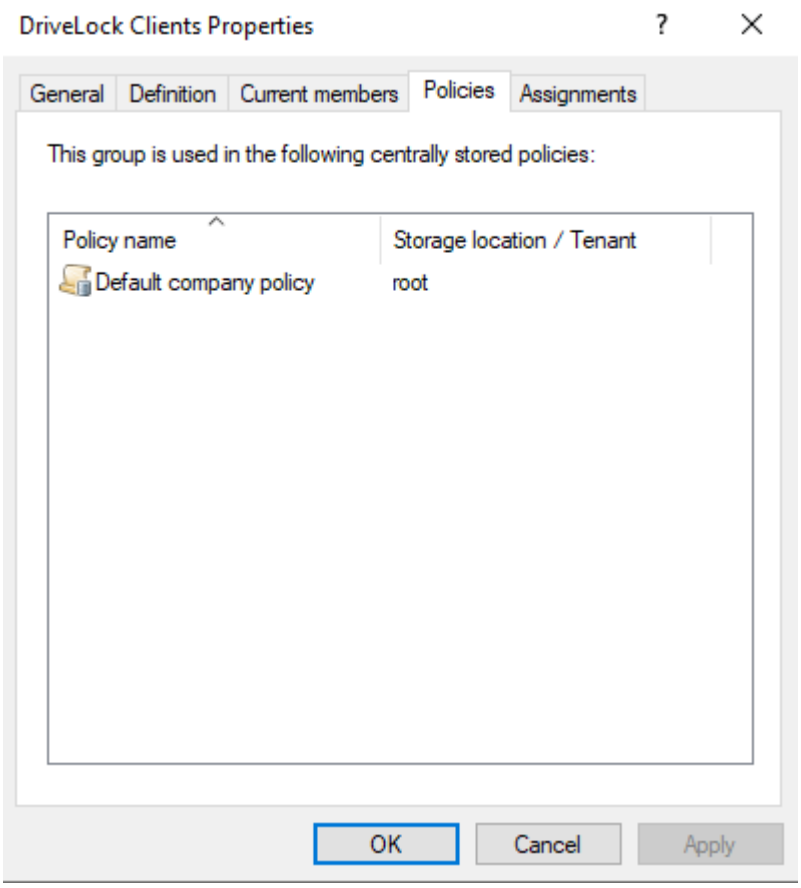
4.2.4 Using groups in policies

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: In order to use groups in policies, you have to define them first. We do not provide any default DriveLock groups which you can use out of the box.

After defining your DriveLock group, it will appear on the **Policies** tab to show you where it is being used.

In the example below, the properties dialog for the DriveLock Clients group (see example in Creating static computer groups) shows the policy where the group is being used (here the Default company policy).



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 only temporarily disconnected (offline) from the DES will be updated with the current policies (and group settings) the next time they connect.

4.3 Policies

4.3.1 Deploying DriveLock configuration settings

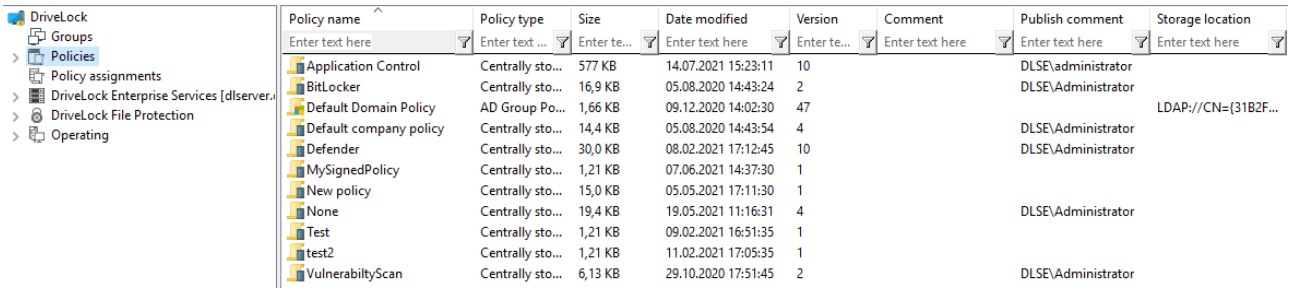
There are several ways to distribute configuration settings to clients. The steps to configure settings are identical in all types of policies. You can configure the same parameters, whitelist rules, or network settings.

The following configuration matrix provides an overview to help you determine which configuration type is best for you:

	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

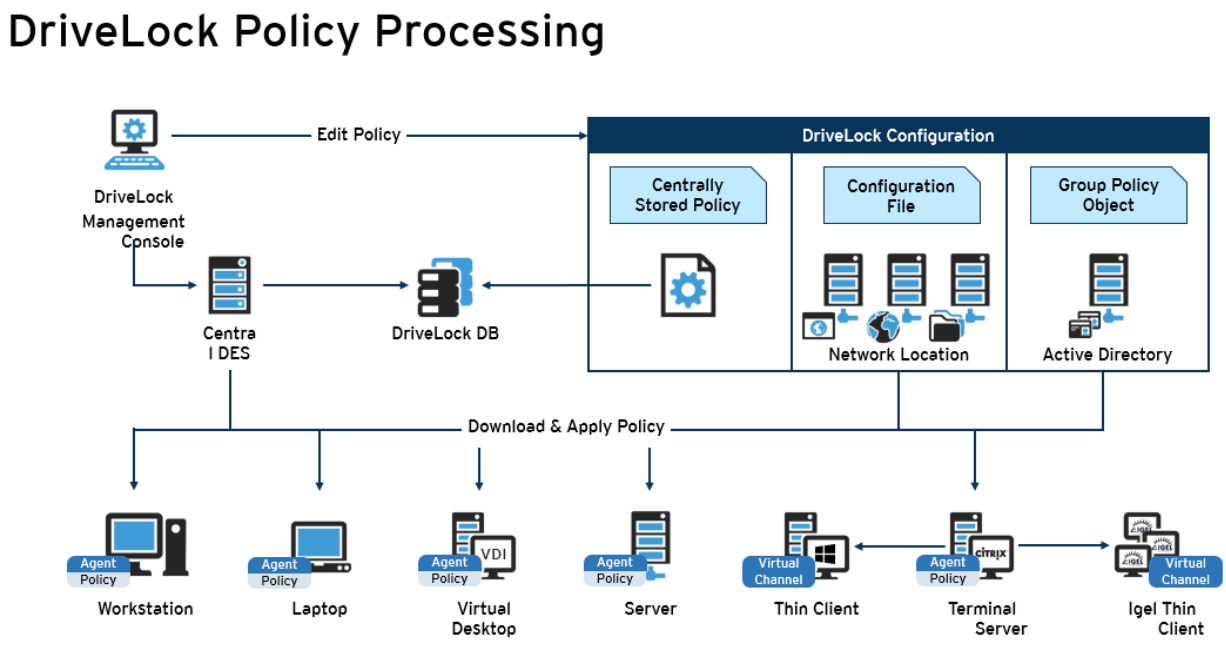
Warning: Before distributing settings to multiple clients on the network, we recommend that you first test them on one or more test clients.

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



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.

4.3.2 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 applic-

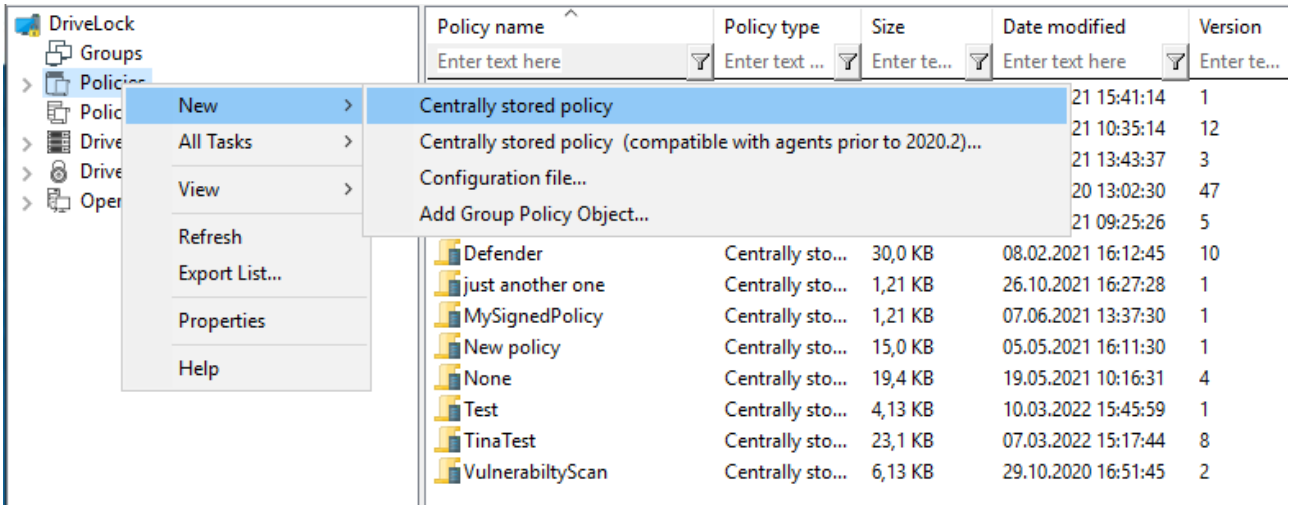
Order, policy name	Assigned to	Description
		ations for servers

4.3.2.1 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 (compatible with agents prior to 2020.2)...**. These agents cannot yet handle the new policy format.



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)

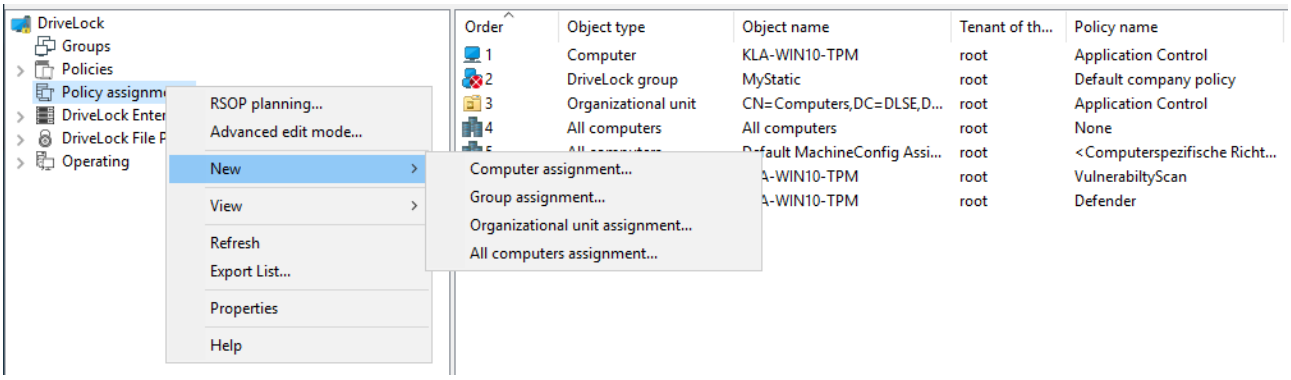
In the **Configuration** menu, open the **Policies** view. Click the **Create policy** button. Then the DOC Companion starts, if it is not already running. Then the Policy Editor opens and you can edit, save, publish, and then assign the policy directly in the DOC. For more information, see the separate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

4.3.2.2 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.

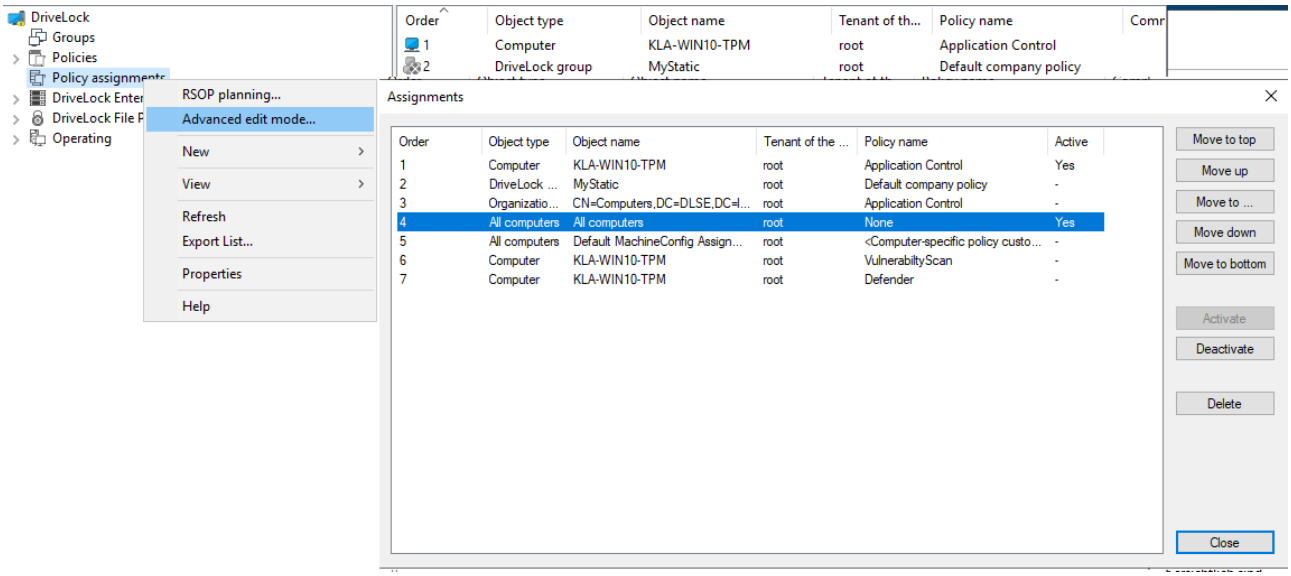
Note: Before using static and dynamic DriveLock groups in policy assignments, you need to have defined them first. When the DriveLock group has been successfully applied to a policy, it appears on the Policy assignments tab of the group properties.



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.



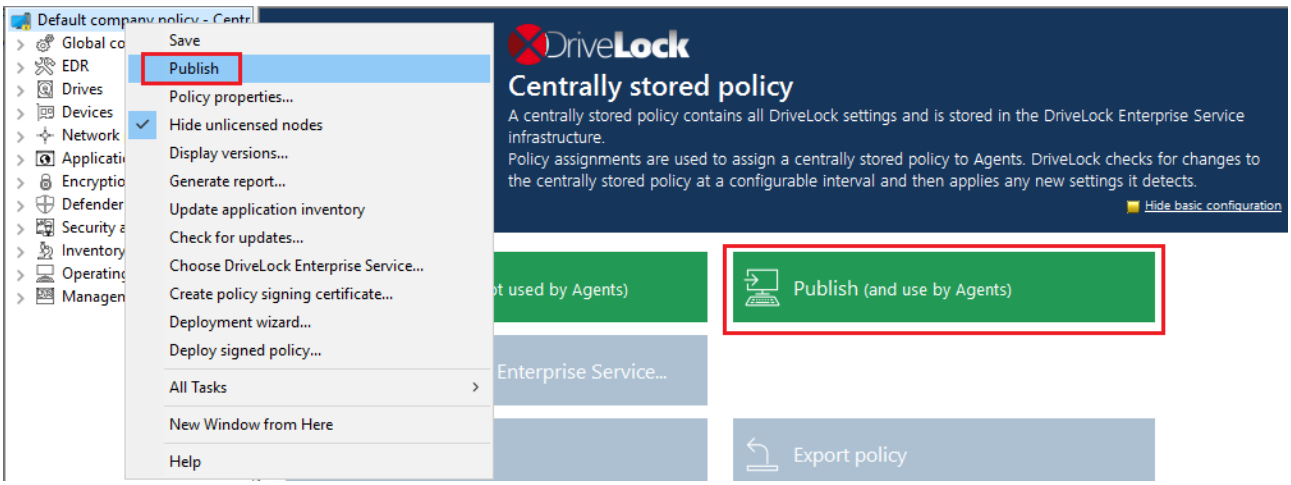
In the DriveLock Operations Center (DOC)

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.

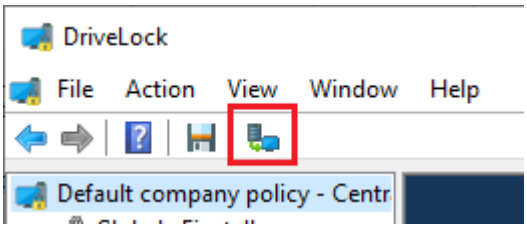
Also in DOC, you have the option to assign a policy to all computers (this option is enabled by default) or to specific targets (AD computers, DriveLock groups, Azure AD groups, AD groups or OU containers).

4.3.2.3 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:



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.

4.3.3 Group policy object

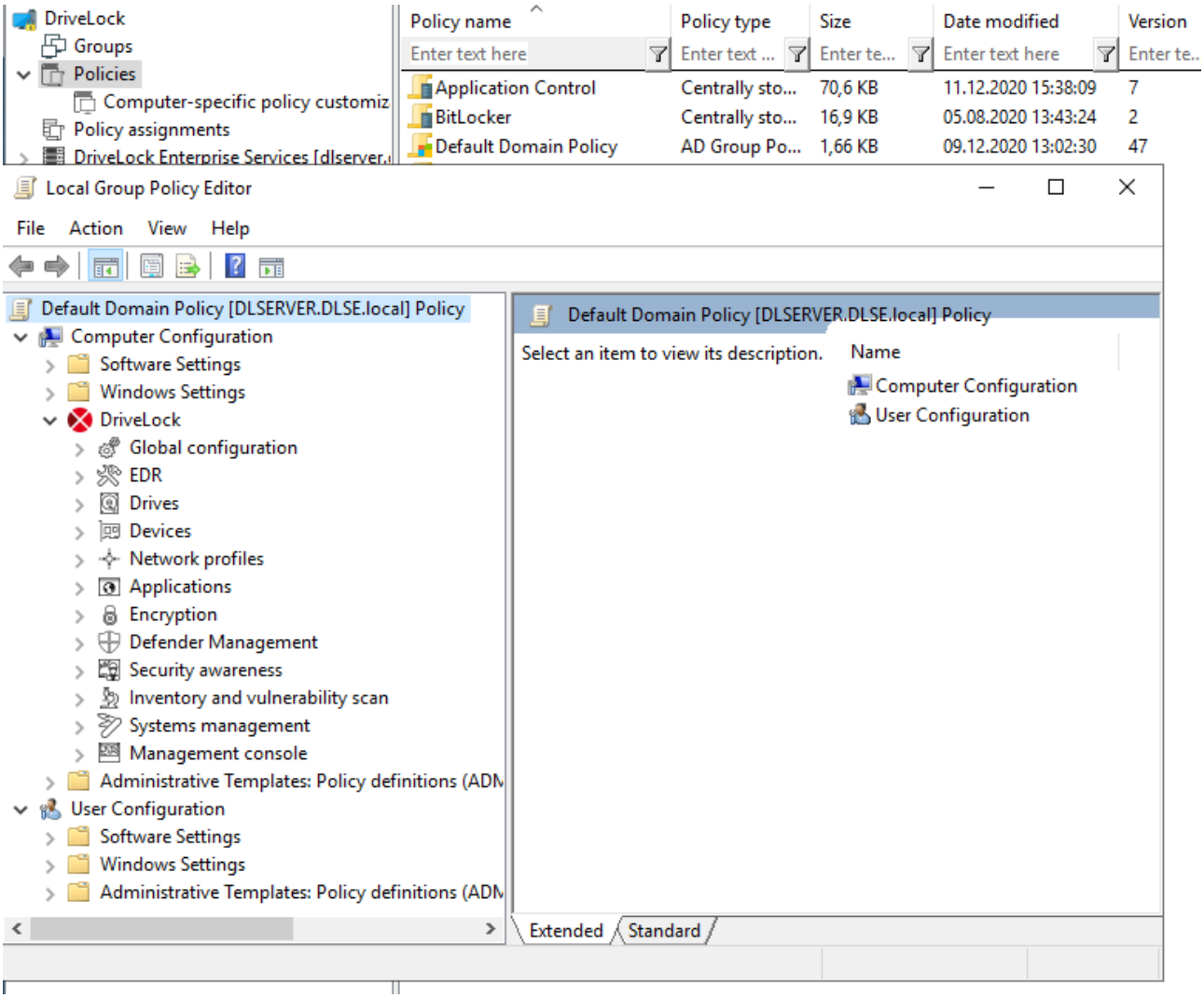
Another way of configuring the DriveLock Agent on multiple computers in a network is by using an Active Directory Group Policy. DriveLock can be configured by using the Group Policy Object Editor in conjunction with the DriveLock Management Console (MMC) snap-in. This snap-in is automatically installed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



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`

4.3.4 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).

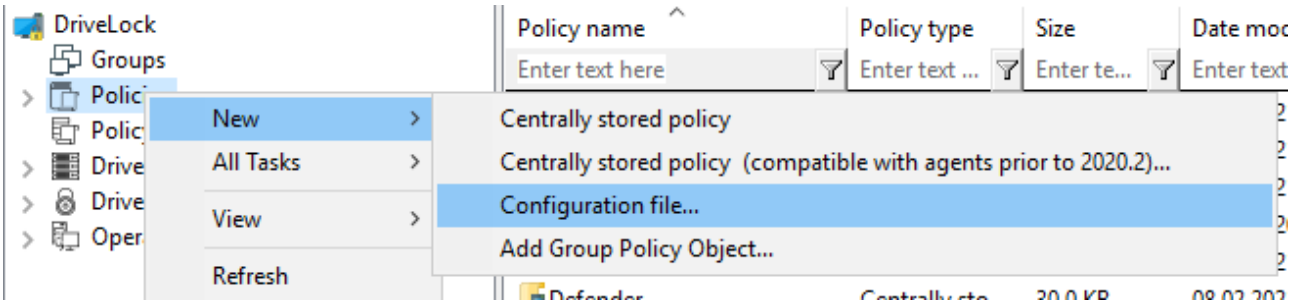
In system environments without Active Directory or a DriveLock Enterprise Service, DriveLock settings can be distributed using a configuration file. This file can be accessed on a central network drive using a UNC path or via HTTP/FTP.

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.

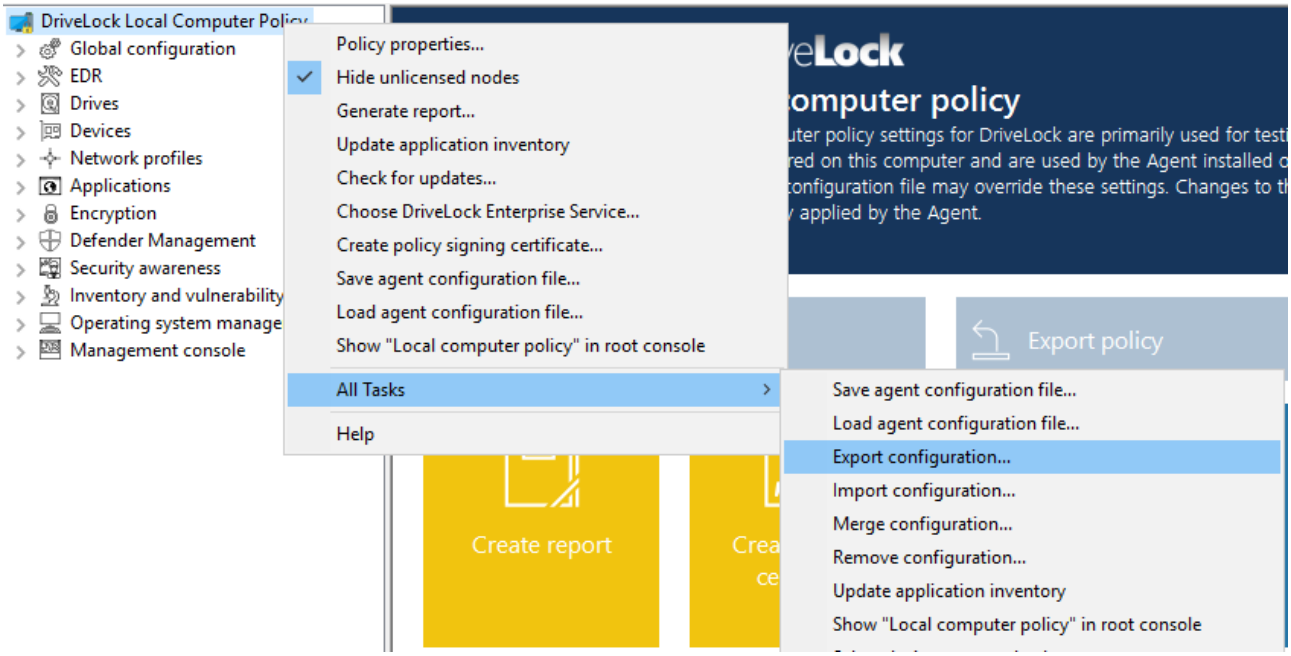
When installing the DriveLock Agent, you must include the information from where the agent should load its configuration. The easiest way to accomplish this is by using the Deployment wizard. Open this wizard by right-clicking **Policies**, then **All Tasks** and then **Deploy configuration file...**.

4.3.5 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.

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.



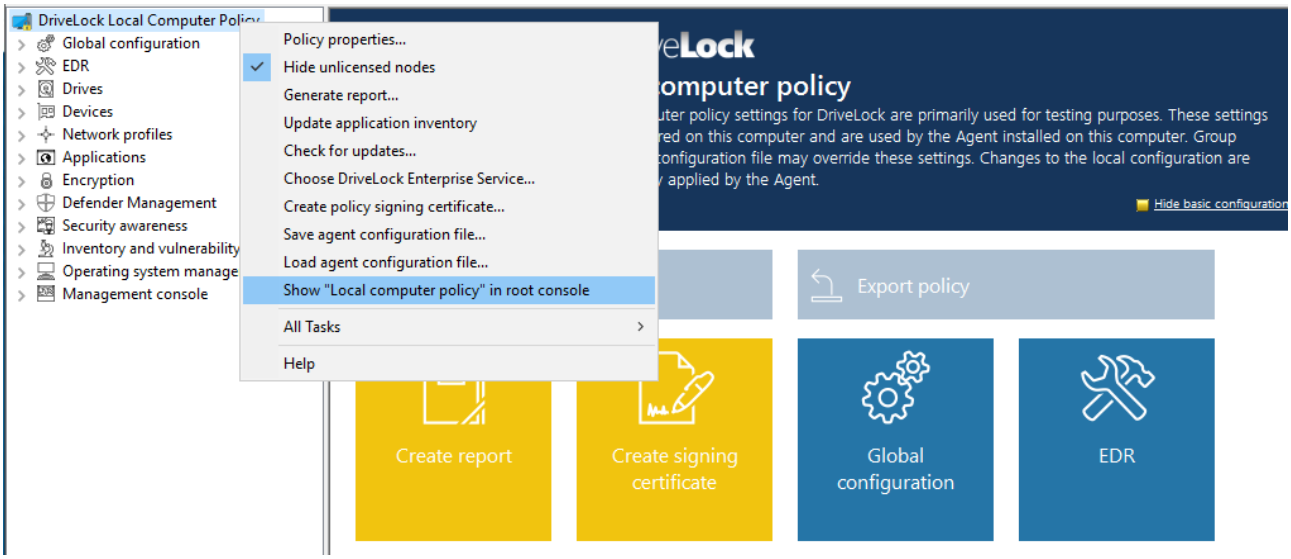
Note: You can also import a local configuration if, for example, you have previously exported a policy from a group policy and then imported it into a local DriveLock configuration.

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.

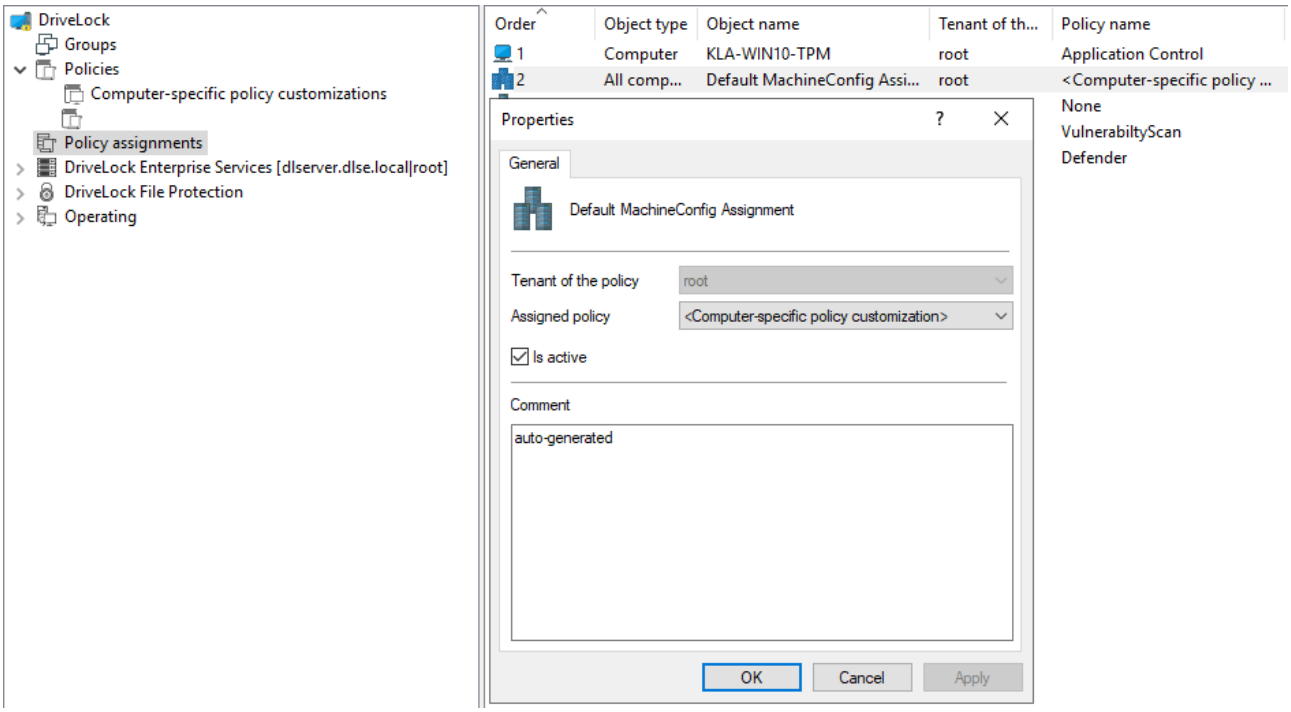
Remove configuration: Use this command to delete an existing DriveLock configuration (local or in group policies).

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.



4.3.6 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.



- 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.

4.3.7 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.

4.4 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.

4.4.1 RSoP planning

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

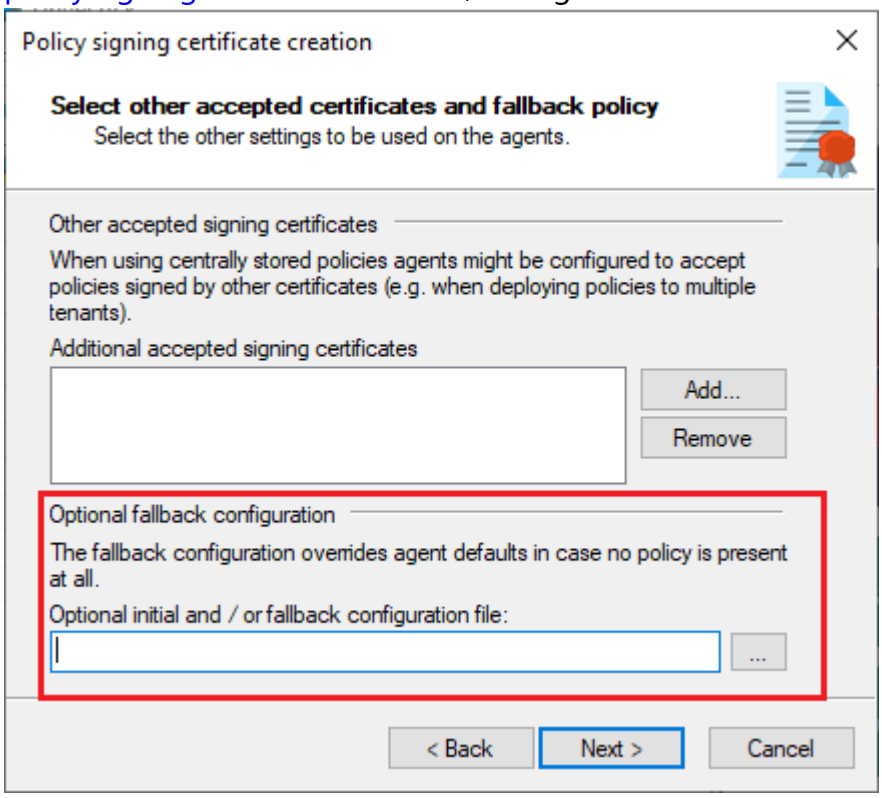
In the DriveLock Management Console (DMC)

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

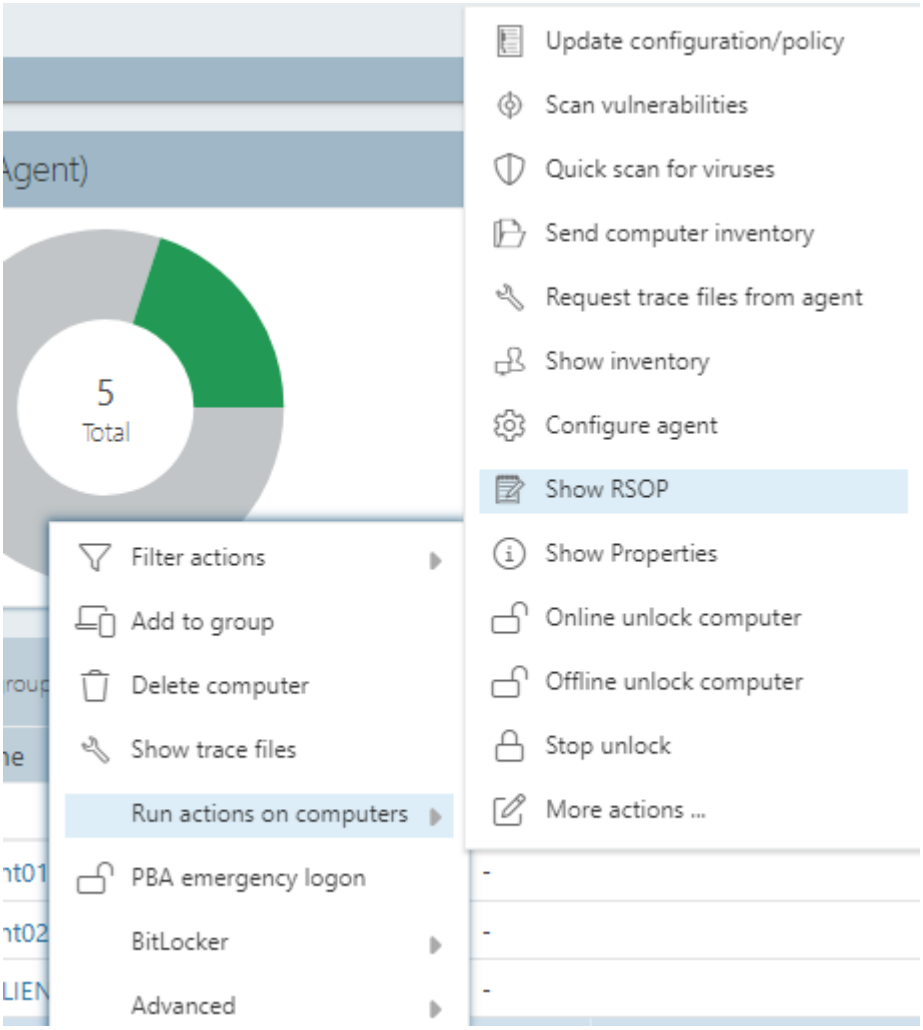
policy signing certificate creation, see figure:



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:


Update configuration/policy
Scan vulnerabilities
Quick scan for viruses
Send computer inventory
Request trace files from agent
Show inventory
Configure agent
Show RSOP
Show Properties
Online unlock computer
Offline unlock computer
Stop unlock
More actions ...
Filter actions
Add to group
Delete computer
Show trace files
Run actions on computers
PBA emergency logon
BitLocker
Advanced
5
Total

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.

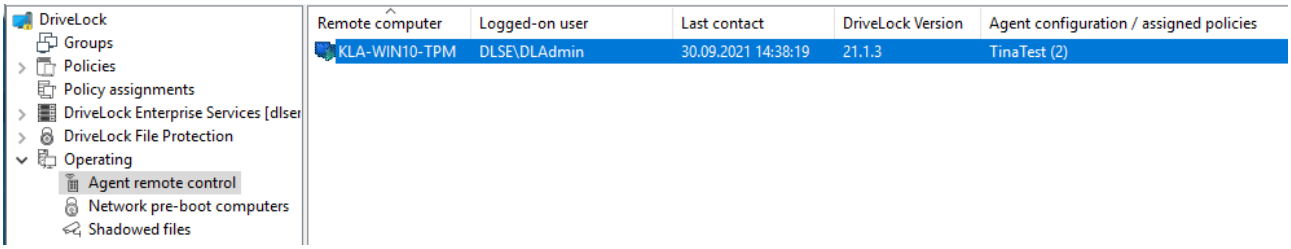
The **Use remote control trough DriveLock Enterprise Service (proxy)...** options control the behavior of the DriveLock Management Console when connecting to a DriveLock Agent via remote agent control:

- **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).

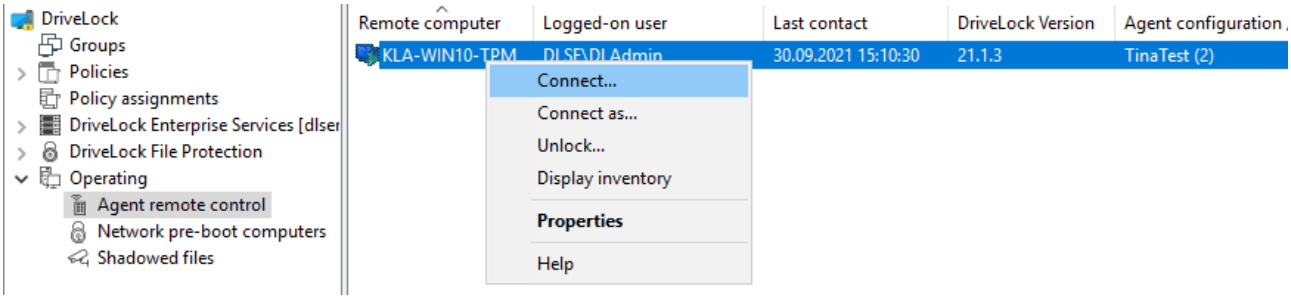
4.5.1.2 Show active DriveLock Agents

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.



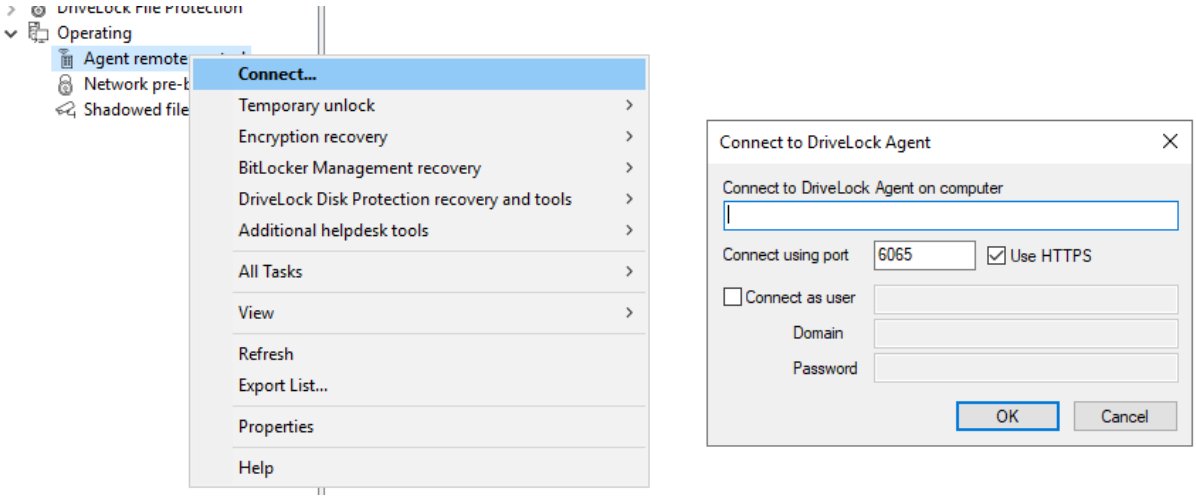
4.5.1.3 Connect to a DriveLock Agent

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:



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.



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 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.

4.5.1.6 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.

4.5.1.7 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.

4.5.1.8 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 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.

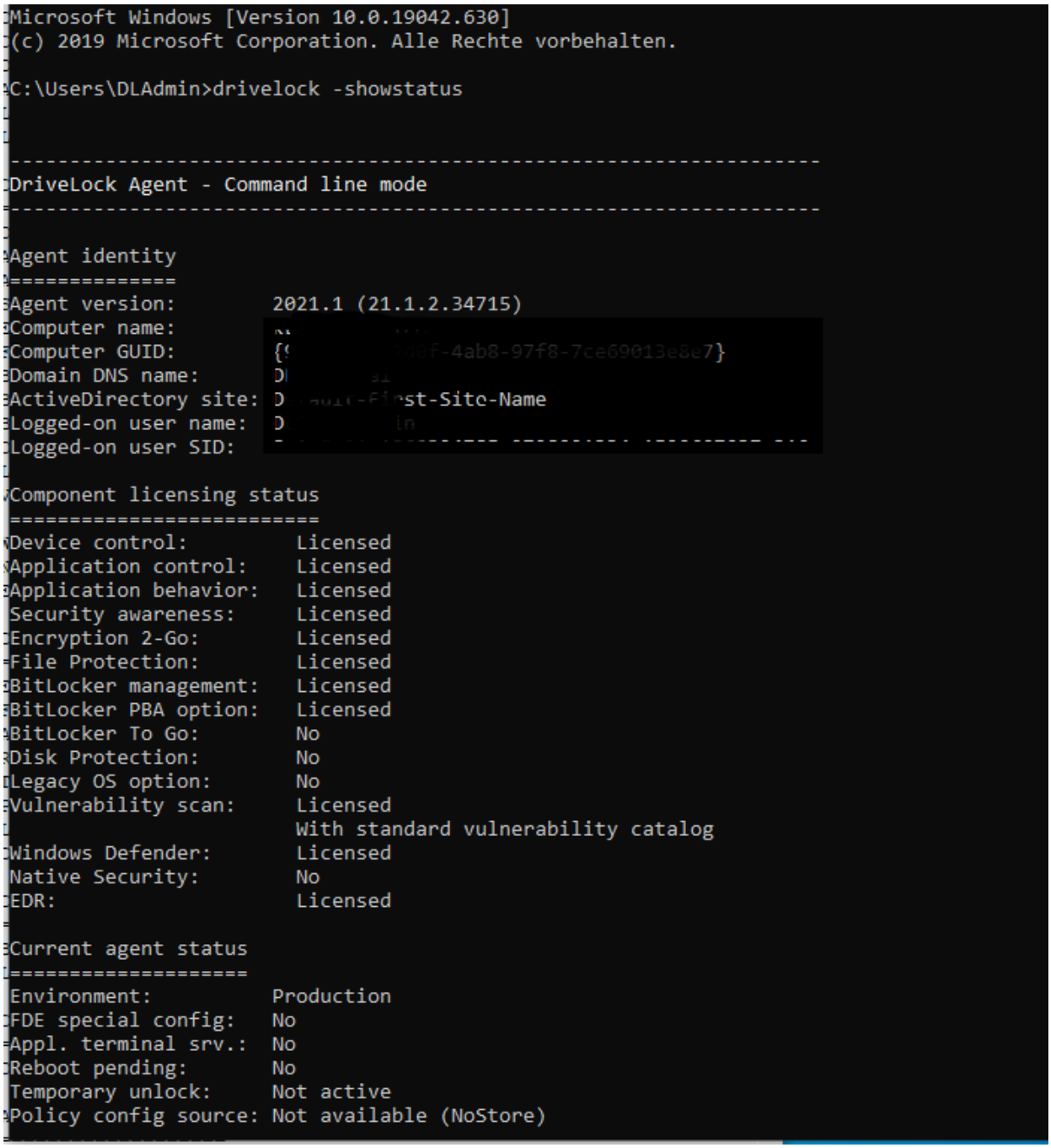
Note: For more information on troubleshooting, see Knowledge Base articles KBA00106: Collecting and Submitting Diagnostic Data from DriveLock Agent - Trace (DriveLock Support Companion) and KBA00422: Collecting Diagnostic Information. If you need more information, please contact DriveLock Support.

5.1 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:

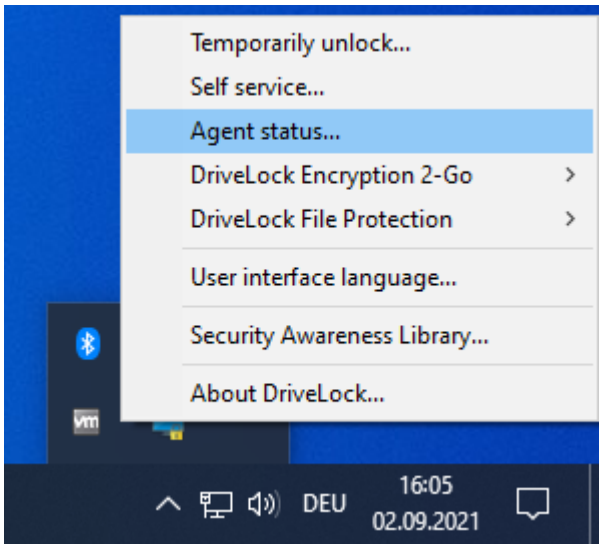
1. **Command line command**

   Open a command line window and type `drivelock -showstatus`:



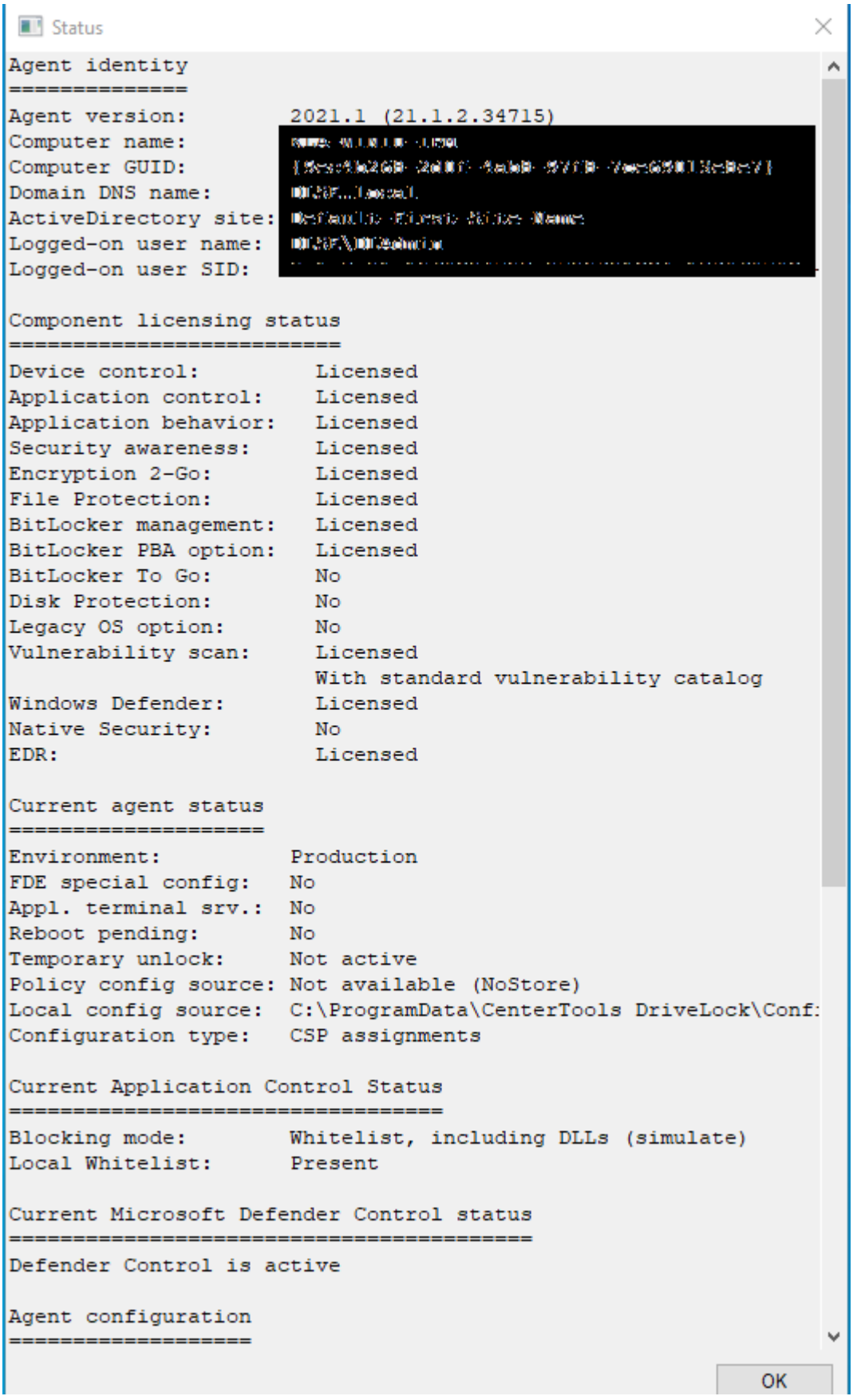
You will receive detailed information about the licenses, configuration and status of the individual components.

2. Via the tray icon on the DriveLock Agent:



Select **Agent status**....

This opens a new window, where you can also see detailed information in the same way:

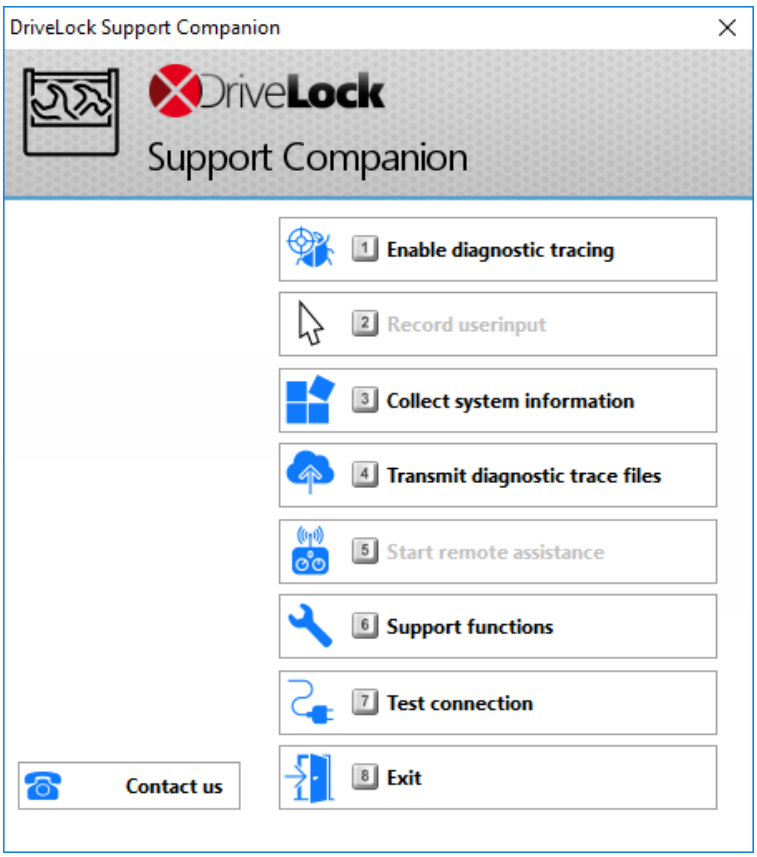


You can select this text and use it via copy & paste.

5.2 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.



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 join token from the DOC.

Copyright