DriveLock Documentation

DriveLock Product Documentation 2024.2

DriveLock SE 2025

Table of Contents

1 Welcome to DriveLock

The DriveLock HYPERSECURE platform is designed to protect you against cyberattacks of all kinds and to prevent the loss of valuable data. In this documentation, you can find out how to use DriveLock's Security Controls and how they work.

> Note: For information on the new features in the current version, click here.

DriveLock offers two solutions: the cloud-based Managed Services and the local on-premise version. Managed Security Services offers hosting of the complete DriveLock solution in the cloud and scores with significant advantages in terms of security, cost efficiency, scalability and management by our security experts. The on-premises solution is the locally installed standard version and can offer customized control for your company.

Please follow the links for an overview of the DriveLock infrastructure in the cloud or 'On-Premise'.

Depending on which solution you are using in your company, different information is relevant for you. For example, the Installation section is particularly important for DriveLock 'On-Premise', as you install and manage DriveLock in your own infrastructure.

> Note: Additional information is available on request for customers of DriveLock Managed Security Services.

The information on the DriveLock features is valid for both solutions. Click the links to go directly to the subject area you are interested in:

- Application Control,

- Device Control,

- DriveLock Encryption with the features Disk Protection, File Protection, BitLocker Management, BitLocker To Go, Encryption 2-Go and DriveLock PBA,

- Defender Management,

- Security Awareness and

- Vulnerability Management.

Information on using DriveLock on client computers with Linux or mac operating systems can be found here:

- Linux Agents

- macOS Agents

2 What's new in version 2024.2?

Please find the new features and bug fixes in the current patch version at DriveLock Online Help.

> ⊘ Warning: Please note that some issues may cause a change in product behavior when you install the update. Before updating, make sure to check your settings to see if your existing environment is affected. The issues are labeled with the ⚠ icon.

Please find the bug fixes in version 2024.2 in the release notes at DriveLock Online Help.

The major version 2024.2 contains the following new features and general improvements.

Device Control

- End users can send unlock requests for composite and MTP devices.

- Administrators can configure drive classes in the DOC.

- CSVs exported from the DMC can now be imported into device or drive rules in the DOC. In addition, these CSVs can now be exported in the DMC not only from device or drive collections, but also directly from a list of simple device or drive rules.

- Drives can now be managed in remote sessions on non-terminal servers.

- Accepting the usage policy and using the self-service unlock now both work with user names in UNC format (Name@Domain).

- Archive scanning can now be done across encrypted containers and SMB shares

- Hardware information is displayed in event columns

- Simulation mode can be enabled for individual device classes

- Defender scans may be temporarily deactivated during remote unlock

- Content scanner event: For blocked files, the file header (beginning of the file content) can be attached to the event that reports a failed content scan. This data can be used to customize the content review.

⚠ **New system groups and modified group evaluation**

- DriveLock now introduces system groups that automatically include all computers or all users.
  In addition, the evaluation of groups has been adapted (applies to both computer or user groups):

Behavior before 2024.2: If all groups used in a group were excluded, all computers that were not in the excluded groups were members of the group.
Example: You had a 'Servers' group that contained all servers. You want to create a computer group 'Workstations' that contains all computers in your company except the servers. To do so, you added the 'Server' group as an exclusion in this group.
New behavior from 2024.2: If all groups in a group are only exclusions, this is no longer interpreted as 'all except'. This means that all other computers are no longer automatically members.
In the above-mentioned *example*, you must include the 'All computers' group in the 'Workstations' group and exclude the 'Servers' group.
To maintain the previous result for existing groups, the All computers or All users group is automatically added to the groups to which this behavior change applies during the update.
Note on creating new groups: If you want to create a new group that contains all computers that are not included in certain groups, you must now explicitly add the All computers group to achieve the desired result.

macOS

- You are now able to encrypt USB drives on macOS with Encryption 2-Go

- DriveLock Notifier for macOS: The new menu bar app "DriveLock Notifier" provides quick access to encryption and recovery.

- The macOS agent now supports the Windows hardware ID from the parent USB device, numeric USB IDs for vendor, product and revision, as well as Windows rules for vendor, product and revision names (all optionally with S/N) for blocking drives.

- The macOS agent can be distributed via MDM

Linux

- Device Control on Linux now supports vendor and product information on Linux.

- Devices the Linux agent cannot assign to any other device class can now be controlled via the new device class "Unknown Linux device" in the policy

- Devices the Linux agent cannot assign to a device class can now be controlled via user-defined device classes with a configured USB class property

- AlmaLinux is supported as a new Linux distribution on endpoints

Application Control

- You can now manage Application Behavior Control rules in the DOC

- Enhanced display and added settings for managing Application Control rules in the DOC.

- Filter for file size in application control rules.

- More detailed information on the file is now supplied for event 596 (file added to local whitelist). Application control rules can now also be created from this event.

- Simplified process analysis with process tree in DOC.

BitLocker Management

- Automatically encrypt devices during provisioning with TPM.

DriveLock Operations Center (DOC)

- The DriveLock Operations Center now has a dark mode in addition to the familiar light mode. You can find the corresponding setting via the menu item "Customize appearance" in the user settings.

- It is now possible to specify for every list view whether you want the total number of entries to be determined and displayed.

- The display mode of any string field via the context menu can now be changed between single-line and multi-line.

- In the event view, there are new filter options for the affected objects (application, hardware ID, drive ID). The view must be reset to default in order to display the columns.

- The export to Excel has been replaced by the export in CSV format. This allows you to specify both the amount of data to be exported and the format.

- The column selection and the setting for displaying the total number of entries can now be saved for each list view in both the Detail View and the Object View.

- Evaluate, distribute, and modify licenses, and create license policies

- Evaluate licenses on a tenant basis for managed service environments

General improvements and changes

- Platform API extensions: Endpoints and groups can be managed via API.

- Automatic deletion of inactive computers: The settings for deleting inactive computers automatically have been extended and there is now also an option to protect

computers from being deleted automatically.

- Centrally manage encrypted folders

- Integrate risk assessments and training with Human Risk Assessment & Security Awareness

- The login screen behavior for DriveLock PBA is aligned with Windows

- Use the new DriveLock Server Installation Wizard for database installation and server certificate management (replacing the older tools Database Install Wizard.exe and ChangeDesCert.exe)

- Allow the DriveLock Enterprise Service to use a group-managed service account (gMSA) as a login account.

System requirements update

- For the DriveLock Enterprise Service, in addition to .NET Framework 4.8, a.NET Core 8.0 Runtime is required.

3 Installing DriveLock On-Premise

If you are running DriveLock on-premises, you need to install the DriveLock management components on your server and the DriveLock Agent on the client computers in your network.

As an alternative to installing and setting up your environment on your own, DriveLock also offers a comprehensive security solution through our cloud-based Managed Security Service. The service includes hosting the entire solution, managing it with security experts, and tailoring security standards to individual requirements.

> Note: Please note that there is additional documentation available for Managed Security Service customers.

3.1 Before installing the DriveLock Enterprise Service (DES)

We recommend the following preparatory steps before you start installing DriveLock.

Necessary preparations:

- Create an account used to run the DriveLock Enterprise Service (DES). This account does not need to have administrator rights.

- To install the DES you need at least a Windows Server 2012 R2

- The DES requires Microsoft SQL Server 2016 SP1 or newer. If this is not available, you can also use the SQL Server Express version that is provided for installations with up to 200 clients and test installations.

  > Note: Click here for more information on updating older SQL Server versions.

Optional:

1. If you have your own certificate authority, create a server certificate for client-server authentication.
   Specifications of the SSL certificate used for DES:
   - Signature algorithm: sha256SA

   - Public key length: RSA 2048/4096 bit

- Advanced use:
    - Server authentication (1.3.6.1.5.7.3.1)
    - Client authentication (1.3.6.1.5.7.3.2)
- Key usage: Digital Signature, Key Encipherment
- We recommend that the certificate has a friendly name. The private key must be exportable if the certificate is to be used by all DriveLock components.
- DNS alias: if a DNS alias is used for the DES server, the certificate must also be issued for this DNS alias
- The certificate needs to be installed in the Local Computer – Personal store before the DriveLock installation
  Further information can be found in the Trusted certificates chapter.

  > ⚠ Warning: DriveLock does not support wildcard certificates for the DES.

2. If you do not want to use the Microsoft SQL Express Server supplied (for small environments and test environments), you will need a Microsoft SQL Server (see above).

3. If the user installing the DES does not have the necessary permissions on the database server, the database administrator should make the following preparations:
   - Create a Microsoft SQL Server database for DriveLock
   - The login used during installation requires only the **public** SQL Server role and must be a member of the **db_owner** role in the DriveLock database.

4. If you want multiple users to be responsible for DriveLock administration, it is useful to create an AD group for the users that will have administrative permissions for DriveLock.

> 📝 Note: Further information on these topics can be found in the current release notes on DriveLock Online Help.

3.2 Preparations for installing the database

> 📝 Note: If you want to change database settings at a later date, you can do so in the DOC at *Settings* ⚙ *-> Backend -> Server settings or Database & event data maintenance*. For more information, please refer to the technical articles "Database Guide" and "Database Migration" on DriveLock Online Help.

The following accounts are involved in the installation:

- The DES service account is the Windows account used to run the DES service. This is specified during installation and gains access to the database through the installation.

- The Windows account that installs the DES and has local administrator rights. This is usually the logged-in user who performs the installation.

- By default, the account used to access the database is the same account that performs the installation. However, you can specify a different Windows or SQL Server authentication in the installation wizard.

Permissions for the database installation

The account used to access the database during installation requires the following privileges:

SQL server roles:

- **dbcreator**: needed to create the database

- **securityadmin**: needed to create the login for the DES service account

Alternatives for enterprise environments:

- A SQL Server administrator can arrange for creating the database and the login for the DES service account. The login used during installation requires only the **public** SQL Server role and must be a member of the **db_owner** role in the DriveLock database.

- During the installation, you can choose whether to create the database or use a prepared database. You can also specify whether to create the login for the DES service account or not. This will allow customizing the required permissions on the SQL Server for the installation login.

- Future updates will only require membership in the **db_owner** role of the DriveLock database for the installation login.

Permissions of the DES service account on the database

For operation, the DES service account requires the following role memberships in the DriveLock database:

- **db_datareader**: Read data

- **db_datawriter**: Write data

- **srcsystem**: custom role installed by DriveLock, allows to run stored procedures and use custom table types.

For database maintenance (index maintenance), backups and deletion of old data, the DES service account additionally requires role membership for **db_owner**. This is optional and recommended for operation with SQL Server Express, where no SQL jobs can be created for these tasks. During installation it is possible to select whether the DES service account gets this permission.

3.2.1 Procedures according to database environment type

Overview of the different database installation scenarios by environment type:

	Scenario 1: Small environments	Scenario 2: Large environments	Scenario 3: Enterprise environments
Database server	SQL Express	Microsoft SQL Server	Microsoft SQL Server
Create the database manually	no	no	yes
Required permissions	SQL Express and DES are installed during the DriveLock setup (DLSetup.exe). The user account executing the installation will be the administrator of the SQL Express database.	Login to SQL Server with the roles **dbcreator** and **securityadmin**	The login used during installation requires only the **public** SQL Server role and must be a member of the **db_owner** role in the DriveLock database.
Required options for database installation:			
Create database	yes	yes	no
Create database	yes	yes	no

login			
Make DES service account the owner of the database	yes	no	no
Database maintenance, data cleansing and backups	via DES	set up via SQL Server	set up via SQL Server

> Note: Click here for more information or go to the DriveLock Database Guide in the Technical Articles at DriveLock Online Help.

3.3 Installing the DES and the DriveLock Management Console (DMC)

The installation wizard supports you with installing the DriveLock components. Proceed as follows:

1. Run the **DLSetup.exe** file from the ISO image.

2. Choose your language and accept the DriveLock EULA.

3. Select the following components:
   - DriveLock Management Console (DMC)

     > Note: We recommend that you also install the DMC on the server. However, you can also install these separately on individual client computers if, for example, different employees are to work with the management components on these computers.

   - Enterprise Service
     Optionally, you can install a Microsoft MS SQL Express Server as a database server.
     Beyond 200 devices (enterprise environment), a fully featured SQL Server is recommended.

     > Note: DriveLock supports Microsoft SQL Server and Microsoft SQL Server Express as database systems. The exact specifications can be found in the current release notes on DriveLock Online Help.

4. The next dialog will show you the selected components.

The following options are available:

- The **Do not download updated files- use locally stored files only** option allows you to install the versions stored in the current directory.

- If you do not want to install the previously selected components immediately but only download them over the Internet, you can select the **Download files only - do not install** option.

5. Now click **Next** to start the download or installation. In the last dialog you get a listing of the successfully installed components.

6. Next, the wizard which helps you install the DriveLock Enterprise Service appears. It is only available in English.

3.3.1 Installing the server

Please do the following:

1. In the welcome dialog, click **Next** and then confirm the End User License Agreement (EULA) in the following dialog.

2. Now indicate the role your new DriveLock Enterprise Service (DES) will take. Select the **DES** option to create a central DES.

> ☑ Note: The first DES you create must always be a central DES.

You can select the **Linked DES** option if your infrastructure is already set up with a central DES and you want to register or add a linked DES. In this case, no database needs to be created.
Please note that in the vast majority of cases it is not necessary to create a linked DES!
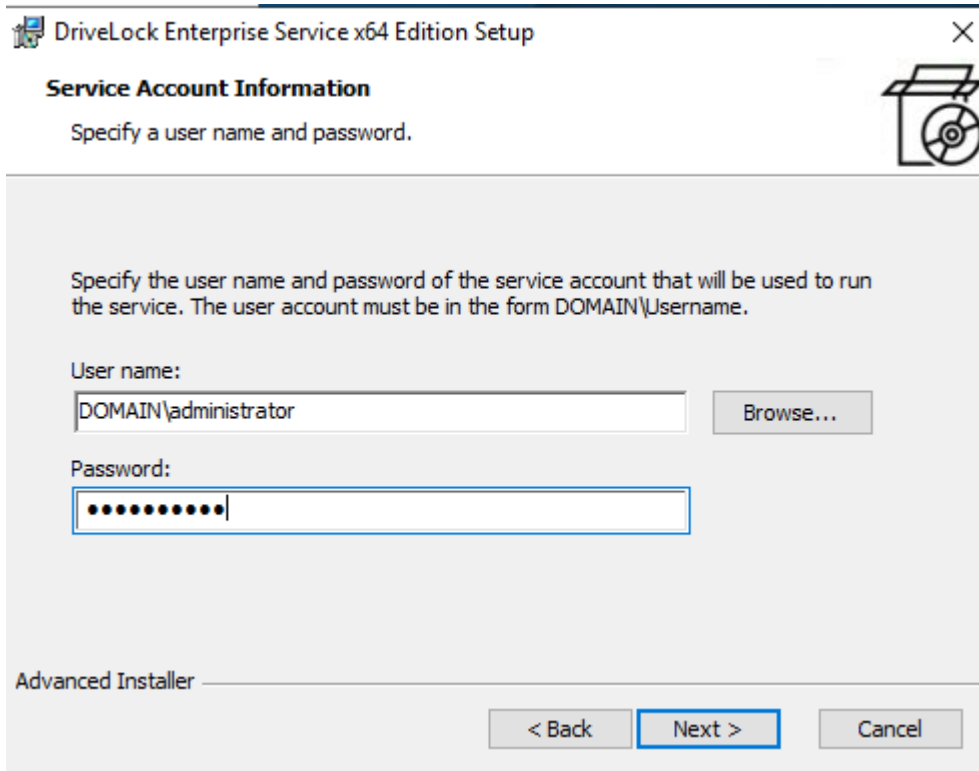
> ☑ Note: If you are using DriveLock Managed Services, you can use a linked DES in addition to the central DES in the cloud.
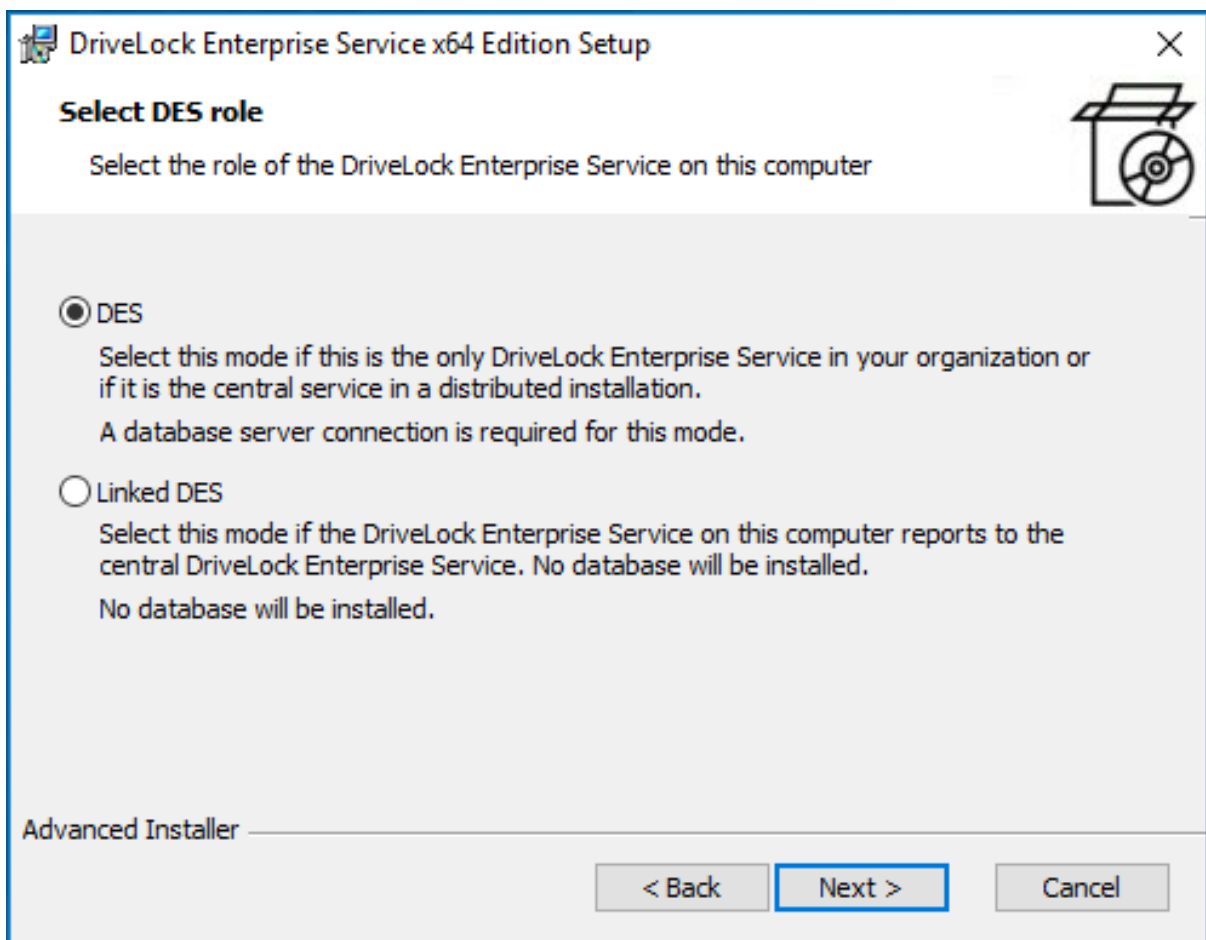
3. In the next dialog, enter the service account and the corresponding password you want to use for running the DriveLock Enterprise Service.
Click **Browse...** to select an existing account.

> 🖉   Note: Group managed service accounts (gMSAs) are supported.

4. Click **Install** in the next dialog to continue installing the DES.

5. Click **Finish** to complete the installation. The DriveLock Server Setup wizard then starts automatically.

3.3.2 Procedure in the DriveLock Server Setup Wizard

Proceed as follows in the wizard:

1. In the **Welcome to the DriveLock Server Setup** wizard dialog, click **Next**.

2. Select the **SSL/TLS certificate** from the computer's certificate store in the following dialog.
If it is an installation in a test environment, you can also have DriveLock generate a self-signed certificate. The certificate must fulfill certain requirements, see Trusted certificates.

Please note the following:

- In addition to HTTP communication, which uses the certificate from the certificate store, DriveLock uses an MQTT broker that requires the certificate as a file. To do so, the certificate must be exportable together with the private key.

- If the private key cannot be exported, the wizard will inform you on the following page. You then have the option of generating a self-signed certificate for the MQTT broker.

- If you decide to use a self-signed certificate for all communication, we recommend entering the certificate in the trusted certificates in the policy so that the communication between DES and agent is secure.

3. In the following dialog, select the option **Specify login account for DES** if you want to create a new database.
This option is selected by default if you selected the DES option when installing the server.

4. Next, enter the connection data for the database server.
   - Here you can optionally specify a different user for database access. Windows and SQL Server authentication are possible. This data is not stored and is used exclusively for the installation or update.

   > Note: If you also want to specify the port, the Server Setup Wizard supports the following notation:
   > FQDN,Port\Instance (e.g.: myDLServer,14330\SQLEXPRESS)

   - After entering the server name, click the **Test connection** button. If a green tick appears, the connection has been established. If there are any connection problems, these will be displayed in the area under **Messages** . You can then find an appropriate solution.

   - Select **Install a new database** as the action.

5. There are several options for creating the database, depending on certain scenarios.
   - **Create database**:
     This option is set by default. The database is created on the SQL server. The account that performs the installation must have the appropriate permissions on the SQL server (dbcreator role). If you deselect this option, you must provide a database. The schema is then installed in this database.

   - **Create database login on SQL server**:
     This option is also set by default. A login is created for the **DES service account**. The account that performs the installation must have appropriate permissions on the SQL Server (securityadmin role).

   - **Give DES service account full permission on the database (db_owner). Recommended for SQL Express**:
     This option is not set by default. This gives the DES service account maximum rights to the DriveLock databases and enables it to perform tasks such as maintenance (index maintenance), cleaning up old data records and backing up the database.

For larger environments or when operating on a full SQL server, we recommend switching this option off.

6. Next, enter the administrative user accounts for the DriveLock management components. This is usually the DriveLock administrator who performs the installation.
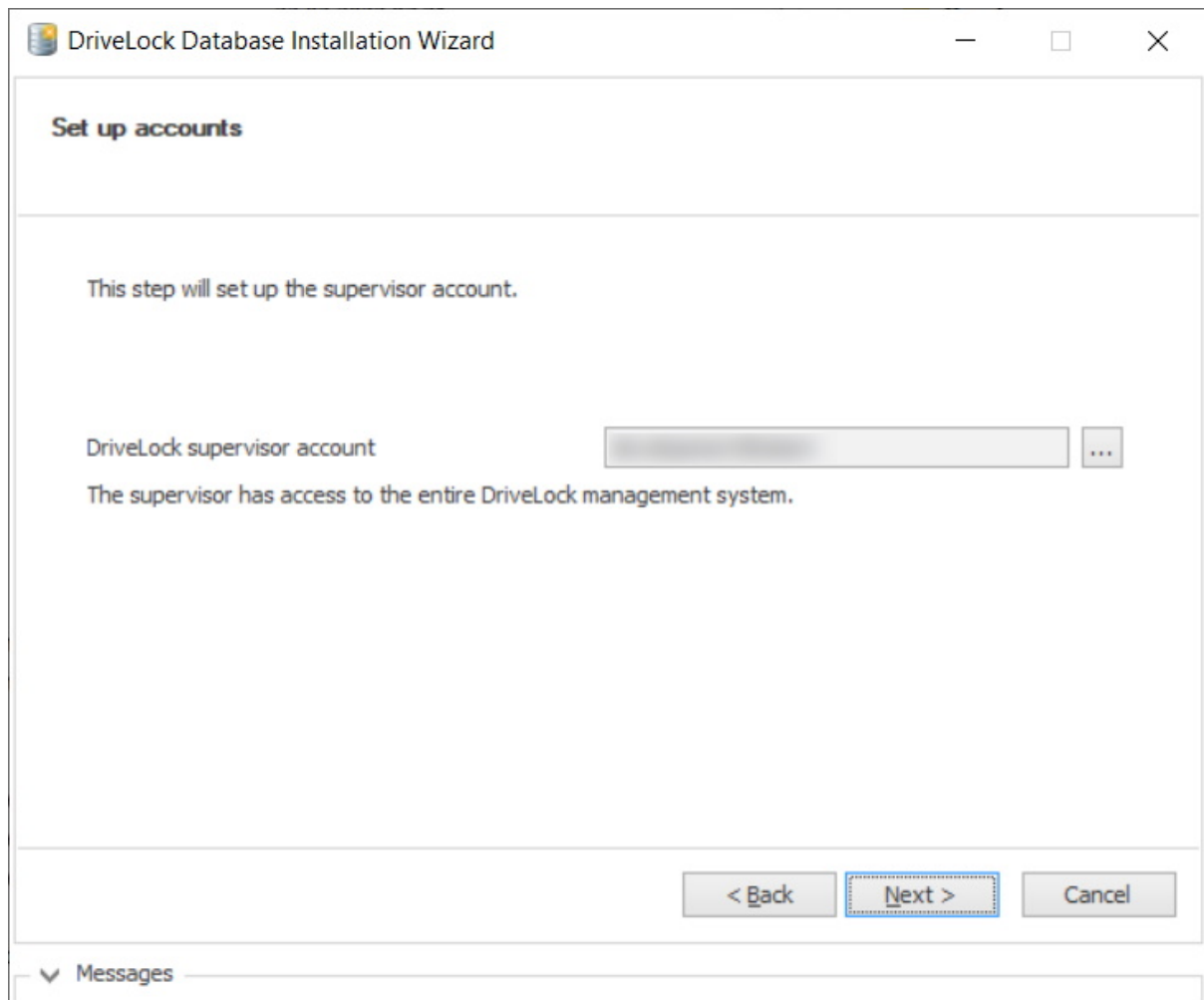
7. In the next dialog, specify whether you want to activate database maintenance or backup. Accept the standard options.

8. Finally, a summary is displayed. Click **Finish**. The DriveLock Enterprise Service (DES) will now start automatically.

3.3.3 Installing a linked DES

To install a linked DES, proceed as described in the chapter Installing the server. In this case, however, select the **Linked DES** option.

After you have completed the initial installation, the DriveLock Server Setup Wizard starts automatically. After the welcome dialog, select the **SSL/TLS certificate** from the computer's certificate store in the following dialog. Click here for more information.

In the next dialog, select the role of the DES. There are two options here.

For DriveLock On-Premise:

1. Select the option **Linked DriveLock Enterprise Service**.

2. Enter the registration data in the next step.

3. Enter the address of the central DES and a DOC account that has the right *Register linked DES*.

4. Click Connection test to check the connection to the central DES.

5. In the next step, enter the connection data. To do so, the central DES address must be specified with the port. In the list of tenants, you will only see the tenants you are authorized for. You can then select the corresponding tenant. Click **Register server** to complete the process.

In cloud environments:

1. The **Linked DriveLock Enterprise Service to connect to the cloud** option is used if you are working with the DriveLock Managed Service solution and have agents that do not have a direct internet connection. In this case, the connection to the DriveLock Cloud can be established via the linked DES as an intermediary.

2. To connect to the cloud, you need a registration API key. You can generate it in the DriveLock Operations Center (DOC) by selecting *Settings -> APIs* and then creating the key.

3. In the next dialog, copy the API key into the text field.

4. Click **Register server**.

> ✏️ Note: Please note that multi-factor authentication must not be activated during registration!

3.4 Initial configuration in the DriveLock Management Console

As soon as you have completed the installation of the DriveLockEnterprise Services (DES) and the DriveLock Management Console (DMC), a new **DriveLock** entry will appear in your Start menu. Start the **DriveLock Management Console** here.

Alternatively, you can also log in directly to the DriveLock Operations Center (DOC).

3.4.1 First configuration steps

First, a wizard appears to help you set up the connection settings to the DriveLock Enterprise Service (DES).

Please do the following:

1. After confirming the Welcome dialog, select the **Use DriveLock Enterprise Service** option in the next dialog.
    - Enter the server name and port. Use a fully qualified name when doing this. Use 6067 as port. For more information on ports, please visit here.
    - Select **root** as the default tenant from the drop-down list at **Tenant**.
    - If you want to specify a different user for your server, specify the appropriate information. This can be useful for restricting rights, for example.

2. If the DES uses a self-signed certificate, you must then confirm the certificate as trust-worthy.
    - Click the **Certificate... button**to verify that it is indeed the certificate that the DES is using.
    - Check the option **Don' ask me again for connections to this server**.
    - Confirm with **Yes** to use the certificate.
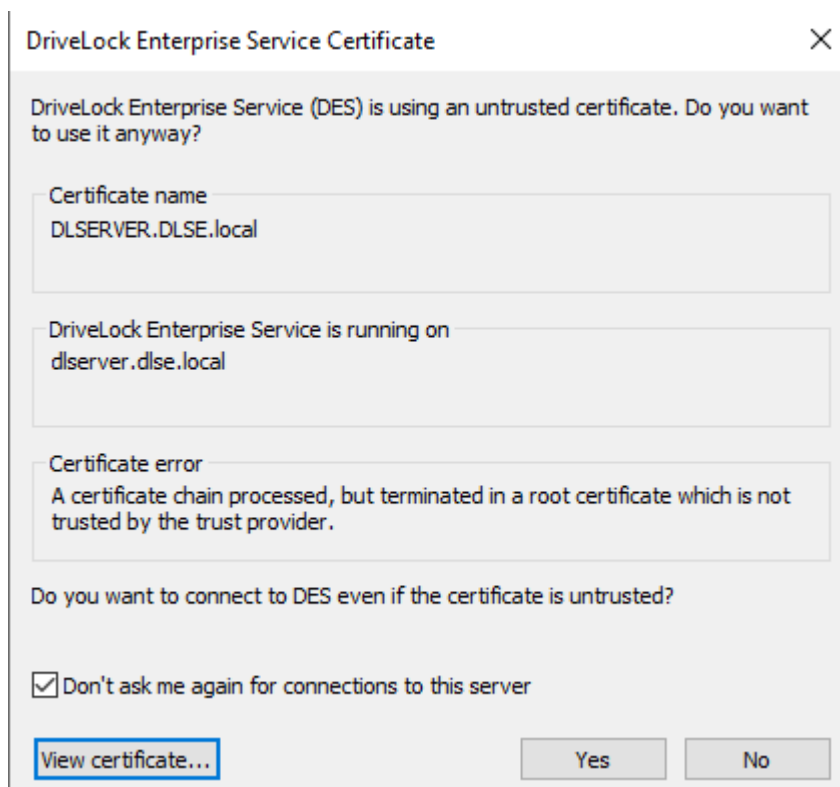
3. In the final dialog, you specify how often you want to check for new versions of the DriveLock Management Console. The version status is queried directly via the DriveLock Cloud.

4. Click **Finish** to confirm your entries.
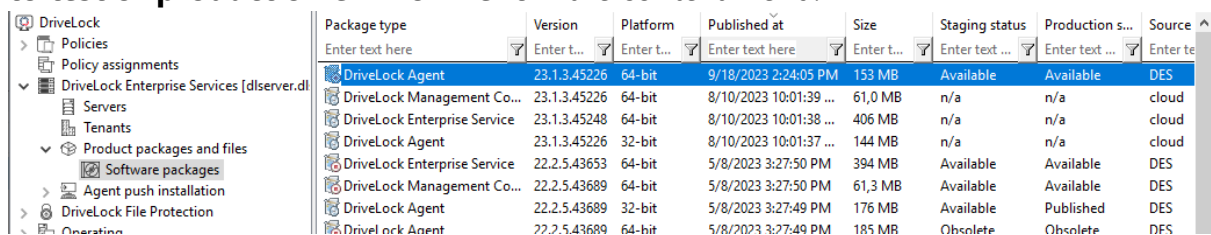
3.4.2 First upload of the agent packages to the DES

We recommend uploading and publishing the agent packages to DES to ensure that the automatic update and push installation work.

Please do the following:

1. The DriveLock ISO image contains the two msi packages for the DriveLock Agent. Copy them to any location on your computer.

2. Then go to the **Product packages and files** node in the DriveLock Management Console, select **Software packages** and choose **Upload package** from the context menu.

3. Select the relevant package (or the two agent packages) and upload them to the DES. They will then appear in the list of software packages.

4. Now publish the packages in the staging and/or production environment, see illustration.
    Make sure that the package is actually **published** in the production environment (**Production status** column) and is not just **available**. You can do this by selecting **Publish to test or production environment** in the context menu.

3.4.3 First steps for creating policies

All the settings the DriveLock Agent needs are stored in a DriveLock policy. Each DriveLock module (such as Device or Application Control or Encryption, for example) has its own area within the policy where all settings for that module are stored.

The reasons why working with centrally stored policies (CSPs) has proven successful for DriveLock include the following:

-   CSPs are stored in the DriveLock database; agents get them from there via the DriveLock Enterprise Service.

-   CSPs are automatically subject to versioning; administrators can edit or publish them separately.

-   It is possible to create any number of policies (or just one) and assign them to agents. Please also refer to the note in the Licenses section.

In the following, you create your first centrally stored policy, make some basic settings and then assign the policy.

3.4.3.1 First centrally stored policy

Please do the following:

1. To create your first centrally stored policy, go to the Policies node, open the context menu, select **New** and then **Centrally stored policy...**.

2. Enter a name and store the policy.
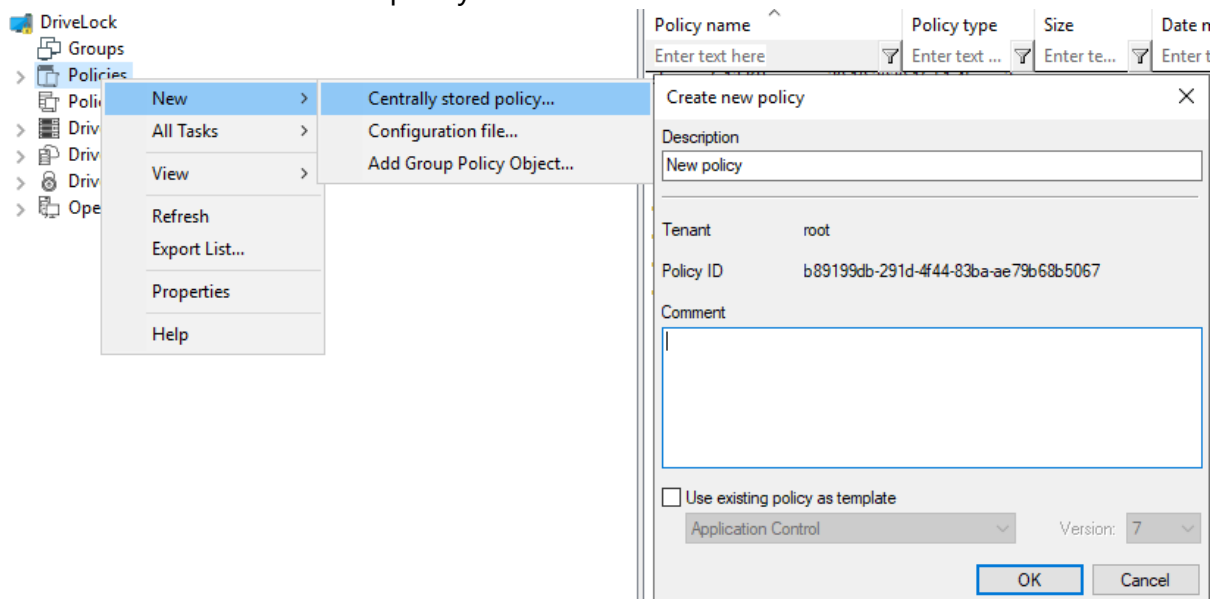
3. The new policy now appears in the list.

4. Then go to the **Global configuration** node first. The settings described below are basic settings and provide a minimum configuration. Click here for more information on the other settings.

3.4.3.1.1 Licenses

First enter your DriveLock licenses directly in the policy.

> Note: If you want to use a single policy for all your settings, you can simply specify the license settings in it. However, if you create several policies, we recommend creating a separate license policy that contains only the license settings and that is then assigned to the agents.

Please do the following:

1. Go to the **Settings** subnode and select **License**.

2. On the **Licenses** tab, you will enter your purchased licenses. You can do this directly by adding a license file or a license key, depending on what you have available. A wizard will guide you through the activation process.
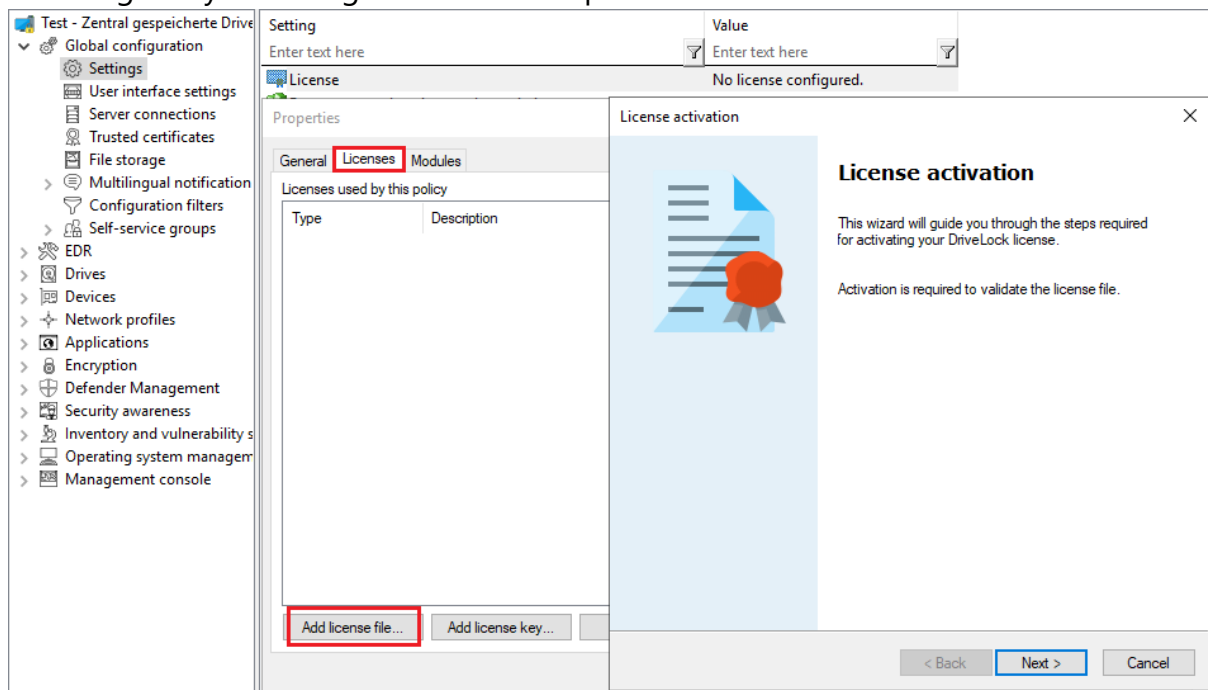
3. Once the license is entered into the system, your licensed DriveLock modules will be displayed on the **Modules** tab.

4. Select all of them here and click the **Edit** button.

5. Now you can specify the computers where the modules will be available. Click **Add** and select **< Any computer >** from the list.

> ☑ Note: You can also specify other settings here and restrict the modules to individual computers, groups or OUs.

6. Confirm your selection and save your license settings.

> ☑ Note: To hide modules you have not licensed in the policy, go to the top level of the policy and select the **Hide unlicensed nodes** context menu command.

3.4.3.1.2 Agent user interface settings

To indicate on the client computer that the DriveLock Agent is active, we recommend the following setting:

1. In the Global configuration node, open the **User interface settings** and the **Taskbar notification area settings**.

2. On the **General** tab, select **Display notification area icon** and then one of the two options **Display popup window** or **Display balloon message**, depending on how you want to inform the users.
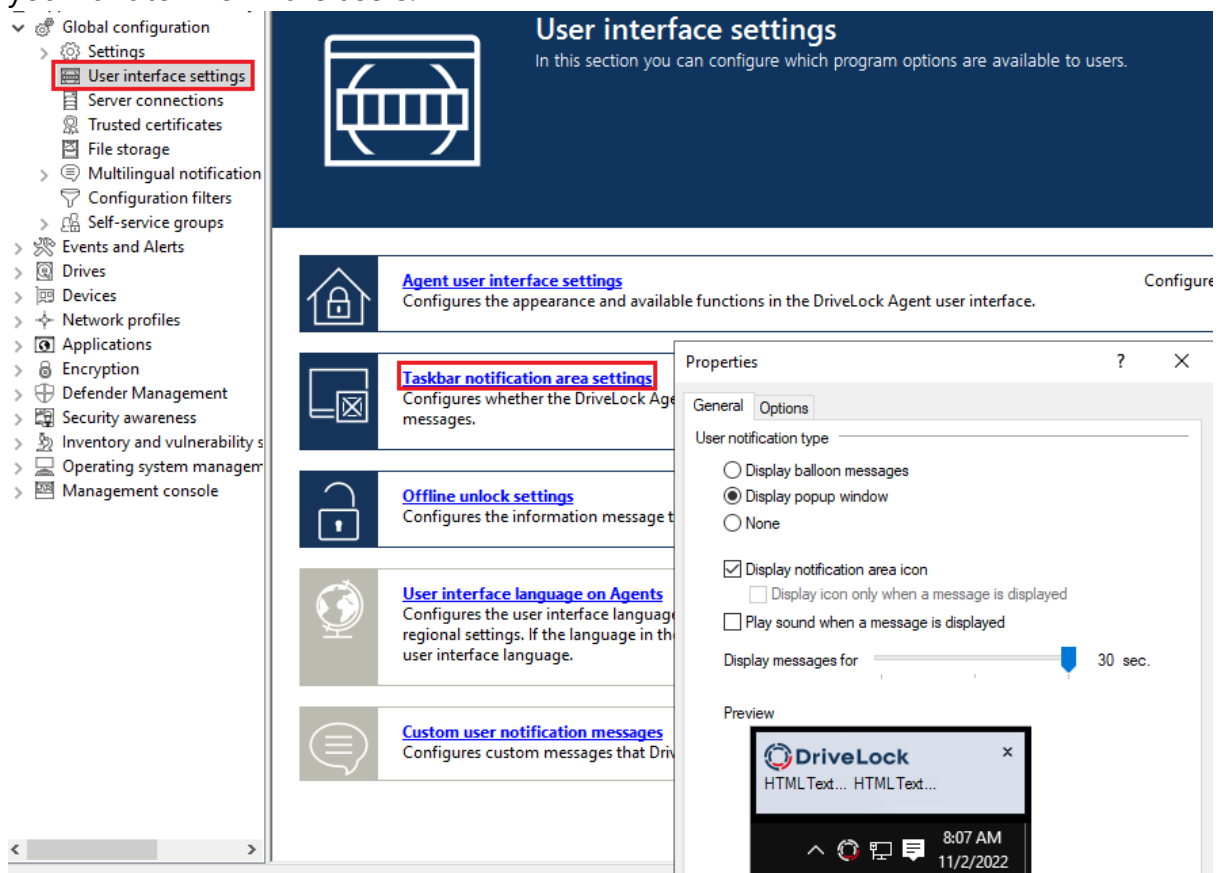
3. Confirm your settings with **Apply** and **OK**.

3.4.3.2 Saving and publishing a policy

Any changes to policies should always be saved and published.

Save : Changes are saved for DriveLock administrators.

Publish : The policy is saved and published to all agents as the current active version.

3.4.3.3 Assigning a policy

Centrally stored policies need to be manually assigned to create a relationship between the policy and DriveLock Agent on a client computer (or computers). Assignment targets can be all computers or individual computers, groups or organizational units.

Proceed as follows in the DriveLock Operations Center (DOC):

1. Open *Administration -> Policies -> Policy assignments*.

2. Open the assignment dialog via or via the context menu of a policy.
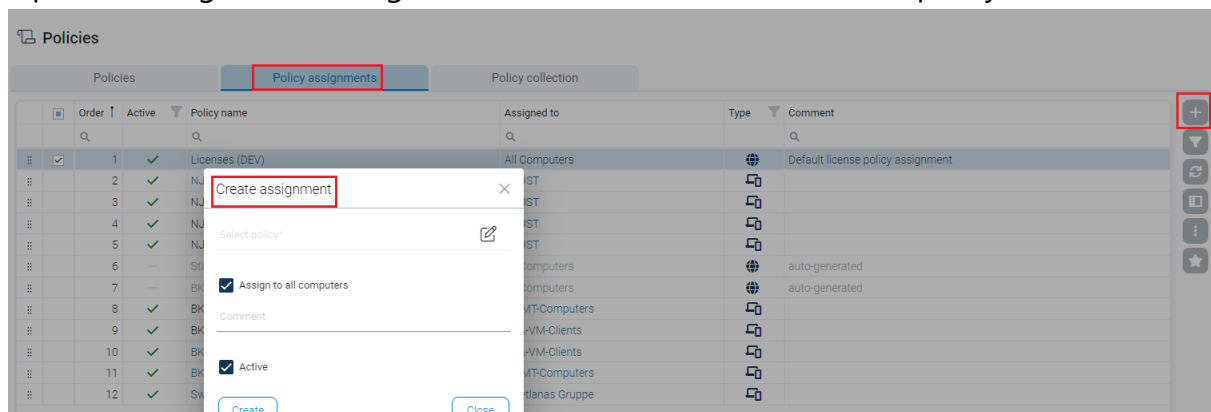
3. If you want to restrict the assignment to individual computers, groups or OUs, remove the checkmark next to **Assign policy to all computers** and select the relevant objects.

4. The assignment is now available and can be moved to different places in the list or deactivated.

Proceed as follows in the DriveLock Management Console:

1. Go to the **Policy assignments** node and open the **New** command from the context menu.

2. Select **All computers assignment...**.

3. Select the policy you have just created as **Assigned policy**, enter a comment if necessary and confirm with **OK**.
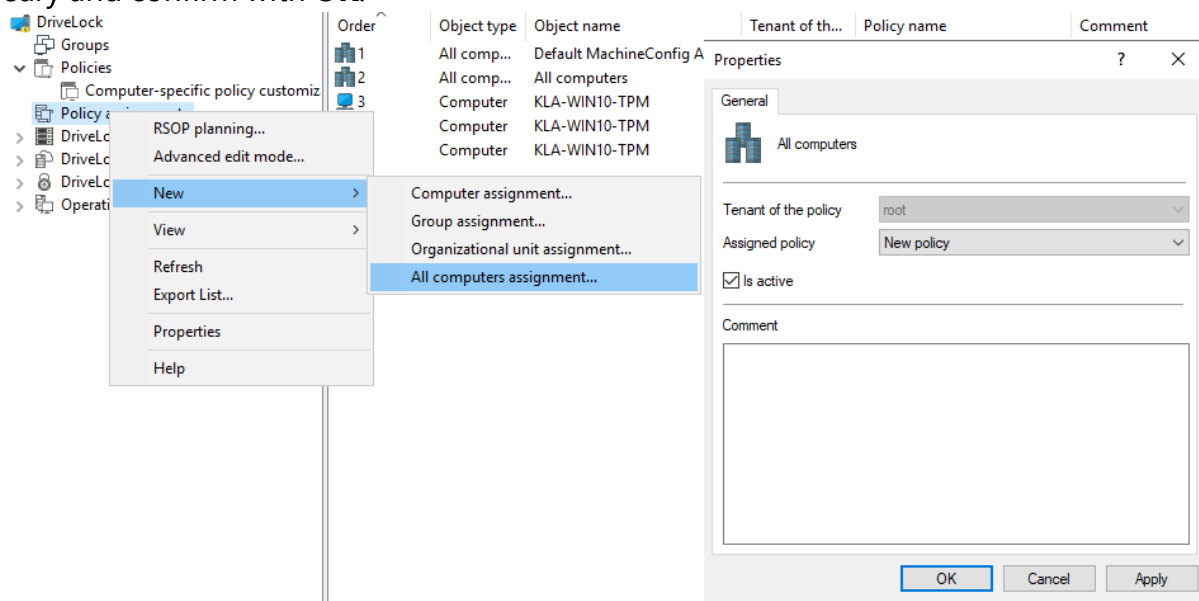
4. Your policy is now ready to be assigned to agents.

3.4.4 First login to DriveLock Operations Center

Open the DriveLock Operations Center (DOC) via the Start menu item **DriveLock Operations Center Weblink**.

Please note the following:

- Only AD users can log in.

- Warnings may be issued in certain cases because SSL certificates are used.

- You can set or change the language at this point.

- The AD group for the administrative users can be entered in the Settings view under Accounts.

4 Installing the DriveLock Agent

Every client computer must have a DriveLock Agent installed on it to control access to devices, drives, files or applications and to distribute encryption settings. The DriveLock Agent is provided as an MSI package, with one package for 32-bit and another for 64-bit systems. Select the correct package based on the Windows version on the client computers.

> Note: The MSI packages for the DriveLock Agent are located on the DriveLock ISO file or downloaded from the Internet by the DriveLock Installer. In the Management Console, the packages can be found in the **Product Packages and Files node** at **Software Packages**.

Basically, the MSI package can be installed either manually or automatically. For test installations we recommend manual installation, in all other cases you can use the automated installation method.

If you are not using a software distribution system, DriveLock Enterprise Service provides the option to distribute DriveLock Agents to all or to individual client computers on the network. A fully automated push installation can be performed via the DriveLock Operations Center.

If you distribute the Agent MSI package using a software distribution system, it must first be customized to ensure that each DriveLock Agent receives the correct policy immediately after installation. This can be done in several ways:

- By creating a modified Windows installation package (MSI file) or a Windows Installer transform (MST file).

- By using Windows Installer command line parameters.

4.1 Installation requirements for the DriveLock Agent

Please find detailed information on the supported versions and the installation requirements for the DriveLock Agent in the current release notes at DriveLock Online Help.

4.2 Deploying agents via MSI

Please do the following:

1. Go to the **Policies** node in the DriveLock Management Console, open the **All Tasks** context menu and select **Deploy centrally stored policy...**.

2. Start the Agent Deployment Wizard. The wizard queries all required parameters and generates the corresponding output.

3. In the second dialog, select the centrally stored policy you have created for use by DriveLock Agents and the server where the central DriveLock Enterprise Service is installed.

4. In the next dialog, select the type of installation package you want the wizard to create:

    - Microsoft Installer File (MSI): Creates a new Microsoft Installer package that contains the previously specified settings.

    - Microsoft Installer Transform file (MST): Creates a Microsoft Installer Transform (MST) file with the selected 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 the path and name of the original DriveLockAgent.msi file and the new MSI file.

6. Start the agent deployment.

4.2.1 Installation via command line

You can specify additional options when installing the agent via a command line or a script. Also, you can determine from where the agent gets its configuration settings and how they are accessed.

You may use the following syntax for unattended installation without displaying the installation wizard and with default settings:

```
Msiexec /i DriveLockAgent.msi /qn
```

The following example shows an installation with custom parameters:

```
msiexec /i DriveLockAgent.msi /qn USECONFIGFILE=1 CONFIGFILE-
E="\\fileserver\share\drivelock.cfg" USESVCACCT=1 SVCACCOUNT-
```

```
=domain\user SVCPASSWORD-
D="UCXUUZXY5LJLTJ2BAFPZTZ42JKBKPYCKCLVUXBEYYH2K6OZA"
```

Available options when configuring the DriveLock Agent via a centrally stored policy:

`USESERVERCONFIG=1`	Indicates that a centrally stored policy is being used.
`CONFIGID=<GUID>`	`<GUID>` is the GUID of the centrally stored policy in the form: XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXXX
`CONFIGSERVER=<name>`	`<name>` is the server name on which the DriveLock Enterprise Service has been installed and from which the policy is to be loaded
`TENANTNAME=<tenant>`	`<tenant>` is the tenant name the policy is to apply to. If you have not configured any tenants, please use "root" as tenant name.
`USEPROXY=1`	Indicates that a proxy is to be used

`PROXY=named;<proxy>:<port>`
 	
`PROXY=pac;<pac url>`
 	
`PROXY=netsh`
	`<named>`: use specific proxy
	
	`<pac>`: use Proxy Auto Configuration Script with URL
	
	`<netsh>`: use system proxy set with netsh

`PROXYACCOUNT=<authscheme>;`
 	
`<proxyuser>;<proxypassword>`
	Specify an account if the proxy requires authentication.
	
	`<proxyuser>`: User
	
	`<proxypassword>`: Password

	`<authscheme>`: possible values for the authentication scheme are `basic`, `ntlm`, `passport`, `digest`, `nego-tiate`.

.

4.3 Agent push installation

Configuration: DOC -> Settings (cogwheel) -> Installations

If you are working with DriveLock On-Premise, you can install your DriveLock Agents manually or automatically on the client computers of the end users (target computers) using 'push installation'.

Please do the following:

1. Open the DriveLock Operations Center (DOC).

2. Click the ⚙ icon in the window header.

3. Here you select **Installations** and then the Install **Agent** tab.
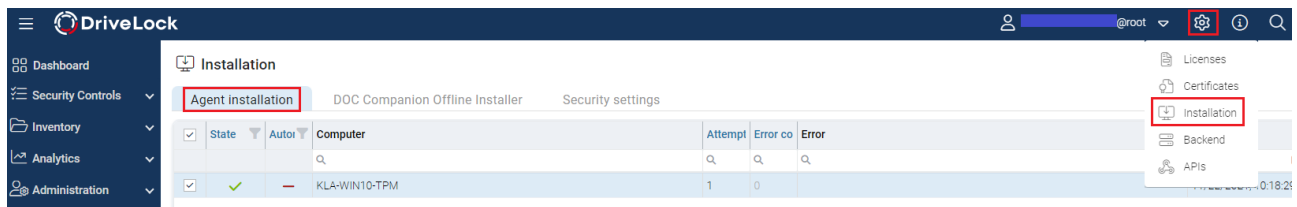
1. Enter your DES and the name of the client computer where you want to install the agent. Repeat the process to add multiple computers.

2. The push installation may take some time. Once it has been successfully performed, the status of the computer is indicated with a green check mark.

Push installation options

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

2. **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.

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

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

5. **Force removal of installed DriveLock Agents**: This option serves as a repair setting and should only be used if a previous DriveLock installation failed and the agent cannot be uninstalled with the usual methods.

6. **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. This is also used for the agent configuration.

7. **Configuration type**: Select the type of policy used to configure the computers here. As a rule, select Policy Assignment here (default option).

> Note: The push installation will only start if both a 32-bit and 64-bit version of the DriveLock agent is available in the software packages published in the test and production environment.

4.3.1 Requirements for the push installation

For the push installation to work, the DriveLock Update Service (DlUpdSvc) is copied, installed and started on the respective computer via administrative access. Next, the DlUpdSvc retrieves the currently released installation package via the DES and performs the agent 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 in the network.

- 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.

4.3.2 Settings for the push installation in the DOC

Configuration: DOC -> Settings ⚙ *-> Backend -> Server settings -> Configuration -> Push installation*

The global settings for push installation are configured independently for each DES. This means that they can be configured differently for different organizations within a company.

4.4 Checking the DriveLock Agent

You can verify the installation and the state of the agent on the client computer as follows:

- Check for the DriveLock Agent icon in the Windows system tray.
  If you open the context menu, you can also display the **agent status** here.

- Open the DriveLock Agent user interface. On the **Status tab** you can view the configuration status of the agent by clicking on the corresponding icon.

- Check whether DriveLock and DriveLock Health Monitor are active in the Services list. Both services must be running.

You can also use the following command line:

- `sc query drivelock` and/or `sc query dlhm`: to search for DriveLock services

- `drivelock -showstatus`: to check the status of the agent configuration

When using the push installation:

- Check the Windows event log for messages from the "DLUpdate" service. This service logs all errors that occurred during the installation in the application log. In addition, a log file of the push installation is written to "c:\windows\dlupdatexxx.log" (xxx is replaced by the current date and time).

Verification in the DOC

- The **Computer** view provides you with the agent status including all available properties.

4.5 Uninstalling the DriveLock Agent

There are two ways to uninstall DriveLock Agent, depending on whether you want to keep the agent configuration on the client computer or not.

Default uninstallation:

Uninstalling the DriveLock Agent will remove only the DriveLock Agent program files by default. All configuration files and registry entries are preserved.

Advanced uninstall:

In order to uninstall the DriveLock Agent along with all configuration files, you need to run the MSI parameter in the comma`REMOVEDATA=1`nd line.

```
msiexec /x <MSI Product GUID> REMOVEDATA=1
```

Example:

```
msiexec /x {E9EC6C0E-CFC2-4BBD-BE4D-8E0A353E4EB8} REMOVEDATA=1
```

This mode deletes the following on the DriveLock Agent:

- All program files

- All registry keys in HKEY_LOCAL_MACHINE

- All files from "C:\ProgramData\CenterTools DriveLock\".

- Firewall rules

The following files are not deleted:

- Log directory, usually in C:\ProgramData\CenterTools DriveLock\.

- User entries in the registry

- DriveLock events

- Firewall rules defined in the policy and created by the DriveLock Firewall component.

Tip: We do not recommend uninstalling the agent via the Windows user interface, but via the command line (using the `msiexec /x` command) or via software distribution tools.

Uninstalling the agent can be influenced by two policy settings:

- **Password for uninstalling DriveLock**: To prevent a DriveLock Agent from being uninstalled on a computer without permission, you can assign a password for the uninstallation for protection.

- **Run DriveLock agent services in unstoppable mode**: It is not possible to uninstall the agent if unstoppable mode is activated.

5 Operation and maintenance

5.1 Database maintenance

Configuration: DOC -> Settings ⚙ *-> Backend -> Database & event data maintenance*

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.

- In the **Clean up event data now** section, you can limit the growth of the SQL database by having the DriveLock Enterprise Service automatically delete old events. To do so, use the **Start cleanup** option. Enter the maximum age of the 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.

- You can **start database maintenance** in the **Database maintenance** section. By default, all events older than 30 days are automatically deleted on a daily basis. Maintenance of the indexes on the table columns is also activated via this option. This optimizes the search. By default, database maintenance is performed automatically on a daily basis.

- The **Delete inactive computers** section allows you to free your system of any inactive computers. Inactive computers are clients with DriveLock Agents installed that have not logged back into the server for a certain period of time. You can specify this time here and also the number of inactive computers you want to have deleted per cleanup. In this context, 'delete' means that the computer will no longer appear in your lists and displays and that group memberships, events and recovery data, along with all other data, will be deleted (depending on the option selected). However, the DriveLock Agent remains on the computer so that it can reappear in the system when you log on again.

    To automate this action, you can specify the following setting: *DOC -> Settings* ⚙ *-> Backend -> Client settings -> Maintenance -> Delete inactive computers*.

Note: If you want to protect certain computers from being deleted, DriveLock provides a static group by default you can add these computers to. This 'DoNotDelete_ComputerGroup' then contains, for example, computers belonging to management, administrators or employees that may be offline for longer periods without actually being classified as inactive. It is created by the system as soon as you have activated the automatic deletion of inactive computers and can also be deleted again if deactivated. The group name and description can be customized and individual members can be removed.

6 Updating DriveLock

It is not necessary to uninstall an older version of DriveLock, the update is performed automatically by installing a newer package "on top" of the older version.

> Note: Please update the DriveLock Enterprise Service (DES) first and all other components afterwards.

Please note that the DES, the database and the agent are updated differently.

6.1 Updating the DES

> Note: When updating the DriveLock Enterprise Services (DES) from version 2021.1 to higher versions, please note the following: Before you start the update, you need a valid license including maintenance. You can renew them in your current DriveLock Operations Center (DOC). If you have any questions about your license, please contact DriveLock Support.

Confirm the certificate you have selected for the communication between DriveLock Management Console or the DriveLock agents and the DES. An additional dialog in the server installation wizard shows you the certificate.

6.2 Updating the database

> Note: Please note that the database temporarily requires more memory during a database update.

To update the database, start the Server Setup Wizard. After the connection test, select the option **Check / update an existing DriveLock database**. A dialog then appears in which the database versions are displayed.

If you want to create a new supervisor account, check the corresponding option and then specify the supervisor's account in the following dialog. The supervisor role has elevated privileges (e.g., permission to make infrastructure or configuration changes to one (or more) tenants).

6.3 Updating the DriveLock Agent

> Note: The version of the DriveLock Agent may be lower, but never higher than the version of the DriveLock Enterprise Service. We recommend that all DriveLock components have the same version.

Manual installation

You can install the new update manually. In this case, simply install the new Windows installation package (MSI). You do not need to change the agent configuration, because your existing configuration will be kept during the update.

Automatic installation

The automatic update of the DriveLock agent to a new version must be configured in a policy.

To do so, open the **Settings** sub-node in your policy under **Global configuration** and select **Automatic update**.

The agent checks the published software packages on the DES for a newer version. If a newer version is available, it will be downloaded and installed.

If you have published a new version on the DES and want to trigger an automatic update, you can use the command line `drivelock -updateproduct` on the agent computer.

6.3.1 Notes on updating the DriveLock Agent

Please note the following when you update the DriveLock Agent to a newer version:

1. Before starting the update:
   - If you do not update the agent using DriveLock's autoupdate mechanism, the setting **Run DriveLock Agent in unstoppable mode** in the DriveLock policy should either be disabled or set to 'Not configured (default)'.
   - If you are using hard disk encryption, you can use the setting Delay decryption by x days.

   > Note: This option was introduced because it could happen that an invalid policy configuration was assigned to the agent after a DriveLock update or a change to another group and decryption then started immediately. The delay prevents this and allows time to correct the configuration, even if it was created by mistake.

2. During the update:
   - Perform the upgrade with a privileged administrator account. This is automatically true for the auto update.

3. After the update:
   - If you are using File Protection or Disk Protection, a reboot after the DriveLock Agent update is required to update the driver components. This reboot is

recommended once the components have been updated. If you are using a software deployment tool for the update, add this step to the update procedure or restart the updated computers manually.

6.3.2 Notes on manual updating

- If you want to run `DriveLock Agent.msi`, it must be done from an administrative command window via `msiexec`. Double-clicking the command from the Windows Explorer does not work.

- If you update manually by starting `msiexec` msiexec or DLSetup.exe, it may happen that Windows Explorer does not close correctly. As a result, the Windows user interface disappears (black screen) and does not restart even after the agent update. If this happens, you will have to start the Explorer manually via the Task Manager or initiate a reboot. This mainly affects customers who are using client management software that may be running the `msiexec` in a user session. The problem can be solved by adding the following parameters to the msiexec call:
  - `MSIRESTARTMANAGERCONTROL=Disable`

  - `MSIRMSHUTDOWN=2`

6.3.3 Automatic updates

DriveLock Agents can be automatically updated to a newer version. The same applies to the DriveLock Management Console (DMC)

Under **Enabled automatic updates**, select the components that you want to update automatically. In the example below, only **DriveLock Agent** is selected, i.e. it is automatically updated to the next version on all client computers that receive this policy.
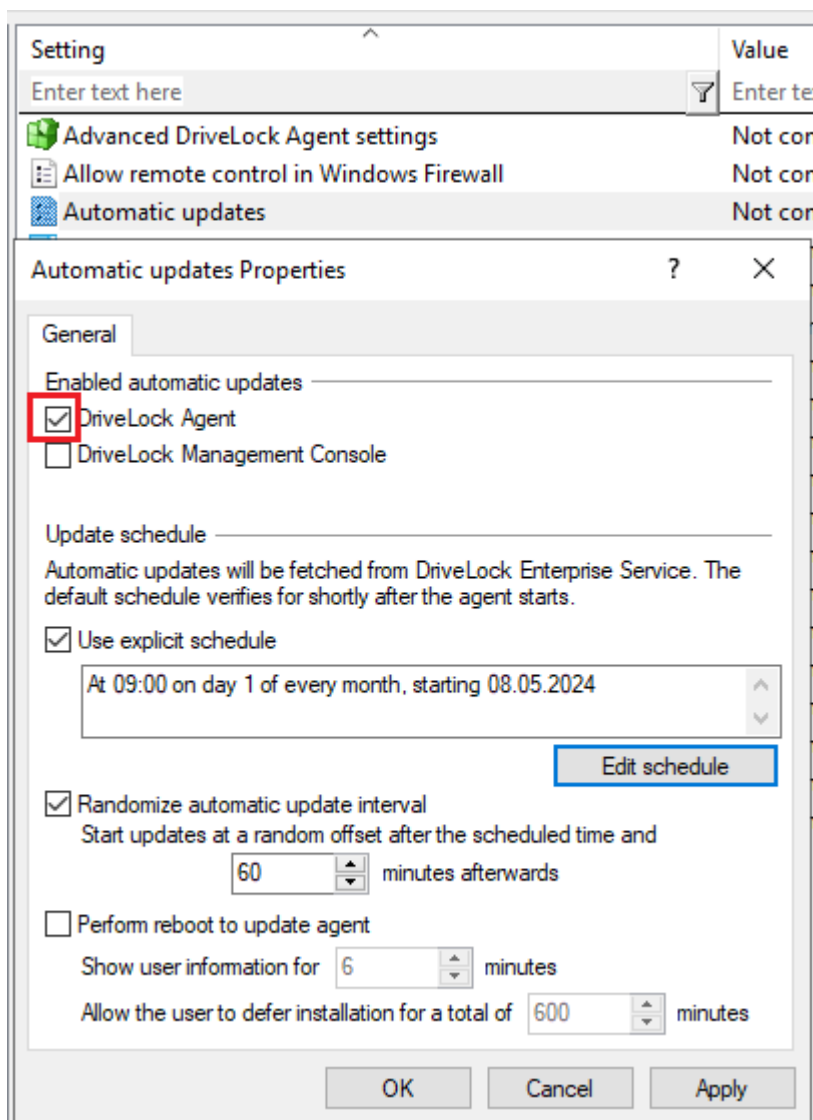
By default, the agent then randomly checks for newer versions on the DES within 60 minutes of system startup and continues to do so every 60 minutes thereafter. If so, the DES will download and install it immediately. The random timing ensures that not all computers in a company start updating or downloading 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.

In the DriveLock Operations Center (DOC), you can monitor the automatic update based on events.

Please note the following information in the event of an error:

If an error occurs during the automatic update because no server connection could be established, this is usually due to the fact that the redirect URL is not included in the firewall rules. In this case, please add the following call to your firewall rules: https://dlpackages.blob.core.windows.net/*

7 Working with DriveLock

The following consoles are available for working with DriveLock:

- DriveLock Operations Center (DOC)

- DriveLock Policy Editor

- DriveLock Management Console (DMC)

> ☑ Note: Please note that not all functionalities are equally available in all consoles. This also depends on whether you are working with DriveLock on-premise or as a managed service. More and more functionality is being moved into the DOC from version to version, replacing the DMC in the long term.

7.1 General notes

DriveLock Managed Security Services and DriveLock 'On-Premise' use an almost 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-premise: Login via e-mail activation or via SAML; login as AD user or via membership in an AD group; login with Windows Authentication

     > ☑ 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-premise: Executing the push installation

3. Configure the DriveLock Agent
   - Managed Services: The agent cannot be configured remotely

   - On-premise: The agent can be configured via the remote agent control (client, policy, etc.)

7.1.1 Signing in to the DOC

DriveLock On-Premise customers have two options for opening 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.

From your browser directly, by manually entering the URL **https://DES-SERVER:4568** in the browser. DES-SERVER must be the host name of your DriveLock Enterprise Server (DES) in this case.

> ⚠ 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.

7.1.2 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. Further information on certificates can be found here.

> ☑ 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.
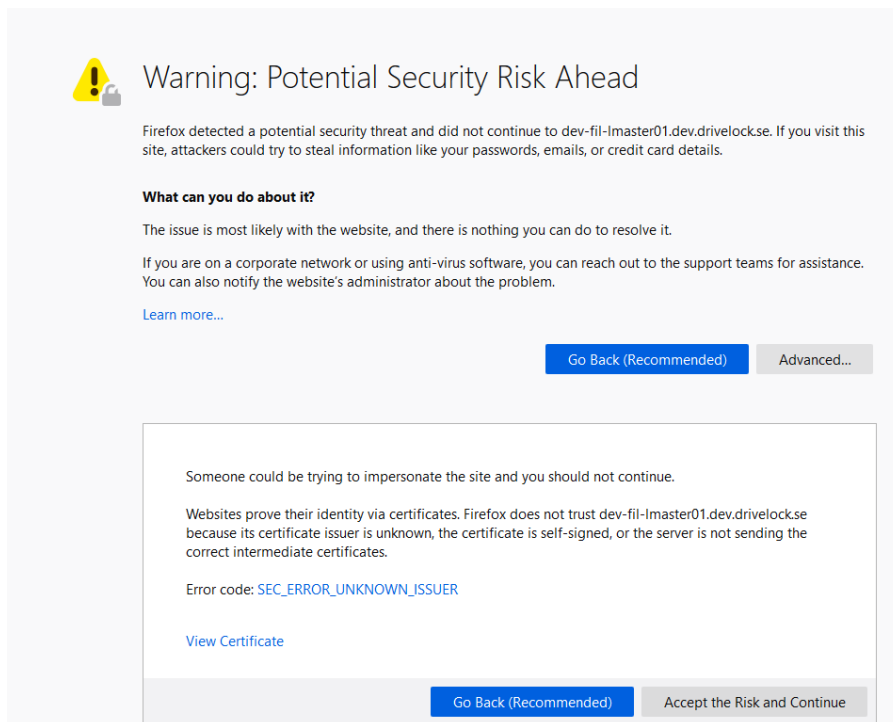
For Google Chrome and Microsoft Edge, the following applies:

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

7.1.2.1 Import 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.
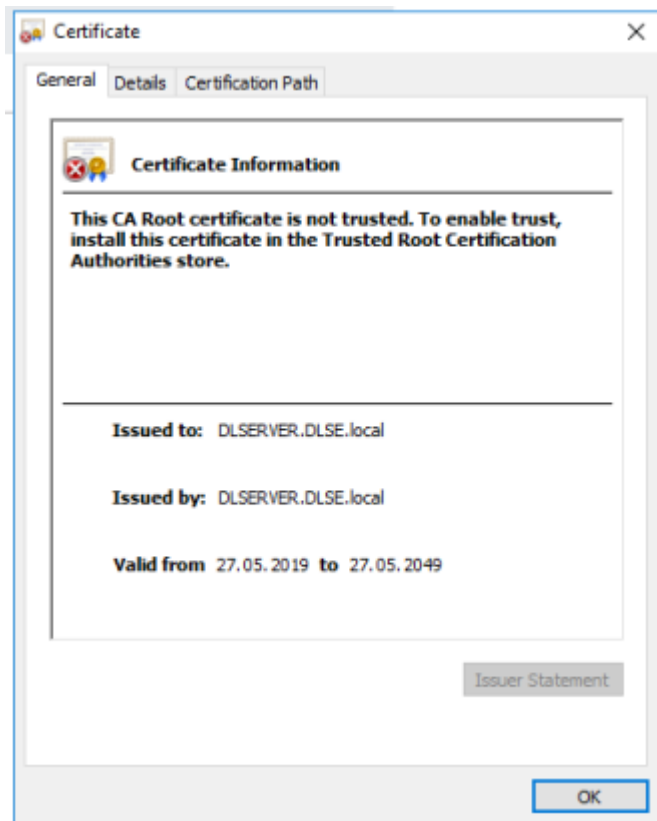
3. Store the certificate in a directory on your computer.

4. Open the certificate's context menu and click **Install Certificate**.
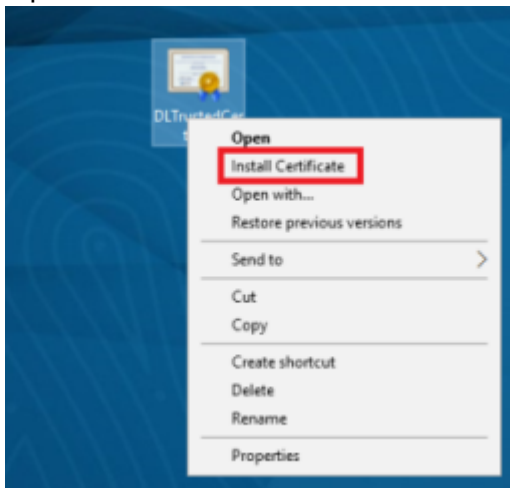
5. The Certificate Import Wizard opens. On the first page, keep the default X.509.

6. On the next page, select Local computer.

7. On the third page, select **Trusted Root Certification Authority** as the certificate store:
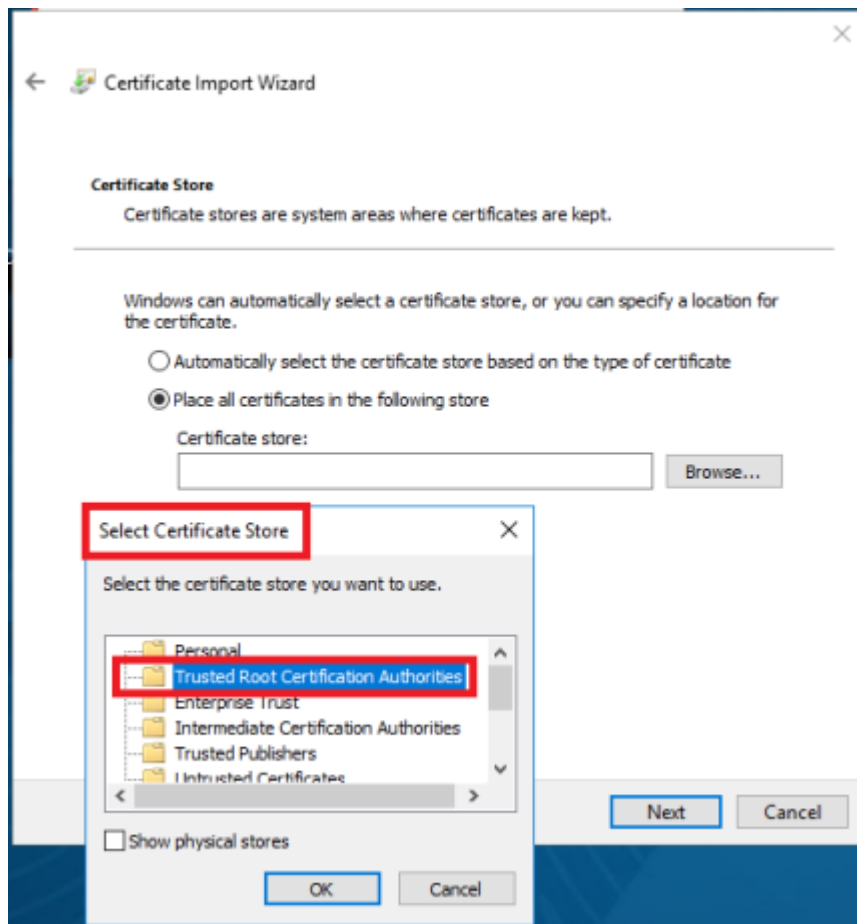
8. In the next dialog, click **Finish**.
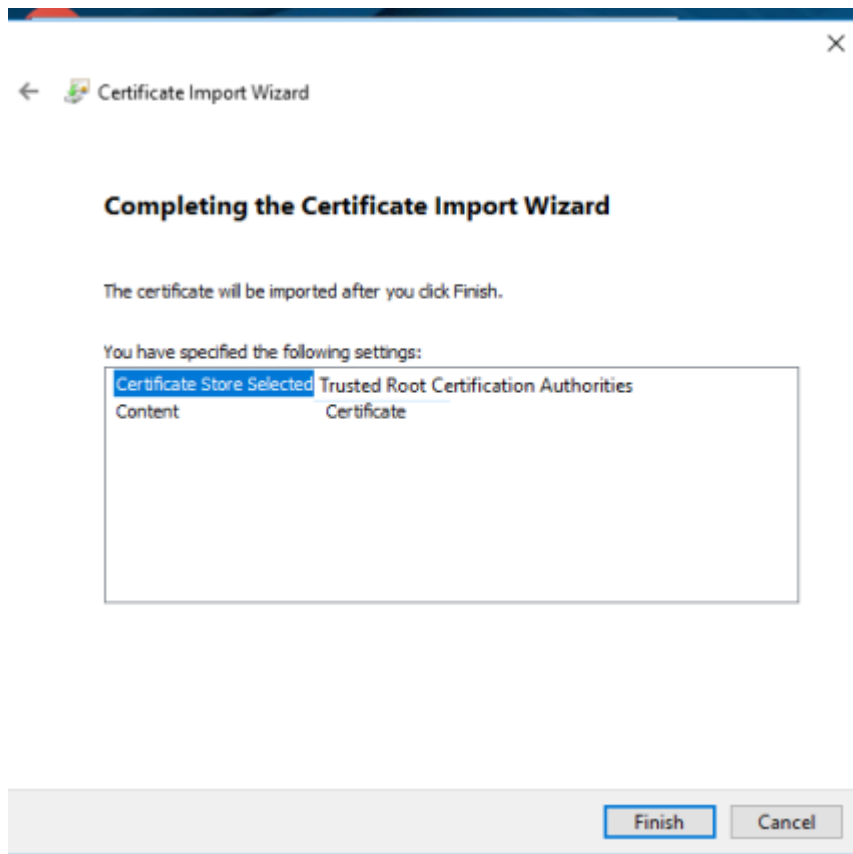
9. Now the certificate is registered and the next time you open the DOC, you will be taken directly to the logon screen without any error message.

> ⊘ 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):
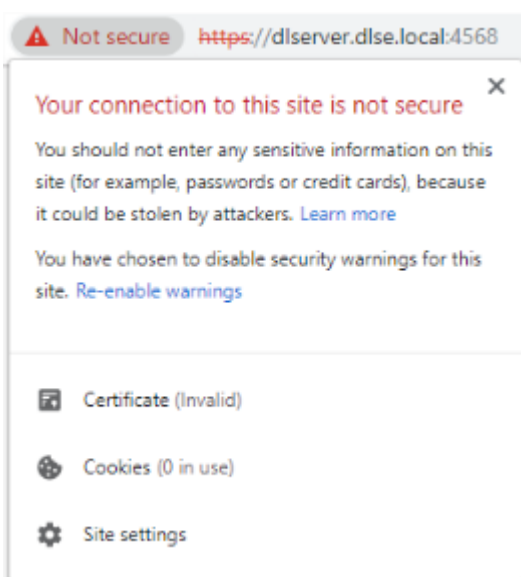
7.1.3 DriveLock in Active Directory, Microsoft Entra ID or workgroups

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 the Microsoft Entra ID integration is also available. DriveLock computer groups or Microsoft Entra ID computer groups can be used anywhere where AD computer groups or OUs can be used.

DriveLock and Microsoft Entra ID user groups, on the other hand, cannot be used everywhere.

Please note the following:

- In a DriveLock On-Premise installation, you use the local users of the computer on which the DES is installed to manage the environment.

- If you are using DriveLock Managed Services, you can use a Microsoft Entra ID integration to log in to the DOC or 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.

7.2 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), the DriveLock Agent (which is distributed on the client computers), inventory and event display functions, and the DriveLock Enterprise Service (DES) with the associated databases for the on-premise version. Combination modules can be added to some main modules (e.g. Encryption 2-Go to Device Control, see table below).

> Note: Starting with DriveLock version 2024.2, licenses are managed centrally in the DriveLock Operations Center (DOC) and automatically entered in a license policy. This policy is automatically assigned to all computers.

Licenses that are entered via the DriveLock Management Console (DMC) in a policy and uploaded to the server are automatically entered in the license list and the license policy in the DOC. You still need to activate the modules in policies, see Best practice for licensing.

> Note: A DriveLock license includes the modules purchased (e.g. Device Control, Application Control, each including a quantity).
> To ensure that a DriveLock module works correctly, the licence for it must be entered in a policy and you must activate the module. The DriveLock license is issued as a file or a license key (both types of licence are equally valid).

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).

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

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
Device Control	BitLocker To Go	Control and encrypt external media with BitLocker To Go
BitLocker Management		Management of Microsoft BitLocker functionality
BitLocker Man-	DriveLock PBA	Pre-boot authentication management

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

⚠ Warning: The licenses for Disk Protection and BitLocker Management cannot be active at the same time. If you want to use Disk Protection and BitLocker at the same

> ⚠ time, please make sure to enter the respective licenses in separate policies. The policy assignments must be set up so that a client only receives one of the two licenses through the policies.

> ☑ Note: As of version 2023.1, the functionality of the Risk & Compliance (EDR) module is largely part of the DriveLock Zero Trust Platform. To use MITRE Attack rules, you will now need a license for Application Control.

7.2.1 Managing licenses in the DriveLock Operations Center (DOC)

Configuration: DOC -> Settings (gear icon) -> Licenses

As of DriveLock version 2024.2, licenses are managed centrally in the DOC and automatically entered in a license policy.

- The **Licenses in use** tab provides you with an evaluation of the allocation and use of your licenses. Please note that computer and user licenses are displayed separately. This is particularly important when using terminal servers. License usage is based on which computers and users have reported in the last 30 days.
  Please note: for security awareness, usage is calculated based on users, not computers.

- On the **Licenses** tab, you can see which DriveLock modules are licensed, what type of license they have, and when maintenance expires.
  This is where you manage your licenses (see also Best practice):
    - Add licenses as a file or key

    - Remove expired and no longer required licenses

- To extend licenses, add the new or extended license file or the license key. Existing licenses are overwritten by the extended license.

- Please note the following for expired licenses:
    - Subscription licenses have an expiration date. Once this is reached, you no longer have access to the DriveLock functionality.

    - Perpetual licenses have a maintenance end date. After this date, the product can no longer be updated to a new version.

- Under-licensing: To determine the license usage, the computers and user data that have activated a module for licensing are evaluated.

> ☑ Note: If you have any questions about licenses, please contact your DriveLock sales partner or the DriveLock Managed Services team.

7.2.1.1 Compatibility of licenses

The DriveLock license concept is downward compatible, i.e. the licenses can be entered in the respective policies as before. However, we recommend moving to a single license policy, as introduced in version 2024.2, see Best practices for licensing.

If necessary, you can remove the licenses from existing policies; the module assignment can be retained. If the list of licenses does not contain all the licenses used to date, you can extract them from existing policies in the DOC.

7.2.1.2 Evaluating licenses

Licenses are always evaluated on a tenant basis, as each tenant has its own license policy. There is one exception in on-premises installations: while the evaluation in the root tenant is global, it remains tenant-specific in all other tenants.

7.2.2 Entering licenses in policies (DMC)

You can configure the **Licenses** in the **Global configuration** node in the **Settings** subnode.

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.

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

Properties   ?   ×

General   Licenses   Modules

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	

OK   Cancel   Apply

The **General** tab displays the license status of each module. Please find information on how to activate modules here.

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 you need to specify a proxy server for your Internet connection, click on **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: We recommend transferring the licenses to the DriveLock Enterprise Service after successful activation. 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...** .

7.2.3 Transferring licenses to the DES

When you create a new DriveLock configuration and import a license file, you can transfer it to the DriveLock Enterprise Service (DES). This activates additional functions for various areas (e.g. Security Awareness Content AddOn, vulnerability scanner) 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 so, select the **Licenses** tab.

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.

Licenses are managed via the DriveLock Management Console (DMC) and in the DriveLock Operations Center (DOC).

7.2.4 Activating DriveLock modules in policies (DMC)

On the **Modules** tab, you can configure which module you want to activate on specific agents.

With this information you can

- prevent a particular module from being used 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 also configure different modules in different policies.

Properties   ?   ✕

General   Licenses   **Modules**

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 >	-
		-

[Activate for < Any computer >]   [Set to 'Not Configured']   [Edit...]

[OK]   [Cancel]   [Apply]

7.2.5 Best practice for licensing

Once you have received your DriveLock license as a key or file, proceed as follows:

1. Open the Settings ⚙ in the DriveLock Operations Center (DOC) and select the **Licenses** menu command.

2. Enter your license on the **Licenses** tab. An overview shows you a summary of the license information.
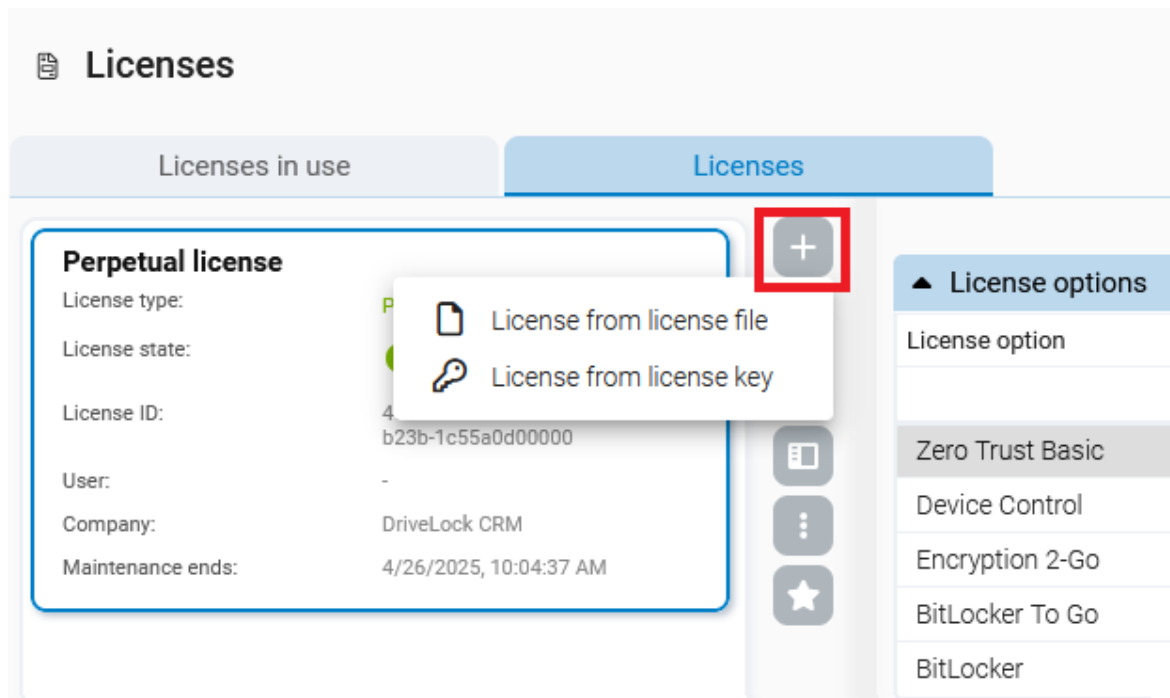
3. DriveLock now automatically creates a license policy that is assigned to all agents. This means that a license is available, but the DriveLock modules are not yet active.

> ☑ Note: The assignment of the license policy is given a low priority so that existing policies with licenses are not overwritten.

4. Next, activate the modules.

> ☑ Note: We recommend that you create individual policies for your respective DriveLock modules, e.g. a policy with settings for Application Control, one for Device Control, etc.

Open the relevant policy in the DMC Policy Editor and go to **Licenses** in the **Global configuration**. Open the **Modules** tab here.

5. Specify for which DriveLock Agents the modules will be active, e.g. on all or only on certain computers.

Procedure for license updates:

When updating, licences can be extracted from existing policies and entered into the license policy. Existing licenses are not deleted from the existing policies. This makes it easier to switch to the new license management method from version 2024.2.

To do this, select the following menu command:
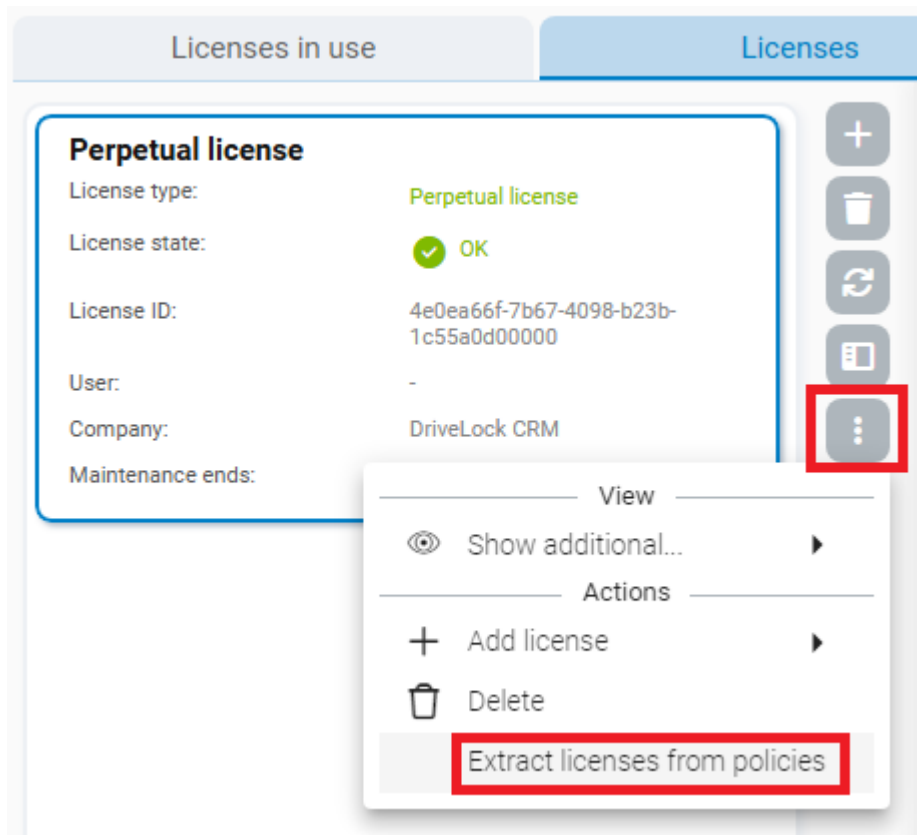
7.3 Communication structure

7.3.1 DriveLock Architecture - On-Premise

The central DriveLock Enterprise Service (DES) relies on a database for storing the configuration and feedback from the agents.

You can also use linked DES that do not access the database directly, but interact with it via the central server. In large DriveLock environments, this can reduce the use of system resources and network bandwidth of the central DES.

- Architecture with central DES:
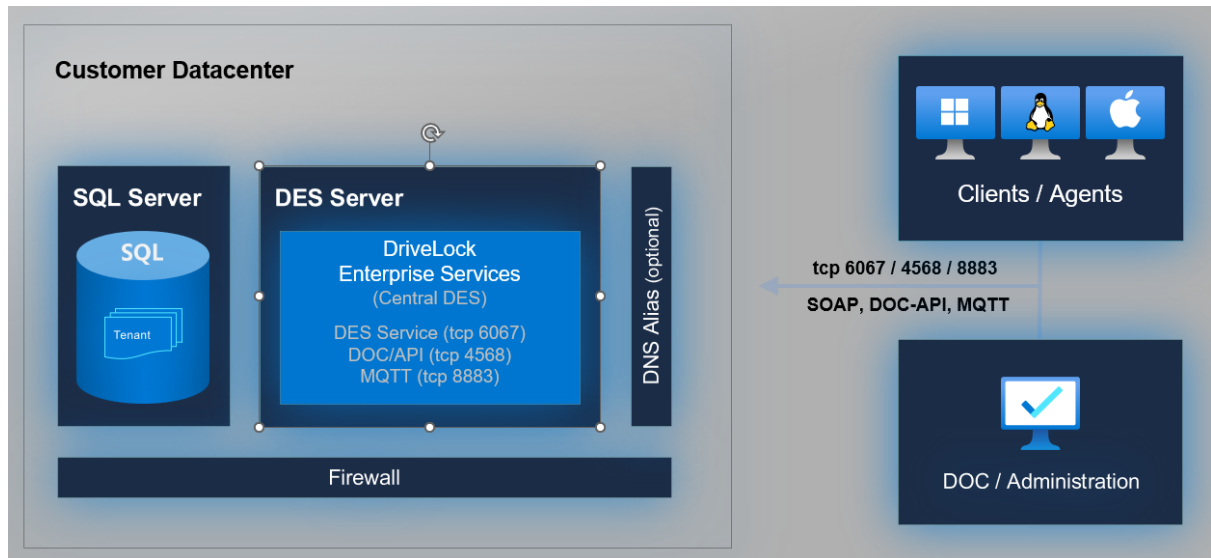
- The architecture with linked DES and ports can be found here:

7.3.1.1 Network communication structure and ports

The following figure shows the network communication between the various DriveLock components, including the ports used for this purpose:
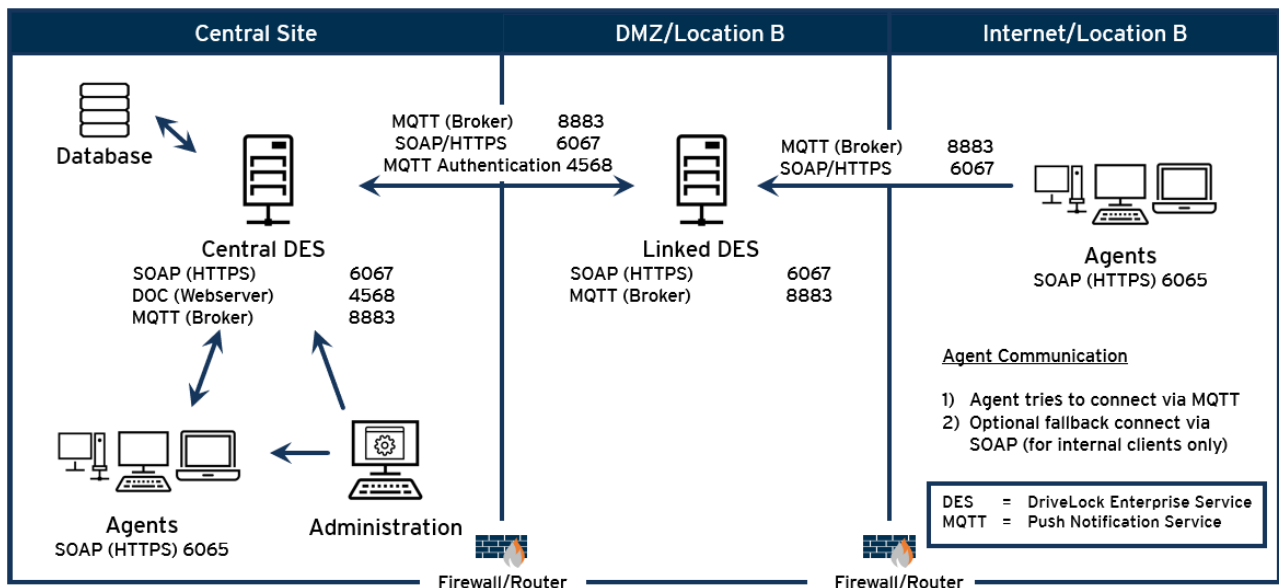
List of required ports:

Database:	
MSSQL ports	1433/1434
Transmission protocol HTTP:	
DES	6066
DriveLock Agent	6064
Transmission protocol HTTPS:	
DES	6067
DriveLock Agent	6065
Network protocols:	
MQTT (Broker)	8883

DOC (web server) / MQTT authentication	4568
LDAP	389

> ⚠ Warning: Please note that DriveLock does not support any change of the MQTT port! If the corresponding port is already used by another application, it must be changed or removed, or you must install the DES on another server.

7.3.2 DriveLock Architecture - Cloud

The architecture in the cloud environment looks like this:
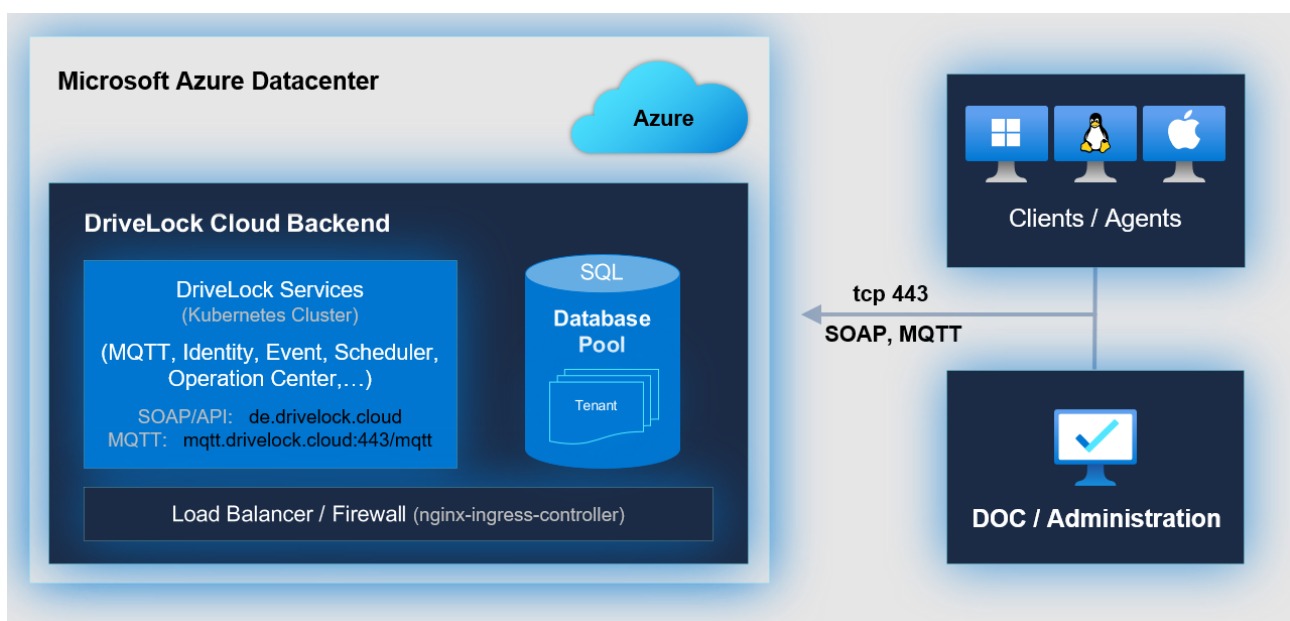
> 📝 Note: Please note that the MSI packages for the DriveLock agent are stored at the following URL and can be downloaded from there: https://dlpack-ages.blob.core.windows.net.

7.3.3 Files, directories and services for DriveLock

In the context of antivirus software, you may need to define exclusions.

In some cases, installing DriveLock Disk Protection may fail because of an antivirus software quarantining the hidden directory C:\SECURDSK. If this occurs, please disable your antivirus protection for the duration of the Disk Protection installation. We recommend that you configure your virus scanner with an exception for the folder.

> Note: The same applies if there is more than one Disk Protection encrypted partition in a system (which can be a logical partition on the same media where C: is located, or located on a separate hard disk or SSD).

If you encounter any other unexpected issues related to antivirus software, please find below the list of executable files, directories and services that are used by DriveLock:

Files and directories:

- "C:\SECURDSK" (EFS).

- "C:\Program Files\CenterTools\DriveLock" (application directory).

- "C:\ProgramData\CenterTools DriveLock" (cache/working directory)

Processes/Services:

- **DriveLock**
  Display name: DriveLock
  Executable path: "C:\Program Files\CenterTools\DriveLock\DriveLock.exe"

- **dlhm**
  Display name: DriveLock Health Monitor
  Executable path: "C:\Program Files\CenterTools\DriveLock\DLHM.exe"

- **StorageEncryptionService**
  Display name: DriveLock Full Disk Encryption Encryptor
  Executable path: "C:\Program Files\CenterTools\DriveLock\DlFdeEncSvc.exe"

- **ClientDataManager**
  Display name: DriveLock Full Disk Encryption Manager
  Executable path: "C:\Program Files\CenterTools\DriveLock\DlFdeMgr.exe"

- **dlupdate**
  Display name: DriveLock Update and Installation
  Executable path: "C:\Windows\DLUpdSvc.exe"

- **dessvc**
  Display name: DriveLock Enterprise Service
  Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DES.exe"

- **DESTray**
  Function: Displayed in the taskbar with the DES icon
  Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DESTray.exe"

- **DesRestarter**

Function: Restarts the DES service

Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Ser-
vice\DesRestarter.exe"

8 DriveLock Operations Center (DOC)

The DOC is a modern browser-based user interface for the DriveLock Zero Trust Platform. The DOC can be used by customers of DriveLock Managed Security Services who use our cloud-based security solution, as well as customers who use DriveLock 'on-premise' and manage it themselves.

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.

The DOC also provides the following features: Inventory, creating event and statistics reports or forensic analysis, performing maintenance tasks or installing the DriveLock Agents.

With the help of the DOC Companion, you can easily access the Policy Editor. This allows you to edit and create policies, and access settings that are not yet available in DOC.

8.1 DOC Companion

The DriveLock DOC Companion is an app that serves as an interface between the DriveLock Management Console (DMC) and the DriveLock Operations Center (DOC). It enables performing a number of important DriveLock functions originally only possible with an installed DMC.

As of version 2022.2, the DOC Companion can also be installed using the DOC Companion Offline Installer.

The DOC Companion is accessed for the following functions:

- Create and edit policies
- Display the Resultant Set of Policies (RSoP)
- Display inventory data
- Unlock computers online and stop unlocking
- Configure the agent (not available for Managed Services)
- Show the agent's properties
- Check certificates for centrally managed folders

> ⚠ Warning: Once you select one of these actions in DOC, the first thing you need to do is **download** the DOC Companion App, save it, and then start the DOC Companion.

8.1.1 Starting the DOC Companion

When you start the DOC Companion the first time, the system distinguishes between two scenarios:

- If the DriveLock Managament Console (DMC) is already installed on your system, the actions that require DOC Companion are performed through the existing DMC.

- If no DMC is installed yet, the DriveLock DMC snap-in will be registered and executed as soon as you select one of the actions. This simply downloads a "DMC extension package" and does not install DMC locally.

After downloading the DOC Companion App, start the DOC Companion via the following dialog:

Connecting to local DOC Companion

If the DOC Companion has not started yet, please start it now.

Start DOC Companion

Cannot connect?
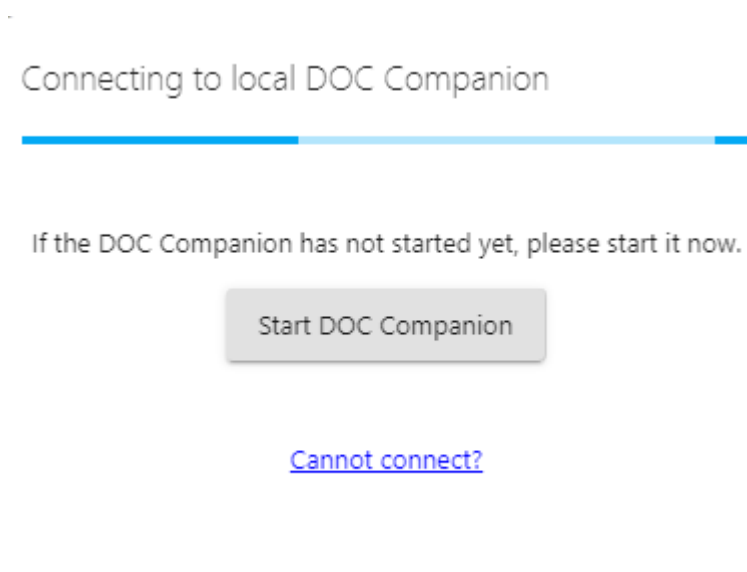
In the Start menu, you will see the **DriveLock DOC Companion** entry.

Every time you start the DOC Companion, the system checks if an update is available. If a newer version of DOC Companion exists, it will be automatically downloaded from the DriveLock Enterprise Service (DES).

Every time you exit the DOC Companion, you need to reconnect to the last channel you were using before you can run any actions.

8.1.2 DOC Companion Offline Installer

The DriveLock DOC Companion is also available as a separate installation package containing the Policy Editor. The package is intended for easier installation in larger system environments and also facilitates rollout during release processes. Unlike DOC Companion, which can be restarted over and over again, DOC Companion Offline Installer does not reload the Policy Editor, but installs it across all computers.

> 🗒 Note: Note that it is not possible to automatically update the components in this case.

It is possible to prevent users from starting or downloading the DOC Companion by selecting the option **Allow installation of the DOC Companion only via the offline installer**. This is useful if, for example, helpdesk users are not supposed to have access to the Policy Editor.
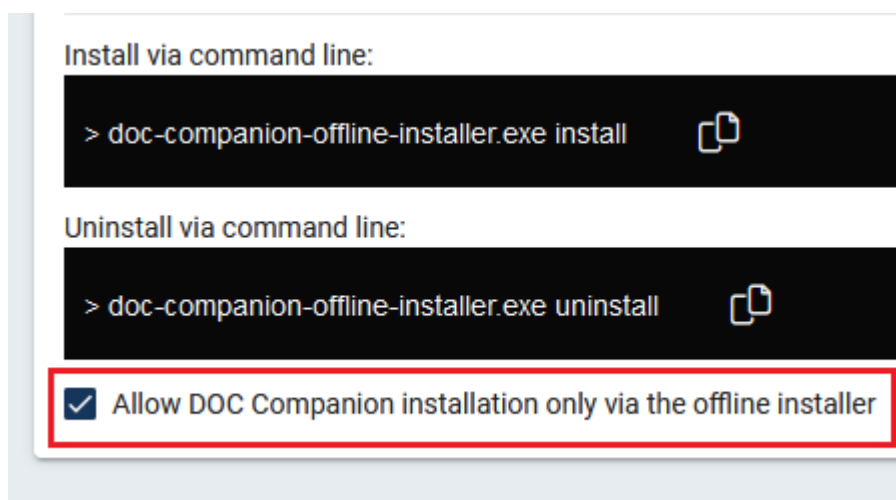
8.1.3 Troubleshooting and restrictions

Potential issues:

You can't connect to the saved DOC Companion?

- Click the **Cannot connect?** link. Make sure that the channel you are currently using matches the channel displayed in the taskbar. If this is not the case, you can generate a new channel via the link in the dialog.

You want to download the DOC Companion App again and/or use another user channel?

- Open the menu under your user account and click **Edit account**. Then click **Reset all view settings** and confirm.

> Note: Note that this will also reset other settings in your DOC views.

Restrictions:

We do not support proxies at present.

8.2 Windows authentication

Configuration: DOC -> Administration -> Accounts -> Windows authentication

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.

Please note that the following restrictions apply when logging in with Windows authentication:

- If a user belongs to the "Protected users" group, it is not possible to log in to the DOC using Windows authentication. However, logging in with a password works.

- It is also not possible to log in to the DOC via Windows authentication if users have logged in to Windows with a smartcard. At present, this is not supported.

8.3 SAML authentication

Configuration: DOC -> Administration -> Accounts -> SAML authentication

> ✒ Note: If you want to set up SAML on Microsoft Entra ID, you can find further information [here](#).

SAML is an open standard for authentication that can be used to implement single sign-on (SSO). With SAML, you can log in to Microsoft Entra ID, for example, and authenticate yourself as a user. The DriveLock Operations Center (DOC) uses this login, so you no longer need to log in with an email and password.

SAML refers to identity providers and service providers. For example, Microsoft Entra ID can be 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 the case of Microsoft Entra ID in particular, login is also supported via group membership of a Microsoft Entra ID group. In this case, the Microsoft Entra ID integration must be configured and a role assignment to a Microsoft Entra ID group must exist in the DOC. After logging in via SAML, an account is automatically created for the Microsoft Entra ID user on the DOC side. This requires configuring SAML authentication in DOC first. Then configure the Microsoft Entra ID integration and refer to the SAML configuration there.

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.

8.3.1 Using Microsoft Entra ID for SAML SSO

Configuration: DOC -> Administration -> Accounts -> SAML authentication

Before you can use Microsoft Entra ID for single sign-on with SAML, a few configuration steps are necessary.

> ✒ Note: You will need to copy some data during configuration. We recommend opening a text file in which you save the following information: redirection URL, content of the XML file, application ID, etc.

Please do the following:

1. Open the **SAML authentication** tab in the DOC under **Accounts** and create a new SAML configuration.

2. In the **Identity Provider** section, copy the **redirect URL** (or callback URL) for the identity provider settings into your text file.

3. Log in to your Azure portal and select **Microsoft Entra ID** in the **Azure services**.

4. Open the **App registrations** menu under **Manage** on the **Overview** start page and select **New registration**.
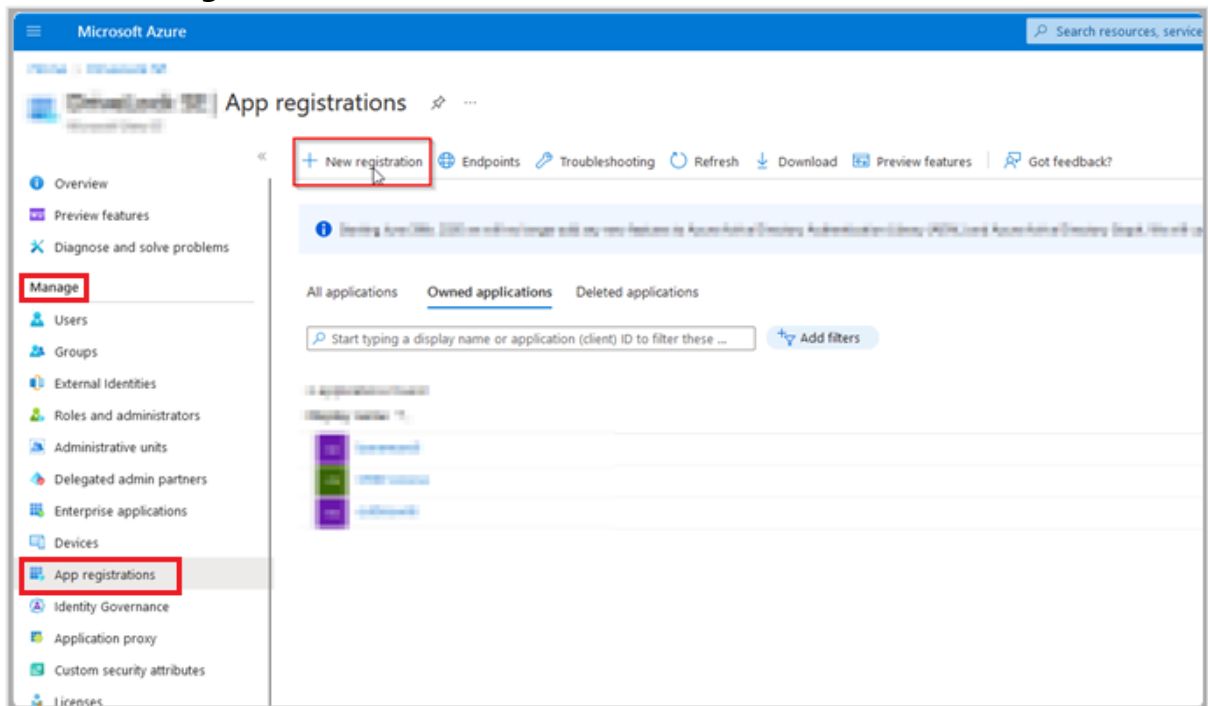
5. Register the application by entering a descriptive name and select the option **[...]** **Single tenant** under **Supported account types**. In the example below, the name is 'my-saml-configuration'. Also select the option **Single-page application (SPA)** under **Redirect URI (optional)** and then copy the redirect URL from your text file into

the field outlined in green.

Then click on the **Register** button.

6. Once the application has been created, you will be redirected to the **App registrations** start page. Select the **Authentication** menu item. Here you can check the redirect URL and adjust it if necessary. Check **ID tokens** (see figure) and save your settings.

7. Next, open the **Token configuration** menu item. Here you select **Add optional claim**.

8. Select the following options in the **Add optional claim** dialog:

9. Activate the Microsoft Graph e-mail authorization and then click on **Add**.

Some of these claims (email) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

☑ Turn on the Microsoft Graph email permission (required for claims to appear in token).

Add   Cancel
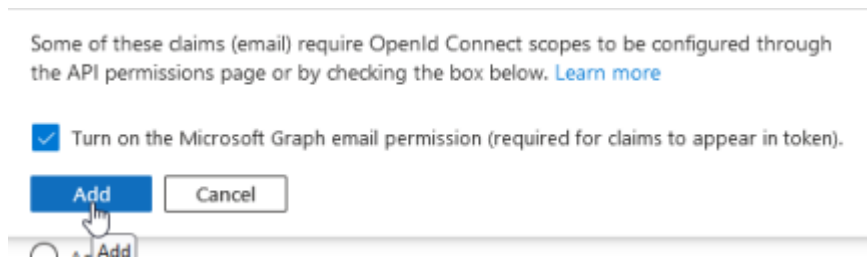
This allows you to set the Graphs authorization directly via the wizard:
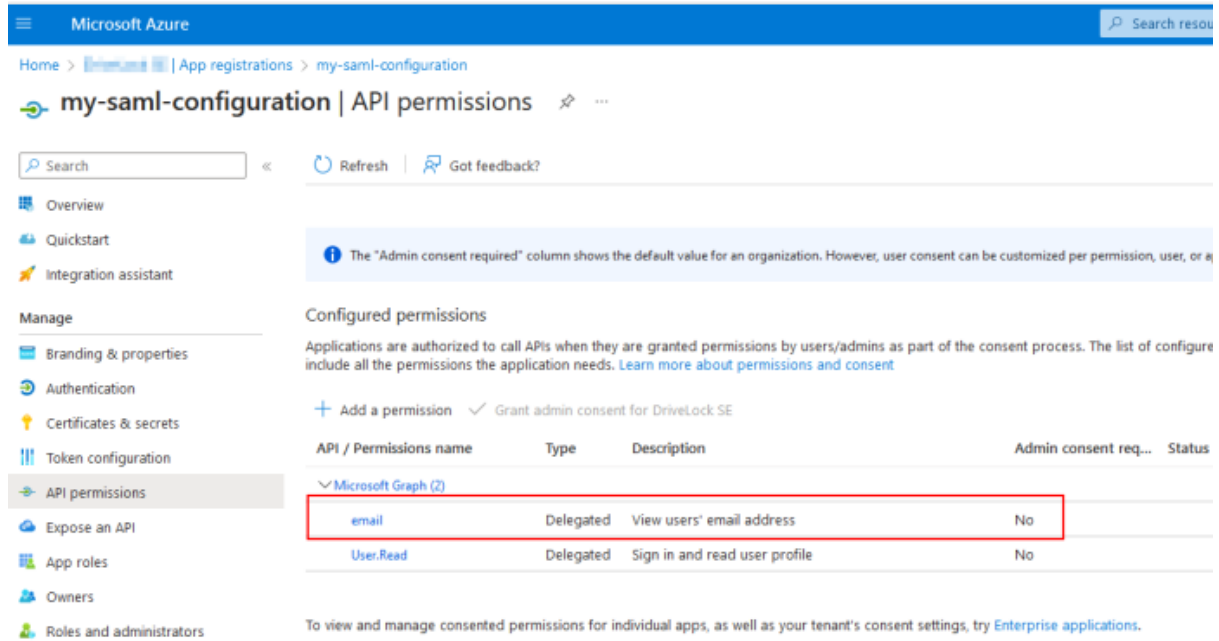
10. Once you have completed the above steps, click **Overview** again, which will take you back to the start page of your SAML app registration.
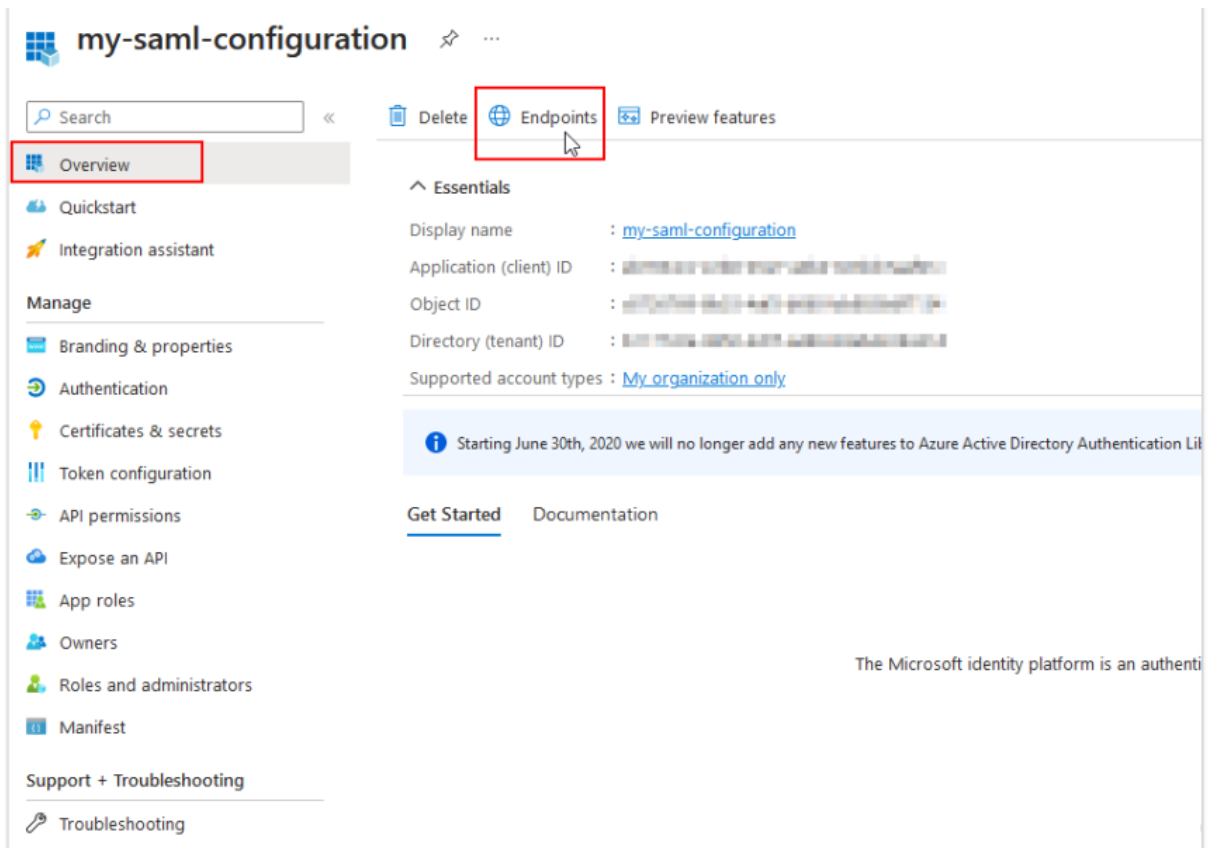
11. Here, click **Endpoints**. Various endpoint definitions are displayed.

12. Copy the URL to the XML file under **Federation metadata document** into your text file.

13. Return to the start page of your SAML app registration and copy the **application (client) ID** into your text file.
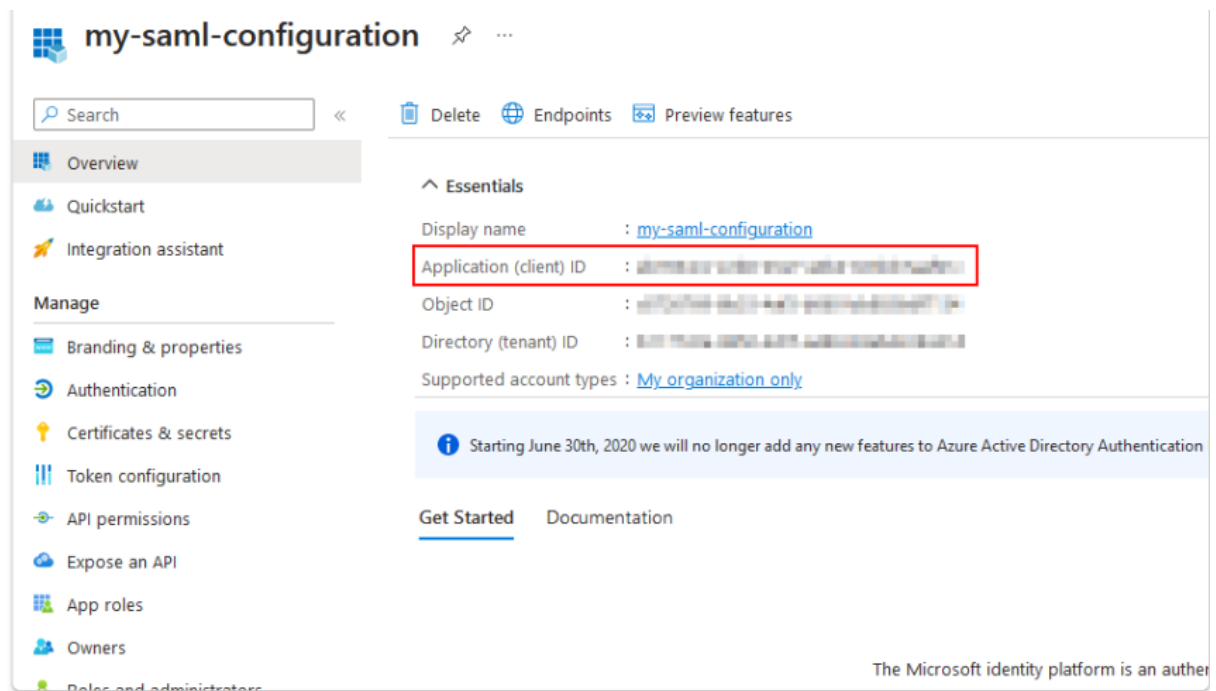
14. The configuration within Azure is now complete and you can now continue with the configuration in the DOC. To do this, go to the **SAML authentication** tab again (see Point 1).

15. In the **Service Provider** section, enter the copied Application ID from your text file under **Entity ID of the service provider**.
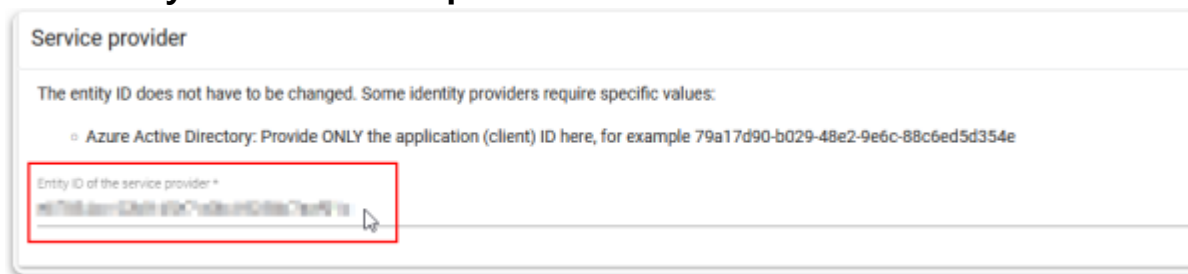
16. Finally, in the **Identity provider metadata** section, insert the URL from your text file and click **Import**.
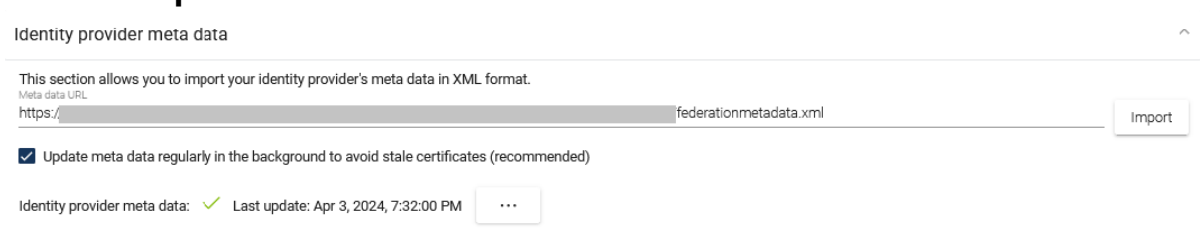
17. Make sure that you have set SAML as the active provider by ticking the **Active** box.
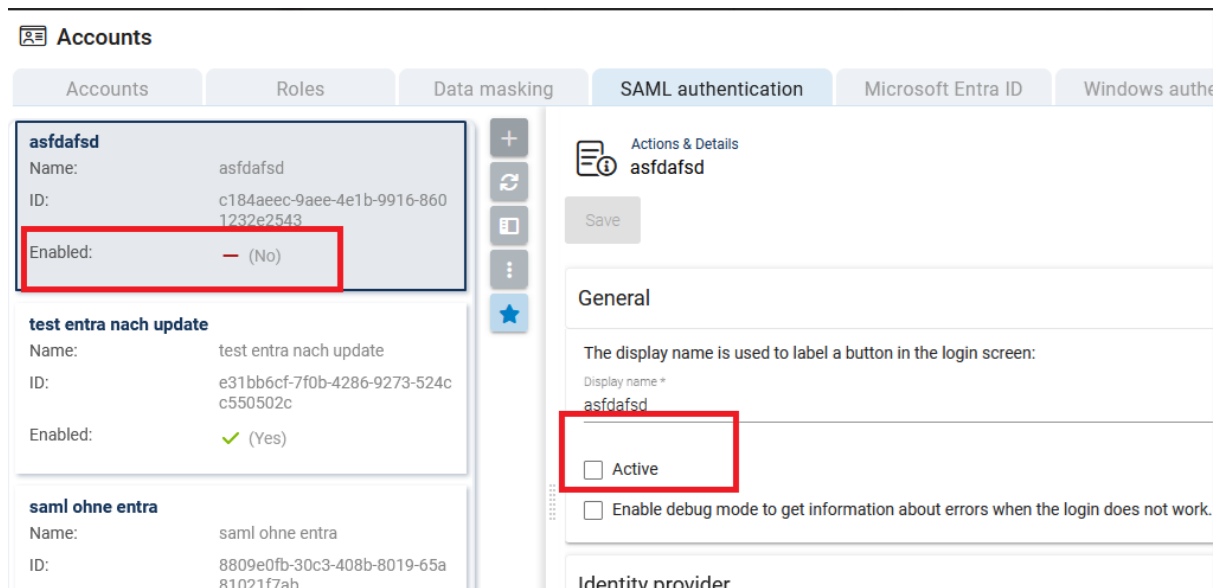
18. Save your SAML configuration.

19. Optional: If you want to use the Microsoft Entra ID integration in addition to the SAML configuration, you can link the SAML configuration you have just created with your Microsoft Entra ID configuration to enable logins via group memberships.

8.4 Password constraints

Configuration: DOC -> Administration -> Accounts -> Password constraints

This feature is currently only available for DriveLock Managed Services.

Password constraints can be used to configure password preferences that meet the security requirements of your organization. They apply to user authentication in the DOC. To manage password constraints, you must have the Manage accounts permission / role.

Password constraints are evaluated when

- a new account is activated,

- when the password is reset ("Forgot password" link on the login page), or

- the password is changed.

☑ Note: These constraints do not affect any existing passwords used by current users.

Currently, you can configure:

- Minimum password length

- Number of lower or upper case characters

- Number of digits and special characters

- Block recent passwords

8.5 Multi-factor authentication

Configuration: DOC -> User account in the taskbar-> Multi-factor authentication

For a more secure login procedure at the DOC, you can set up a multi-factor authentication method (MFA). A common authenticator app (e.g. on a smartphone) is required to generate a time-based one-time password (TOTP).

User side:

Users can select a convenient MFA method and manage it. They can also delete or deactivate it. In addition, they can specify that they are no longer asked for a code on a particular device for their particular login method (only again after 90 days).

To activate the MFA, users proceed as follows:

1. Open the menu under your account and select the **Multi-factor authentication** option.

2. The **Existing methods** dialog opens. To configure a new MFA, click ⊞ and follow the instructions in the dialog that follows.

> ⚠ Warning: Once the MFA is enabled, logging in to the DriveLock Management Console (DMC) with the same user is no longer possible. Note that this does not affect editing policies via the DOC.

On the administrator side:

Administrators can see which users have MFA enabled and can also disable it in an emergency.

> ✎ Note: Audit events are generated for the MFA actions to ensure they can be traced.

8.6 Reports in the DOC

Configuration: DOC -> Analytics -> Reports

In the DriveLock Operations Center (DOC), you can create reports in which you can track activities and trends. Reports can be saved as PDFs, printed or emailed to document the details of these activities.

> Note: Reports can only be created or managed with the appropriate permissions.

Event reports provide information on specific events and list them in a table. Event reports can also be customized, saved, released, printed, exported and provided automatically. You can also save the results in various output formats, e.g. as a PDF, CSV or JSON file.

Each report can be created according to a schedule and sent by email or saved in a directory (e.g. on a network share). This allows people to receive regular reports without needing access to the DOC. For example, to create an automated report for blocked drives, select the Device Control - Blocked Drives report template.

As an extension to report creation, data in reports can be displayed in plain text with the corresponding role permission ('Display masked data in reports in plain text'). Data masking must be activated as a prerequisite. Click here for more information.

8.6.1 Configure reports

If you are creating a report in DOC for the first time, click **Configure new report**.

Give your report a descriptive name and select any report template. If you want to design a report completely according to your own ideas, use the **Empty** template.

Your report is automatically opened in the **Contents** menu. To edit the report directly, click . You can now open a line menu, similar to editing the dashboard, to insert widgets, lists, charts, etc. into your report.

In the **Settings** menu, you can specify how many reports you want to create and how frequently, where you want to show the report, who you want to share it with and the format in which it is displayed.

Optionally, you can select the display of line numbers to ensure a better overview in the reports.

If data masking is activated you have the appropriate permissions, you have the option of specifying here that the data is to be displayed in plain text. Read more here.

Under **Created reports**, you can see how many reports have already been created. You can also download the report locally as a PDF here.

In the **Detail view** , the report is displayed as a preview image and can be opened by clicking on the image.

8.6.2 Unmasking data in reports

In order for masked data to be displayed in plain text in reports, certain requirements must be met:

- Data masking must be activated

- Permission to unmask data must be available

- The setting must be set individually for each report

Please note the following:

- If you want to send the report by e-mail, the data will remain unmasked and will remain visible to everyone who sees this e-mail. This may lead to a breach of data protection.

- Once you select one of the options in the **Share report** section, data masking is automatically activated again. This means that the option under point 2. below is not even visible for shared reports, even if all the requirements above are met.

Please do the following:

1. Under *Analytics -> Reports*, open the report you want to remove the data masking for.

2. Under Settings, check the option **Show data, [...] in plain text [...]**, as illustrated in the figure below.
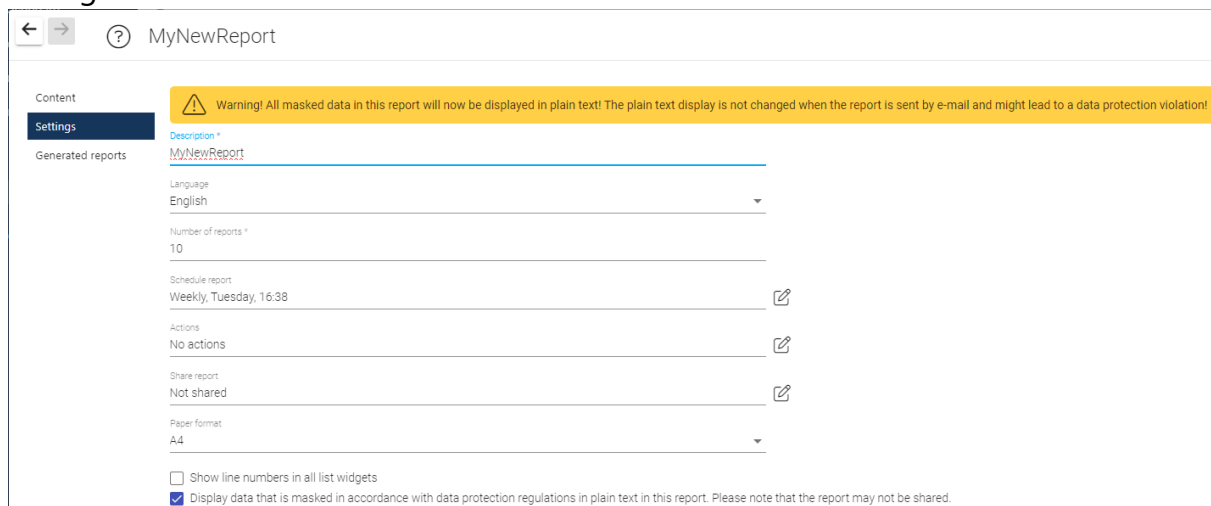
3. Your report is now displayed in a different color in the list of reports.
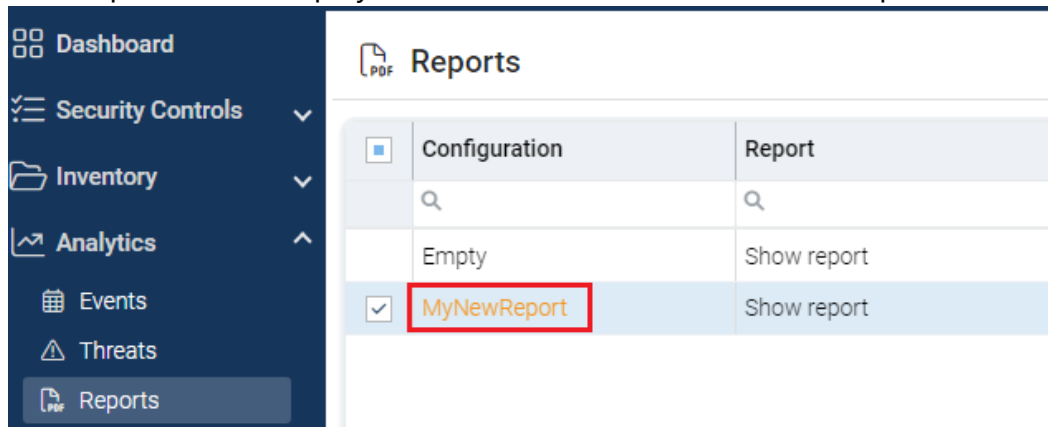
8.6.3 Taking over reports from other users

If a user is not available or cannot be deleted, it is possible to take over their reports so that they can be edited by another user.

To do so, you must have the general role permission ' Take over user configuration data'. You can only take over the reports of another user if you have this permission. This is configured here: *Administration -> Accounts -> Roles -> Role authorizations -> Account management -> Take over user configuration data*

The following menu command can then be selected:
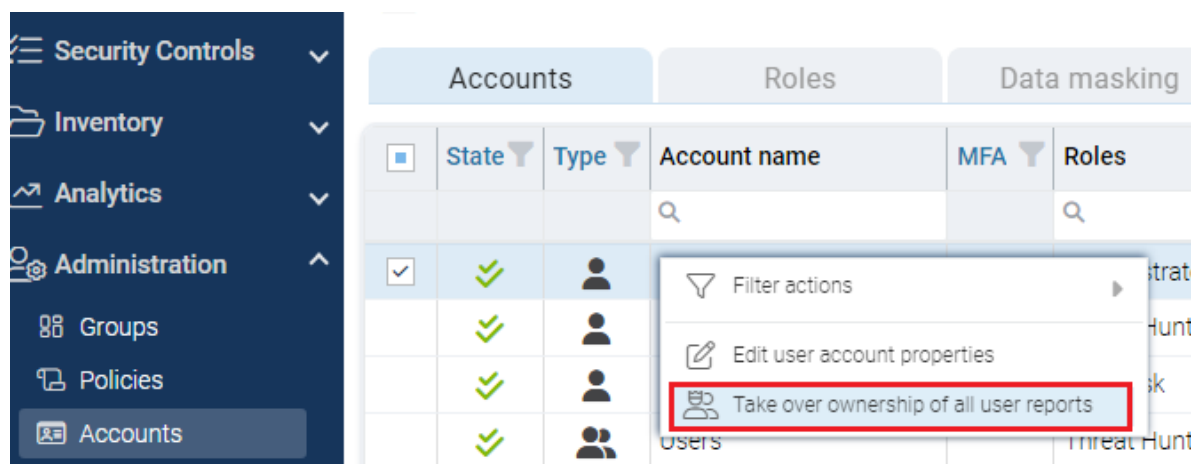
9 DriveLock Management Console (DMC)

The DriveLock Management Console (DMC) is a MMC snap-in and can be used both as a stand-alone console and as an additional component of an existing administrative configuration in a Microsoft Management Console (MMC).

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

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

After installing the DriveLock Management Console, you can start it via the Windows Start menu under **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**. Use the **context menu -> View -> Taskpad view** to switch back.

9.1 General notes

9.1.1 Changing the language of the user interface

Right-click DriveLock and select **All Tasks-> User interface language**. Then select the language of your choice under **User interface language in:**.

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

9.2 Agent remote control

DriveLock allows you to connect to a remote computer that already has 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.

> 🛑 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.

9.2.1 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 list from DriveLock Enterprise Service** option is set by default.

You can use the Show **computer as offline if 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:
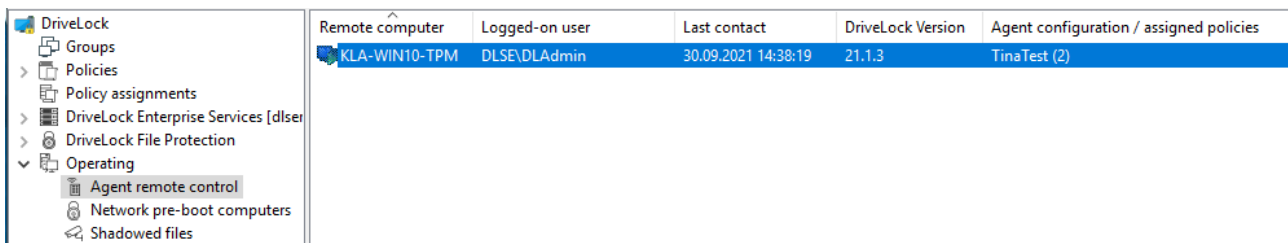
- **Always** : DriveLock Management Console connects exclusively through DriveLock
Enterprise Service.

- **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).

9.2.2 Show active DriveLock Agents
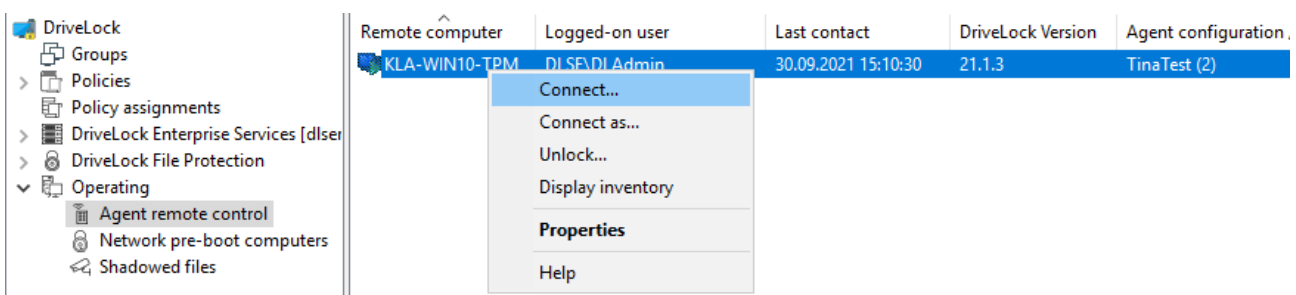
By default, the DriveLock Management Console displays all client computers it could find in the environment in the**Agent remote control** section of the **Operating** node.

9.2.3 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.

111
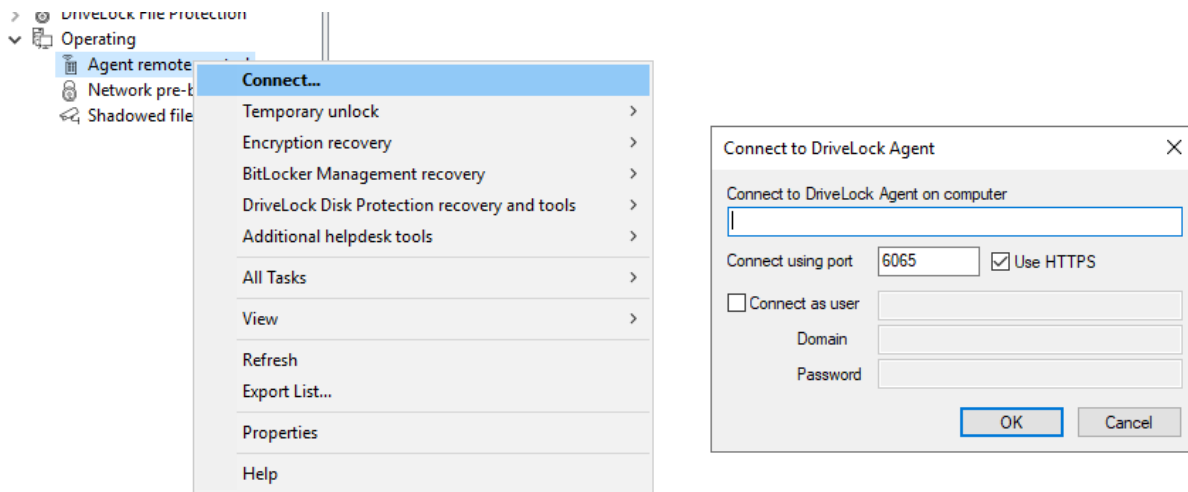
🖋 Note: To connect to a remote computer, you must allow incoming connections from TCP port 6064 and 6065 (default) and the DriveLock program in the firewall settings.

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.

9.2.4 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 info**rmation**, 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 further information on the tabs, please refer to the corresponding chapters.

9.2.5 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.

9.2.6 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.

9.2.7 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 change the agent's encryption or change the 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. Go to DriveLock Encryption for more information.

Click **Re-upload recovery key** if no recovery data is available 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.

9.2.8 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.

9.2.9 Enable 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.

9.2.10 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.

In the **DriveLock Operations Center (DOC)**, use the context menu command **Online unlock computer** under **Run action on computer** (see figure). After opening the DOC Companion, follow the steps below. This also applies to the context menu command Offline unlock computer.
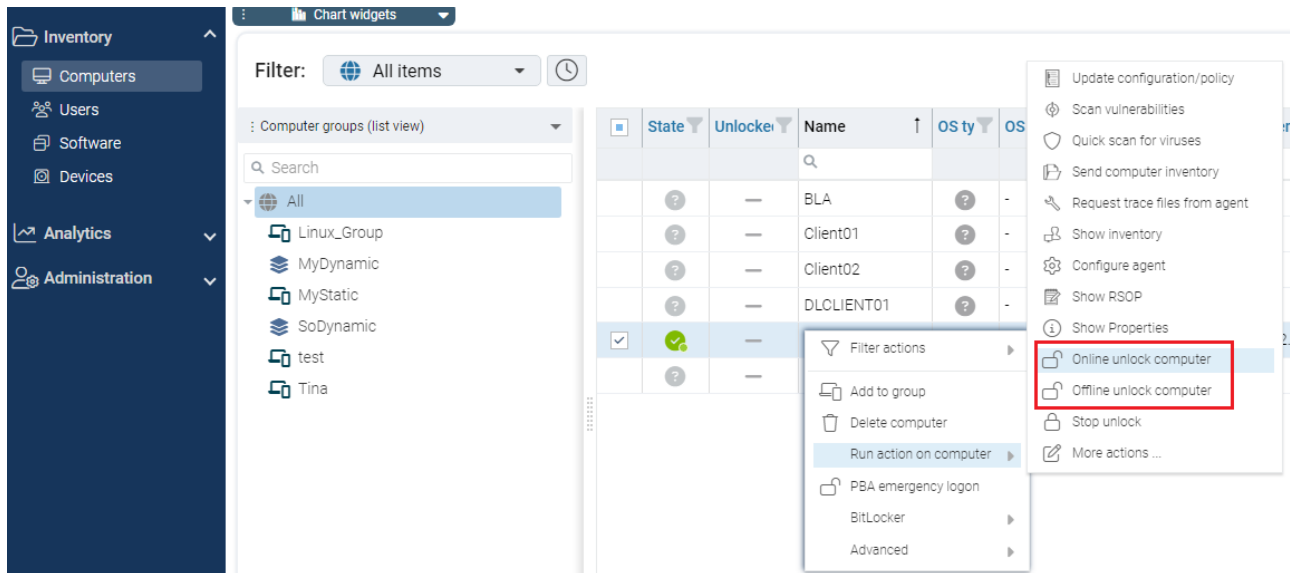
Proceed as follows in the **DriveLock Management Console (DMC**):
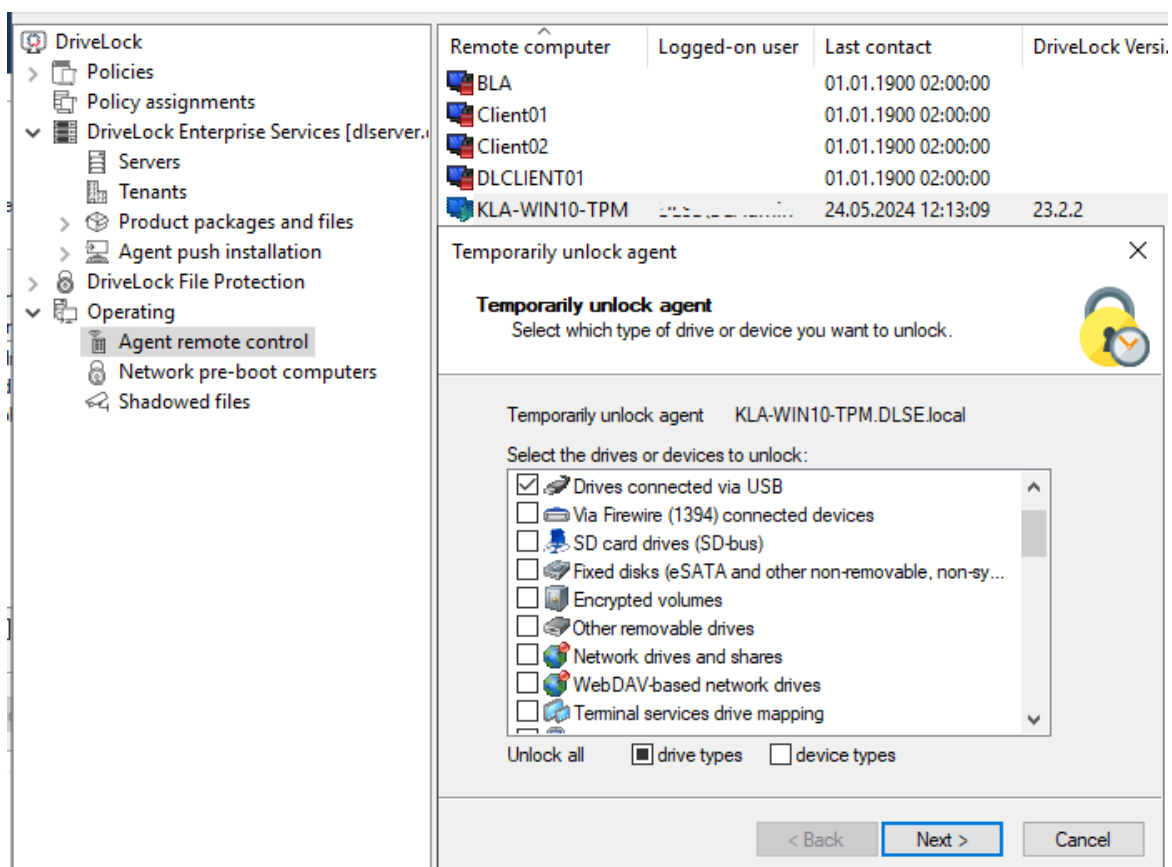
1. Either click the **Unlock temporarily** button in the agent's properties dialog or the menu command **Unlock temporarily...** from the context menu. If you want to unlock multiple agents, open the menu command **Unlock multiple agents...** in the context menu of the **Agent remote control** node using 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 for which enforced encryption has been activated. Further information on enforced encryption can be found here.
   - **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. Further information on Microsoft Defender Management can be found here.

> 📝 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 unlock offline agents

To unlock agents offline that are not connected to your network, you must follow the steps 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.
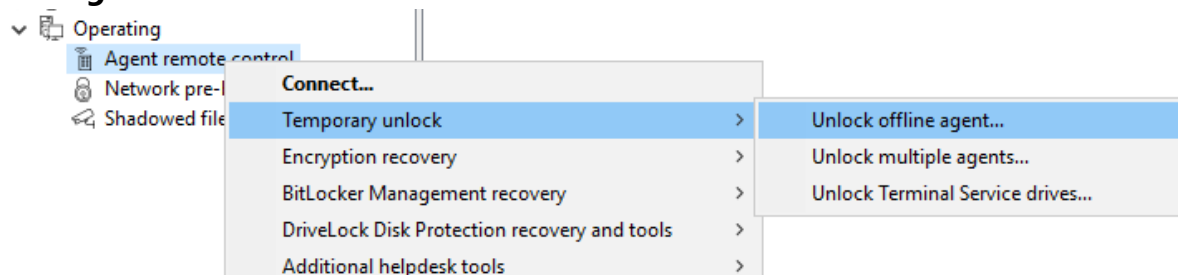
2. Now enter the password for the offline unlock, or select a certificate, depending on the setting you have specified in the offline unlock settings in your policy. You can import a certificate from a file or from the Windows certificate store on the local computer. To import a certificate from a file, 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.

9.2.11 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.

10 Managing the DriveLock environment

Keeping your IT infrastructure secure is the most important task of DriveLock. Designed for efficiency, the DriveLock environment features comprehensive certificate management, authorization concepts, various security settings and reporting options, API key management, Azure AD integration and flexible data masking options. In the on-premise version, you need to configure the security-related server components DriveLock Enterprise Service (DES) and clients yourself.

- **DriveLock Enterprise Service (DES)**

  The DriveLock Enterprise Service is the centerpiece of your on-premise security environment. It allows you to manage and enforce security policies on your DriveLock agents. When using DriveLock on-premise, you configure the DES yourself.

- **Tenants**

  Tenants are a way of dividing your DriveLock on-premise environment into logical units. This is particularly useful if you use DriveLock in a multi-tenant environment or want to isolate different departments or business units from each other.

- **Certificates**

  Different DriveLock modules use different certificates for the secure encryption, decryption and recovery of data.

- **Microsoft Entra ID management**

  The integration of Microsoft Entra ID into your DriveLock environment enables seamless management of users and groups. This facilitates the provision of security policies and the adaptation to the user structure of your organization.

- **Permissions in the DOC**

  Assigning roles and permissions allows you to control access to functions and data within the DriveLock environment. This ensures that users can only perform the tasks assigned to them.

  - **API keys**

    API keys are required to enable programmatic access to the DriveLock interfaces. They provide a secure way to access your environment without having to use a user name and password. Managing these keys allows you to control and monitor access to your DriveLock environment.

- **Security settings**

  These include securely adding agents via a join token, comprehensive firewall rules that control traffic to and from your DriveLock agents, password policy configuration, access control and data security settings.

- **Data masking**

  Data masking is an important measure to protect sensitive data and ensure that only authorized persons can access it. You can mask sensitive data in reports to protect confidentiality. This is particularly important when creating reports for different users or departments.

- **Reporting and event management**

  Environment management also includes continuous monitoring of events and reporting. DriveLock offers extensive reporting features that allow you to track security incidents and identify potential threats. This information is crucial for reacting quickly to security problems and taking proactive measures to improve security.

10.1 Server

The DriveLock Enterprise Service (DES) is the central server component of DriveLock. 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 Operations Center (DOC) or the DriveLock Management Console (DMC) as an interface for database queries and for saving and loading important files (e.g. recovery keys).

> 🗹 Note: On-premise customers can continue to configure the DES in the DMC and, starting with version 2024.1, also in the DOC. Managed Services customers can only make DES settings if they are using linked servers.

10.1.1 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 only occur in larger system environments (e.g. with multiple locations), when using DriveLock Managed Services and when installed by a Security Service Provider (SecaaS). In the vast majority of cases, it is not necessary to create a linked DES!

10.1.1.1 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 200,000 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.

The cache setting can be specified here: *Settings* ⚙️ *-> Backend -> Client settings -> Default values -> Events -> Processing -> Maximum permitted number of events*.

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

10.1.1.2 Linked servers

Linked servers are suitable for locations with insufficient Internet connections. They are directly connected to the central DES and can transmit a large number of events to the DES in a compressed and bandwidth-saving manner only at scheduled times.

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

Please find information on registering a linked DES here.

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.

10.1.1.2.1 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
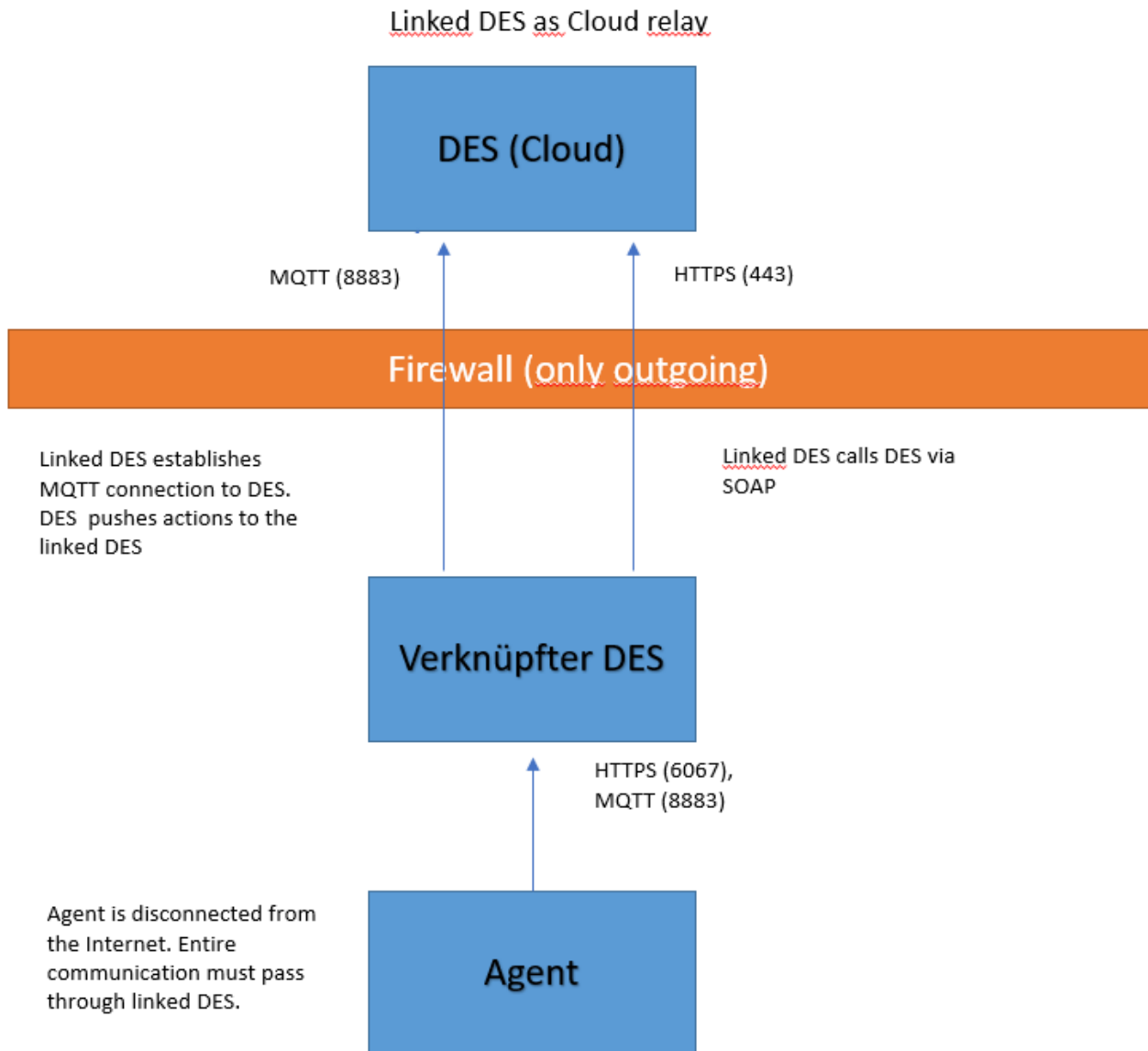
10.1.1.2.2 Register linked DES as cloud relay

Follow these steps to register a linked DES:

1. Generate an API key that allows the linked DES to be registered in the cloud tenant.

2. To do this, open the **APIs** view in the DOC via the settings (cog icon) and the **APIs** menu command. You can add an API key via the selection menu, see the figure below:
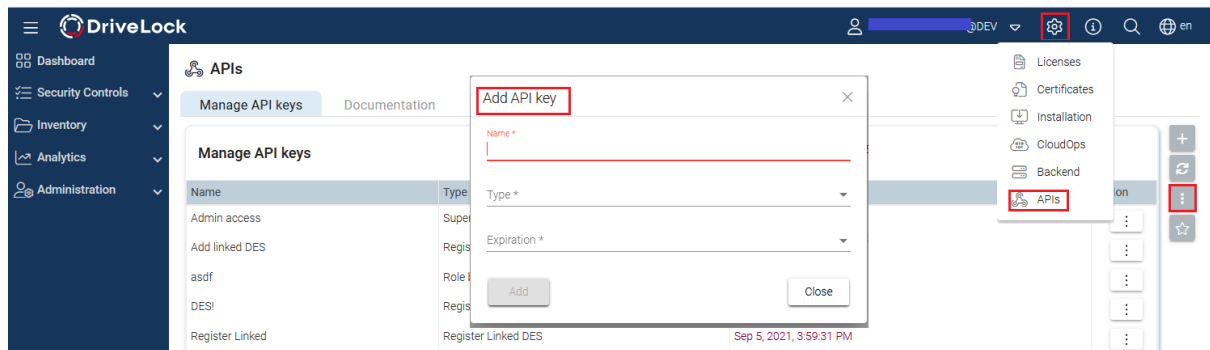
3. Create a new key of the type **Register linked DES.**.

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 Server Installation Wizard.

6. In the next dialog, copy the API key into the text box.

7. Click **Register server**.

10.1.2 Server settings

> Note: As of version 2024.1, the settings for all DES (central and linked) are very limited in the DriveLock Management Console (DMC). Most of the settings can now be found in the DriveLock Operations Center (DOC) at the following location: *Settings* ⚙ *-> Backend -> Server settings*.

In the drop-down list on the left-hand side, you can display or configure default values or go directly to a specific central or linked server in the list and make your configuration.

Default values are set at the top level, but can be overwritten for individual servers if required. Explanations for the respective setting can be displayed by activating the help button in the button bar.

All DriveLock Enterprise Services that are registered are displayed in the DMC under **Server**. In the properties dialog of a DriveLock Enterprise Service, only the Licenses tab remains active.

10.1.2.1 Proxy server settings

Settings ⚙️ *-> Backend -> Server settings -> Internet*

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:

- **Proxy server**: The specified proxy server is used to access the Internet. It may be necessary to specify a port, separated by ':', e.g. proxy.internal.example.com:8080

- **Proxy authentication**: If anonymous access via the proxy is not possible, this option is activated.

- **Proxy user**: This is the user who accesses the proxy server.

- **Proxy password**: The password that matches the user.

- **Proxy authentication mode**: Various authentication modes are available to authenticate against the proxy server.
    - **Windows authentication**: Windows integrated login, the service account of the DriveLock Enterprise Service is used for Internet access and not the proxy user.

    - **NTLM**: The user specified there is used for Internet access. The password is transmitted encrypted.

    - **Basic**: The user and password are transmitted in plain text.

> ✏️ Note: The selected authentication mode must be supported by the proxy server!

10.1.2.1.1 Proxy settings on the DriveLock Agent

You can also specify the settings for the proxy server 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 <auth-scheme>;<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 `drive-lock -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 or set with the `drivelock -setproxy` command can be deleted with `drivelock -remove-proxy`.

10.1.2.2 Network settings

Settings ⚙ *-> Backend -> Server settings -> Network*

You can configure network settings for the central DES and for linked DriveLock Enterprise Services.

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

> ☑ Note: Please note that the port specification can also be set in other places in the DriveLock Management Console (DMC). The certificate for the DES is also associated with the port!

The **address for agents** refers to the address that is given to the client as the server address during push installation, for example. 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. This setting has to be configured consistently and should be set to the same value for all DriveLock Enterprise Services.

10.1.3 Tasks of the DriveLock Server Setup Wizard

The DriveLock Server Setup Wizard on the DES Server has the following tasks:

- install and update the database on the central DES,

- to register the linked DES,

- specify the SSL/TLS certificate used by the DES for communication between servers and agents, and

- change the account used to run the DriveLock Enterprise Service.

The DriveLock Server Setup Wizard starts automatically after running the `DES64.msi` (new installation of the server - also known as MSI setup). It guides you through the installation or update of the database and sets up the certificate when you are installing the DriveLock Enterprise Server for the first time.

You can call up the wizard manually at a later time to perform all of the above tasks. You will find it in the DriveLock installation directory (e.g. C:\Program Files\CenterTools\DriveLock Enterprise Service\DriveLock Server Setup Wizard.exe)

> ☑ Note: As of version 2024.2, the Database Install Wizard.exe and ChangeDesCert.exe tools are no longer available.

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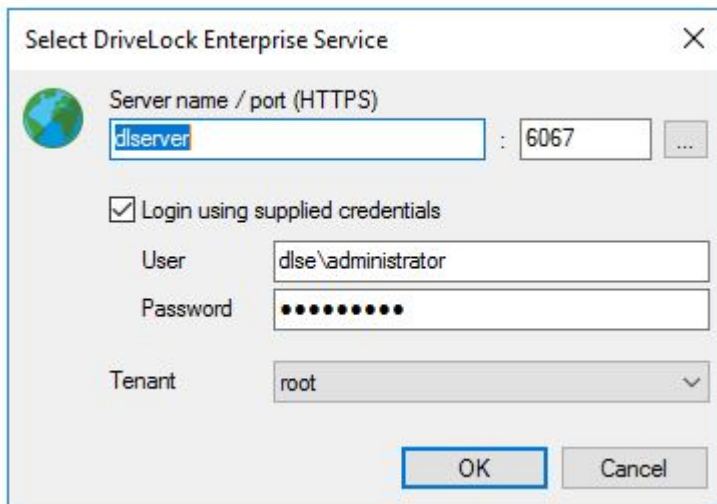
The DriveLock Management Console connects to the DriveLock Enterprise Service at various points to store information there (e.g. license data or centrally stored policies) or to retrieve data from the DriveLock Enterprise Service. First, you have to configure a connection to the DriveLock Enterprise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

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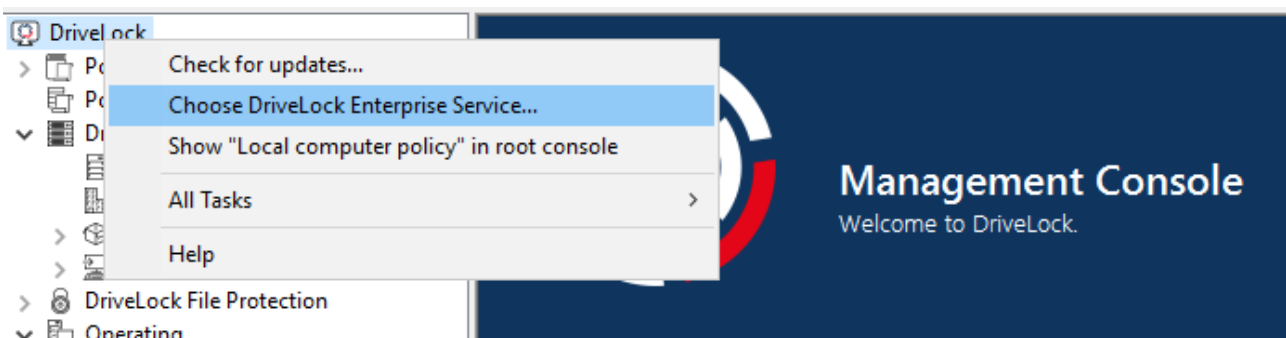
Or right-click **DriveLock Enterprise Services** and select **Choose DriveLock Enterprise Service...** from the context menu.

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

> 📝 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 was able to determine the DriveLock Enterprise Service when it was first started, it is already entered. 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 for the connection to the DES must also have the corresponding permissions. An authorized account / group can either be specified during the installation of the DES (see DriveLock installation), or it can be set up later via the DES 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).

10.1.5 Start actions on the DES

You can start actions manually via the context menu of a DES.

In the DriveLock Operations Center (DOC), select the server and then click ⸬ on the right:
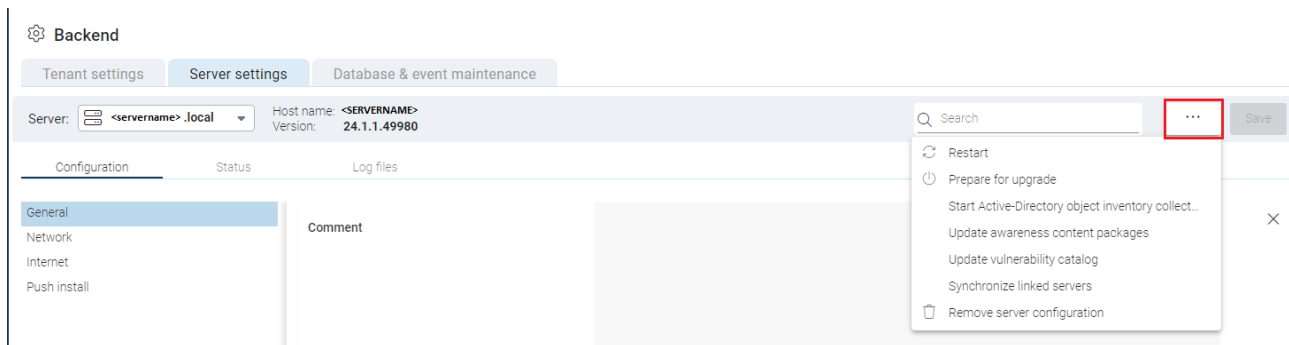
In the DMC, open the context menu of the server and select **All Tasks**:
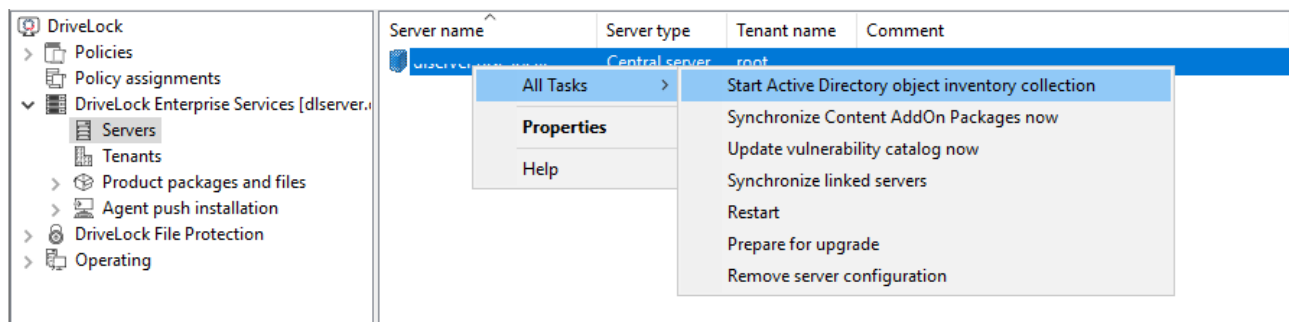
The following options are available:

1. **Start Active Directory object inventory collection**: The DriveLock Enterprise Service automatically identifies all computers, users, OUs and groups in the current domain once every 24 hours and compares them with the data stored in its database (synchronization).

2. **Update awareness content packages**: If you use Security Awareness, you can use this command to update the content packages and then download them to the DES.

3. **Update vulnerability catalog now**: If you are using the DriveLock Vulnerability Scanner, you can use this command to update the vulnerability catalogs.

4. **Synchronize linked servers**: Select this command if you want to synchronize various 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. The DES now processes all pending events. You can get an overview via the taskbar icon:
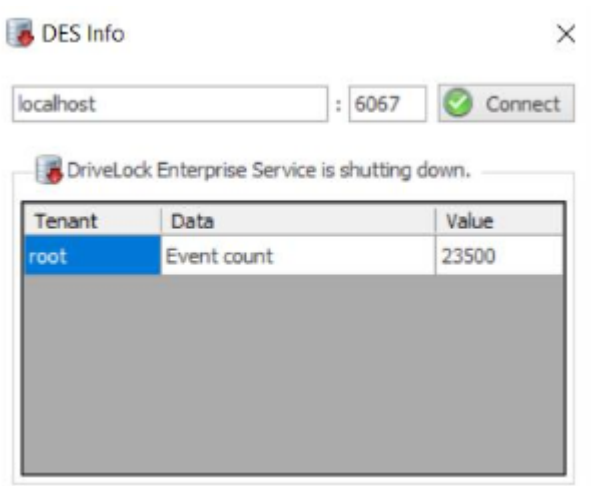
Once all pending events have been processed, you can install the DES-MSI.

> ☑ Note: We recommend this procedure in large environments.

7. **Remove server configuration**: This command deletes the complete server configuration. This is useful, for example, if you want to remove servers that are not in use.

Please note that as of version 2024.1, the settings for activating the debug log can no longer be found in the manual actions, but in the server settings in the DOC.

10.1.6 DES status

You can display the **status** of a particular server in the DOC. Here you will find all information about the server. The log files are also located next to it.

⚙ Backend

Tenant settings	Server settings	Database & event maintenance

🖳 Server ▾	Hostname: **SERVER**
	Version: **24.1.0.49326**

Configuration	Status	Log-Data

Status:	**Running**
Timestamp:	**Apr 23, 2024, 5:08:48 PM**
Path:	**C:\Program Files\CenterTools\DriveLock Enterprise Service\DES.exe**
Version:	**24.1.0.49326**
Started at:	**Apr 23, 2024, 12:26:37 PM**
Local time:	**Apr 23, 2024, 5:08:48 PM**
CPU usage:	**4%**
Processor count:	**2**
Working set (memory):	**226.63 MB**
Total memory:	**4.00 GB**
Available memory:	**715.63 MB**
Handles:	**1483**
Threads:	**44**
Free space on C:\	**62.66 GB**

In the DMC, you can monitor and check the accessibility of the DriveLock Enterprise Service using the DES taskbar icon. If the service is not available, this is shown 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.
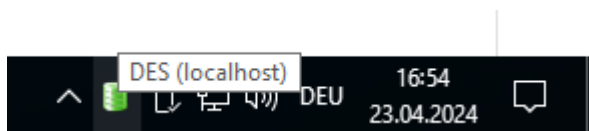
You can see different connection information like the address, database server, database type, database name or its version. Right-clicking on the icon opens a context menu that allows you to quickly restart the DriveLock Enterprise Service or perform actions useful for support.

10.2 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. This logical and physical separation is referred to as multi-tenancy. 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").

In the **DriveLock Management Console (DMC**), the default tenant of a server can be selected via **DriveLock** -> Right-click -> **Select DriveLock Enterprise Service...** -> <Select server> -> **Tenant** .

In the **DriveLock Operations Center (DOC)**, the Tenant settings can be found in the Settings 🔧 under **Backend**.

10.2.1 Creating or deleting a tenant

The default tenant **root** is created automatically as soon as you have completed the installation of the DES and the databases.

To create another tenant, right-click on Tenants under DriveLock Enterprise Services and select **New** and then **Tenant**.
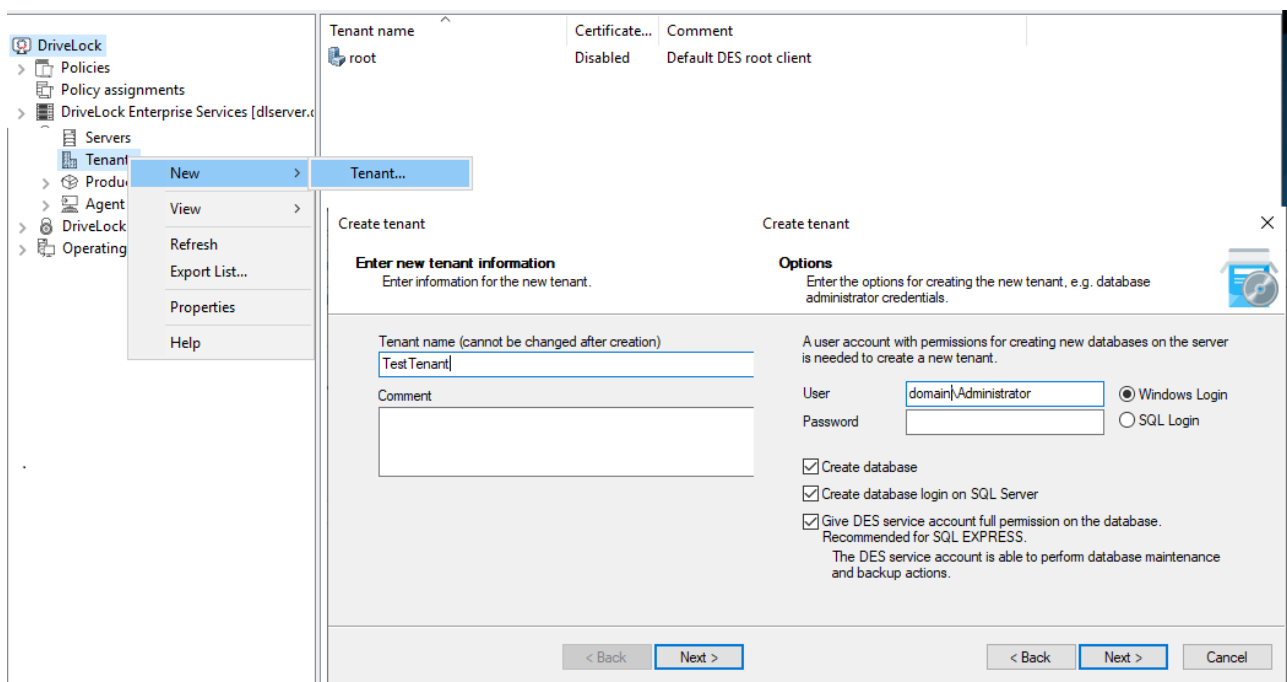
Specify a name for the new tenant. It must not contain any special characters or umlauts. The maximum length of the name is limited to 50 characters.

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.

10.2.2 Tenant settings

Configuration: DOC -> Settings ⚙ *-> Backend ->Tenant settings*

> ☑ Note: You can display information on the individual settings directly by clicking the help button in the button bar.

Explanations of individual settings:

Telemetry data

This is diagnostic data that DriveLock uses to obtain information about the use of the functions and properties of the DriveLock environment (e.g. licensing data, number of DriveLock agents, database server version). They are an important means of improving the product. No personal data is transferred or stored during data collection.

The setting can be deactivated by selecting the **Defaults** option in the **Tenant settings** and then deactivating **Send telemetry data to DriveLock**.

> ☑ Note: Please note that this setting is automatically activated starting with version 2024.1 and is set to activated again with every new update.

E-mail

In the **E-mail templates** section, you can customize all the templates provided by DriveLock according to your own requirements. This also applies to the texts for event notifications or invitation e-mails for security awareness campaigns.

Maintenance

10.2.3 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.

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

10.3 Active Directory 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 Enter-

prise 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.

There are two ways to configure the AD inventory.

1. AD inventory is collected from the server
   Configuration: DOC -> Settings (cogwheel) -> Backend -> Server settings -> General -> AD inventory
   With this option, the DriveLock Enterprise Service automatically determines the AD inventory of the server's current domain once every 24 hours. It is stored in the tenant assigned to the server (for central DES, this is the 'root' tenant). This action can also be triggered manually.

2. AD inventory is collected by the DriveLock Agent (per tenant)
   Configuration: DOC -> Settings (cogwheel) -> Backend -> Client settings -> Inventory -> Activate automatic AD inventory via agents
   With this option, the DriveLock Enterprise Service automatically determines an agent for each domain known in the database. The identified agents collect the AD inventory and send it to the DES.
   You can also initiate this action manually for a selected agent in the DOC by choosing the following from the context menu: Run action on computer -> More actions -> Show all actions -> Category: Inventory -> Send Active Directory inventory.

10.4 Certificates

Configuration: DOC -> Settings ⚙ -> Certificates

Certificates can be stored 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

135

Default certificate name	Intended use	Private key	More information
DLBlEmer-gencyLogon.cer	Emergency login with BitLocker	DLBlEmer-gencyLogon.pfx	BitLocker certificates
DLFDERecovery.cer	Data recovery with Disk Protection	DLFDERecovery.pfx	Disk Protection Certificates
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	Temporary offline	*Matching private key*	more information

Default certificate name	Intended use	Private key	More inform-ation
name e.g. Tem-pUnlockCert.p7b	release		

10.5 Ways to use Microsoft Entra ID integration

Companies managing their infrastructure and user permissions centrally via the Microsoft Entra ID cloud platform (formerly Azure Active Directory or Azure AD) will be able to synchronize the existing groups into DriveLock and use them to assign access permissions and DriveLock security policies in the same way as previously possible with a local Active Directory.

Computer groups from Microsoft Entra ID are treated like static groups in DriveLock, except that they are maintained automatically by synchronization and not manually by the user.

It helps you achieve the following goals:

1. **Assign policies to computer groups**

   Computer groups that are connected to a Microsoft Entra ID serve 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 Microsoft Entra ID groups in the same way as static groups. Rules for individual computers need to be created using the computer name.

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

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

4. **Login based on roles and permissions via Microsoft Entra ID user groups**

   When assigning roles, you can select a Microsoft Entra ID user group. When a user logs on to the DOC via SAML, the DES determines the Microsoft Entra ID user groups

of which the user is a member. The remaining logic is no different from standard AD.

5. **Self-service**

Microsoft Entra ID user and computer groups can be used in the self-service unlock

10.5.1 How to configure Microsoft Entra ID integration

Configuration: DOC -> Administration -> Accounts -> Microsoft Entra ID

For information on using the Microsoft Entra ID integration, please refer to this overview page.

By integrating Microsoft Entra ID, selected groups and their members are synchronized from Microsoft Entra ID to DriveLock. Please follow some configuration steps in Microsoft Entra ID first and then add the generated data to the corresponding text boxes in the DriveLock Operations Center (DOC).

> 📝 Note: You will need to copy some data during configuration. We recommend opening a text file in which you save the following information:
> Primary domain, Tenant ID, Application ID, Client secret value

Please do the following:

1. Log in to your Azure portal and select **Microsoft Entra ID** in the **Azure services**.

2. On the **Overview** start page, copy the entries in the **Tenant ID** and **Primary domain** fields and paste the copies into your open text file.
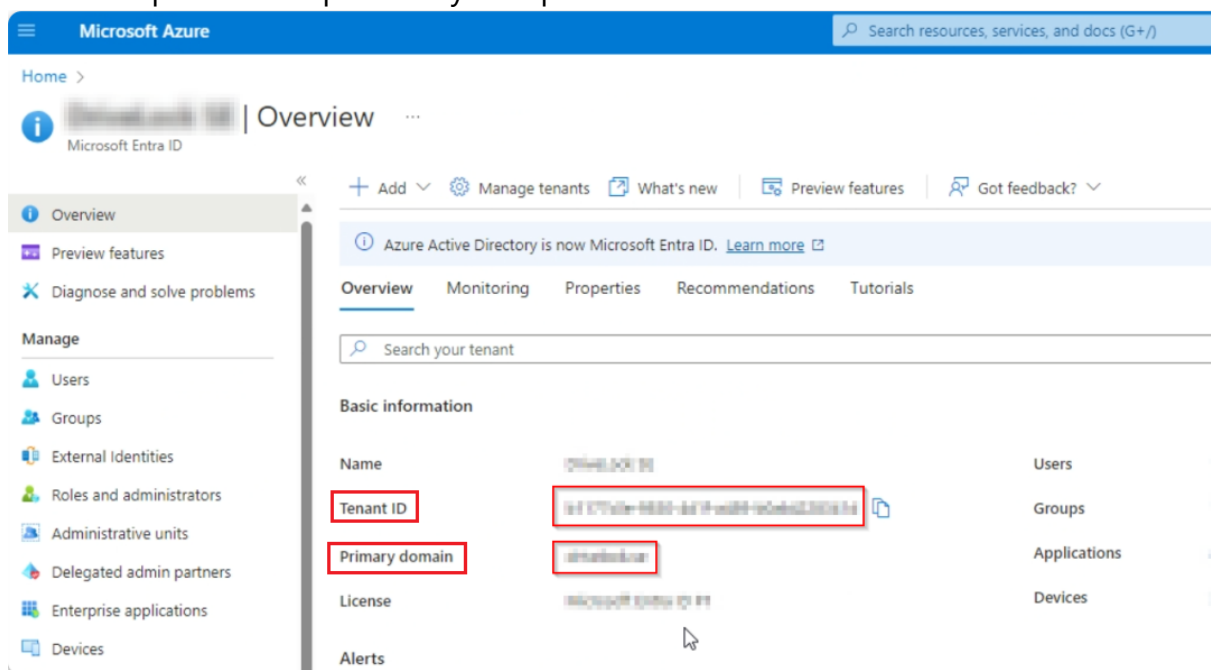
3. Then click on **App registration** in the **Manage** menu and select **New registration**.
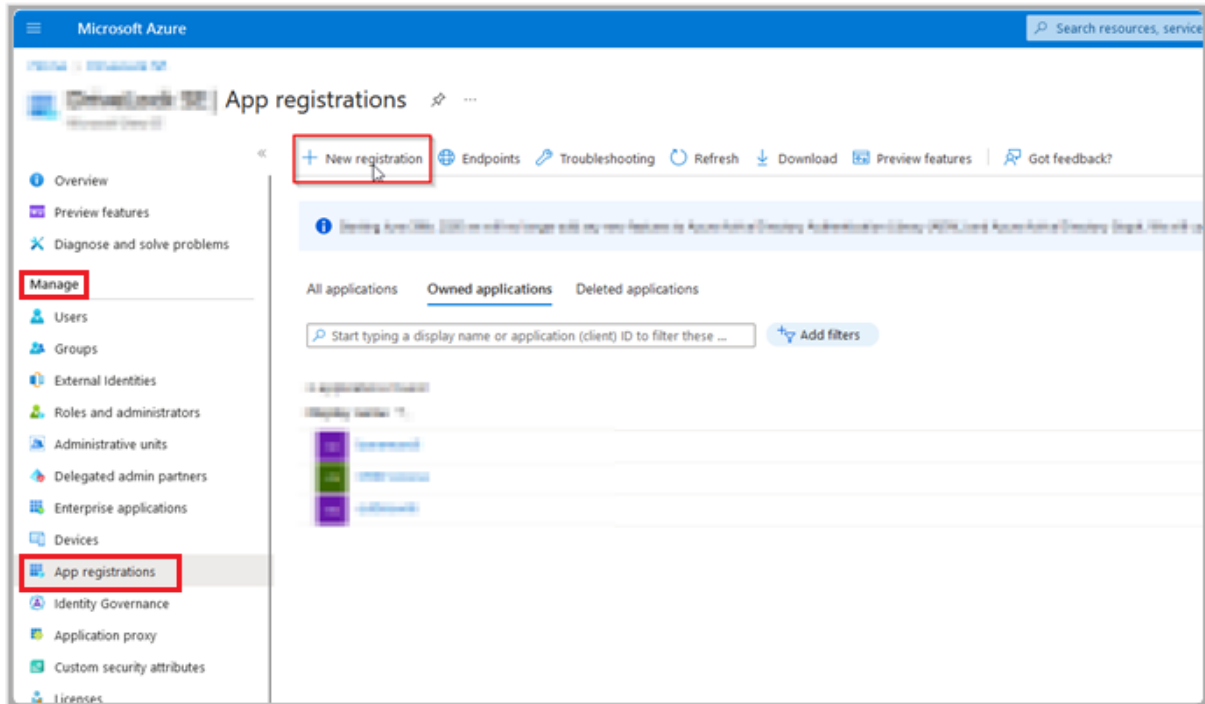
4. Register the application by entering a descriptive name and select the option **[...]
single tenant** under **Supported account types**. In the example below, the name is
'my-entra-ad-connection'. Click **Register** to create the application.

5. You will then be redirected to the **App registrations** page. Copy the **application ID** and paste it into your text file.
   In the example below, the **application ID** has the value 22657c93-2598-4423-820f-5f5ca28e4ac8.
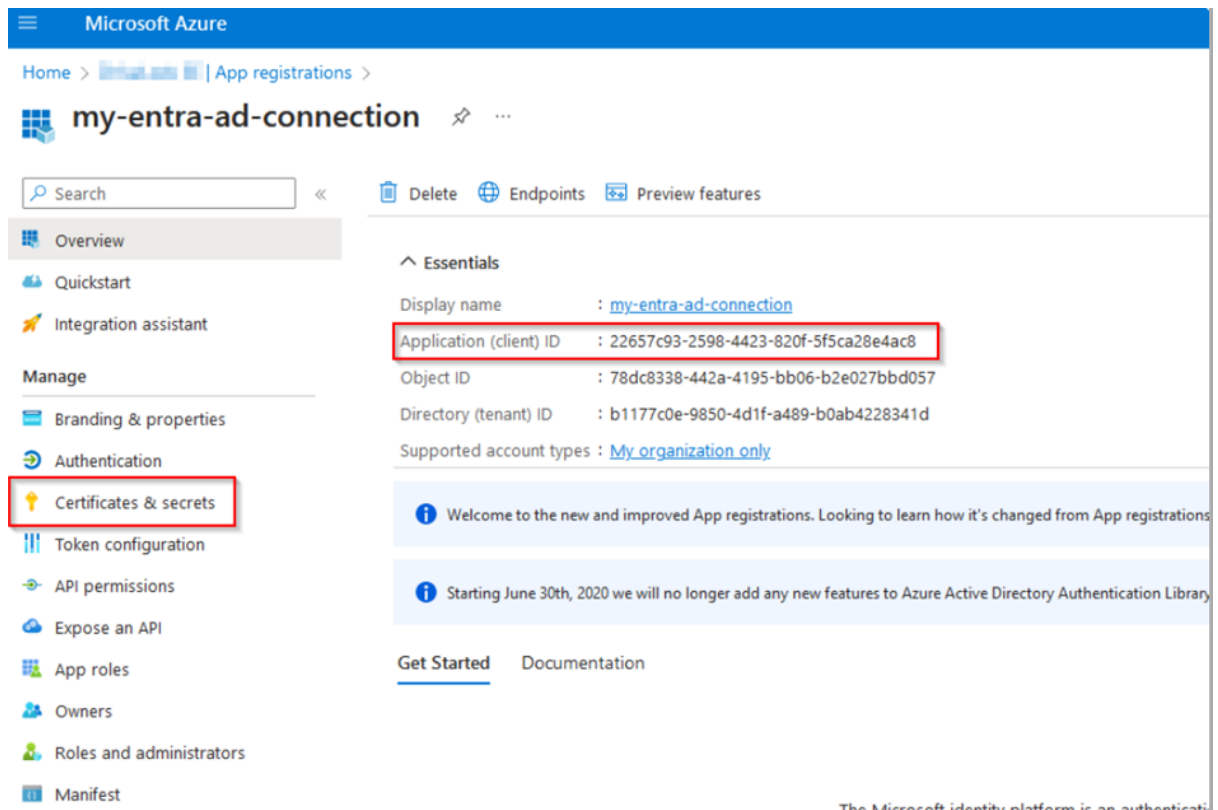
6. Next, create a new secret client key. To do so, select the **New client secret** option in the **Manage** menu under **Certificates & secrets**.
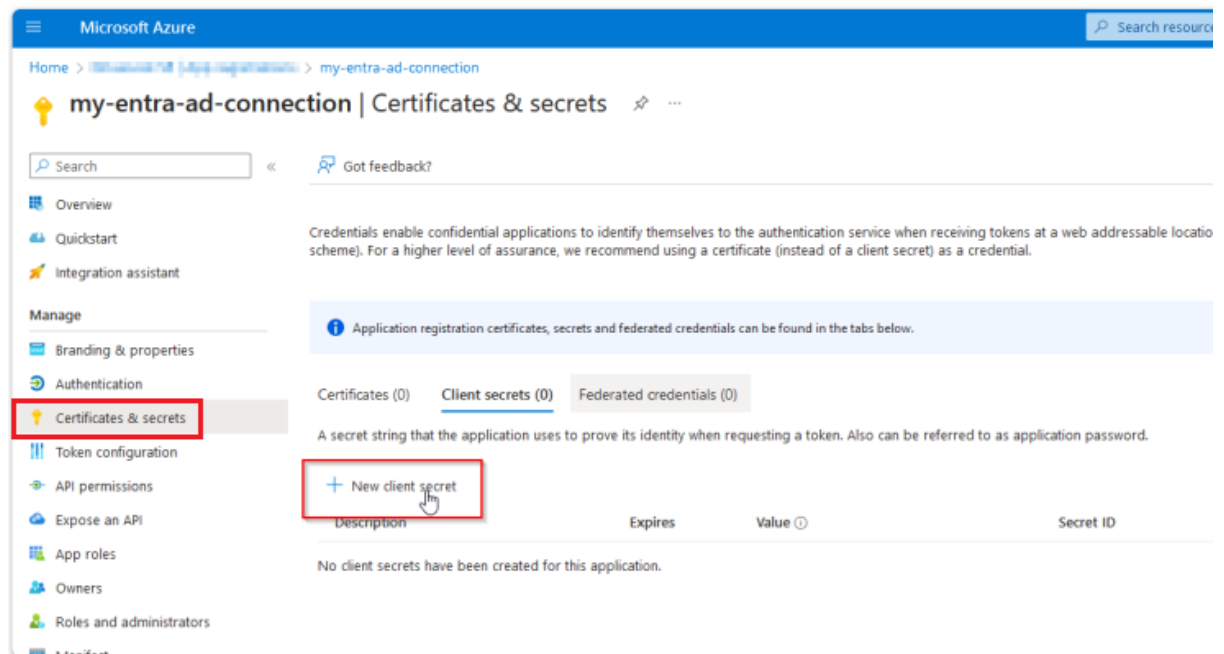
7. Create a new client secret with a name and an expiration date.
   In the example, the client secret **my-entra-secret** is valid for 6 months.

8. The client secret is now displayed under **Client secrets**. Copy the value and save it in a safe location. Please note that this value is only displayed once!
   In the example below, the value is pcd8Q~T4occKAWxBf9Z2F4co8TCrCQZ6xa5W.c2g.

9. Next, set the API authorizations. To do s, open **API permissions** in the **Manage** menu.

10. Select **Add a permission** and the Microsoft API **Microsoft Graph** provided on the right. Here you select **Application permissions** as the authorization type.

11. Use the search function to search for **Directory** and then select the entries **Device.Read.All**, **Group.Read.All** and **User.Read.All**.

12. Your authorizations should now be set up as follows. Make sure that **Grant admin consent** is granted.

13. Save your entries and close the Azure Portal. Then go to the DriveLock Operations Center (DOC).

14. You now need your copied details in the text file.

15. In the **Administration** menu, open the **Accounts** submenu and go to **Microsoft Entra ID**. Click on the icon to add your new configuration.

16. Enter your **Primary domain** as the Microsoft Entra ID domain name, click **OK** and save your configuration.

17. Enter your **Tenant ID**, **Application ID** and your **Client secret** below.

18. You can then test your connection.

19. Then select the **groups** you want to synchronize. Microsoft Entra ID synchronization includes all groups and the subgroups they contain. To do so, check the box next to Enable **Microsoft Entra ID synchronization**.
    The synchronization takes place as follows:
    - once a day by default,

    - by right-clicking on a Microsoft Entra ID group and clicking the menu command **Synchronize with Microsoft Entra ID now** or

    - by selecting a Microsoft Entra ID group in the group management and clicking the menu command **Synchronize with Microsoft Entra ID now**.

    > ☑ Note: If you want to manage the groups completely on the Microsoft Entra ID side, we recommend creating a "Microsoft Entra ID Sync Group" that includes all the groups you want to synchronize. Then you only select this group on the DriveLock side.

20. You can optionally create a **SAML configuration** with the Microsoft Entra ID configuration. This allows you to log in with Microsoft Entra ID users who have been assigned rights via membership of a Microsoft Entra ID group.

10.6 Data masking

Configuration: DOC -> Administration -> Accounts -> 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.

A special role permission (role) is required for activating or deactivating data masking.

Data can also be masked in reports or you can remove data masking that has already been activated.

> ☑ Note: Please note that data masking is not yet implemented for the macOS agent.

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.

- **With approval by**: If you use this option, you need to provide a contact person to authorize unmasking. In the text field below, you can enter the required 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 **Data masking mode** section you can specify which data you want to mask.

- **Full**: All user and computer names are 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 data protection, it may make troubleshooting more difficult.

- **Only user data**: 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.

  > Note: In environments where it is easy to draw conclusions between computer names and users, it may be useful to have the computer names masked.

- **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.

> ⚠️ Warning: Please note that changes to the data masking mode must always be saved to take effect.

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.

> 🖉 Note: Note that in the **Inventory** menu, in the overview of all **users** or **computers** , the respective names are always displayed in plain text. This is also the case when displaying group memberships. All other information is of course masked if set accordingly.

More options of data masking:

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).

Here you can also find the **Mask or unmask data temporarily** option for reversing the data masking. 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. This may be relevant if you want to display data for demo purposes only in an 'anonymized' way and need to mask it for a short period of time.
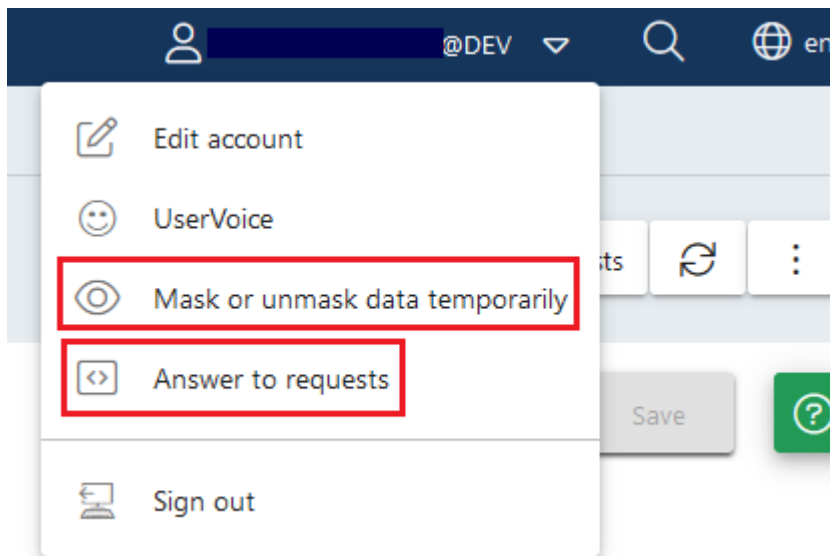
Applying data masking when filtering by "user name".

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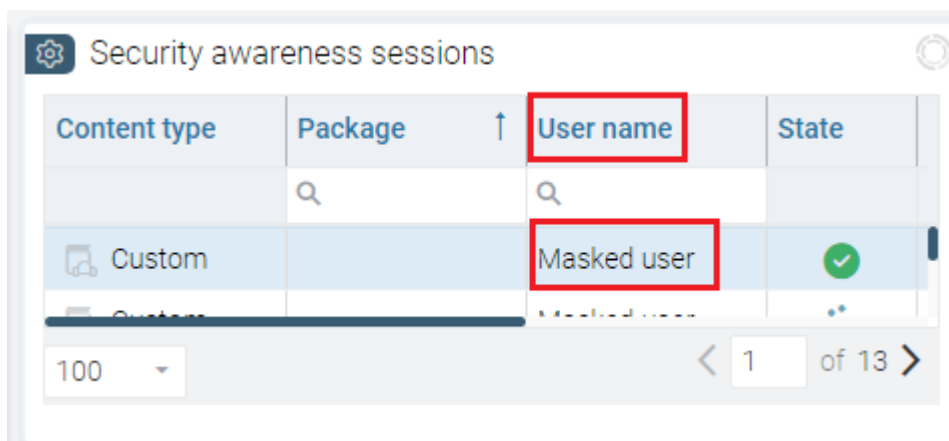
Additional notes

When data masking is disabled, you cannot cancel but temporarily enable data masking with the **Mask or unmask data temporarily** option. In the opposite scenario, where all data is currently masked, you cannot mask any data, but you can temporarily unmask the data.

Example: All the user data is masked, but the computer data is not. An administrator wants to identify the user when a specific event occurs, so here it would be useful to show the data temporarily. In this case, the **Mask or unmask data temporarily** option can be used. At the same time, a temporary masking of the computer data can be requested.

Changing the event masking configuration

For each event, you can change the data masking settings individually or by selecting multiple events.

These settings are convenient because they can be set quickly and are saved directly. This requires that the data masking mode is set to Individual.

When this is not so, you will get a message as shown below. Although you will be able to save your input, it will not take effect until the mode is globally set to Individual.

10.7 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.

10.7.1 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
File logging	Yes	Yes	Yes	Yes
Shadow copy	Yes	Yes	Yes	Yes
Requires DriveLock Agent locally	Yes	Yes	Yes	No
Requires DriveLock Agent	No	No	The virtual client is used	Yes

Function	FAT Clients	Windows Embedded Client	Virtual Clients	Thin Clients
on the TS			instead of the terminal server.	

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)

A virtual client is a virtual computer with 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.

10.7.2 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.

10.7.3 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 far do you go into detail? 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 lock 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....**
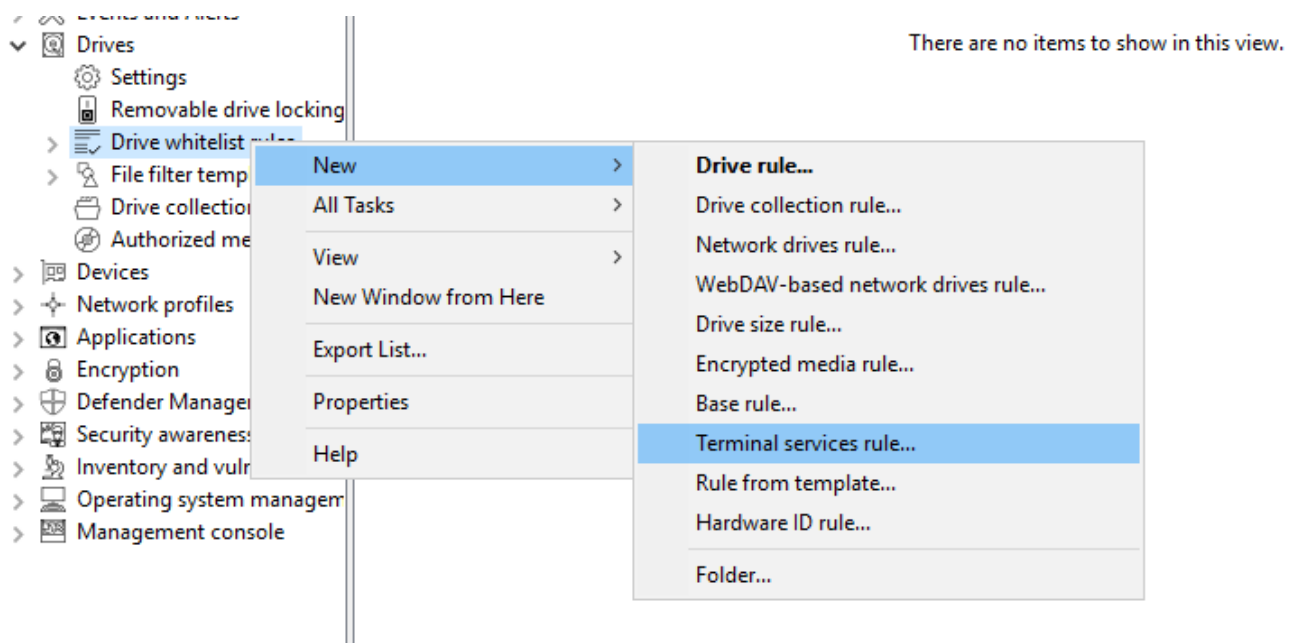
Next, select a letter from the drop-down menu and activate the appropriate protocol that is used in your environment. Permissions are assigned on the Permissions tab:

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.

10.7.4 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: Further information can be found under Application Control.

10.8 Permissions in the DOC

Configuration: DOC -> Administration -> Accounts -> Accounts or Roles

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).

User accounts and permissions can be defined in the **Administration** menu in the **Accounts** view.

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.

- Microsoft Entra ID accounts
  The groups and memberships of Microsoft Entra ID can be synchronized. In combination with the login via SAML, the user's group memberships are queried by Microsoft Entra ID. This enables role assignments to the Microsoft Entra ID groups in which the user is a member, similar to 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.

10.8.1 Manage API keys

Configuration: DOC -> Settings (cog icon) -> APIs

API keys provide programmable access to the DriveLock Enterprise Server (DES) interfaces. They are used for authentication, similar to a conventional user login, but using a key instead of a user name and password.

> ✒ Note: See the **Documentation** tab for details on the interfaces.

Types of API keys

1. Role-based permission
   - Recommended use for controlling and assigning specific permissions
   - Creates a technical user with the name of the API key

- Possibility to assign rights in detail by assigning roles

2. Supervisor
   - Enables unrestricted actions without being limited by rights and roles
   - This type of API key is only available in the on-premise version

3. Register linked DES
   - Enables the registration of a linked DES
   - Only available in the Managed Services version
   - No need with existing standard proxy that supports WebSockets

Possible actions

- You can create a new API key via ⋮ or ＋.

- Click the ⋮ menu in the **Action** column if you want to change the runtime of an API key or regenerate it completely. If you change the runtime, the current key will be updated. Regenerating creates a completely new key that can be used independently of the old key.

Conceptual design of an API

Handling an API in the DOC is treated in the same way as handling an account. An API manager therefore needs the following additional roles and permissions to work effectively:

- An API manager can only pass on the permissions they own.

- The purpose of the restricted access is to prevent an escalation of rights and security risks.

- To ensure that no one is granted more rights than originally intended.

When appointed as an API manager, the individual automatically receives the following permissions. They allow the API manager to efficiently manage and control the APIs and the associated permissions and roles.

- `Accounts_Manage`
- `Accounts_Read`
- `Permissions_Manage`
- `Permissions_Read`

> ❗ Warning: It is essential for reasons of data protection and security that the API manager only passes on the rights that they hold themselves in order to ensure a high level of security and minimize risks.

10.9 Security settings for agent installations

Configuration: DOC -> Settings (cog icon) -> Installations -> Security settings

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	The agent tried to register with the invalid join token '%1'.

	audit	
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 exist-ing 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

10.9.1 Add new agents securely

Configuration: DOC -> Settings (cog icon) -> Installations -> Security settings

On the **Security settings** tab, you can specify that a DriveLock Agent may only be added to a client 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 com-puter. 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.

10.9.1.1 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.

10.9.2 DriveLock in virtualization environments

Configuration: DOC -> Inventory -> Computers

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.

10.10 Product packages and files (On-Premise)

10.10.1 Product update

You can access the DriveLock installation packages that are managed locally or available online in the DriveLock Management Console 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.

10.10.2 Check for updates

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

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:

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.

10.10.3 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.

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.

11 Policies

11.1 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 under Policies.

Architecture

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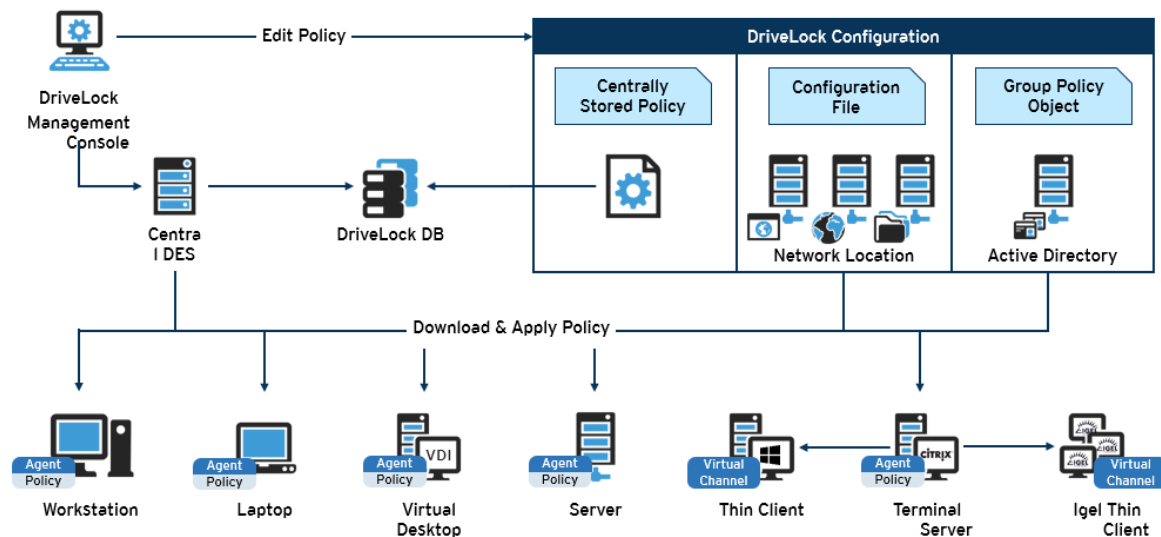
> ⚠ Warning: If using Microsoft Group Policy, we recommend that you also use the Group Policy permissions concept to ensure that only authorized administrators can view or modify the DriveLock configuration policy. If you are using configuration files, use Windows file access permissions for this. For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

11.2 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
Disk Protection laptops	Laptops	Disk Protection
Application Control Servers	Servers	Allowed applications for servers

11.2.1 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 an older DriveLock version than version 2020.2 installed, please select the **Centrally stored policy (compatible with agents prior to 2020.2)**... option. These agents cannot yet understand the new policy format.
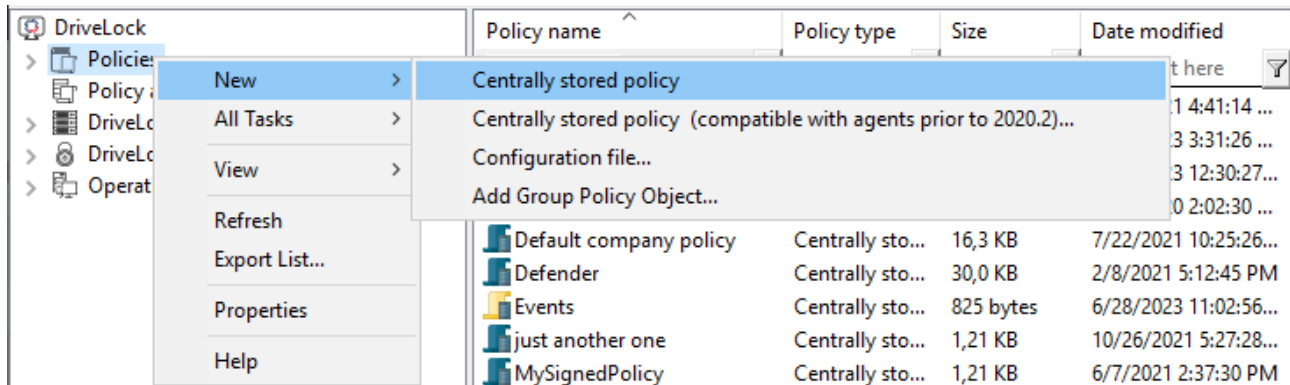
Assign a name, select a tenant, and enter a brief description of the policy.

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)
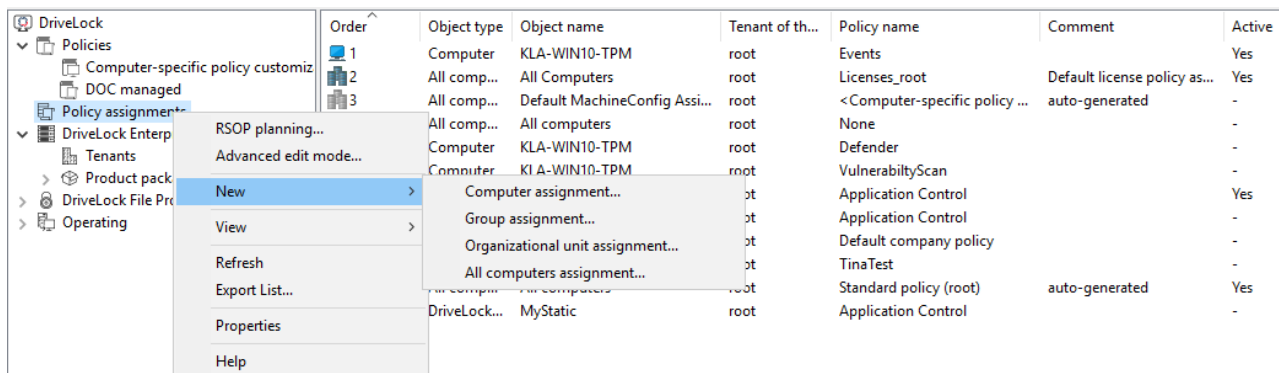
In the **Administration** menu, open the **Policies** view. Click the **Create policy** button. The DOC Companion will then start if it is not already running. Then the Policy Editor opens and you can edit, save, publish, and then assign the policy directly in the DOC.

11.2.2 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 **Policies** menu under **Administration**, you can create, edit, drag and drop and activate or deactivate policy assignments in the same way as in the DMC.

In the DOC, you can also assign a policy to all computers (this option is activated by default) or to specific targets (AD computers, DriveLock groups, Microsoft Entra ID groups, AD groups or OU containers).

11.2.2.1 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 (CRA)

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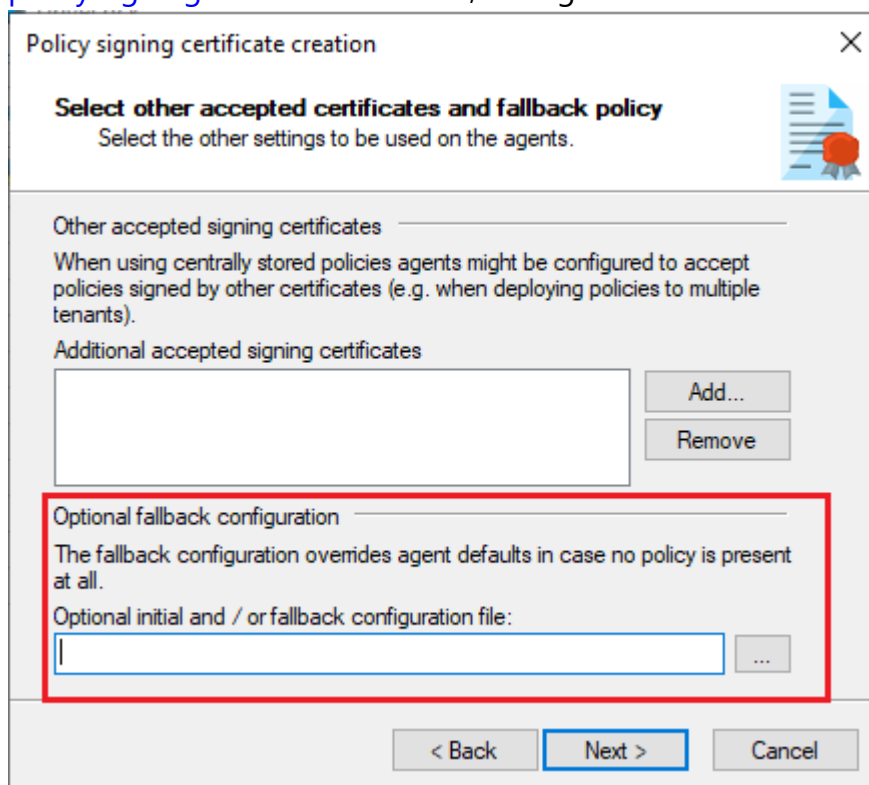
You can view the RSoP via Agent remote control to see the policies that the agent has been using.

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:
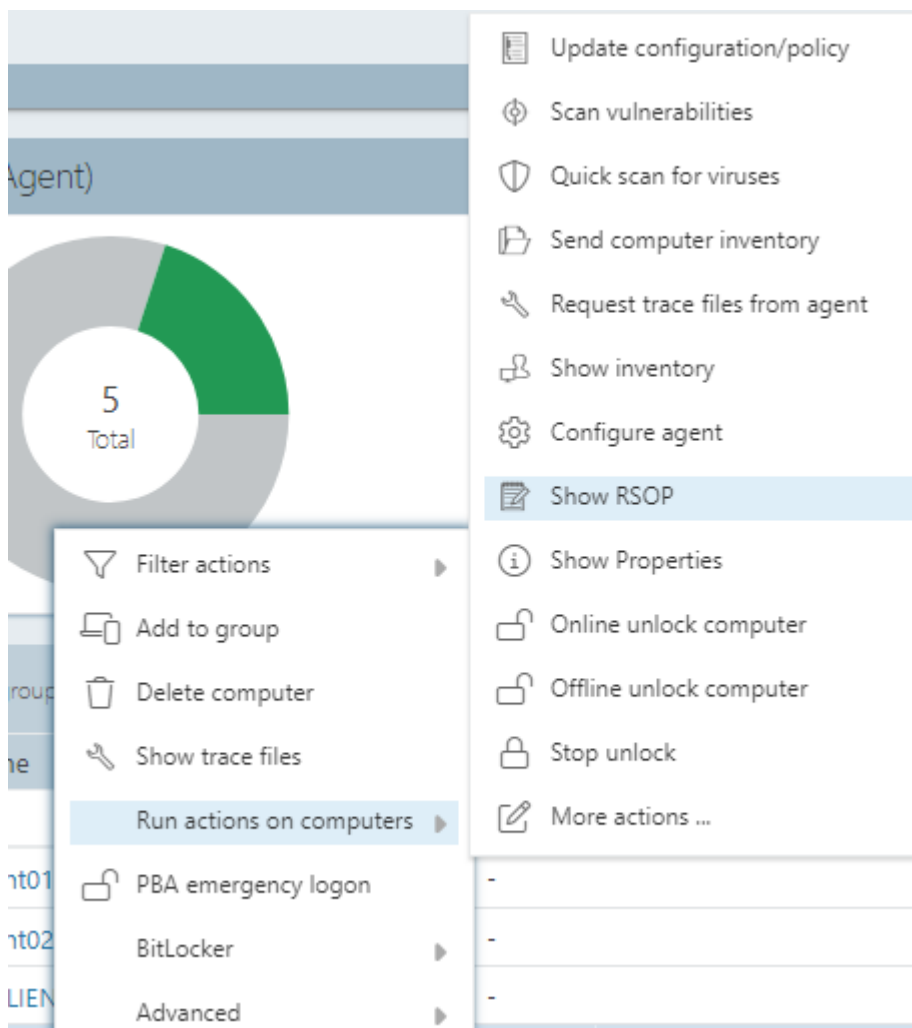
11.2.3 Publish policies

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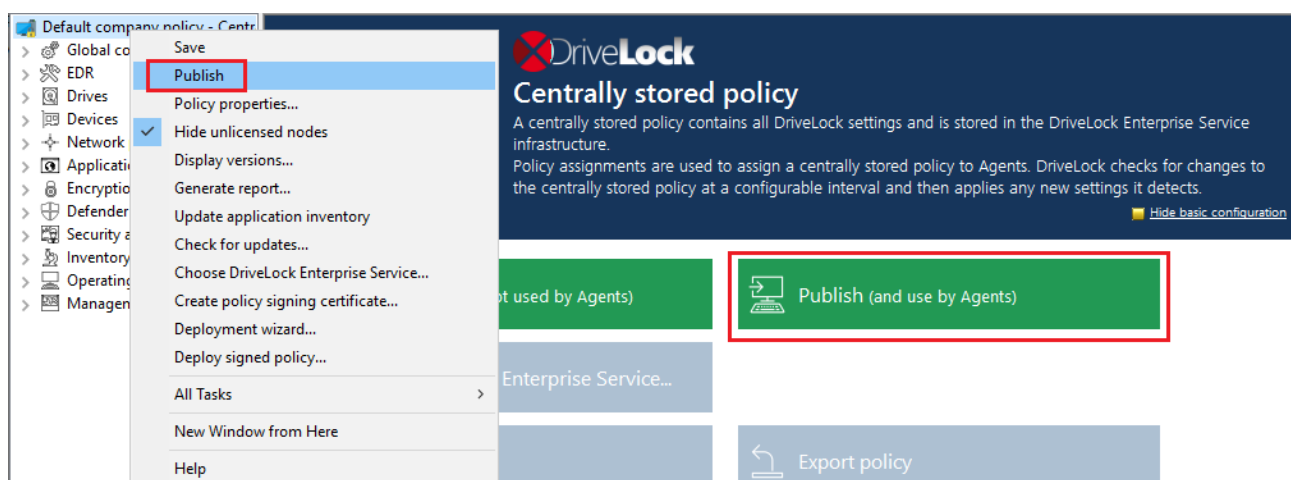
Or simply in the menu bar by clicking the following icon:

DriveLock

File   Action   View   Window   Help

Default company policy - Centr
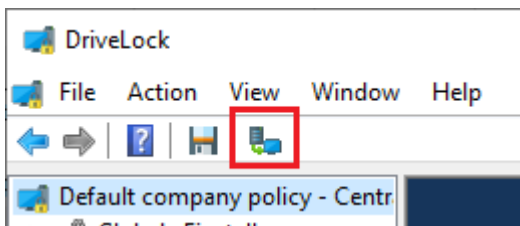
Optionally enter a **publish comment** in the dialog and confirm with OK.

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.

11.2.4 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.

11.2.5 Policies and rules in the DOC

Configuration in DOC: Administration -> Policies

In the DOC, you can quickly create policies with similar properties and functionalities to those offered by the Policy Editor. You no longer need to switch to the policy editor via the DOC Companion. It is also still possible to create drive and application rules and, from version 2024.1, also rules for devices. These rules can be added to the policies created in the DOC.

You can also create rules based on events, which are then added to a specific policy. This also works for individual drives, applications or devices as well as on the basis of unlock requests.

Policies can also be renamed in the DOC.

11.2.5.1 What you need to know about policies in the DOC

Starting with version 2024.1, the DriveLock Operations Center (DOC) now offers you the option to create and edit not just one policy, but several policies directly from within the DOC. Compared to regular policies created with the Policy Editor, they can also be restricted to certain functions (e.g. only to Application Control).

The policies created in the DOC are displayed with the policy type 'DOC managed'. They are not opened via the DriveLock Companion and then edited using the Policy Editor, but instead you can edit them within the DOC. A column for the policy type can be added in the policy view in the DOC. In the DriveLock Management Console (DMC), you will see the **policies** as usual in the Policies node, here also with the type **DOC managed** or, if it is a conventional policy from the Policy Editor, **DMC managed** with or without (old).

Once you have created a first (initial) policy in the DOC, it is called the **standard policy <tenant name>**. It has the following properties:

- The standard policy is automatically created by the server when you create your **first** rule in the DOC.

- Each change to the included rules creates a new version. It is automatically published.

- A policy assignment is automatically created by the server when the first policy 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.

- The standard policy only applies to the respective tenant, which is why the tenant is also contained in the name. There is only **one** standard policy per tenant.

- You can set the following permissions:
    - Manage rules: Create, modify and delete rules

    - Manage objects in rules: Add or delete the managed objects (i.e. drives, devices, applications, campaigns) in rules

    - Read rules: Display the rule

When you edit rules in the DOC, you can select the policy you want to save the rules in.

Restrictions

> Note: We recommend editing the standard policy **exclusively** in DOC. You may also open and view them from the DMC. Please note, however, that you cannot make any changes in the DOC during this time.

- Policies managed with the DOC can only be evaluated by DriveLock Agents with a 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.

11.2.6 Computer-specific policy customizations

A Computer Specific Policy Adaptation (CPA) is technically a centrally stored policy that only contains settings for a single computer. Unlike normal centrally stored policies, however, these are not assigned individually, but via a single policy assignment whose assigned policy is the computer-specific policy customization.
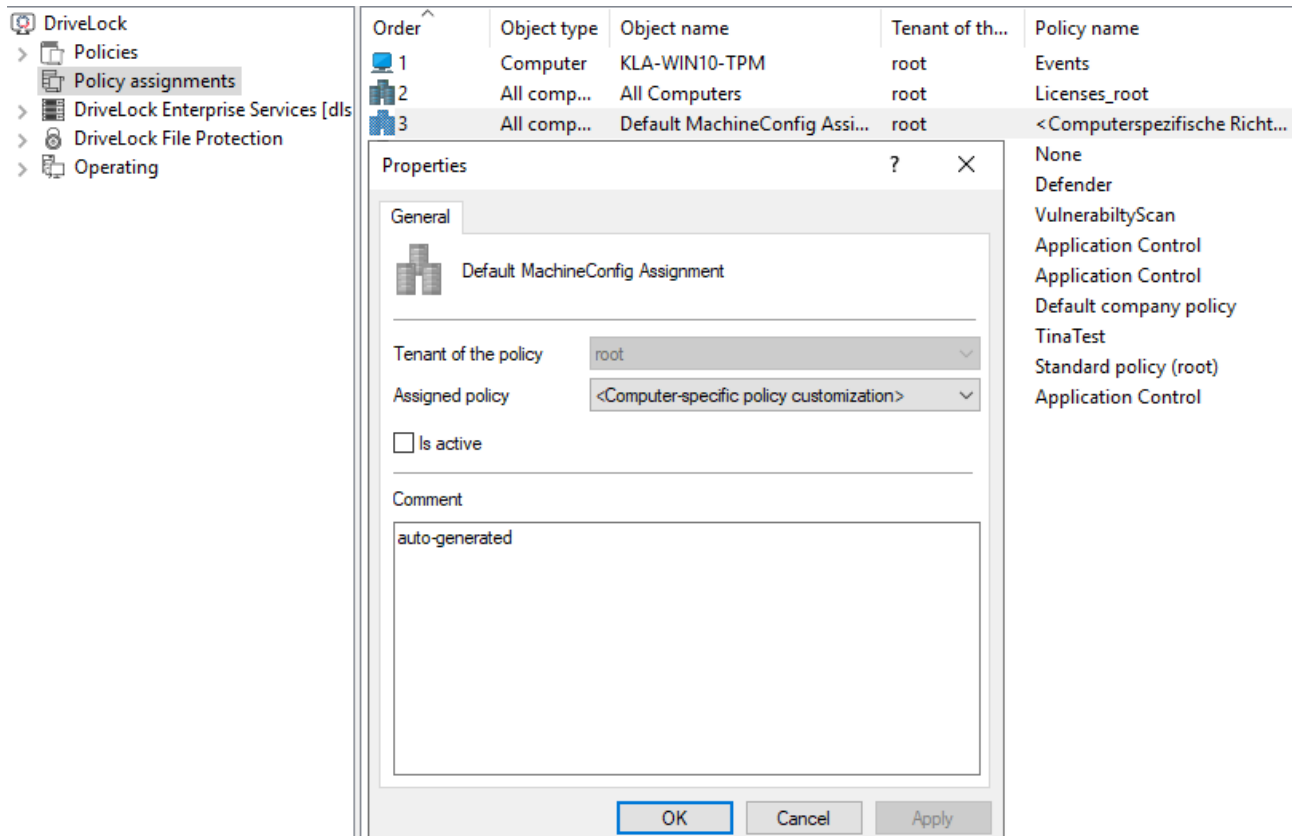
- By default, this assignment is created by the name **Default MachineConfig Assignment**. It provides the CPA associated with each computer.

- 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.

11.3 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 that contain DriveLock settings, right-click on **Policies** -> **New** -> **Add group policy object** in the DMC.

Then select the relevant 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`

11.4 Configuration files

Instead of group policies or centrally stored policies, DriveLock can also be configured centrally in other operating system environments.

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.

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.

In the DriveLock Management Console (DMC), right-click on **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, 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...**.

11.5 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 .dlc.

> 📝 Note: The **Export configuration** (Import configuration or Merge configuration) options are also available for centrally stored policies and they are not limited to the local policy in any way.
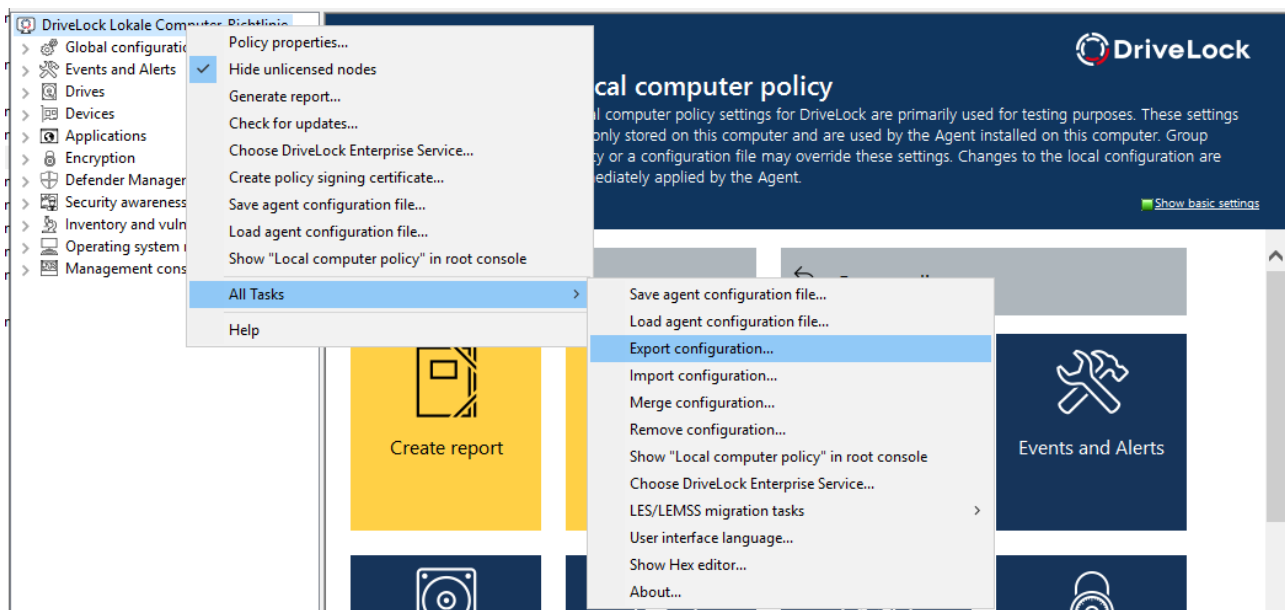
> ✎ Note: You can also import a local configuration if, for example, you have previously exported a policy from a group policy and then imported it into a local DriveLock configuration.

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.

11.6 DriveLock Policy Editor

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

> ✎ Note: If you want to edit policies from the DOC, the DOC Companion is launched first and then the Policy Editor opens.

11.6.1 General notes

11.6.1.1 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.
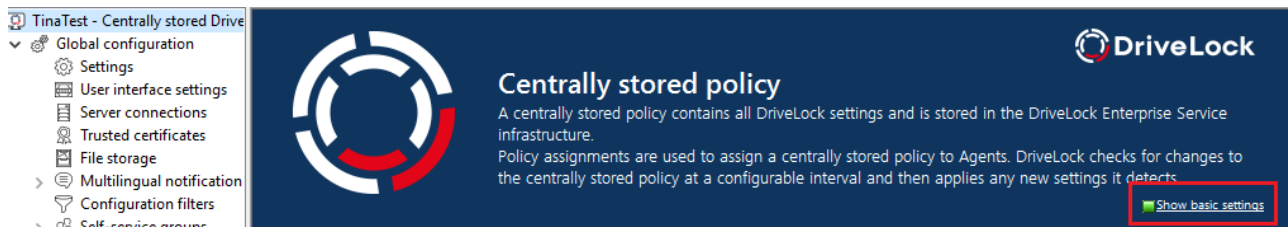
There are two top-level options: **Show basic settings** or **Show all settings** Depending on the selection you make, you will see different views of the nodes (see example below for the **Global Settings** node)

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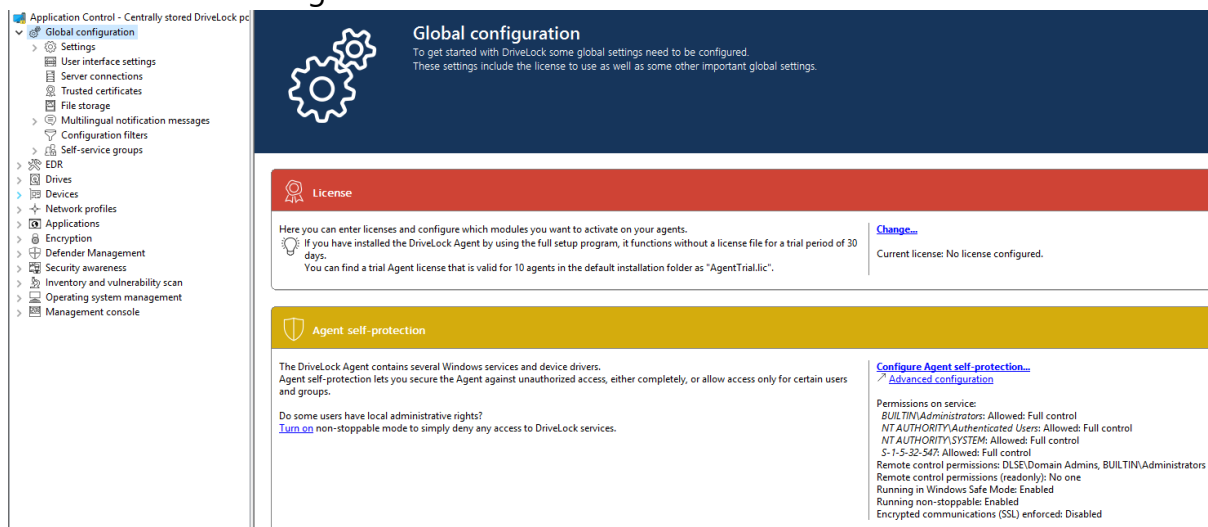
- View with all settings:
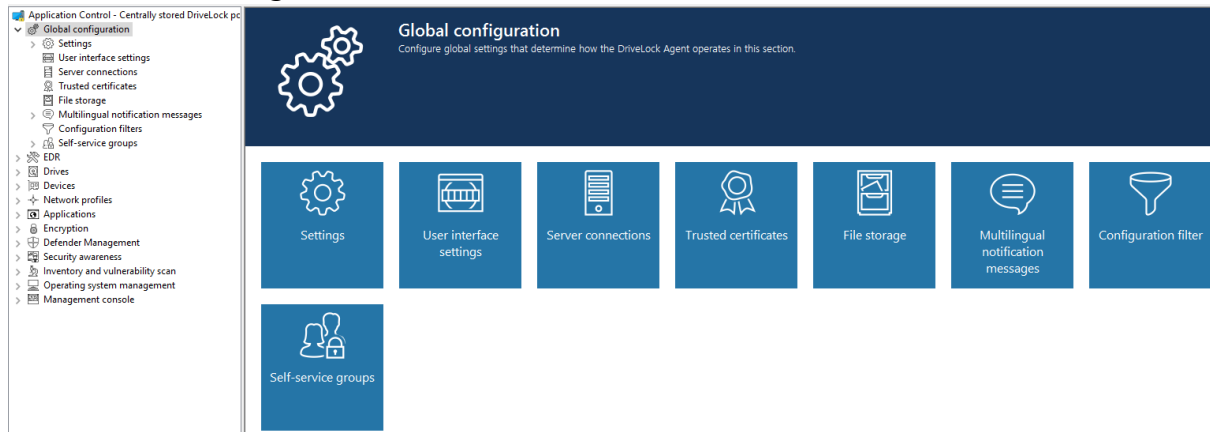
For some nodes in the Management Console or Policy Editor, you also still have the option to switch from a user-friendly and structured **taskpad view** to a simple **list view**.

Here is the taskpad view using the **Settings** node as an example :
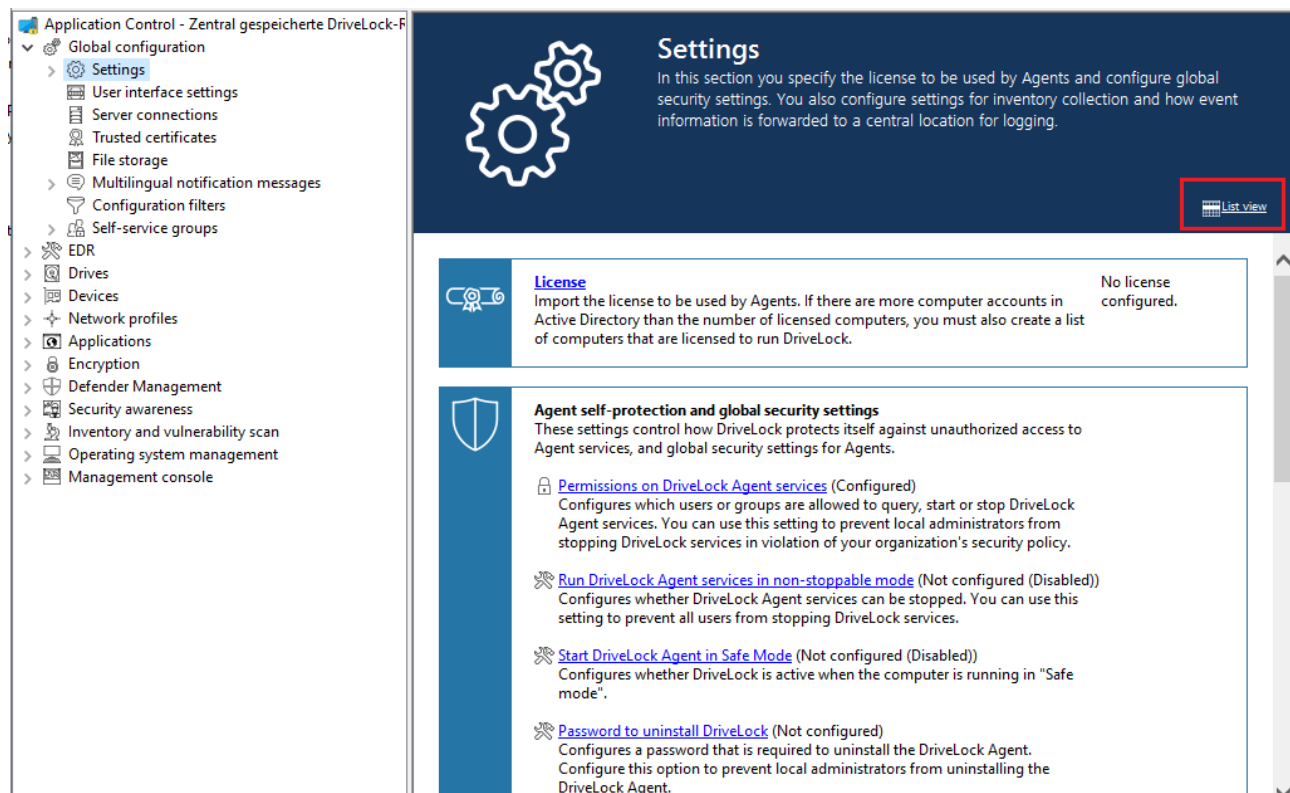
11.6.1.2 Generate configuration report

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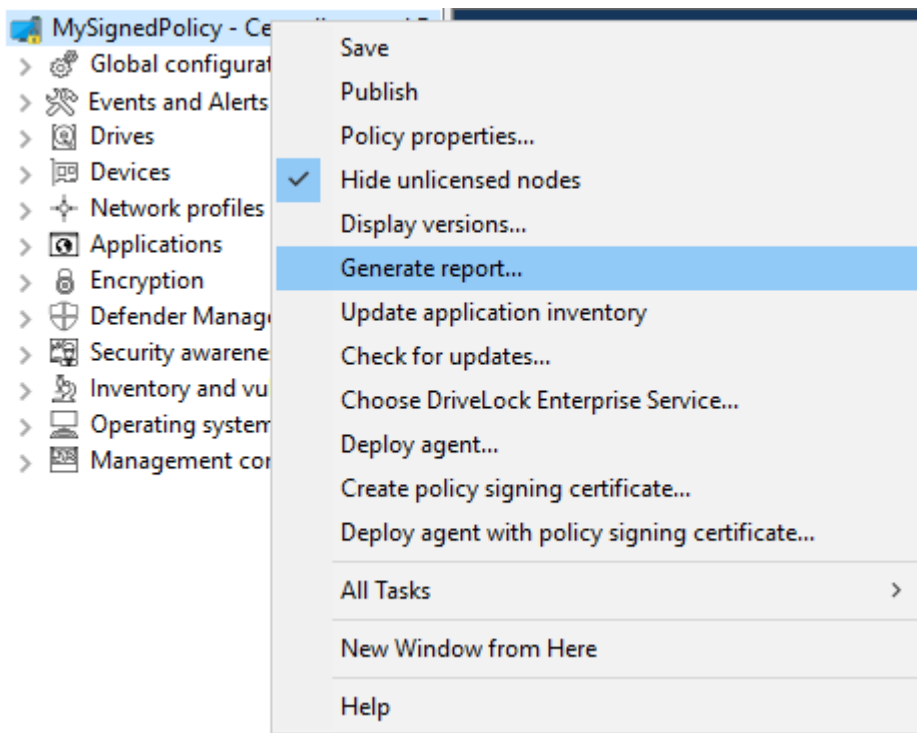
Use the scroll bar and the "+" and "-" icons to navigate through the report.

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.

11.6.1.3 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

11.6.1.3.1 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.
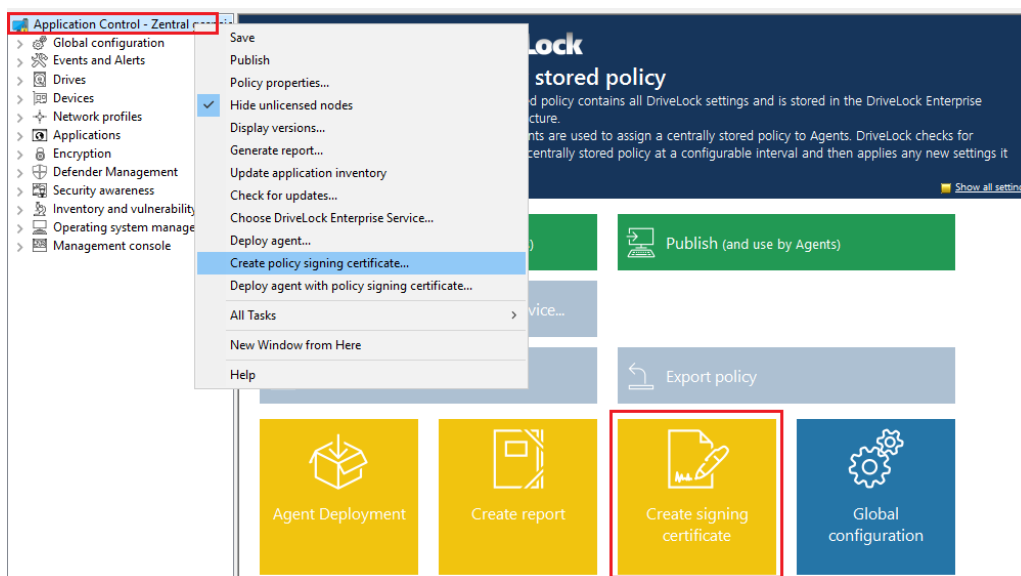
A wizard will start to guide you through the steps of creating them.

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. Set this up.

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:
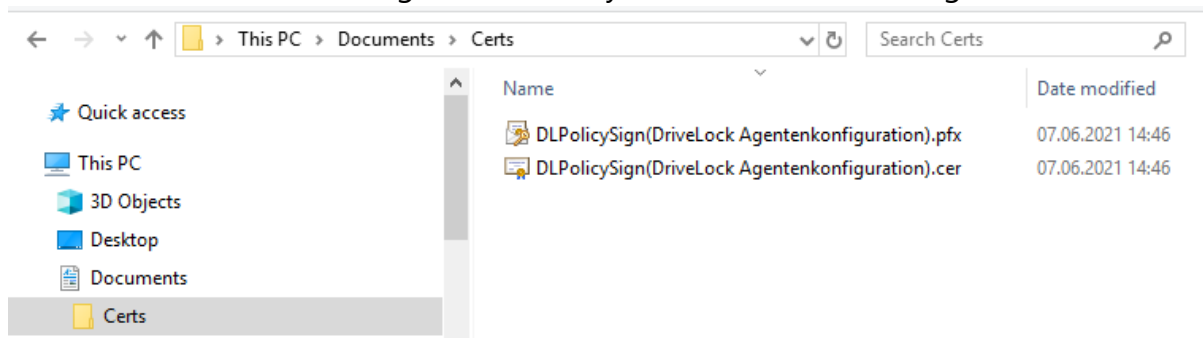
11.6.1.3.2 Signing a policy

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.
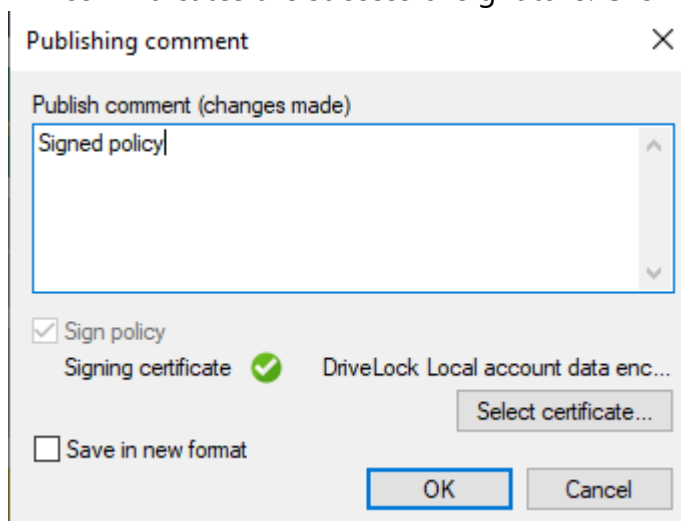
DriveLock

11.6.1.3.3 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.

Click here for detailed information on installing DriveLock Agents.

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.
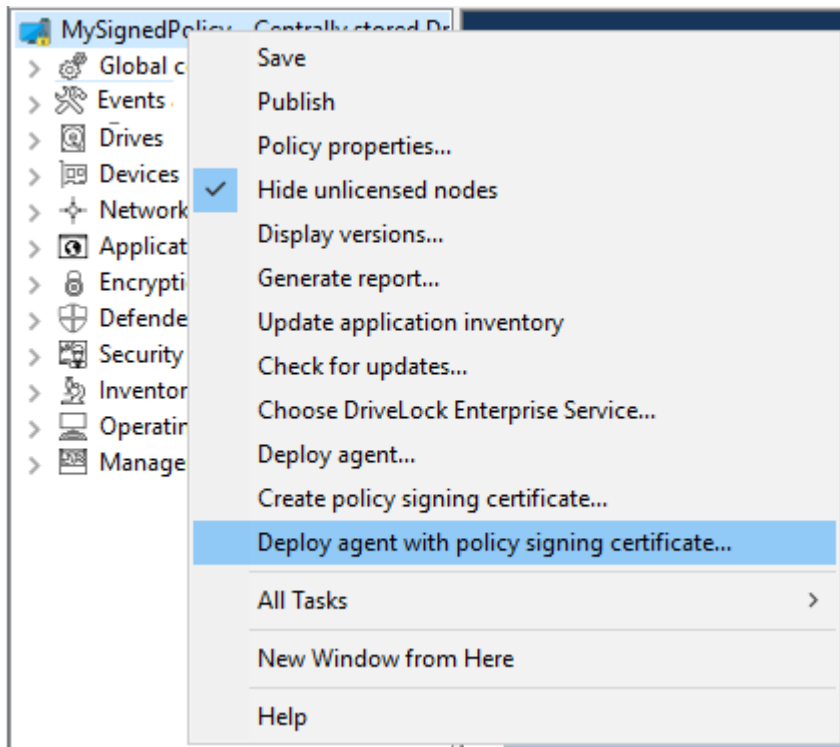
2. Using this wizard, you will create a prepared installation package, which you can then use to install the DriveLock Agents on your network.

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.

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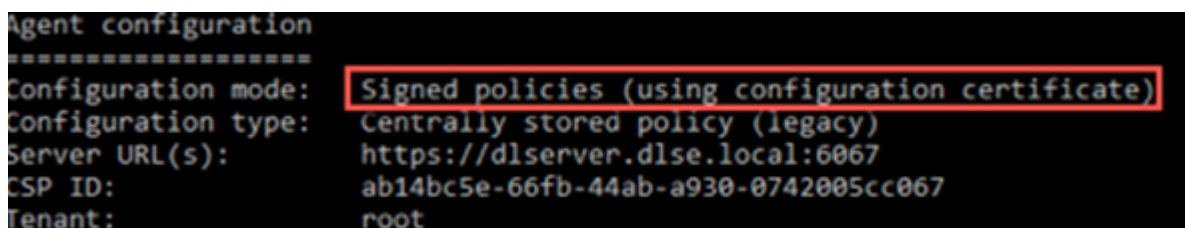
If you want to reconfigure an already installed agent to accept only policies signed with a specific certificate, you can do so with the following command line command:

```
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
```
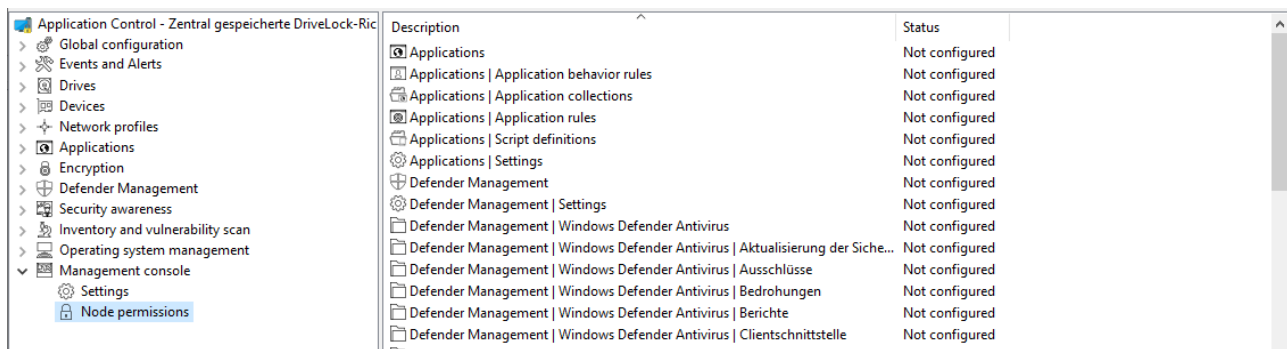
11.6.1.4 Node permissions in the Policy Editor

In this section you can specify management console settings, especially permissions for using the console.

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.

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.
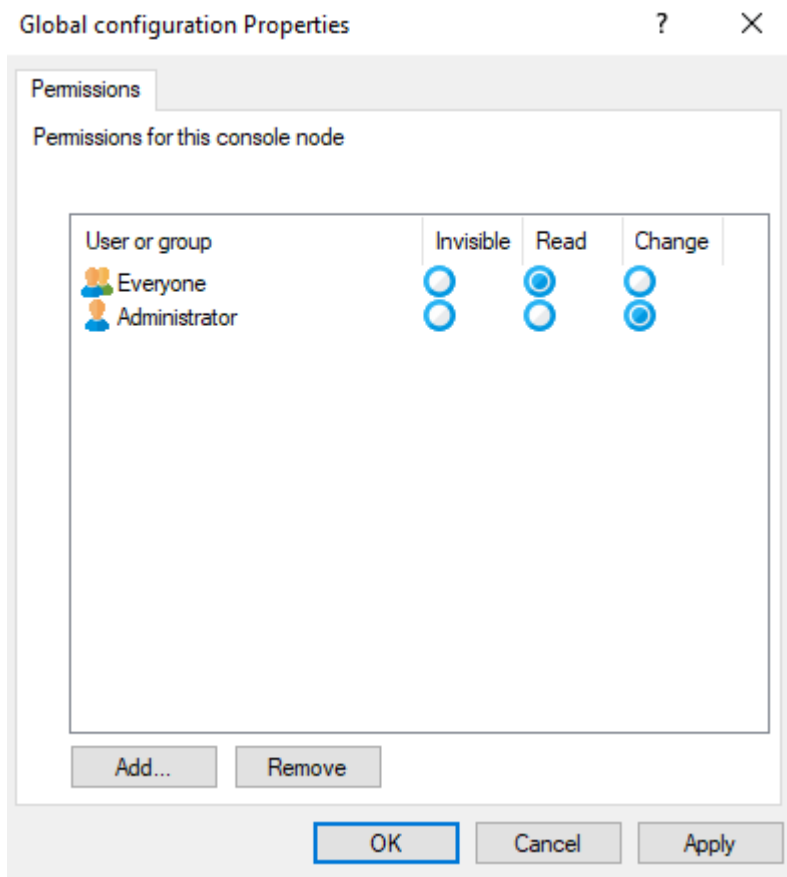
Click Add to assign a new user or group to this node. Select a group or user and click Remove to remove the selected account from the list.

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.

12 Groups

12.1 DriveLock groups

Configuration: DOC -> Administration -> Groups

There are several DriveLock groups:

Static computer groups are defined by manually adding computers, groups or organizational units from the AD object inventory, from individual computers (which are added individually by name) or from existing DriveLock groups (also Microsoft Entra ID 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 also create a copy of an already existing group.

Microsoft Entra ID groups are synchronized to DriveLock by triggering the Microsoft Entra ID integration. Click here to learn more about the settings you need for this.

Static user groups are defined by manually adding users or groups from the AD object inventory, from individual users (which are added individually by name) or from existing DriveLock user groups (also Microsoft Entra ID groups).

DriveLock system groups: These groups are the All computers or All users group (<All computers>;<All users>). It contains all existing computers and users as logical members.

12.2 Static computer group

To create a static computer group, proceed as follows:

1. Click **+** and select **Create static computer 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. In **Definitions** you may now add static group members. Click **+ Add group member**. Here you have the following choices:

- AD Computer / AD Group: select individual computers or groups from the AD object inventory and add them to your static group.

- OU container: Select 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).

- Microsoft Entra ID group: If you have already integrated Microsoft Entra ID groups in DriveLock, you can also select them here.

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

5. Once you have updated the configuration, you will see a list of computers belonging to your static group in the **Reported members** detail view. In the **Membership determined by agent or server** columns you can see how the group membership was determined. If groups are added in the DriveLock Operations Center (DOC), you can see 'Server' as the source. As soon as the client reports its group membership back to the DES, the column entry is Client.

For information about the **Assigned policies** and **Used in policies** views, see the Using groups in policies topic.

12.3 Dynamic computer group

To create a dynamic computer group, proceed as follows:

1. Click **+** and select **Create dynamic computer group**.
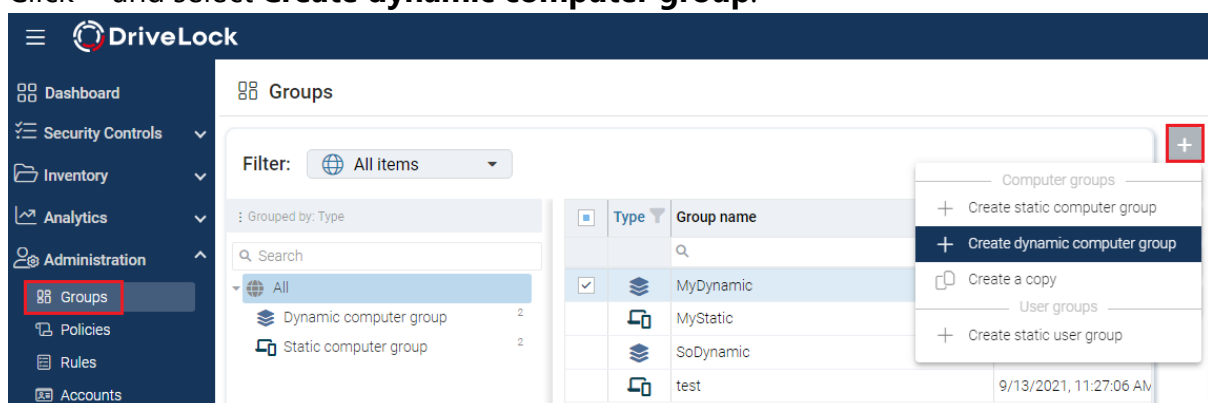
2. Specify a name for the group and optionally add a description.

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.

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

12.3.1 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 cri-terion	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 department (Department attribute from AD).
AD memberships (DN format)	2023.1	String	LDAP path e.g. CN=Computers,DC=example,DC=com
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)

Filter cri-terion	Available from DriveLock version	Type	Value, name, example
BIOS vendor	2022.1	String	
BIOS version	2022.1	String	
BIOS timestamp	2022.1	Date / Time	
Computer name	2019.1	String	
Defender Service ver-sion	2022.1	String	
Defender status	2022.1	Enum	Active, Inactive, Partially active
Distin-guished name	2022.1	String	CN=PC01,C-CN=Computers,DC=DLSE,DC=local
Domain name	2022.1	String	
DriveLock version	2019.1	Version	

Filter cri-terion	Available from DriveLock version	Type	Value, name, example
IP4 range	2019.1	IP address list	Enter the corresponding IP4 ranges
IP6 range		In the range of	
Is server	2019.1	Boolean	Yes, No
Is staging	2019.1	Boolean	Yes, No
Open vul-nerability	2022.1	Stringlist	Enter the name of the vulnerability
Registry	2019.1	unknown, integer	Enter the registry key and name
SMBIOS ver-sion	2022.1	String	
TPM version	2022.1	Version	
TPM exists	2022.1	Boolean	Yes, No
Windows ver-sion	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 (wild-cards 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

For example

12.4 Static user group

To create a static user group, proceed as follows:

1. Click **+** and select **Create static user group**.
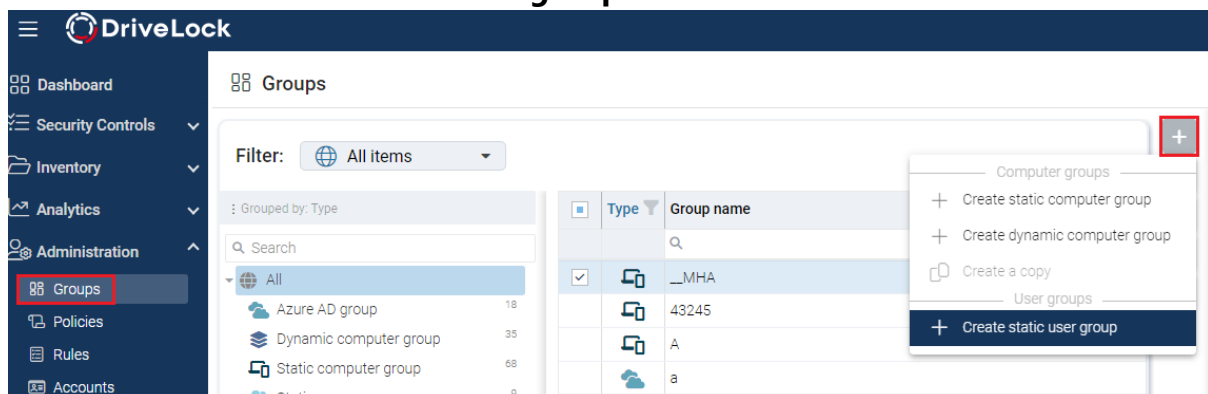
2. Specify a name for the group and optionally add a description.

3. Your group appears in the list. Click on the name to edit the group.

4. In **Definitions**, you can now add members to the group. Click **+**.
   Here you have the following choices:
   - Users: Select users from the AD object inventory and add them to your static group.

   - User name: Add individual users by name to the group.

   - Static user group: you can also add a previously created user group.

   - Microsoft Entra ID group: If you have already integrated Microsoft Entra ID groups in DriveLock, you can also select them here.

   - AD Group: Select and add an AD group directly from AD.

5. Listed below **Used in Policies** are the policies where you added the user group.

6. **Used in Security Awareness Campaigns** lists the campaigns that are assigned for the user group.

12.4.1 Configure user group queries

This setting allows you to configure a query for group memberships. The agent can be configured so that it queries all user groups from the DriveLock Enterprise Service (DES), or only users it knows. The load and speed of the data transfer is also affected by this.

Several options are available with this setting:

- **Query groups only for known users**: Select this option to query group memberships for known users. Group memberships cannot be determined for unknown users. This option is fast because less data is transferred.

- **Query groups for all users**: This option queries the group memberships for all users. This may take longer and generate more data load.

- **Query groups for all users on terminal servers only**: Select this option to query the group memberships for all users on terminal servers. On all other computers, only the group memberships of known users are queried.

12.5 DriveLock system groups

From version 2024.2, the "All computers" or "All users" group can be explicitly added to a group. This group then contains all computers or users that exist in your company. All computers are members of this group, but only the computers whose DriveLock agents respond to the policy query are shown as active in the DOC.

Example:

You have a 'Server' group that contains all servers. You want to create a computer group 'Workstations' that contains all computers in your company except the servers. To do this, add the "All computers group" to this group and then exclude the 'Server' group.

12.6 Using groups in policies

Static and dynamic computer groups, and user groups as well, can be used in all whitelist rules (drive and device whitelist rules), application rules, file filter templates and configuration filters. You can also 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.

12.7 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.

13 Global configuration

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

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

The following settings are available:

- General settings (e.g. for licenses) and configuration filters

- Agent user interface

- Server connections

- Certificates

- File storage

- Multilingual notification messages

- Self service rules

- Networks

13.1 Settings

13.1.1 Entering licenses in policies (DMC)

You can configure the **Licenses** in the **Global configuration** node in the **Settings** subnode.

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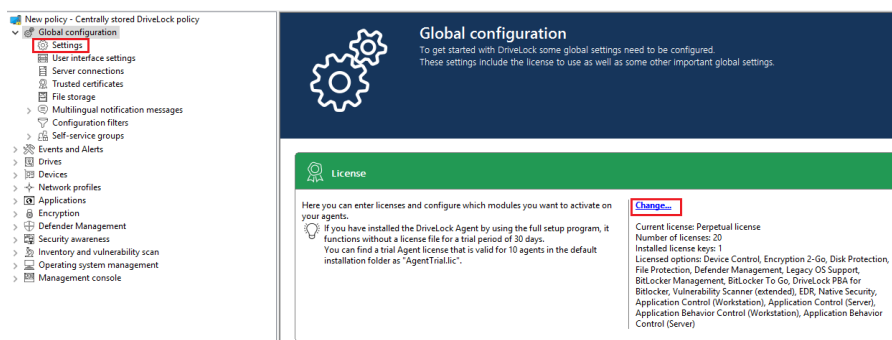
Click **Change...** to open the license dialog.

The **General** tab displays the license status of each module. Please find information on how to activate modules here.

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 you need to specify a proxy server for your Internet connection, click on **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: We recommend transferring the licenses to the DriveLock Enterprise Service after successful activation. 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...** .

13.1.2 Policy settings for agent remote control

> ❗ Warning: You must define permissions in order to perform remote control actions on DriveLock Agents.

Under **Remote control settings and permissions** in the corresponding policy in the **Global configuration Settings**, you can configure different permissions for users (see figure) so that DriveLock agents can be remote-controlled. In addition, you define further connection settings here.

- **Read permissions** tab: here you specify users or groups who are only allowed to request information from DriveLock agents during remote connection actions.

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

13.1.3 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:
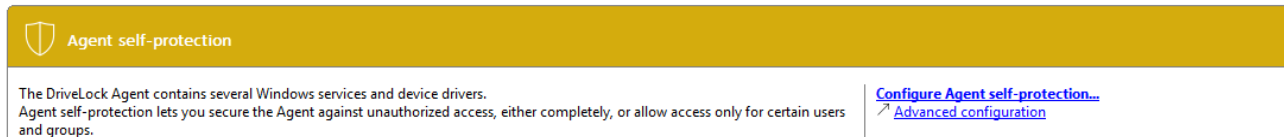
Alternatively, you can set the following settings separately via **Advanced Configuration**:

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

13.1.3.1 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.

13.1.3.2 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.

13.1.3.3 Start DriveLock Agent in safe mode

If this option is activated, the DriveLock Agent is also started in Windows Safe Mode.

This has the advantage that DriveLock also protects the computer in question in safe mode. However, this may limit the possibility of troubleshooting if you have inadvertently configured DriveLock in such a way that working with the computer is no longer possible (for example, if you have locked network cards and input devices).

> 📝 Note: In safe mode, the setting Update configuration only after all protective mechanisms are active on the agent is always deactivated.

13.1.3.4 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
```

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

13.1.3.5 Agent remote control settings and permissions

> ⚠️ Warning: You must define permissions in order to perform remote control actions on DriveLock Agents.

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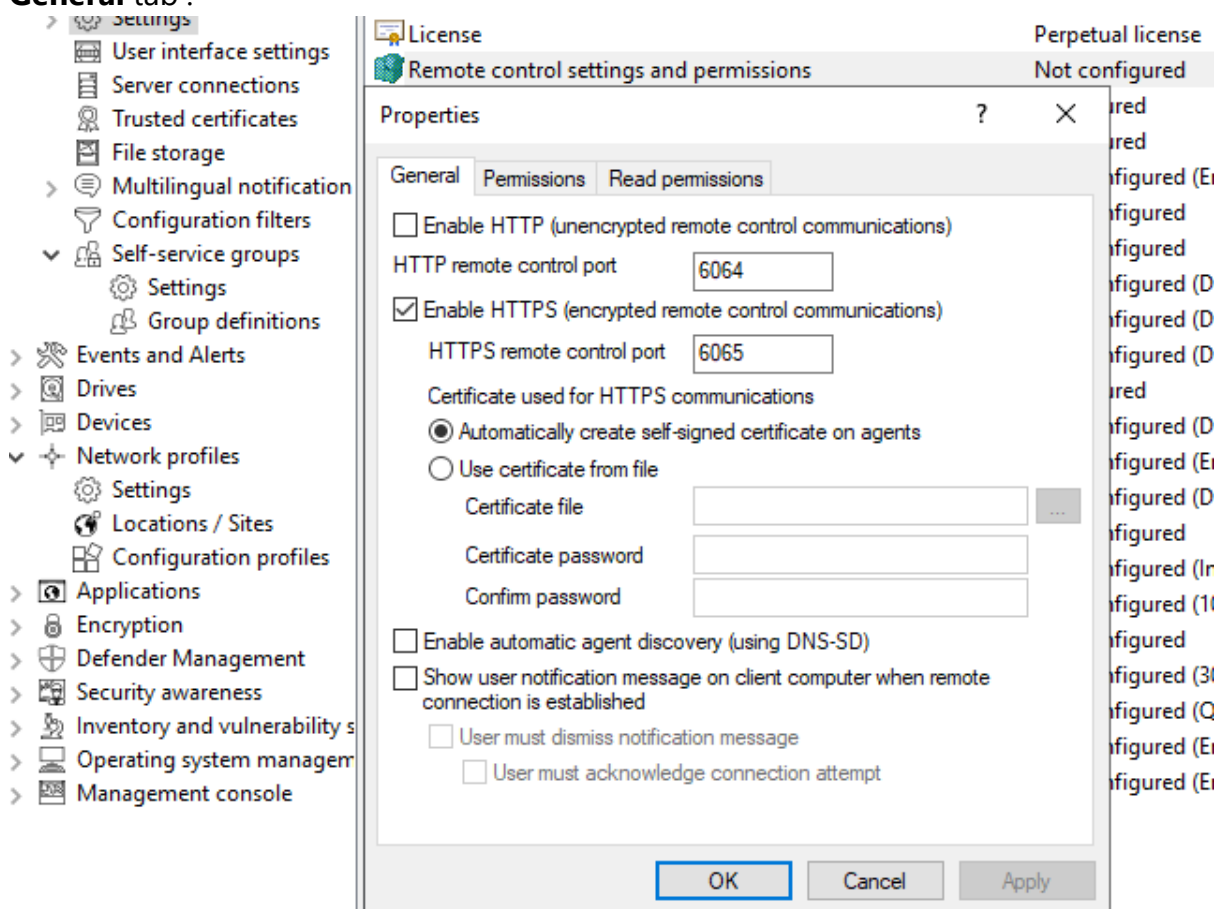
- The remote control port 6064 is set for unencrypted and 6065 for encrypted connections. You can change these ports if necessary. The **Enable HTTPS (encrypted remote control communication)** setting is the default.

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

> ⚠️ Warning: If you access your agents only via MQTT, it is possible to disable HTTP or HTTPS at this point. However, it is then mandatory to ensure that MQTT is always enabled for agent remote control to work.

- 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.

13.1.4 Set DriveLock simulation mode

The DriveLock simulation mode allows you to use DriveLock and distribute the configuration without causing any disruption to users 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.

In Application Control, you can set two different simulation modes, one for whitelist and one for blacklist.

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.

13.1.5 Advanced settings

These are special settings for communication with the DriveLock agent.

13.1.5.1 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.

13.1.5.2 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.

13.1.5.3 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.

13.1.5.4 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.

13.1.5.5 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.

13.1.6 Logging settings

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

13.1.6.1 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.

13.1.6.2 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.

13.1.6.3 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.

13.1.6.4 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.

13.1.7 Event evaluation

You can configure the following settings globally for events:

Evaluate event filters

Evaluate 3rd party events

13.2 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:
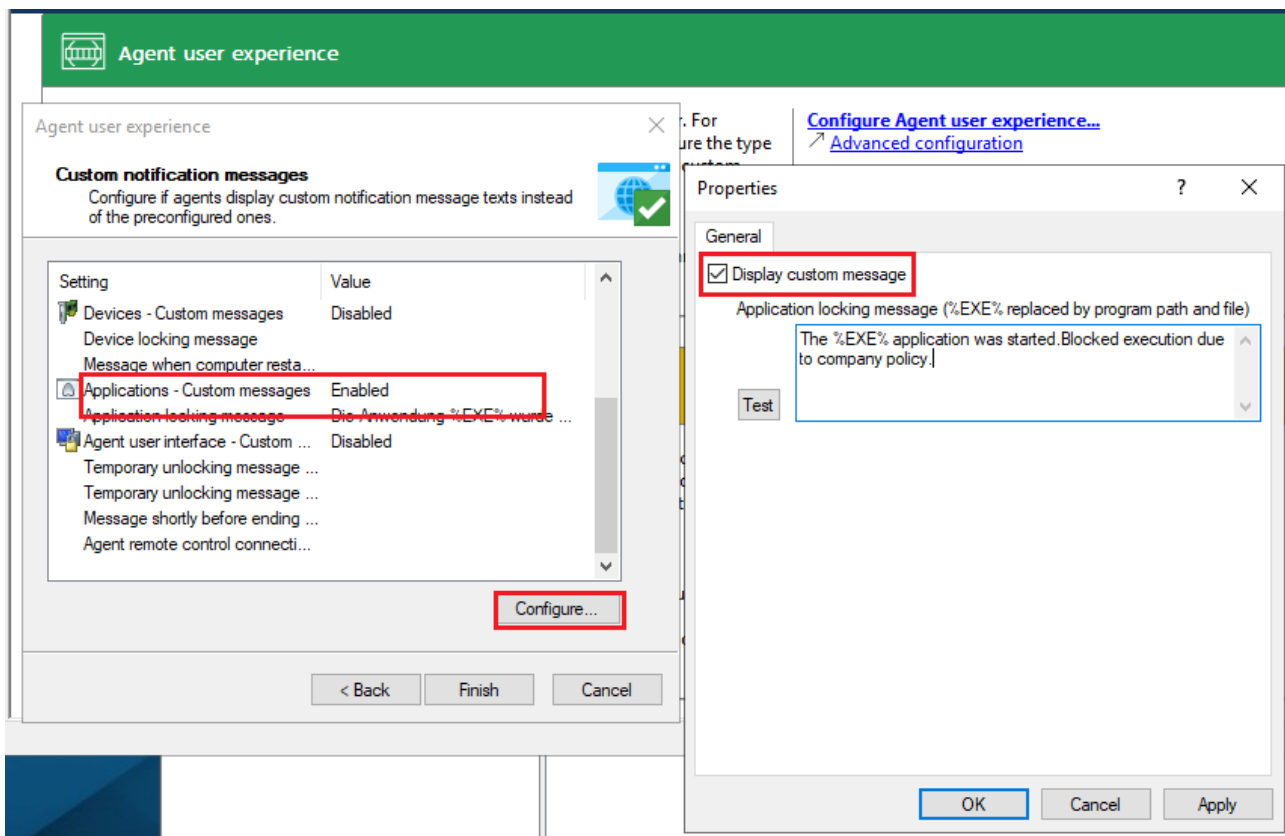
13.2.1 Agent user interface settings

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 on self-service rules here and on security awareness here.

13.2.2 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** .

13.2.3 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:
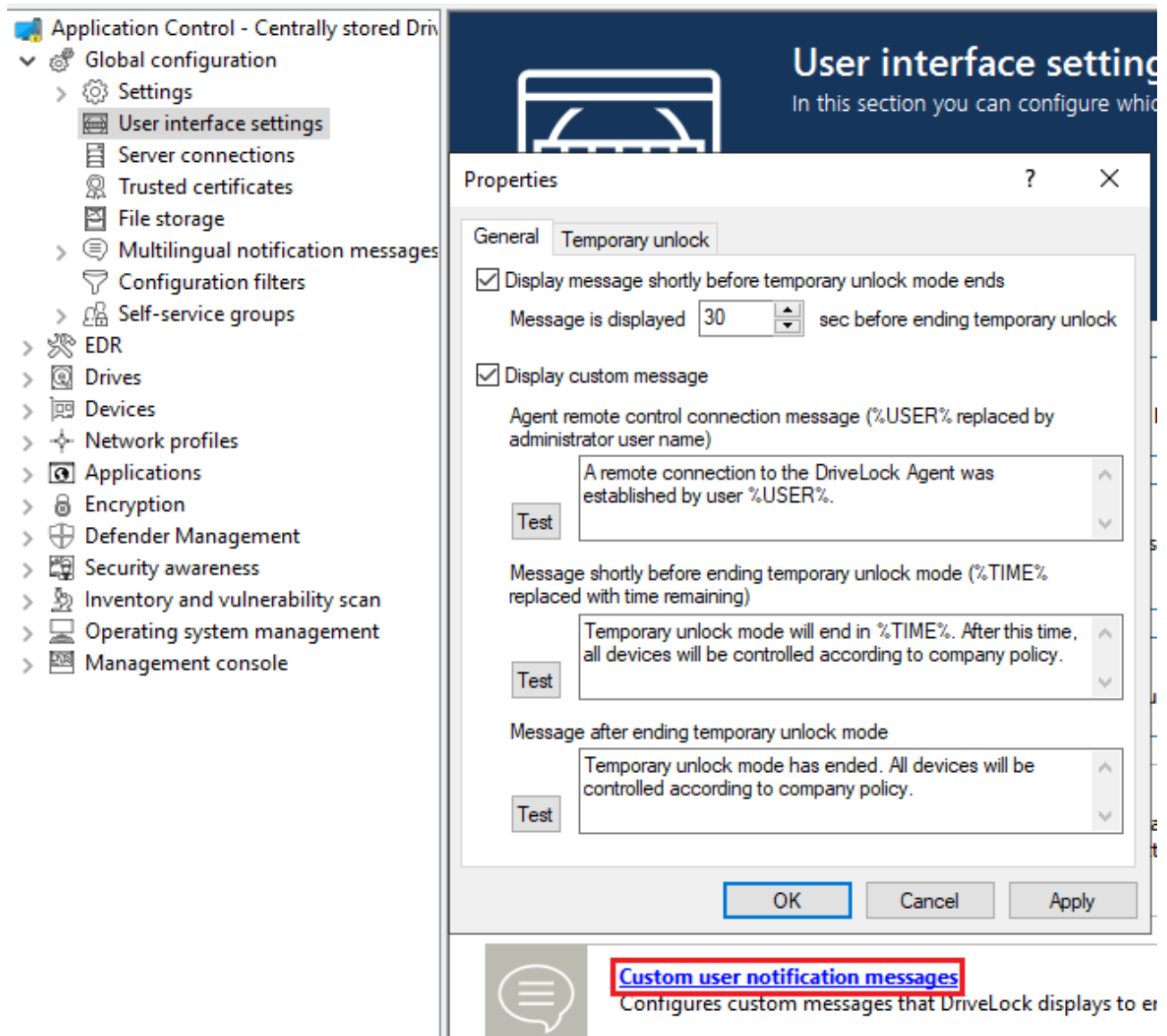
- **Show message just before temporary unlock ends** : This option is enabled by default. If necessary, you can set the time here for the notification to appear.

- **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.

13.2.4 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).

13.2.5 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.

13.2.6 Using custom logos

It is possible to integrate your company logo in the notifications to the end user on the DriveLock Agent. The DriveLock default logo will then be replaced by your own logo in the following places: In all wizards (e.g. self-service release, password recovery, encryption, etc.), in the dialog for confirming usage policies and in all systray notifications.

In order to be recognized by the system, the logo files must meet the following requirements:

- The logo file for the usage policy (or self-service unlock wizard) must have the name **DLWizardLogo.bmp** and a size of 48 x 48 pixels

- The logo file for the systray notifications must have the name **DLPopupLogo.png**, a size of 200 x 28 pixels and a bit depth of 32.

Please do the following:

1. Open the policy in which your settings for the agent user interface are saved.

2. Under **Global configuration**, go to the **File storage** sub-node. Copy the two logo files here.
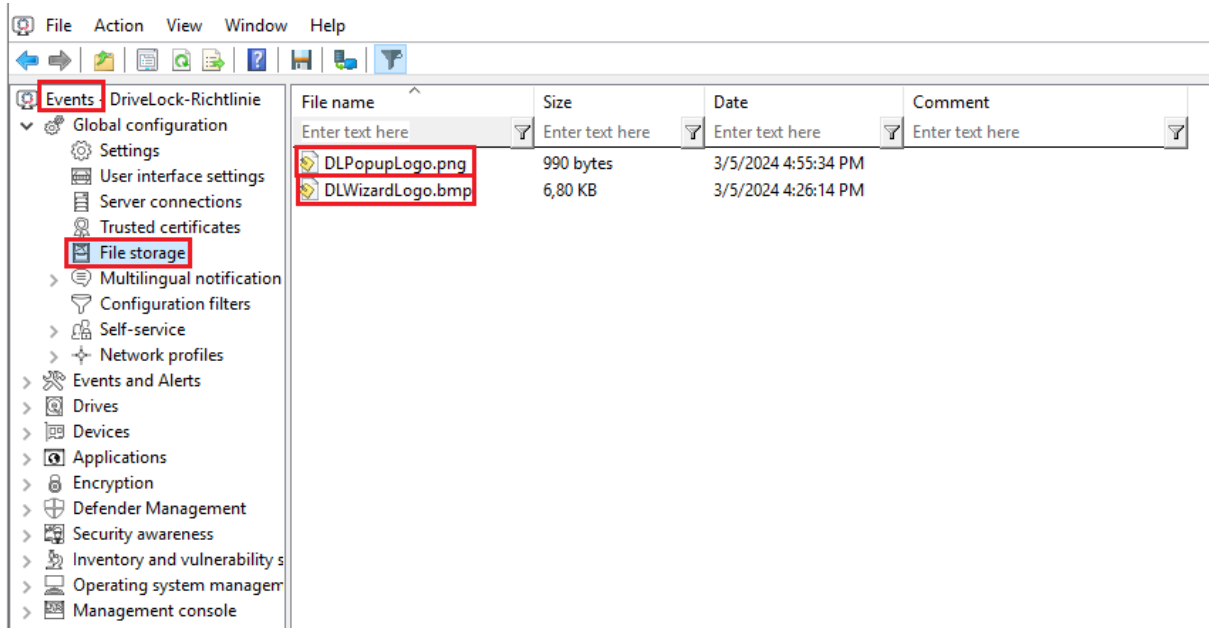
3. Save and publish the policy and assign it to the agents.

The following customized messages are now displayed on the agent side:

Example of systray notification:
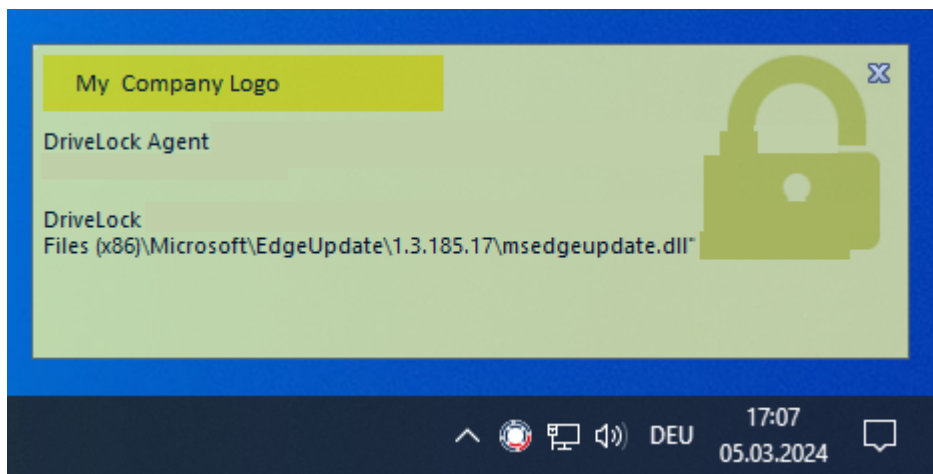
Example of self-service unlock wizard:
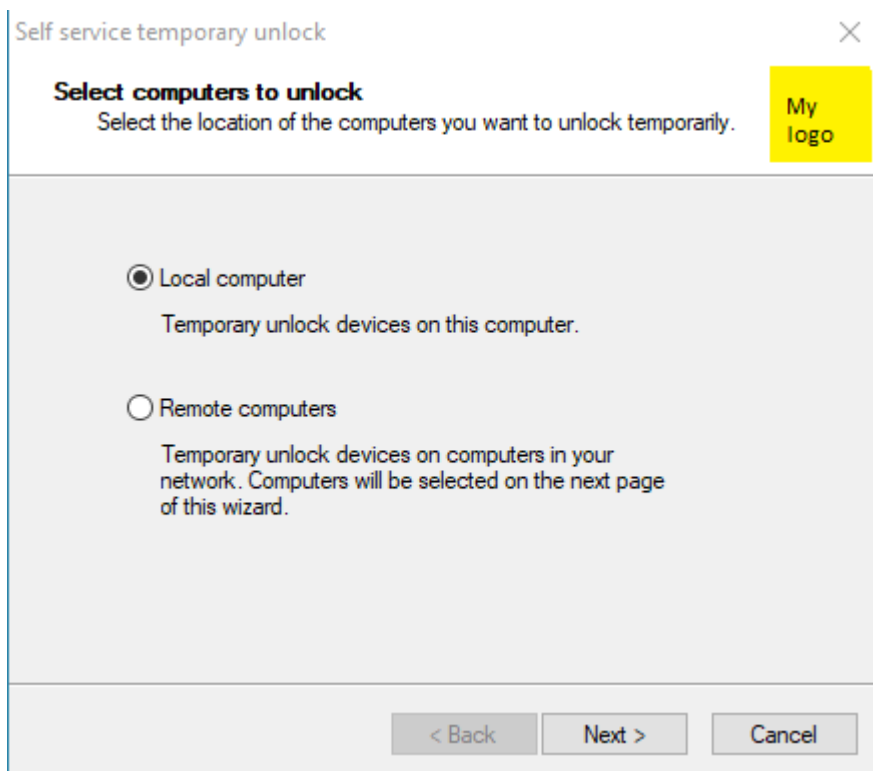
13.3 Server connections

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, proceed in the same way.

13.3.1 Configure server connections

In the DriveLock Operations Center DOC, server connections can be configured in the server settings.

To add a new connection in the DriveLock Management Console (DMC), right-click **Server Connections** and then select **New** and **Server Connection**.
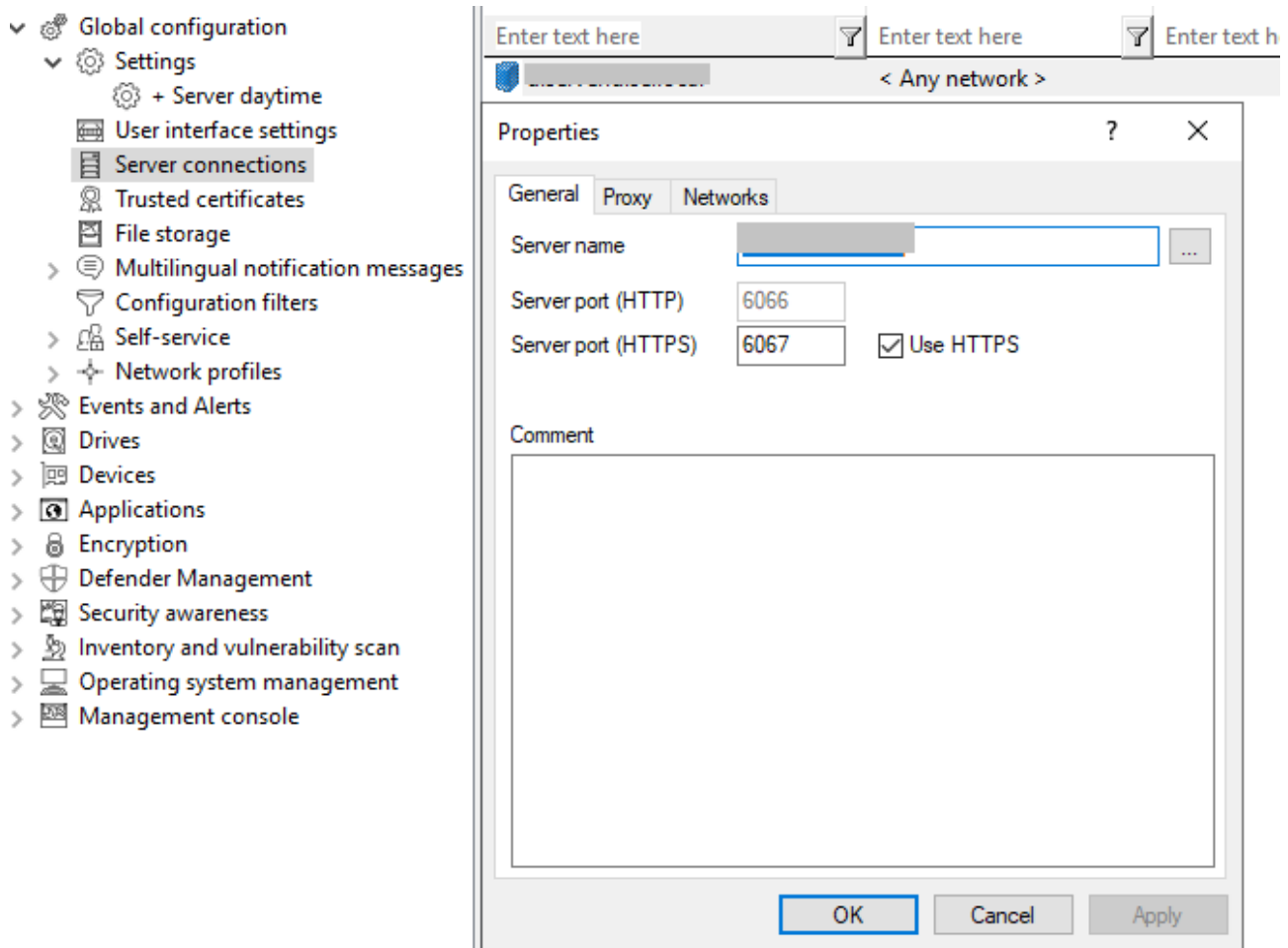
On the **General** tab, specify the **Server name**. If you have changed the default ports during its installation, change them here accordingly. By default, DriveLock Enterprise Service uses ports 6066 and 6067 to receive events from agents.

- The **Use HTTPS** option is selected by default. DriveLock automatically creates an appropriate certificate which is used for the SSL connection.

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.

13.3.2 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** and enter the corresponding 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.

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

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

13.4 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 a policy's global configuration.

> **❗ Warning:** If you want to replace an existing DES server certificate, the new certificate must be imported into the computer certificate store and the private key must be configured so that it can be exported.

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.

Please find further information on the selection of trusted certificates here.

> **📝 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.

13.4.1 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).
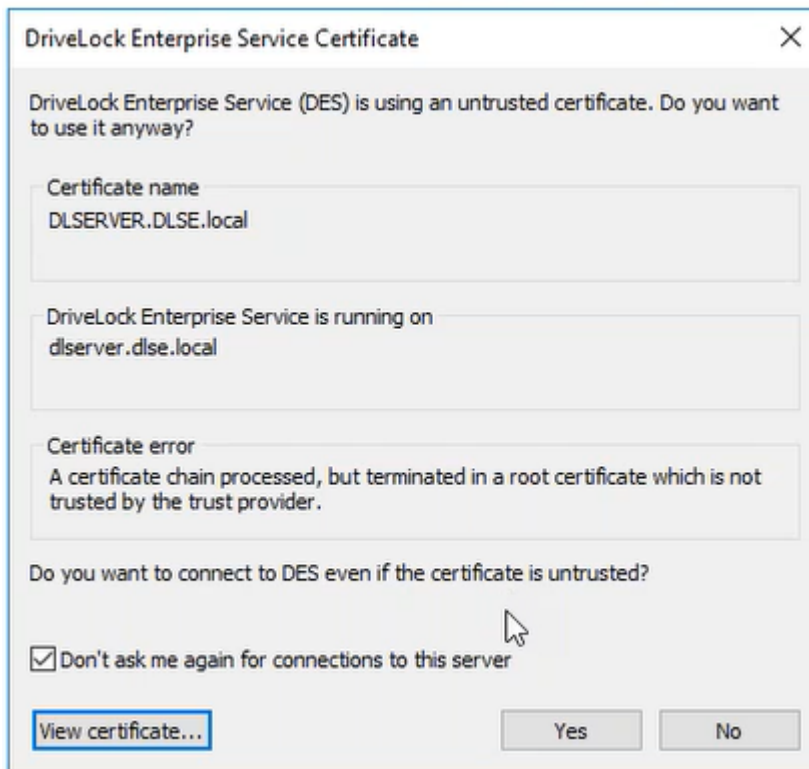
> ⚠ Warning: Please note that self-signed certificates are initially classified as untrusted by Windows because the root certificate cannot be verified.

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.

13.4.2 Select trusted certificates

> ☑ Note: We recommend using this setting to increase the security requirements for communication between DriveLock Agent and DriveLock Enterprise Service. Unless you specify certificates, DriveLock cannot ensure that the agent is communicating with the right DES.

> ⚠ Warning: If you are using self-signed certificates,make sure to enter them here.

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).
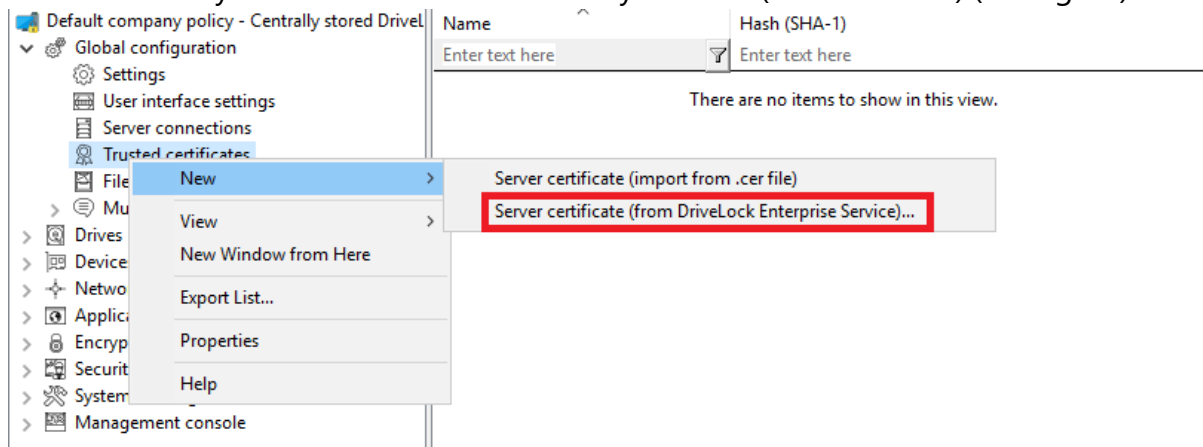
   After that, place a check mark next to those DES (or linked DES) certificates with which the agent communicates (in the example below DLSERVER.DLSE.local...):
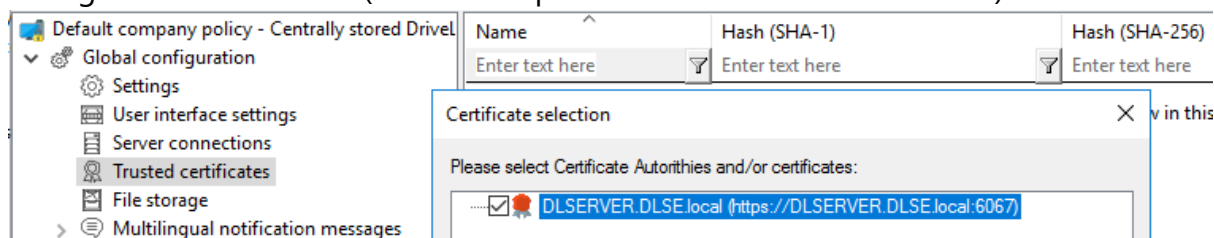
2. If you have specified your own server certificate for communication, you can select it here and use it in your policy:
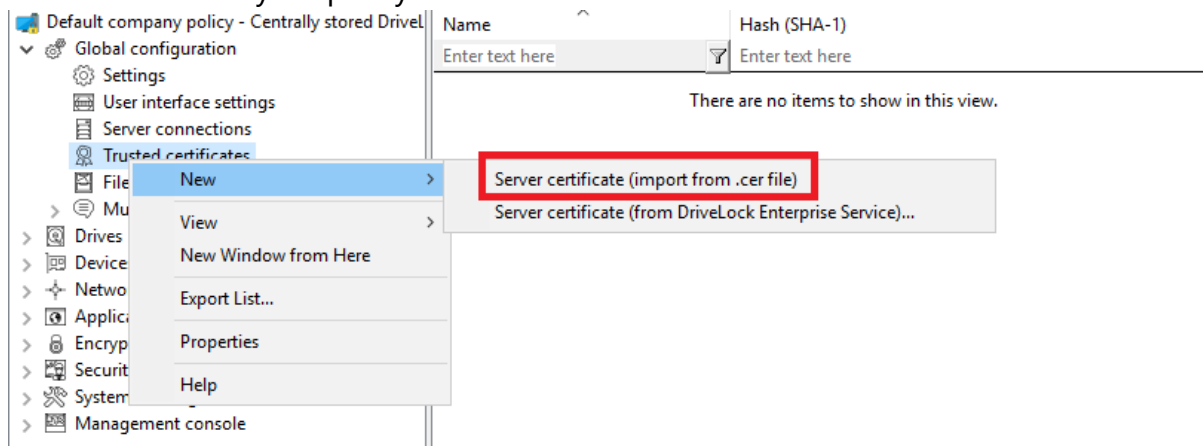
   In the next step, select the appropriate certificate in the directory structure.
   You can also import the root CA certificate with this option. This will make DriveLock agents trust all certificates with this root CA. If your DES certificates have the same root CA, you no longer need to list them individually.

The list of trusted certificates now displays the corresponding information about the certificate (for example, name and hash values SHA-1 and SHA-256).
The DriveLock Agents to which you then assign your policy will trust the server certificate and communicate only with the appropriate trusted servers.

13.5 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.

Once you have imported files into the policy file storage, these are automatically distributed to the agents together with the other settings. For example, you can store your own logo files here, which are then displayed in various dialogs and notifications for end users. Click here for more information.

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.

Click **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 store. 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.

13.6 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.

13.6.1 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.

You define the texts for usage policies on the **Usage policies** tab.

- 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.

13.6.2 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. However, the available languages must first 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.
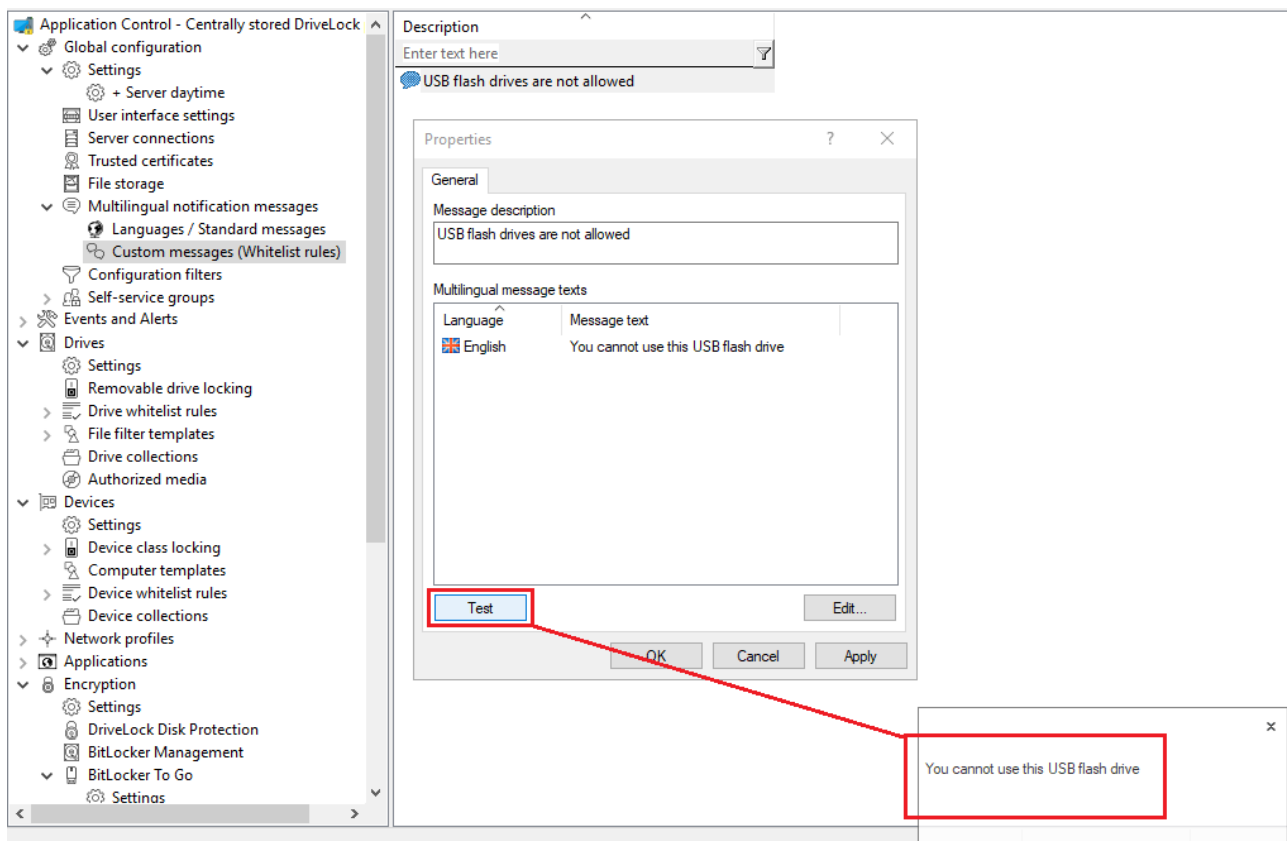
Repeat these steps to enter the respective text for all languages.

> ☑ Note: The use of multilingual messages is defined within the respective whitelist rules.

13.7 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.

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

13.7.1 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).
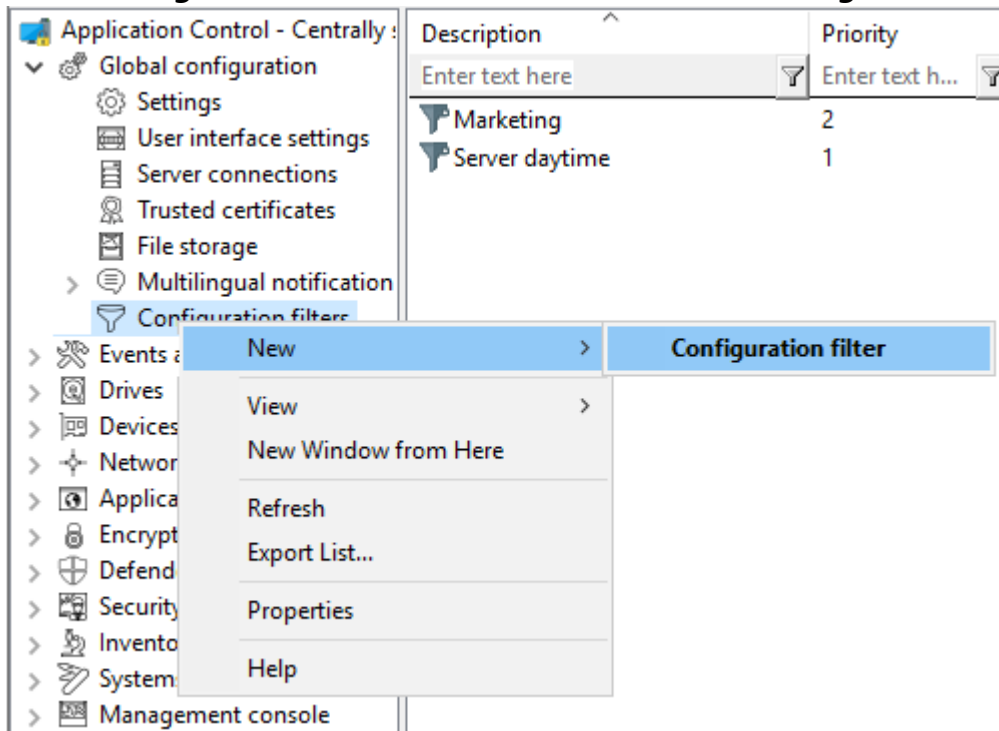
2. In the configuration filter properties, enter a description and, if necessary, a comment. In the example below, the configuration filter is called **Marketing** .

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 can find a use case 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:
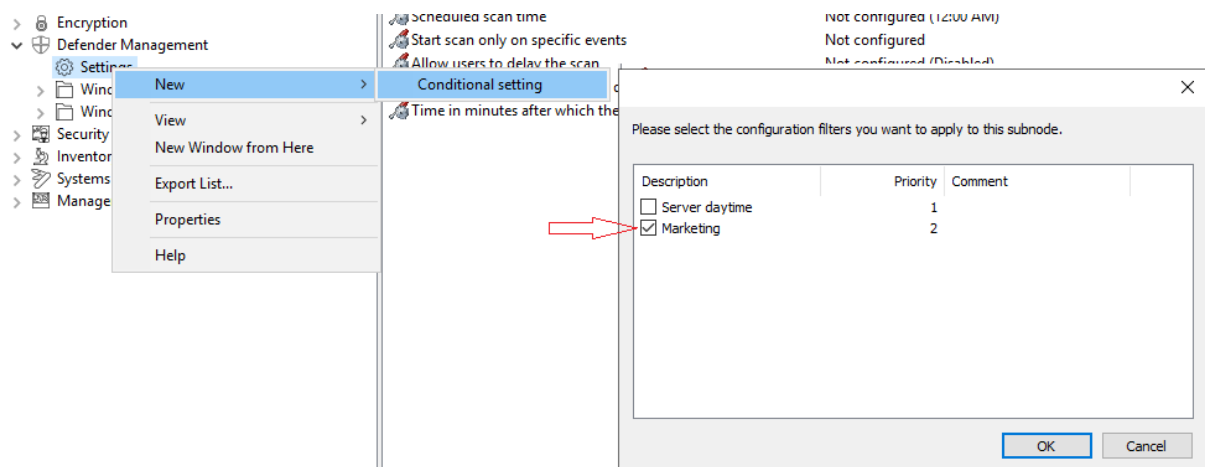
6. Then select the setting that should explicitly apply to the marketing computers. In the example, Defender Scan should be started on the marketing computers only when no users are logged in:
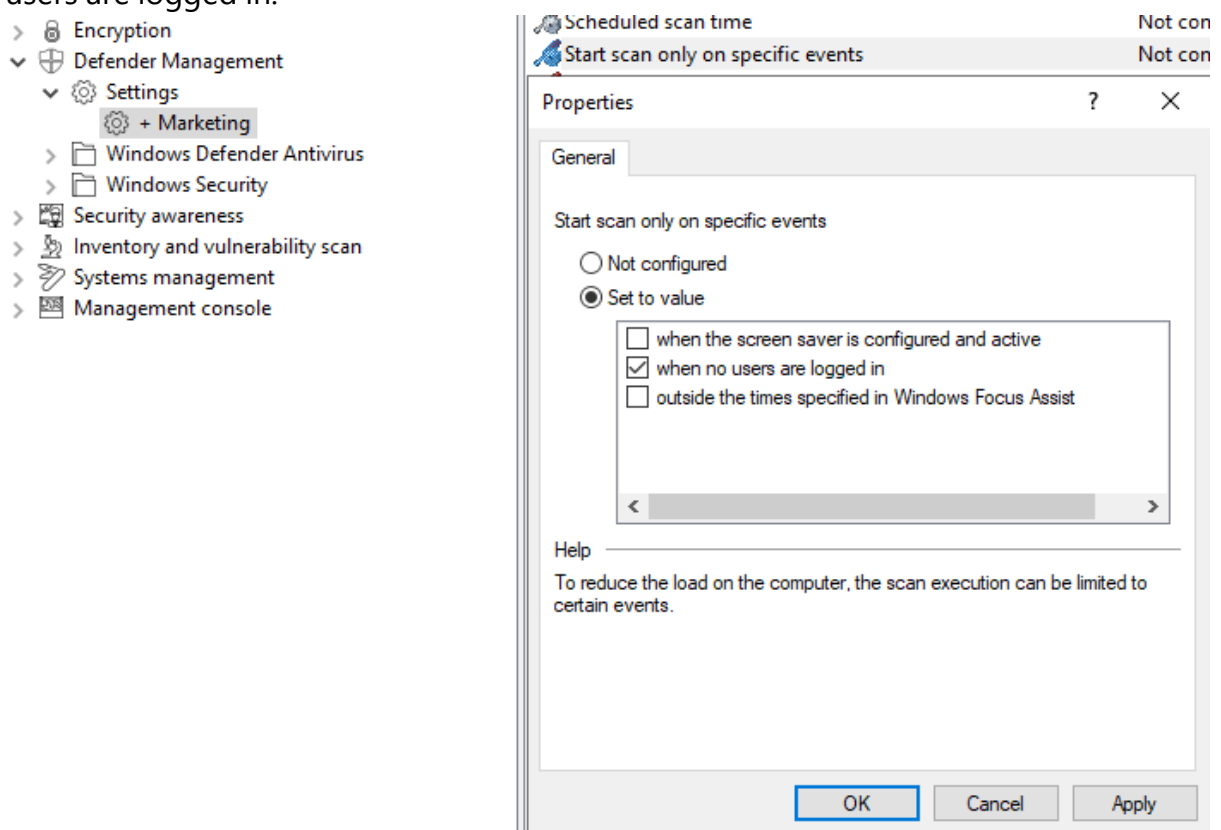
7. Save your setting and then assign the policy.

13.7.2 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.
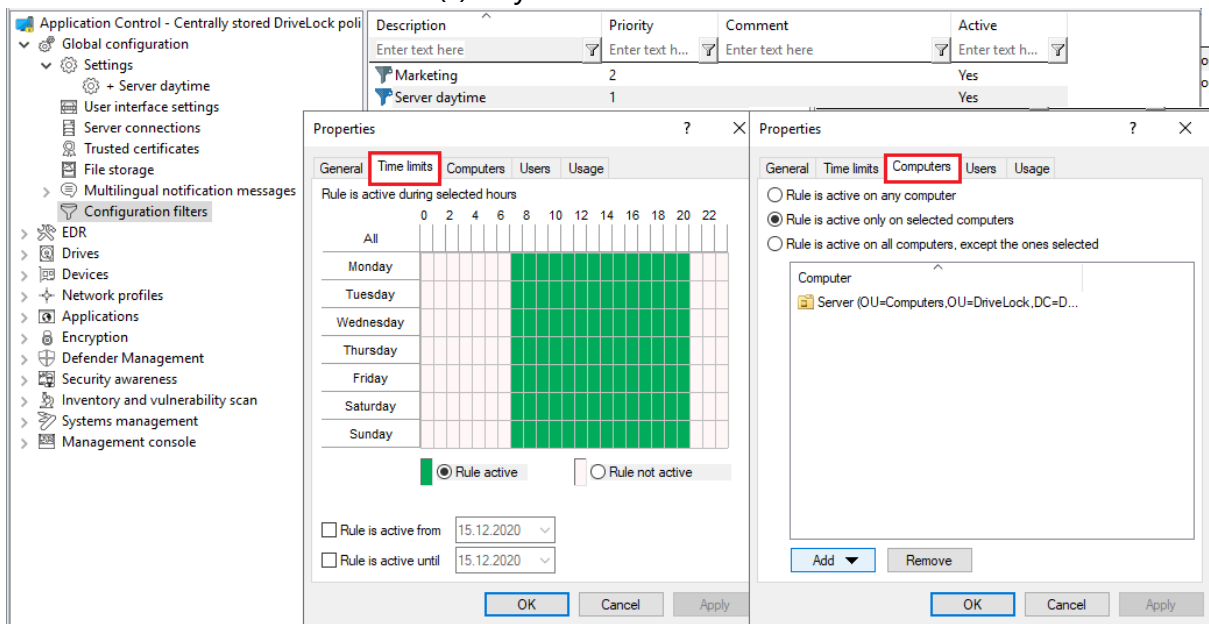
5. Save the configuration filter.

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** .
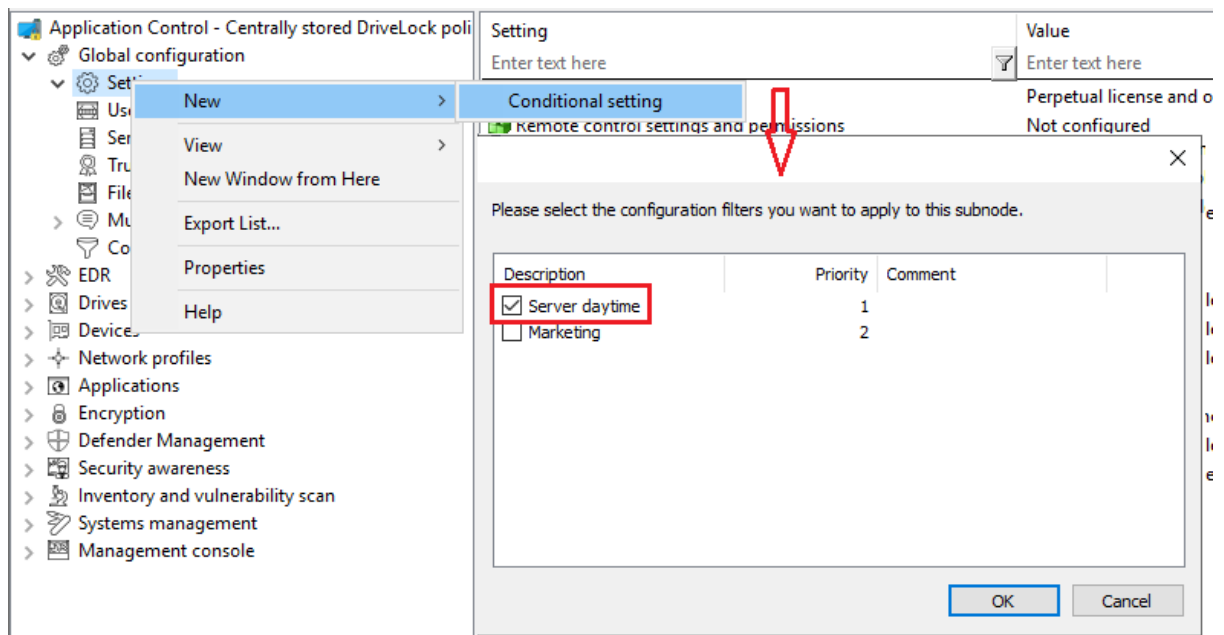
8. Then, in this conditional setting, open the **Automatic updates** option and uncheck **DriveLock Agent** which is checked by default .
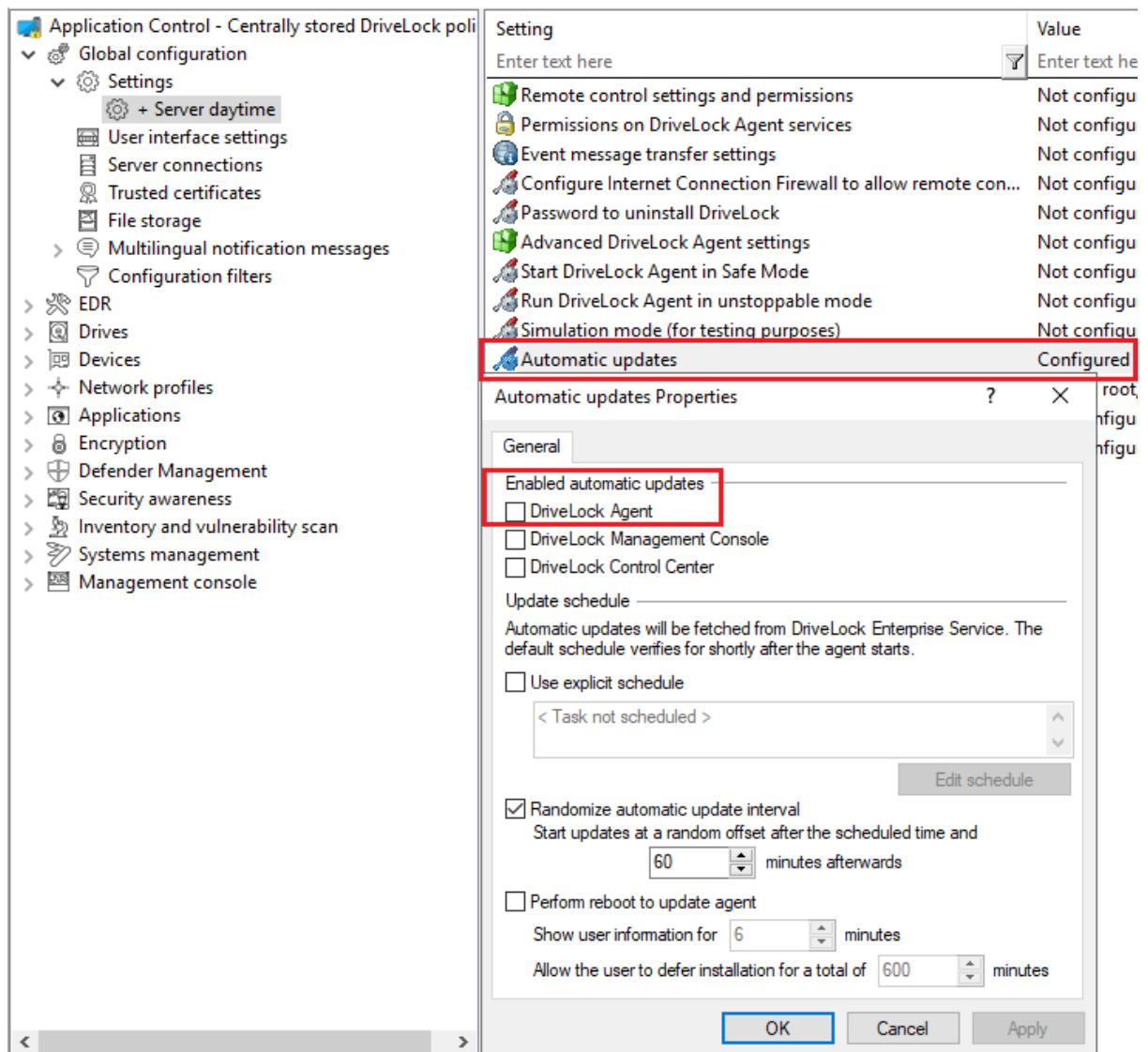
9. Save your configuration.

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.

13.8 Self service rules

Using self-service rules, you can allow authorized users to unlock DriveLock Agents themselves without having to use the DriveLock Management Console (MMC) or the DriveLock Operations Center (DOC).

How to unlock agents is explained here.

13.8.1 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 release wizard** the user gets the possibility to use another account for login at the beginning of the self-service wizard.

13.8.2 Definitions for self-service

To allow users to use the self-service unlock, they must be included in a self-service rule. 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 rule.
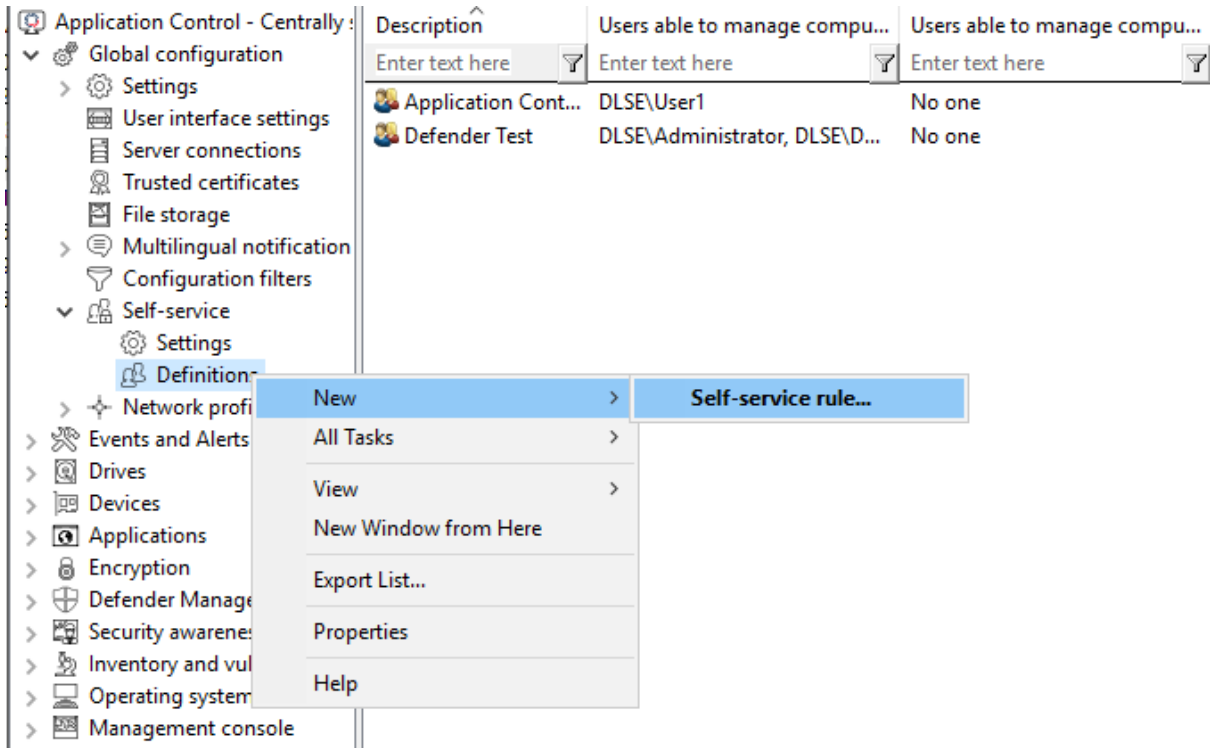
2. On the **General** tab, enter a short description and a comment to identify this self-service rule. Use the **End user information** field for an explanation of when and for what the user should use this rule. This text is then displayed in the wizard if more than one group is configured and selectable.

3. On the **Self-service** tab, select the device types and modules to be shared and the time for sharing.
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 .

13.8.3 Starting the self-service wizard

The self-service share 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**
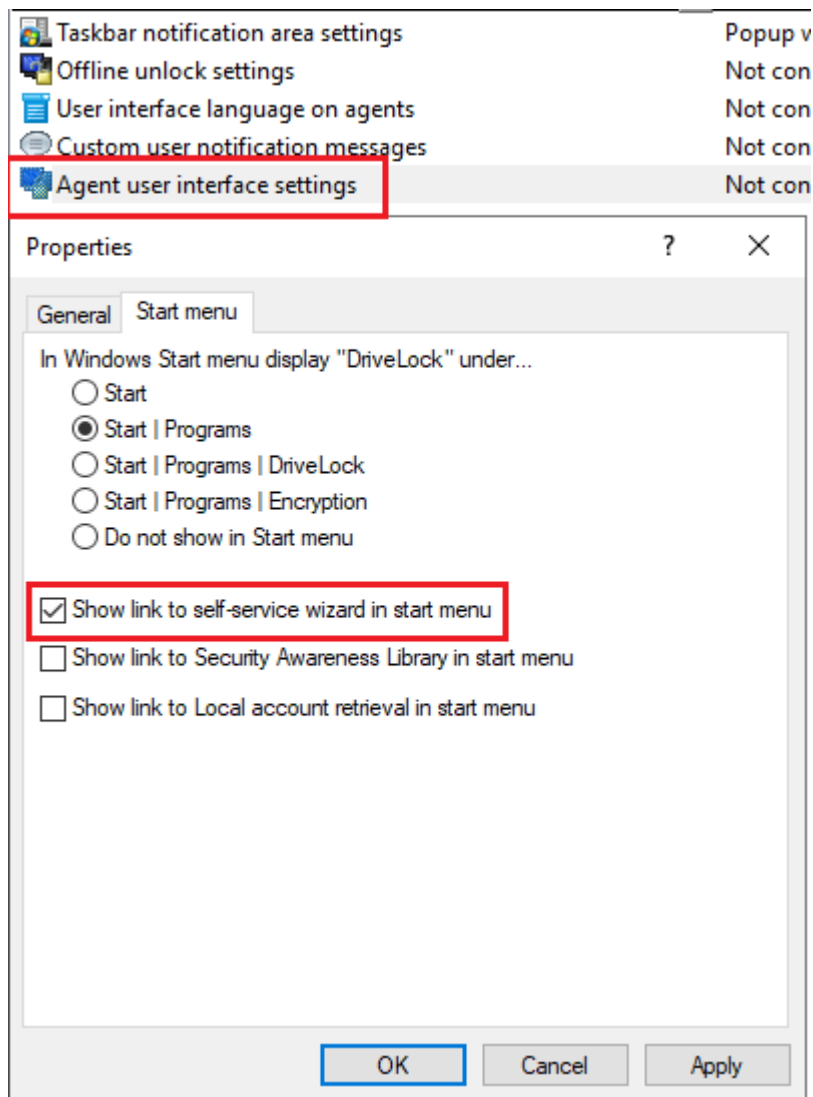
2. In the **Taskbar notification area settings** on the Options tab. Add Self-service... and set the entry to the desired position.
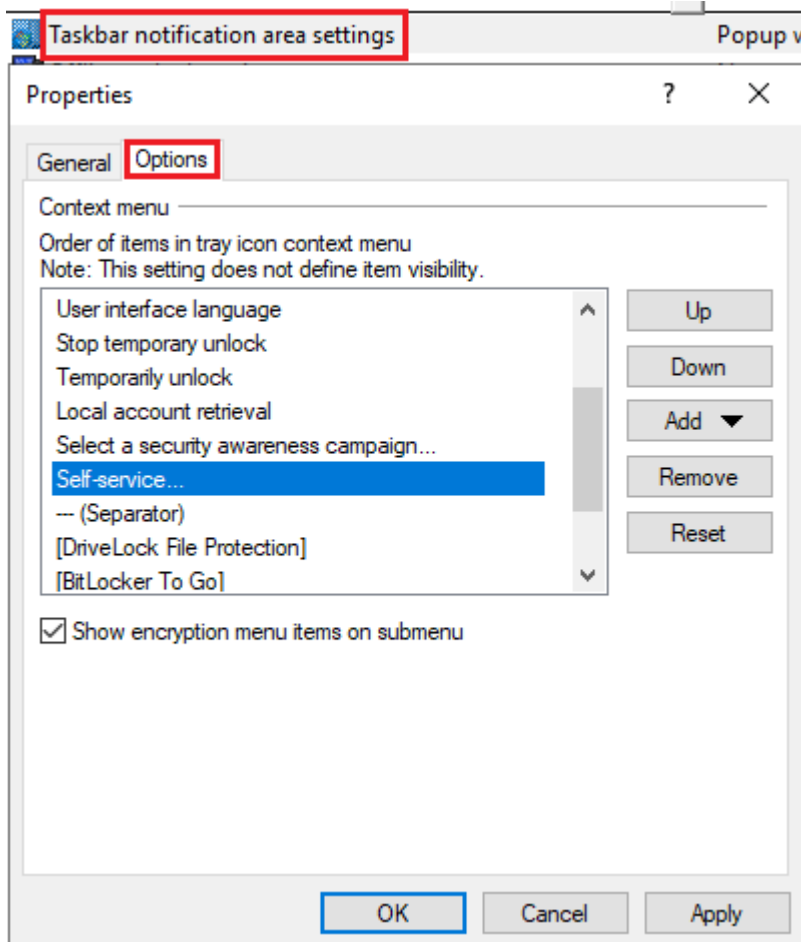
3. You can also set up the Self-service wizard to start as soon as a usage policy is applied. You can find out more here.

13.8.4 Use case for self-service with Application Control

Goal : Simple self-service with the goal of allowing specific users to 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 rule. 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:
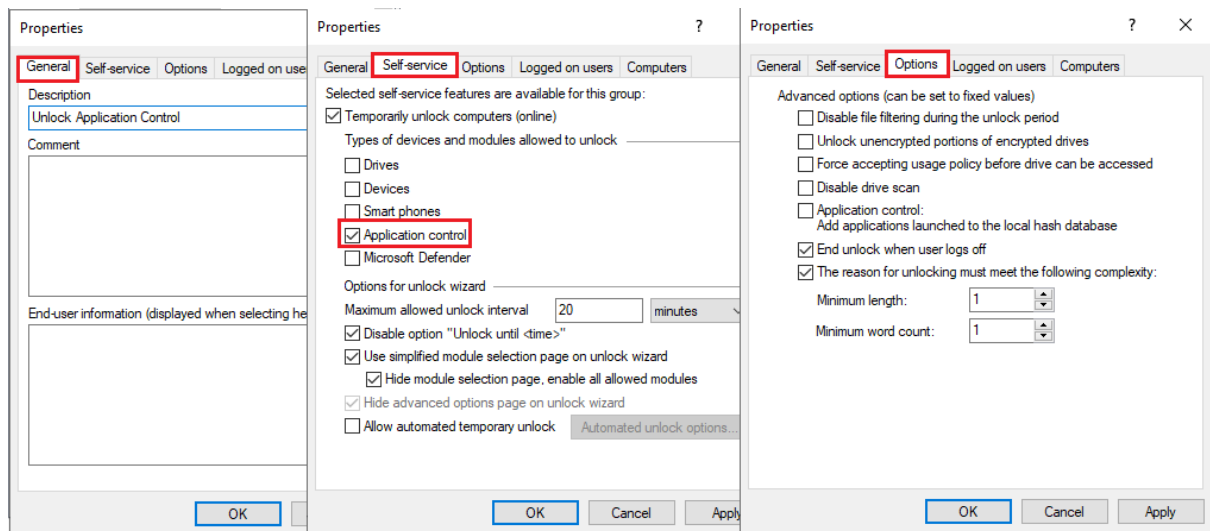
3. On the **Registered Users** and **Computers** tabs, select the users and computers you want to enable self-service sharing for. Use the Add button for this purpose. See example below:
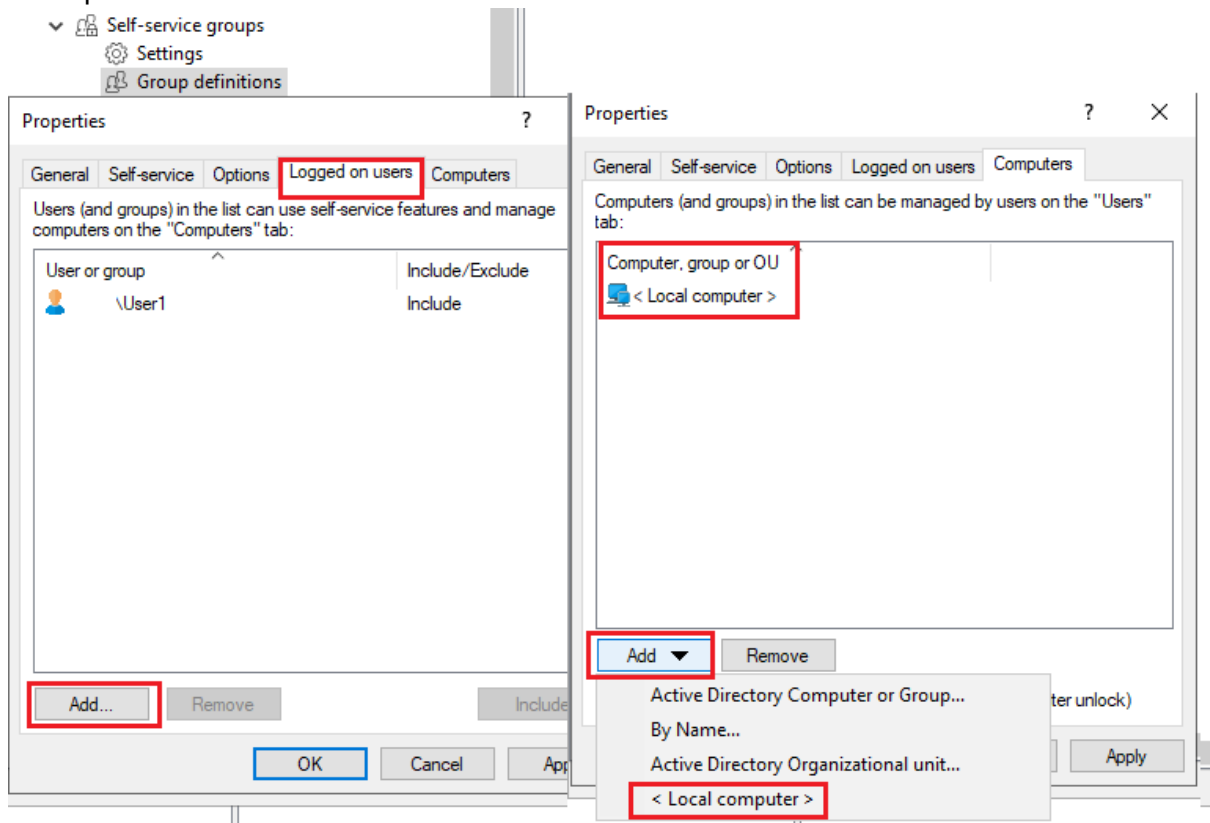
4. Set the appropriate settings for the SB share in **Global configuration**, as shown here (explained under 1. and 2.).

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.
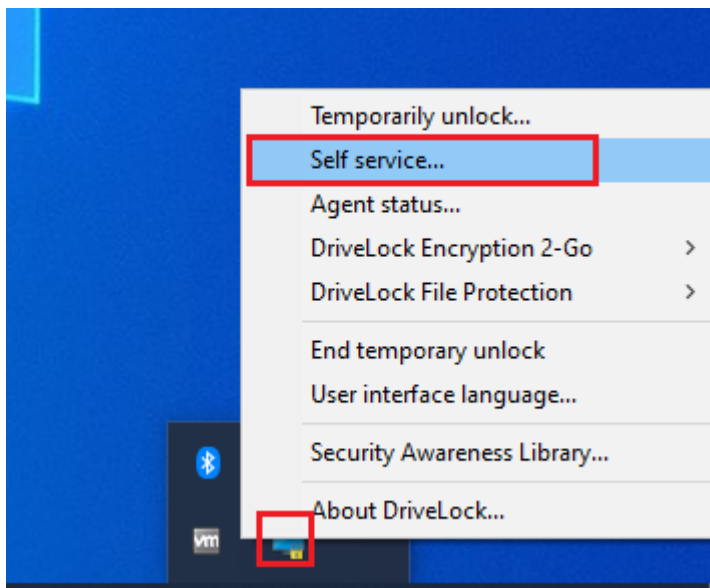
13.9 Networks

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.

13.9.1 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:
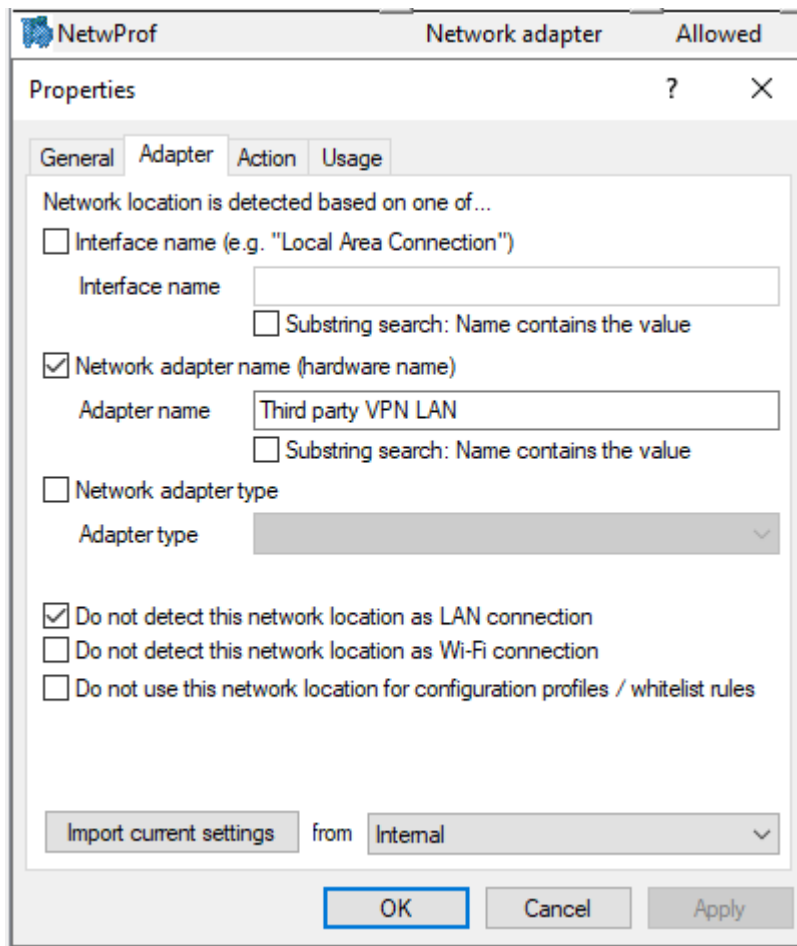
- **Allow users to configure personal networking profiles (compatible with agents prior to version 2022.2)**: This setting can only be used for agents with older versions (before 2022.2). This feature is no longer available for new agents.

13.9.2 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.
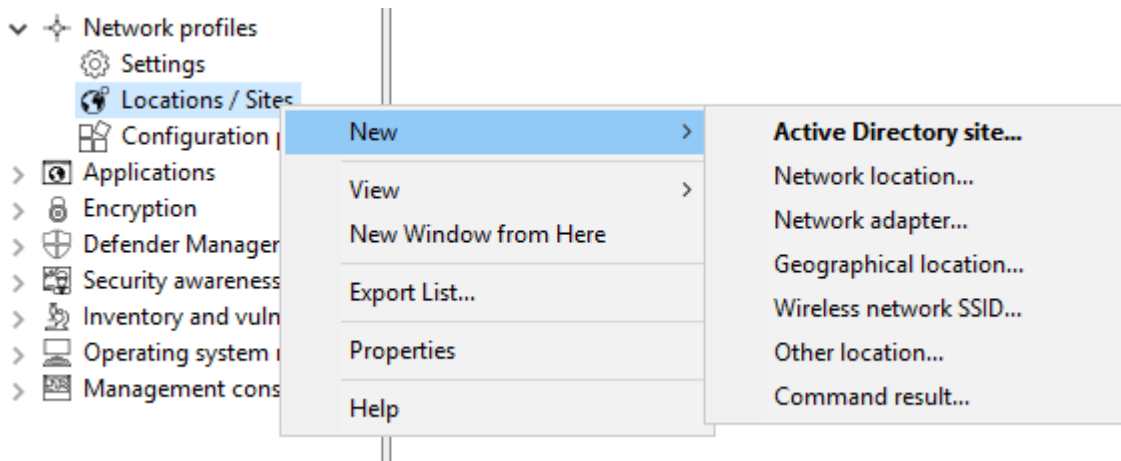
The following types of sites are available:

- **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").

13.9.3 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 .
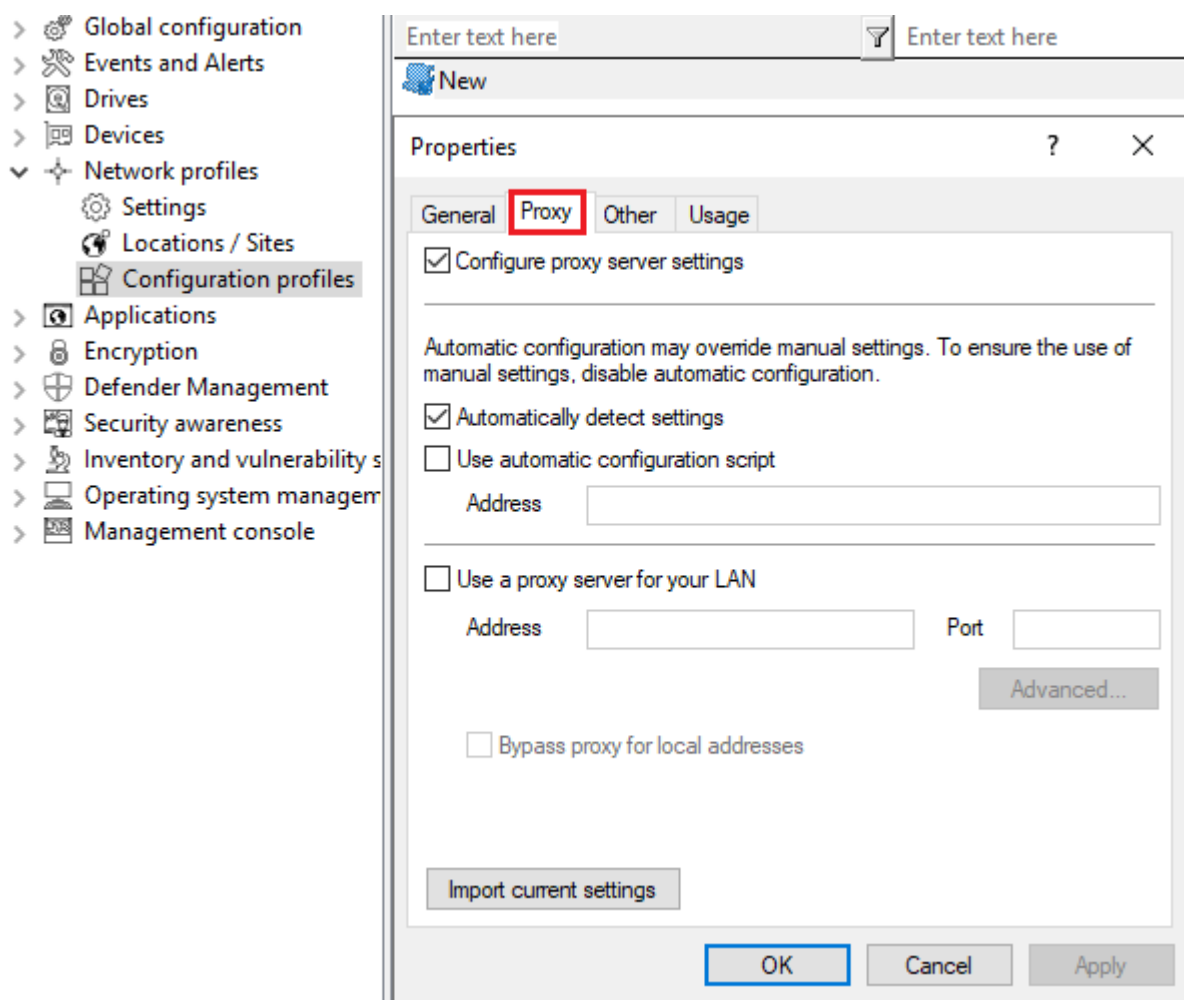
To enable that Internet Explorer settings are automatically adjusted, enable "Configure proxy server settings". Then you can read out the currently valid settings from the local con-

figuration 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.
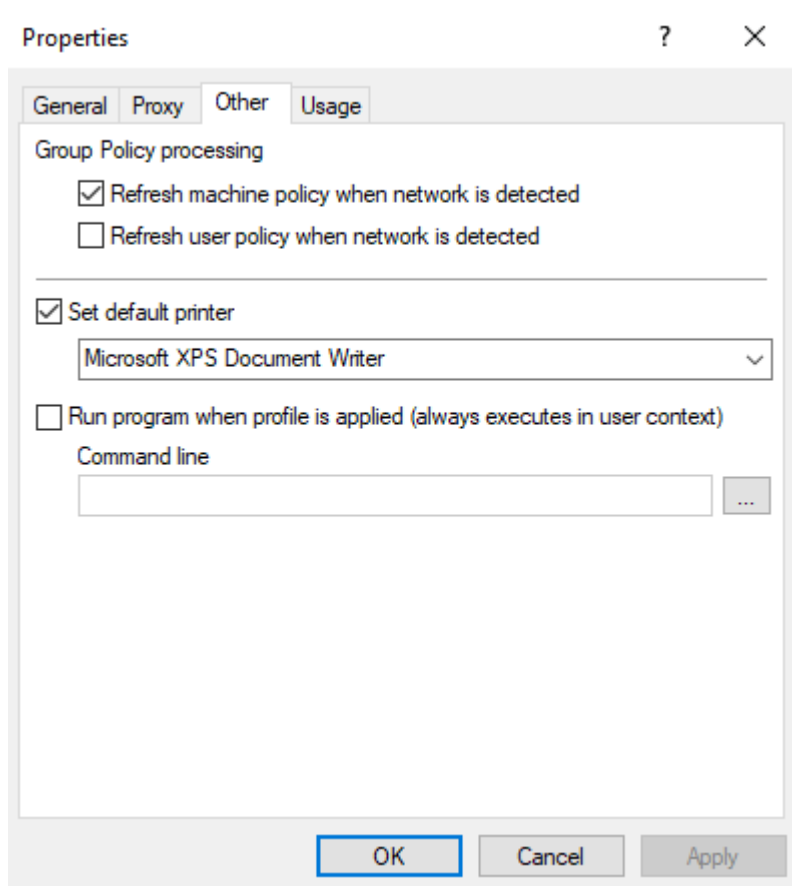
Select a printer from the drop-down list if you want to change the current default printer.

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 "*".

14 Application Control

14.1 Overview

DriveLock has different feature sets to offer.

	Application Control (Legacy)	Application Control	Application Behavior Control (ABC)	Application monitoring
Whitelisting or blacklisting of applications	yes	yes	-	-
File properties rule	yes	yes	-	-
Hash database rule	yes	yes	-	-
Special rule	yes	yes	-	-
Whitelisting or blacklisting of DLLs	-	yes	-	-
Whitelisting or blacklisting of scripts	-	yes	-	-
Local whitelist	-	yes	-	-
Predictive whitel- isting	-	yes	-	-
Application col- lections	-	yes	yes	yes

Local learning	-	yes	yes	-
Application behavior rules	-	-	yes	Reporting
• File accesses	-	-	yes	Reporting
• Registry accesses	-	-	yes	Reporting
• Script execution	-	-	yes	Reporting
• Starting applications	-	-	yes	Reporting
• Loading DLLs	-	-	yes	Reporting
Application behavior recording	-	-	yes	-

> Note: The legacy application control license cannot be combined. Both application control with machine learning function (Application Control) and application behavior control can be used individually or combined.

14.2 Features

The Application Control feature allows you to selectively restrict or allow the use of applications on your corporate computers.

DriveLock Application Control includes several functions:

- Application rules: You can use blacklisting and/or whitelisting to define simple rules as to which applications are executed and which are blocked. This lets you control the use of any application on computers where DriveLock is installed. Application unblocking or blocking can be defined based on various filter properties.

- Application behavior rules: Define exactly what applications are allowed to do, for example, the permissions they get, the directories they can write to, and the processes they can start. By recording application behavior via remote agent control, you can automatically generate application behavior rules.

- Local learning: In addition to the rules you define in policies, you can also make the DriveLock Agent learn locally what DriveLock Application Control allows.

14.3 Overview in the DriveLock Management Console

In the Taskpad view of the **Applications** node, you can configure basic settings for Application Control. From this overview, you can quickly set the scan and blocking mode, configure standard application rules (four special rules) as well as other application rules, application behavior rules, application collections and script definitions.

You are also provided with samples of rules that are already preconfigured to represent useful scenarios. If you select the option **Add out-of-the-box recommended block rules** or **Add out-of-the-box sample rules**, the new **Recommended block rules** folder will be created to contain these blacklist rules.

Whenever you change the settings, such as the **scanning and blocking mode**, this is reflected in color (e.g. green, if the current mode is set to Whitelist).

You can also select the individual settings on the left in the DriveLock Management Console. Click **Advanced configuration** to open the corresponding subnode.
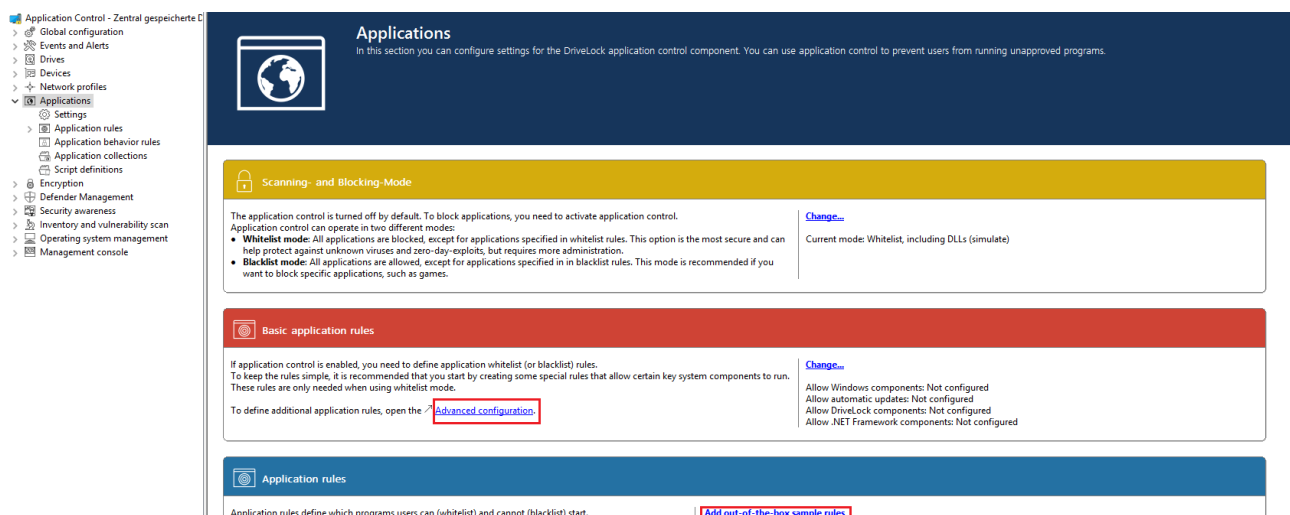
14.4 Application Control events

All events on the corresponding DriveLock agents are automatically displayed by feature in the DriveLock Operations Center (DOC) under **Events** and in the DriveLock Management Console in the **Events and Alerts** node.

DriveLock Agent sends events when an application is executed or blocked. The application database is filled with this event information. The events must be configured in the policy so that they are sent to the DriveLock Enterprise Service (DES).

The following events are crucial:

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

In the **Application Control** folder you can check all related events and configure responses if necessary.

The figure shows the event that indicates a change in the learning or control status of an application:
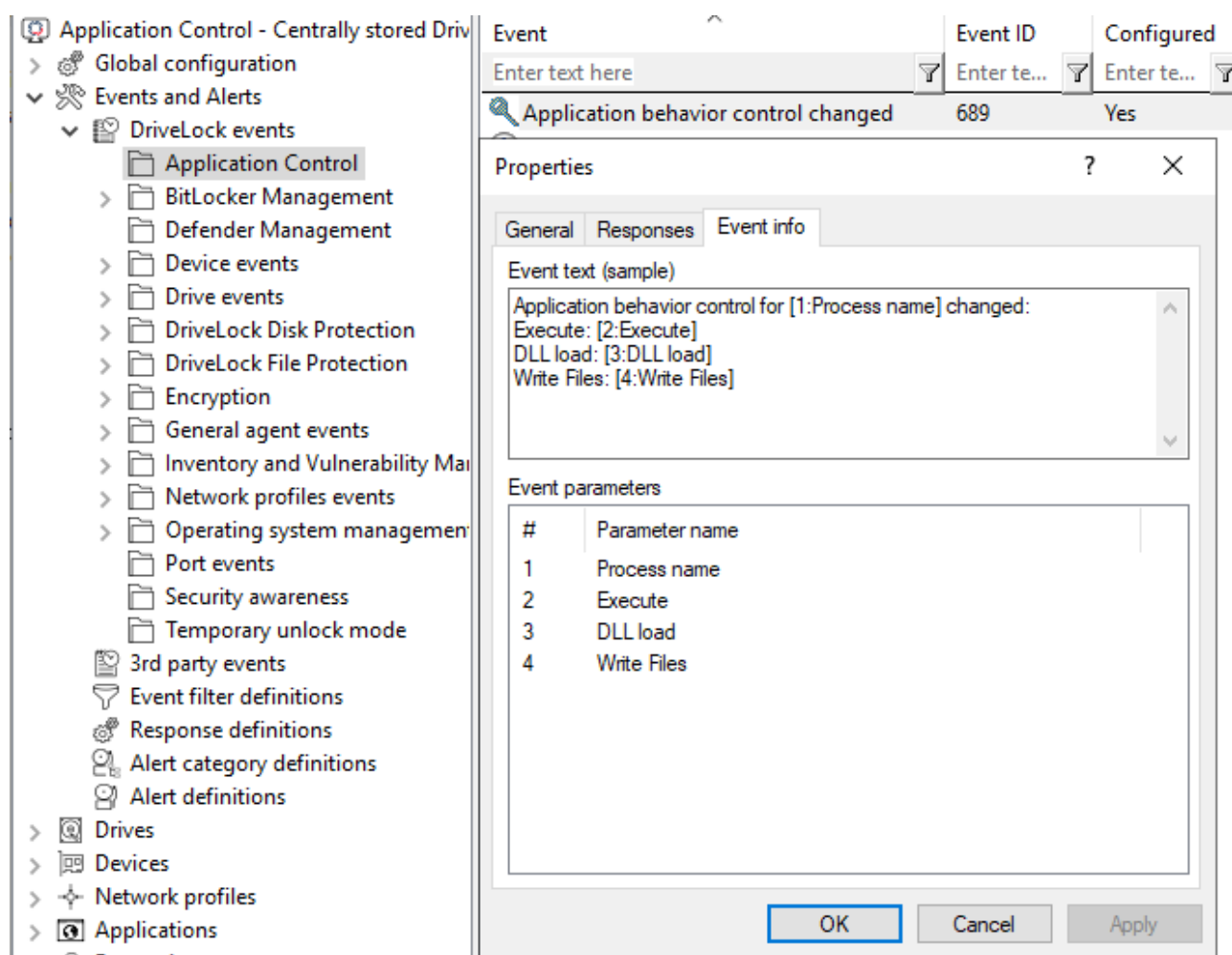
A detailed description and list of all DriveLock events can be found in the DOC.

14.5 Settings

The following settings can be configured for DriveLock Application Control:

1. General settings:
   - Scanning and blocking mode
   - General hash algorithm
   - Always audit application execution
   - Custom user notification message

2. Troubleshooting settings (driver settings)

   > 📝 Note: We recommend using these settings only after consulting DriveLock support.

   - Application control caching
   - Cache lifetime ("time to live")
   - Paths without hash generation for executed applications

3. Setting for trusted processes

4. Local whitelist:
   - Activate local whitelist
   - Predictive whitelisting based on digital signatures

5. Settings for local learning:
   - Directories learned for the local whitelist
   - Additional extensions learned for the local whitelist
   - Upload local whitelist to DriveLock Enterprise Service
   - Start learning the local whitelist automatically

6. Settings for application behavior control
   - Duration of the learning phase for application behavior control
   - Ask user in case of unusual application behavior

> 📝 Note: The use of conditional settings (configuration filters) is also possible here.

14.5.1 Scanning and blocking mode

When executable programs are scanned or blocked, DriveLock checks the file while it is being loaded into memory by the Windows operating system. Depending on the result of the check and the rules configured in the DriveLock policy, DriveLock allows or denies program execution.

Scanning or blocking DLLs also works in this way. When programs load DLLs, all of them are checked as they load.

> ⚠ Warning: If you plan to activate Application Control in whitelist mode including DLLs, you must ensure that you do not block any DLLs that are required for your system to function fully.

Note that Windows installs numerous DLLs that are not identified as part of the operating system or the .NET Framework. Also, not all of these DLLs are installed in the Windows system directory and some do not have a ("valid") Microsoft signature. This is why none of the special rules cover such DLLs.

Example:

Some versions of Windows come with Microsoft OneDrive installed as a standard feature. OneDrive is installed in the user profile and is not part of the operating system. However, the Windows Explorer reloads OneDrive DLLs. Windows Explorer will quit if these DLLs are not whitelisted in your rules.

Best practice:

We recommend that you enable predictive whitelisting or local whitelisting before you enable DLL blocking. In any case, you should start in simulation mode and evaluate the application control events in order to whitelist all DLLs required by the system.

14.5.1.1 Simulation

Before you really start blocking programs, make sure to use one of the two simulation modes (whitelist (simulate) or blacklist (simulate)) to test the effects of your rules in advance. During a simulation, DriveLock generates event messages for started or blocked applications based on configured rules, but execution itself is neither allowed nor prevented.

Use the simulation modes to identify applications that users are running before you enforce any blocking rules. Use the Windows Event Viewer for analysis or examine the data in the DriveLock Operations Center (DOC) to quickly find corresponding events.

14.5.1.2 Whitelist or Blacklist

To fully enable Application Control, select Whitelist or Blacklist from the drop-down list.

If you select Whitelist, all applications will be blocked unless there is a suitable application rule that removes this block.

Blacklisted applications, by contrast, do not initially prevent any application from running unless there is a specific rule that blocks them.

14.5.1.2.1 Whitelist mode

In whitelist mode, all applications are allowed that match a whitelist rule. Using blacklist rules, you can block individual applications in this case as an exception to an existing whitelist rule or template.

Priority: blacklist rule - whitelist rule - other settings

To allow all users to run all programs in the Program Files folder, create a directory rule and allow all applications within this folder to run. To prevent one of these applications from running on one computer, create a blacklist rule for only this application and apply it to the computer.

14.5.1.2.2 Blacklist mode

When using the blacklist mode, all applications are allowed to run unless they are listed in blacklist rules or templates. Use blacklist rules or templates in this mode to specify the applications that users are not allowed to start. Use whitelist rules in this mode to define exceptions to blacklist templates or rules.

Priority: whitelist rule - blacklist rule - other settings

Example: Users in your organization are not allowed to run the program "Skype". However, your CEO must use Skype when being out of the office. To allow this, create a blacklist rule to block Skype for all uses. Then define a whitelist rule allowing the Skype application and configure it to apply to only the CEO's account.

14.5.2 General hash algorithm

With this setting, you specify a fixed hash method that is used for reporting, for the local whitelist and for creating new rules.

You can change the hash algorithm later or use a different hash algorithm in rules. In this case, the agent may have to calculate multiple hashes of a file, which can lead to slight performance losses.

> ❗ Warning: DriveLock Agents prior to version 2022.1 only use the configured hash algorithm, which means that rules with a different hash algorithm will not work on these agents.

The SHA-256 hash method is recommended.

14.5.3 Always audit application execution

If you want to collect information as events about started programs independent of the selected operation mode, choose **Always audit application execution (independent of blocking mode)** and check **Enabled**.
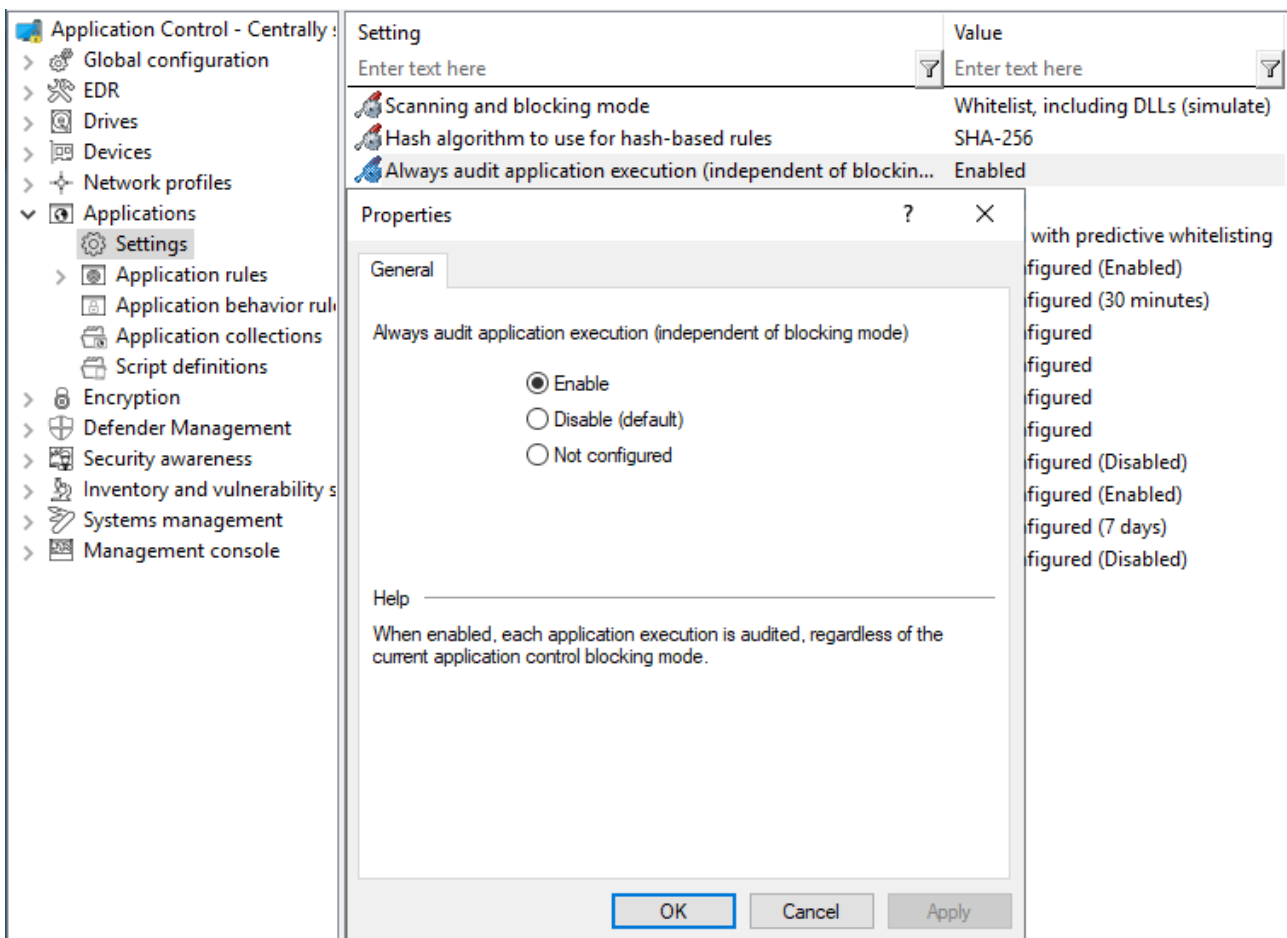
> ☑ Note: However, logging each successful program startup can slow down system performance. Sending all events to the DriveLock Enterprise Service also increases the network load and database size.

14.5.4 Custom user notification message

You can define a **custom user notification message** for each whitelist rule. Unless specified otherwise, DriveLock will display this message when the Application Control blocks an application.

If you configured a multilingual message text for the current language, DriveLock will display the standard messages defined for this language instead of the message configured in this dialog box.

Select **Display custom message** to enable the messages and type the message to be displayed to the user. Use the %EXE% variable in the message to inform the user of the name of the application that was blocked. It is replaced by the path and file name at runtime.

Click Test to preview the message.
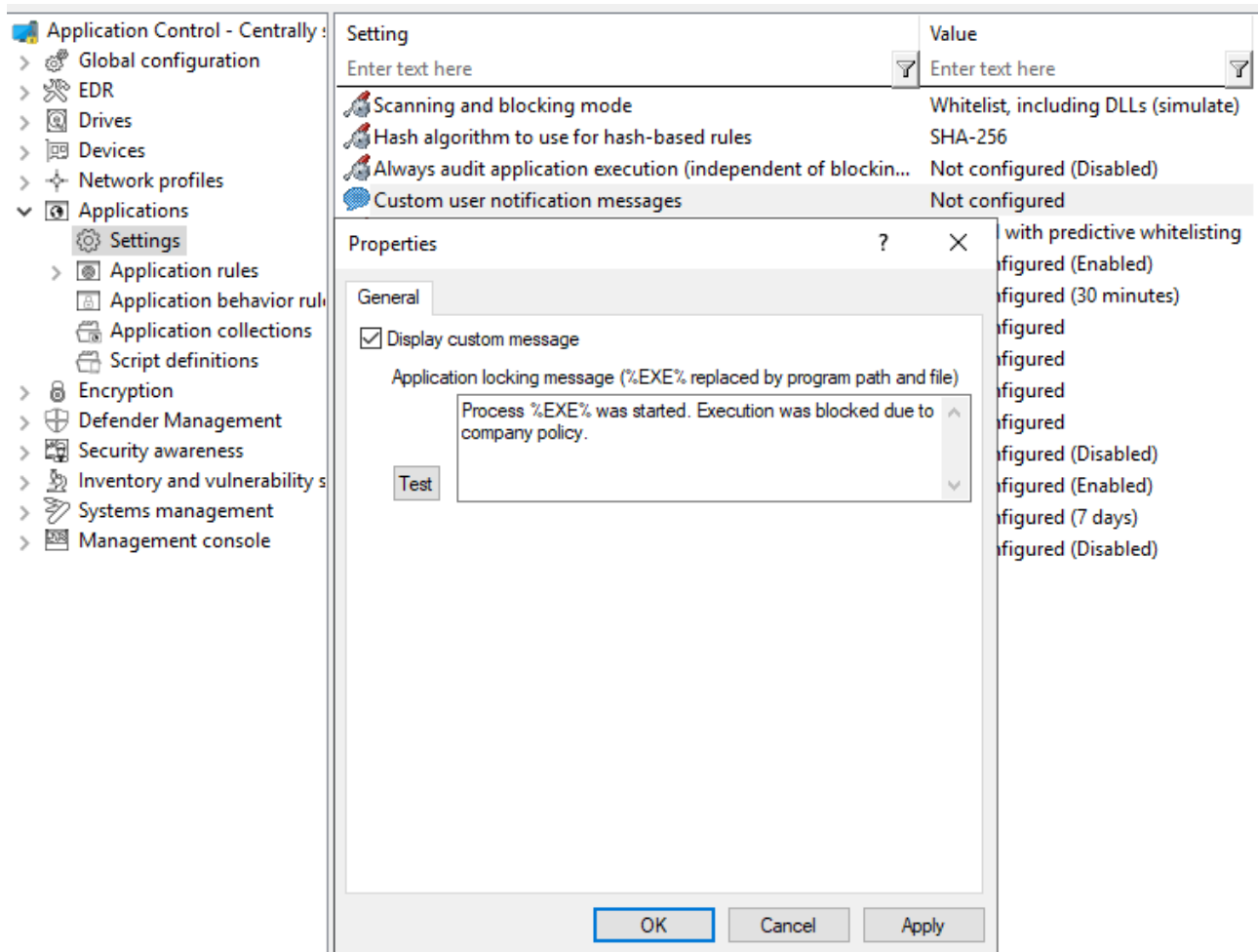
14.5.5 Trusted process

This setting can be configured if you are using client management software for software distribution in your company. On the Local Learning tab in some application and application collection rules, you can also specify whether this client management software is given special permissions (for example, whether it can start other programs that are not on the whitelist) and is therefore considered trustworthy.

The following configuration options are available:

1. **Not configured** is the default option.

2. **Set to configured list**:
   Add the name of the software. This software is checked when the DriveLock Enterprise Service starts.

14.5.6 Activate local whitelist and predictive whitelisting

Use these central settings to activate or deactivate the use of the local whitelist or predictive whitelisting.

1. **Enable local whitelist**:
   Once the policy with this setting is assigned, the DriveLock Agent starts the learning mode and afterwards activates the local whitelist with the learned applications.

2. **Predictive whitelisting based on digital signatures**:
   This setting offers the following automatism, especially for update processes: Files are automatically added to the local whitelist if they either have the same product description or the same digital signature as the signatures of the files learned in the local whitelist.
   Use this option to quickly and easily allow update processes (e.g. of browsers). Creating well-defined rules for updating applications via local learning (for example, using learning behavior recording, using the recording results in application behavior rules, or specifying permissions accurately) is more time-consuming, but it gives you a more reliable result.

   > ✔ Note: As of version 2024.1, predictive whitelisting is deactivated by default and must be activated manually. Please ensure that the settings of older and newer agents do not differ, as this can otherwise lead to changes in behavior.

14.5.6.1 Display local whitelist via agent remote control

When you use Application Control in conjunction with local learning, a database of applications approved for this computer is created on the DriveLock Agent (local whitelist). You can connect to an agent and view the contents of this database or delete individual entries.

Display application control whitelist:

1. Open the **Operating** node in the DriveLock Management Console and select **Agent remote control**.

2. Select **Display local application control whitelist** from the context menu of the relevant DriveLock Agent.
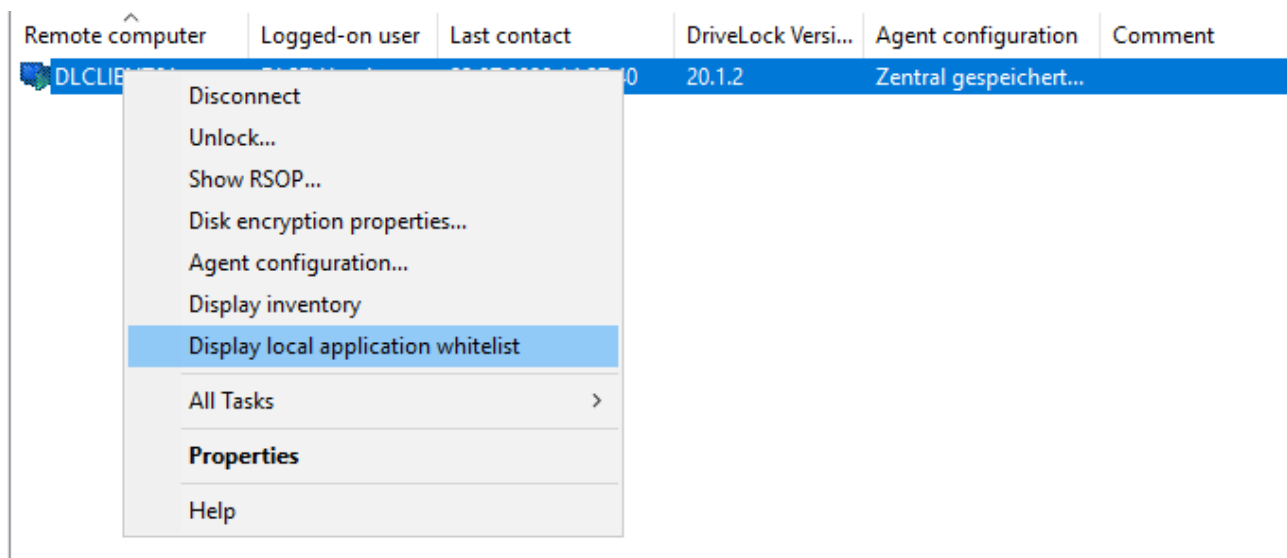
If you want to delete individual entries, possibly because too many applications have been learned, proceed as follows:

1. Double-click the relevant agent to display its properties.

2. On the **Application Control** tab, select the **Display...** button.

3. A window with a structure similar to Windows Explorer opens. Opening the database may take some time depending on its size.

4. You will see the learned applications here. Select the entry you want to delete.

14.5.6.2 Local learning

DriveLock Application Control provides a learning functionality that can be used to learn the behavior of applications on DriveLock agents.

To do so, the client computer is set to learning mode and a local whitelist (hash database) of the installed programs and DLLs is created. This individual local whitelist then contains the approved files that have been learned locally. Once the learning mode is completed, the local whitelist is activated and only the "learned" programs can be executed. To ensure that Application Control does not block programs that are installed or updated at a later time, you can temporarily reactivate the learning mode for the installation or update

You can activate local whitelisting either by configuring the Local whitelist and predictive whitelisting setting or by creating a Predictive Whitelisting rule.

Local learning is triggered

- by specifying the corresponding learning settings in an application list rule or

- by using an application behavior rule that was automatically created from an application behavior recording.

When the local whitelist is activated, you can define additional settings to configure the learning functionality.

The local whitelist is merged incrementally with the application database on the DriveLock Enterprise Service (DES). When you create file properties rules, you can also select from this global application database.

14.5.6.2.1 Application behavior recording and control

There are two ways to partially or fully automate application behavior control.

1. Using a reference computer
   You can easily track and learn background actions, such as access from applications, running programs, or written files, with the help of behavior recording. The results of this recording can be stored in a file.
   - On a reference computer, enable application behavior recording for one or more applications using the Agent remote control functionality.

   - You will then work with these applications, making sure that all important actions are performed, especially updates and configuration changes. This involves recording the behavior of the applications, such as determining which files are written and which other programs are started.

   - Then you can generate application behavior rules from the recorded data.

2. Automatic learning on individual DriveLock Agents
   - With an application collection rule, you can specify that the behavior of an application is restricted to the actions that are learned during a learning phase. In this case, only the access modes Execute, Load DLL and Write file are supported.

   - During a learning phase, the system learns how the application behaves and after completing the learning phase, any deviating behavior will be blocked.

14.5.6.2.1.1 Configure application behavior recording

Start a behavior recording to find out how an application behaves.

Note: Make sure that the application has been whitelisted.
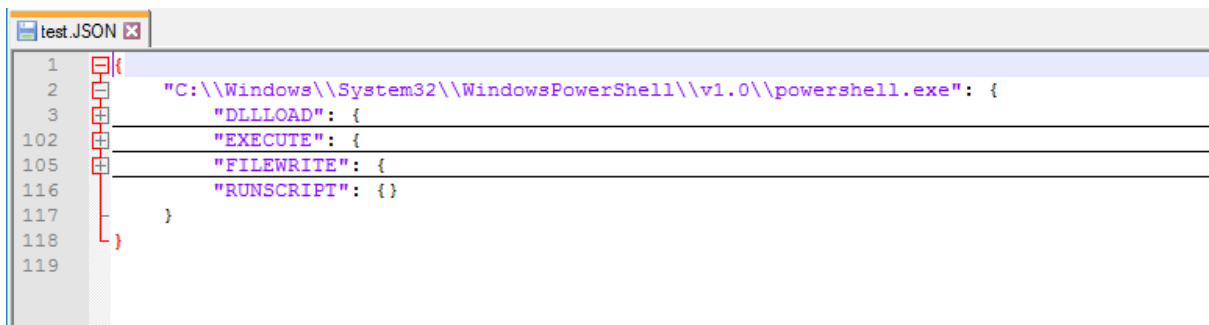
Once you have saved the behavior recording, you can then use it to generate application permissions that are restricted to precisely the learned behavior. This way, only the behavior that is actually needed will be allowed, everything else will be blocked.

Please do the following:

1. Open the **Operating** node in the DriveLock Management Console and select **Agent remote control**.

2. Double-click the relevant agent to display its properties.

3. Select the **Start...** button on the **Application Control** tab in the **Application behavior recording** section.

4. Add directories or programs whose behavior you want to record.

5. Select which kind of accesses you want to record, see example.
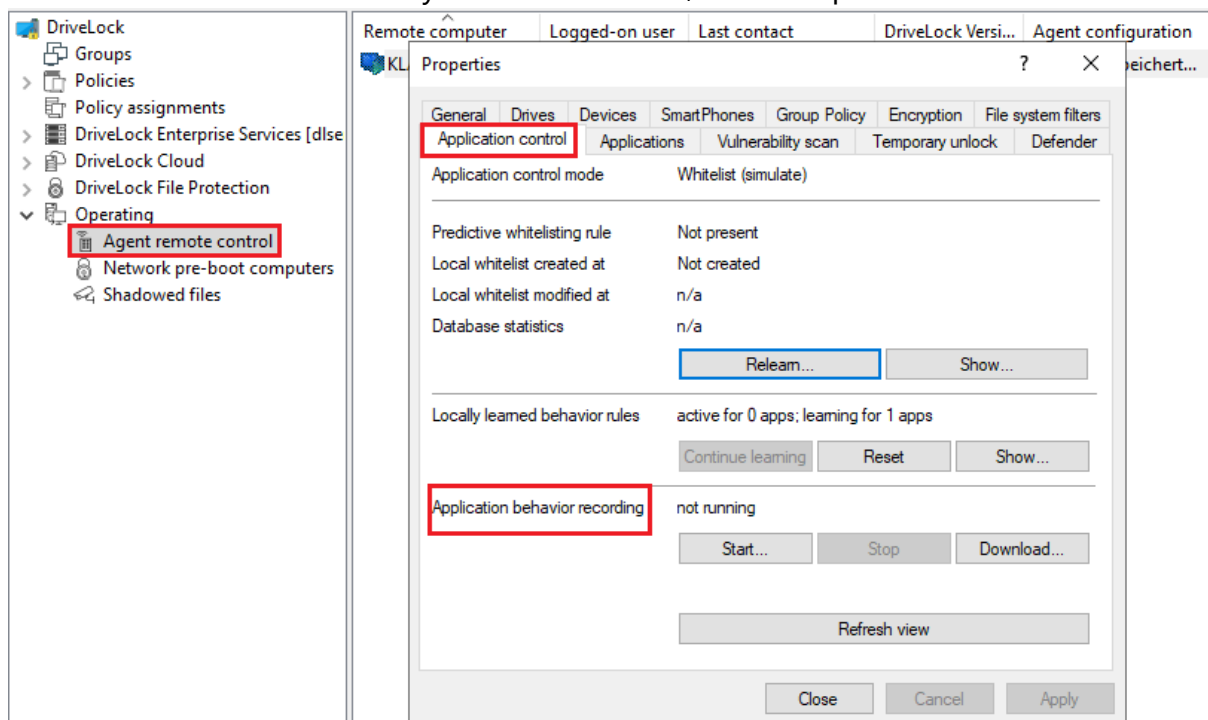
6. If you want to delete a recording that already exists, select the checkbox.

7. It is recommended to limit the recording to a certain period of time. You can enter a maximum of 10 days here, but we recommend a much shorter period.

8. Once you have tested the application, for example on a reference computer, for a certain period of time and collected a sufficient amount of data, click **Download...** to download the behavior recording in a JSON file and evaluate the results.

```
 test.JSON

   1       {
   2           "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe": {
   3               "DLLLOAD": {
 102               "EXECUTE": {
 105               "FILEWRITE": {
 116               "RUNSCRIPT": {}
 117           }
 118       }
 119
```

9. You can now use this results file in an application behavior rule.

14.5.6.2.1.2 Locally learned application behavior rules

The information you see in the **Locally learned behavior rules** section reflects the settings you defined in the application collection rules on the **Local Learning** tab. As soon as an agent uses a policy with these settings, a learning phase is started, thus activating application behavior control. The learning phase for the three modes (load DLL, execute, write files) are independent of each other.

The following states and buttons are available:
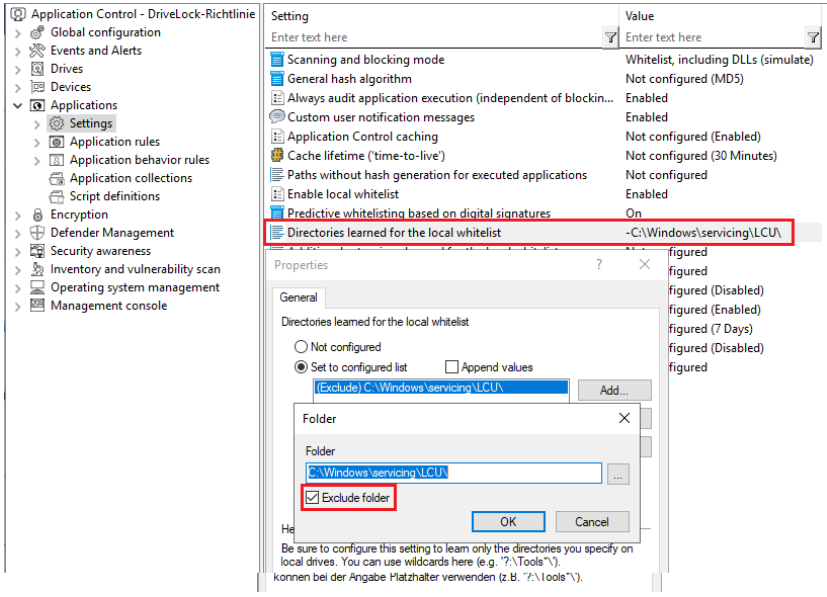
- **not active**: There are no applications specified yet that need to be learned or controlled.

- **active for**: The specified number of applications is blocked when a behavior is detected that has not been learned yet.

- **learning for**: The applications are still in the learning phase.

- **Continue learning**: The start time of the learning phase is reset, the list that has been learned so far is continued.

- **Reset**: The list that has been learned so far is deleted. The activity display returns to **not active**.

- **Show...**: Clicking on this button opens a dialog in which the learned entries are displayed, see figure.
  If you save the result in a JSON file, you can use it to have application behavior rules generated from it. To do this, proceed as described in chapter Generate application behavior rules from behavior recording.
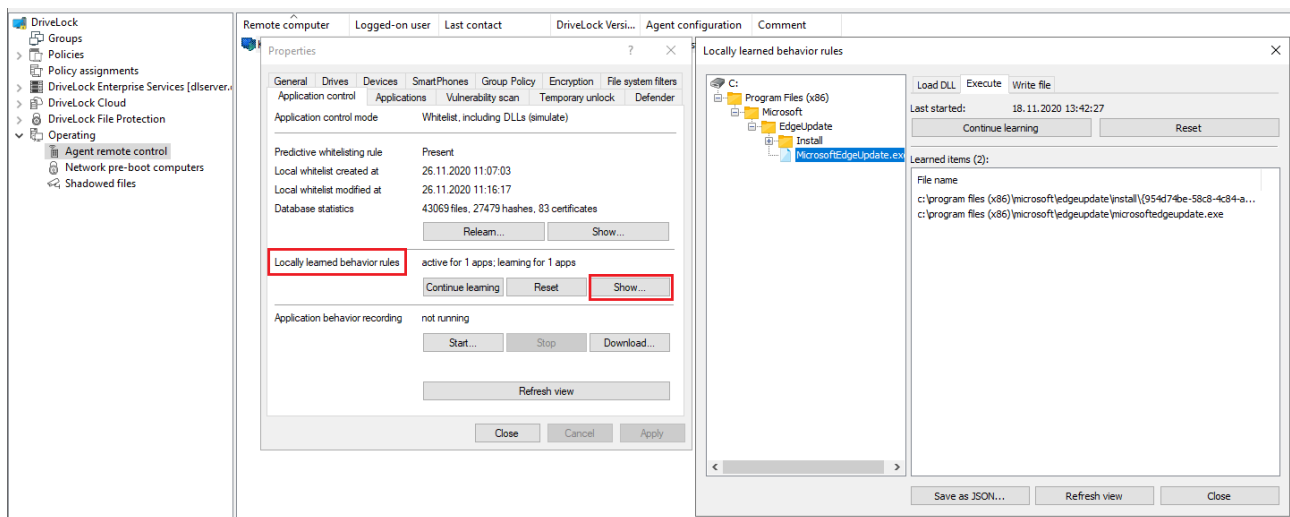
14.5.7 Settings for local learning

You can configure the following settings for local learning:

Setting	Configuration options
Directories learned for the local whitelist	Typically, the files are learned from all local hard drives. You can specify that this is done in certain directories where the software to be learnt is found, for example the Programs directory. Enable the setting by specifying the directories in the list. It is also possible to exclude certain directories from learning. For example, we recommend explicitly excluding the directory C:\Windows\Servicing\LCU in order to accelerate the speed of application learning. Please also exclude C:\Windows\Temp so that not all temporary files are learned, which could pose a security risk under certain circumstances. In the Policy Editor in the DMC, proceed as illustrated in the figure:
Additional extensions	You can specify additional file types in addition to the

Setting	Configuration options
learned for the local whitelist	standard file types to add to the local whitelist. This is useful if an application uses a different file extension for a file type, or in order to learn scripts that are already running on the system.
Upload local whitelist to DriveLock Enterprise Service	Once created, you can have the local whitelist sent to the DriveLock Enterprise Service (DES), which maintains a list of all locally learned files. This list can then be used to generate hash rules. The default option is **Disabled**.
Start learning the local whitelist automatically	Use this setting to define whether local whitelist learning is started automatically (i.e. as soon as the corresponding policy is assigned to the DriveLock Agent) or by users. The default option is **Enabled**. Select **Disabled** if you want to wait until a user actively starts learning. This means that the user is responsible for the initial learning of the local whitelist. You can configure the settings of the agent user interface accordingly. To do so, go to the **Global configuration** node, select Settings and then the **User interface settings** sub-node and then **Task bar notification area settings**. Here you can add the context menu item **Initial local whitelist learning**. Note: Keep in mind that application blocking is disabled in this case until the user has initiated learning.

259

14.5.8 Settings for application behavior control

You can configure the following settings related to application behavior control:

Setting	Configuration options
Duration of the learning phase for application behavior control	This setting lets you specify a period of time during which an application learns and records everything it will do on the DriveLock Agent. The corresponding rules are generated based on the learned behavior. The default option is **Not configured**. Choose **Set to value** to specify a time period. Once the application is started the first time, a countdown begins. After the time is over, everything that does not comply with the learned behavior is blocked.
Ask user in case of unusual application behavior	When application behavior control is enabled for a DriveLock Agent and the learning process has been completed, any application behavior that differs from what was learned is considered 'unusual'. The default option is **Disabled**. Select **Enabled** if a user must confirm or reject the unusual behavior. Behavior confirmed is subsequently learnt.

14.6 Application rules

The following application rules are available:

- File properties rule
  Allows you to filter by a number of different file properties:
  Path, hash, owner, product information and certificate.

> ✏ Note: Note that different filter properties also have different advantages and disadvantages in terms of security, evaluation speed and maintainability.

- Application hash database

  Allows you to combine a large number of hashes into a single rule.

- Application collection rule

  Use this rule if you want to use existing application collections (as a collection of paths), but especially to enable learning settings for Application Behavior Control.

- Special rule

  Allows you to unblock predefined program groups.

- Predictive whitelisting rule

  If you do not want to use the global Local Whitelist and Predictive Whitelisting setting, you can assign this rule to specific computers.

- (Deprecated) Application template:

  This rule is only present for backward compatibility for older DriveLock versions

You can use **folders** in the **Application rules** node to group rules thematically, e.g. by manufacturer or type of software, and manage them better. In order to control processes such as browser updates, for example, it is practical and convenient to store all the application rules required to do so in a folder named after the browser. You can also assign appropriate access rights.

14.6.1 Pros and cons of different filter properties

In deciding what criteria to use for blocking or allowing applications, you have to consider a number of different aspects. Some criteria ensure a high level of security, but require more administrative effort, while others can be evaluated very quickly, but offer less security. The table summarizes these aspects.

Filter property	Advantages	Disadvantages	Notes
Hash	unique for each file allows you to precisely control which applications are allowed and which are not	high maintenance effort when new files are added (e.g. by updates)	very high security

Filter property	Advantages	Disadvantages	Notes
File path and owner	very fast, because the file content does not have to be checked (high performance)	only secure if the user is not allowed to write to the path	lower security (except, for example, when using a soft-ware deploy-ment tool).
Product information and cer-tificate/signature (the same applies to file path and owner)	small number of rules can cover many files and continues to work after updates	possibly more is allowed than intended (for example, pro-grams signed with the same certificate) Please note that the product information is not secure without sig-nature	medium secur-ity

We recommend combining the criteria to cover as many aspects as possible.

To achieve a high level of efficiency when evaluating rules, the **Finish rule evaluation once the result has been determined** setting is enabled by default. This setting ensures that rules for file path and file owner are executed first. Once a rule has been found that allows an application, the other rules are not evaluated at all, because they will no longer influence the final decision on whether the application is allowed or not (that is, the result).

Example: You create two rules. In rule 1 (file properties rule) all files under the **path** C:\Win-dows are allowed. In rule 2 (application hash database rule) you include all Windows files. If a user starts C:\Windows\notepad.exe, then rule 1 takes effect and the hash database rule is

not even checked. If the setting is disabled, rule 2 will be checked too (including the hashes), in which case this process will take much longer.

If you are only using simple whitelist rules, this works well, because there is no need to check the time-consuming rules when a quick rule takes effect. In contrast, if you are using additional blacklist rules or local learning rules, they still need to be checked after a simple whitelist rule has already taken effect. In this case, all these rules must be evaluated quickly in order to benefit from the faster rule evaluation.

How to set priorities for application rules

You can set a priority for application rules on the Options tab. As soon as a suitable rule has been found, rules with a lower priority are no longer executed. In this way, you can also create whitelist rules in whitelist mode, which have a higher priority than blacklist rules.

Example: A blacklist rule blocks exe files in the Downloads folder. A whitelist rule allows programs that are signed by Microsoft. With the same priority setting, the blacklist rule would take precedence. If you now give the whitelist rule a higher priority, the Microsoft programs can still be executed.

14.6.2 Rule types

When configuring application rules, you can specify different rule types:
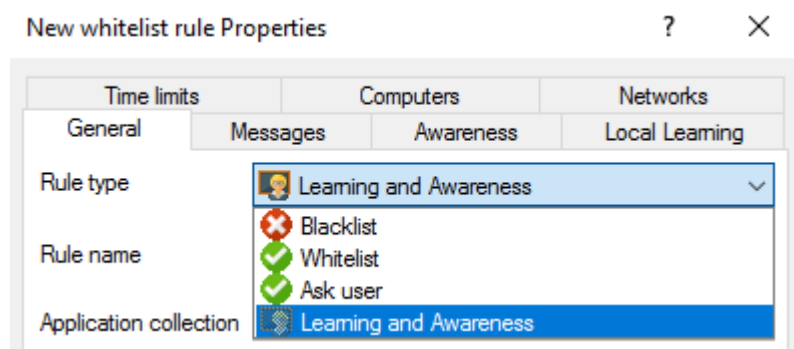
- **White or blacklist rules** (also known as **allow** or **block rules**): With these rule types, you define which applications are allowed and may be executed on the DriveLock Agent or which applications are prohibited and blocked.

- **Ask user**: With this rule type, an application is allowed (whitelist), but the user must confirm its start.

- **Learning and Awareness**: This rule type ensures that only the learning settings on the **Local Learning** tab take effect or that the awareness campaigns specified on the **Awareness** tab are displayed. This means that you can configure settings for an application without actively allowing (whitelist) or blocking (blacklist) it.

- The **Local Learning** tab appears in the following rules: File properties rule and Application collection rule.

- Here you can find out how to use the settings on the **Local Learning** tab.

- You can find a sample configuration for displaying an awareness campaign here.

14.6.3 File properties rule

This rule allows you to specify different file properties to filter by.

The following options are available:

1. **Path**: Select a path from which applications may be started (or should be blocked) or a specific file within a specified directory. To do so, click **...** . This option checks if the path of the file meets certain conditions.

   > 📝 Note: The other boxes in the dialog will be filled in automatically as soon as you have made a selection here. Then, check the options you want to filter by.

   You can also select an application from the list of currently started programs (option **From running processes...**) or from the application database (option **From application inventory...**).
   To view information about currently running applications from another computer where DriveLock is installed and running via the remote connection, select the **on Agent** option, enter the name of the computer, and then click **Connect**.
   Also select one of the two options in the drop-down list:
   - **equals**: is true if the path corresponds to the specified text, where wildcards can be used. If the text does not contain backslashes, only the file name is checked.

   - **contains**: applies if the specified text occurs anywhere in the file path.

2. Then assign a **rule name** and select the **rule type**, that is, the way the rule will be implemented. For more information, please visit here.

3. **Hash**: This option verifies that the hash value of the file contents matches the specified value. The system stores this value when creating the rule and compares it with the currently calculated value at runtime. If both match, the rule is activated. Use this option, for example, for a single application that you want to allow or block via whitelist or blacklist.

4. **Owner**: Use this option to restrict the starting of an application to a specific file owner. For example, you can use this setting to allow all programs installed by an administrator or by a trusted installer account, while blocking all applications that were

installed by other users. This also allows for automatically blocking all applications that can be run without prior installation.

The following **owner types** can be selected or are automatically entered depending on the selection:

- **Administrators group**: This option covers all local administrators. To allow the file, the administrators group must be the explicit file owner.

- **Trusted Installer** and **Local System**: These default Windows accounts must be file owners so that the file is allowed.

- **AD user or group**: Select an AD user or group as file owner here. This is where the SID is checked.

- **Name (user / group)**: You can manually add a user or group here. Here the name is checked.

> ✏️ Note: If you assign a group, the file owner must be the group, not a member of that group.

5. **Description**: Enter the file description here, e.g. 'Paint' for the mspaint.exe file.

6. **Version**: You can have the version checked to prevent users from running other or older program versions, e.g. you can allow Firefox version 83.0.0.7621 or higher and block all previous versions that might contain security vulnerabilities. Select the appropriate option from the drop-down menu, e.g. greater than or equal to.

7. **Product**: Enter the product name here, e.g. Microsoft Windows operating system.

8. **Certificate validation**: This option allows you to whitelist signed software or blacklist unsigned software.
   You can also use the browse button to select certificates via the application inventory.

> ✏️ Note: Note that Windows files are not signed. You must also enter a file path here, for example.

9. **Subject**, **Issuer**, **Thumbprint** and **Serial number** are additional certificate properties. The serial number is only unique in combination with the publisher.

> ⚠️ Warning: In addition to some additional options, this rule combines the file owner, file path, hash, and publisher certificate rule options from previous versions. Please note that file property rules are only compatible with DriveLock Agents prior to

> ⓘ version 2020.2 if only those combinations of properties are checked that correspond exactly to the setting options of the respective old rule types. For example, if you combine the path with the owner and the publisher, the (old) agent cannot interpret the rule type accurately and will therefore ignore the rule.

In the DriveLock Management Console, the dialogs look like this using the 'Firefox' example:

14.6.4 Application hash database

To facilitate application control configuration, DriveLock provides the option to create application hash databases and use them in whitelist or blacklist mode. Hash databases can be created by automatically searching for applications in a directory or directories (and their child directories), calculating their hash values and saving them to a file. A hash database of all installed programs can also be created from the hard disk of a reference system.

Follow these steps to create an application hash database:

1. In the **Applications** node, select **Application rules**. Next, select **New** from the context menu and open the **Application hash database** dialog.

2. Initially no database is selected on the **General** tab. You can either create a new database file or select an existing one.

> ✒ Note: DriveLock provides a utility program **DriveLock Application Hash Database Tool** that can also be used to generate a hash database. The utility is located in the installation directory of DriveLock (C:\Program Files\CenterTools\DriveLock MMC\Tools\DLExeHasher.exe).

3. The value that is already preset in the hash procedure is listed in the **Hash algorithm used in database** section.

4. To create a new database, click **Database file** and then click **Create new**.

5. In the Comment (System name) box, type the name of the computer to be scanned. With this information, it is easier to assign multiple database files during a migration at a later date. Type or click **...** to select the directory to be scanned for applications.

> ✒ Note: You can scan a directory on a remote computer by specifying the UNC path for this directory.

The **Hash algorithm for executable hashes** defines the algorithm used for this database. Initially the general hash algorithm is set here. Select **Scan executables and dynamic link libraries** to scan DLL files in addition to EXE files.

6. Click **OK**. DriveLock starts a recursive scan of the specified directory and all child directories below it.

> 📝 Note: Please note that scanning larger directories or UNC paths may take some time. Please do not interrupt the process.

> 📝 Note: No duplicate entries are generated during the search. If it finds the same file in a different directory, DriveLock does not add the hash value to the hash database again. This has no effect on how the rule is applied because applications are evaluated based on their hashes and not a specific location. Also, this behavior allows for differential scanning, which only adds applications that are not already in the database.

7. When DriveLock has finished detecting all program files and has calculated all hashes, it adds all applications it detected to the template and displays the previous dialog box.

8. Add a description (**Rule name**) and enter additional information in the **Comment** text box if necessary.

9. Click **Database content** to view, edit or merge the programs that are included in the database.

10. Click **Database content** and then click **View / edit** to view the database content.
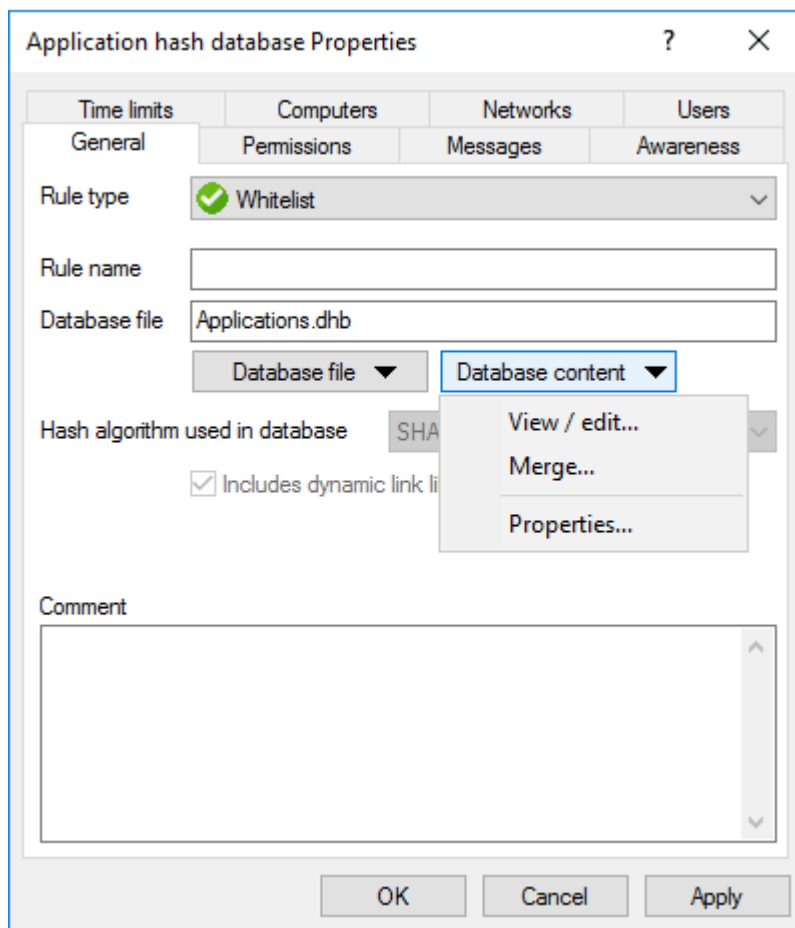
11. The left pane displays the folders that were scanned. Select a folder to display all programs that were found in this folder in the right pane.
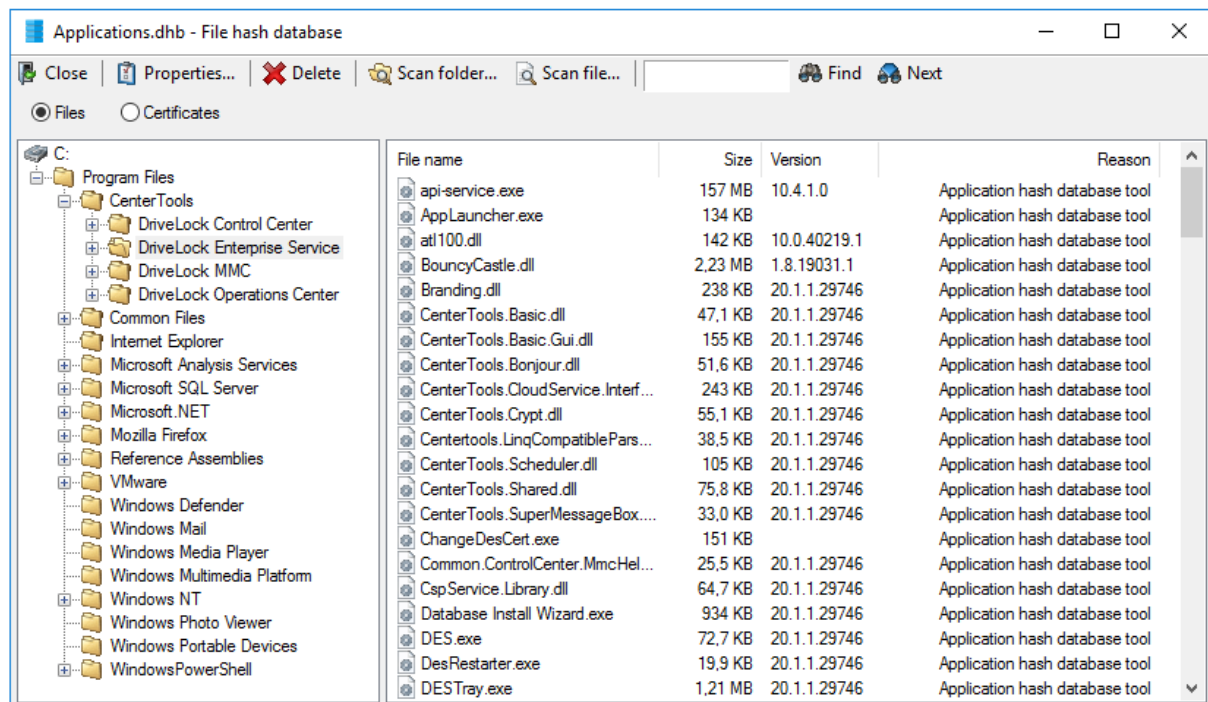
12. To add additional hashes, click **Scan folder** or **Scan file**. Click **Delete** to remove the selected application hash or folder. To view additional information about the hash database, click **Properties**.

13. To close the hash database viewer, click **Close**.

> ☑ Note: You can also use the standalone Application Hash Database Tool, DLExeHasher.exe, to view, edit and merge hash databases.

14. Click **Database content** and then click **Merge** to add the content of another database.

15. Type or select the path of the database file containing the entries to be added. Alternatively you can use the file selection dialog.

16. Click **OK** so that DriveLock merges the database content.

17. Then it displays the template properties again.

18. Click **OK** to exit the dialog and save the changes.

> ☑ Note: Even if you are using a whitelist rule based on a hash database of all installed applications to control a computer, it is recommended that you also use some special application rules for programs that are part of the operating system. For technical reasons, they are loaded faster than the information from the hash database and are therefore made available to the DriveLock Agent much sooner when Application Control is started.

14.6.5 Application collection rule

> ☑ Note: This rule has no user restrictions.

In the task pad view of the DriveLock Management Console (DMC), you can find two examples that are included and can be used immediately. With one rule you can learn and control the behavior of different browsers and with the other one that of different e-mail clients (the corresponding application collections are created simultaneously in the **Application collections** folder).

Based on the behavior of browsers during updates, the following example explains the dialog options:

1. The **General** tab contains the following information:
   - **Rule type**: Learning and Awareness
     The **Learning and Awareness** option only controls the learning settings, but does not determine whether a specific program may be started or not (as would be the case with the white or black list options).

     > Note: This decision is based on the hashes of the files (in hash rules), which are automatically managed by Application Control.

   - **Rule name**: Learn the behavior of browsers

   - **Application collection**: Browsers
     Make sure that the application collection contains all common browsers and exists already.

2. The following options are available on the **Local Learning** tab:
   - **The application may start programs that are not included in any whitelist**
     By selecting this option, any service process that is to execute a browser update can be started, even if this service process is not explicitly whitelisted. This option also allows the service process to start the actual browser update, which is not whitelisted either.

   - **Learn all program files written by this application (including child processes)**
     To enable the browser update to terminate the actual browser and service process and to replace the corresponding files with the updated version of the browser, all child processes of the service process must be automatically added to a whitelist.
     This means that the actual browser, being a child process of the service process, will be able to start programs that are not explicitly allowed. In addition, all the files that the browser writes are also automatically added to the whitelist.

   As neither of these options are wanted for browsers, it is important to configure the browser so that such permissions are not passed on to the process. This is why you select the following option:
   - **This application never gets the permissions listed above**

   In the section **Learn and control application behavior** you also specify that browsers learn locally

- which programs they start,

- which DLLs they load and

- which directories they are allowed to write their files to.
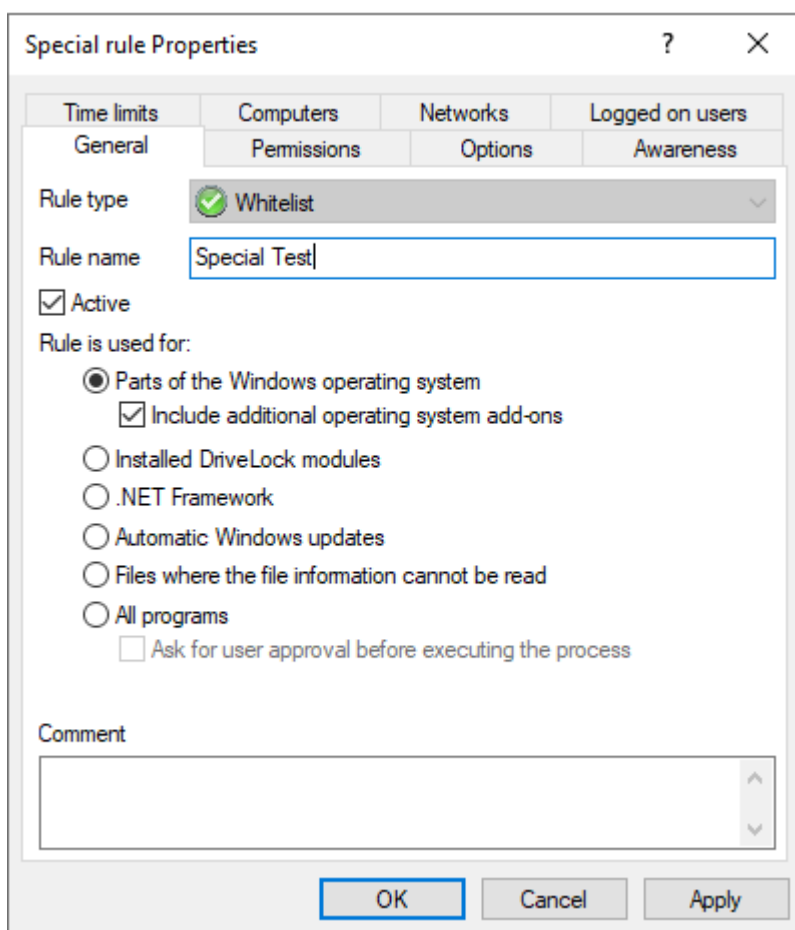
Conclusion: With these settings, the applications that are specified in the rule get exactly the rights they need on the respective DriveLock Agent where the application behavior is recorded. In this way it is even possible to learn different download directories for applications on different agents.

14.6.6 Special rule

You can use the special rules to easily identify all program files on a computer that meet a certain criterion, for example, to determine whether a file is part of the Microsoft operating system, or belongs to the installed DriveLock, or is a .NET program. You can also use the special rule to override a blacklist rule, for example, so that some users, such as the service administrators, can run all programs.

> Note: Special rules can only be used as whitelist rules.

You can select from the following options in the dialog:

Rule is used for:

1. Parts of the Windows operating system
   - includes all programs protected by the Windows System File Protection (WFP)

   Include additional operation system add-ons addresses programs in
   - C:\windows
   - C:\windows\system32

- C:\windows\servicing

- C:\windows\pchealth\helpctr\binaries (Help Center)

- C:\windows\application compatibility scripts

- C:\windows\explorer.exe

- C:\Programs\Internet Explorer

- C:\Programs\Windows Defender

2. Installed DriveLock modules
    - Programs in the DriveLock installation directories, for example the DOC Companion Offline Installer. This only includes DriveLock files that have already been installed with administrative rights. This means that users are not allowed to execute any DriveLock files.

3. .NET Framework
    - all programs in C:\Windows\Microsoft.NET

4. Automatic Windows updates
    - all processes initialized by the Windows Update Agent

5. Files whose information cannot be read
    - can be used as a fallback if for any reason DriveLock is not able to access or read information details from a specific file

6. All programs
    - can be used in conjunction with rule limitations for example, to allow access to all programs for the Administrators group, optionally including a user approval before executing the process.

    > Note: This user permission does not affect the priority of the rule.

14.6.6.1 Basic application rules

To create basic application rules, click **Change** in the Taskpad view.

Select the type of rules to use and then click Finish. DriveLock creates the corresponding special rules.
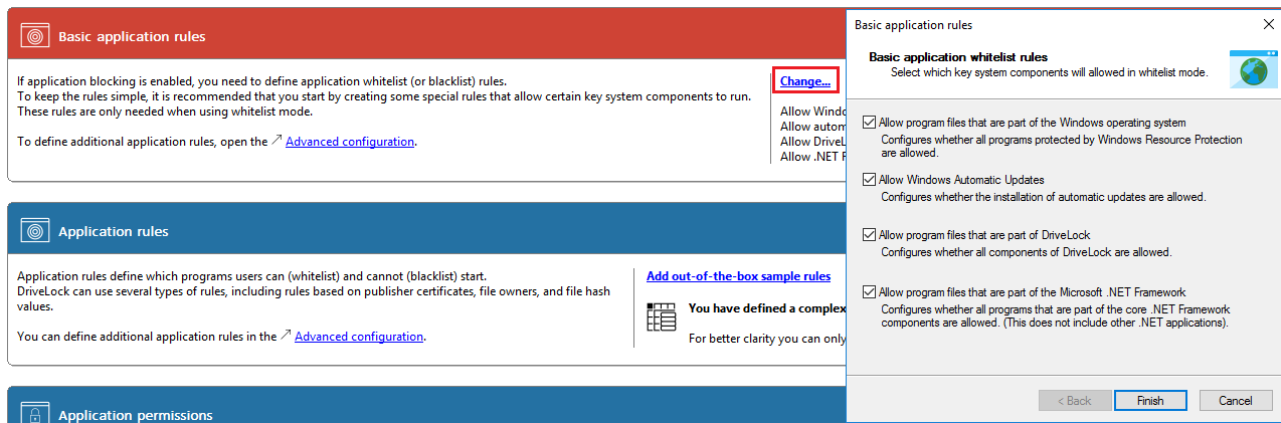
14.6.7 Local whitelist rule

The local whitelist rule is only to be used as type 'Whitelist'.

If you select **Enable predictive whitelisting**, :
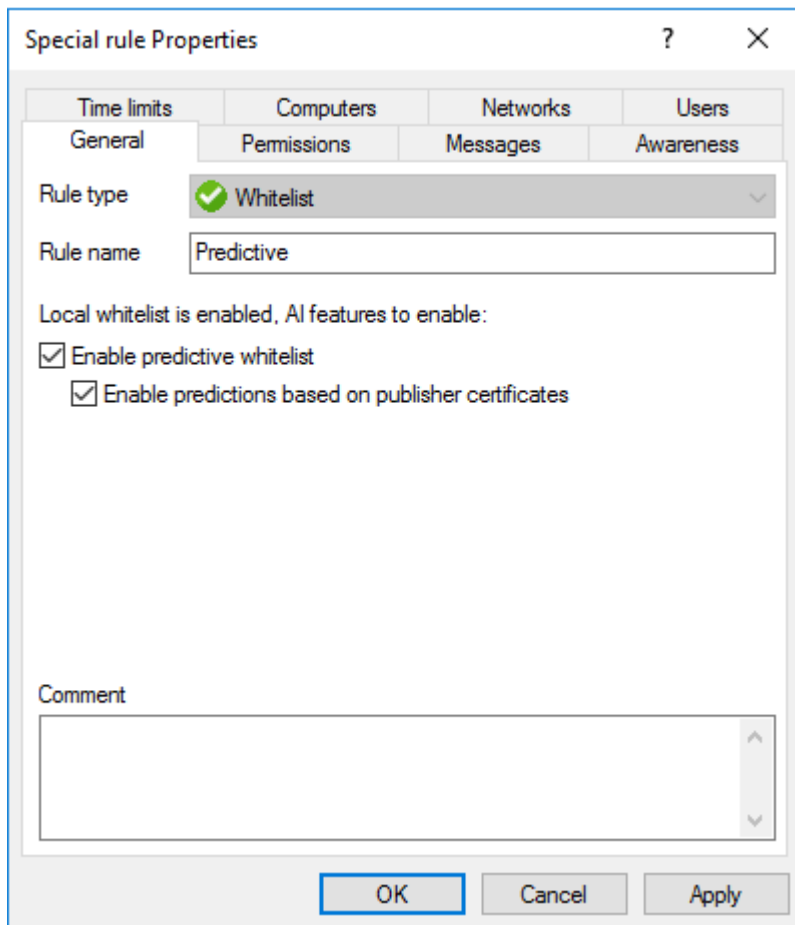
By selecting the **Enable predictions based on publisher certificates** option, DriveLock uses algorithms to detect new versions of signed software even if the certificates are not completely identical.

See also the Local Whitelist and predictive whitelisting setting.

Note: Note that this setting only works if the new version can be recognized prop-erly.

14.6.8 Application template (deprecated)

Application templates can contain one or more applications that are either blocked (black-list) or allowed (whitelist).

> ⚠ Warning: Please note that this application rule is obsolete and should not be used anymore. We recommend using application hash database rules instead.

14.7 Application rules in the DOC

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

Application rules can be created in the following places in the DOC:

1. In the **Security Controls** menu in the **Applications** view. In this view, you can see a summary of all the important information about the applications that are deployed on your agents. Application rules can be created here on all tabs.
   - Installed Software or Binaries: Lists processes that can be used in application rules.
   - **Rules**: All already created application rules are listed here. You will have to enter all the data manually if you choose this option.
   - **Events**: Events that provide data about applications can be used as a source for an application rule. 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 **Events** view:
   You can view the events for application control by selecting the **Application Control** option in the vertical split of the window.

3. In the **Inventory** menu in the **Software** view

4. In the **Administration** menu **in** the Rules view

> ✐ Note: For more information, see File properties rule.

14.7.1 Creating application rules

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.

> ✐ Note: Further information on application rules can be found here.

14.7.1.1 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.

14.7.1.2 Using file information from binaries

The **MSI**, **Folder** or **Executable file** options can be used to create several application rules at the same time.

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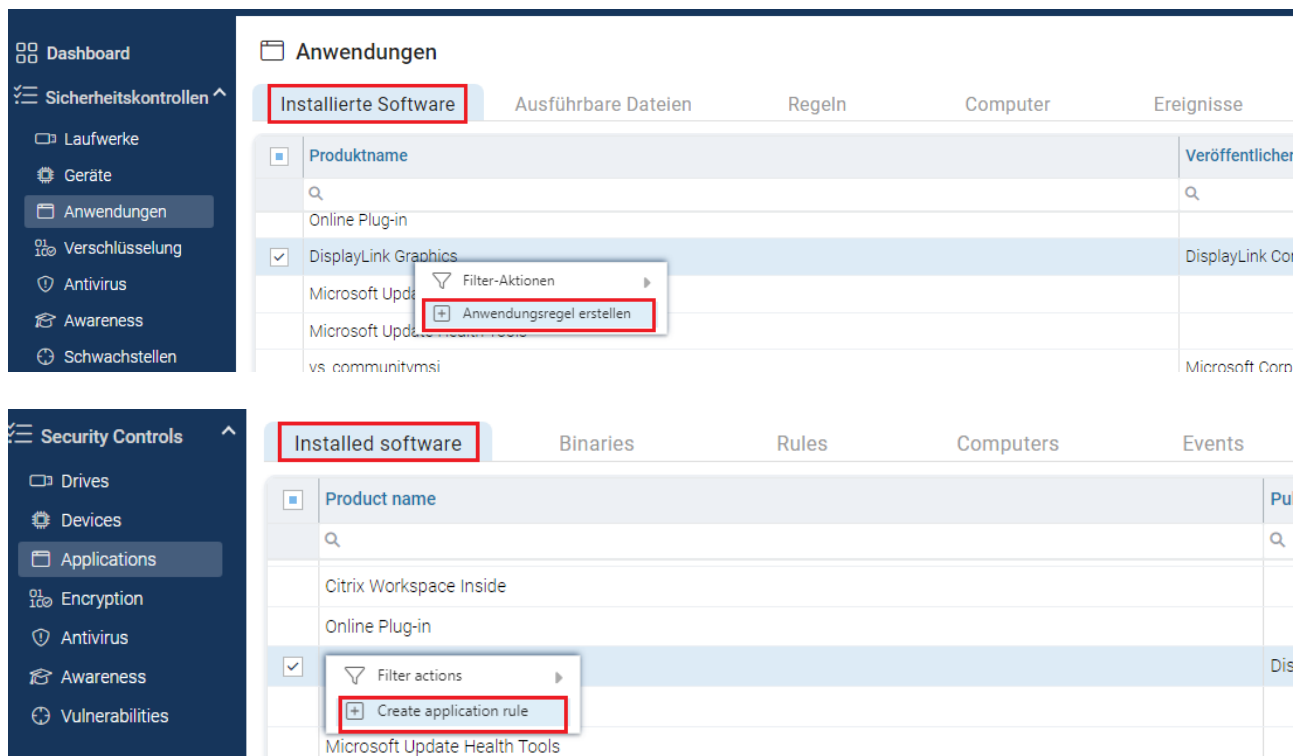
The rules are grouped and saved using the specified name and are then displayed in the Application rules section. Here you can edit, activate, deactivate or delete the individual rules.

> ☑ Note: Further information on application rules can be found here.

14.7.1.3 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.

14.8 Application behavior rules

Use application behavior control to accomplish the following results:

- Prevent an application (or process, script) from being started from within an allowed application, thus causing a potential danger to your system.

- Specify which type of access you want to grant a particular application (e.g. read or write access to files or the registry).

For this purpose, the following options are available. You can...

- determine in which order (priority) application behavior rules are processed,

- specify the action to be taken when a particular application is accessed (for example, the application is blocked or not),

- determine whether an application permission can be passed on to child processes,

- specify different file and folder filters or

- specify script types that are allowed for running scripts.

Also, starting with version 2020.1, you can create a behavior rule based on a stored recording of application behavior on the DriveLock Agent.

All application behavior rules can be arranged in the DriveLock Management Console in a user-defined folder structure.

14.8.1 Defining application behavior rules

You can create application behavior rules as follows:

1. In the Taskpad view, select **Add behavior rule...** or click **New** in the context menu of the **Application behavior rules** subnode, creating a new behavior rule. In this context menu you can also create **folders** to group related application behavior rules.

2. In either case, the properties dialog box as shown below will appear, allowing you to enter your details.

3. Enter a description on the **General** tab and add a comment if necessary.
   In the figure below you can see one of the supplied sample permissions.

4. The **Enable rule** option is set by default.

5. The **Priority** option provides you with several choices.
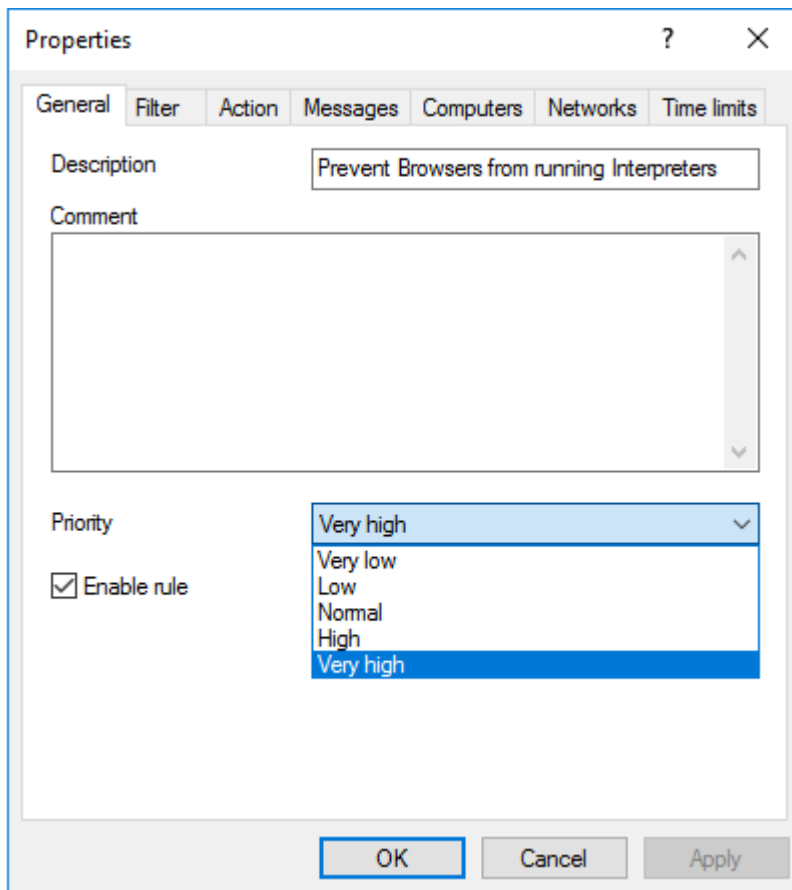
> **Note:** Generally valid application behavior rules get a lower priority, special ones a higher one. The priorities vary according to the use cases. High-priority rules are processed before low-priority rules. The system checks the rules in the specified order, and if a rule matches, it is applied.

You can reduce or increase the **priority** in the DriveLock MMC.

Example: Combine rules, e.g. create a rule that allows the Browser to start Windows Media Player with high priority and another rule that forbids the Browser to start any other programs with a lower priority.

6. Continue your input on the Filters, Action, Messages and general settings for rules and permissions (Computers, Networks, Times) tabs.

Please find practical examples in the use cases.

14.8.1.1 Information on the Filter tab

The following settings are available here:

1. **Accessing application**
   Here you can either specify the full path or the name of the application you want to control, e.g. C:\Program Files\Mozilla Firefox\firefox.exe or just firefox.exe. Wildcards are allowed.
   Note that you can select application collections here, provided you've created them already. Please refer to the corresponding chapter for more information.

2. **Pass on to child processes**
   Select this setting so that your application permission is valid not only for the processes that meet the **Accessing application** requirement, but also for all children. This setting affects not only the immediate child processes, but all of their children as well.

   > Note: This is particularly useful if you select **Block** as an action on the **Filter** tab because it prevents your application behavior rules from being bypassed by starting another process.

   Example: You create an application permission that prohibits your browser from starting Powershell. By selecting this option you can prevent Powershell from being started from the command line anyway (which is a child process).

3. **Access mode**
   The access mode is a filter parameter for the application permission. Here you can define the action the accessing application should take.

4. Additional specifications (target)
   Depending on the access mode you choose, you enter different targets in the next text box (a path can be specified in all cases).

   > Note: Starting with version 2020.1 you can enter several specifications here. This reduces the number of rules.

Access mode	Target	Explanation
Execute	Started application	Enter the name of the application that is not supposed to be started (in this case, you would choose Block as an action). Optionally, you can specify a **command**

Access mode	Target	Explanation
		line parameter here that will restrict the execution of the called application to a greater extent. Use case 1 Note that you cannot enter parameters in Windows XP!
Load DLL	DLL name	Enter the DLL that may only be loaded from a specific directory, for example. Use case 2
Run script	Script name	Enter the script you want to restrict from running. Use case 3 Please note that DriveLock only considers the script types defined in the Script definition subnode.
Read / write file	File name	Enter a file name or a directory the accessing application is allowed (or not allowed) to read or write to. Use case 4 for read access Use case 5 for write access
Read / write	Registry key	Enter the respective registry key (e.g.

Access mode	Target	Explanation
registry		`HKEY_LOCAL_MACHINE\SOFTWARE\Mi-crosoft\)`, that may or may not be accessed (read or write access). Wildcards are allowed. Use case 6 Please note that this access mode is only available for Windows 7 and higher!

14.8.1.2 Information on the Action tab

On this tab you determine how application control will respond to the entries on the **Filter** tab.

Please do the following:

1. Select the appropriate action:
    - **Allow**: Select this option if you do not require any further action. This setting corresponds to 'Allow'.

    - **Block**: Choose Block if you want to prevent specific events depending on the access mode or the target. For example, this action prevents an application or script from running, or a DLL from loading. This is the default setting.

    - **Ask user**: To let users decide which action they want to allow, select this option. Then, for example, it is up to the user to decide whether a Powershell script is run or not.

        > Note: Rule evaluation is stopped for these options (Allow, Block and Ask user).

    - **Modify reporting**: No further action is taken with this option, it only changes the reporting. Further below you can indicate whether the command line will be displayed in the event. Note that with this option the evaluation of the rules continues.

> 🖉 Note: Please note that these actions provide additional protection for particularly vulnerable processes. 'Allow' can still be blocked by a setting in a white or black list, but 'Block' overwrites the setting in a whitelist rule!

2. Specify one of the following mechanisms that applies to targets other than the ones defined on the **Filter** tab:

   - **Block access to other targets**
     Allow access only to the targets that are explicitly allowed, and block all other targets.

   - **Block access by other applications**
     Only applications with explicit permission are allowed access, all other applications are blocked.
     Example: No other application may access the bank directory other than the bank application from use case no. 4.

3. Determine which events will be generated:
   The **Generate audit events when access is denied** is the default option. You can additionally or alternatively select the **Generate audit events when access is allowed** option. Use this option, for example, if you want to allow execution of specific scripts in a rule and want to generate the associated events. All events are displayed in the DriveLock Operations Center (DOC). Both options are also suitable for the simulation mode.

> 🖉 Note: Please note that a large number of events will be created if you select both options.

4. The option **Show command line in event** specifies that the corresponding event reporting a (allowed or blocked) process start may also display command line parameters in the **Events and Alerts** node, **Application Control** sub-node. The option is disabled by default.

> 🖉 Note: Please note that the command line may contain confidential data, such as passwords.

14.8.1.3 Information on the Messages tab

The standard message texts for Application Control that are displayed on the DriveLock Agent are configured in the **Global configuration** node, sub-node **Multilingual notification texts**, option **Languages / Standard messages** on the **Applications** tab.

1. There is only one option on this tab available for **application behavior rules**, and it is enabled by default:

   - **Display message when access is denied**: Select a default text from the drop-down list or define your own text to be shown to the user when access is blocked.

   - Depending on the access mode, the following wildcards are allowed:
     - Access mode Execute:
       %EXE% for the name of the application; %PARENT% for the name of the program that starts the application.

     - All other access modes:
       %EXE% for the name of the application; %TARGET% for the access target.

2. There are three options for **application rules**:

   - **Display custom message in user notification**: Again, you can select a standard text or define your own text.

   - Check **Display no message when this rule is activated** if the user does not need to know when an application is blocked (by a blacklist).

   - By default, events are generated when applications are blocked. If these events are not required, check **Do not generate audit events when this rule is activated** .

14.8.1.4 General settings for rules

The following tabs appear in various application and behavior rules.

1. **Logged on users** tab:
   By default, the rule is active for all logged on users and groups.

2. **Computers** tab:
   - Select the computers the rule applies to.

   - For example, you can create a behavior rule only for a special group of computers that contains computers with a newer version of the DriveLock Agent.

3. **Messages** tab:
   For more information about the options on this tab for application rules or application behavior rules, click here.

4. **Networks** tab:
   Determine the network connections the rule applies to.

5. **Time limits** tab:

- If you want the rule to apply only for a specific period of time, you can specify an individual time frame here (e.g. only on weekdays from 09:00 to 17:00)

- It is also possible to specify a date for the start and end of the validity period.

- 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.

6. **Permissions** tab:

- Determine the users or groups the rule is active for.

- Check **Selected users and groups** to activate the rule for a specific group of users only. To include another group or user in the list, click Add. Click Remove to delete the previously selected entry.

14.8.2 Generate application behavior rules from behavior recording

Whenever applications require access that is not apparent to the user (writing temporary files, creating configuration files or caches, etc.), DriveLock records these background actions and allows you to control them.

To have application behavior rules generated automatically from the result of the behavior recording, proceed as follows:

1. In the context menu of the **application behavior rules** under All Tasks, click the menu item **Generate behavior rules from the application behavior recording...** .
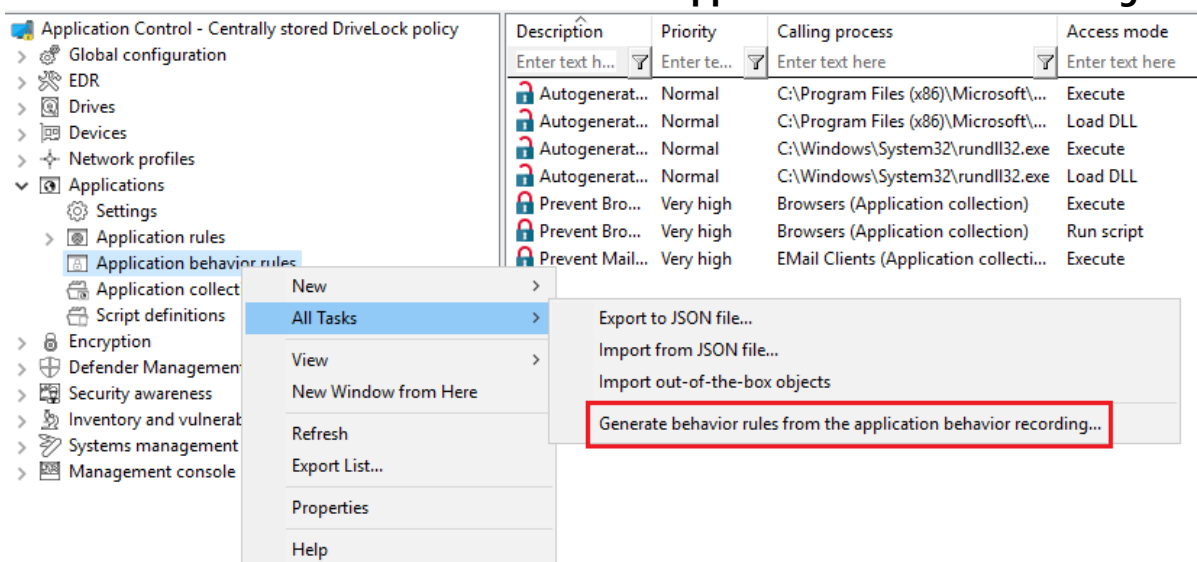
2. Select the data source for the recording results in the following dialog. This information can be obtained from the DriveLock Agent on the local or remote computer or

from a pre-existing results file.
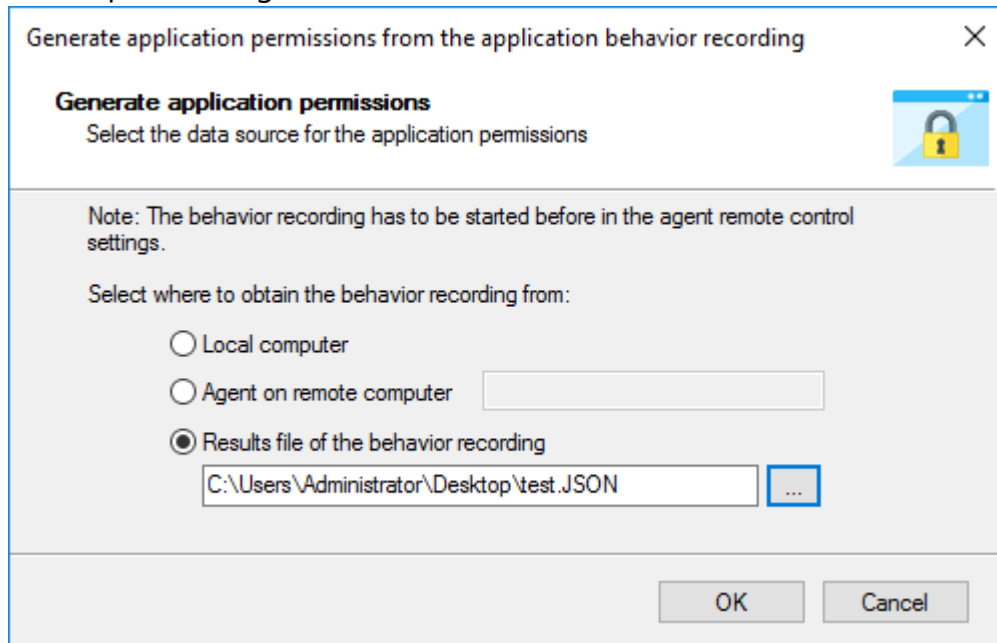
3. In the next dialog you configure the following:
   - Select an application (or multiple applications) and specify whether to use the entire path or only the file regardless of where it is stored. For example, for browsers we recommend that you use the name without the path.

   - Specify the access modes you want to create rules for and whether or not to combine multiple files using wildcards. **Never** is recommended for the **Execute** access mode, because it involves only a limited number of files (and rules to be created from them) that do not require combining. However, when **writing files**, it **always** makes sense to use wildcards and not to create rules for each individual file written (even if the number is low).
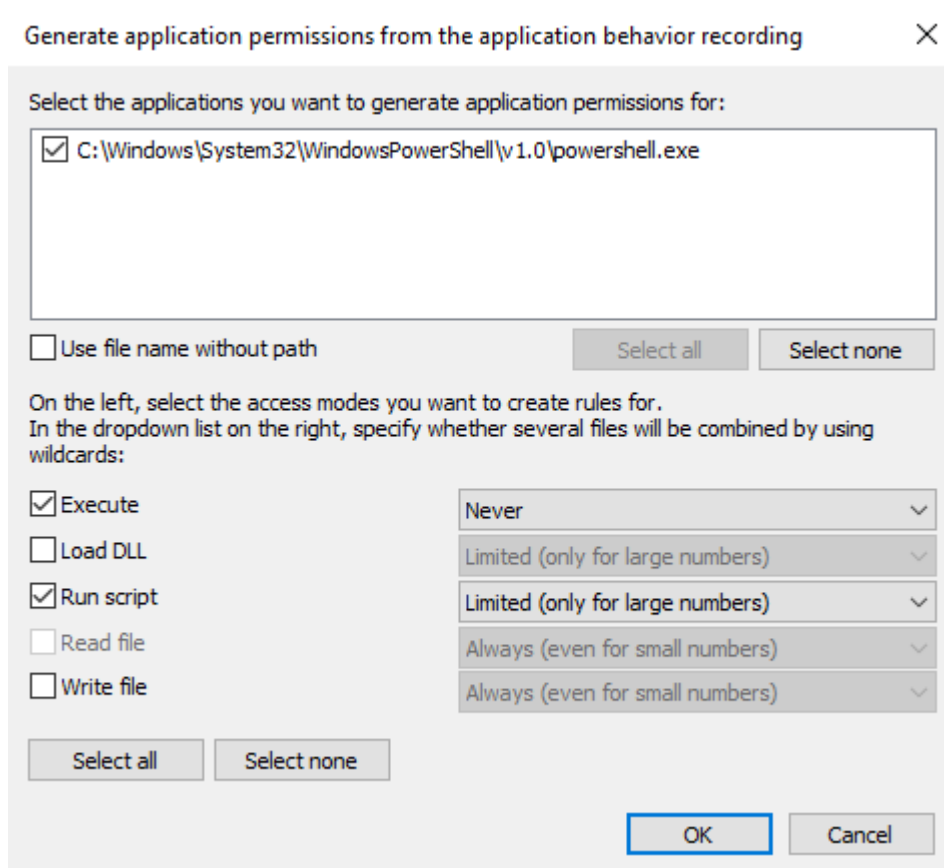
4. In the next step, the rules generated automatically are displayed as **Autogenerated rule** in the node **Application behavior rules**. The **Reaction** tab shows that the executing application is allowed (Allow), all other accesses are blocked.
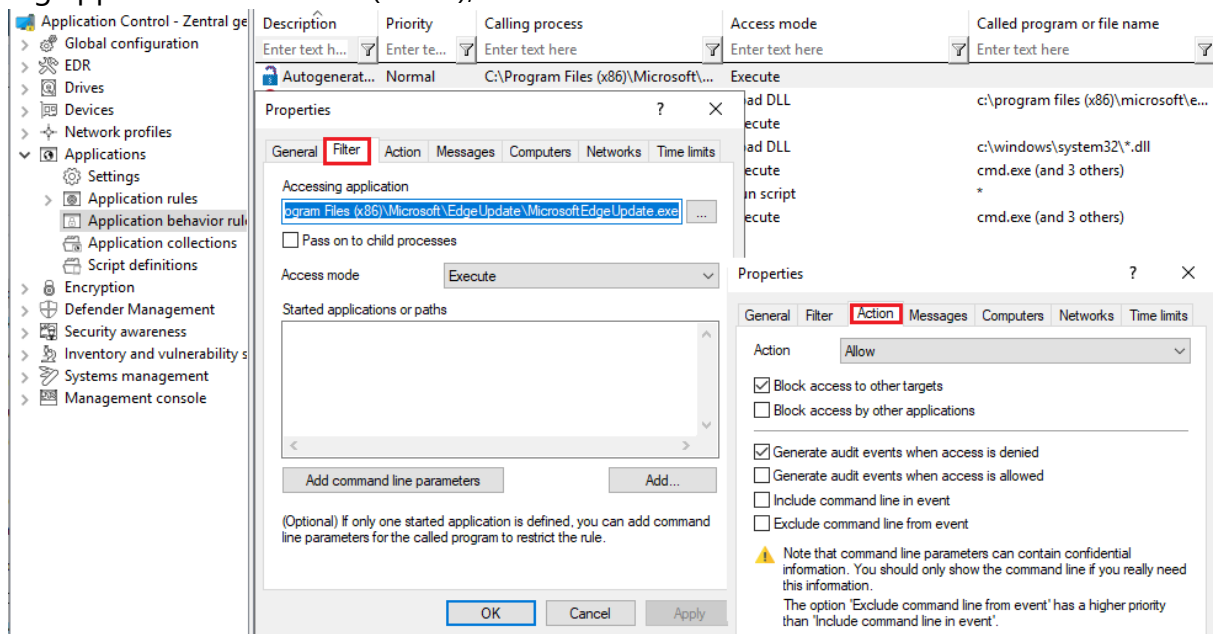
Tip: Create a separate folder for these application behavior rules so that they can be easily distinguished from the existing ones.

Summary: Creating application behavior rules automatically provides a much leaner and clearer set of rules and reduces the time spent on monitoring or analyzing events.

14.9 Application collections

Application collections are a set of applications that belong together in terms of subject matter or program. You can use them in the corresponding application behavior rules or application rules.

Rather than creating individual rules for each application, you can create a rule for multiple applications (on the application collection) at once. This reduces your set of rules and keeps it simple.

Example: Three application behavior rules should apply to three applications each:

- Rule no. 1 defines that no other applications are allowed to start from within a specific application.

- Rule no. 2 defines that applications are not allowed to write to a specific directory.

- Rule no. 3 defines that applications may only write text files to a specific directory.

> Note: By using lists, the number of rules can be reduced.

Create application collections based on the following example or use the provided application collections displayed in the taskpad view.

14.9.1 Application collection for Microsoft Office products

Scenario: You want to group different Microsoft Office products in an application collection to be able to use them in application behavior rules or application collection rules.
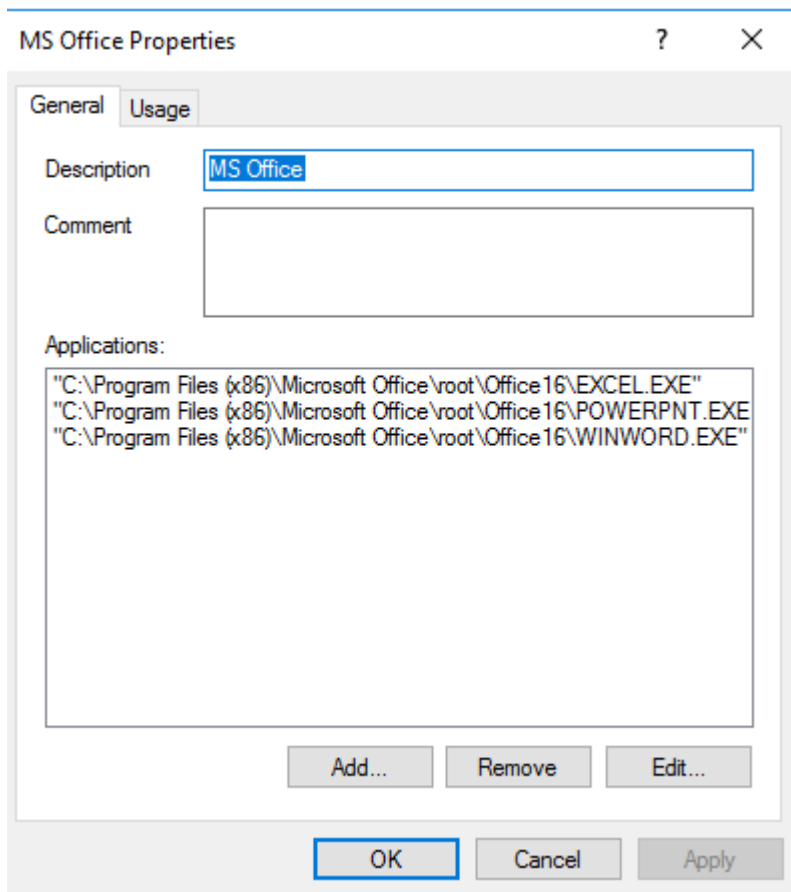
1. Select the **Application collections** sub-node and open the context menu.

2. Choose **New** and then **Application collection**.

3. Enter a unique description, here MS Office.

4. You can optionally enter a **comment**.

5. **Add** the paths to the applications you want to include. You can later remove applications or edit the paths.

6. Save your collection and use it now in application behavior rules.

The behavior and application rules for which this collection is used are displayed on the **Usage** tab.
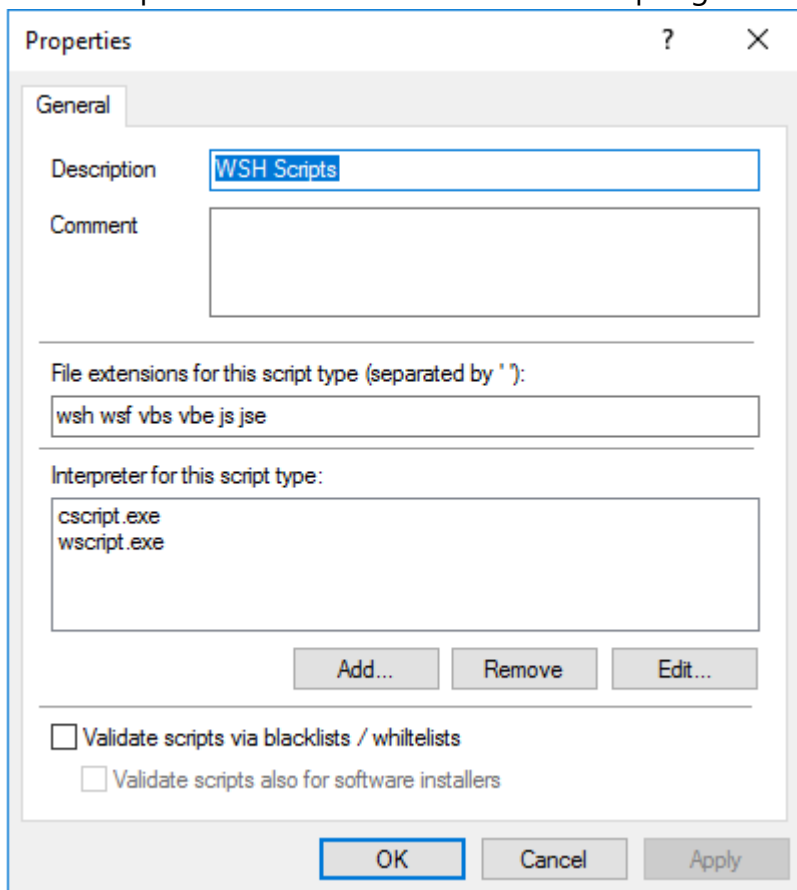
14.10 Script definitions

To be able to use the Run script access mode with the application behavior rules, you must define the appropriate script types.

This definition tells application control which file accesses it should interpret as script execution.

Please do the following:

1. Open the context menu of **Script definitions**.

2. Click **New** and enter your definition in the following dialog.
   The example below defines the Windows Scripting Host.

3. Enter the extensions that apply to the script in the **File extensions for this script type** text box. Simply enter a space between the extensions.

4. Enter the interpreters that can interpret your script in the **Interpreter for this script type** text box.

5. With the **Validate scripts via blacklists / whitelists** option, you can specify to have scripts checked in blacklists or whitelists in the same way as DLLs or EXE files. For more information on blacklisting and whitelisting, see the corresponding chapters.

6. Select the **Validate scripts also for software installers** option if you want the validation to also apply to scripts started by software update processes.
   Example: msiexec.exe is a trusted installer and may only be started if the corresponding MSI file is also trusted.
   The Trusted process setting allows you to create a fixed list for such processes.

14.11 Use cases

14.11.1 Using wildcards in rules

When using wildcards in rules, be aware that wildcards are interpreted differently in different situations in Application Control or Application Behavior Control.

Simple pattern matching (file properties rules)

? ? corresponds to one character

* corresponds to no character or multiple characters

Examples:

"abc?xyz" corresponds to "abc1xyz" but not "abcxyz" or "abc123xyz"

"abc*xyz" corresponds to "abc1xyz" or "abcxyz" or "abc123xyz".

C:\Pro*\test.exe corresponds to C:\ProgramFiles\test.exe or C:\ProgramFiles\tools\test.exe

Pattern matching for paths (application behavior rules and application collections)

? ? corresponds to one character

* corresponds to no character or several characters but no path separators (\\)

****** corresponds to no or multiple 'directories' in a path

Examples:

C:*\temp corresponds to C:\Windows\temp but not C:\temp or C:\Windows\System32\temp

C:**\temp corresponds to C:\Windows\temp or C:\temp or C:\Windows\System32\temp

C:\Pro*\test.exe is equivalent to C:\ProgramFiles\test.exe but not C:\ProgramFiles\tools\test.exe

C:\Pro***\test.exe corresponds to C:\ProgramFiles\test.exe or C:\ProgramFiles\tools\test.exe

14.11.2 Application behavior rules

14.11.2.1 Use Case 1: Prevent PowerShell from starting

Scenario: You want to prevent Powershell from starting when a user launches a browser (here Internet Explorer), which could potentially install malware on the agent computers.

1. Start out with entering a description and a **Comment** if required on the **General** tab. As this is a rather general rule, enter a low **Priority** for it. Check **Enable rule** (default).

2. On the **Filter** tab, specify the following:
   - Enter the full path to the iexplore.exe in the **Accessing application** text box
     Alternatively, you could also use an application collection that contains different browsers.
   - Check **Pass to child processes** to prevent the browser from calling Power-shell.exe from the command line (cmd.exe) (this is a child process).
   - Since you want to prevent PowerShell from starting from Internet Explorer, specify Execute as **Access mode**.
   - Browse for a file or for a folder in the **Started applications or paths** text box, e.g. powershell.exe as file name in this example.

> Note: We recommend specifying only the file name with blocking rules so that all instances can be included. When you specify the full path, please note that several program instances may exist, e.g. powershell.exe may be located in two different directories C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe or in C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.

3. Specify the following on the **Action** tab:
   - The measure you want to use is to **block** the access.

4. For all other options, keep the default settings.

Conclusion: Every time the iexplore.exe is called and tries to start PowerShell, PowerShell will be blocked.

14.11.2.2 Use case 2: Restrict loading a DLL

Scenario: You want to specify that DLLs may only be loaded from certain directories.

In this specific case, you want to prevent Windows Media Player from loading DLLs from network drives.

Proceed as shown in the figure:

1. Create an application permission where you define that the Windows Media Player application wmp.exe may only load DLLs from **\DLL4WMP\ .
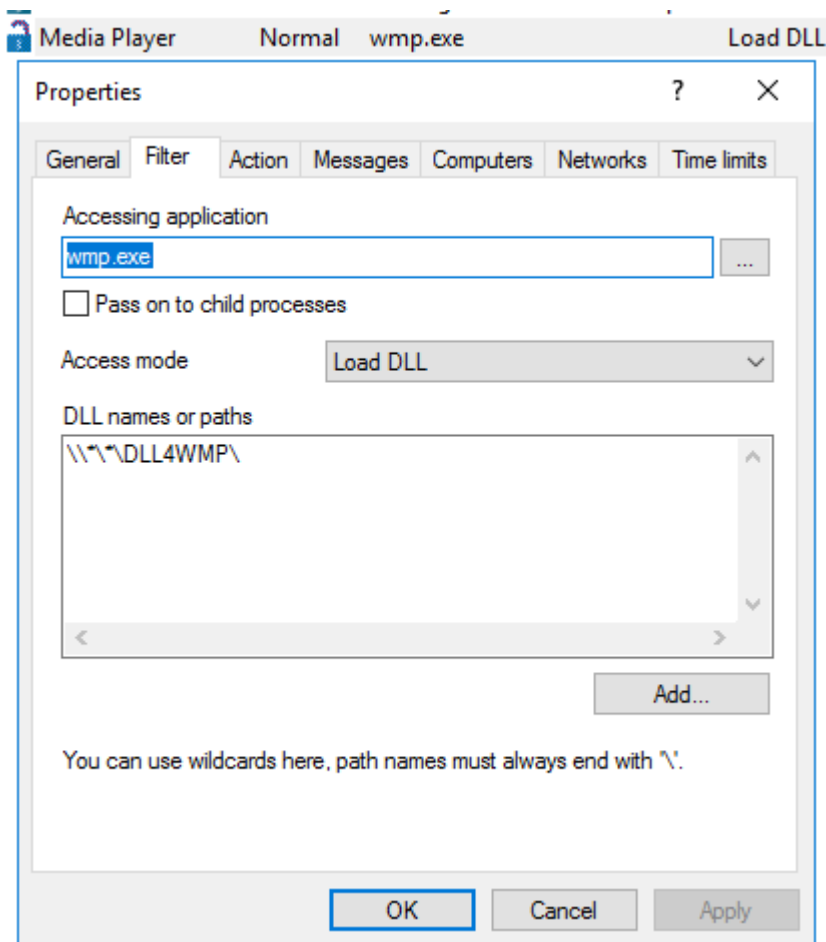
2. Select the following options on the **Action** tab:
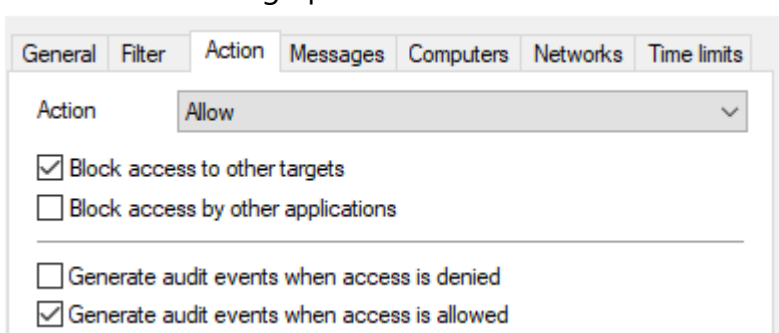
- Select **Allow** as the action and check **Block access to other targets** to ensure that the DLL is only allowed to be loaded from the specified target.

- Select **Generate audit events when access is allowed**.

> Note: Note that rules with 'Allow' have priority over 'Block'!

14.11.2.3 Use case 3: Run scripts

Scenario: You don't want browsers to run VB scripts (*.vbs).

Proceed as shown in the figure:

1. As **Accessing application**, select the application collection you created for your browser.

2. You can check the **Pass to child processes** option in this case. In this way it is possible to prevent the specified VB script from being started from a child process (e.g. from the command line).
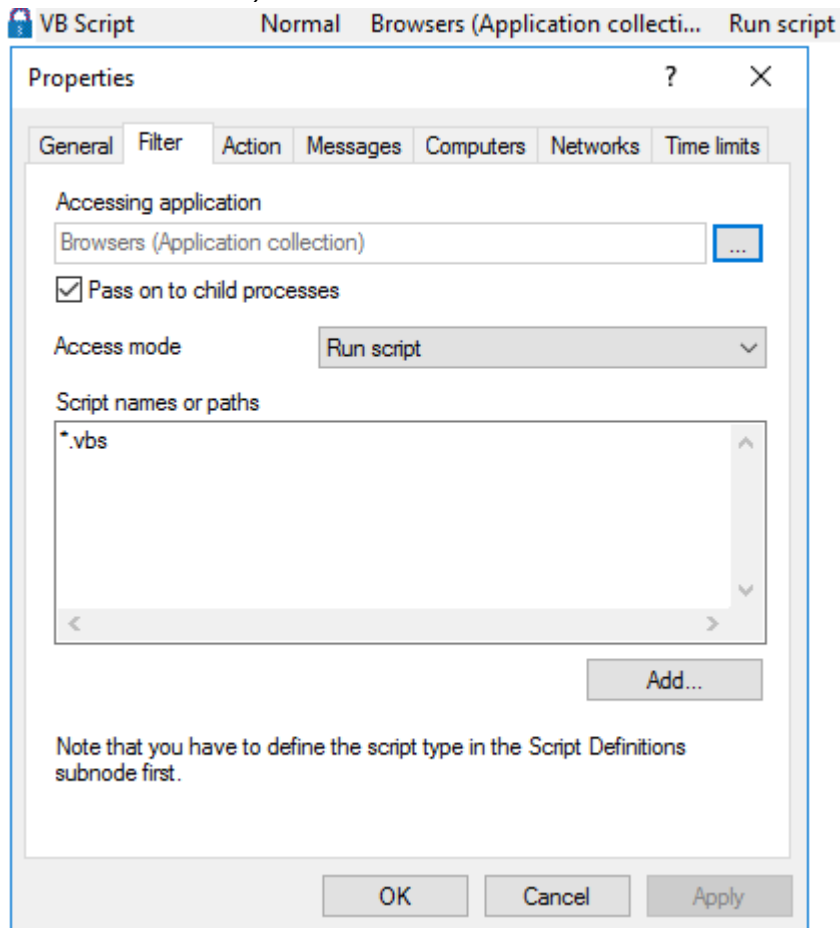
3. On the **Action** tab, select **Block** as the action.

4. For all other options, keep the default settings.

14.11.2.4 Use case 4: Read a specific directory

Scenario: You want to ensure that only your own banking software has read access to a specific directory. You do not want any other application to have read access to this directory. It would be possible for malware to gain read access to this directory via a security vulnerability in the browser and thereby read out your bank details. You need to prevent this from happening.

Proceed as shown in the figure:

1. Start out with entering a description and a **Comment** if required on the **General** tab.

2. On the **Filter** tab, enter Banksoftware.exe as **Accessing application**. As **Access mode** select **Read file** and under **File name** enter the path (in the example C:\Bankdata\).
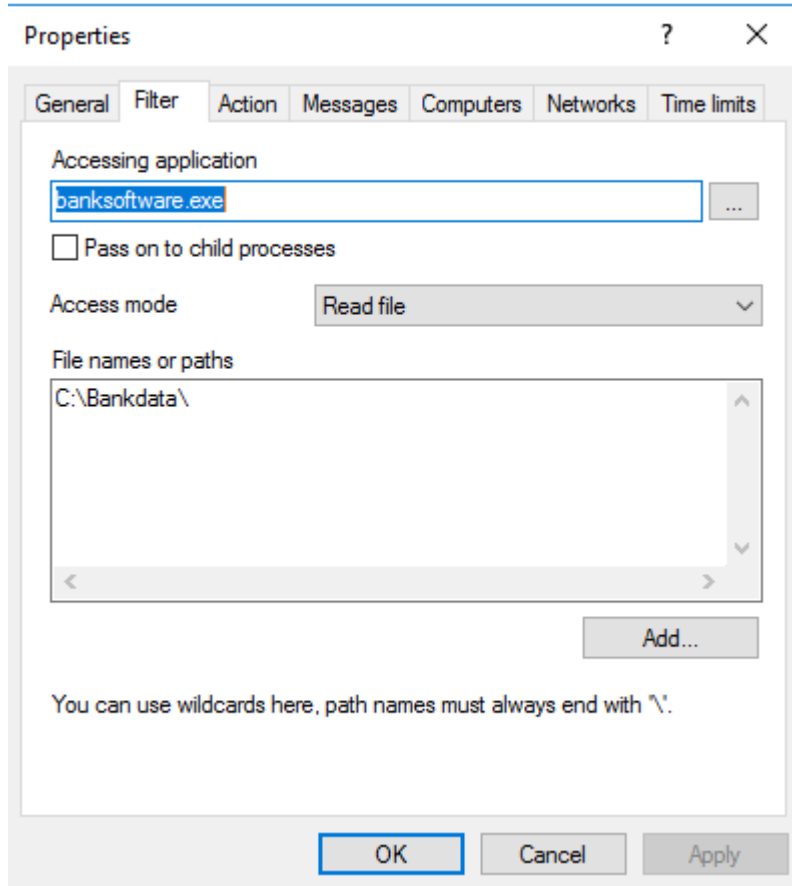
3. Specify the following on the **Action** tab:
   - Select **Allow** as the action and check **Block access by other applications** to ensure that only your own banking software has read access to the specified destination.

- The **Generate audit events when access is denied** is the default option.
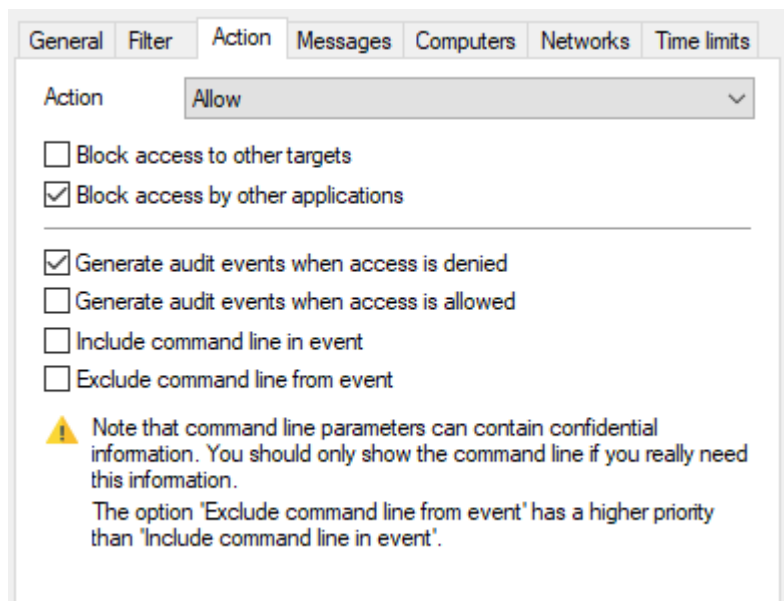
14.11.2.5 Use case 5: Write to a specific directory

Scenario: You want to specify that a particular browser (here it's Mozilla Firefox) is not allowed to write to the Documents folder. As you want to specify this for all and not just specific users, you will use a wildcard.

Proceed as shown in the figure:

1. Start out with entering a description and a **Comment** if required on the **General** tab.

2. On the **Filter** tab, enter the path to the browser as **Accessing application**.
    - To prevent the browser from being able to write to the directory via child processes anyway, check the option.

    - As **Access mode** select **Write file** and enter the path with wildcard (in the example C:\Users*\Documents\) in the **File name** text box.
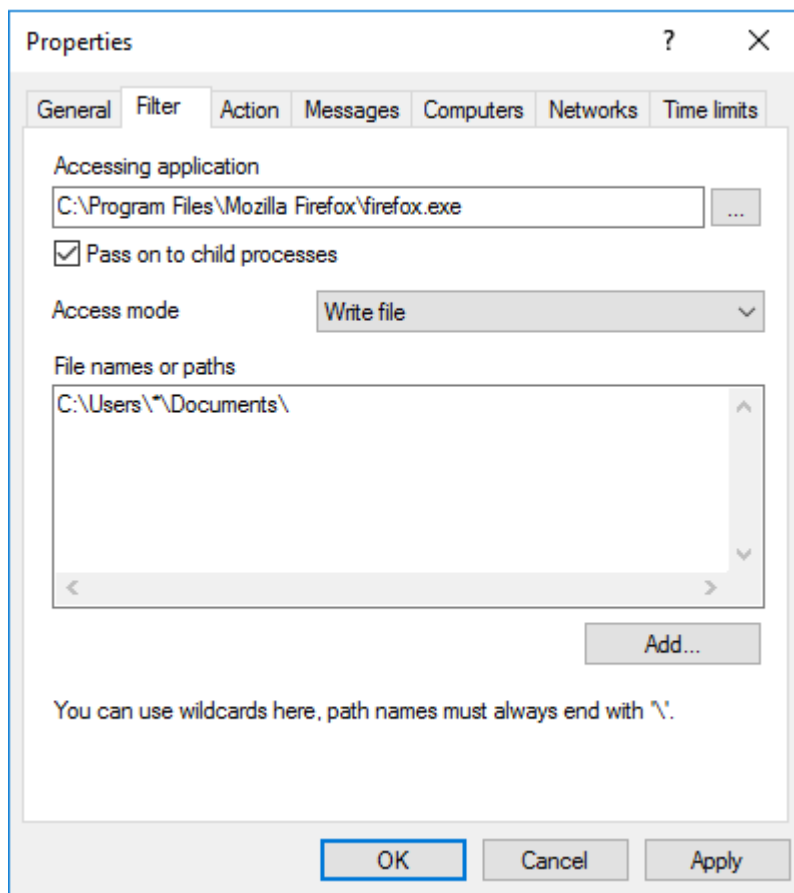
3. On the **Action** tab, select **Block**.

4. For all other options, keep the default settings.

14.11.2.6 Use Case 6: Restrict registry access

Scenario: You want to control registry access for your banking software from use case 4. Create two application permissions so that only the Banksoftware.exe is allowed to read the registry in the specified key.

Proceed as shown in the figure:

1. Start out with entering a description and a **Comment** if required on the **General** tab.

2. On the **Filter** tab, enter banksoftware.exe as **Accessing application**. As **Access mode** select **Read registry** and enter the key in the **Registry key** text box (in the example HKEY_CURRENT_USER\SOFTWARE\Bank Software\).

Properties   ?   ✕

| Computer | | Netzwerke | | Zeiten |
| Allgemein | Filter | | Reaktion | Nachrichten |

Ausführende Anwendung

banksoftware.exe   ...

☐ An untergeordnete Prozesse vererben

Zugriffsmodus   Registry lesen

Registry-Schlüssel

HKEY_CURRENT_USER\SOFTWARE\Banksoftware\

Hinzufügen...

Bei der Angabe sind Platzhalter zulässig, es dürfen nur Schlüssel
angegeben werden (keine Werte), der Schlüssel muss immer mit '\' enden.

OK   Cancel   Apply

Properties   ?   ✕

| General | Filter | Action | Messages | Computers | Networks | Time limits |

Accessing application

banksoftware.exe   ...

☐ Pass on to child processes

Access mode   Read registry

Registry keys

HKEY_CURRENT_USER\SOFTWARE\Banksoftware\

Add...

You can use wildcards here, enter only keys (no values) and always end
the key with '\'.

OK   Cancel   Apply

3. Specify the following on the **Action** tab:
   - Select **Allow** as the action and check **Block access by other applications** to ensure that only your own banking software has read access to the registry key.
   - The **Generate audit events when access is denied** is the default option.
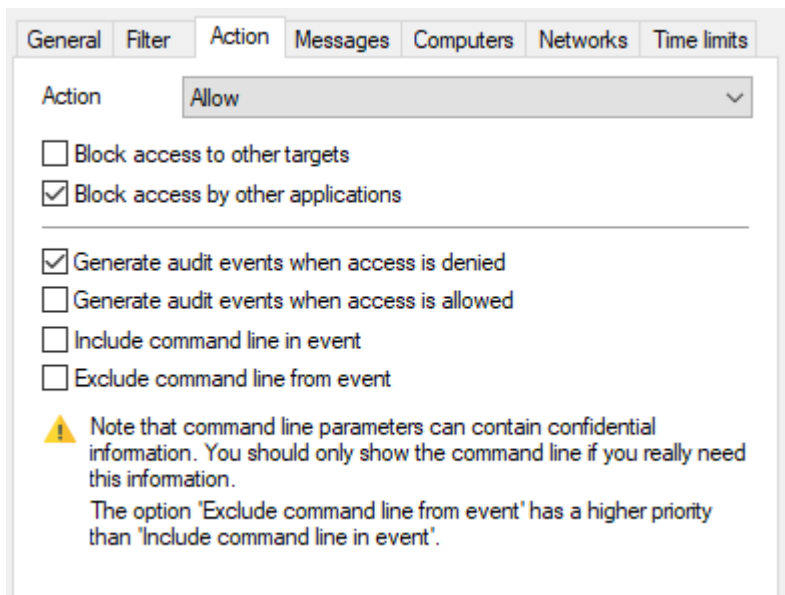
14.11.2.7 Use case 7: Detecting attacks with the example MITRE ATT&CK™ rules

DriveLock provides rules based on the MITRE ATT&CK framework. You can import these rules in the **Events and Alerts** node.

Some of these rules are stored in separate folders in the **Application behavior rules** node, see the figure below.

> 📝 Note: The purpose of these rules is not to block or allow actions, but simply to report certain events on the particular computer, that are then processed by the event filters and alerts.

14.11.3 Application rules

14.11.3.1 Use case 8: Show security awareness campaign when starting Outlook

Scenario: You want to display a security awareness campaign every time the user starts Outlook. Create a new file properties rule for this purpose.

Proceed as shown in the figure:

1. Specify the following on the **General** tab:
   - **Rule type**: Learning and Awareness

   - **Rule name**: Outlook

   - Choose the appropriate path. The other fields are filled in automatically.

   - Select the filters you want to create the rule by, and select the appropriate check-boxes.

   - Add a **comment** if necessary.

2. Open the **Awareness** tab.

Select the campaign from the drop-down list under **Add**.

> 🖋 Note: Make sure to set the **If used in rules** option on the **Trigger** tab in the properties dialog of the security awareness campaign.

For the **Phishing** campaign, the following information appears on the **Usage** tab:
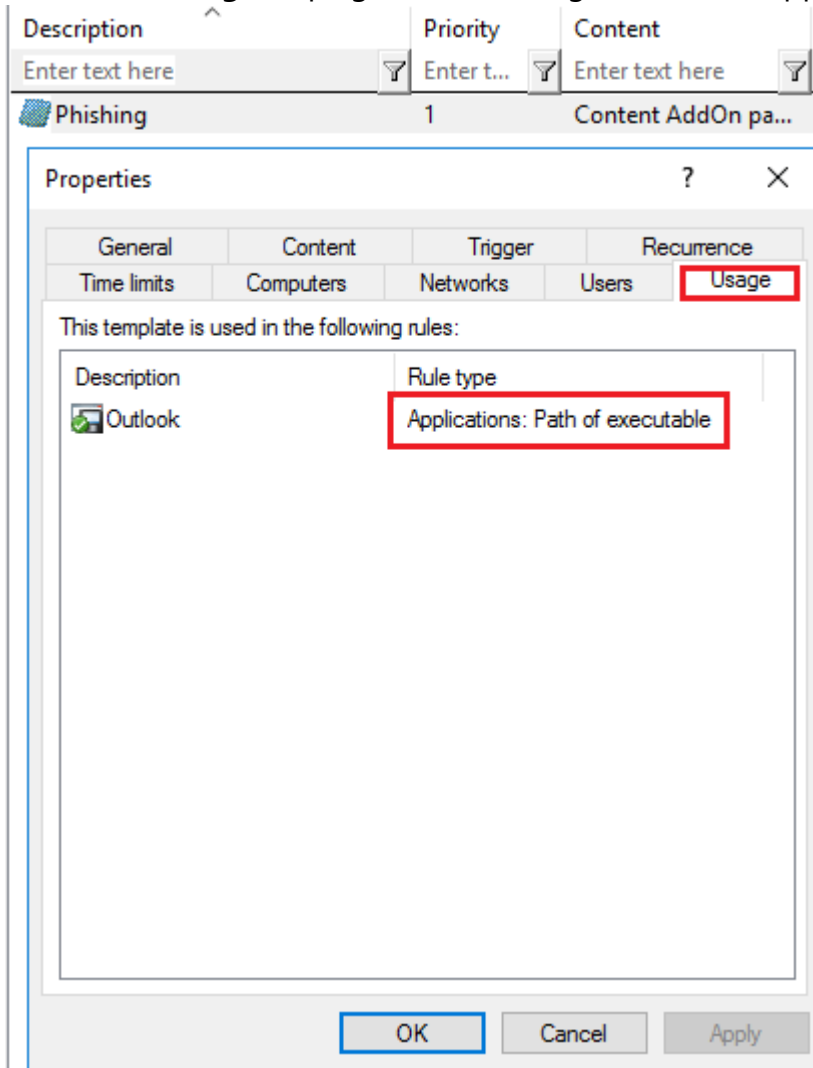
3. For all other options, keep the default settings.

14.12 List of Application Control terms

Term	Explanation
Application collection	Grouping of several related applications in terms of subject matter or program. An application collection is used in application rules or in application behavior rules.
Application rules	Application rules can be used to allow or block individual applications, as well as configure local learning and the dis-

Term	Explanation
	play of awareness campaigns.
Application behavior	Application behavior includes all actions an application executes, such as starting additional applications or DLLs or writing to specific directories.
Application Behavior Control	Monitoring the behavior of applications. DriveLock monitors and controls the activities of applications running on the agent.
Application behavior rules	Application behavior rules define the actions an application is allowed or not allowed to perform (for example launching other programs, loading DLLs, reading or writing files or the registry, executing scripts).
Blacklist	A negative list containing non-permissible and untrustworthy targets. By blacklisting it is possible to block specific applications.
Local learning	In the course of a learning phase, the DriveLock Agent learns what is allowed on the particular client computer: starting applications or DLLs, or performing actions such as writing to specific directories.
Local whitelist	The local whitelist is a hash database rule that is generated locally. It can be pre-filled with executables (allowed files) in certain directories and can be extended accordingly.
Simulation mode	During a simulation, DriveLock generates event messages for started or blocked applications based on configured rules, but execution itself is neither allowed nor prevented.
Application behavior recording	Recording of application behavior on the DriveLock Agent; to be saved as a JSON file and to generate application behavior rules from it.
Whitelist	A positive list containing allowed and trusted targets. Only these may be executed.

15 Drive and 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,

15.1 Controlling 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.

15.1.1 Drive control overview

The following figure shows how the different elements are related to each other.
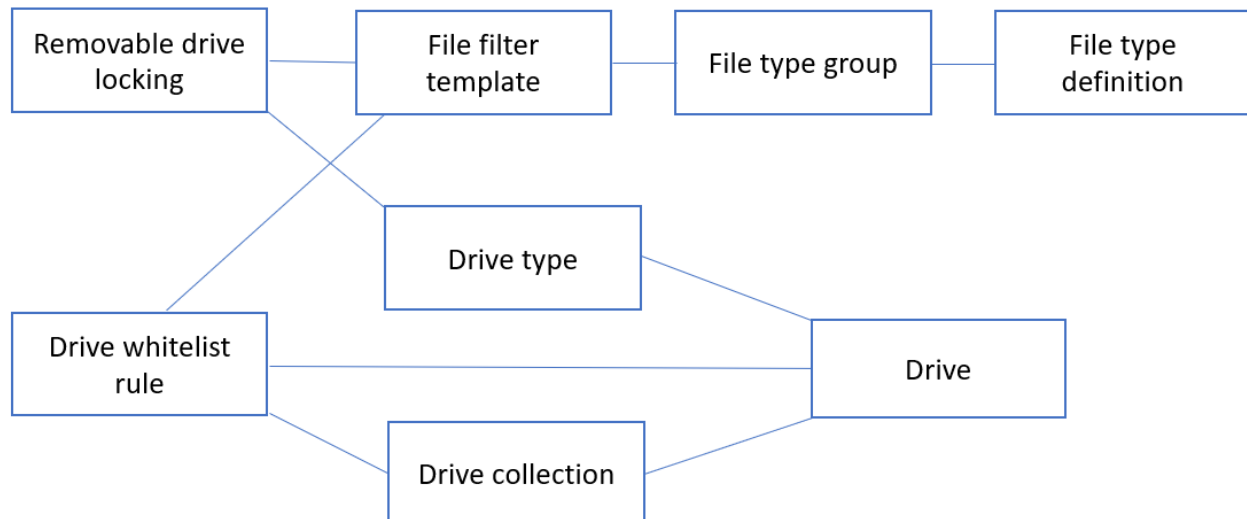
The removable drive locking settings are used to specify the type of drive you want to lock at a general level. Here, you can use file filter templates, file type definitions or file type groups that you have created earlier. In this case, proceed as follows: first define the file type, then specify 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.

15.1.2 Settings

You can specify the following settings when configuring how to lock or unlock drives.

- Global security settings

- Custom user notification messages

- Configuring file hash generation

- Volume identification file settings

- Shadowing configuration

- Hard drive self-monitoring (SMART) configuration

- Advanced settings

309

15.1.2.1 Global security settings

Setting	Functionality
Always allow access to admin- istrators	It is possible to allow access to drives for all members of the Administrators group, regardless of which whitelist rules or set- tings 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.

15.1.2.2 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 mes- sages. You can also use some of the HTML tags for formatting your message (for example `<b>Text</b>`).

> 📝 Note: If you configured a multilingual message text for the current language, DriveLock will display the standard messages defined for this language instead of the message configured in this dialog box.

15.1.2.3 Configuring file 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 to examine file transfers and track files in your organization more closely.

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. There may be a requirement to use a specific hash algorithm because of corporate policies.

To enable the generation of content hash values, select the **Generate digest from file con- tents** option and set whether they will be generated synchronously or delayed. For larger files, generating these hash values can take some time.

15.1.2.4 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)

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.
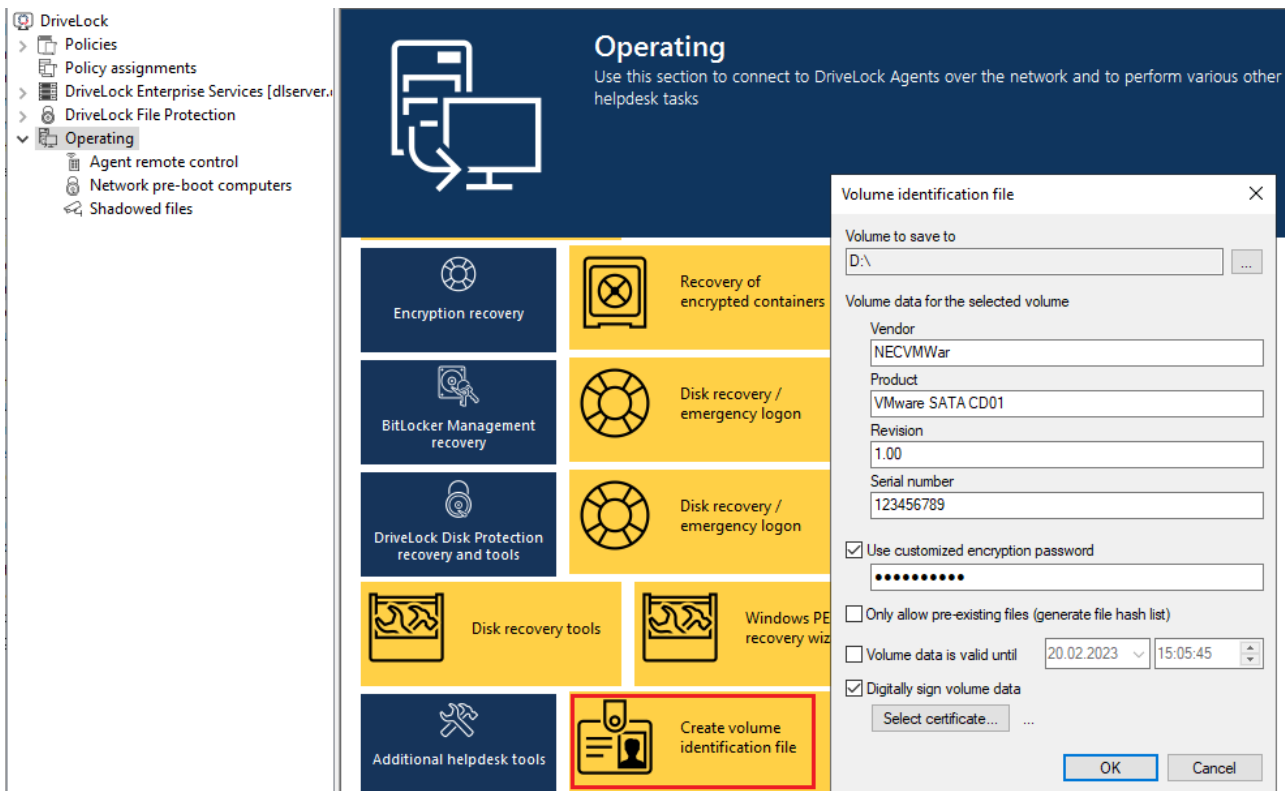
15.1.2.5 Shadow copies

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 con-
nection, 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.

15.1.2.5.1 Shadowing configuration

You can configure settings for shadow copies as follows.
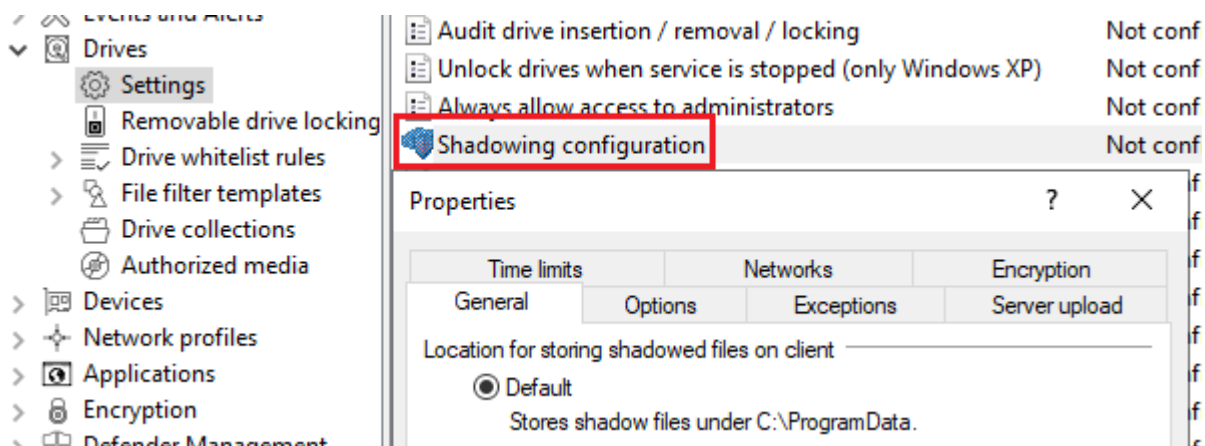
1. On the **General** tab, specify:
   - **Location for storing shadowed files on client**: The shadow copies are stored
     in the `C:\ProgramData\CenterTools DriveLock\ShadowFiles` folder
     by default. However, it is also possible to specify a different storage location. To
     do so, select "Fixed 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 auto-
     matically 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.

15.1.2.6 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.

15.1.2.7 Advanced settings

Setting	Functionality
Audit device insertion / removal / lock	If activated, matching audit 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)

15.1.2.8 Allow end user to request drive unlock

If you do not yet have any rules configured for particular drive types, you can use this setting to allow end users to ask for drives to be unlocked.
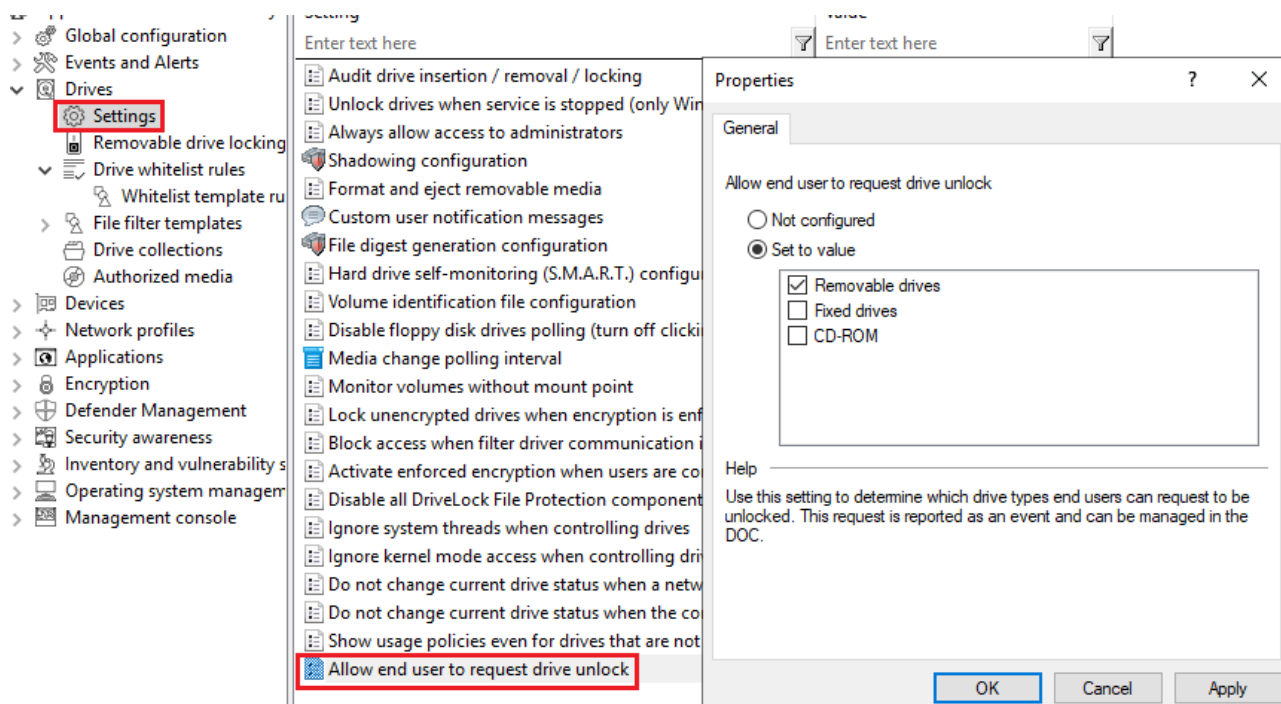
If configured, this setting will show a menu command on the DriveLock Agent that allows the user to submit an unlock request. The request is will then be submitted as an event (ID 754) and can be viewed in the DriveLock Operations Center (DOC).

Tip: Create a dashboard widget showing the end-user requests and/or the corresponding event. Then you can respond directly. Additionally, you can also create a notification rule.

Then, you can create a drive rule from this event (or add it to an existing drive rule) and unlock the drive.

15.1.3 Removable drive locking

The basic configuration allows you to easily enable or disable basic blocking settings and add whitelist rules. To specify detailed settings for controlling drives, click **Advanced configuration** in the various sections. Here you can find additional configuration options.

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. Further information can be found in the Encryption 2-Go chapter.

- 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.

15.1.4 Drive whitelist rules

Different types of whitelist rules are available and can be used to define drives according to specific criteria:
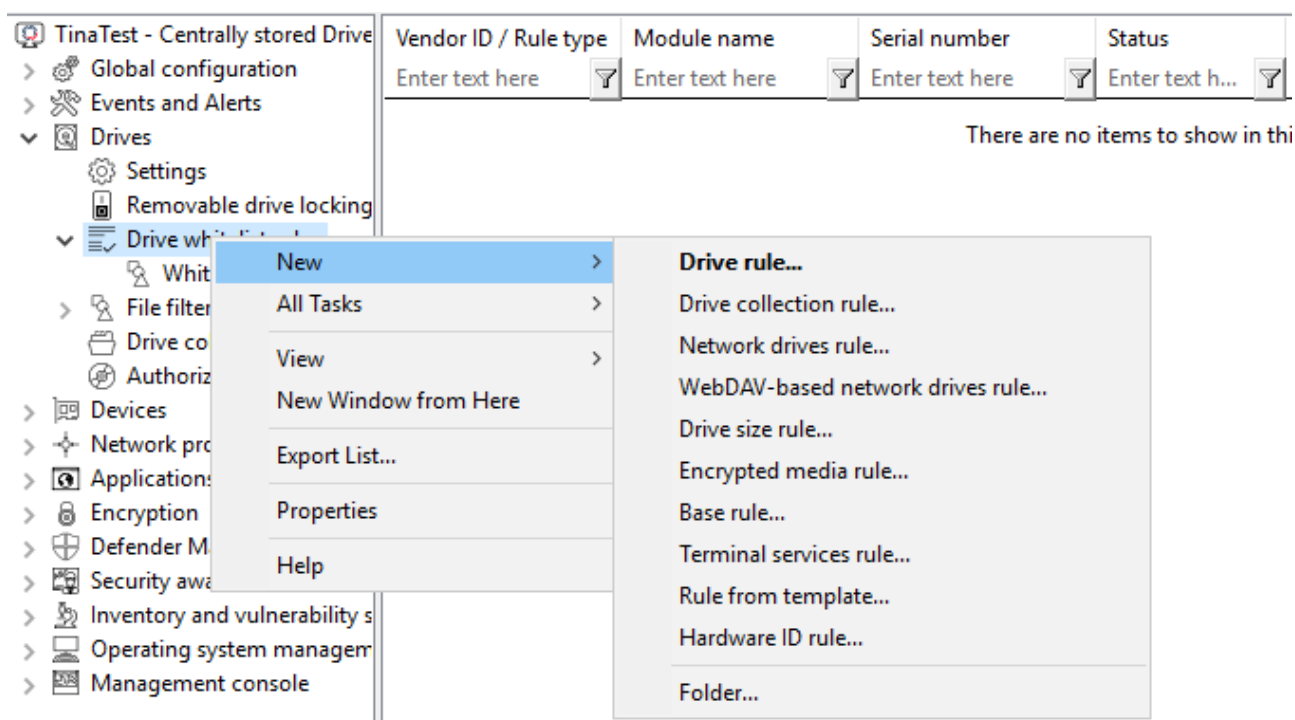
- **Drive rule**: Use this rule to specify a particular drive based on its manufacturer, product or serial number, for example.

- **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 is only possible, however, if you have configured DriveLock so that the agent does not 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. Set priority of the rule (on the **Options** tab)

2. Drive rule (a rule with a serial number has a higher priority than a rule without).

3. Drive size rule

4. Base rule

5. General removable drive locking settings

> ✏️ Note: A general rule has a lower priority than a special rule.

15.1.4.1 Basic drive whitelist rule

You can easily create drive whitelist rules in the basic configuration. Proceed as follows to do so:

1. Click the **Add whitelist rule...** link to create a new whitelist rule.

2. Now provide the following information:
   - **Vendor ID**: Name or abbreviation of the drive vendor. You can also select a drive by searching for it with the **...** button.
     The **Installed drives** dialog opens. Here you can select local drives or drives on a DriveLock Agent using the **On agent** option. You can use the **Connect** button to connect to the corresponding agent.

     > ☑ Note: DriveLock reads the hardware information from the Windows operating system. For this reason, DriveLock is only able to list drives that are actually in the Windows operating system.

   - **Product ID**: Unique ID of the product, assigned by the vendor.

   Each drive contains some information about the hardware it is based on (for example, the name of the vendor and the name of the product).

   > ☑ Note: With both options you can use wildcards: * for several characters, ? for exactly one character.

3. A serial number is added automatically if you check **Only allow selected serial numbers** in advance. Click **Add** to add more serial numbers.

4. On the **Permissions** tab, you can define the users or groups that will have access to the drive.

5. On the **Options** tab you configure additional settings (file filters, shadow copy, encryption, etc.).

15.1.5 Drives in the DOC

Drive rules can be created in various places in the DOC.

1. *Security Controls -> Drives -> Configuration -> Rules*

2. *Analytics -> Events*

Drive events can be used as a source for a drive rule. Click the **Add to rule** menu item to add the drive to an existing rule. Via the **Create rule** menu item, you can create a new rule that already contains the data for the respective drive.

3. *Inventory -> Devices -> Drives*

4. *Administration -> Policies*

15.1.5.1 Creating drive rules

Please do the following:

1. Once you have selected the **Create rule** option, a dialog opens in which you can add the drives for which you want to create a rule under Drives. You can select whether to add the drive from the inventory and or via the product and vendor ID or the hardware ID / serial number.
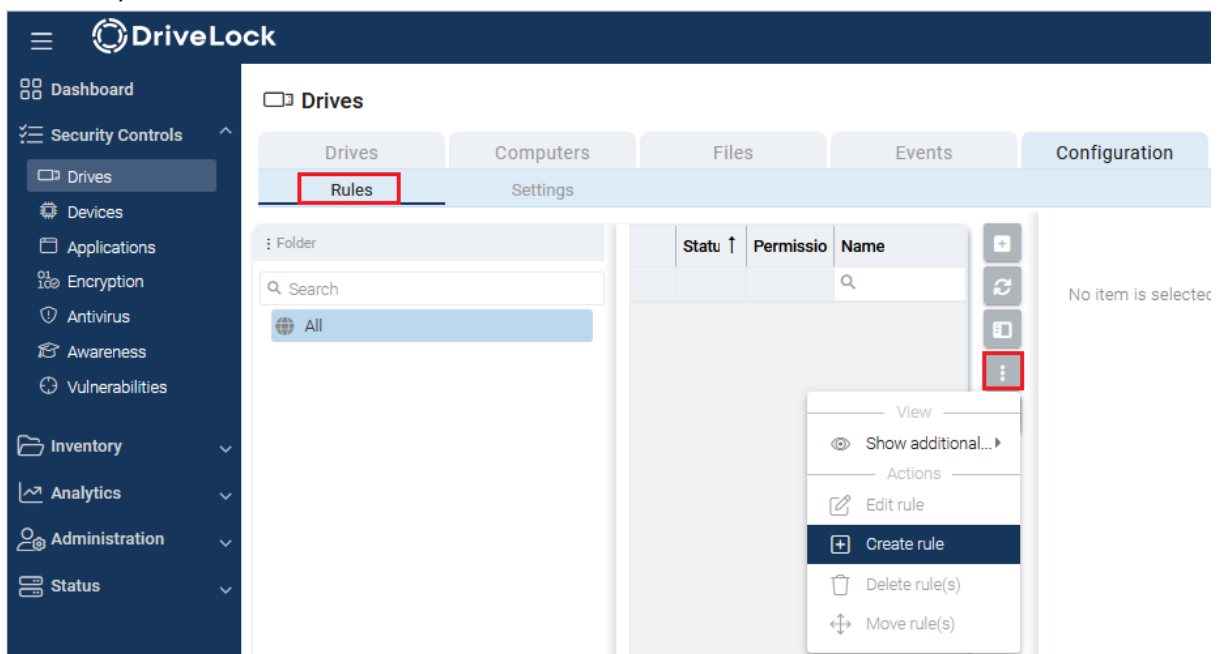
Note: Hardware IDs can also be used with Linux and macOS Agents.

2. In addition to the rule name, you can also configure the following in the **basic properties**:
   - **Usage policy**: A drive may only be accessed once the user has accepted a usage policy. This can be additionally secured by entering the Windows password.
   - In the **Encryption** section, for example, you can specify whether the drives are encrypted automatically or whether no encryption is required.

> ☑ Note: Please note that encryption and recovery must be configured in a different policy for enforced encryption.

- In the **Permissions** section, users and groups can be selected from the AD inventory and added 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.

15.1.6 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.

15.1.7 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.

15.1.7.1 Creating a new file filter template

Follow these steps to create a new File filter template:

1. Select **New** and then **Template**.
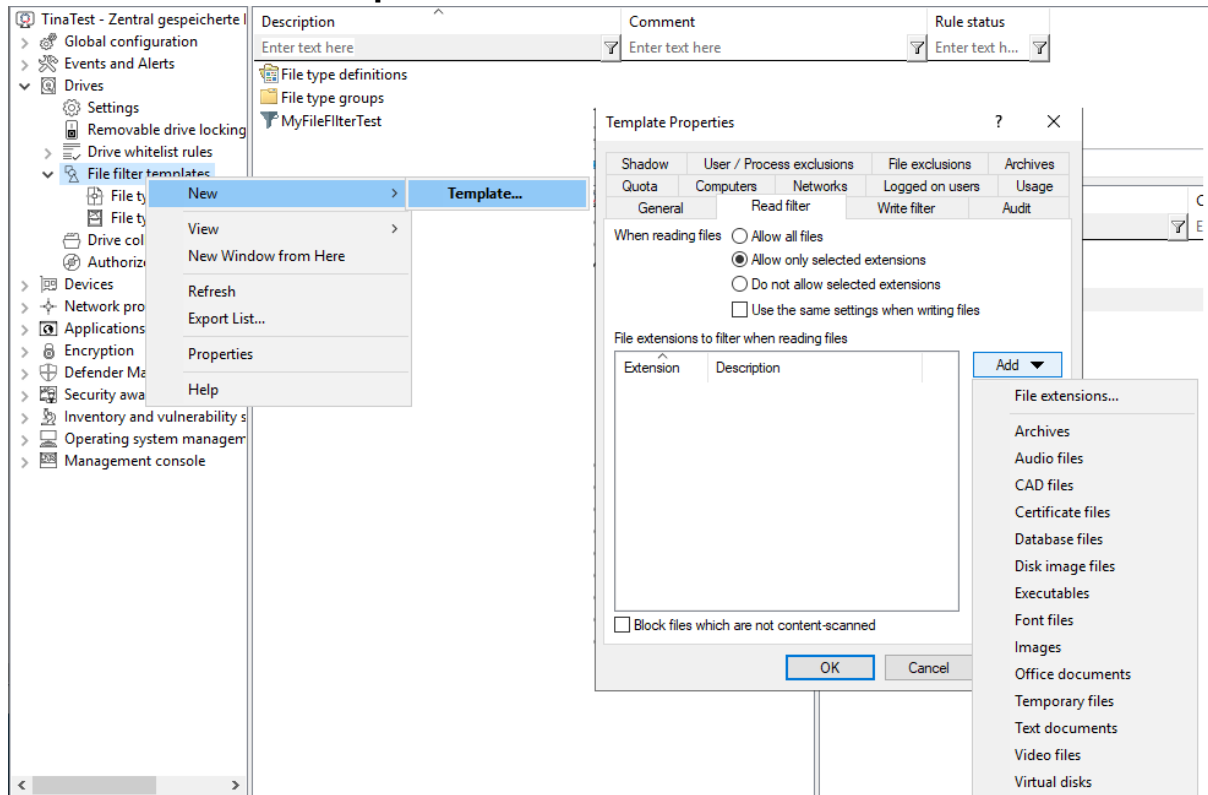
2. On the **General** tab, enter a name in the **Template description** field and optionally a comment.

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.

15.1.7.2 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**.

15.1.7.3 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.

15.1.7.4 File filter template for encrypted drives

To apply a file filter template to encrypted drives, you need to add a 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 and create a whitelist rule. Check the **Filter files...** option and/or **Audit and shadow files...** and select a template.

15.1.8 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.

15.1.8.1 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.
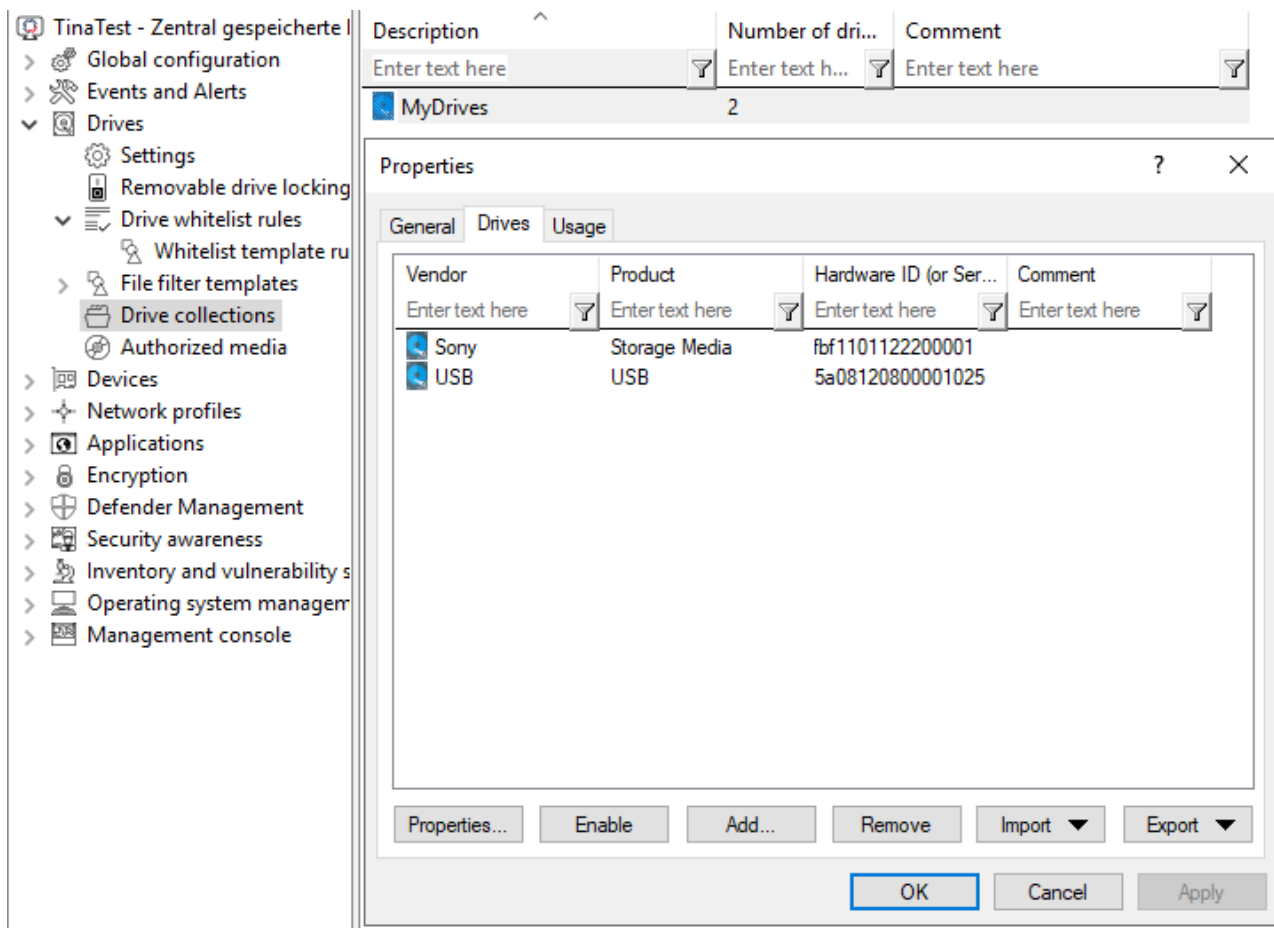
If you want to add new entries, click **Add** and, if necessary, select whether you want to add a drive based on its product or manufacturer ID or using the hardware ID (only for drives that provide this information - if not, only the hardware ID is queried). In the next dialog, enter the required information or select it in the usual way from the currently connected drives by clicking the **...** button. 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 list for a limited time, select the drive you want and then click **Disable**. 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.

15.1.9 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.

15.2 Controlling devices

DriveLock operates with whitelist rules. This basic concept implies that all devices are generally blocked 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): as of version 2024.1, custom device classes can also be used here
- 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.

If several rules apply, they are prioritized according to the following criteria:

1. Priority set on the Options tab

2. Rule type (prioritized from 1 to 3)
    1. Hardware ID and device collection

    2. Bluetooth

    3. Bus

3. Rules that allow something have a higher priority than rules that block something

4. Rules with awareness settings have a lower priority than rules without

15.2.1 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 specified multilingual user messages in the global configuration section, DriveLock displays the default messages in the current language instead of these messages.
    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.

15.2.2 Device class locking

DriveLock distinguishes between different types of devices. By default, DriveLock does not initially lock any devices (or device classes). If you lock a device class, all devices belonging

to this class (or which are connected via the same controller or the same 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 .

To lock devices via your device class in the DOC, open *Security controls -> Devices -> Configuration -> Device classes*.

You can set up locking for the following **adapters and interfaces**:

- Serial (COM) and parallel (LPT) interface

> ✏️ Note: Please note that the setting for blocking these interfaces must be set manually once you have updated to version 2024.1.

- 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

- Unknown Linux device (new device class from version 24.2 for devices that were found by Linux Agents and for which no classification is possible)

- 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 the corresponding device. The configuration is identical for all device classes except interfaces and Apple and Android devices (treated as drives).

15.2.2.1 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:
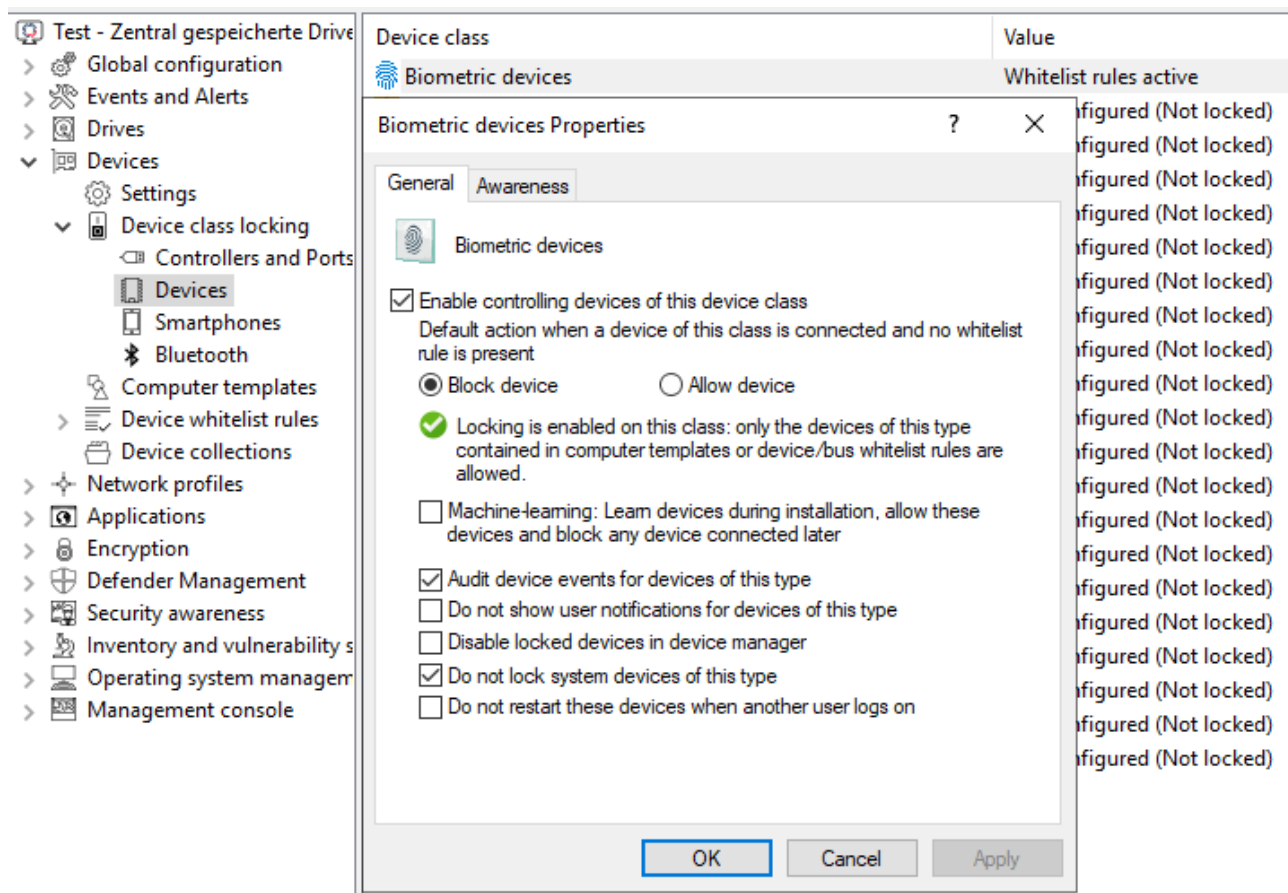
- **Enable controlling devices of this device class**: Enable blocking or allowing the selected device class. Select the appropriate option.

- **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 audit events are generated. If this option is set, the events are transmitted to the configured locations (e.g. 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 enabled by default initially. 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.

15.2.2.2 Blocking interfaces

The configuration of the two interfaces COM and LPT is limited to blocking or allowing for some or all users.

> Note: From version 2024.1, these interfaces are no longer blocked by default.

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.

On the **Messages** tab, you can enter a user-defined message that is displayed to the user on the client as soon as an interface is blocked. If you do not save your own message, a notification generated by DriveLock will still be displayed. If you do not want any notifications to be displayed at all, please check the option **Do not display any notifications**.

> Note: 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", as Windows does not enable hardware detection on the serial interfaces (COM).

15.2.2.3 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.

> ☑ Note: Please note that Apple devices are classified as 'regular' devices in the DOC.

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.

Click here for more information about the **Awareness** tab.

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.
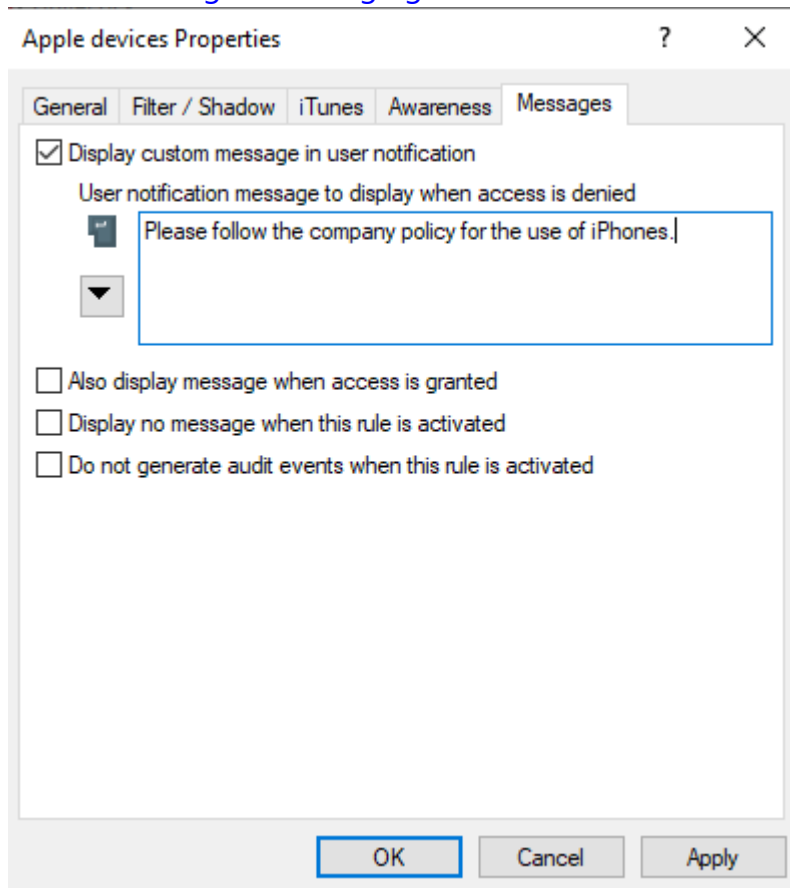
- If you want the message to be displayed even if access by the user is possible, enable the corresponding option.

- To disable the display of notifications in general (including the display of standard notifications), enable **Do not show 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**.

15.2.2.4 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.

Concrete 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).
  Further information on Bluetooth services can be found at Microsoft under the following link.

> ⚠ 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.

15.2.3 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.

15.2.3.1 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.

15.2.4 Device whitelist rules

Whitelist rules for devices are created in the same way as drive rules. From version 2024.1, cross-device class whitelist rules can also be configured for **all classes**.

The following example shows the creation of a rule for a biometric device.
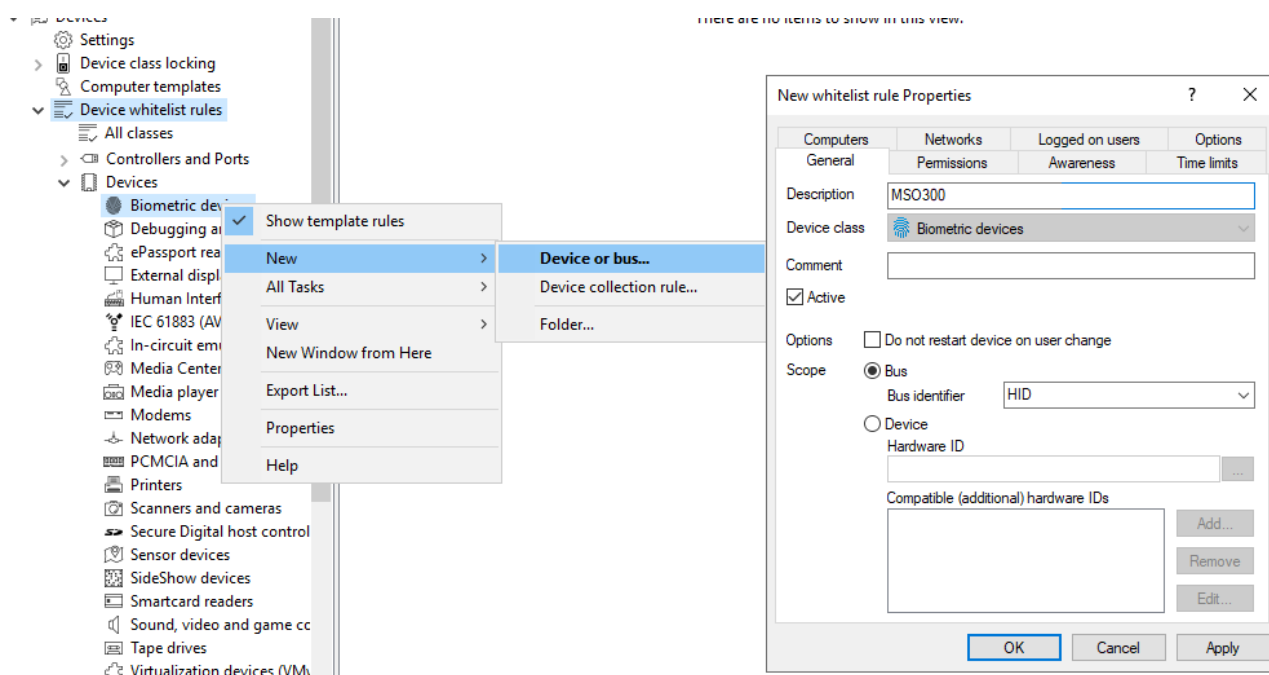
In the **Description** field enter a name, in this case it is the MSO300 series biometric device. You can additionally add a comment.

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.

15.2.5 Devices in the DOC

Starting with version 2024.1, you can also set rules and policies for devices in the DOC and control devices based on their device classes. Custom device classes can also be created for device classes, which allows you to control devices that are not provided by DriveLock as default devices.

Just like the drive rules, you can create device rules in various places in the DOC.

1. *Security Controls -> Devices -> Configuration -> Rules*

2. *Analytics -> Events*

   Device events may be used as a source for a device rule. A device is added to an existing rule via the menu item **Add to rule**. Via the **Create rule** menu item, you can create a new rule that already contains the data for the respective device.

3. *Inventory -> Devices -> Devices*

4. *Administration -> Policies*

15.2.5.1 Device classes in the DOC

Open *DOC -> Security Controls -> Devices -> Configuration -> Device classes*.

Starting with version 2024.1, you can also generally block or allow device classes within the DOC. Apple devices are considered devices in the DOC unlike with the Policy Editor in the DMC.

If you cannot find your device class in the list, you can create a customized device class for it. The advantage of this is that COM and LPT ports can be controlled as a device class. It is also easier to use device collections with different device classes.

1. Select the menu command **Create custom device class**.
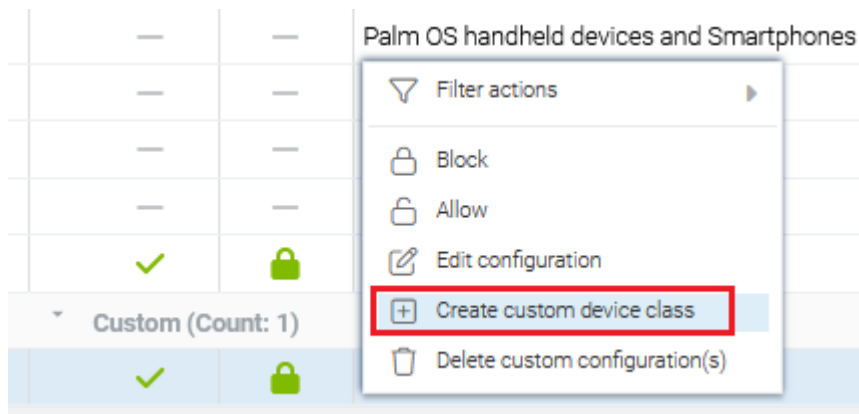
2. Enter a **name** and enter the **device ID** of the Windows device class.

3. Optionally, you can configure additional settings.

15.2.5.2 Use case: Unlock request for a device in the DOC

The following questions are answered in this use case:

- How do you lock a device via its device class in the DOC?

- How can you unlock the locked device for users?

- What do you do in the DOC as soon as a user has created an unlock request for this device?

Open *DOC -> Security Controls -> Devices -> Configuration -> Device classes*

1. In the example, you want to block the use of **Android devices**. Select this entry from the list and open the context menu. Click **Block**. A green lock indicates the lock status 'locked'.

2. Optionally, you can configure individual lock settings by selecting **Edit configuration** in the context menu, for example, or simply clicking on the device class. The options correspond to those in the Policy Editor and are explained here.

3. Is the unlock request option already set up on your DriveLock agents? If not, please configure it first in the **Global configuration** in the Policy Editor. Click here for more information.

4. An Android device is now connected on the DriveLock Agent. A message indicates that it is locked. To be able to connect it anyway, the user selects the option **Request unlock** via the DriveLock icon in the taskbar.

5. The following dialog shows the device, the user selects it accordingly and then clicks on **Request unlock**. A reason for the release must be given before it can be sent.

6. Back in the DOC, you will see the new request from the Android device shortly afterwards under *Administration -> Unlock request*.

7. You now have the following options in the detail window:
   - **Approve unlock and create new rule**: You can create a new device rule directly during the unlock process.
   - **Approve unlock and add to rule**: If you have already created a rule, for example one for all allowed devices, you can simply add the Android device.
   - **Deny**: If you do not agree to the device being unlocked, you can send the user the reason for the denial as a message. The device will remain locked until further notice.

8. Unless denied, the requested device can now be used on the DriveLock Agent and is allowed for further use.

9. The device is now displayed in your list of devices. Here you can also see all **device activities** in the detail window, for example when the device was unlocked (allowed)

or when it was added to a rule. The related objects (for example the computer the device was connected to) are also displayed.
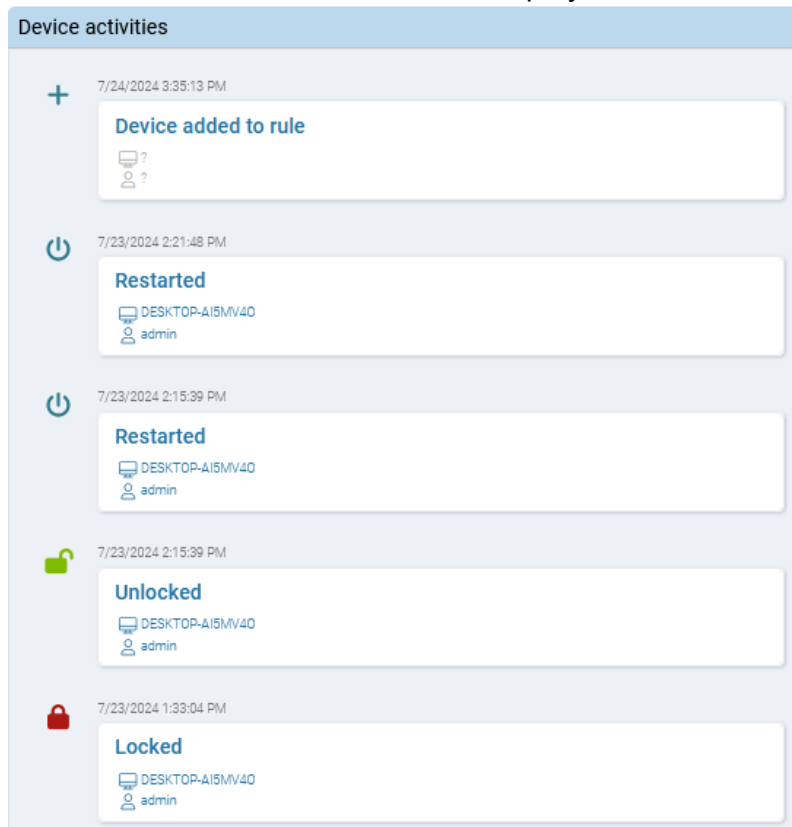
15.2.6 Device collections

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.

From version 2024.1, device collections can also contain device classes of different types. In a policy from the Policy Editor, use the **All classes** option for this.

> Note: If the device collections also contain MTP devices, it is not possible to use access permissions for DriveLock groups.

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.

15.2.6.1 Creating device collections

To create a new collection, 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.
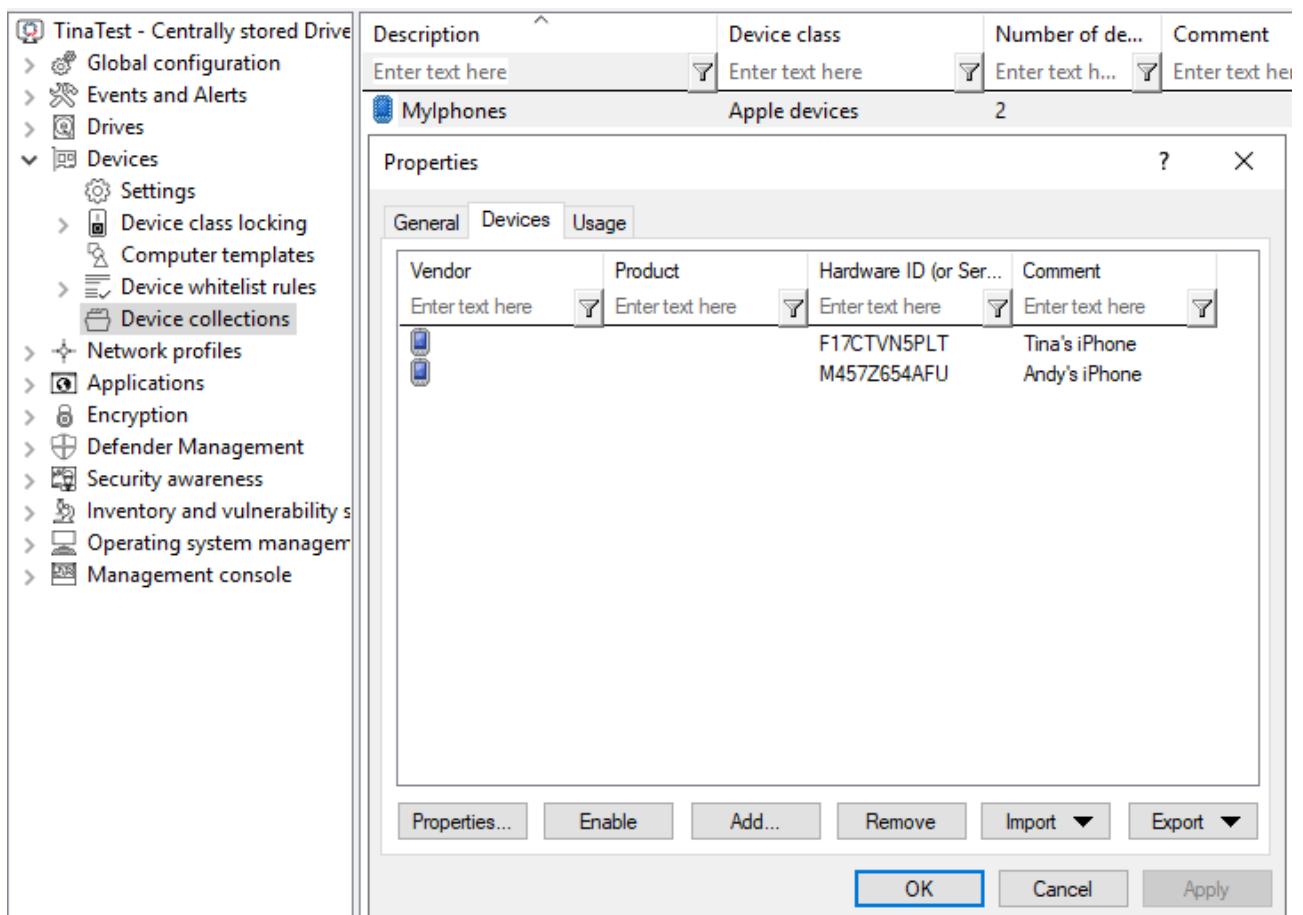
Here you can display, deactivate, edit and delete existing entries. New entries can be added as well.

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 con-

nected 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.

15.2.7 Controlling Bluetooth controllers, devices, and services

There are different types of Bluetooth devices representing various physical or logical devices:
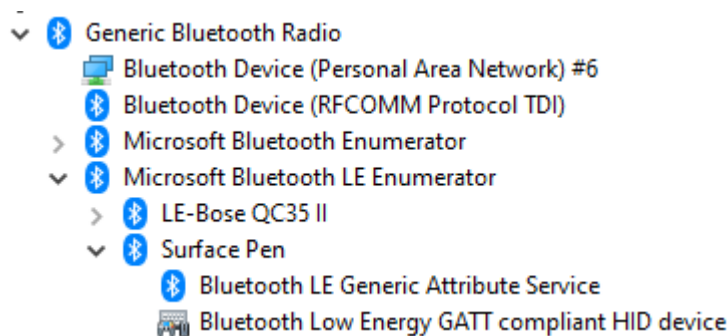
Bluetooth radio adapters

These devices are either built into the PC or connected to it via USB. They transmit and receive Bluetooth signals to and from peripheral devices. USB devices have their own hardware ID, which can be used in whitelist rules. You can also create a bus-based rule for the USB bus, see the figure below:
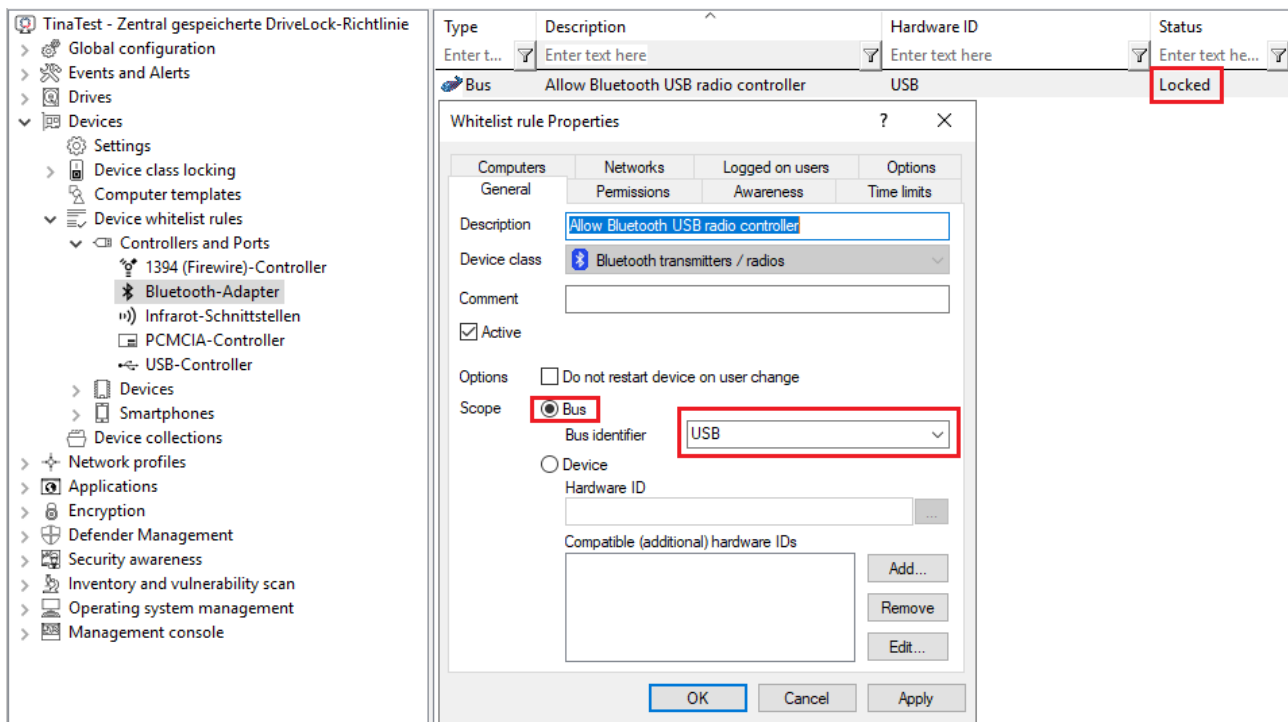
Bluetooth Windows devices
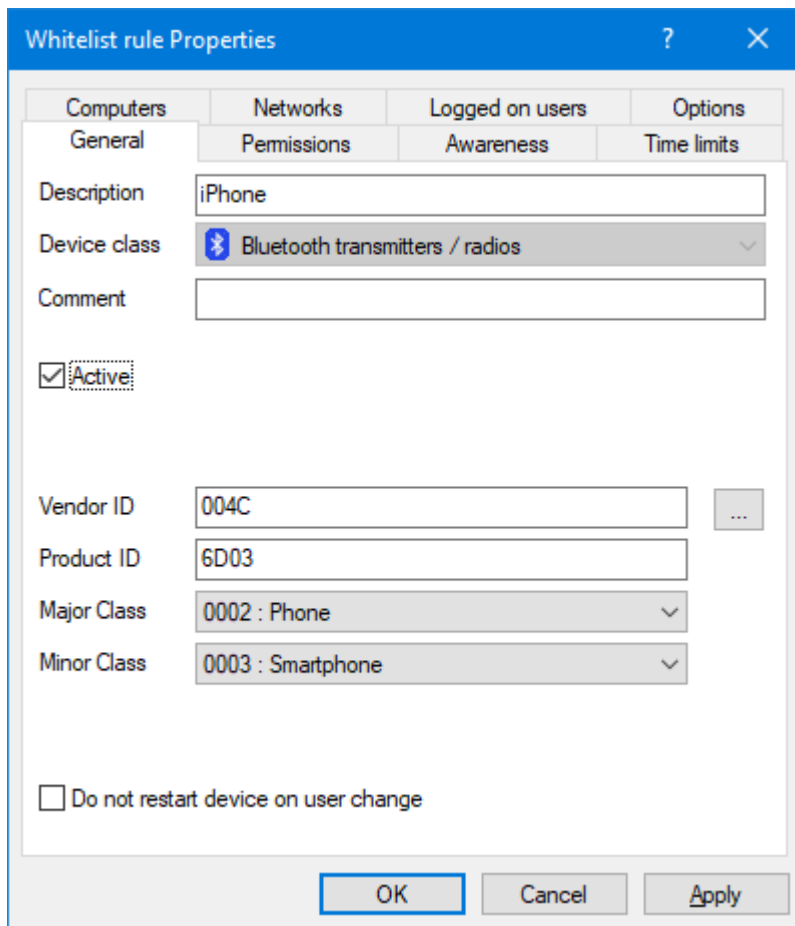
In this category, there are three fundamental Bluetooth devices: Microsoft Bluetooth Enumerator, Microsoft Bluetooth LE Enumerator, and Bluetooth Device (RFCOMM Protocol TDI). They are treated as system devices and do not need to be explicitly whitelisted if the "Do not block system devices of this class" option is enabled. If not, they can be unlocked via hardware ID or via the Bluetooth bus.

Bluetooth devices

These devices are logically sorted according to the enumerators mentioned above. Controlling them is challenging as their hardware IDs are not unique and can change even after re-pairing. Therefore, there is a new rule type for Bluetooth devices based on manufacturer, product, and classes.

The rule editor can only retrieve properties from devices that are already paired, either locally or through an agent. Paired devices are stored in the system, even when not connected. When Bluetooth device control is enabled, DriveLock also generates Bluetooth-related events, including their properties. The two screenshots below illustrate two rules:

Rule 1 for a classic device (iPhone):

Rule 2 for an LE device (Surface Pen). No classes are configured for the LE device as it is not part of the Bluetooth LE standard.

Bluetooth services

Each Bluetooth device provides a set of services. Starting from version 2023.1, they no longer need to be explicitly whitelisted. The whitelist rule of the parent device will be used.

Peripheral devices

Peripheral devices provide the actual functionality. Under Windows, they do not belong to the Bluetooth class of devices but can be found under Human Interface Device, Audio devices, Sensor Devices, and many more. They must be whitelisted under their respective device class. T The easiest way to do this is to create bus-based rules for the following buses: BTHENUM (classic devices), BTHLEDEVICE (LE devices), BTHHFENUM (hands-free devices).

16 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

16.1 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
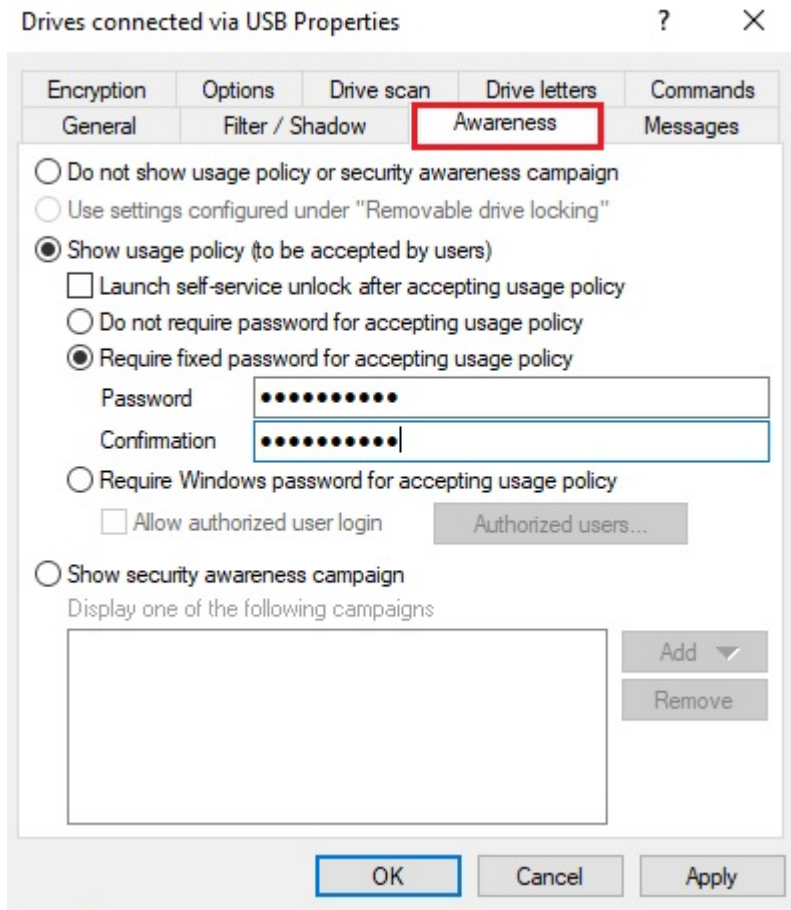
or a device rule:
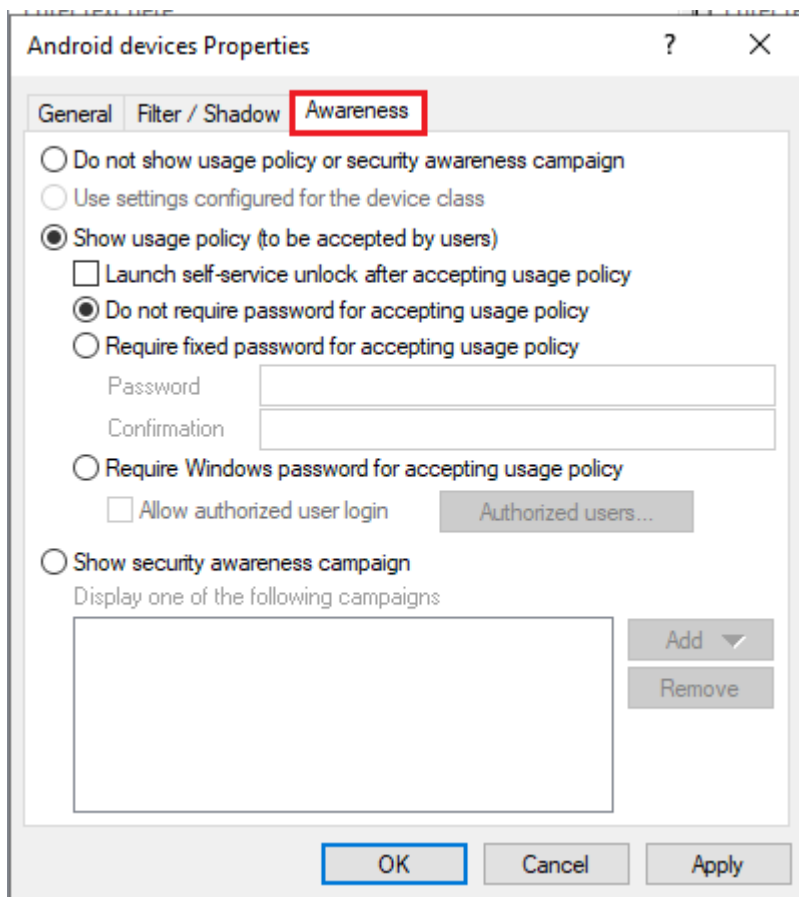
To do so, select the **Show usage policy option (to be accepted by users)**.

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 started automatically.

  > ⛔ Warning: If the accepting user does not have permission for self-service unlock, the usage policy can still simply be accepted without the self-service unlock being started. If you want to specify users who are allowed to accept the usage policy, you can enter them in the list using the **Authorized users** option.

- **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 lets you unblock the file with a different user account than the one that is currently logged in, by entering the user name and the appropriate password. Optionally, you can specify the authorized

users for this via the **Authorized users** button.

> ⛔ Warning: Please note that the registered user must also be specified here in order to accept the usage policy!

- **Show security awareness campaign**: Click here for more information on awareness campaigns.

16.2 Commands

On the **Commands** tab you can configure the execution of command lines (see illustration with example command).

- 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).

16.3 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.
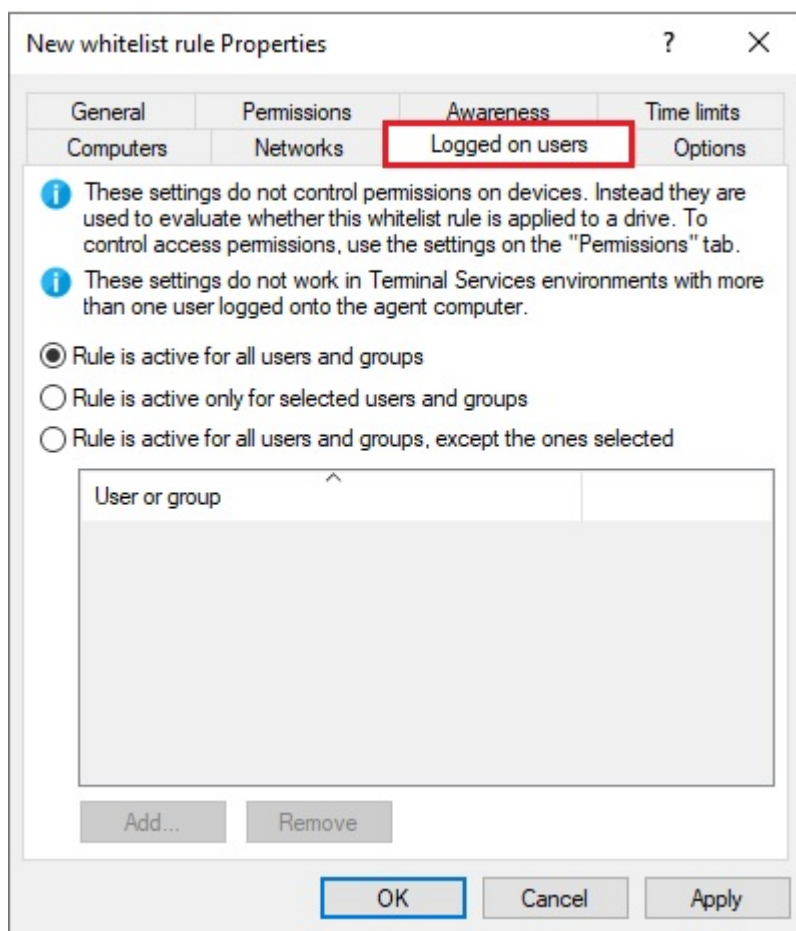
Choose one of the following options:

- 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.

16.4 Computer

Use the **Computers** tab to specify on which computers the whitelist rule should be valid.
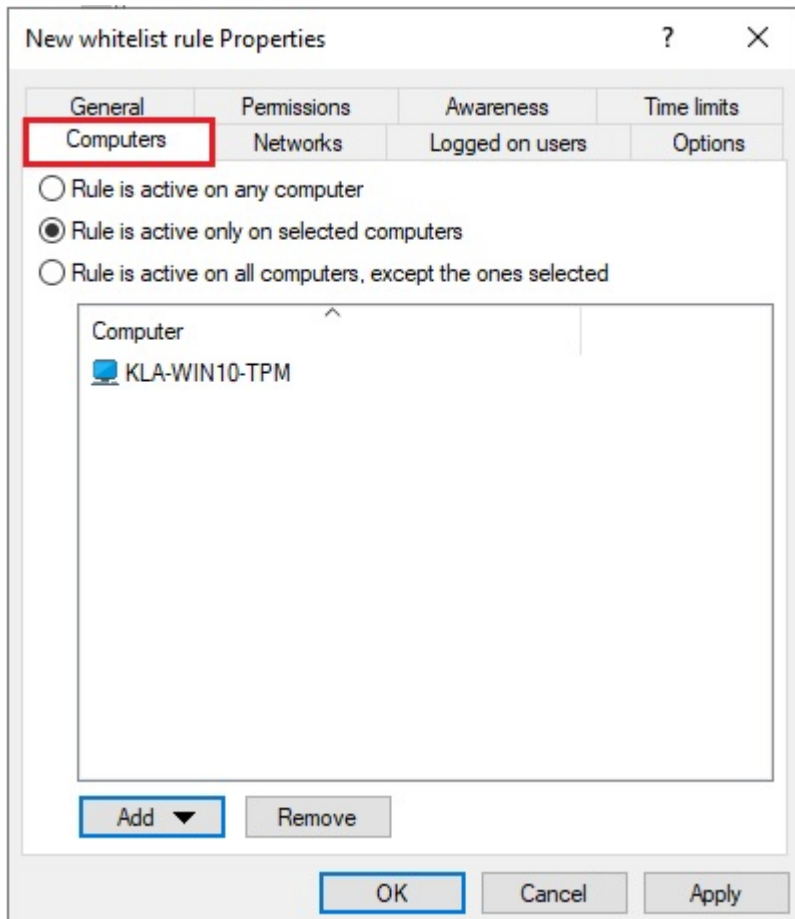
Choose one of the following options:

- 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.

16.5 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.

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.

16.6 Drive letters

On this tab you can specify which drive letters will be used when a certain removable disk is connected to the computer.
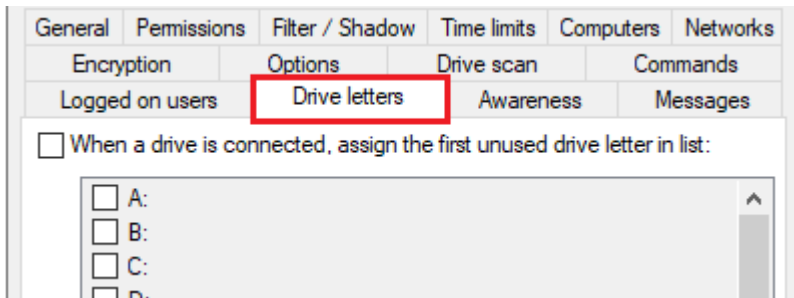
If you enable more than one letter, DriveLock Agent will automatically assign the first free letter to the drive.

> ✏️ Note: Please be sure not to conflict with drive letters already assigned (e.g. for network shares or user home directories).

16.7 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.

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.

Click here for more information on Defender Management.

16.8 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.

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.

16.9 Networks

On the **Networks** tab you can specify the active network connections the rule will apply to.
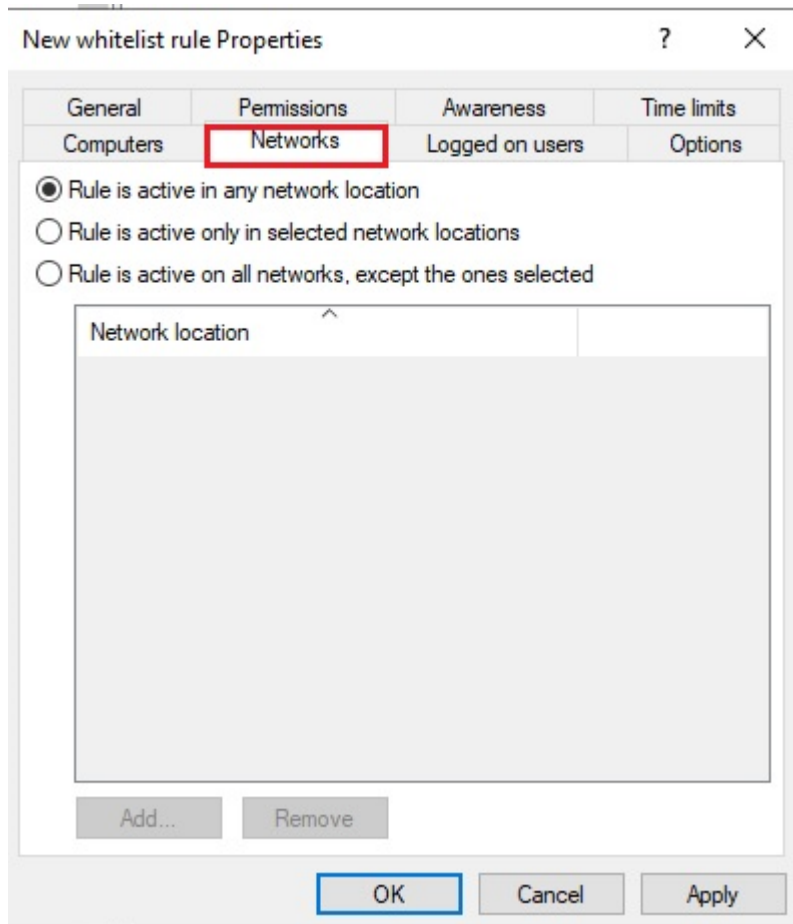
Choose one of the following options:

- 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
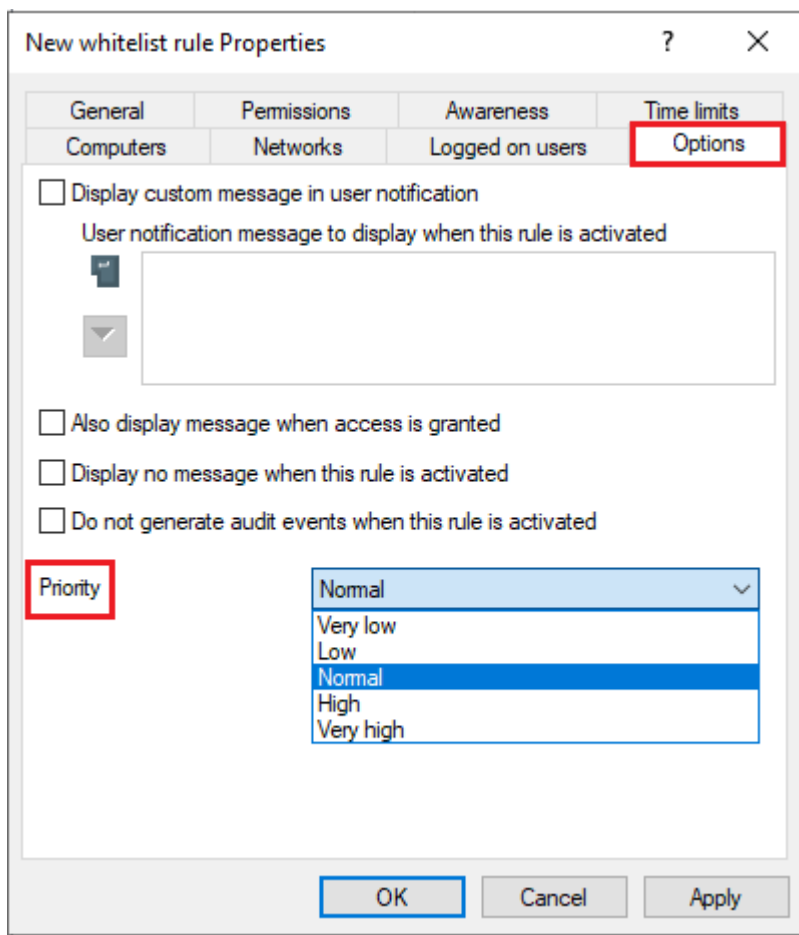
Click Add to add more network connections to the list. Remove deletes previously selected network connections from the list.

For more information on creating network profiles, click here.

16.10 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.

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 con-

figuration 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**.

The **priority** can also be set here. The default setting is normal.

16.11 Encryption

The **Encryption** tab has nothing selected by default.
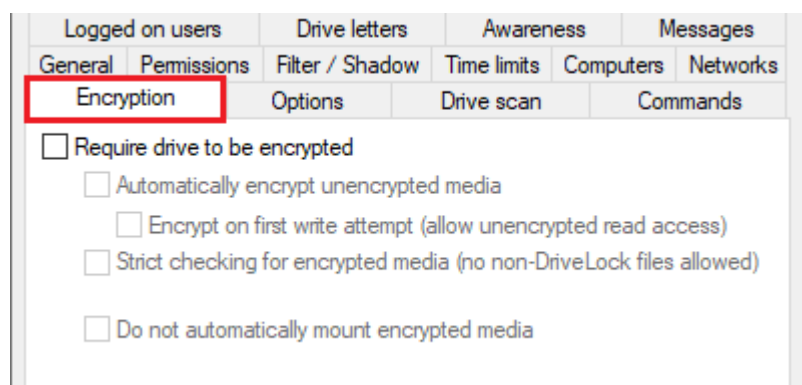
Checking **Require drive to be encrypted** ensures that a mounted drive must be encrypted in order to be used. In addition, you can specify that unencrypted drives are automatically encrypted.

> 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 con-
  tainer 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 "encryp-
ted".

You can additionally specify that already encrypted media should not be connected auto-
matically. In this case, the user can start this process manually.

Click here for more information on encryption with DriveLock.

16.12 Time limits

To ensure that a rule only applies to a very specific time period, you can specify an indi-
vidual 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.

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.

16.13 Permissions for users and groups

Select the **Permissions** tab to specify which users or groups will have access to the drive.
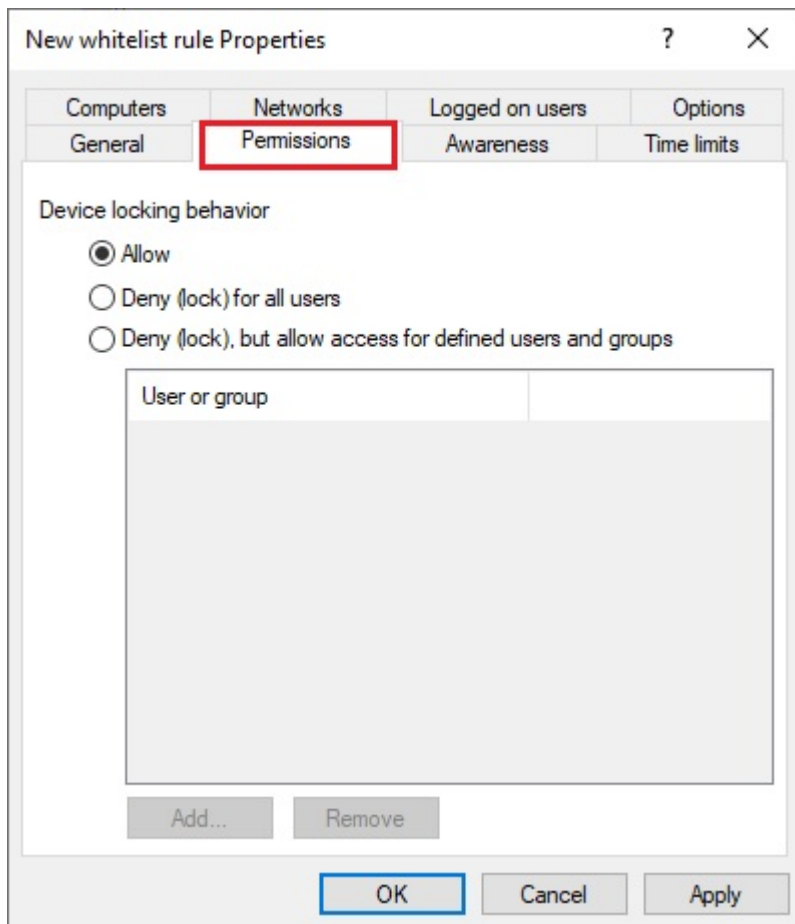
The following options are available:

- 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.

17 Encryption

DriveLock data encryption and Zero Trust security approach ensures you are always protected. With DriveLock, you can choose from a variety of encryption modules:

- **DriveLock Disk Protection**

  Transparent and fast hard disk encryption

- **DriveLock BitLocker Management**

  Hard disk encryption with Microsoft BitLocker - enhanced with important additional functions

  > 📝 Note: The DriveLock Pre-Boot Authentication (PBA) is used for both BitLocker Management and Disk Protection.

- **DriveLock BitLocker To Go**

  Encryption of removable media with Microsoft BitLocker To Go - enhanced with important additional functions

- **DriveLock Encryption 2-Go**

  Container-based encryption of removable media such as USB drives, CD/DVD or removable disks

- **DriveLock File Protection**

  File-based encryption of directories and files

17.1 License settings

To use the different encryption modules, you need different licenses. The license settings can be found in the Policy Editor under **Global configuration** or in the DriveLock Operations Center in the **Settings** menu (cog icon) under Licenses.

Click here for general information on licensing.

> ❗ Warning: It is not possible to assign the Disk Protection and BitLocker Management licenses in the same policy at the same time!

17.2 DriveLock BitLocker Management

DriveLock BitLocker Management offers you a number of advantages when compared to the usual Microsoft BitLocker solution:

- Manage encryption with BitLocker technology from a central location

- Keep track of all client computers whose hard disks are encrypted with BitLocker

- Easily integrate native BitLocker environments in DriveLock BitLocker Management

- It supports smartcard and token in addition to common BitLocker authentication methods.

- Monitor the encryption and decryption status of individual devices in the DriveLock Operations Center (DOC)

- Manage BitLocker recovery keys securely from a central location

- Quickly decommission devices when they are lost or stolen in case they are re-connected to the network

- Prevent unauthorized access in the case of decommissioned or recycled terminal equipment

- The DriveLock pre-boot authentication for BitLocker allows you to unlock the system partition via your Windows logon. This eliminates the need to enter the computer-specific BitLocker password.

17.2.1 General information

BitLocker Management helps you manage the encryption with BitLocker on client computers across your network from a central location.

Once you have licensed BitLocker Management, saved the policy, and reopened it, the new BitLocker Management sub-node appears in the corresponding policy in the **Encryption** node. Open the new subnode to specify the settings for encryption, installation and authentication and to generate the encryption certificates.

> ☑ Note: If you are using BitLocker Management for the first time, start by creating the certificates.
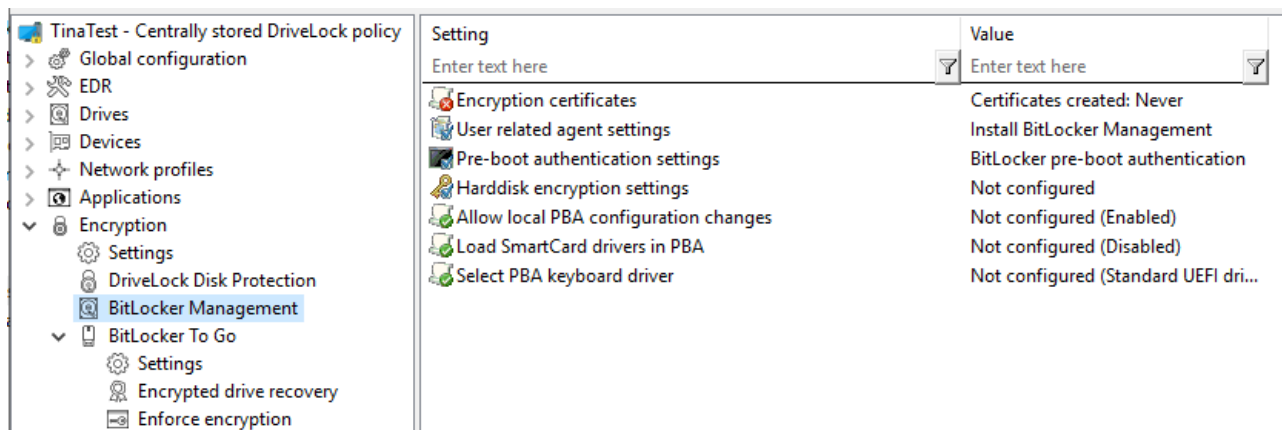
17.2.1.1 System requirements

📝 Note: For information on general system requirements (hardware and operating system requirements), see the latest Release Notes at DriveLock Online Help.

🔴 Warning: In some cases, it may be necessary to prepare the hard disk with the boot partition prior to using it with BitLocker. In this case, please perform the following steps:
Check the status using "manage-bde -status c:"
If the following error message pops up, "ERROR: The volume C: could not be opened by BitLocker. This may be because the volume does not exist, or because it is not a valid BitLocker volume." make sure to prepare the hard disk.
See https://docs.microsoft.com/de-de/windows-server/administration/windows-commands/bdehdcfg. In an admin command line, you can prepare it by using "bdehdcfg.exe -target default" or "bdehdcfg.exe -target default -restart -quiet" (without prompting for scripting)

DriveLock BitLocker Management supports the following operating systems:

- **Windows 7**

    🔴 Warning: A legacy license is required for Windows 7 starting with DriveLock version 2023.1.

    - Starting with Windows 7 SP1 (version 6.1.7601)

    - only 64 bit operating system

    - only Ultimate and Enterprise Editions

    - an existing Trusted Platform Module (TPM chip or vTPM) is mandatory

- **Windows 8**

- starting with Windows 8.1, Update 1 (version 6.3.9600)

- 32 bit and 64 bit operating systems

- only Professional and Enterprise Editions

- no TPM required (recommended for security reasons)

- **Windows 10 and higher**
  - starting with Windows 10 1607 (version 10.0.14393)

  - 32 bit and 64 bit operating systems

  - only Professional, Enterprise and Education Editions

  - no TPM required (recommended for security reasons)

> ⊕ Warning: Please note that the BitLocker feature for server operating systems is not installed by default.

DriveLock PreBoot Authentication (DriveLock PBA) for Bitlocker only supports the following operating systems:

- **Windows 10 and higher**
  - UEFI firmware required

  - 64 bit operating systems

  - only Professional, Enterprise and Education Editions

  - no TPM required (recommended for security reasons)

17.2.1.2 Algorithms for DriveLock BitLocker Management

BitLocker Management uses the following algorithms for hard disk encryption, depending on the operating system used. The methods of the relevant previous versions are also supported. See System requirements.

Operating system	Algorithm
Windows 7	• AES 128 bit with diffuser • AES 256 bit with diffuser • AES 128 bit • AES 256 bit
Windows 8.1	• AES 128 bit • AES 256 bit
Windows 10 and higher	• AES XTS 128 bit • AES XTS 256 bit

Note: The default algorithm for data drives is **AES 128** (this is the most compatible algorithm for almost all operating systems).

Note: Make sure to select the right algorithm. The above standard algorithms are the best choice in this case. When you integrate existing BitLocker environments, choosing the right one will affect how fast DriveLock can decrypt and re-encrypt the environment.

17.2.2 Policy settings

17.2.2.1 Encryption certificates

To use BitLocker Management to encrypt hard drives, you first need encryption certificates. DriveLock requires these certificates for both encryption and recovery (to provide the recovery key and for a possible emergency logon).

DriveLock automatically inserts the encryption certificates into the Windows certificate store.

> ☑ Note: It is absolutely necessary to store the encryption certificates in another secure location in the file system or on a smartcard.

BitLocker encryption certificates consist of two parts, the actual certificate (see figure below **DLBiDataRecovery.cer**) and the private key (see figure below **DLBiDataRecovery.pfx**):

DLBIDataRecovery.cer	04.12.2018 ...	Security Certificate
DLBIDataRecovery.pfx	04.12.2018 ...	Personal Information Exchange

The certificate for emergency logon consists of the following parts:

DLBIEmergencyLogon.cer	04.12.2018 ...	Security Certificate
DLBIEmergencyLogon.pfx	04.12.2018 ...	Personal Information Exchange

> ⛔ Warning: Prevent these certificates from being overwritten, as they are required for the clients' system recovery.

When you create a new policy to use for controlling BitLocker Management (BitLocker policy), always generate new certificates first. Proceed as described in chapter Creating encryption certificates for BitLocker Management.

17.2.2.1.1 Create encryption certificates

Please do the following:

1. When you are finished creating the BitLocker policy and licensing BitLocker Management, save and reopen the policy. Only then you will see the BitLocker Management sub-node.

> ☑ Note: A text message indicates that no encryption certificates have been gen-
> erated yet:

2. Click the **Encryption certificates** option or open the link in the text message.

3. In the Encryption certificate Properties dialog, select the **Generate certificates** but-
ton.

   You can import any existing certificates by clicking the **Manage certificates** button. If
   you do so, make sure that you do not overwrite any existing certificates because oth-
   erwise recovery will be impossible.

4. Follow the wizard and specify a **certificate backup location**. This can either be a
   folder in the file system or a smart card.
   If a smartcard is used for storage, you will be prompted to enter the PIN for accessing
   the smartcard.
   The option **Also save certificate in the database (for use in DOC)** is set by default
   so that you can access the certificates from DriveLock Operations Center (DOC).

   > ☑ Note: Please make sure that the appropriate security requirements regarding
   > storage location and access are met.

5. In the next step, define the passwords for the private keys (see figure).

   > ☑ Note: In this dialog, you specify the password for both the emergency logon
   > certificate and the recovery certificate.

6. Next, DriveLock generates the encryption certificates in the location you specified.

17.2.2.2 User-related agent settings

By default, DriveLock Agent users are informed about the installation of the DriveLock PBA and their client computer is restarted after 30 seconds after the installation of the DriveLock PBA. You can change these settings if necessary.
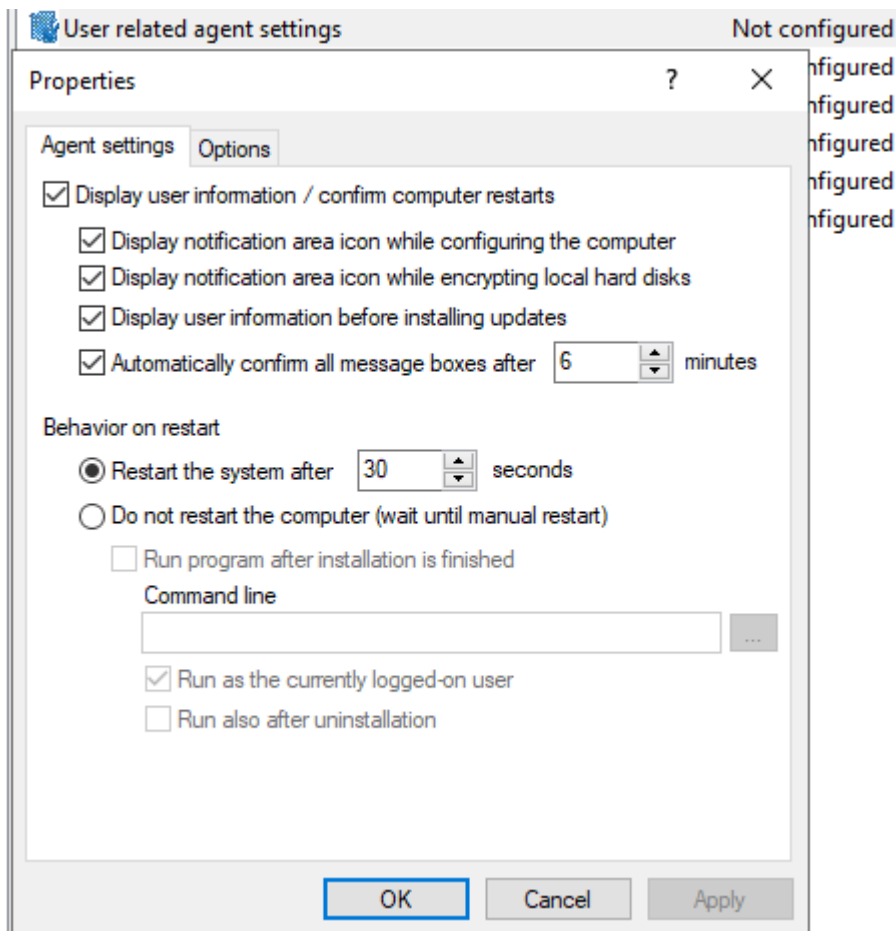
Agent settings tab

On this tab you can decide whether notifications are displayed or not, and you can also choose when they appear in the notification area: during configuration, during encryption and/or before installing updates.

Select the **Do not restart computer (wait until manual restart)** option if you want to control it yourself. This allows you to start your own installation script, for example, with a shell command after the installation.

Two options are available:

- **Run as the currently logged on user**: The script runs with the rights of the user who is currently logged on. Normally it would run under the local system account.

- **Run also after uninstall**: The script runs during installation and uninstallation.

Options tab

Show BitLocker Management logon messages: Select this option if you want the pre-boot authentication information to appear in the notification area of the client computer after logon to Windows.

A message with detailed information will appear on the client computer (see figure):
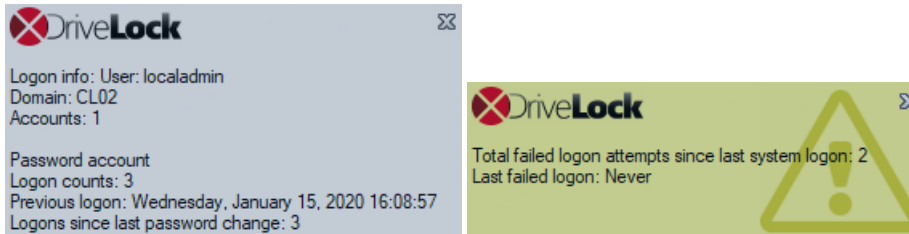
17.2.2.3 Hard disk encryption settings

17.2.2.3.1 The General tab

On this tab you set the values for encryption and decryption with BitLocker.
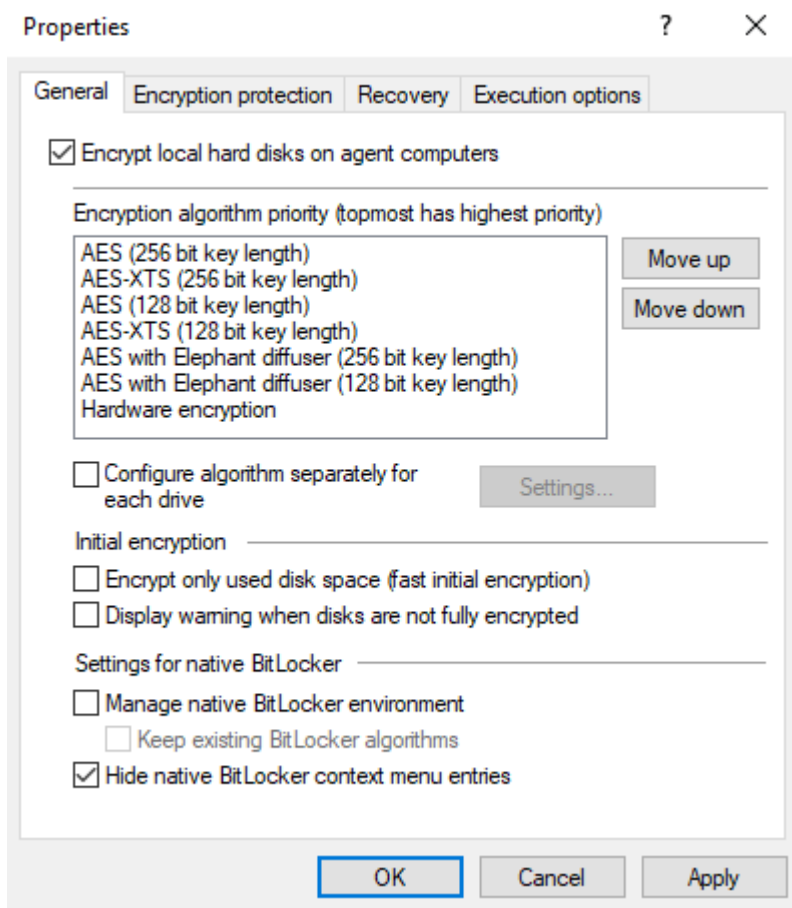
The following options are available:

1. **Encrypt local hard disks on Agent computers**:
    *   Select this option to start the **encryption** of the hard disks with BitLocker. Before you do so, check that all other encryption settings (see below) are specified.

        > ⊘ Warning: As soon as you check this option and the policy has been assigned and updated on the client, the encryption process starts!

    *   To allow **decryption** (see detailed description in the decryption topic), uncheck the option and, if necessary, specify a delay in days.

> ⚠️ Warning: The decryption process starts as soon as you disable the option and no delay is specified (and the policy is assigned and synchronized by the client).

2. **Encryption algorithm priority**:
   - The list of the different encryption methods is processed from top to bottom. Once BitLocker Management finds a suitable algorithm that can be applied to the client, it will use it for encryption.

     > ✏️ Note: We recommend placing the strongest algorithm at top level.

   - You can also sort the algorithms manually according to your requirements.

   - Hardware encryption algorithm:
     This is a special algorithm some producers build in to their hard disks. If you want to use this algorithm, please move it to the top of the list.

   - Example:
     You may want to move the **AES with Elephant diffuser (128 or 256 bit key length)** entry up if you have many computers with Windows 7 systems to encrypt, so that this algorithm is preferred.

3. **Configure algorithm separately for each drive**:
   - Select the required encryption algorithm for the system drive and the data drives by clicking the **Settings** button or choose 'Not encrypted' if no encryption is required.

   > ✏️ Note: Please ensure that the drive letter and system partition assignment is the same for all computers this BitLocker policy is assigned to.
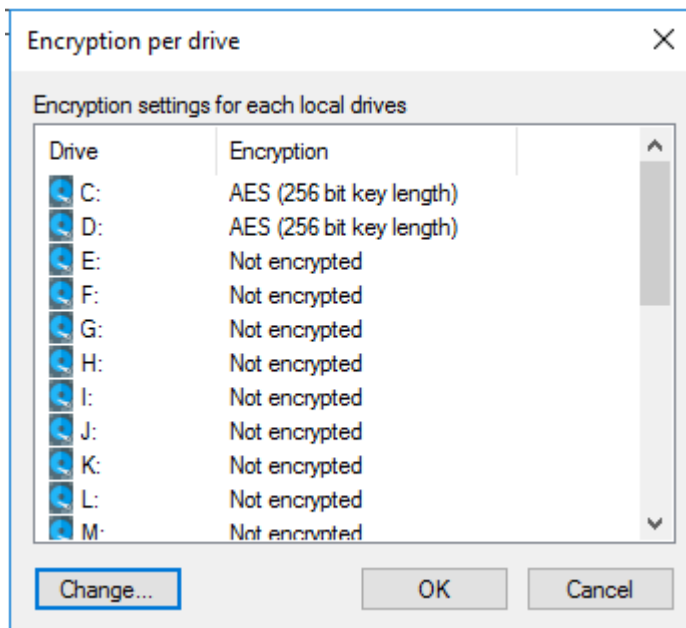
If you select the **Do not change encryption status** option, either the already existing algorithm will continue to be used or the drive will remain decrypted.

4. **Initial encryption**
   - **Encrypt only used disk space (fast initial encryption)**
     - Select this option if you want to encrypt only the used disk space.

     - Background:
       With Windows 8, BitLocker introduced a feature that the hard disk does not have to be fully encrypted, but only the part where data is stored. Encryption is much faster for this reason.

     - Issue:
       Data that has been deleted from the hard disk and that is no longer visible in the Explorer may actually still exist and the original data can be accessed with special tools.

       > Note: We recommend that you only enable this option if you want to encrypt new hard disks, for example. Make sure that there is no old sensitive data on the hard disk. Likewise, this option is recommended for all SSDs.

   - **Display warning when disks are not fully encrypted**
     Each time the system is rebooted or the DriveLock Agent is restarted, the system checks whether all hard disks are already fully encrypted according to the settings. If this is not the case, the user is notified accordingly.

5. **Settings for native BitLocker**
   - **Manage native BitLocker environment**
   Select this option if you want to manage existing (native) BitLocker environments with DriveLock BitLocker Management. Please refer to chapter Integrating existing BitLocker environments for more information.

   > ☑ Note: Once you select this option and assign the policy accordingly, a wizard opens on the client computers with native BitLocker-encrypted (and thus locked) data drives; this wizard prompts the user to take over the drives. This is where you must provide the passwords for the locked partitions before they can be taken over.

   - **Keep existing BitLocker algorithms**
   Partitions that are already encrypted with BitLocker but do not match the algorithm defined in the policy retain the existing algorithm. Re-encryption is no longer necessary with this option.

   - **Hide native BitLocker context menu entries**
   This option is enabled by default. It hides all BitLocker options in the Windows Start menu or in the Explorer so that the native BitLocker dialogs are not displayed. This limits the chance of accidentally encrypting a hard disk or a drive with BitLocker but without DriveLock.

17.2.2.3.2 The Encryption protection tab

1. **Encrypt only if pre-boot logon succeeded at least once**
   This is a preventive measure that keeps encryption separate from the initial logon to the PBA. Encryption is delayed until the first logon is successful.

2. **Response to configuration changes**
   - **Delay decryption by [x] days**:
   This setting delays the decryption for the specified number of days. This may be useful so that the client computers and their users can be properly prepared for decryption.
   The default value is **3** days. This value provides additional protection against misconfiguration. If you want to perform decryption immediately, change the setting to 0 days.

   - **Do not decrypt**:
   This option is enabled by default. Its purpose is to prevent unintentional decryption of BitLocker encryption when the configuration is changed, for example,

after DriveLock Agent updates, if group memberships are changed, or if the policy is no longer used by the DriveLock Agent.

> ⚠️ Warning: Note that decryption is triggered only by disabling the **Encrypt local disks on agent computers** option described above. Decryption starts once the DriveLock Agent receives the configured policy with the mandatory decryption setting.

17.2.2.3.3 The Recovery tab

On this tab you specify where the encrypted recovery data should be stored. These are the settings you need when you start the recovery process.

The following options are available:

Recovery key rotation

Use the **Maximum BitLocker recovery key age** in days setting to define the period for regular key rotation. This option ensures that the recovery key is replaced regularly. This prevents misuse of the recovery key. Here, the specification '1 day' refers to 24 hours. The recovery key is uploaded to DES immediately after the swap.

DriveLock Enterprise Service:

Select this option if you want to send the encrypted recovery data to the DriveLock Enterprise Service (DES).

File server (UNC path)

If you select this option, your encrypted recovery data is stored on a server, for example. When you select this option, you can specify a user name and password under the **Log in to file server** option.

Local folder on Agent computers (not recommended)

We recommend this option only if you store the key files on a secure storage medium (e.g. USB device) or move them to a secure location later.

17.2.2.3.4 The Execution options tab

You can select options for starting and delaying encryption, and for forced encryption on this tab.

You can configure whether BitLocker encryption on the DriveLock Agent should start depending on certain events, or whether the user can delay the encryption. The objective is to disturb the user as little as possible and to keep the computer performance constant without compromising the protection provided by the encryption.

You can only select the **Start enforced encryption after x hours** option if you have selected the BitLocker PBA in the Pre-boot authentication settings and specified a password there. If the user has not assigned their own password by the time the specified time expires, encryption will be performed using the specified password. The counting starts the moment when the password dialog is displayed for the first time.

With the **Encrypt hard disk independently of user interaction (only possible if TPM is enabled)**, you can ensure that an agent's hard disk is encrypted even if the user has not yet logged on to the DriveLock PBA or has not yet entered a password for the BitLocker PBA. This option is only effective if TPM is active on this system.

With the **Start encryption only in the following events:** option you can specify conditions when encryption may start. For example, if you want to specify that encryption should start only on a client computer if no users are logged in, check the option as illustrated in the figure below:

> **Note:** When selecting the option **when no application is running in full screen mode**, make sure that the application is actually running in full screen mode and not just maximized. This option is particularly important when running CAD/CAM applications, for example.

In the lower section, you specify the maximum number of hours users are allowed to delay encryption. A value of up to 9000 hrs. is possible here. You also specify how long the delay notification is displayed to the user. Once this time has expired and the user has taken no action on their client computer, the encryption will start automatically. The same applies if no user is logged in.

> 📝 Note: As soon as the user receives the delay notification, encryption will start and the protectors will be created automatically. Immediately after that, encryption is paused and then resumes once the user clicks Encrypt in the notification or the delay time expires (without user interaction). Then encryption continues. The system is already secure at that point and the user must already provide a password (or PIN in the case of TPM) when rebooting.

17.2.2.4 Pre-boot authentication settings

17.2.2.4.1 Authentication type

Your choice of pre-boot authentication type (PBA) differs depending on whether the computers whose hard disks you want to encrypt contain a Trusted Platform Module (TPM) or not.

In the example below, the BitLocker pre-boot authentication is explicitly used. For information about DriveLock pre-boot authentication for BitLocker, refer to the corresponding chapter.

The following options are available on the **Authentication type** tab:
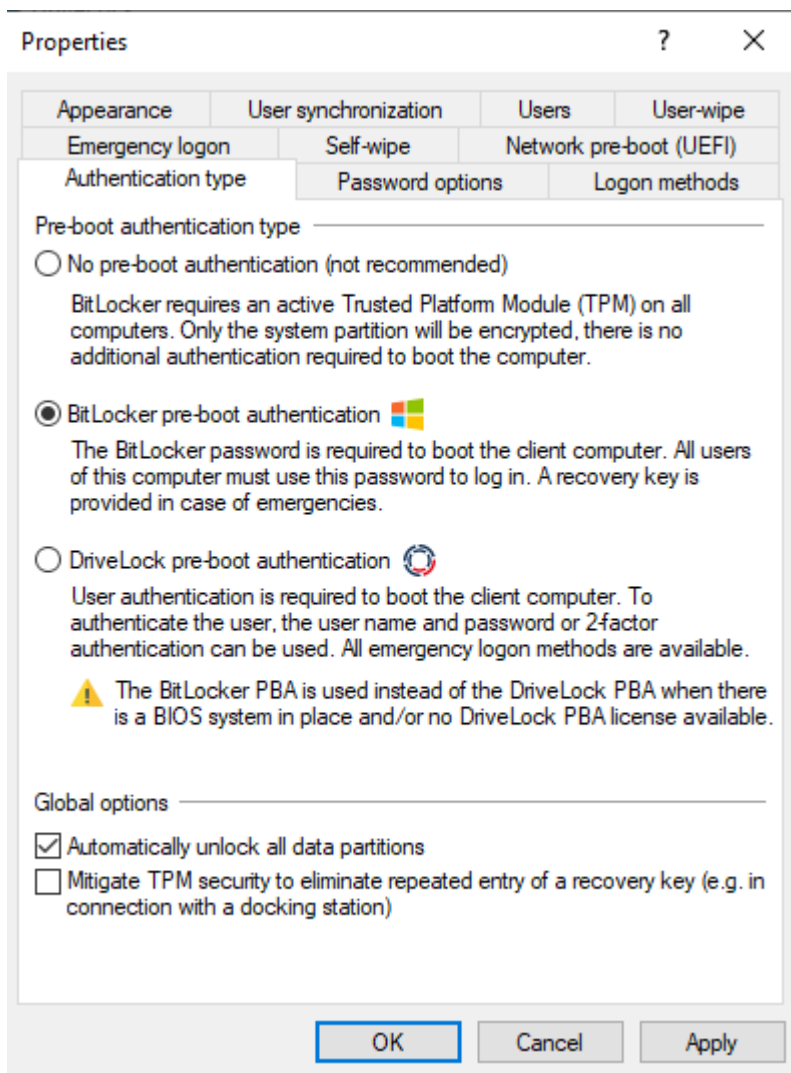
1. Select the first option **No pre-boot authentication (not recommended)**,
     - if there is a TPM built in on the hard disks you want to encrypt. In this case, an additional authentication when booting the computer is not required.

> ✎ Note: The protector DriveLock uses is called **TPM only**.

- Here, BitLocker accesses a TPM which has to be activated first in BIOS.
- If you chose this option, you can close the dialog and continue because you do not need to specify a password on the next tab.

> ⊘ Warning: This option is not recommended because there is a risk of bypassing the encryption of the system partition.

2. Select the second option **BitLocker pre-boot authentication** (see figure),
   - if there is no TPM built in on the hard disks you want to encrypt or if you are not sure whether it is active.
   - In this case, DriveLock uses the original Windows BitLocker PBA.
   - Open the **Password options** tab to assign a password or select one of the other options.

> ✎ Note: The options on this tab are only available if you have selected **BitLocker pre-boot authentication**as the **authentication type**.
> The other tabs are inactive because the corresponding options refer exclusively to the **DriveLock pre-boot authentication** type.

3. In both cases, we recommend checking the **Automatically unlock all data partitions** check box. With this option set, both the system partition and all data partitions are unlocked after authentication on the computers you assign the BitLocker policy to.

> ✎ Note: Unlike Microsoft, DriveLock unlocks the data partitions automatically for all users of a computer. The unlocking process by DriveLock BitLocker Management is independent of the Windows BitLocker function, which means that the call `manage-bde -status` still returns "`Automatic Unlock: Disabled`" for drives unlocked by DriveLock.

4. The **TPM** platform validation can be modfied with the **Mitigate TPM security ...** option. The option is useful, for example, when BitLocker-encrypted laptops keep requesting the recovery key as soon as the laptop is not connected to the docking station. The new option affects any pre-boot authentication type, as DriveLock uses TPM-based protection mechanisms as soon as TPM is available (TPM only, TPM/PIN, TPM/StartupKey). The option is disabled by default.

17.2.2.4.1.1 Option: DriveLock pre-boot authentication

Open the **Pre-boot authentication settings** and first select the **DriveLock pre-boot authentication** option on the **Authentication type** tab.

> 🗒 Note: If this option is not available, verify that the DriveLock PBA option is correctly licensed and that you saved and reopened the policy after activating the license option.
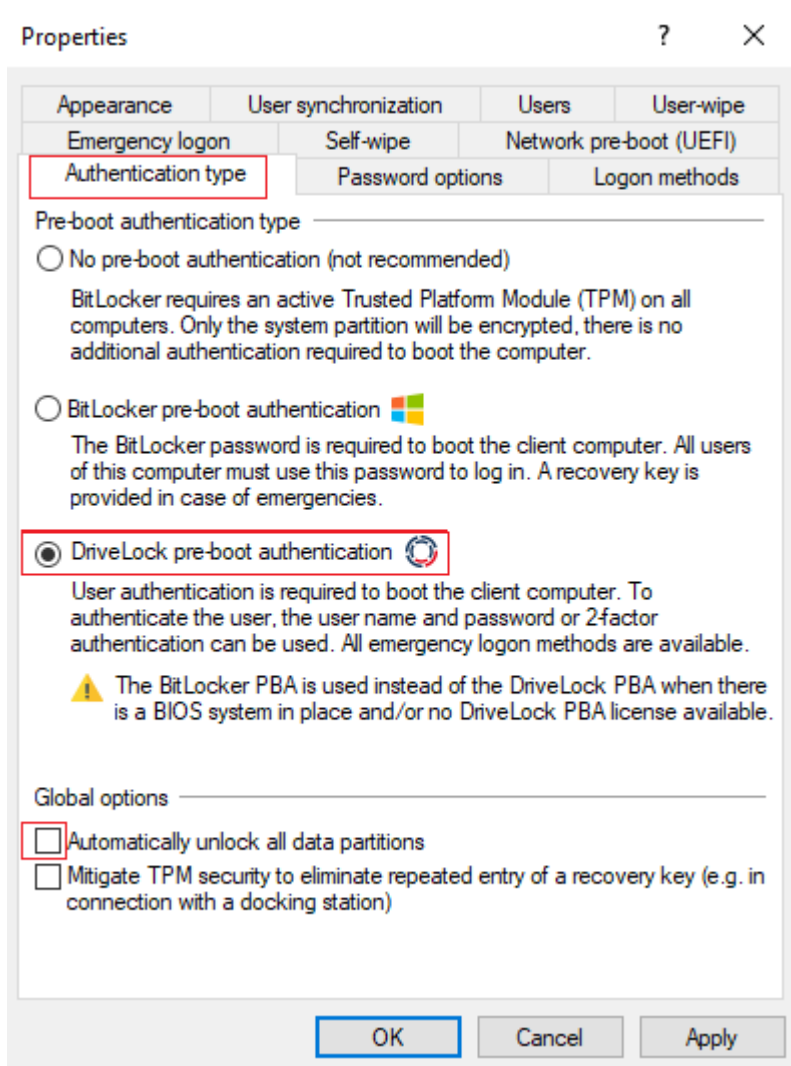
> ⚠ Warning: This option is only available for computers running Windows 10 and higher and UEFI firmware. We do not support server systems, older systems or systems with legacy BIOS.

Please note the following:

- If the client computer does not meet the requirements, the **BitLocker pre-boot authentication** option is automatically used.

- The **Automatically unlock all data partitions** option has no effect on DriveLock pre-boot authentication because data drives are generally unlocked automatically.

You cannot select any options on the **Password options** tab. If you want to configure settings on this tab (e.g., for computers where DriveLock pre-boot authentication cannot be used), you must temporarily enable the **BitLocker pre-boot authentication** option.

17.2.2.4.2 Password options

On the **Password Options** tab you have the following options:

Warning: Please note that this password setting applies to the end user only.

1. You specify a **BitLocker password** and select none of the other options in the in the top part of the dialog:
   - The encryption process starts when you activate it and/or assign the policy. The user of the client computer is allowed to change the password later or continues to use the password you specified.

   > Note: Please note that you are responsible for communicating the password to the users over a secure channel.

2. You check the **User cannot change password** box:
   - Please specify a fixed password which the user can never change. The initial encryption process starts automatically even without the user being logged on to the client computer, after you activate it and/or assign the policy.

   - As soon as the user starts the computer, the BitLocker password must be entered to unlock the encrypted hard disks.

   > Note: Please provide users with the appropriate password information over a secure channel.

   - The password is entered independently of the encryption progress, i.e. as soon as encryption is started, the BitLocker password must be entered in the PBA.

3. Check the **User must specify the password for encryption** option (see figure):
   - The user can specify a password, you do not enter a password here.

   > Note: In order for encryption to start at all, users must enter the password.

   - If required, you can define the requirements the user password must meet.

   - The encryption process starts as soon as the user specifies the password.

   - The password may be changed later.

   - With the **Maximum password age** setting, you specify the number of days after which the end user must change the password again.

   - Use the **Reject the 'x' last used passwords** setting to specify that a certain number of passwords which were used last are no longer permitted. In the example above, the last 2 passwords used are rejected.

Use the options below **Password must meet the following requirements** to specify the exact criteria that a password assigned by the user must meet. The option is selected by default.

1. You can select the **Allow numbers only** option if all client computers are equipped with a TPM which means that 6 characters are allowed.

   > ⚠️ Warning: If there is no TPM on client computers or non-system partitions need to be encrypted as well, the default is still at least 8 characters. (Microsoft default for passwords on data partitions).

2. The **Allow numbers and Latin based characters** option restricts the usage of allowed characters. Special characters can no longer be used with this setting. Please note the information in the BitLocker pre-boot authentication chapter.

3. With the **A valid password must contain at least...** options you define the number of letters, numbers and special characters:
   - The password must be between 8 and 20 characters long. A number below 8 or higher than 20 leads to an error message.
   - Define the minimum requirements (number of letters, number, special characters etc.).
   - If you select the **Treat numbers as special characters** option, numbers count as numbers and also as special characters. Please make sure that the numbers and special characters correspond.

4. The **Dictionary file** option allows you to select a dictionary in which you have set passwords that must not be used. The dictionary file must have been previously created in the file storage. When a password is assigned, this file gets checked and the password is allowed or rejected accordingly.
   In the figure above, the *blacklist4.txt file is used as the dictionary file.

   > 📝 Note: Note that passwords are also denied if there is any part of the password in the dictionary (for example: if the dictionary contains "it", passwords such as "hit", "kitten" or "favorite" are not allowed).

17.2.2.4.3 Logon methods

The following options are available on this tab:

Select the **Enable Single Sign-on for Windows** option to require only a single logon to the client computer. The Windows login screen will no longer appear.

The following authentication methods are available:

- **Local user access**: This option is enabled by default. This method allows local Windows users to authenticate to the system using their local Windows username, password, and local system name.

- **Domain user access (with password)**: This method allows Windows domain users to authenticate to the system using their Windows domain username, password and domain name.

  🛑 Warning: Users can only log on to the domain if the Windows and Pre-Boot options have been set.

- **Domain user access (with token)**: This method allows Windows domain users to authenticate themselves with a smartcard / token and PIN.

Enable logon using password tokens: This method allows the pre-boot authentication for a password token user. If you check this option, then you need to select at least one more Windows authentication.

🛑 Warning: Prior to configuring the DriveLock PBA for token access only, make sure that a valid token exists for both the PBA and the Windows logon (unlock).

Other options in the dialog:

- The **Maximum number of logins before lockout** option causes a user to be locked for a certain period of time after the specified number of failed logins to protect the system from a brute force attack with automatic logon scripts. Change the default values according to your corporate security policies.

- If you are using certificates for authentication, you can specify the number of days after which DriveLock alerts users before certificates expire.

- The **Count failed logons globally for all users** option is enabled by default. Instead of counting up failed attempts for a single user, the failed attempts counter is incremented independently of users.

- With the **Disable pre-boot authentication until first Windows logon** option, the PBA is deactivated until the first user has logged on to Windows. It is used to avoid

that only users whose names have been entered on the Users tab in the pre-boot authentication users option may log in. Thus, without a valid Windows logon beforehand, the users specified in the policy are ignored.

17.2.2.4.4 Appearance

On this tab you can define how the DriveLock PBA is displayed to users on their client computers.

- There are several **background images** to chose from. Choose one of them.
- You can also select your own **custom background image** by selecting one from the file system or the policy file storage.
- The **Show password** option allows the user to briefly view the entered password in plain text.
- If required, you can enter your own display test in the text box below the **Show pre-boot user information message** option.

17.2.3 Decryption

Decryption is triggered with a single setting, which is set in the **Hard disk encryption settings** on the **General** tab.

You can monitor the decryption process, just like the encryption process, in the DriveLock Operations Center (DOC).

The event report (BitLocker Events) also contains information about the decryption of individual computers.

17.2.3.1 Decrypting encrypted drives

To start decrypting encrypted drives, proceed as follows:

1. Open the respective BitLocker policy.

2. Open the **Hard disk encryption settings** dialog and go to the **General** tab.

3. Uncheck the **Encrypt local hard disks on Agent computers** option.
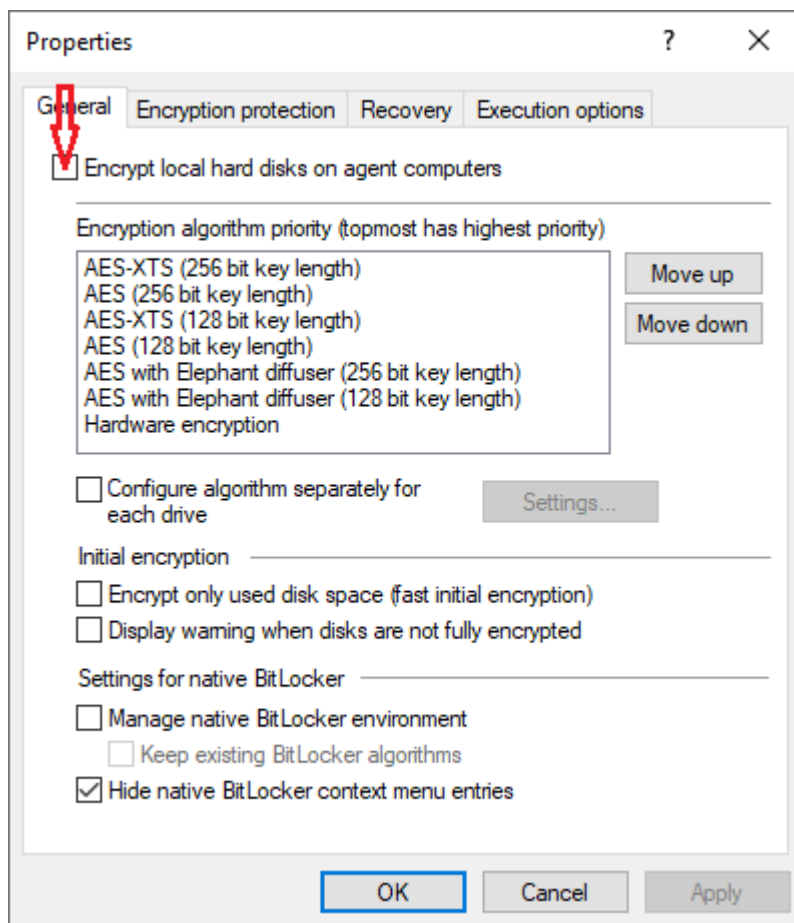
4. On the **Encryption protection** tab, set a value for the **Delay decryption by *x*** days setting. The default value is **3**, which means that decryption starts after 3 days. Depending on the value, decryption is delayed by x days .

> 📝 Note: In order to start the encryption process immediately, enter the value **0** here.

5. **Do not decrypt** is the default setting, which is intended to prevent unwanted decryption. It is deactivated as soon as you enter a value for the delay.

6. Click **OK** to confirm your settings.

7. The following message appears in the status bar of the client computer that is being decrypted.
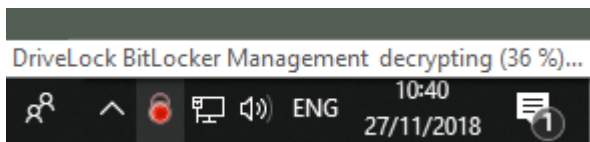
17.2.4 Override policy settings (BitLocker)

To disable specific encryption settings on individual client computers, you can override the respective policy settings.

> ⚠️ Warning: Note that the policy settings will not be re-enabled until you undo the reconfiguration.

Please do the following:

1. Open the **Agent remote control** in the **Operating** node of the DriveLock Management Console.

2. Select the DriveLock Agent you want to change the policy settings for.

3. From the context menu, select the menu item **Disk encryption properties...**.

> 📝 Note: Please note that a connection between DES and DriveLock Agent must exist to display the encryption properties.

4. On the **General** tab you can see information about DriveLock Agent encryption. Click the **Reconfigure agent...** button.

5. If you select the **Override policy settings** option and keep the **Override general deployment settings** option checked (default), the DriveLock Agent will be decrypted immediately and BitLocker will be disabled (see figure below).
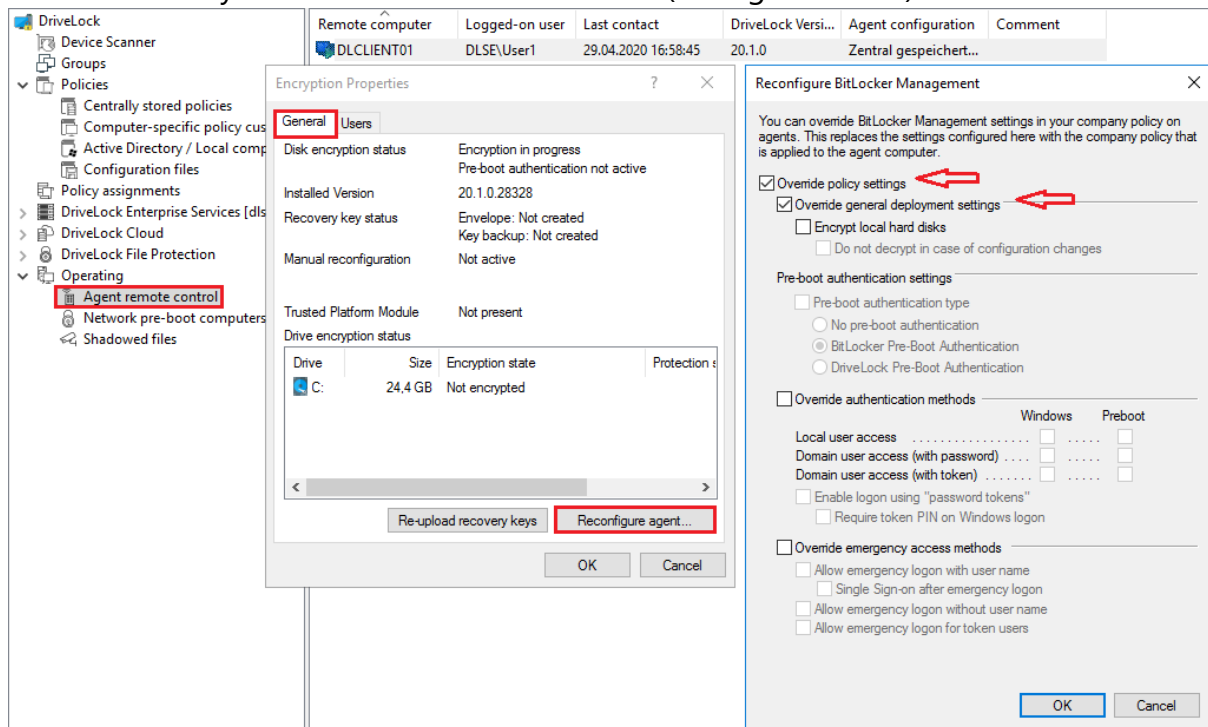
6. By setting the **Encrypt local hard drives** option, the encryption settings from the policy (e.g. algorithm or fast encryption) are taken over.

7. If you select the option **Do not decrypt on configuration changes**, the corresponding policy option (Do not perform decryption) is overwritten.

8. If you click **OK** now, your settings will be applied to the selected client computer with immediate effect.

17.2.5 Sample configuration

Please find below a sample configuration for encryption involving the user entering a password on the client computer.

To quickly and easily encrypt the drives on your client computers, follow the instructions below in the specified order.

This sample process starts with licensing DriveLock BitLocker Management and ends with encrypting the hard drives on the client computers.

> 📝 Note: For more information on the individual steps, see the cross-references.

1. Create a new policy or use an existing one.
   In this document, the policy is referred to as the 'BitLocker Policy'.

2. Enter the appropriate licenses in the policy and license all computers.

3. In the policy, open the **Encryption** node and select **Hard disk encryption** in the **BitLocker Management** sub-node. Read more here.

4. First, create the encryption certificates.

5. Open the Deployment settings and specify the notifications you want the user to get.

6. Next, specify the Pre-boot authentication settings.
   - On the **Authentication type** tab, select **BitLocker pre-boot authentication**. Check the **Automatically unlock all data partitions** box.
   - On the **Password options** tab, select the **User must change password** option and specify the complexity requirements you want for the password.

   Apply your changes by clicking **OK**.

7. Specify the following in the Hard disk encryption settings:
   - Open the **General** tab.
     1. First of all, check the **Encrypt local hard disks on Agent computers** option.
     2. Then set the entry **AES-XTS (256 bit key length)** to the highest position in the encryption algorithm priority.
     3. Optionally check the **Configure encryption settings per drive** box and select the encryption algorithm mentioned above for the drives C: and the

> expected data drives via the **Settings** button. You can also specify **Not encrypted** if you do not require encryption.

4. Click **OK** to close the dialog.

5. In the Initial encryption section, check the **Encrypt only used disk space (fast initial encryption)** option; in the Initial protection section, select '**0**' for the number of days the decryption will be delayed.

- Next, open the **Recovery** tab and select the first option **DriveLock Enterprise Service**.

Click **OK** to close the dialog.

8. Save and publish the policy.

9. Your settings will be activated the next time the client computer's configuration is updated.

10. Depending on the setting, the hard disk encryption is executed immediately on the client computers or after the user enters the password.

17.2.6 Recovery

17.2.6.1 Recovering encrypted hard disks

If users can no longer access their hard disk (system partition) encrypted with DriveLock BitLocker Management, for example because they have forgotten their BitLocker password, the recovery certificate and the associated private key must be used to provide access.

> Note: The upload of the recovery data starts when all drives that are needed for encryption have begun encrypting.

In this case, you need to start the recovery process. For this purpose, DriveLock offers you two possibilities:

1. To start the recovery process in the **DriveLock Operations Center**, select the appropriate **computer** from the Computers view. Open the context menu and select the **BitLocker** submenu and then **Show recovery key**.
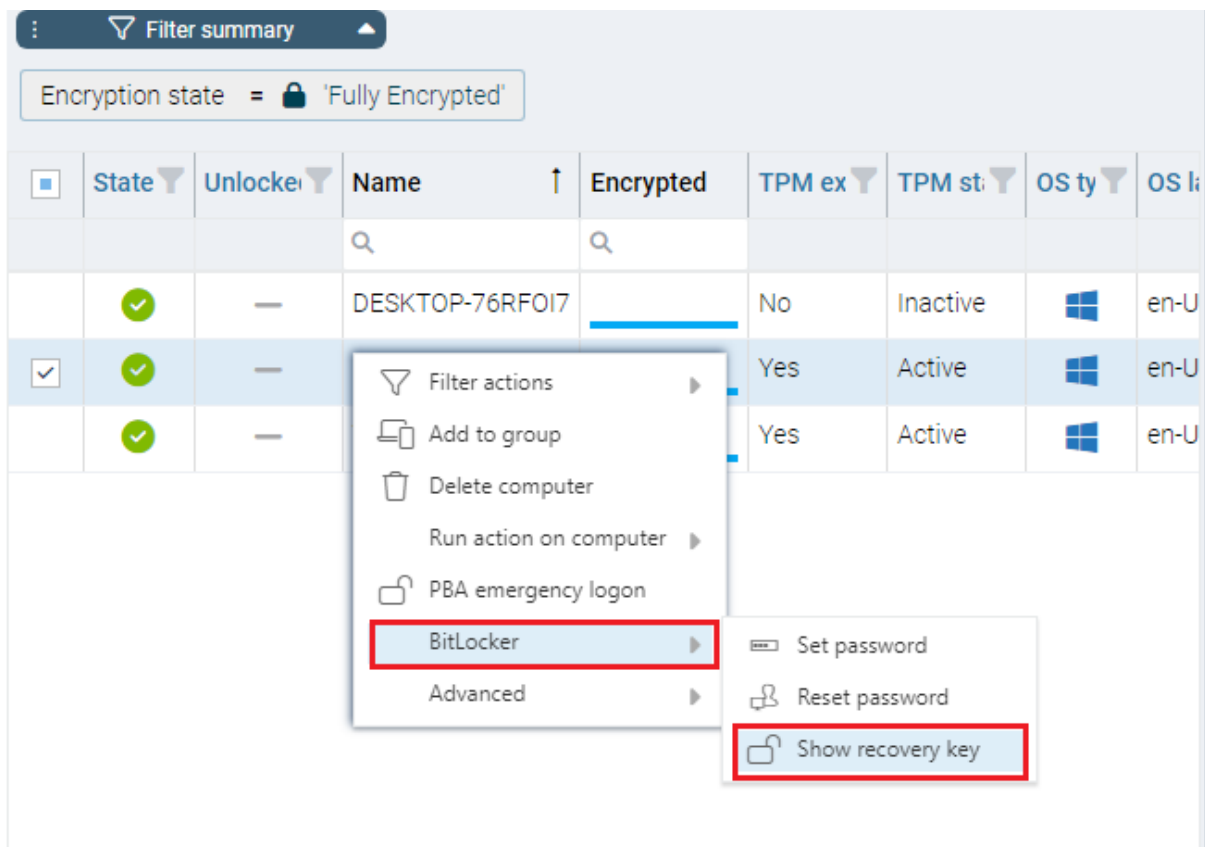
2. To start the recovery process in the **DriveLock Management Console**, select the **Operation** node, then open the context menu of the **Agent remote control**, and then select the **BitLocker Recovery** menu item (see figure).
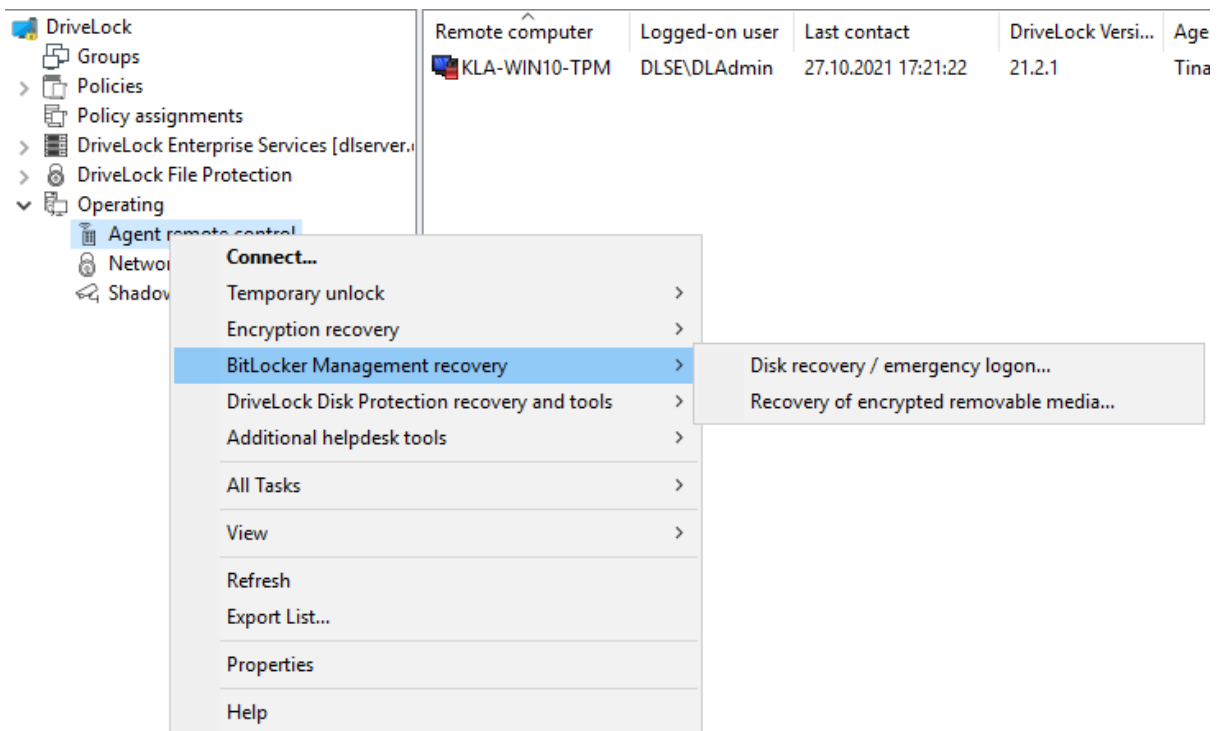
Here, the recovery wizard opens and guides you through the respective steps.

17.2.6.1.1 How to unlock BitLocker-encrypted data partitions

Data partitions that were previously used in other computers and that were also managed with DriveLock cannot be unlocked automatically. There are two ways to unlock them using the `blunlockdatadrives` command line parameter: with an API key or by entering user name and password.

- When entering a user name and password, the call syntax is:

```
DriveLock -blunlockdatadrives -user:JohnDoe@company.com -password:
"mypassword &%"
```

In this example, the user "JohnDoe" must have appropriate permissions, which are set in the DriveLock Operations Center in the Permissions/Role Assignments section. The role **Display recovery key** must be assigned.

- The syntax when using an API key is:

```
DriveLock -blunlockdatadrives -password: "Acne-
fi6C+mxjDM/1AZb76vH9zuh17WFd2EnigJODrDDdA+Sy3V3V512kPKWWivrhMA=="
```

As an example, the following API key was created in the DOC: `Acne-fi6C+mxjDM/1AZb76vH9zuh17WFd2EnigJODrDDdA+Sy3V3V512kPKWWivrhMA==`. This can now be used as a substitute for user name/password.

Click here for more information on creating an API key.

17.2.6.2 Procedure in the Policy Editor

To recover access to an encrypted drive, Please do the following:

1. Open the Recovery Wizard (either from the DriveLock Operations Center or the DriveLock Management Console).

2. In the first dialog, select the **BitLocker recovery key** option.
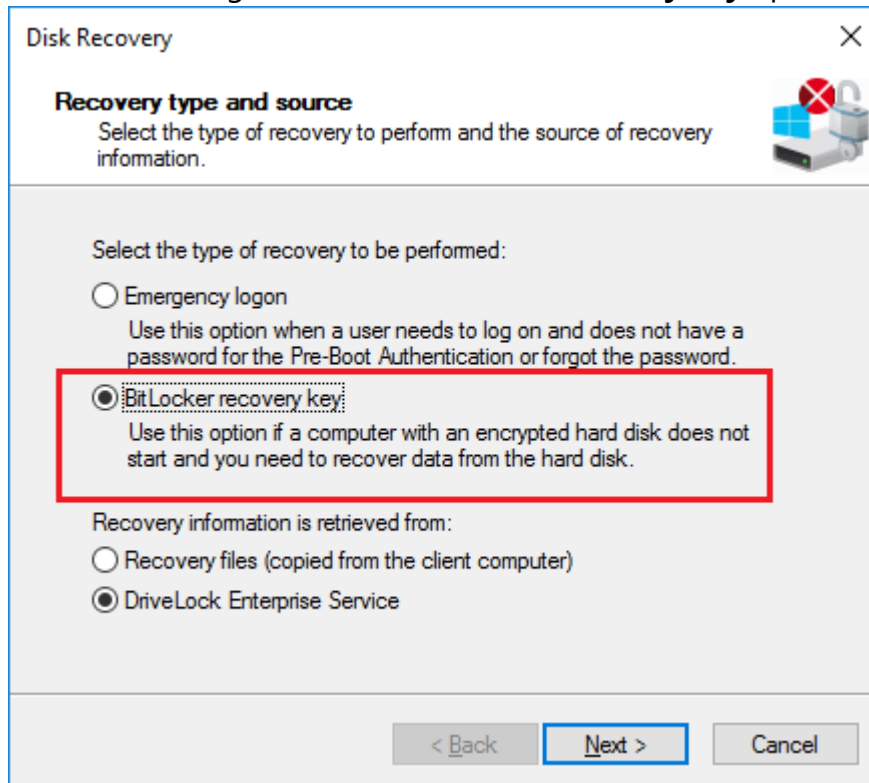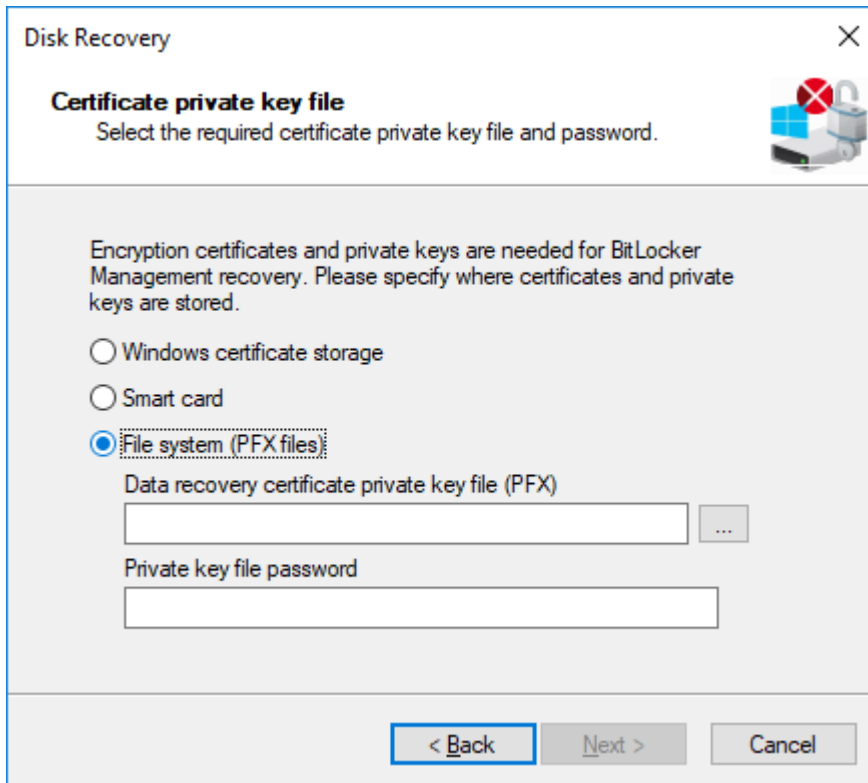
> ☑ Note: For information on **emergency logon** to the DriveLock PBA, refer to the corresponding chapter.

Select where the **recovery information is retrieved from:**.

> ☑ Note: Which option you select, depends on your settings in the encryption settings dialog. We recommend the DriveLock Enterprise Service option.

3. In the next dialog, select the location of the certificate and/or private key (*.PFX file).

You can also access the information stored in the **Windows Certificate Store**.

> Note: If you specified earlier in the encryption settings dialog that the recovery information resides in the file system, please enter the matching password for the private key here.

4. Next, select the client computer that needs recovery from the list. Use a filter, if required.

5. Continue by requesting a recovery key in the next dialog.

6. Wait a moment while DriveLock retrieves the recovery information.

7. The next dialog issues the recovery key.

> Note: Select the drive defined as system partition on the client computer.

Disk Recovery

Creating recovery information...
Creating recovery information...

The recovery data was retrieved successfully.
Please forward the data retrieved to the end user or use the key directly.

Drive to be recovered: C

Recovery key
304117-478742-036190-637087-061743-
423313-076505-639540

< Back   Finish   Cancel
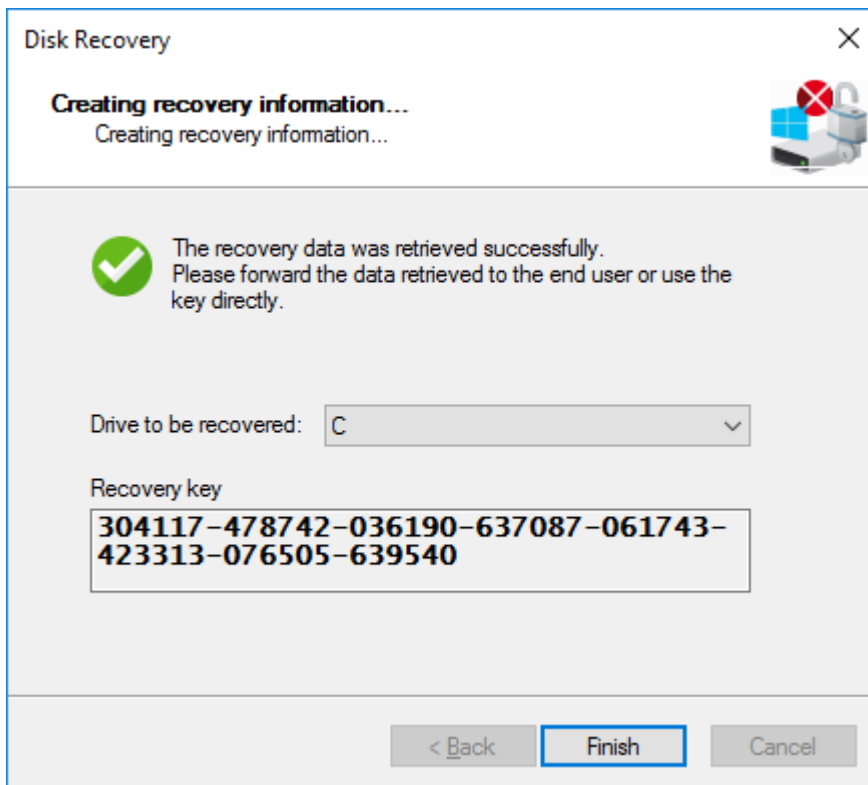
8. Now tell the user the recovery key.

> Note: Please note that you are responsible for communicating the recovery key to the users over a secure channel.

9. Last, the user enters this key in the **BitLocker recovery** dialog when starting the client computer.

> **Note:** Note that this recovery key represents a major security risk. For this reason, BitLocker Management initiates a password change on the user side and replaces the recovery key with a new one.

10. The Change BitLocker Password wizard starts on the client computer and the user must specify a new password.

11. As soon as this is done, the user can enter this password when starting up the client computer.

17.2.6.3 Procedure in the DOC

If recovery data is available, a wizard opens where you first select the certificate or certificate file. If several data sets are available, you can also select the corresponding one by date here.

You can find more information about certificates here. Once the recovery key is displayed, proceed as described from step 8.

17.2.6.3.1 Recovery with key ID

Recovery using challenge/response is possible even if no DriveLock Agent is installed on a client machine or the original assignment to an endpoint is unknown.

Helpdesk staff can still perform a recovery operation here by entering the key ID displayed to the end user.

To do so, select the following option in the Security controls in the **Encryption** menu on the **Recovery** tab:

17.2.7 Taking over native BitLocker

17.2.7.1 Integrating existing BitLocker environments

It is now simple to include hard disks and data drives from client computers that have already been encrypted in advance with native BitLocker into DriveLock BitLocker Management. DriveLock BitLocker Management allows you to control encryption and decryption from a central point without having to deal with the encryption state of individual client computers.

Enable the **Manage existing BitLocker environment** option in your BitLocker policy to specify that DriveLock can start the integration. By assigning the policy to the respective client computers, BitLocker Management is activated.

> 🗹 Note: If you do not enable this option and there are drives in your environment that have been encrypted with BitLocker before, DriveLock ignores these drives. They remain encrypted but cannot be managed with DriveLock BitLocker Management.

System drives differ from data drives:

- **System drives:** DriveLock automatically takes over system drives that have been encrypted before with native BitLocker; they do not necessarily have to be re-encrypted. In the background, DriveLock adapts the algorithms and exchanges protectors (even External keys are deleted and re-created). If the encryption algorithms match, this is a very quick process; if they do not match, DriveLock re-encrypts the drives. Depending on the system and partition size, this may take a longer time.

  > 🗹 Note: If the option **Encrypt only if pre-boot login succeeded at least once** was enabled on the Encryption protection tab, the drive must be decrypted first. After successful login to the DriveLock PBA, the drive is then re-encrypted.

  Since users unlock the system drive directly by logging on to the system or entering their BitLocker password, no further action is required from the user.

- **Data drives:** Data drives are neither unlocked nor integrated in DriveLock BitLocker Management automatically. Users will have to take action here: A wizard pops up on the client computer where the user selects the partitions that need to be unlocked. Then, the user enters the original BitLocker password and specifies a new one. The prerequisite for this is that you select the **User must change password at first encryption** option in the **Password options** dialog. However, if this option is not selected

and a password is preset, make sure to let the users know. In this case, a password change is not required; the users simply select the drives that need to be unlocked and enter their original BitLocker password.

Recovery keys: DriveLock BitLocker Management also creates new recovery keys when taking over original BitLocker environments.

Encryption algorithms: If you adhere to the Windows default settings for encryption algorithms, DriveLock BitLocker Management can take over native BitLocker environments easily and quickly.

17.2.7.2 Additional modifications of BitLocker policies

You will need to modify an existing BitLocker policy in the following cases:

- if the client computers the existing BitLocker policy is assigned to have changed (e.g. drive changes) or

- if the settings for encryption or decryption have changed, or

- if you upgrade your DriveLock agents to a higher version. For more information about updating the DriveLock Agent, refer to the Release Notes.

The encryption behavior changes depending on the setting in the respective policy.

> Note: Policy changes are applied in the next configuration update.

These are the different scenarios:

- **Re-encrypt already encrypted partitions**
  If the encryption algorithm is changed in the policy, the system will decrypt the partition first and then immediately encrypt it again using the newly set algorithm.
  For example, if you had specified the algorithm AES 128 bit key length and changes it to AES-XTS 128 bit key length, encryption restarts.

- **Exchange protectors of already encrypted partitions without new encryption**
  If the encryption algorithm already corresponds to the algorithm specified in the policy, this approach is followed.
  There are two possible reasons for such a behavior:
    - In the first case, a change from TPM/PIN to TPM (and vice versa) leads to the exchange of protectors.

    - In the second case, DriveLock is to integrate existing BitLocker partitions that have already been encrypted with the algorithm specified in the policy.

- **Decrypting partitions**

  Decryption is always triggered if either

  - the **Encrypt local hard disks on agent computers** option has been unchecked or

  - a drive is set to **not encrypted** in the **Configure encryption settings per drive** option, or

  - the **Bitlocker Management** option is disabled in the License Options under **Licensed Computers**.

- **Encrypt newly added partitions**

  The encryption should always be triggered when new hardware or a new drive are added (in the **Configure encryption settings per drive** option). By doing so, you ensure that all data on new computers and drives is protected by BitLocker.

17.2.8 DriveLock Agent

17.2.8.1 BitLocker pre-boot authentication

Please note that **an English keyboard layout** may be enabled when logging on to the BitLocker PreBootAuthentication (see figure below). Use the INSERT key to display the entered password if in doubt.

> ⚠ Warning: Please inform the users of this information and point out that special characters on an EN-US keyboard are occupied by other key combinations and that Y and Z are interchanged.
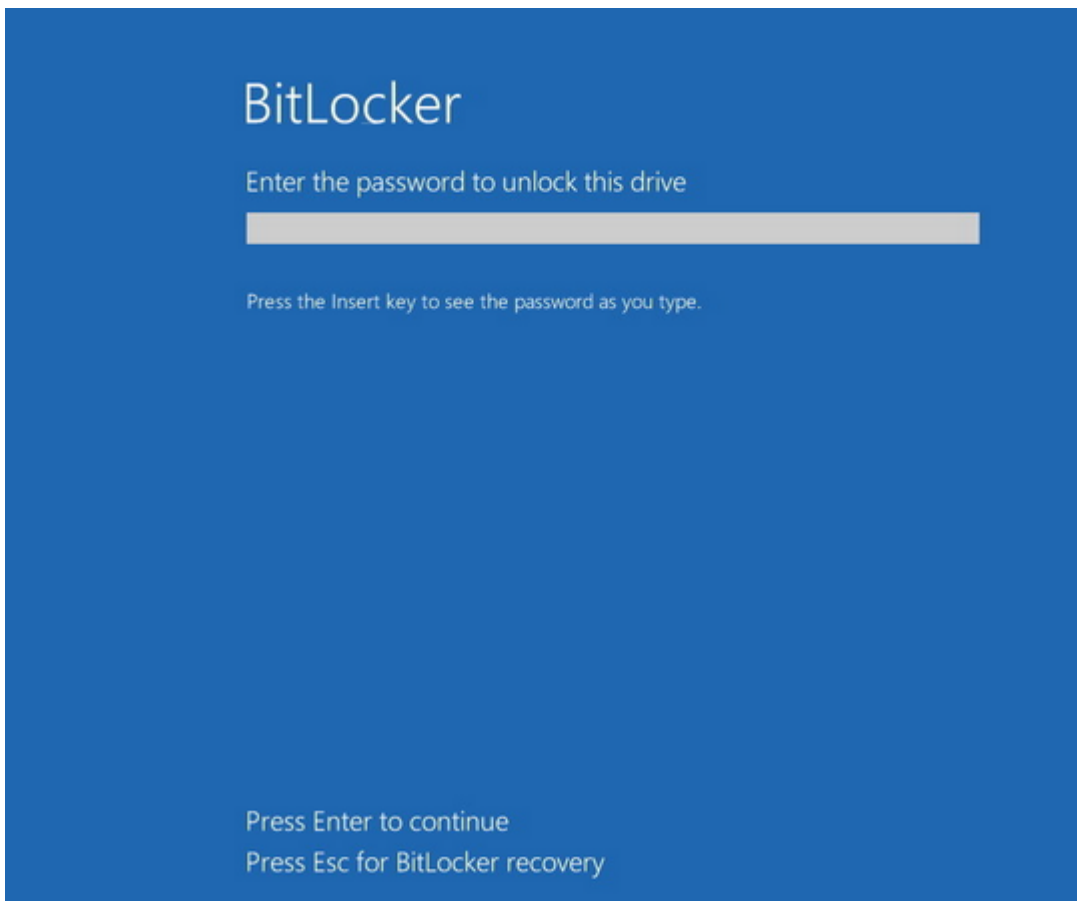
17.2.8.2 BitLocker Management on client computers (DriveLock Agent)

When your BitLocker policy is assigned to the appropriate client computers, disk encryption is initiated. Depending on the settings you specified in the Pre-Boot authentication settings dialog, encryption starts with or without the user having to enter a password.

> Note: Please provide users with the appropriate password information.

The user may also redefine the password later. The **DriveLock Agent** on the client computer provides the **Change BitLocker password** button on the **Encryption** tab for this purpose.
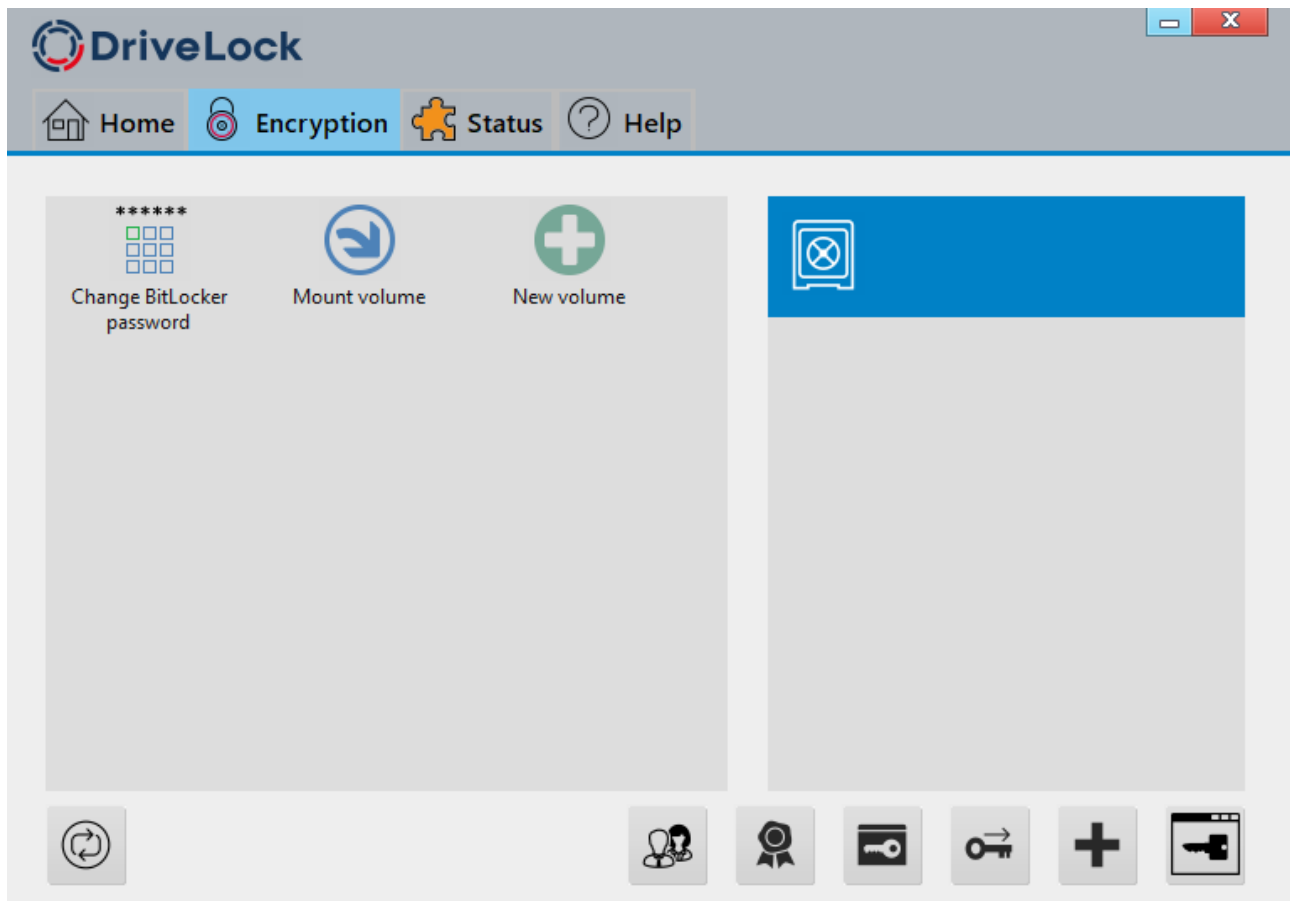
17.2.8.3 Encrypting client computers

On the client computers, the hard disk encryption and the corresponding password entry are carried out as follows:

1. In one case, the user starts the (unencrypted) client computer and logs on to Windows as usual. In the other case, the user is already logged in and the DriveLock Agent has just been assigned the new BitLocker policy.

2. Two options are available:

   a. If you specified a set password, the encryption process starts automatically and immediately without the user's interaction (no password entry or definition required).

   The user can only follow the encryption process in the status bar.
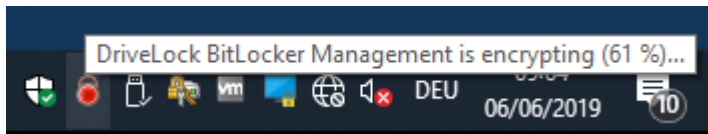
When the encryption process is finished, DriveLock issues the message described in item 5.

b. If the user must specify their own password, a wizard starts where the user defines an authentication password.

3. In case b. the user now assigns a password. The policy requirements are checked and only valid passwords are accepted.

4. As soon as the password has been defined and confirmed, the encryption process starts.

5. When this process is complete, the following notice appears on the user's screen:
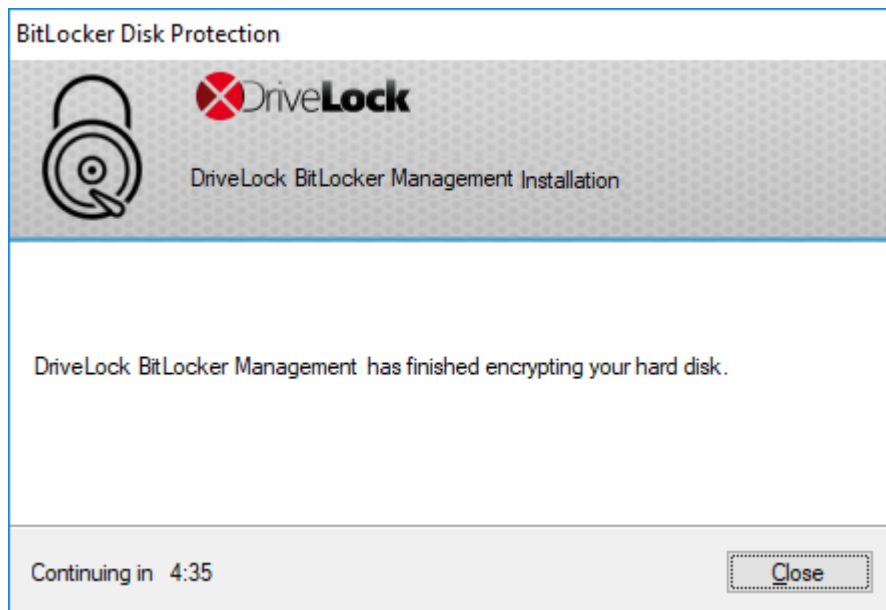
6. The next time the client computer starts up, the user enters the BitLocker password as pre-boot authentication thus unlocking the encrypted system partition (and the data partitions, where applicable).

In case a. the client computer starts without the user having to enter a password.

17.2.8.3.1 Delay encryption

Users can delay the encryption by selecting the appropriate time in the notification (see figure). Depending on how many hours are specified as the maximum value on the Execution options tab, the user can specify the time until the dialog is displayed again in the **Delay by** dropdown list. Encryption is then delayed for that long. When the specified maximum time is used up, encryption starts. It also starts if the user does nothing while the dialog is displayed or clicks on **Encrypt** .

17.2.8.4 Integrating data partitions with existing BitLocker

The procedure for unlocking data partitions that were encrypted with original BitLocker and are to be transferred to DriveLock BitLocker Management is based on two settings in the **Password options** of the BitLocker policy:

- A BitLocker password has to be set
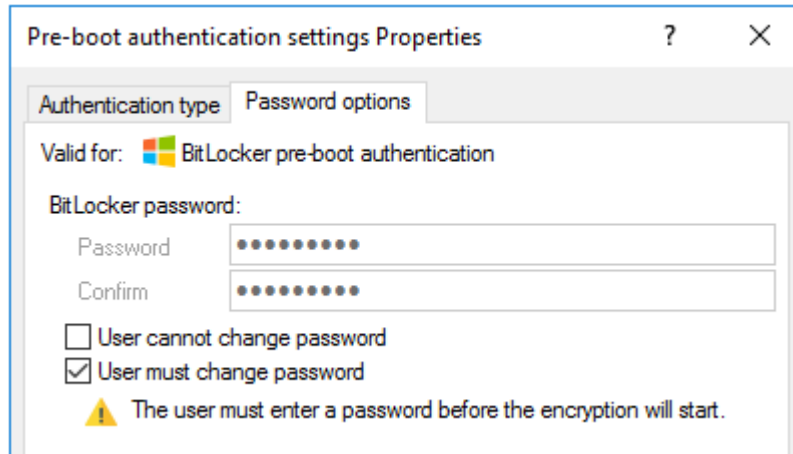
   or

- the BitLocker password is preset.
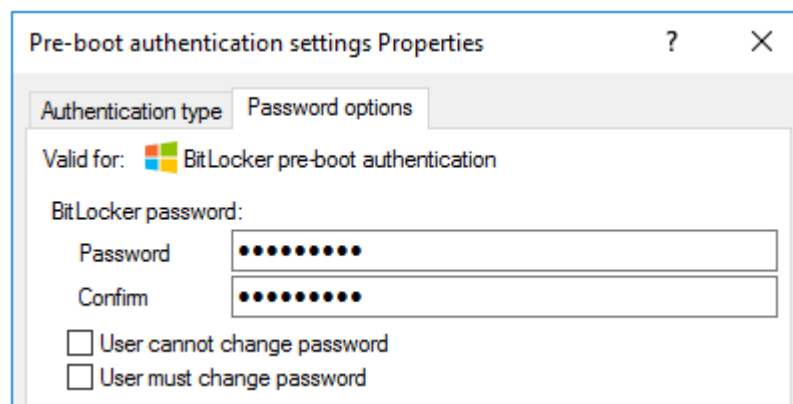
Depending on the selected option, a different wizard opens on the client computer.

- One wizard prompts the user to change the password on the following dialog pages.

- The other wizard only contains information on how to integrate the native BitLocker environment:

The second wizard dialog is the same in both cases; here, you are asked to select the data partition you want to unlock.

Select the drive (or the drives) you want to unlock and enter the original BitLocker **password**. Then you can click **Next**.
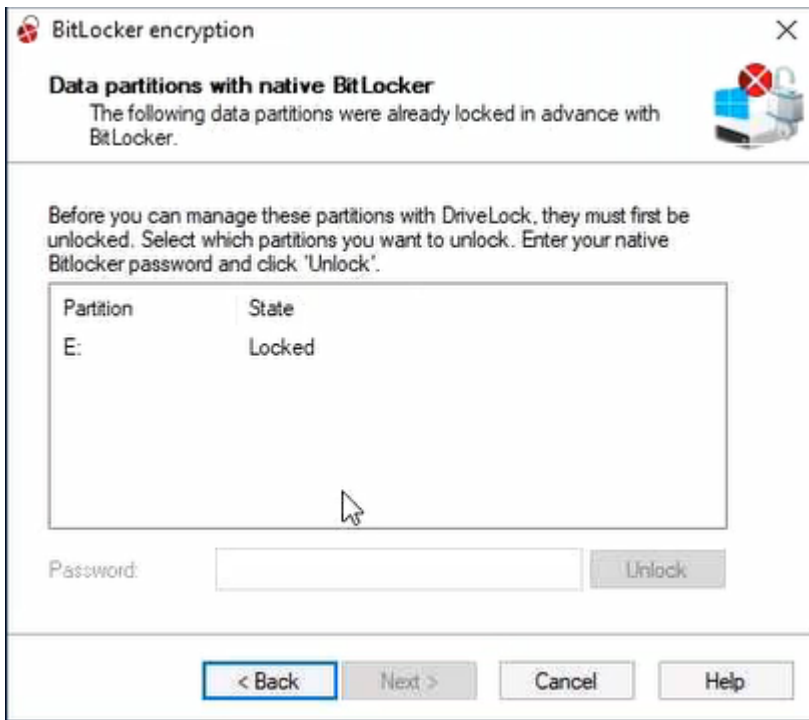
If a new password is required, a further dialog appears where a new password must be assigned.

Complete the final dialog by clicking **Finish**.

> Note: In the background, DriveLock BitLocker Management implements the integration by replacing protectors and taking over encryption algorithms.

416

17.2.9 Tracing BitLocker actions

In the DriveLock Operations Center (DOC), you can track all BitLocker actions with the help of the respective events.

You can also use tracing in detailed diagnostic logs. For example, this is important in order to trace errors during the import of original BitLocker environments. The tracing file is called `DlSvcBitLocker.log`, see figure below. Here you can easily identify the actions DriveLock performs when taking over existing BitLocker environments.

You can enable the creation of trace logs via the command line, with the help of the DriveLock Management Console or via the DriveLock Support tool `DLSupport.exe` (which resides in the DriveLock installation directory).

17.3 DriveLock pre-boot authentication

DriveLock Pre-Boot Authentication (PBA) can be used for both DriveLock encryption technologies - BitLocker and Disk Protection (Full Disk Encryption, FDE). A separate license is required for DriveLock Pre-Boot Authentication for BitLocker.

> ⊖ Warning: Please note that the PBA only works on UEFI systems from Windows 10 environments.

> ☑ Note: Since DriveLock Legacy BIOS Pre-Boot Authentication is no longer supported starting with version 2022.2, the system checks if there is an active Legacy BIOS PBA on the system when installing an agent. In this case, no update or installation of the agent will be performed.

DriveLock pre-boot authentication offers you a number of benefits:

- Login with user name / password

- Recovery using challenge response procedure

- Single sign-on (SSO) for Windows logon

- Login with Smartcard

- Support for other keyboard layouts and virtual keyboard

- Exchangeable PBA background images

17.3.1 Pre-boot authentication settings

These settings can be configured for both Disk Protection and BitLocker Management. Please note that the DriveLock PBA for BitLocker Management requires a separate license based on the BitLocker Management license.

For BitLocker Management you can configure PBA settings on the following tabs:
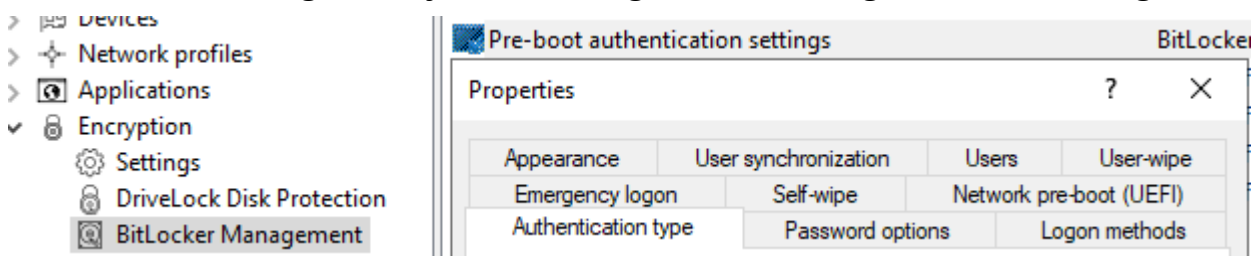
Logon methods

Authentication type

Appearance

Password options

For Disk Protection you can configure PBA settings on the following tabs:
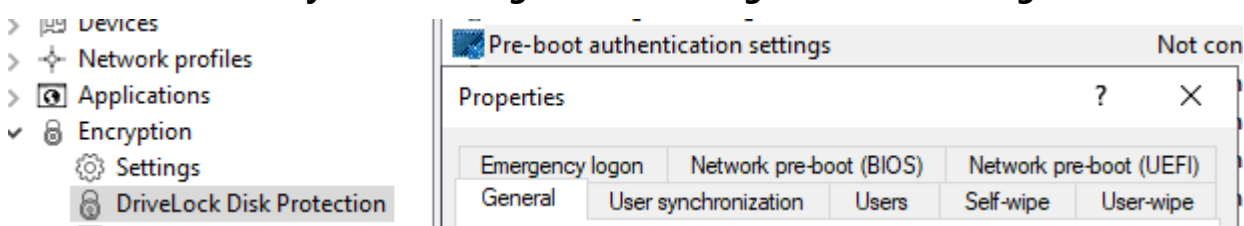
General

Network pre-boot (BIOS)

For both modules, you can configure the PBA settings on the following tabs:

Users

User synchronization

User wipe

Network pre-boot (UEFI)

Emergency logon

Self-wipe

17.3.1.1 Users

On this tab, you specify the settings for DriveLock PBA users.

- DriveLock adds every user to the pre-boot authentication database that has been successfully logged on to Windows. For this reason, the **Automatically add Windows users to pre-boot authentication** option is set by default. If you deselect this option, users are no longer added automatically.
  Using the **Add**, **Remove** or **Edit** buttons you can modify existing users, remove them or add new users to the database.

  > Note: A Windows user account does not necessarily have to exist for a PBA user, you can create additional credentials (username / password) just for pre-boot authentication (e.g. an emergency account).

- If you activate the option **Always use downlevel logonnames during single sign-on**, the user logon is only possible with the so-called downlevel logon names. They take the format "DOMAIN\username". Logon with User Principal Names such as benutzername@domain.org is not permitted anymore.

17.3.1.2 User synchronization

The **Synchronize Active Directory users to pre-boot authentication** option is not set by default, as AD users are automatically entered in the PBA database as soon as they log on to the PBA.

> Note: Use this option only if you want to preconfigure the PBA by manually adding users from AD to the PBA user database before they log on.

In this case, add the appropriate AD groups and users that you want to synchronize to the PBA database.

> Note: Please note that the members of the "Domain Users" group will not be synchronized. This group employs a mechanism based on the user's "primary group ID" to determine membership, and does not typically store members as multi-value linked attributes.

As an initial password, you can assign a **fixed password** (identical for all users), the **user name**, or any available **AD property value**.

Notes on Disk Protection:

DriveLock distinguishes four types of pre-boot users in Disk Protection:

Added via	Description
DlFdeUser	User was created locally with `DlFdeUser.exe`
Policy	User was created via policy - and will be synchronized/removed with policy changes.
Windows logon	User was created by Windows login - password is synchronized on each successful Windows login.
Active Directory	User was synchronized from AD groups - and will be deleted if removed from AD group or user synchronization. The password is synchronized locally each time Windows logs in successfully.

- The `DlFdeUser.exe` command can also delete other user types. These will be added back the next time you log in to Windows or load the policy.

- The first time Windows users log on to a client computer that is protected with DriveLock Disk Protection and Pre-Boot Authentication (PBA), their Windows credentials are not yet synchronized in the PBA database. They need to log on to the PBA with either a preconfigured user added via DlFde or the policy, or another authorized user logs on to the PBA to display the Windows logon dialog.

- Users added via AD are synchronized each time the policy is uploaded. When you add or remove users from the configured AD groups, they will also be added or removed from the PBA database during the next synchronization on all affected computers.

17.3.1.3 User wipe

To configure user wipe, select the **User-wipe** tab, check **Enable user-initiated wipe**, and enter a wipe suffix.

Enabling this option allows a valid PBA user to make the system inaccessible.

17.3.1.4 Network pre-boot (UEFI)

For more information on this tab, please click here.

17.3.1.5 Emergency logon

Use these settings to specify which logon methods are available in case a user is no longer able to log on to the DriveLock PBA (for example because the password is missing).

We recommend using the default settings.

- **Allow emergency logon with user name**: This default option lets users log on in an emergency by entering their name. This affects Windows domains or local Windows user password accounts added to the PBA user database. It permits a one-time pre-boot access to the system.

  > Note: Note that a user must have successfully logged in to pre-boot authentication at least once before this feature is available to that user. Users who have never logged in before, must use the Allow emergency logon without user name procedure.

- **Single Sign-on after emergency logon** allows users to log on to Windows and work with it if they forget their password - even if an administrator has not yet reset the password.

- **Emergency logon without user name** allows a one-time pre-boot access to the system for all users who have never been logged into the system before. Single sign-on (SSO) is not possible in this case.

- Please note that if you enable the **Allow emergency logon for token users** option, the corresponding settings for logon with tokens must also be specified on the tabs **Logon methods** (for BitLocker Management) or **General** (for Disk Protection).

  > Note: Enabling this option allows smartcard / token users, who have misplaced their token or forgotten their PIN, to use the emergency logon procedure for token users. This procedure allows a one-time pre-boot access to the system without using a token.

17.3.1.6 Self-wipe

Self-wipe has two main application scenarios. Either you want to protect the data on a lost PC that no longer connects to the DES and/or you want to force mobile users to regularly connect to the company network.

To configure self-wipe, open the **Self-wipe** tab, select **Enable self-wipe when the computer is offline** and configure the settings that are suitable for you as described in the dialog.

> ☑ Note: After the specified offline time has elapsed, DriveLock deletes all users from the PBA database so that logging in is no longer possible and the system can no longer be unlocked. To be able to access the system partition again, you need the BitLocker recovery key that was stored on the DES before encryption. To do so, the system drive must be connected to another system as a data drive.

17.3.2 PBA settings in the List view

There are three settings for pre-boot authentication available only in the list view of the **DriveLock Disk Protection** and **BitLocker Management** nodes.

These are:

- Allow local PBA configuration changes
- Select PBA keyboard driver
- Load SmartCard drivers in PBA

17.3.2.1 Allow local PBA configuration changes

You can use the 'dlsetpb.exe' command line tool to modify the PBA configuration on a computer.

This setting determines whether these configuration changes are maintained or overwritten (with the settings from the policy, e.g. which keyboard driver to use) the next time the policy is updated. By default, the changes from the command line tool are kept.

> ☑ Note: When updating from a version prior to 2020.2, all settings are treated as if they were set by the command line tool.

17.3.2.2 Select PBA keyboard driver

This setting allows you to specify the keyboard driver for the PBA.

For example, if the default driver you are using does not recognize different keyboard layouts, you can select a driver from DriveLock here. The combi driver combines both keyboard and mouse drivers in one. If this doesn't lead to the result you want, you can also use the (older) DriveLock keyboard driver.

> 🖊 Note: You may need to set different drivers on different devices.

17.3.2.3 Load SmartCard drivers in PBA

Use this setting to specify whether you want to enable the DriveLock SmartCard driver. If you want to use SmartCards and the default driver does not recognize them, you can use this setting.

> 🖊 Note: You may need to set different SmartCard drivers on different devices.

> ⚠ Warning: The DriveLock PBA requires smart card readers to have a CCID V1.1 compliant interface.

17.3.3 PBA settings in the DriveLock Operations Center (DOC)

You may want to disable the PBA, for example, when updates are pending that require a reboot.

> 🖊 Note: This setting applies to both DriveLock and BitLocker PBA.

Open the **Encryption** dashboard in the DOC. Get a list of encrypted computers from either the **Computer encryption state** widget or the **Encryption information** widget. Select the appropriate computer. You can also select it directly in the **computer** view.

In the context menu, select **Run actions on computer** and then **More actions**. In the next dialog, select **Show all actions**.
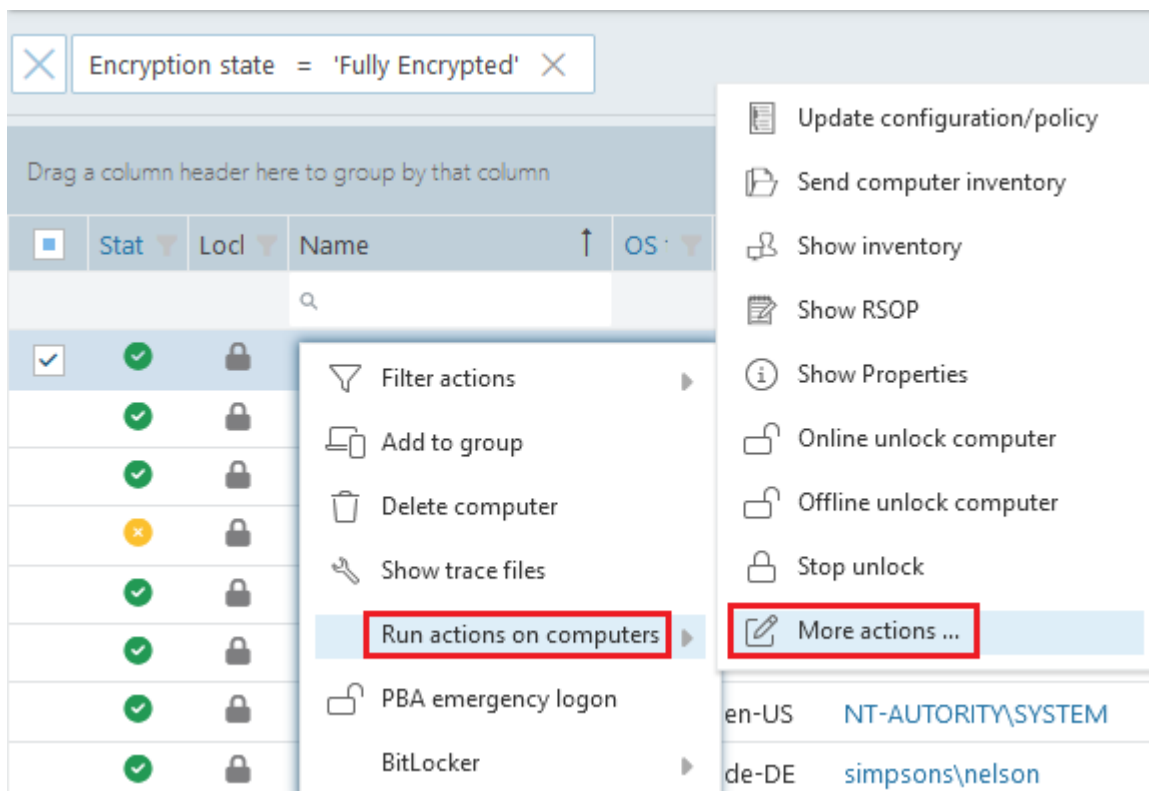
In the Pre-Boot Authentication section, check Suspend PBA and then scroll down a bit to view the settings:

You can specify this setting for a certain number of restarts or for a certain period of time. This action is defined once, i.e. it can be renewed at any time.

The status is displayed in the computer details.

17.3.4 Override policy settings (DriveLock PBA)

To disable specific pre-boot authentication settings on individual client computers, you can override the respective policy settings.

> ⊘ Warning: Note that the policy settings will not be re-enabled until you undo the override option.

Please do the following:

1. Open the **Agent remote control** in the **Operating** node of the DriveLock Management Console.

2. Select the DriveLock Agent you want to change the policy settings for.

3. From the context menu, select the **Encryption properties...** menu item.

4. On the **General** tab you can see information about DriveLock Agent encryption. Click the **Reconfigure agent...** button.

5. Set the **Override policy settings** option and leave the **Override general deployment settings** option checked (default).
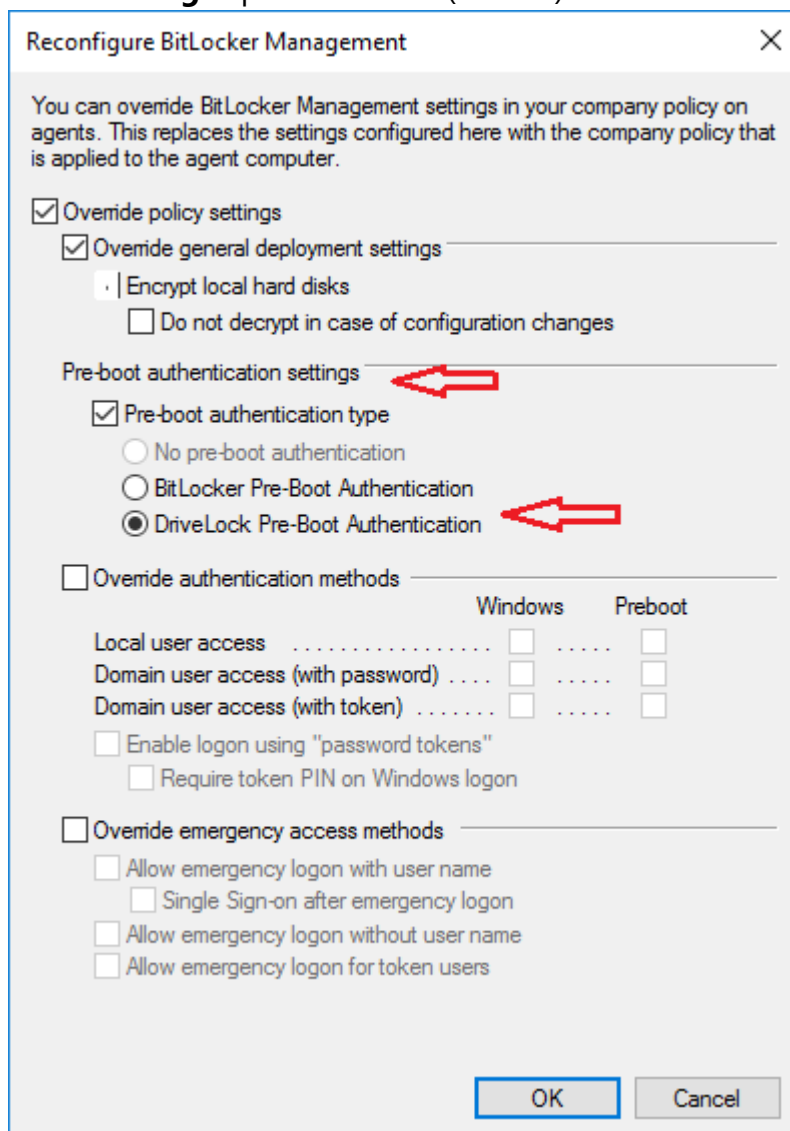
6. Select the appropriate PBA in the Pre-boot authentication settings section.

   📝 Note: If there is no TPM, the **No pre-boot authentication** option is automatically grayed out (see figure above).

7. The **Override authentication methods** and **Override emergency access methods** options are active only if you selected DriveLock pre-boot authentication. Both options override the corresponding settings in the policy. For more information, see the Logon methods and Emergency logon chapters.

8. If you click **OK** now, your settings will be applied to the selected client computer with immediate effect.

17.3.5 Network pre-boot authentication (UEFI)

This add-on to the DriveLock pre-boot authentication enables simplified management of client computers (Drivelock Agents) in network environments.

Upon reboot, the operating system drive of a client computer can be automatically unlocked if it is connected to a corporate network via cable. In this way, client systems that meet the hardware requirements can be booted in Windows without user interaction.

You can, for example, configure the feature so that client computers can be booted automatically only when they are on the network. Booting without a network is not possible!

If no network connection is available, alternatives may be permitted (e.g. emergency logon requiring user and password entry).

This also makes it easier for administrators to roll out software patches to unattended client computers, for instance.

Note the following limitations:

- Only UEFI firmware is supported

- Only wired network is supported

- Only network adapters that UEFI offers for PXE boot are supported

- The DriveLock network PBA does not provide any network drivers of its own

The following rules apply:

- The network PBA and the DriveLock Enterprise Service (DES) must have the same date / time

> ⬤ Warning: In the event of a time change (for example, winter time to daylight saving time), you run into a mismatch between server and system time if your DriveLock Agents were shut down prior to the change (thus using the 'old' time), but the time on your server has already been changed. In this case, the login to the network PBA is blocked. End users must select a different logon method once (user name / password entry) or you need to adjust the system

> ⚠ time manually. Once both times are synchronized, logging into the network PBA will work again.

- To negotiate the key pairs, the secure network connection under Windows to the DES is required (HTTPS/SSL)

- Connections via proxy are not supported in the network PBA

- In the DriveLock Operations Center (DOC), automatic logon can be temporarily disabled for each DriveLock agent (more information can be found here)

> ⚠ Warning: To ensure that the network PBA works, a server connection must be specified in the policy in the **Global settings** node, **Server connections** subnode.

17.3.5.1 Network pre-boot (UEFI)

> ☑ Note: The settings on the **Network Pre-Boot (UEFI)** tab are available for both DriveLock Disk Protection and DriveLock BitLocker Management, depending on the license, as DriveLock pre-boot authentication is used for both modules.

The following settings are possible on the tab:

1. Check the **Enable network pre-boot authentication** option to enable the feature. However, you must also select at least one of the two options below (automatic or AD logon).

2. The **Allow automatic logon to the network** option enables authentication to the client computer without any user interaction, provided that a network connection is available.
   Once the policy with this setting is assigned to the DriveLock Agent (client computer), this is what happens in the background:
   - a special network user is created in the PBA database ('AutoLogon user') along with an auto-generated user password

   - an RSA key pair is exchanged between the DriveLock Agent and the DriveLock Enterprise Service (DES)

     > ☑ Note: Automatic logon to the PBA will only occur if this key exchange is successful.

> ⚠️ Warning: Note that the client operating system can only be started if there is a network connection between DriveLock Agent and DES.

See this use case for more information.

3. When you select the automatic login, the **Allow other logon methods** option is always also selected by default. This option will guarantee that the authentication is still possible even without a network connection.

> ⚠️ Warning: If you remove the checkmark here, the possibility of a local logon or logon via challenge response method no longer exists. In the event that the configuration becomes invalid, the system cannot be booted any longer. All user accounts are automatically deleted from the PBA, AD synchronization and user import are no longer enabled!

4. The **Number of network logons to be successfully completed before disabling failsafe** option is set to the default value of 3.
Context: An additional local AutoLogon user is configured in the network PBA to serve as a failsafe in case the network PBA is unable to boot over network.
When the specified successful network logons have been performed, the local AutoLogon user is deleted and after that it is only possible to boot via the network autologon.

> ⚠️ Warning: This option can only be set initially, it has no effect on systems that are already running. For safety reasons, make sure not to select a number too high.

5. **Allow logon via Active Directory (AD)**: Select this option to obtain credentials from the AD.

6. **Allow network logon for all AD users**: Select this option to ensure that users can be logged on who are already known in the AD but not yet in the PBA database.
See this use case for more information.

7. **User logon must only occur via network authentication**: The network PBA only allows logons if the user credentials can also be verified online against AD. This means that a network logon is a prerequisite; without a network, only a challenge-response procedure is available.

8. **Number of automatic retries until the network connection is established**: Specify how often the system should automatically try to establish a network connection.

9. **Time between retries**: Specify the seconds that may elapse between retries. Default value is 5 seconds.

Example: To ensure that a router has enough time to establish a network connection, you can increase the number of automatic retries and adjust the pause accordingly. If the pause is set to 0, the process will be repeated immediately.

17.3.5.2 Use case 1: Automatic logon

Certain use cases require that the operating system of a client computer may only be started if there is a network connection, e.g. ATMs or special notebooks that may be used exclusively in the corporate network. In the event that this type of computer is stolen, the operating system can no longer be started without a network connection and the hard disks cannot be decrypted accordingly.

Follow these steps for configuration (the settings on the other tabs are explained in the corresponding descriptions):

1. Select the basic setting **Enable network pre-boot authentication**.

2. Select **Allow automatic logon to the network**.

3. Remove the checkmark at **Allow other logon methods**.

4. Leave the default value for failsafe at 3. This way you can make sure that only after 3 successful network logins there is no other way to log on. This option is intended for both testing purposes and as a failsafe.

5. Leave the default value 3 at **Number of automatic retries until network connection is established**.

6. Likewise, you can leave the pauses between retries at 5 seconds.

7. **Apply** your changes by clicking **OK**.

17.3.5.3 Use case 2: Network login for all AD users

Two use cases:

- An employee (new user) needs to log on to a particular client computer in Windows, even though the user has never logged on there before. The client computer is connected to the corporate network.

- A user has forgotten or changed their password. No challenge-response procedure needs to be performed when the client computer is connected to the network. The administrator can reset the Windows password and the user can log in to the network PBA via AD. If the AD logon is successful, a single sign-on into Windows takes place and the new user credentials are synchronized back into the PBA.

Follow these steps for configuration (the settings on the other tabs are explained in the corresponding descriptions):

1. Select the basic setting **Enable network pre-boot authentication**.

2. Select **Allow automatic logon to the network**.

3. Keep the check mark at **Allow other logon methods**.

4. Leave the default value for failsafe at 3. This way you can make sure that only after 3 successful network logins there is no other way to log on. This option is intended for both testing purposes and as a failsafe.

5. Select **Allow logon via the Active Directory (AD)**.

6. Select **Allow network logon for all AD users**.

7. Based on whether or not you want to enforce network logon, select or uncheck the **User logon must only occur via network authentication** option.

8. Leave the default value 3 at **Number of automatic retries until network connection is established**.

9. Likewise, you can leave the pauses between retries at 5 seconds.

10. **Apply** your changes by clicking **OK**.

17.3.5.4 Network PBA settings in the DOC

To configure network pre-boot authentication settings in the DriveLock Operations Center, proceed as follows:

1. Select the **Computer** section and open the BitLocker dashboard.

2. Select the DriveLock Agent you want to change the settings for.

3. In the detail view on the right side, open the drop-down menu and select Configure detail view.
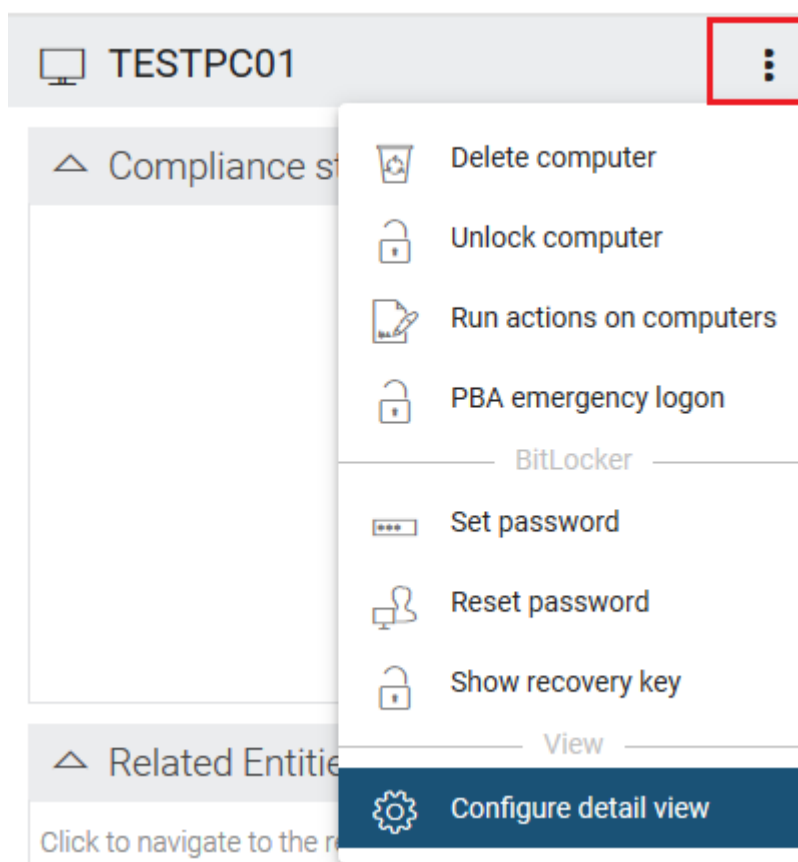
4. Select **Network pre-boot authentication** from the list and check the box next to **Show** and optionally **Expand** (depending on whether you want to display the element open immediately).

5. The **Allow automatic logon to the network** option can only be enabled or disabled.

> Note: The policy with this setting must have been assigned to the DriveLock Agent (client computer) and applied there.

433

17.3.6 Settings for emergency logon

If users are no longer able to log on to pre-boot authentication (for example, because they forgot their password), you will need to configure the emergency logon settings.

> 📝 Note: For more information on the interaction between administrator and end user, click here.

Please do the following:

1. To start the recovery/emergency wizard, open the **Operating** node in the **DriveLock Management Console** and right-click the **Agent remote control** sub-node to open the context menu.

2. Here you select **BitLocker Management recovery** and then **BitLocker Management recovery / emergency logon** (see figure).
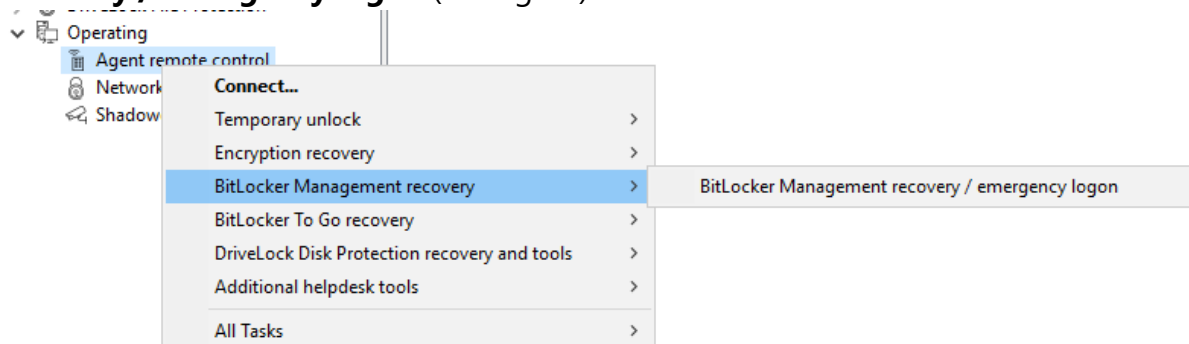
3. The recovery wizard opens.
   Select **Emergency logon**. If your recovery keys are sent to the DriveLock Enterprise Service, do not change the default setting **DriveLock Enterprise Service**. To specify the path to the required recovery keys later, select **Recovery files (copied by agent computer)**.
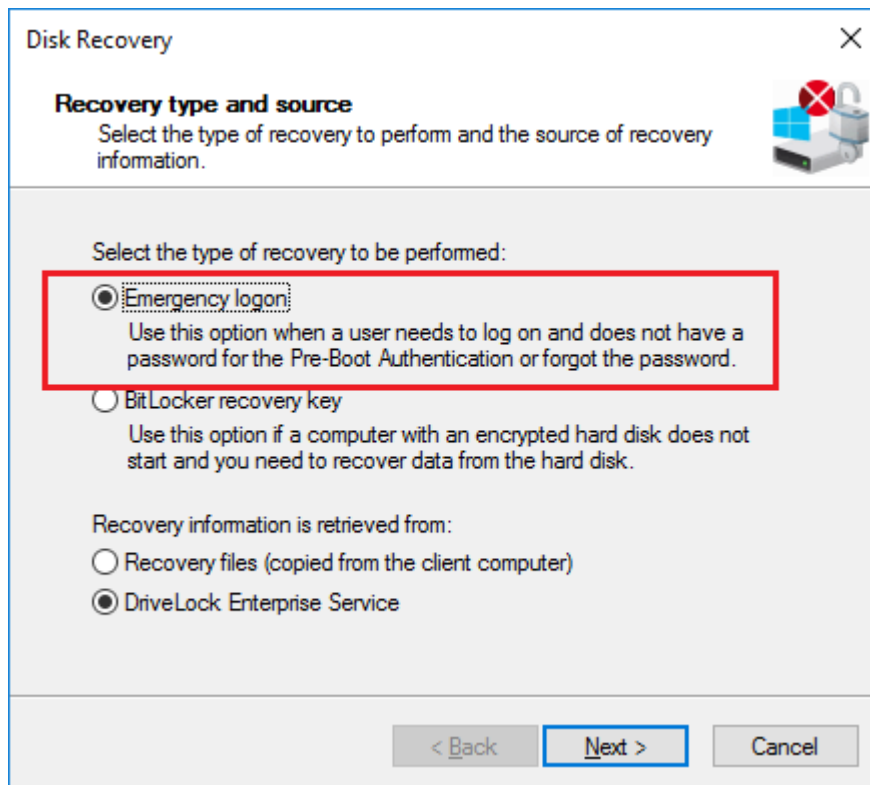
4. For the emergency logon procedure you need the private key of the recovery cer-
tificate. In the second dialog, specify the storage location, either Windows certificate
store, a smart card or a PFX file together with the respective password. For more
information on certificates, please click here. Click **Next**.

5. The third dialog provides a list of computers where you can select the computer to
restore. Check the option **only show the most recent entry for each computer**.
Click **Next**.

6. Next, you will see the dialog for entering the user's request/recovery code.
Enter the code in the appropriate text boxes (see figure). You can optionally specify
the name of the user.

> ⊗ Warning: The recovery code provided by the user is mandatory.

7. Click **Next** to generate the response code.

8. Tell the user the **response code**.

9. Click **Finish**.

17.3.7 DriveLock Agent

17.3.7.1 Installing the DriveLock PBA on the DriveLock Agent

Please note the following:

1. Once the client computer has started, a message appears indicating that the DriveLock PBA is being installed.

2. When confirmed, the computer is restarted.

> 🖉 Note: In case no user is logged in, the computer is restarted immediately.

3. After restarting the client computer and logging on, another dialog box appears (see figure), informing the user that DriveLock PBA is now active.

4. At the same time the encryption starts; restarting or shutting down the computer is now possible at any time.

17.3.7.2 Login to the DriveLock PBA

Please consider the following when logging in:

1. As soon as the client computer is booted, a short text is displayed indicating that DriveLock pre-boot authentication is active.

2. Immediately after the text display and even before the start screen is displayed, hot keys can be used.

3. The login page opens when you press any key or click the mouse button.
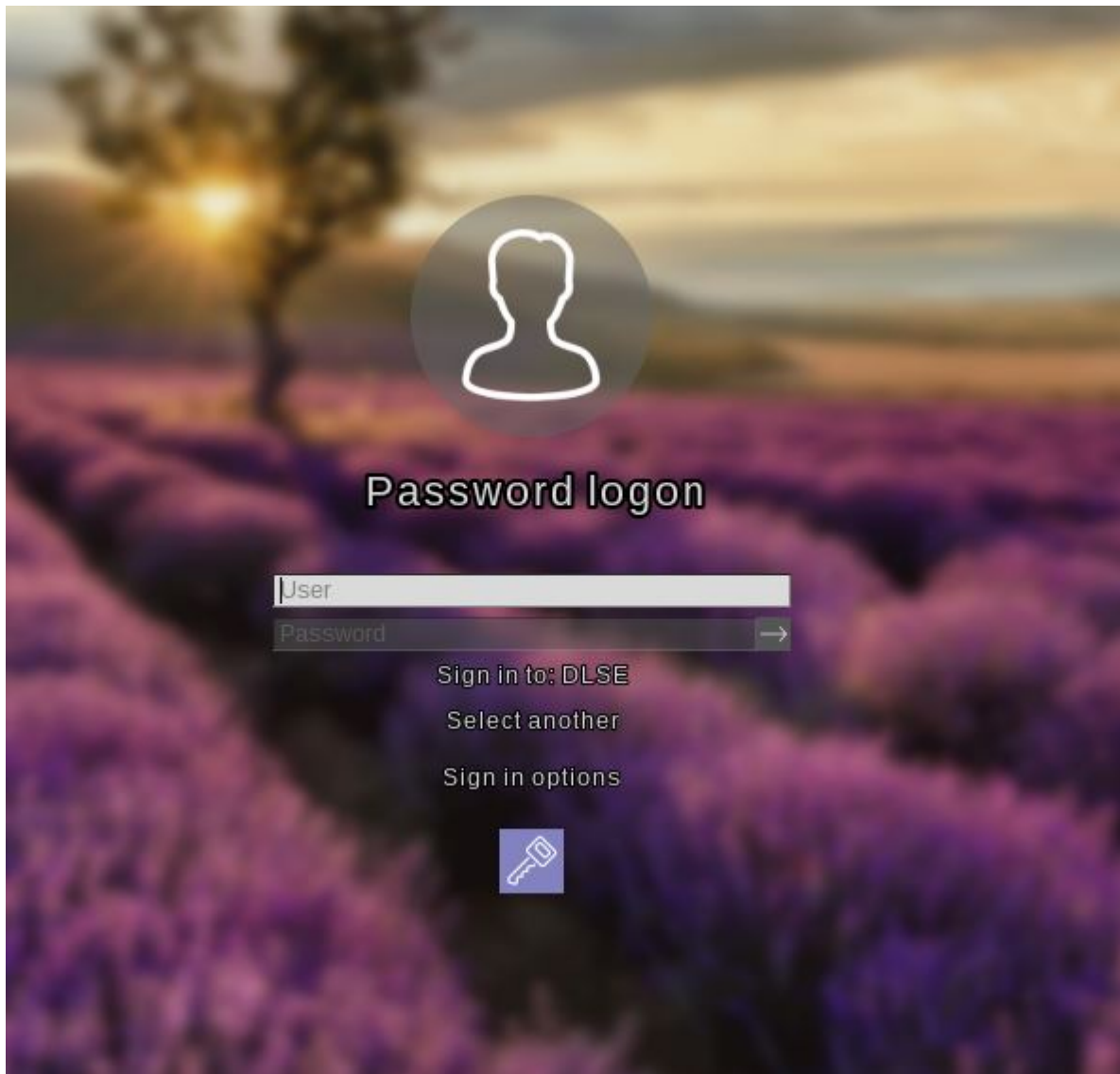
Using function keys is not required anymore, but possible.

4. Please enter the Windows credentials on the login page.

> ⚠ Warning: The most recently logged on user is not saved or displayed for security reasons.

Please note the following:

- Please note that the user must have previously logged on to Windows if you have selected the option "Synchronize Windows users automatically". For more information, refer to the chapter User synchronization.

- You can also import users from Active Directory beforehand with a policy setting. For more information, refer to the chapter Users.

- Passwords must contain only ASCII-128 characters for authentication to be successful in the PBA

5. Click **Select another** to select the domain. A list of the available domains is displayed.

6. If no keyboard is available (for example, on a tablet computer), an on-screen keyboard can be displayed by clicking the **keyboard icon** in the lower right corner.
   A green checkmark is displayed on the keyboard icon. The keyboard appears when the cursor is in a text field.

   The speech bubble icon allows you to set the language of the login interface.

7. You can reach all fields and options also using <Tab>, <Shift-Tab> and the arrow keys, if there is no mouse available.

8. By selecting the language (in the figure '**GER**') in the lower right corner, you can select a different keyboard layout.

9. You can log in either by clicking the arrow next to the password or by pressing <Return>.

10. By default, the user is also logged on to Windows (Single Sign On). You can disable this feature in the policy.

17.3.7.3 Network pre-boot authentication

Once the policy containing the network PBA settings is assigned to the client computer and the computer is started, the following scenarios are possible:

1. **The client computer is connected to the corporate network**

   When booting the client computer, a notification appears that DriveLock pre-boot authentication is active.
   Then the following login screen appears, see the figure:

   > Note: No user interaction is required.
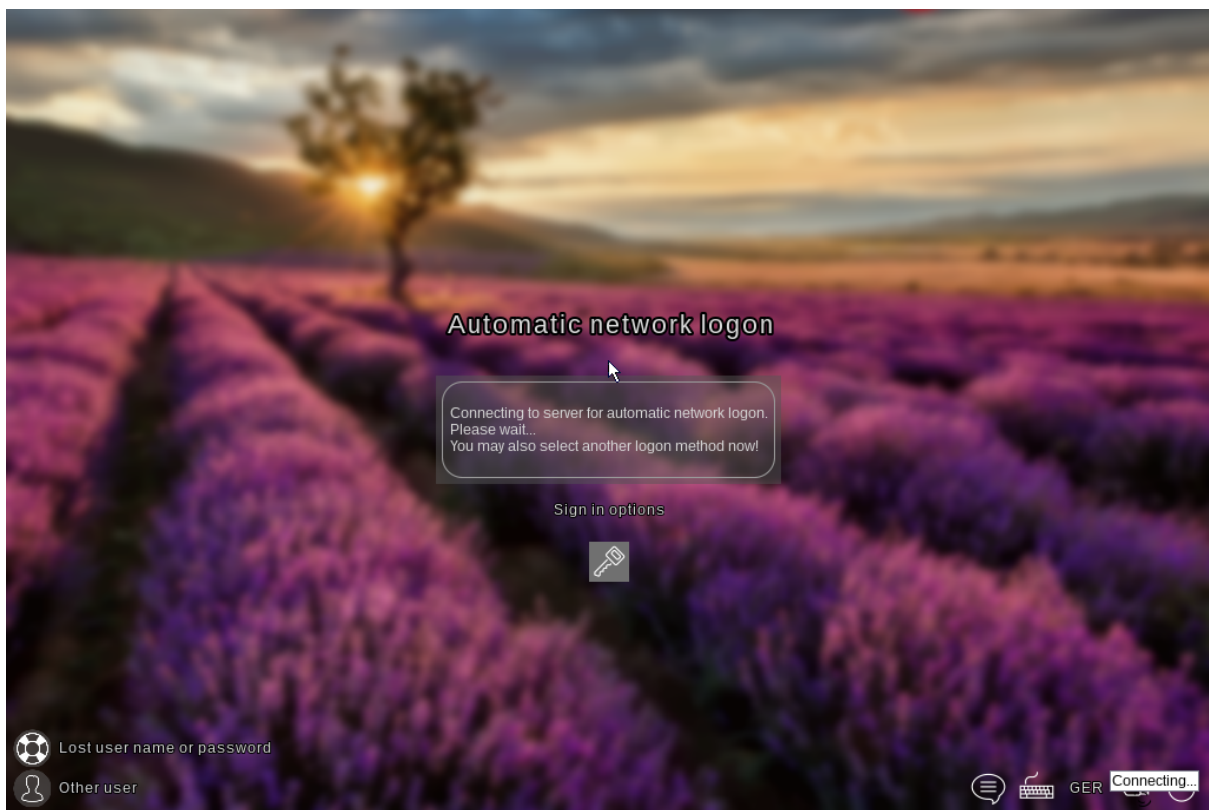
   > Note: By clicking the key icon within 10 seconds it is possible to switch to the PBA login mode with user name and password entry, if enabled.

   The next step shows the Windows login screen where the Windows credentials are entered.

2. **The client computer cannot connect to the corporate network**

As soon as the client computer is booted, the notification indicating that DriveLock pre-boot authentication is active also appears. However, the login screen now indicates that the automatic network login has failed. Depending on the configuration in the policy, the system will try to connect automatically a few times.
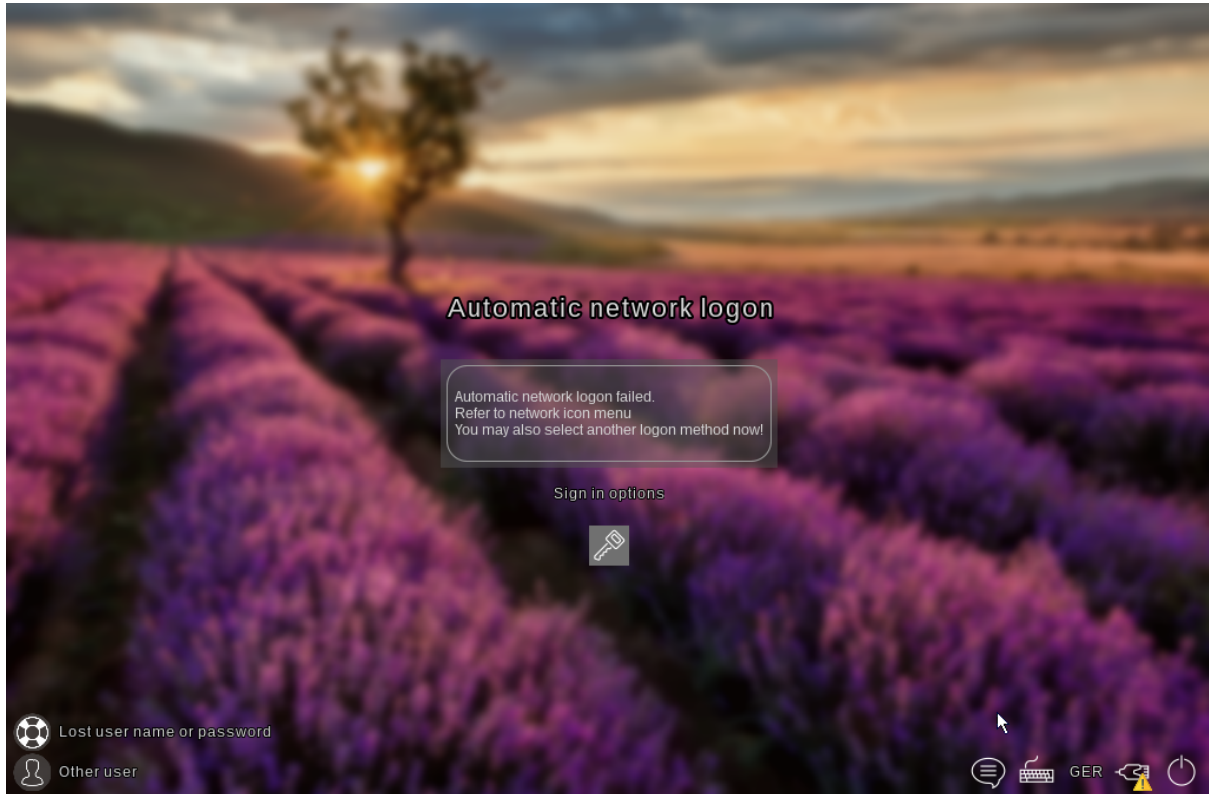
If no connection can be established, the user has the following options according to the policy settings:

- Try to re-establish the network connection
  The following options are available from the **network icon menu** in the taskbar:
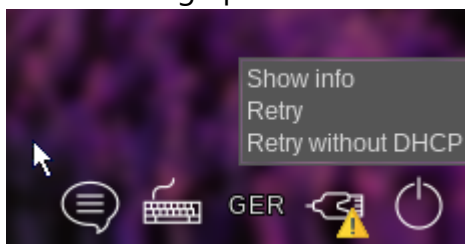
- Select another login method (user name/password entry), if enabled. Here, single sign-on is active and logging in to the DriveLock PBA is required only once.

> ⛔ Warning: Unless another login method is allowed, it is not possible to start the client computer's operating system without a network connection.

> ☑ Note: For more information, including how to use shortcut and function keys, see the Login to the DriveLock PBA chapter.

17.3.7.4 Emergency logon with recovery code

Scenario:: A user of a DriveLock Agent has forgotten their password and cannot authenticate to the DriveLock PBA. The user asks the administrator for help.

User and administrator now perform the following actions:

1. User action:

1. Select the **Lost username or password** option on the left side of the login screen.
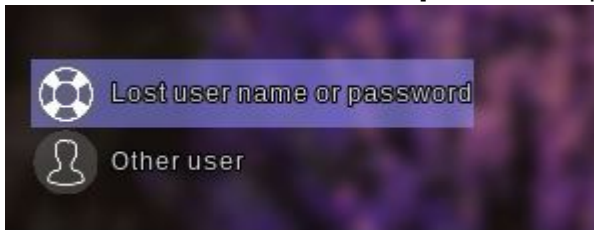
2. A new login screen will then appear, displaying your request or recovery code.

3. Inform the administrator of the recovery code and machine name, including the user name if necessary.

> 📝 Note: You must provide the machine name and recovery code while the user name is optional.

2. Administrator action:

1. After the user has been informed, you have immediately called up the recovery wizard and have now reached the input mask for the request or recovery code.

2. Enter the **recovery code** to generate the **response code**.

3. Now communicate the **response code** to the user.

> ⚠ Warning: The request code and the response code are both generated once and can only be used once.

3. User action:

1. Enter the **response code** in the appropriate text boxes in the DriveLock PBA.
   In case you make a mistake while entering the code, you will be shown error digits in different colors.
   If you have entered everything correctly, you can log back into the system by clicking the arrow button.

2. Sign in to Windows.

> ⚠ Warning: Note that Single Sign-On is not active now!

17.3.7.5 Windows authentication

Each time a user successfully logs on to Windows manually, the most recent Windows password is added to the pre-boot user database. The same happens when a user changes his

personal password in Windows.

The logon behavior depends on the setting in the DriveLock policy:
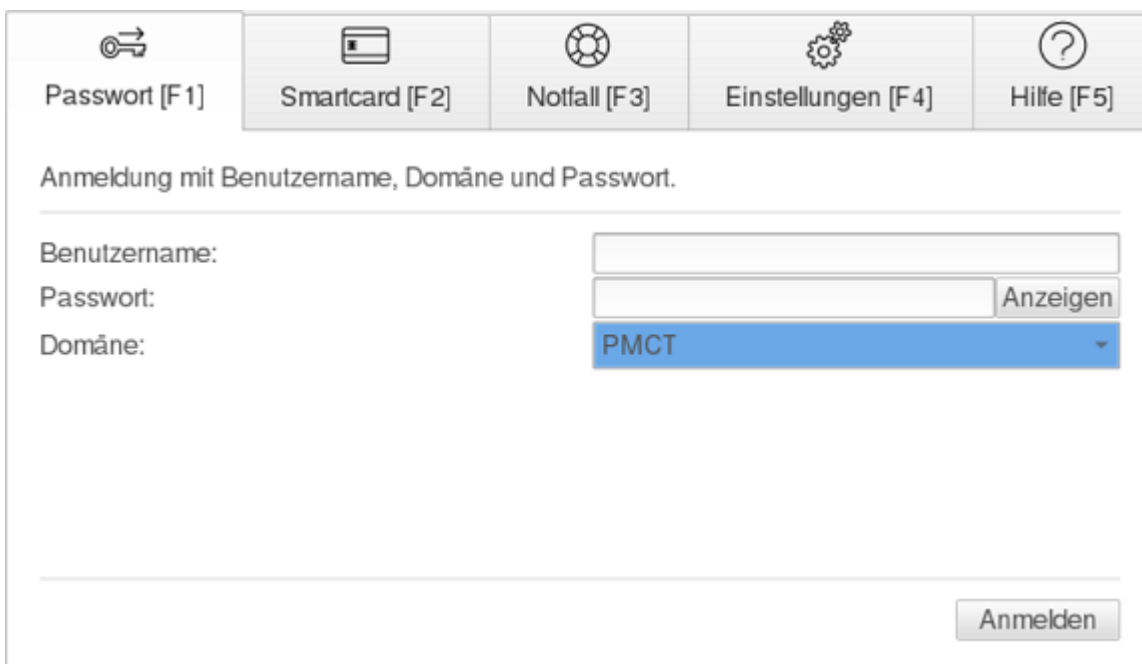
- Automatic: **Single Sign-On mode** is enabled: the user is automatically logged on to Windows.

- Manually: **Single Sign-On mode** is turned off: the Windows logon screen is displayed and the user must log on with their personal credentials.

17.3.7.6 BIOS pre-boot authentication
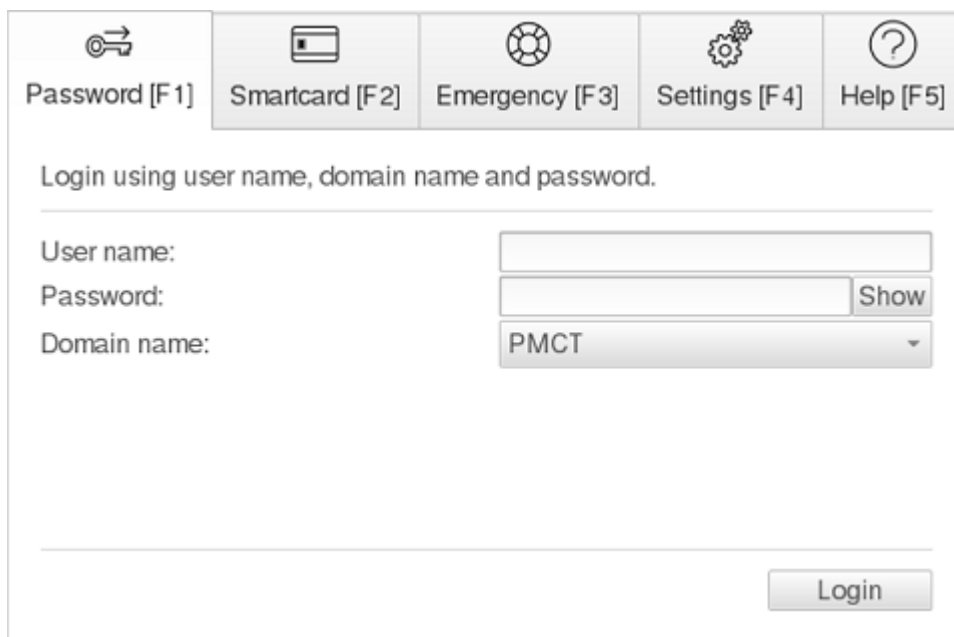
If the Disk Protection PBA has been installed on a legacy BIOS system, the authentication will work as follows.

Authentication with user name, password and domain name

If you enabled the Local user access or **Domain user access (with password)** authentication methods in the **Pre-boot authentication settings**, DriveLock Disk Protection displays the following screen:

If both authentication options Local login and/or Domain user (with password) are enabled, you can switch to the smartcard login screen by pressing the F2 key.

The **Domain** name field lists all available domains if Domain user access (password) is allowed. The local system name may also be entered in this field. Use the [arrow-up] and [arrow-down] to scroll through the list of available domain names.

> Note: In case of consecutive failed pre-boot authentication attempts, the lockout policy is enforced to prevent password guessing. To view details of failed logon attempts and other events use the Windows Event Viewer.

If a user can no longer log on to the system (for example, the user does not remember the correct password), it is possible to start the emergency logon procedure with a user name.

Authentication with smartcard/token and PIN

If the Disk Protection authentication methods **Domain user access (with token)** or Access with Shared Key are enabled, then the Pre-boot authentication window will look like the one shown below:

Passwort [F1] Smartcard [F2] Notfall [F3] Einstellungen [F4] Hilfe [F5]

Anmeldung mit Smart Card (Token) und Pin.

Pin:

Anmelden

Password [F1] Smartcard [F2] Emergency [F3] Settings [F4] Help [F5]

Login using smart card (token) and PIN.

Pin:

Login

If both authentication options Local login and/or Domain user (with password) are enabled, you can switch to the Username/Password/Domain name screen by pressing the F1 key.

At this point, the user can authenticate to the system using their smartcard/token and PIN. Please note that in the case of consecutive failed pre-boot authentication attempts, the lock-out policy is enforced to prevent PIN guessing (open the system event log for more details on failed login attempts and other events).

If a user does not remember the correct PIN and therefore cannot log on to the system, the emergency logon procedure for token users can be started.

17.3.8 DriveLock PBA command line tool

The DriveLock PBA command line tool `DLFDEcmd` can be employed with both BitLocker Management and DriveLock Disk Protection (Full Disk Encryption, FDE). Use this tool, for example, to view the status of the PBA or to initiate an automatic logon (autologon) to the client computer whenever Windows system updates are required.

> ✏️ Note: The display text is adapted accordingly depending on the preferred encryption method (Disk Protection - FDE or BitLocker Management).

Help on how to use the individual commands is available when you use the ' help' parameter to call the `DLFdeCmd.exe` program.

Please find below the detailed description of the individual parameters:

- `SHOWSTATUS`: Displays the current status of the encryption method you are using.

- `CRYPTSTATUS` : Displays information on the current encryption status, e.g. the number of encrypted hard disks.

- `ENABLEAUTOLOGON`: Enables automatic logon as part of disk encryption for the next number of logons.
  Enter the following:
    - `<user>`: PBA user for automatic logon

    - `<domain>`: Domain of the specified PBA user

    - `<password>`: Password of the specified PBA user (* to enter the password, # to enter in a dialog)

    - `<count>`: Number of reboots where automatic logon is activated. Specify 'forever' if you want the automatic logon to be activated indefinitely.

    - `[sso]`: Add "sso" only if you want automatic login with Single Sign On.

  Example: If you enter `enableautologon hans dlse * 2`, the user 'hans' from the domain 'dlse' will be automatically logged in at the next '2' reboots and the password will be entered in the command line.

  > ✏️ Note: For automatic login with a smartcard or token, specify "token" for `<user>` and `<domain>`.

- `DISABLEAUTOLOGON`: Disables automatic logon.

- `SHOWAUTOLOGON`: Shows the settings for automatic logon

- **ENABLERESETSP**: Activates resetting the system protection interrupt vector list after the next reboot. Use this option after updating the system BIOS to store new interrupt vector values and suppress the PBA warning messages. A single automatic logon is required to reset the interrupt vector list.
  Please enter the information in `<user> <domain> <password>` here as well.

- **DISABLERESETSP**: Disables resetting the system protection interrupt vector

- **SHOWRESETSP**: Displays the current settings for resetting system protection

- **ENABLEDELAYINST**: Delays the installation of the hard disk encryption until "DisableDelayInst" is executed.

- **DISABLEDELAYINST**: Disables the delay and performs the disk encryption installation as configured in the policy

- **SHOWDELAYINST**: Displays the current status of the delayed installation

In the figure below, the autologon for BitLocker Management is disabled and the `ENABLEAUTOLOGON` command has not been set here.

```
C:\WINDOWS\system32>DlFdeCmd SHOWAUTOLOGON
-------------------------------------------------------------
DriveLock 19.2.0 : Data protection, encryption, and more
DLFdeCmd         : Full disk encryption command line tool
                   (C) Copyright 2004-2019 DriveLock SE.
-------------------------------------------------------------

BitLocker Management auto-logon is currently disabled.

C:\WINDOWS\system32>DlFdeCmd SHOWRESETSP
-------------------------------------------------------------
DriveLock 19.2.0 : Data protection, encryption, and more
DLFdeCmd         : Full disk encryption command line tool
                   (C) Copyright 2004-2019 DriveLock SE.
-------------------------------------------------------------

BitLocker Management system protection reset is not active.

C:\WINDOWS\system32>DlFdeCmd SHOWDELAYINST
-------------------------------------------------------------
DriveLock 19.2.0 : Data protection, encryption, and more
DLFdeCmd         : Full disk encryption command line tool
                   (C) Copyright 2004-2019 DriveLock SE.
-------------------------------------------------------------

BitLocker Management installation will execute as configured.

C:\WINDOWS\system32>
```

17.3.9 Shortcut and function keys

If necessary, you can use hotkeys to reverse the settings for loading certain drivers and avoid issues when starting the PBA on certain systems:

Key	Function (with default settings)
k	Keyboard drivers are not loaded
l	There are no keyboard layouts available in the PBA other than the default firmware layout
s	No smartcard support
a	All the above functions are selected
b	Switching between keyboard drivers and layouts (b->both)
c	Switching between the keyboard or combined drivers (c->combi)

After that, the current status is briefly displayed before loading the PBA (see example in figure below).

> Note: The combined driver combines both PS/2 keyboard and PS/2 mouse in one driver to avoid incorrect communication between the drivers.

The following function keys can be used within the start screen:

Key	Function
F1	Login with password
F2	Login with token
F3	Emergency logon
F5	Help call
F8	Forced check for tokens

17.4 DriveLock BitLocker To Go

DriveLock BitLocker To Go includes the following features:

- Enforce encryption of external USB storage media

- Enforced encryption of external drives (e.g. eSATA hard drives)

- DriveLock detects USB drives already encrypted with BitLocker To Go and does not re-encrypt them during enforced encryption

- User-defined passwords

- A corporate password can be assigned ensuring that data can only be accessed internally within a company

- Recovery of encrypted data

- Centralized management

17.4.1 Requirements for BitLocker To Go

Before you can use BitLocker To Go to encrypt external USB storage devices or drives, two conditions must be met:

1. You have a valid license for the product.

2. You select BitLocker To Go as the encryption method in the general encryption settings.
   Proceed as illustrated in the figure.
   Select the option **Encryption of removable drives (BitLocker To Go)** at **Available encryption methods for removable drives**.
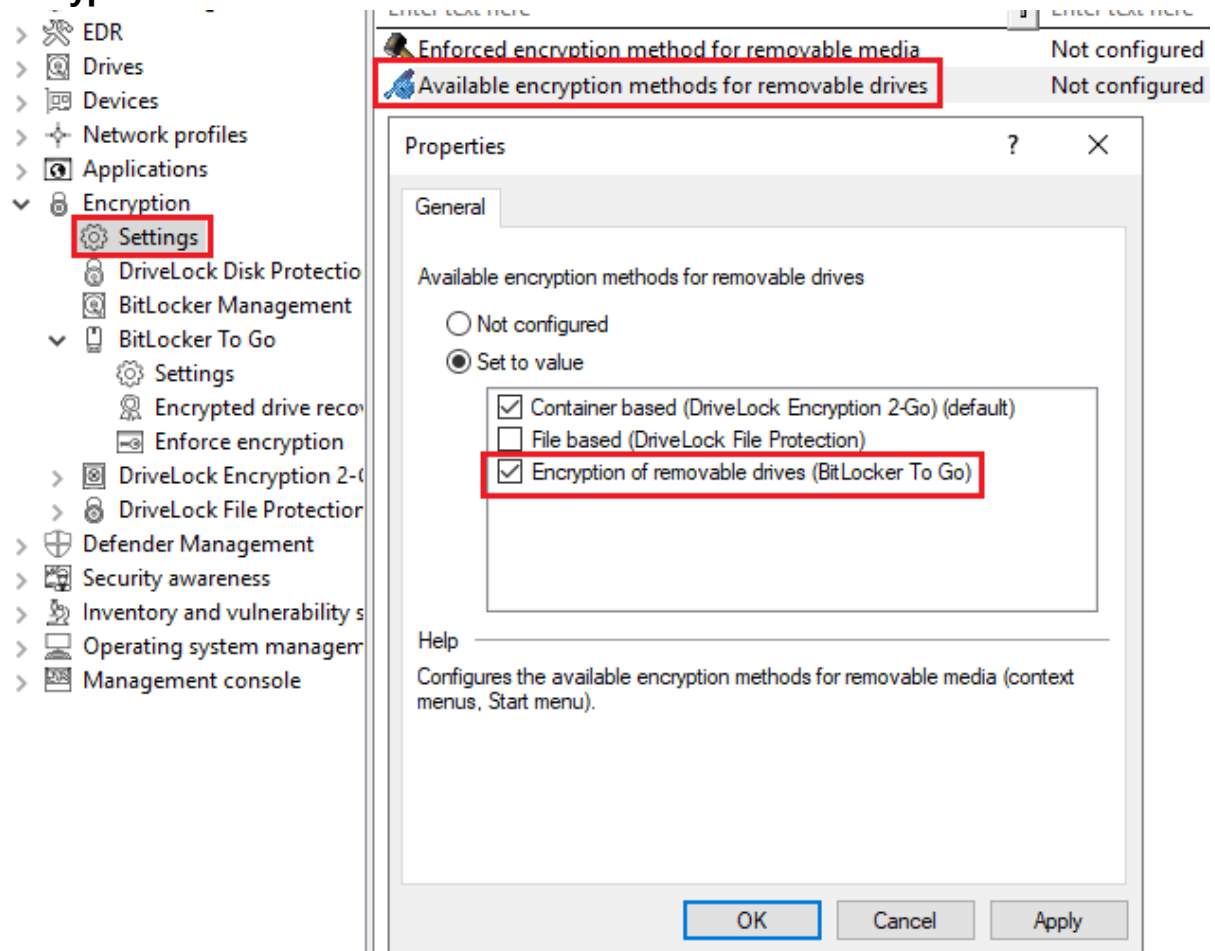
3. To be able to use the enforced encryption, please also select the corresponding method via the **Enforced encryption method** setting. On the other tabs you can enter appropriate notifications for end users.
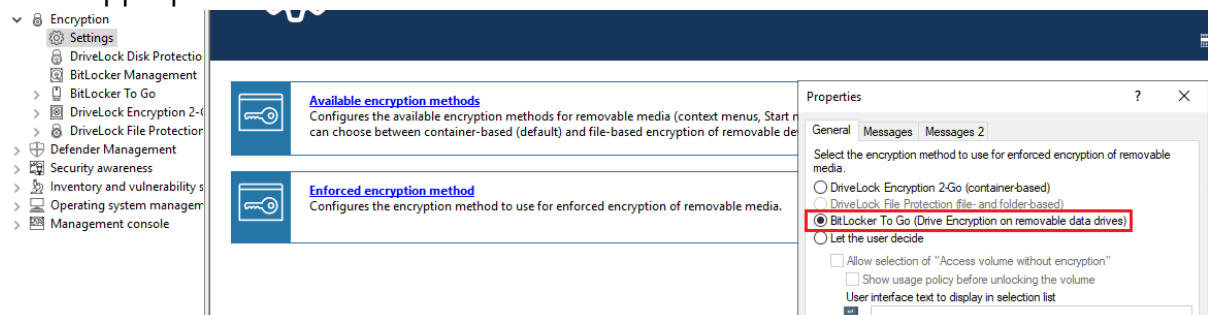
17.4.2 Policy settings

Before DriveLock can encrypt an unencrypted USB storage device with BitLocker To Go, you need to configure a policy with the appropriate BitLocker To Go settings.

Specify the following:

1. General Settings

2. Setting: Encrypted drive recovery
   - Encryption recovery rule (certificate-based recovery)
   - Administrator password for encryption

3. Setting: Enforce encryption

A sample configuration explains all necessary steps.

Once you have completed, saved, and assigned the configuration to the DriveLock agents, a new **DriveLock BitLocker To Go** entry appears on the user's Start menu with submenus for restoring, encrypting, connecting, and changing the password of each USB storage device.

The next time a user connects a USB storage device to the DriveLock Agent, an unencrypted drive is immediately encrypted. DriveLock walks users through the encryption process. USB storage devices that have been encrypted before will be recognized in the corporate network, won't be re-encrypted and can be used immediately.

> Note: Please note that all passwords (user or administrator) should follow the complexity rules (8 characters, upper case, lower case, number, special characters - e.g. DriveLock1$)

17.4.2.1 General settings for BitLocker To Go

You can specify the following policy settings to configure how BitLocker To Go is used on DriveLock Agents:
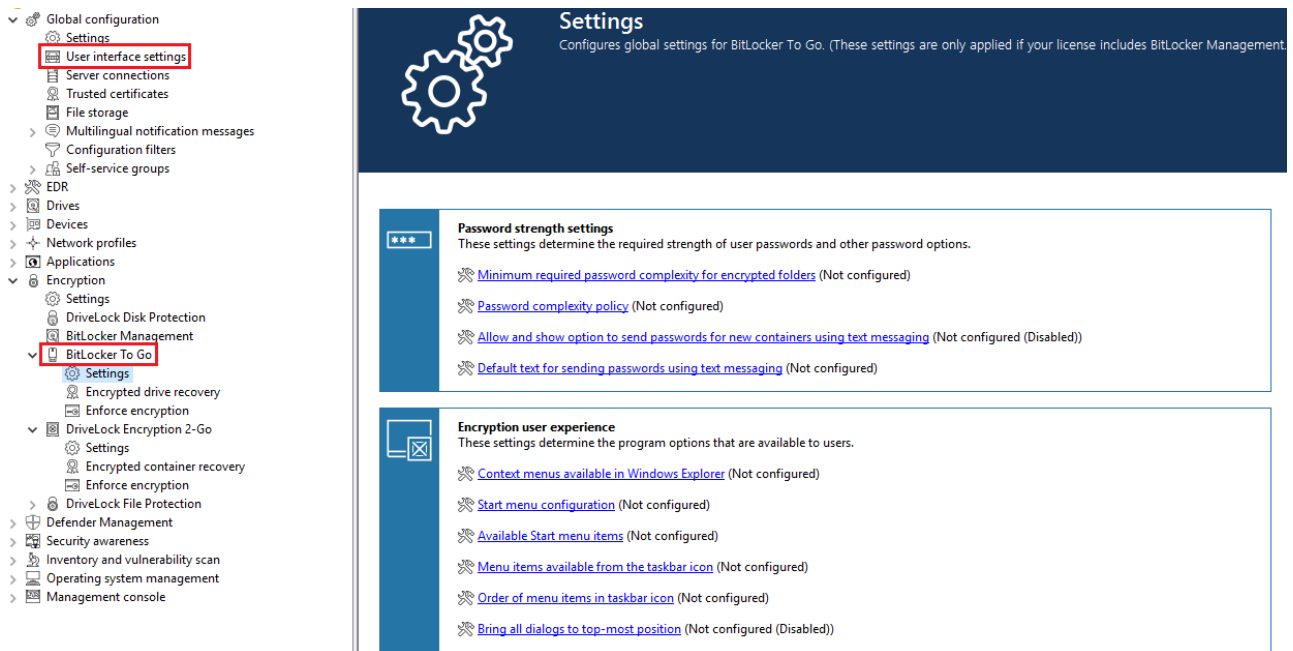
1. **User interface settings** in the **Global configuration** node:
   - By specifying the **Taskbar notification area settings**, you can configure different types of user notifications. You can move the BitLocker To Go entry to any location here.

2. Settings in the **BitLocker To Go** node:
   - **Minimum password complexity for encrypted folders**:
     Specify how complex the passwords must be. If you select **Use password policy**, make sure to define exact requirements.

   - **Password complexity policy**:
     Specify the minimum requirements that users must meet when entering a BitLocker To Go password.

   - Further settings in the **Password strength** and **Encryption user experience** sections:
     The settings affect the display of BitLocker To Go in the Start menu, taskbar or Windows Explorer and are identical to the corresponding settings for Encryption 2-Go.

   - **Manage BitLocker To Go media not encrypted with DriveLock** : Enable this setting to allow recovery information for removable media that are not encrypted with DriveLock to be uploaded to the DES. For this, certificate-based drive recovery and forced encryption must be configured.

For information about the effects of the settings, see BitLocker To Go on the DriveLock Agent.

17.4.2.2 Recovering encrypted drives

To start with, you select the main certificate (or create a new one) that is essential for the recovery process. Then, you assign an administrative password that will be used to encrypt the USB storage devices.

17.4.2.2.1 Administrative password

Use a central administrative password for accessing encrypted removable storage devices.

> 🖉   Note: Ensure that the administrative password is complex enough.

In addition to the central password, you can also create additional administrative password rules and prioritize them differently. By using different passwords, you can provide increased security.

To create a new administrator rule, open the context menu of **Encrypted drive recovery** and then select **Administrative password rule**.

You can restrict the password rules for certain **logged on users** or user groups, **computers** or **networks**. Enter the required information on the tabs in the dialog. See the Use cases for more information.

17.4.2.2.2 Certificate-based recovery

Before creating an encrypted USB storage device, select a master certificate consisting of a public and private key pair. See chapter Encryption certificates for more information.

You can either create a new certificate or use an existing one. Further information can be found in the Create encryption certificates chapter.

You can create several Encryption recovery rules with various certificates, which can be restricted and prioritized differently depending on the information you enter on the Computers, Users, Networks tabs. This is useful if you want to allow different users to restore encrypted data.

> 🖉   Note: Use the standard recovery certificate (lowest priority) as a minimum.

No other information is required in this dialog.

17.4.2.3 Settings for enforced encryption

The default enforced encryption rule is always available. If required, you can create additional rules for specific logged on users, groups, computers or networks. See the Use cases for more information.

When editing the first encryption rule, a description is already entered on the **General** tab. Add a comment and your own text, which is displayed in the user selection dialog.

On the **Settings** tab you can use the default settings or select the following options:

- **Use administrative password. Don't prompt user**: If you enable this option, the storage device will be encrypted with the administrative password only. Users are not prompted to enter their own password during encryption.

- **Prompt user for encryption password**: This setting prompts the user for their own password.

- **Use random password**: With this option, a random password is generated but not saved. To unlock, please add the corresponding users or computers on the tabs **Automatic unlock user** or **Automatic unlock computer**. Please note that these can only be added from the AD inventory.

  > Note: This option requires that you have set an administrative password in the **Encrypted drive recovery** rules.

- **Encryption**: Select the appropriate encryption method. Please note the following:
    - The default option is **AES (256 bit key length)**.
    - Select **AES (128 bit key length)** if compatibility with older systems is critical for you.
    - **AES-XTS (128 or 256 bit key length)** encryption methods are only available for Windows 10 1511 and higher. Drives encrypted with XTS AES cannot be accessed on older versions of Windows.

17.4.3 Sample configuration for BitLocker To Go encryption

To encrypt or unlock removable storage devices (USB storage devices) with BitLocker To Go, follow these instructions in the order given.

> Note: For more information on the individual steps, see the cross-references.

1. Create a policy (or open an existing one) that contains the settings related to BitLocker To Go.

   > ✎ Note: Verify that you have licensed BitLocker Management in this policy and that the option is selected in the **Licensed Computers** section.

2. Go to the **Encryption** node in the policy and click the **Settings** sub-node. At first you define the encryption method.

   > ✎ Note: If you do not select anything here, Encryption 2-Go is the default encryption method.

3. Select the option **Available encryption methods for removable drives**.

4. In the dialog box, select **Set to value** and check the **Drive encryption on removable data drives (BitLocker To Go)** option. Save your settings and close the dialog.

5. Open the **Drives** node. Keep the default value **Not configured (locked)** in the **Removable drive locking** settings for **USB bus connected drives**.

6. Open the context menu from the **Drive whitelist rules** sub-node, see the figure below. Select **Drive rule...**.
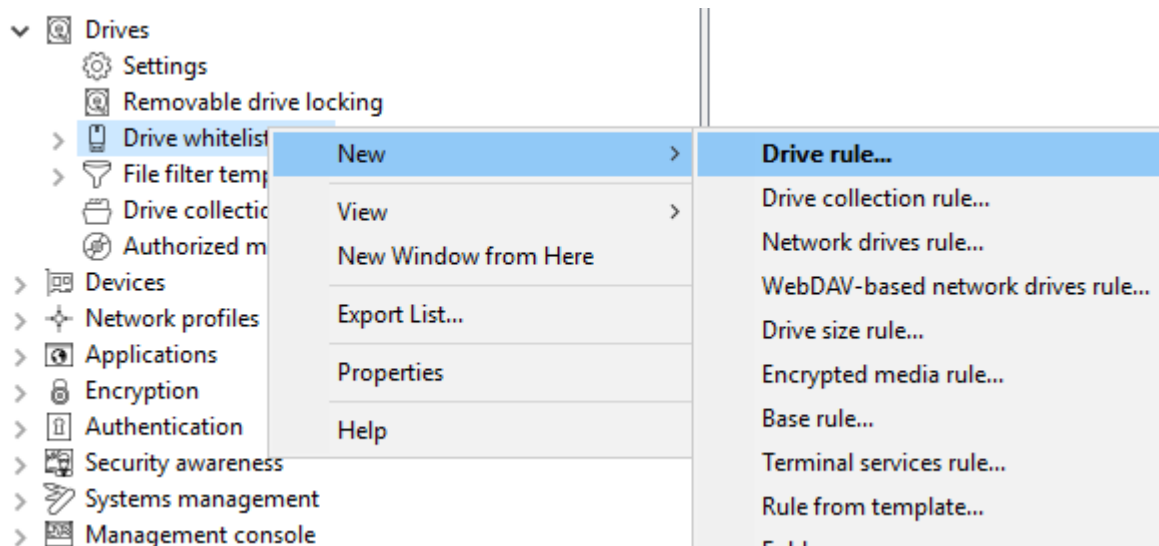
7. Create a drive rule for the corresponding USB drive. To see how this works, click here.

8. Next, open the **Encryption** node again, then the **BitLocker To Go** sub-node and select the option **Encrypted drive recovery** first.

9. Here we have already created two standard rules that cannot be deleted.

- First, open the **Administrative password rule**. Specify a complex administrative password.

- Second, open the rule for **certificate-based recovery**. You will need to specify a certificate, as this is required for recovery. Either create a new certificate or select an existing one. Save your settings and close the dialog.

10. Next, open the context menu of the **Enforce encryption** option, click **New**, and then click **Enforced encryption rule**.
    In the following dialog, enter a description on the **General** tab (the first rule already has the description **Default settings for enforced encryption** in this text field).
    On the **Settings tab**, accept the default settings: **Prompt user for encryption password** and select the option **Attempt to mount using administrative password**.
    This setting ensures that DriveLock can access the administrative password in the background.

11. Last, assign your policy to all or to specific DriveLock Agents.

17.4.3.1 Drive whitelist rules

Please do the following:

1. On the **General** tab, select the USB drive from the list of **Installed drives**.
   In the figure below, this is the USB drive **E:** with the vendor ID **VendorCo**.
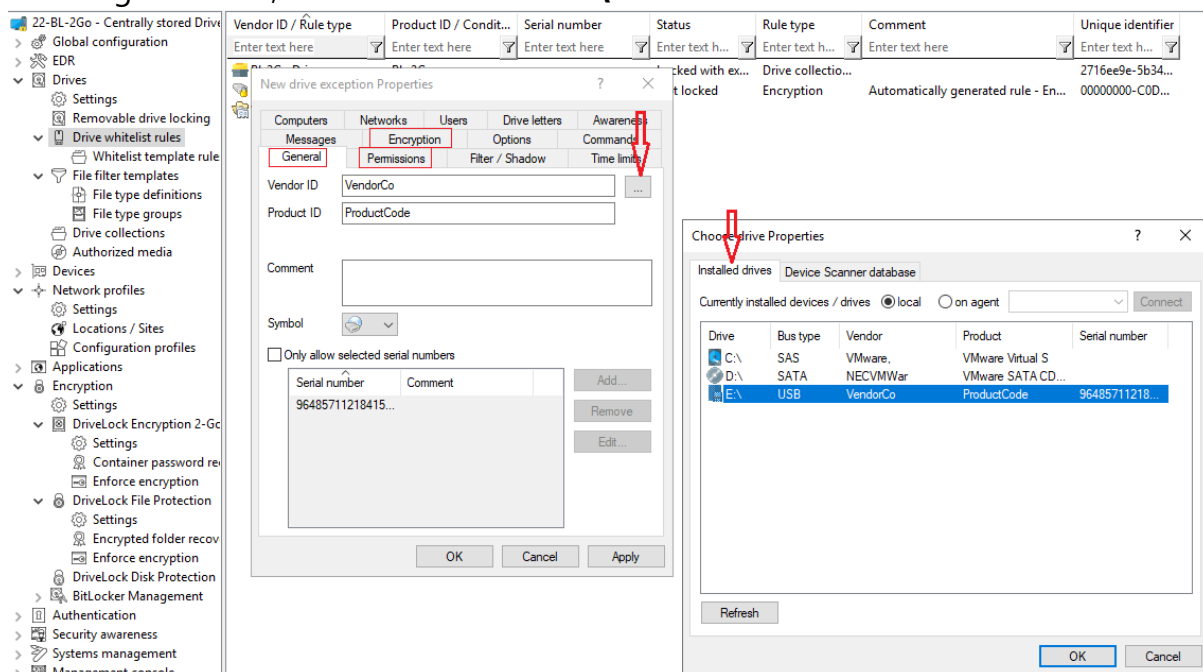
2. On the **Permissions** tab, specify that you want to allow this USB drive.

3. The **Encryption** tab has nothing selected by default.

- Check the **Require drive to be encrypted** option. This will ensure that the con-
nected and allowed USB drive must be encrypted before it can be used.
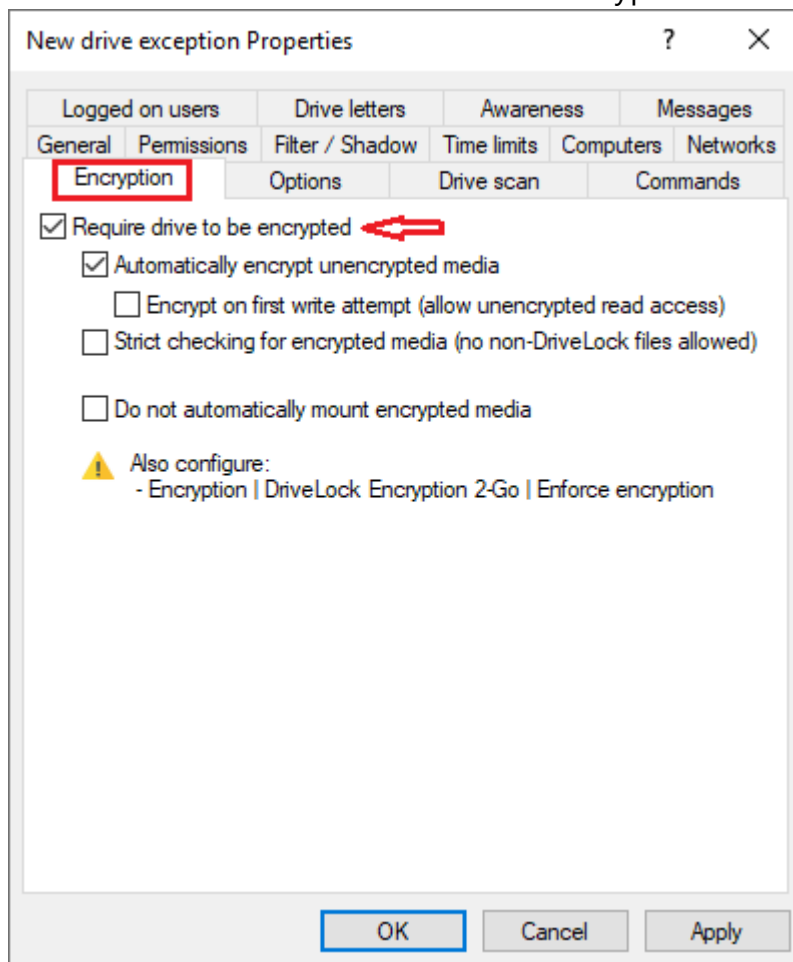
> ✎ Note: This option may have the effect that the access rights are adapted
> to allow the requested behavior.

- Second, check the **Automatically encrypt unencrypted media** option to start
encryption as soon as a user inserts an unencrypted USB drive and to open a wiz-
ard on the DriveLock Agent to guide the user through the encryption process.

- **Encrypt on first write attempt**: Unencrypted drives may be read, but the drive
must be encrypted before writing.

Save your settings and close the dialog.

17.4.4 BitLocker To Go recovery

DriveLock BitLocker To Go provides a recovery procedure which helps users, who forgot or
lost their password, to access their encrypted USB storage device.

The password may be reset even if the client computer is currently not on the corporate network.

This challenge-response procedure is very similar to the one used for temporary offline unlocking of locked drives or devices. DriveLock guides users through the recovery process. Administrators can easily generate the requested response code in the DriveLock Management Console.

17.4.4.1 Recovery procedure

Please do the following:

1. Open the **Operating** node in the DriveLock Management Console and select **Agent remote control**.

2. Select **BitLocker Management recovery** from the context menu and then select **Recovery of encrypted removable media...** .
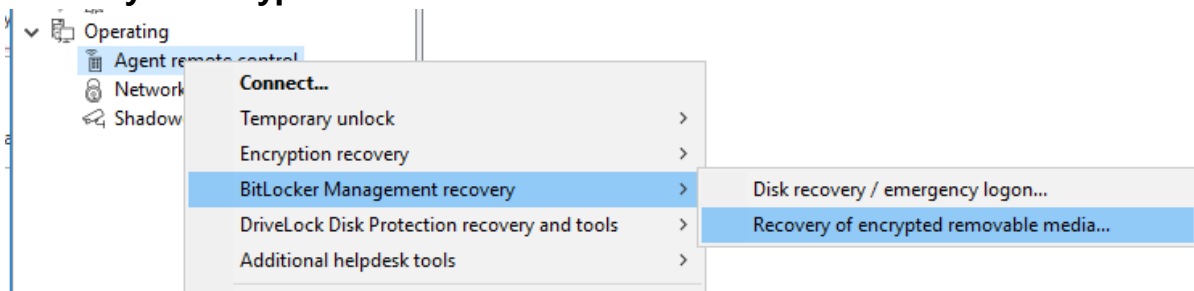
3. In the meantime, the user at the client computer has launched the Recovery Wizard and viewed the **request code**. Ask the user to pass it on to you.

4. Enter the **request code** in the **Encrypted volume offline recovery** dialog, use copy&paste if you wish. The request code is needed to find the information stored on the DES for the encrypted USB storage device. The text field below shows when and by which user the USB storage device was last encrypted.

5. In the next dialog you will see the generated **response code**. Pass it on to the user.

6. Next, the user enters the **response code** on the client computer. In the following dialog the user will specify a new user password for the USB storage device.

17.4.4.2 Recovery in the DriveLock Operations Center (DOC)

You can also restore encrypted USB storage devices with request and response codes from the DriveLock Operations Center (DOC).

Please do the following:

1. Open the **DOC**.

2. In the **Security controls** menu, select **Encryption** and then the **Recovery** tab. Select **BitLocker To Go recovery**.

3. By now, the user on the client computer has launched the Recovery Wizard and retrieved the **request code**.
   Ask the user to pass it on to you.

4. Enter the **request code** in your DOC screen.

5. Select the appropriate **certificate** and the matching password.

6. Click **Generate response code** and share it with the user.

7. Next, the user enters the **response code** on the client computer. In the following dialog the user will specify a new user password for the USB storage device.

17.4.5 DriveLock Agent

17.4.5.1 BitLocker To Go on the DriveLock Agent

When the user plugs in an external USB storage device or external drive to the DriveLock Agent, the following options are available, depending on the policy settings:

1. **Unlocking an encrypted drive**

   To unlock a drive encrypted with BitLocker To Go, a password entry dialog appears immediately. This allows quick unlocking and access to the existing data.
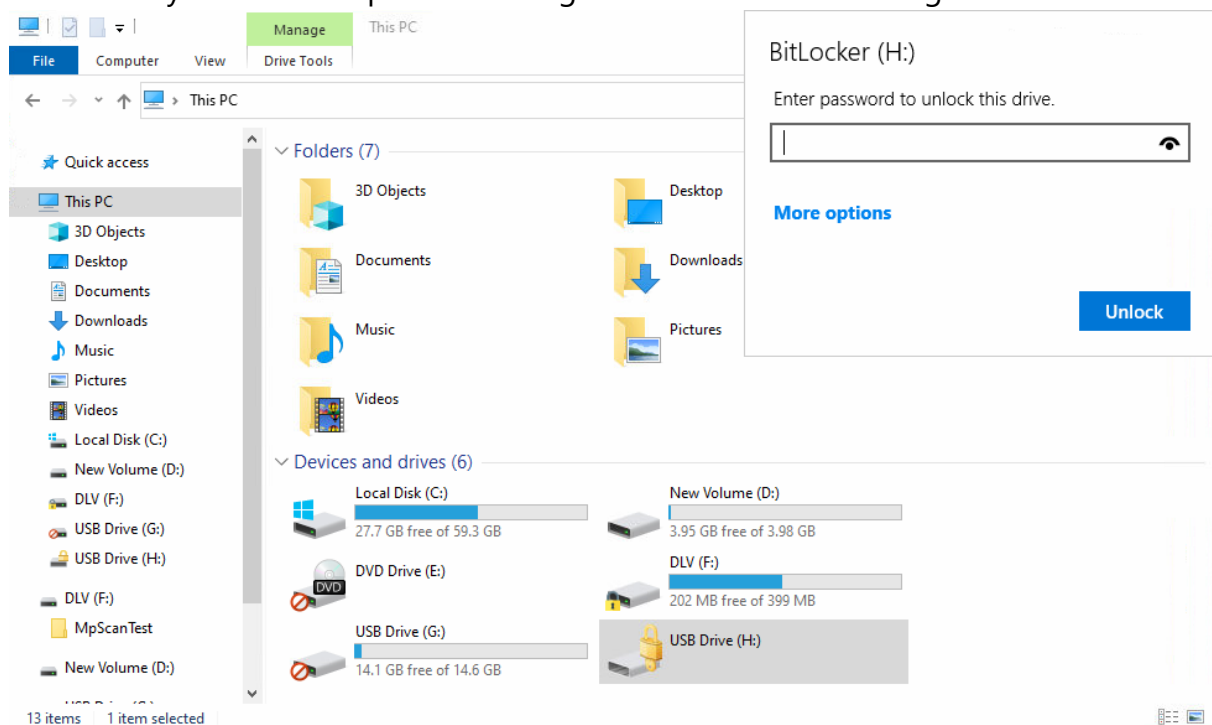
2. **Various options in the context menu in Windows Explorer:**
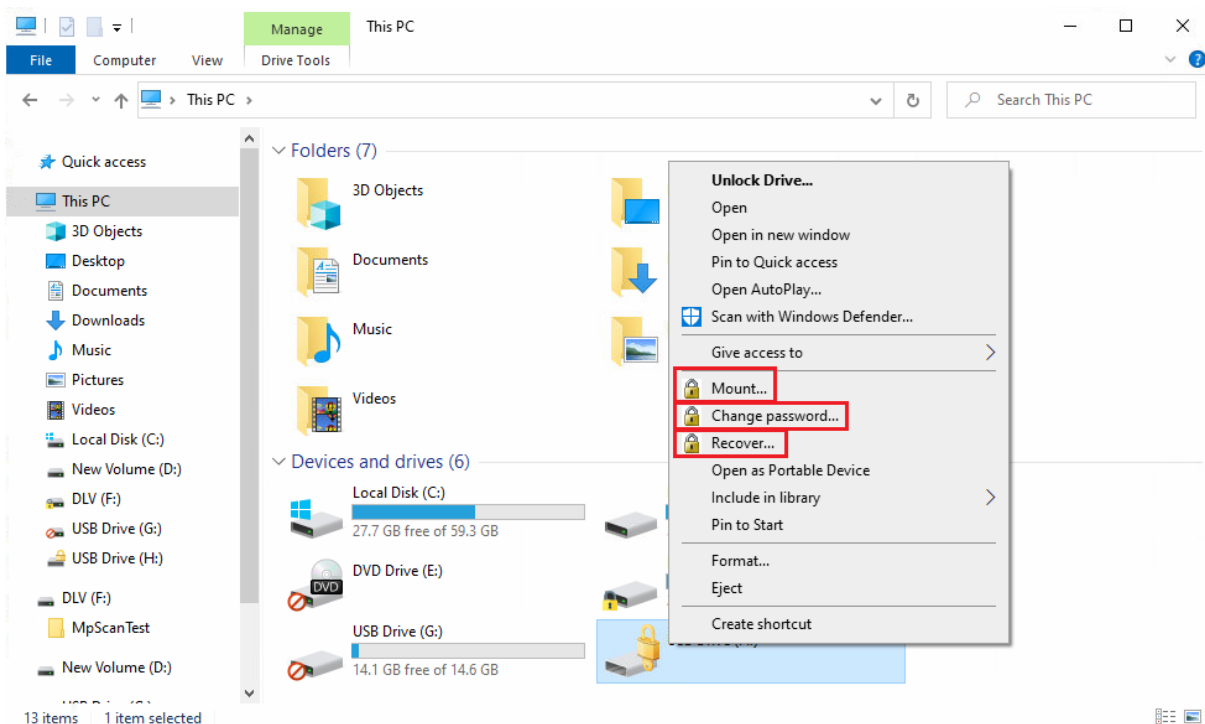
- **Mount...**
  If you want to mount a drive encrypted with BitLocker To Go, clicking this menu item will open a wizard where you can select the appropriate drive letter and enter the password. This option can also be configured so that the password is set as the administrator password and then entered automatically.

- **Change password...**
  To change the password of an encrypted drive, click this menu item. Again, a wizard will open where you can first enter your old password and then your new password.

- **Recover...**
  Use this menu command to restore the password. The recovery process of an encrypted drive takes place between the administrator and the user. For more information, please visit here.

- **Unmount**
  Use this menu command to unmount the drive, even without having admin-

istrator rights.
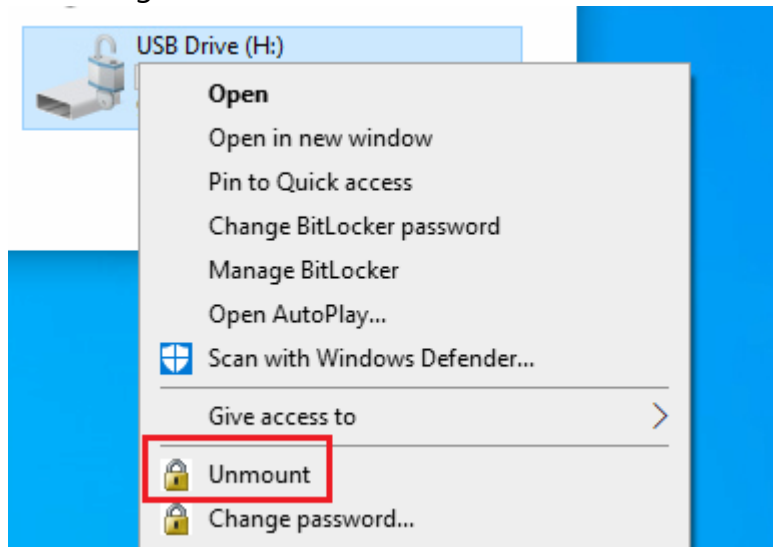
3. **If specified, the different options for BitLocker To Go can also be selected from the taskbar, see the figure below:**
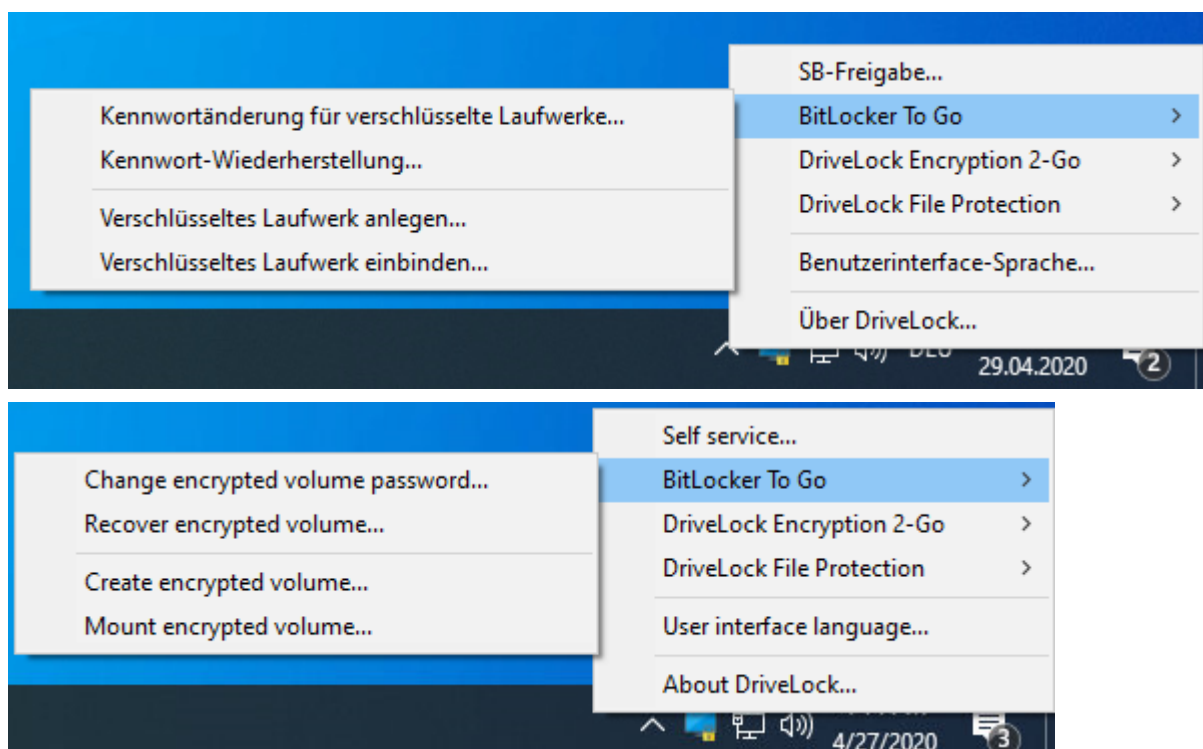
17.4.6 Use cases

Please see the use cases for the following DriveLock BitLocker To Go options:

- Administrative password

- Settings for enforced encryption

17.4.6.1 Administrative password rules

a. **You do not assign an administrative password and allow users to assign a password themselves:**
   - During initial encryption, each user may choose their own password for encryption. An encrypted drive can only be automatically decrypted if you allow the user to save the password. On any other computer it must be entered when connecting.

b. **You assign an administrative password and allow users to assign a password themselves:**
   - During initial encryption, each user may choose their own password for encryption.

   - The administrative password can be used to automatically decrypt data on corporate computers where the DriveLock Agent is running. The user does not have to enter a password.

c. **You assign an administrative password and choose encryption with administrative password:**
   - Users cannot assign their own password during initial encryption.

   - The removable storage device can only be decrypted on corporate computers where the DriveLock Agent is running

   - When connecting the encrypted removable storage device, the user does not need to enter a password

   - Outside the company or on company computers without the DriveLock Agent, the data cannot be decrypted

d. **You create multiple administrator password rules, setting filters for users and/or computers and choosing encryption with administrative password:**
   - Users cannot assign their own password during initial encryption.

   - The removable storage device can only be decrypted on corporate computers where the DriveLock Agent is running

   - When connecting the encrypted removable storage device, the user does not need to enter a password

   - Outside the company or on company computers without the DriveLock Agent, the data cannot be decrypted

- Access is restricted to specific users or to specific computers (e.g. a department or a team):
  You create an administrative password rule that is restricted to user group A. User A1 encrypts a USB stick (forced encryption with administrative password) with administrative password.
  Result:
  The USB stick can only be decrypted if a user from user group A is logged on to a company computer.
  Examples:
    - USB sticks encrypted in the Human Resources department can only be decrypted by the users of the Human Resources department
    - USB sticks encrypted in the Research department can only be decrypted on computers in the Research department

> ⚠ Warning: Pay attention to the priority and filtering options set on the **Logged on users**, **Computers** and **Networks** tabs.

17.4.6.2 Encryption rules

a. **For example, you could choose the user group you want your rule to apply to:**
   - User group A can assign its own password
   - User group B cannot assign its own password

b. **Or you could choose specific company computers you want your rule to apply to:**
   - You do not add an administrative password for USB storage devices that are encrypted on the works council computers.
   - All USB storage devices that were encrypted on the computers in the development department may only be decrypted within the company.

17.5 DriveLock Encryption 2-Go

DriveLock Encryption 2-Go offers secure encryption of external data storage media (such as USB flash drives or SD cards) and secure file deletion using standardized, irreversible procedures.

DriveLock provides two types of encryption for external drives:

- Encrypting drives by creating an encrypted container file, which is then mounted as a new drive in Windows

- Encrypting of all files directly on the connected drive

For security reasons and with regard to compatibility with other operating systems (macOS and Linux), we recommend using the first type.

The DriveLock container file is a file with the extension *.dlv. It can be stored on all types of storage media or on a network share. In order to use a container, DriveLock maps it to a pre-defined or free drive letter so that it can be used just like any other drive within Windows Explorer.

The DriveLock partition is a normal partition that is encrypted by DriveLock. It is possible to encrypt ZIP drives, USB / FireWire hard drives and USB memory sticks, as well as other mass storage devices.

> 📝 Note: Some hardware storage devices do not allow creating an encrypted partition. Please contact the manufacturer of the storage medium for this. You cannot encrypt the drive that contains the Windows operating system files (typically C:\) using this method. You have to use DriveLock Disk Protection to encrypt the system partition as well, if required.

17.5.1 Policy settings

17.5.1.1 Settings

In the Taskpad view, you can configure settings for Encryption 2-Go in the following sections:

- Global settings for encrypting removable storage devices
- Enforced encryption settings
- Configuration of Password recovery for encrypted media

If you click **Advanced Configuration**, all existing settings will be displayed.

17.5.1.1.1 General encryption settings

The general settings for Encryption 2-Go include the following configuration options:

- **Encryption algorithm to be used for encrypted drives**
  Select the encryption method to be used here

- **Password hash algorithm to be used for encrypted drives**
  Select the hash method for the encrypted drives here

- **Method to securely delete files**
  You can specify which method is used so that data is deleted in a secure way.

- **Enforcement of FIPS 140-2 validated cryptography**
  If your organization requires you to use FIPS 140-2 certified algorithms, you can configure it here. When you enable FIPS mode, select one of the following two options:
    - **Off**: Select these settings to also access containers or encrypted drives that have not been encrypted using FIPS 140-2 certified methods. If a user creates a new encrypted container, however, a FIPS 140-2 certified method gets used.

    - **On (disable non-FIPS encryption)** : Use this option if you need to ensure that only FIPS 140-2 certified procedures can be used for both encryption and decryption. Any container or drive encrypted with non-FIPS 140-2 certified methods cannot be decrypted now.

- **Allow quick format of encrypted containers**

467

To shorten the time needed to create an encrypted container, select the **Allow quick format for encrypted containers** option. This means that the DriveLock Agent does not encrypt the entire container, but only the required parts.

- **Minimum required password complexity for encrypted drives**

- **Password complexity policy**
A password complexity policy contains all the requirements that a user password must meet when it is created. This contains the minimum number of characters and the number of special characters that a password must contain.

17.5.1.1.2 Enforced encryption settings

The enforced encryption settings include the following configuration options:

First, select the encryption method to use and configure a hash algorithm.

- Perform Quick format

- **Preserve existing data**: Select this option if you want DriveLock to preserve and encrypt all unencrypted files. DriveLock creates a temporary container in the user's profile on the computer's hard drive, copies all existing files from the drive to this container and then moves this container to the removable drive.

- **Copy DriveLock Mobile Encryption to unencrypted portion**: You also have the option to specify whether the Mobile Encryption application should be copied to removable media during automatic encryption. This allows using it even on computers where DriveLock is not installed.

- **Use complete drive for encrypted container**: Technically, DriveLock needs to calculate the expected maximum size of the encrypted container if the data should be preserved. This may result in some space not being used by the encrypted drive. If you want the container to be able to use all the available space, enable this functionality. In conjunction with this option, DriveLock will fill up all the remaining available space (if available). For this purpose, DriveLock creates hidden system files of appropriate size. If there is more than 2GB of free space, multiple files are created, each no larger than 2GB.

- **Leave unencrypted space on drives**: Select this option if you do not want to use the full space on a drive for encryption. Specify a quantity and define whether the number should be understood as an absolute value or as a percentage value.

17.5.1.1.3 Password recovery settings

This section describes the two configuration steps necessary to be able to reset the password later if required for an encrypted container (for example, a force-encrypted USB stick). In order to use the offline password recovery functionality, you must generate a master certificate consisting of a public and private key pair before creating the first encrypted container.

To do this, click **Create new recovery certificate**. This will start the wizard for generating the main certificate.

Either specify the folder where you want to save the certificate file or, alternatively, choose a smart card as the location.

You can additionally save the certificate and password on the server so that they can be used by the DOC without the file having to exist locally.

Then follow the instructions here from step 3.

17.5.1.1.4 Advanced settings

Below is an overview of all available settings for Encryption 2-Go.

Setting	Functionality
Encryption strength settings	
Enforcement of FIPS 140-2 validated cryptography	Activate the FIPS mode with this setting.
Encryption algorithm to be used for encrypted drives	Configure the encryption algorithm to be used.
Password hash	Specify the hash algorithm here.

Setting	Functionality
algorithm to be used for encrypted drives	
Allow quick format of encrypted containers	Define here if you want to allow the quick format.
Password strength settings	
Minimum required password complexity for encrypted drives	The minimum required password complexity for encrypted drives should be defined to meet company policy. The complexity is calculated based on the characters used as well as the password length.
Password complexity policy	A password complexity policy contains all the requirements that a user password must meet when it is created. This contains the minimum number of characters and the number of special characters that a password must contain. DriveLock can also deny a user password if it occurs in a dictionary.
Container access lockout policy	The lockout policy helps prevent brute-force attacks by locking a container for a specified number of minutes or forever after a defined number of attempts to enter a password.
Encrypted container password saving options	The saved password is automatically used when mounting from this container. This helps with long and complicated passwords.
Allow generation	An additional option is displayed in the creation wizard that

Setting	Functionality
(and display) of random passwords for new containers	allows users to generate random passwords.
Allow and show option to send passwords for new containers using text messaging	When enabled, this option generates an additional wizard page when creating containers and allows passwords to be sent via text message (SMS). The SMS gateway required for this is configured in the **Global configuration** under **Settings** in the **configuration settings for text messages (SMS)**. For more information, please click here.
Default text for sending passwords using text messaging	Sets the default text for sending passwords via text message.
Password recovery settings	
Encrypted volume password recovery methods	DriveLock provides two methods for recovering lost passwords for encrypted containers: • Offline recovery using a challenge response method: A wizard guides you through resetting the password of an encrypted container, even if the computer is not currently connected to the corporate network. • Online recovery through locally installed certificates: If this option is enabled, a password can also be reset without a challenge-response method, provided that the required certificate with private and public key pair is available locally

Setting	Functionality
	on the corresponding computer.
User contact information for offline container recovery	If the user forgets their personal password for accessing the container or encrypted drive, they can use the icon in the taskbar or the Start menu to launch the Password Recovery Wizard. You can specify the text that appears at the beginning of the wizard here.
Encryption user experience	
Context menus available in Windows Explorer	These settings define all the options available from the context menu. The "Not configured" setting activates all options
Start menu configuration	You can define whether the DriveLock Start menu items are displayed and how they are arranged.
Available Start menu items	This option defines the start menu items to be displayed
Menu items available from the taskbar icon	You can define whether all menu items are displayed when using the taskbar icon
Order of menu items in taskbar icon	You can define in which order the menu items are displayed when using the taskbar icon.
Bring all dialogs to top-most position	Specify whether dialogs can be hidden.

Setting	Functionality
Encrypted drives settings	
Encrypted drive file system	The file system for new encrypted drives can be FAT, exFAT or NTFS.
Encrypted drive cluster size	Set the cluster size for encrypted drives here.
Available drive letters for mounting encrypted drives	Configure the drive letters that are automatically assigned to encrypted drives here
Enforce drive letter when mounting encrypted drives	By enabling this setting, only an encrypted drive can be connected to the defined letter
Restrict size of user created drives	Specify a value that indicates the maximum size of encrypted containers.
End user restrictions	
No history for mounted volumes	This option prevents creating history of connected volumes.
Do not allow creation of DriveLock Mobile Encryption Disks	The Mobile Encryption Application (MEA) is required to decrypt data on a computer that does not have DriveLock Agent installed. DriveLock can copy the MEA to a drive along with an autostart file if an encrypted container file is placed on it. Disable this option if you do not want the user to be able to do

Setting	Functionality
	this.
Only allow encrypted containers created with current DriveLock license	If you enable this option, DriveLock will only be able to open containers encrypted by an agent with the same license as the one currently configured
Do not allow opening encrypted containers with DriveLock Mobile Encryption	The Mobile Encryption application is used to decrypt encrypted drives or containers even on systems where DriveLock is not installed.
Do not automatically update DriveLock Mobile Encryption to newer version during enforced encryption	Normally, when you try to connect, DriveLock checks whether the MEA present on a removable disk is the current version and, if necessary, automatically replaces it with the latest version

17.5.1.2 Recovering encrypted containers

In case a user forgets the password to access an encrypted container file or this password is no longer available for other reasons, DriveLock Encryption 2-Go provides two recovery mechanisms.

1. Offline recovery of encrypted containers works in the same way as disk recovery in BitLocker To Go.
   - The password may be reset even if the client computer is currently not on the corporate network.
   - This challenge-response procedure is very similar to the one used for temporary offline unlocking of locked drives or devices. DriveLock guides users through the

recovery process. Administrators can easily generate the requested response code in the DriveLock Management Console.

2. The online recovery process requires the encryption certificate on the DriveLock Agent, a challenge-response process is not needed in that case.

17.5.1.2.1 Administrative password

Encrypted container files can be accessed using a central administrator password.

> Note: Ensure that the administrative password is complex enough.

In addition to the central password, you can also create additional administrative password rules and prioritize them differently. By using different passwords, you can provide increased security.

To create a new administrator rule, open the context menu of **Encrypted drive recovery** and then select **Administrative password rule**.

You can restrict the password rules for certain **logged on users** or user groups, **computers** or **networks**. Enter the required information on the tabs in the dialog. See the use cases for BitLocker To Go, that apply equally to Encryption 2-Go.

Use the **Do not automatically use this password when a user mounts encrypted containers** option only if this rule is used within a user selection rule.

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

- **With any type of encryption** - This identifier is always used.

- **Encryption by users (using command line or GUI)** - This identifier is used only when encryption is performed by a user via command line or through DriveLock's user interface.

- **Enforced or automatic encryption** - This identifier is used only when encryption is performed automatically by DriveLock.

17.5.1.2.2 Certificate-based container recovery

Before creating an encrypted USB storage device, select a master certificate consisting of a public and private key pair.

You can either create a new certificate or use an existing one. For more information, see the Password recovery settings chapter.

You can also create multiple recovery rules with different certificates, which can be restricted and prioritized differently via the Computers, Logged on users, Networks tabs. This is useful if you want to allow different users to restore encrypted data.

> ☑ Note: Use the standard recovery certificate (lowest priority) as a minimum.

No other information is required in this dialog.

17.5.1.3 Enforced encryption (Encryption 2-Go)

Before being able to encrypt USB data storage devices automatically (enforced encryption), you need to configure some basic settings. These include the encryption algorithm and other general conditions, for example how existing data can be transferred from an unencrypted drive during encryption or how large the encrypted area will be. You can create different rules for specific users or computers, or, for example, rules that are applied only to specific network connections.

Up to three different rules can also be combined into one user selection, if required. It is displayed to the user (e.g. when plugging in a USB flash drive) and the user then selects one of the available options.

Examples:

- All USB flash drives shall be encrypted with AES.

- Only the USB sticks of the Executive Board shall be encrypted with AES (FIPS-mode).

- The user is to decide whether to encrypt the entire flash drive or only 50% of the available capacity.

- The user may select one of two options, for example 'Encrypt USB drive completely' or ' Use drive without encryption for read-only after confirming a security notice'.

17.5.1.3.1 Encryption methods

Encrypted drives are organized as individual container files. Access to these files is password protected. Additionally, DriveLock offers the possibility to reset the password offline.

Encrypted data appears to consist of random letters and numbers. File and directory names are also encrypted within an encrypted drive, as is free space. The encryption method defines the way in which data is encrypted on the respective drive.

On current systems, encryption and decryption is carried out using encryption methods implemented in Open SSL:

- AES (Advanced Encryption Standard) is recommended

- You can also select other encryption algorithms in the DriveLock dialogs: Triple DES, Blowfish, Twofish, CAST 5 and Serpent.

DriveLock applies a hash algorithm to encrypt the password that is used to encrypt or decrypt the encrypted drive. DriveLock supports the following **hash algorithms**:

- SHA-256 and SHA -512 are recommended (both also as FIPS version)

- Additional hash algorithms are available in the DriveLock dialogs: RIPEMD-160 and WHIRLPOOL

17.5.1.3.2 Encryption rule

The default enforced encryption rule is always available. If required, you can create additional rules for specific logged on users, groups, computers or networks. See some use cases that apply in the same way to BitLocker To Go.

To create new rules, select **New** and then **Enforced encryption rule...** in the **Enforce encryption** subnode.

The options on the General, Settings, Encryption and File system tabs can be found in separate chapters.

17.5.1.3.2.1 Encryption methods

Encrypted drives are organized as individual container files. Access to these files is password protected. Additionally, DriveLock offers the possibility to reset the password offline.

Encrypted data appears to consist of random letters and numbers. File and directory names are also encrypted within an encrypted drive, as is free space. The encryption method defines the way in which data is encrypted on the respective drive.

On current systems, encryption and decryption is carried out using encryption methods implemented in Open SSL:

- AES (Advanced Encryption Standard) is recommended

- You can also select other encryption algorithms in the DriveLock dialogs: Triple DES, Blowfish, Twofish, CAST 5 and Serpent.

DriveLock applies a hash algorithm to encrypt the password that is used to encrypt or decrypt the encrypted drive. DriveLock supports the following **hash algorithms**:

- SHA-256 and SHA -512 are recommended (both also as FIPS version)

- Additional hash algorithms are available in the DriveLock dialogs: RIPEMD-160 and WHIRLPOOL

17.5.1.3.2.2 General tab (Encryption rule)

When editing the first encryption rule, a description is already entered on the **General** tab. For a new rule, enter a description.

- Add a comment and your own text, which is displayed in the user selection dialog. You can also select a previously configured multilingual notification at this point.

- If you want to use the encryption rule in a User selection rule, you need to select the **Do not automatically use this rule** checkbox.

17.5.1.3.2.3 Settings tab (Encryption rule)

On the **Settings** tab you can use the default settings or select the following options:

- **Use administrative password. Don't prompt user**: If you enable this option, the storage device will be encrypted with the administrative password only. Users are not prompted to enter their own password during encryption.

- **Prompt user for encryption password**: This setting prompts the user for their own password.

- **Attempt to mount using administrative password first**: Initially, the user is not asked for their own password. The user will only be prompted for their own password if DriveLock cannot load the storage device automatically, for example, when the administrative password does not match.

> Note: This option requires that you have set an administrative password in the **Encrypted drive recovery** rules.

- **Disable any administrative password for new drives**: Once a user has set a personal password, the administrative password is deleted when encrypting the USB

storage device. This means that the encrypted data can only be accessed by entering the user password.

- **Users can disable administrative password for new drives**: Select this option to allow users to create "private" USB storage devices without using the administrative password.

- **Use entire drive for encrypted container**: DriveLock uses the full available disk space for encryption. When a drive contains data that will be encrypted, DriveLock needs to estimate how much space is available for the encrypted container when it will be copied to the removable drive. This may result in some space not being used by the encrypted drive.

- **Fill any remaining empty space on drives**: Select this checkbox to have DriveLock fill this remaining space to ensure that users can't inadvertently copy data to the unencrypted space when using the drive on a computer where encryption is not enforced. DriveLock creates a hidden system file sized appropriately for this purpose.

- **Leave empty space of x KB**: In some Windows 7 environments a few kilobytes of space must remain available for the operating system to access a drive.

- **Leave unencrypted space on drives**: Select this option if you do not want to use the full space on a drive for encryption. Specify a quantity and define whether the number should be understood as an absolute value or as a percentage value.

- **Maximum size of encrypted container x MB**: Here you can define the maximum size of the encrypted container.

17.5.1.3.2.4 Encryption tab (Encryption rule)

On the **Encryption** tab, specify the encryption and hash method, file system and cluster size of the container that is then mapped as an encrypted drive.

- **Encryption**: Select the appropriate encryption method.

17.5.1.3.2.5 Volume creation tab (Encryption rule)

The information on the **Volume creation** tab relates to the hardware of the drive to be encrypted:

- **Keep existing data**: Select this option if you want DriveLock to keep and encrypt all unencrypted files. DriveLock creates a temporary container in the user's profile on the computer's hard drive, copies all existing files from the drive to this container and

then moves this container to the removable drive. You can also specify that this temporary folder is created in a place you specify (option "Use custom local temporary folder during volume creation").

- **Copy DriveLock Mobile Encryption to unencrypted part**: You also have the option of specifying whether the Mobile Encryption Application (MEA) should be copied to removable media during automatic encryption. This allows using it even on computers where DriveLock is not installed. In addition, an Autorun.inf file can be created, in which user-specific contents can also be configured.

- **Use custom local temporary folder during volume creation**: If you want to transfer existing data on the flash drive, you can specify a directory here to create the directory with the temporary container.

- **Hide encrypted container file**: If this option is enabled, the EEDATA.DLV file will be marked as "Hidden".

- **Automatically reformat file systems that support no more than 4 GB to exFAT or NTFS**: This setting only affects the file system of the connected device due to the file size restrictions of FAT/FAT32 to < 4 GB. For this reason, USB sticks are automatically reformatted to exFAT or NTFS to ensure maximum utilization of the storage space for the container file.
  Use quick format: Quick formatting is used by default.

> 📝 Note: The MEA now supports exFAT-formatted containers for read and write access on all supported operating systems (Windows, macOS and Linux)

17.5.1.3.3 User selection rule

The settings in this rule determine the appearance of a dialog that is displayed when a user connects a drive and which encryption rules a user can select in this dialog box.

Example of what a user selection dialog might look like:
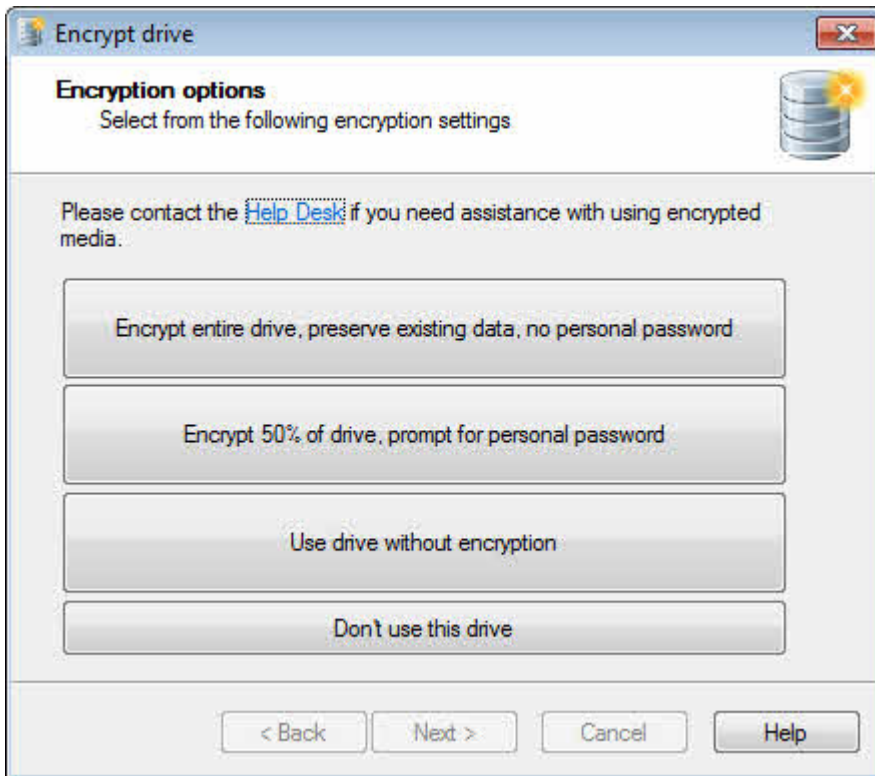
To create it, select **New** and then **User selection rule...** in the **Enforced encryption** sub-node.

On the **General** tab, enter a description and, if necessary, a comment.

On the **Messages** tab you define the texts that will then appear in the user selection dialog. Here you can configure the title, subtitle and help text elements. You can enter all texts either directly or select a multilingual notification message you defined earlier.

On the **Selectable rules** tab you can configure up to three previously created encryption rules using the **Add** button. The order in which you add the rules determines the order in which they will be displayed in the selection dialog box.

- If you enable the option **Allow selection of 'Access volume without encryption'** and the user selects this option, the user will have full read and write access to the drive even if the applicable drive locking rule grants no access or only read access. When enabling this option it is recommended to also select the "Show usage policy before unlocking the volume" checkbox to display a usage guideline to the user before access to the drive is granted.

- In contrast, the last option **"Do not add drive access as selection** " represents the "Cancel" button. If the user chooses this selection option, the drive will be mounted according to the access permissions configured in the drive whitelist rule. The same permissions are also used if the user exits one of the encryption wizards early.

17.5.2 Offline recovery process

1. Open the **Operating** node in the DriveLock Management Console and select **Agent remote control**.

2. Select **Encryption recovery** from the context menu and then select **Recovery of encrypted containers...** :

3. By now, the user on the client computer has launched the Recovery Wizard and retrieved the **request code**. Ask the user to pass it on to you.

4. Enter the **request code** in the **Encrypted volume offline recovery** dialog, use copy&-paste if you wish. The request code is needed to find the information stored on the DES for the encrypted USB storage device. The text field below shows when and by which user the USB storage device was last encrypted.

5. In the next dialog you will see the generated **response code**. Pass it on to the user.

6. Next, the user enters the **response code** on the client computer. In the following dialog the user will specify a new user password for the USB storage device.

17.5.3 Online recovery process

> Note: Online recovery is only possible if a corresponding local certificate is present on the DriveLock Agent and the Agent is connected to the corporate network.

The end user on the DriveLock Agent performs the following steps in the Recover encrypted volume password wizard:

1. Select recovery method
   The end user selects the **Recover online (...)** option here.

2. Specify recovery certificate

    The user will either provide the path to the certificate file along with the correct pass-
    word or refer to a smart card or the certificate in the certificate store.

3. Enter new password

    A new password can then be assigned in the last dialog.

17.5.4 Recovery in the DriveLock Operations Center (DOC)

You can also restore encrypted containers with request and response code via the DriveLock Operations Center (DOC).

Please do the following:

1. Open the **DOC**.

2. Select the **Operation** section and here from the **Restore** submenu, select the **Encryption 2-Go Restore** tab.

3. By now, the user on the client computer has launched the Recovery Wizard and retrieved the **request code**.
   Ask the user to pass it on to you.

4. Enter the **request code** in your DOC screen.

5. Select the appropriate **certificate** and the matching password.

6. Click **Generate response code** and share it with the user.

7. Next, the user enters the **response code** on the client computer. In the following dialog the user will specify a new user password for the USB storage device.

17.6 DriveLock File Protection

DriveLock File Protection provides transparent and automatic encryption across all files and folders. Users working with the files do not 'notice' that they have been encrypted, meaning that the encryption and decryption process takes place automatically in the background whenever a file is being accessed.

File Protection includes:

- File encryption on local computers, central directories on a server, external USB data carriers or cloud-based services (e.g. Microsoft OneDrive, Google Drive)

- Authentication when accessing encrypted directories with user name/password or via X.509-based certificates

- Integrated Public Key Infrastructure (also independent of AD)

DriveLock had already introduced a new encryption format with version 2022.2, which was applied to new DriveLock agents by default. The old format could be retained for existing agents. The DMC has a specific policy setting that allows you to automatically select which format is used or whether both formats are used simultaneously starting with version 2023.2. However, different encryption formats can be defined if required.

Functionality

Every time a folder is being accessed, DriveLock checks whether it is an encrypted folder for all computers where DriveLock File Protection is active. When such a folder is detected, the current user's permissions are validated and encryption or decryption is automatically performed in the background as files in the folder are accessed.

You can exempt specific processes, such as backup programs or file synchronization operations, from the automatic encryption and decryption. This prevents any impact on existing system maintenance routines.

Management of the folders can either be performed centrally for each individual folder via the DES or independently of the DES.

To authenticate users, DriveLock File Protection can use the following two methods:

- Passwords: To access files in an encrypted folder, a user must provide a password.

- Certificates: Authentication uses a certificate from the user's certificate store in Windows or from a smart card or token.
  Click here for further information on how to create certificates.

> ☑ Note: When using centrally managed folders, the only way to authenticate is via certificates.

Before you start using DriveLock File Protection, please consider the following points:

- Do you want to use centrally managed folders?

- Do you want to use user certificates or passwords for authentication?

- How do you want to issue user certificates, if required?

- What settings will apply to the encryption and decryption of data?

- What file protection options are available to the user on their computer?

- What will be the folder structure that you will use for storing encrypted data and files?

17.6.1 Policy settings

The settings for file encryption and decryption and the behavior of DriveLock File Protection on the client computer are made in DriveLock Policy Editor.

Here you can set the following settings:

- Configuring encryption settings

- Configure the encryption user interface

- Configure settings for encrypted folders

- Configure additional settings

- Create encryption certificate

- Use forced encryption

- Specify forced encryption

17.6.1.1 Configuring encryption settings

To configure the encryption settings, click the **File Protection** node, and then click **Settings**.

The following options are available:

- **Encryption algorithm for encrypted folders**: Here you specify the algorithm to be used for encryption and decryption.

- **Hash algorithm for passwords for encrypted folders**: Select the algorithm to be used for creating password hashes.

- **Minimum password complexity for encrypted folders**: The minimum required password complexity for encrypted drives should be defined to comply with company policies. The complexity is calculated based on the characters used as well as the password length. If you want to create your own password complexity policy, select "Password complexity policy" and then configure it.

- **Password policy**: If your policy requires the use of characters that may be both a number and a special character, enable the **Treat numbers as special characters** option and specify the number of characters required.
A dictionary can be a dictionary file in the OpenOffice format or a text file that contains a single word on each line. DriveLock includes OpenOffice dictionaries for English, German, Dutch and French. You can find these .diz-files in the DriveLock installation folder on the administration computer where you installed the DriveLock Management Console (for example "DictEnglish.diz").

> ⚠ Warning: If you specify a custom file, ensure that this file exists on all Agent computers in exactly the same location, as the Agents looks for this file in the location you specify.

You can also add the file to the policy file storage. To do this, select "Policy file storage..." and the corresponding file. Files located in the policy file storage are identified by an asterisk ("*") in front of the file name and are copied to the client automatically.

> ⚠ Warning: When you use a dictionary to validate your passwords, keep in mind that passwords containing any part of a word contained in the dictionary are not allowed (for example if the dictionary contains "it", passwords such as "hit", "with" or "glitter" are not allowed).

17.6.1.2 Configuring the encryption user interface

To configure the settings for the encryption user interface, the following options are available:

- **Available context menus in Windows Explorer**: To set the available context menu items that a user will see after right-clicking on an encrypted directory, click Set to fixed value and select from the three options. If Not configured is selected, all entries will be displayed.

- **Start menu items configuration**: To configure where menu items that are available to users appear on the Windows the DriveLock taskbar icon, click Set to value and then select the items that will be available. If Not Configured is selected, the entries

are displayed under All Programs / DriveLock File Protection.

- **Available Start menu items** : To set the available Start menu items that a user will see after clicking the Windows Start icon, click Set to value and select among the options. If Not configured is selected, all entries will be displayed.

- **Menu items available at taskbar icon**: To set the available taskbar icon menu items that a user will see after right-clicking the DriveLock taskbar icon, click Set to value and select among the options. If Not configured is selected, all entires will be displayed.

- **Order of menu items in taskbar icon**: To set the order of available taskbar icon menu items that a user will see after right-clicking the DriveLock taskbar icon, click Set to value. To change the order of the menu items, select an item and then click Up or Down. To remove an item, select it and then click Remove. To add a separator line, click Add. When this option is set to Not configured, the items are displayed in the default order.

- **User Contact Information for offline recovery**: To set the text that a user will see after right-clicking the DriveLock taskbar icon and selecting the "Restore encrypted folder" option, click Set to value and enter the required text in the text box. If Not configured is selected, no text is displayed. If Not configured is selected, no text is displayed.

- **Format for user display names**: To configure the format in which user names are displayed when administering permissions for encrypted folders, click Set to value and select among the options. If Not configured is selected, the users are displayed in the format [Last name], [First name].

- **Do not show popup messages automatic folder mounting**: To disable the display of popup messages when connecting to encrypted folders, click Enable. If Not configured or Disabled is selected, pop-up windows are displayed.

- **Encrypted folder password saving options**: Select whether and how users are allowed to save passwords of encrypted folders. You can deny saving, allow saving, or allow saving for the current session only. If you select current session only, the password will be deleted, when the user logs off, but it will be valid for all folders secured with the same password. This eases working with multiple encrypted folders keeping security high.

17.6.1.3 Configure settings for encrypted folders

The following options are available to configure the settings for encrypted folders:

- **Available recovery procedures for encrypted folders**: To specify which recovery options are available to a user, click Set to Fixed Value and select among the options. If Not configured is selected, all options will be displayed.

- **Interval between certificate revocation checks**: To set the period of time during which no rechecking of the user's certificate for a successful revocation of the same will take place, click Set to Fixed Value and select among the options. If Not configured is selected, the interval is 24 hours.

- **Access to files in encrypted folders**: To specify how DriveLock File Protection should respond when a user does not have permission to encrypt / decrypt, click Set to Fixed Value and select among the options. If Not configured is selected, access to the directory is denied. The following options are available and respond as follows:
  - **Deny**: Users without permissions cannot access the directory, even if they had appropriate Windows permissions. The Windows message "Access denied" appears.
  - **Allow for administrators**: Users without permissions can access it only if they belong to the group of administrators

> ⚠ Warning: If access is enabled without permissions, the directory responds like a normal Windows directory, meaning that files are not decrypted when opened, but are not encrypted when written either. For authorized users, however, DriveLock File Protection always assumes an encrypted file within an encrypted directory and would also decrypt an unencrypted file, which means that an authorized user cannot do anything with this file and may render it completely unusable when writing.

- **Automatically connect encrypted folders**: To specify how DriveLock File Protection should respond when connecting encrypted drives, click Set to Fixed Value and select among the options. The On option applies if Not configured is selected (show dialog if required). The following options are available and respond as follows:
  - **On (show dialog if required)**: DriveLock File Protection attempts to connect the folder using the user certificate present in the certificate store or a previously saved password. If the user does not have authorization or the password is not correct, a window opens and the user can select an authentication method. This option is useful if passwords are not allowed to be stored, or user certificates are not stored in the Windows certificate store but on external media such as smartcards or tokens.
  - **Display only fully automatic, no dialogs**: DriveLock File Protection tries to connect the folder using the user certificate present in the certificate store or a

previously stored password. If the user does not have authorization or the password is incorrect, the user will be considered as not authorized.

- **Off**: There is no automatic connection to an encrypted directory. The user will be considered an unauthorized user until he right-clicks on the directory and selects the Connect Encrypted Folder menu item.

17.6.1.4 Configure additional settings

Following additional options are available:

- **Files and folders excluded from automatic connection**: To specify directories where DriveLock should not attempt an automatic connection, click Set to Fixed List and edit the list of required directories or files using the Add, Delete and Edit buttons.

- **Backup program names (with access to encrypted files only)**: To specify programs that must have access to encrypted directories even without permission, click Set to Fixed List and edit the list of required programs using the Add, Delete and Edit buttons Enter the entire program name without the path (e.g. backup.exe). Dropbox, OneDrive and Google Drive programs are already included by default.

> Note: Long file names are not supported by the driver to recognize backup programs. Instead, specify the first seven characters, e.g. BACKUP.EXE but MYBACKU for MyBackupBackupAndRestore.exe.

- **Files on network shares for which file region locks are not modified**

  If File Protection is active, locks on file regions for files on network shares are extended to larger regions than requested by the program (because data is encrypted in blocks and therefore more data is affected by a change in the encrypted file than in plain text). This can lead to problems with programs that do not request locks on file regions to secure their file access, but use this mechanism for communication.
  You can use this setting to specify the files for which the restricted regions should not be extended.
  Example: `\\server\share\**\*.lock` would exclude files with the extension "lock" on a specific network share from this mechanism.
  Please note that servers sometimes respond to more than one name. If the share name is already unique, you can also use wildcards `\\*\share\**\*.lock` instead of listing every spelling of the server name
  The evaluation of the names or wildcards works in the same way as with Application Behavior Control rules.

17.6.1.5 Applied encryption format

The new format used for encrypted files is the basis for DriveLock File Protection's future development.

This setting allows you to actively choose between the old or the new format for your DriveLock agents. When you reinstall DriveLock Agent on your clients and enable File Protection, the new format is automatically used. If you have already deployed File Protection on your agents and folders are already encrypted there, you should continue to use the old format.

> ☑ Note: Please note that both formats can be used simultaneously for agents from version 2023.2. For agents with version 2023.1, only either the old or the new format can be used.

The following options are available as fix adjustable values:

- **Automatic (default)**:
  Depending on the existing version on the agents, DriveLock uses the new or the old format (for agents with version 2023.1) or both formats simultaneously (agents from 2023.2).

- **New format**:
  Use this option if compatibility with encrypted folders in the old format is not required.

- **Old format**:
  Use this option if you only want to work with the old format.

  > ☑ Note: Please note that this option must not be used for agents with version 2023.1.

- **New format (reduced functionality)**:
  This option restricts the new format, for example, hiding files will not work in this case. In addition, mounting is impossible when accessing encrypted folders. Use this option only if you have problems with the new format.

- **Old format (legacy mode)**:
  Use this option if you have problems with the old format or if your agents still have version 2023.1.

The two lower settings are only fallback options.

> Note: Please also note that the **Old format** and **Old format (legacy mode)** encryption formats do not support the Distributed File System (DFS).

17.6.2 File Protection users

A File Protection user is required so that users can easily be authorized to access folders without having to pass on passwords. This is achieved by maintaining a user list on the DES where a certificate is stored for each user. To grant access permission to a folder, the user can simply be selected from the list. The access information for this folder is automatically encrypted with the user's certificate. The folder can then be accessed directly without having to perform any further steps.

To be able to use File Protection users, the certificates for users must first be distributed.

Afterwards, you can create and manage the users.

17.6.2.1 Distributing certificates for users

Each time an encrypted folder is accessed, DriveLock File Protection checks whether a user certificate is available in the user's certificate store and whether it can be used for automatic authentication.

The public key infrastructure (PKI) normally used for managing user certificates is not necessary for DriveLock File Protection if you create the certificates via DES.

> Note: If your organization already has an existing PKI and uses it to issue user certificates, you can use this PKI to authenticate users for DriveLock File Protection.

The following options are available for managing user certificates:

- Certificates are managed by the user - a personal (self signed) certificate can be created using the DriveLock Application.

- Certificates are administered using DriveLock. The Certificates (public key) are stored by DriveLock in a database.

- User certificates are managed in an existing PKI in Microsoft Active Directory outside of DriveLock

- User certificates are administered in a third-party Windows compatible-environment without any involvement by DriveLock

17.6.2.1.1 Creating certificates via the Active Directory

In order to be able to encrypt and manage a network drive (UNC path) centrally with DriveLock File Protection, some preparations must be made in Active Directory.

The encryption is based on user-based certificates (EFS certificates). It is necessary to create them for each user at the beginning. The Active Directory is the ideal central issuer for certificates.

Active Directory Certificate Services: Distribute certificates with group policies

An Active Directory-integrated CA provides the ability to automatically distribute certificates to users or computers via group policies. In the following, auto-enrollment is configured by a duplicated certificate template **Basis-EFS**. This is used to encrypt folder contents.

The following steps must be performed in the process:

1. Duplicating the certificate template

2. Issuing the template

3. Creating a group policy

4. auto enrollment and policy activation

5. Testing the automatic enrollment

> 🛑 Warning: Once user certificates have been created and collected by the DriveLock AD inventory, you can define File Protection users in the DOC. Please note that these certificates can only be collected by DriveLock Agents with version 2024.1 and higher.

You can find a use case here.

17.6.2.1.1.1 Duplicating the certificate template

To duplicate the certificate template, follow these steps:

1. On the CA server, open the Certificate Template Console **certtmpl.msc** and right-click **Basis-EFS**.

2. Select **Duplicate Template**.
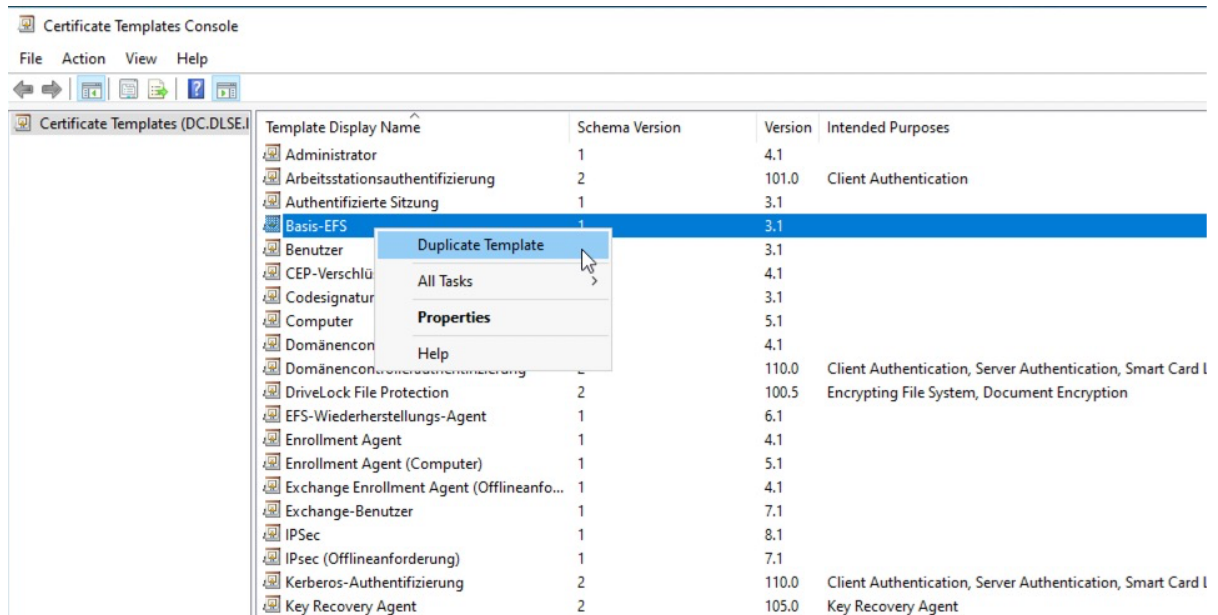
3. On the **General** tab, specify a suitable **name** and the **validity period**.
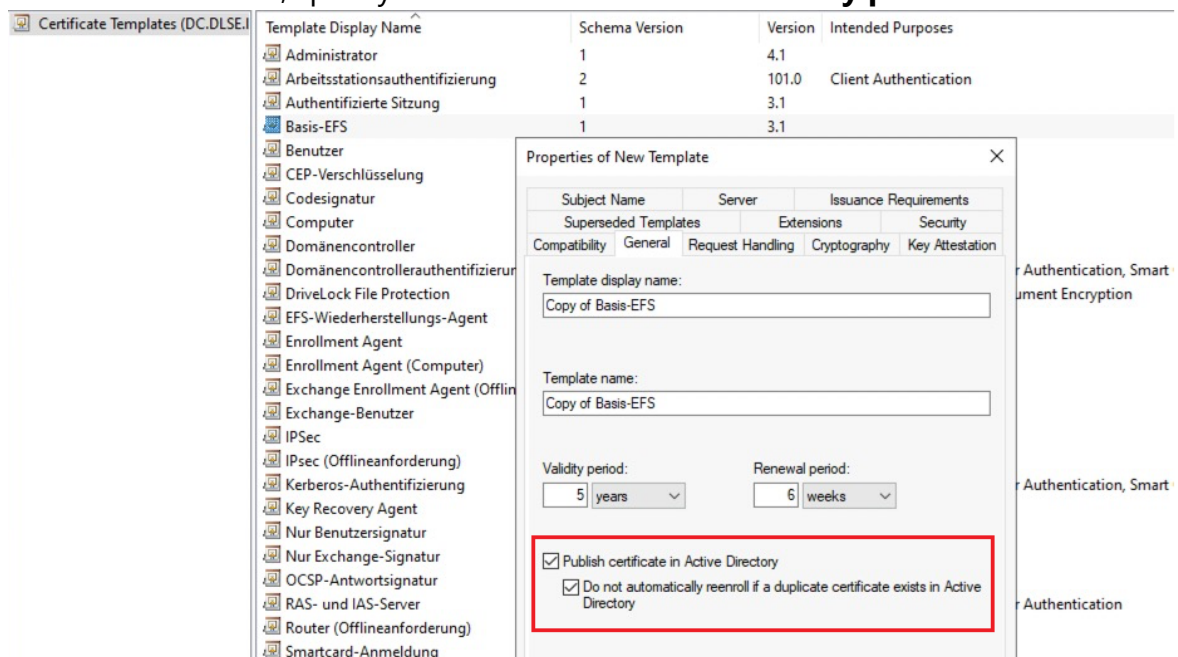
4. Confirm with **Apply**.

5. Now open the **Security** tab in the DriveLock File Protection Properties of the basis-EFS.

6. To configure Auto Enrollment, assign the **Read**, **Enroll** and **Autoenroll** rights to the user and confirm these settings.
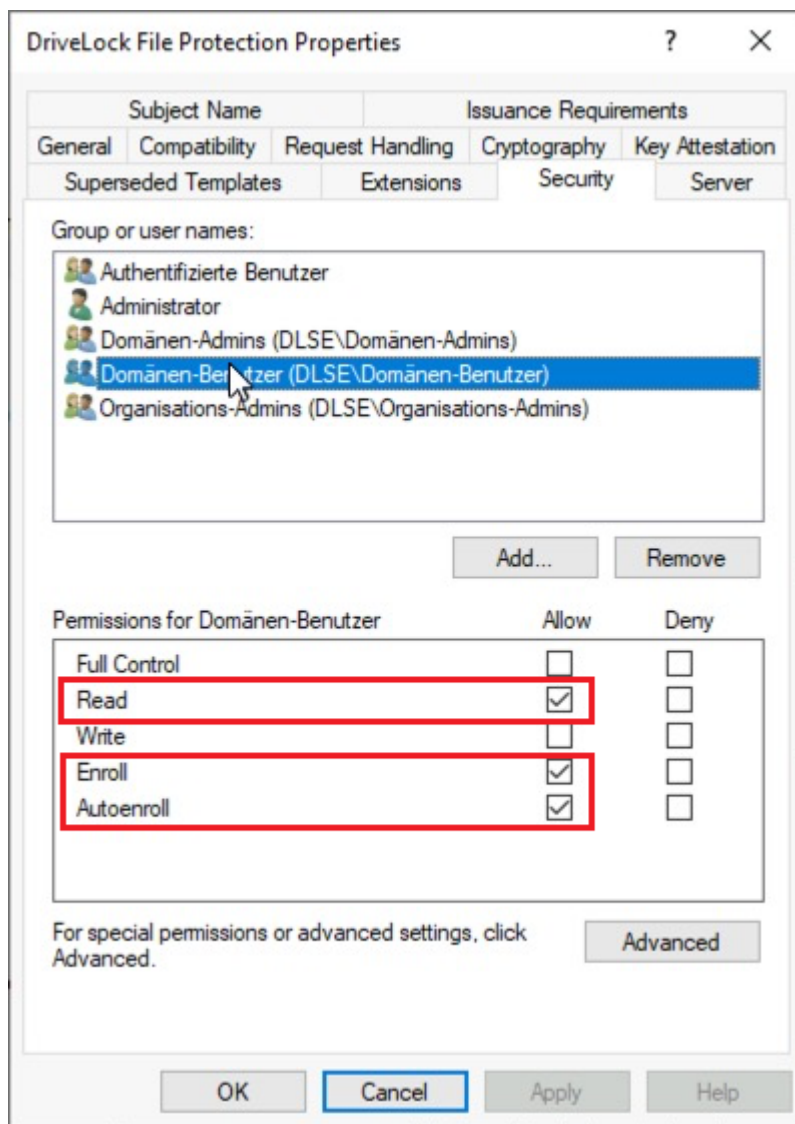
7. On the **Request handling** tab, select **Signature and encryption** as the purpose.
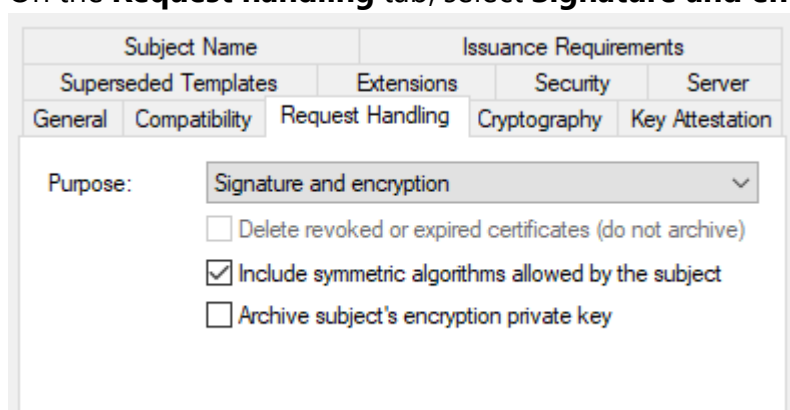
8. On the **Extensions** tab in **Key Usage**, place a check mark next to the **Allow encryption of user data** option and confirm with **OK**.
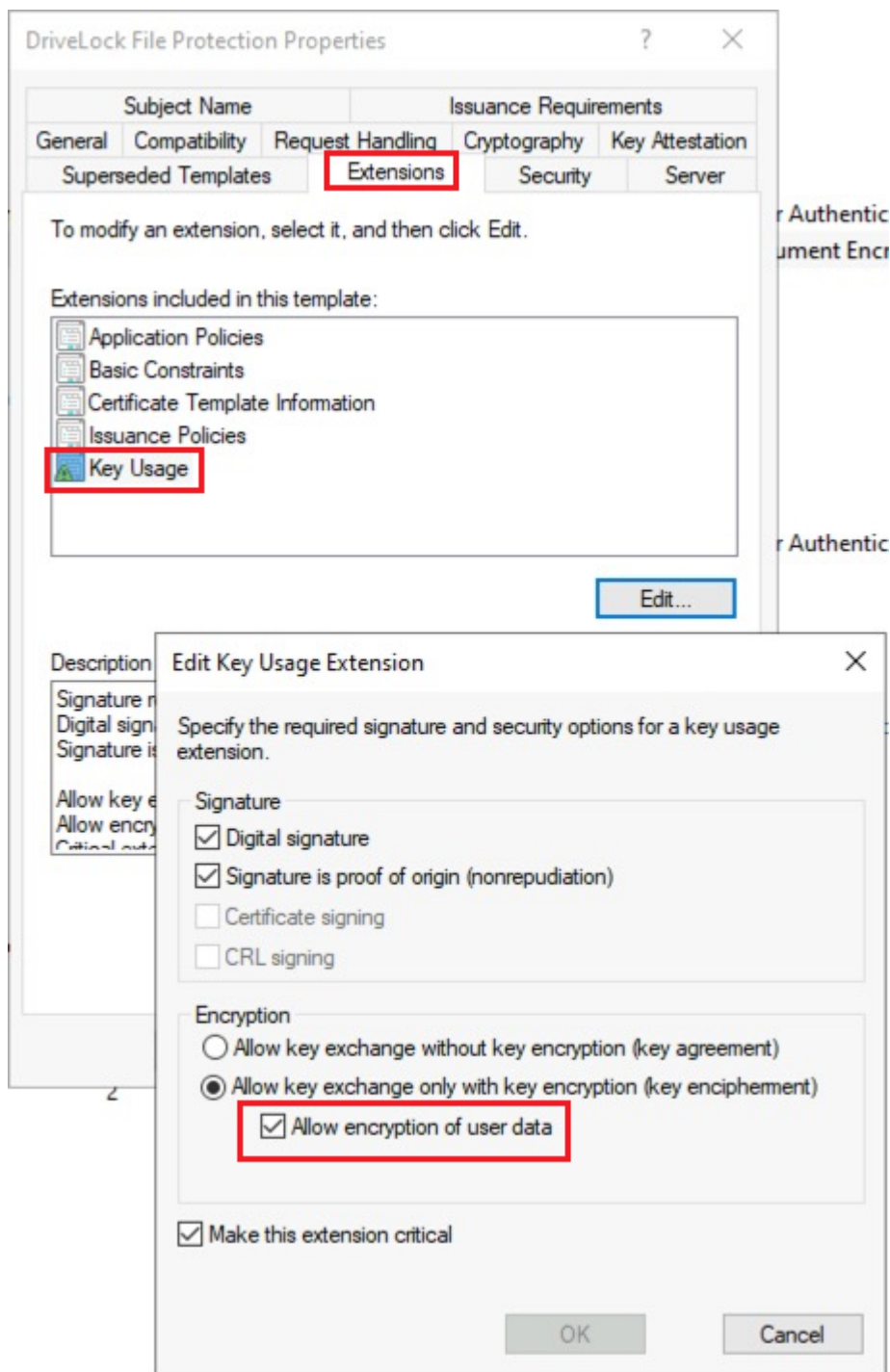
17.6.2.1.1.2 Issuing the template

To issue the certificate template, follow these steps:

1. On the CA server **certsrv.msc**, on the **New** context menu, select **Certificate Template to Issue**.
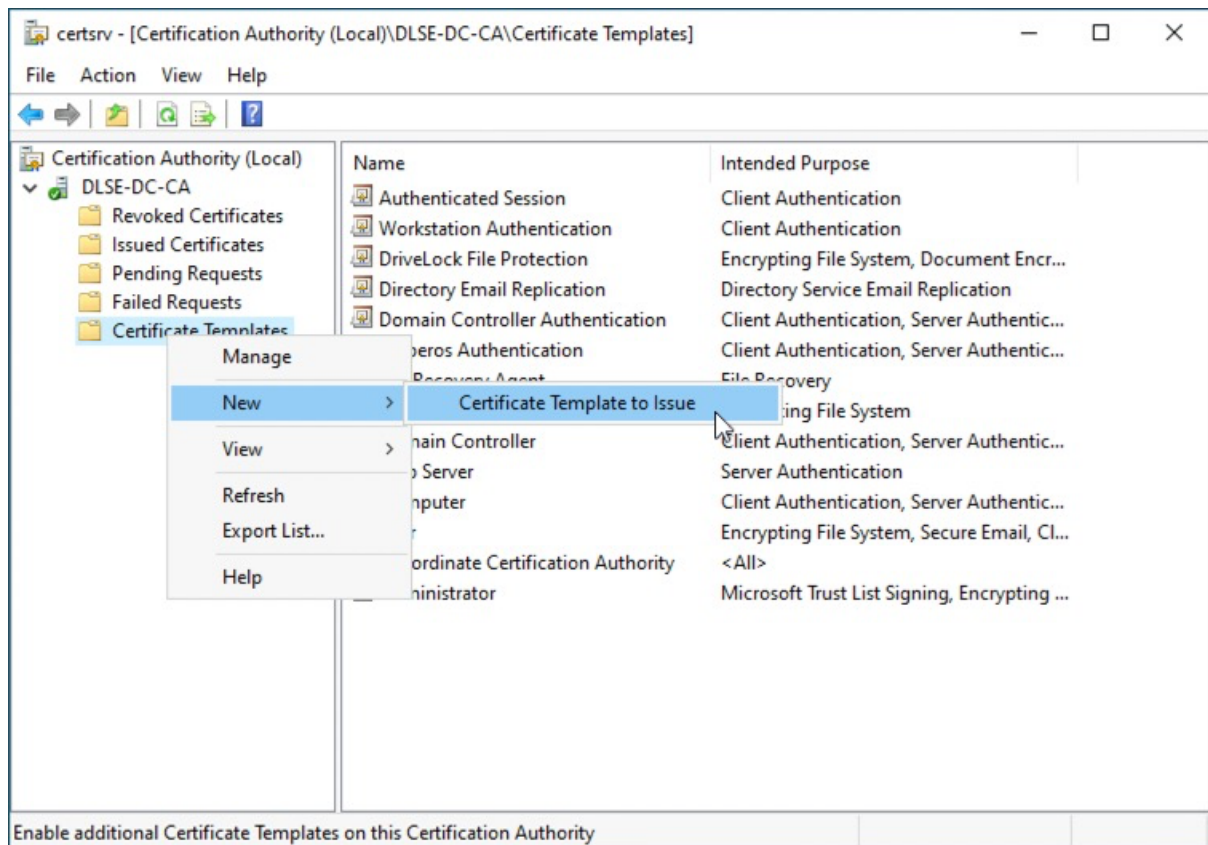
2. Select the template and then confirm with **OK**.
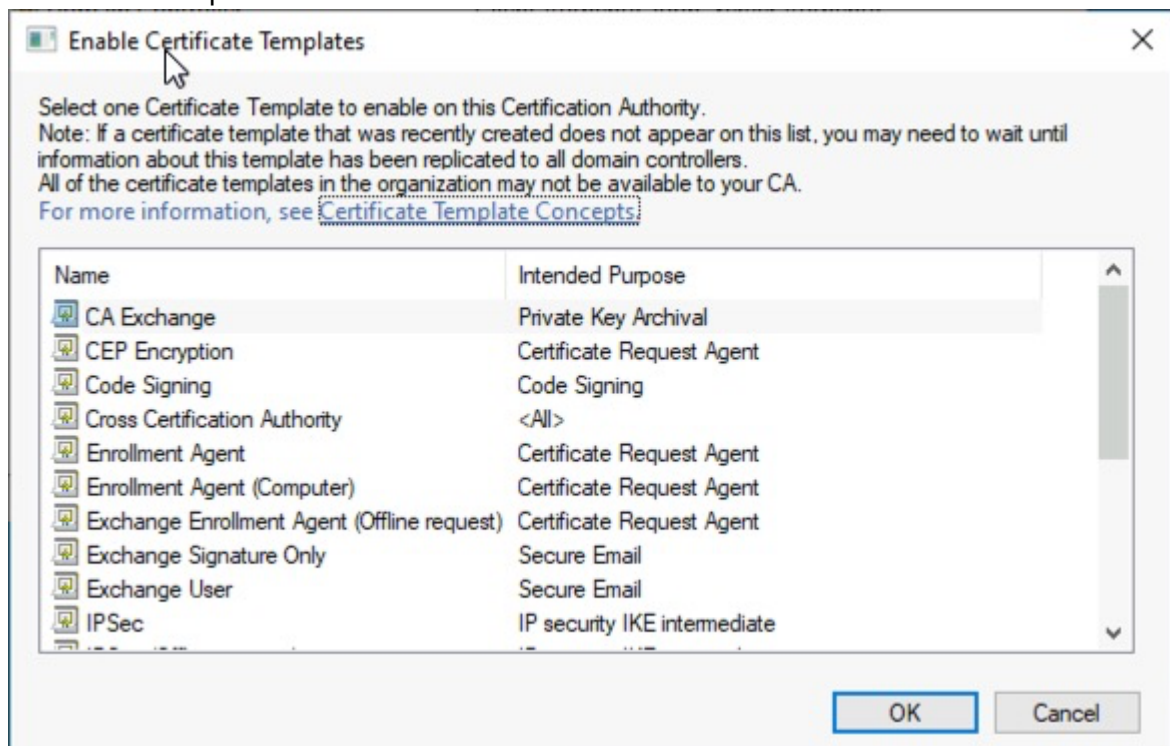
3. Check the template. The template is now configured and issued.

4. Next, set up a group policy.

17.6.2.1.1.3 Creating a group policy

To create a group policy, follow these steps:

1. Open **gpmc.msc** on a domain controller, select the **Group Policy Objects** and then **New** . Enter a descriptive name.
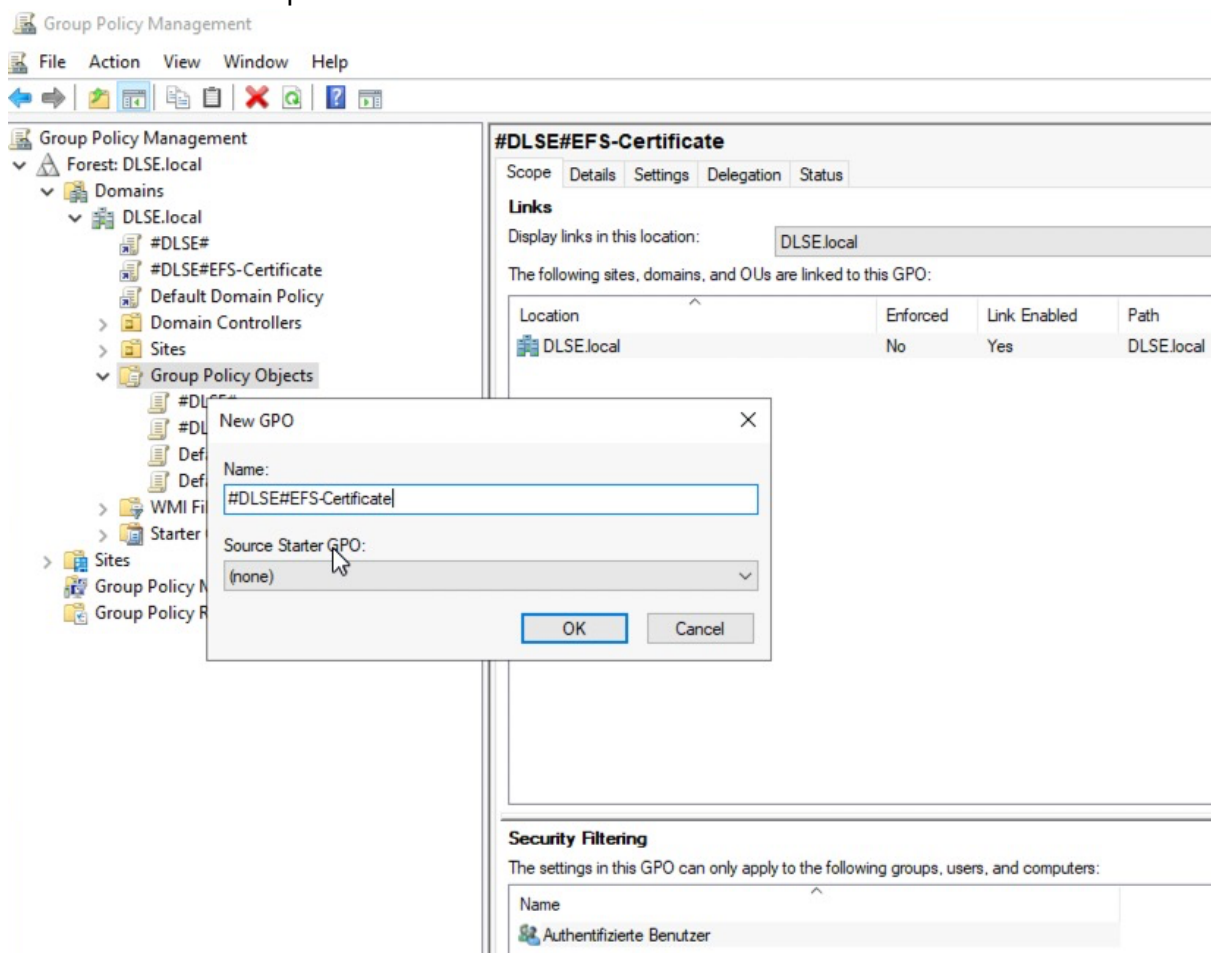
2. Open the context menu of the GPO and select Edit... .
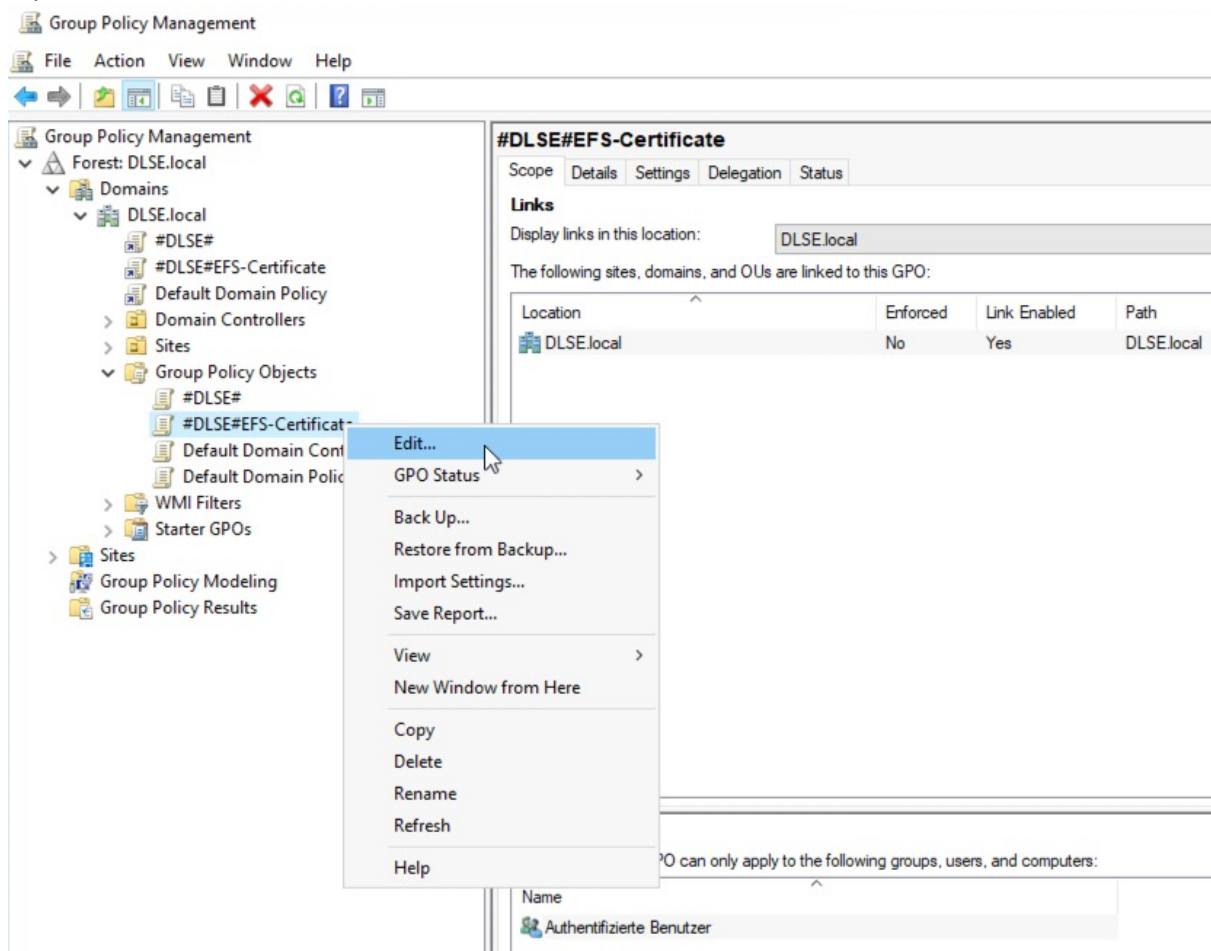
17.6.2.1.1.4 Automatic registration

To automatically register and activate the GPO, follow these steps:

1. Under **User Configuration**, open **Policies**, then click **Windows Settings** and **Security Settings**.
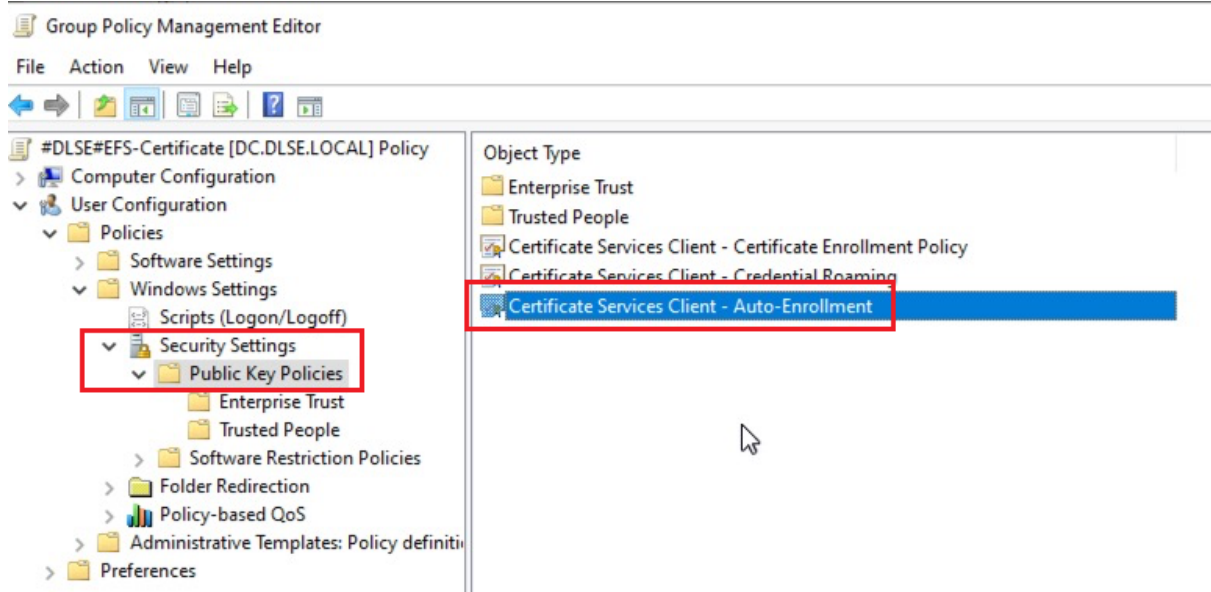
2. Under the Public Key Policies, find **Certificate Service Client - Auto-Enrollment**.
   Open the properties of this object type and select the following options:
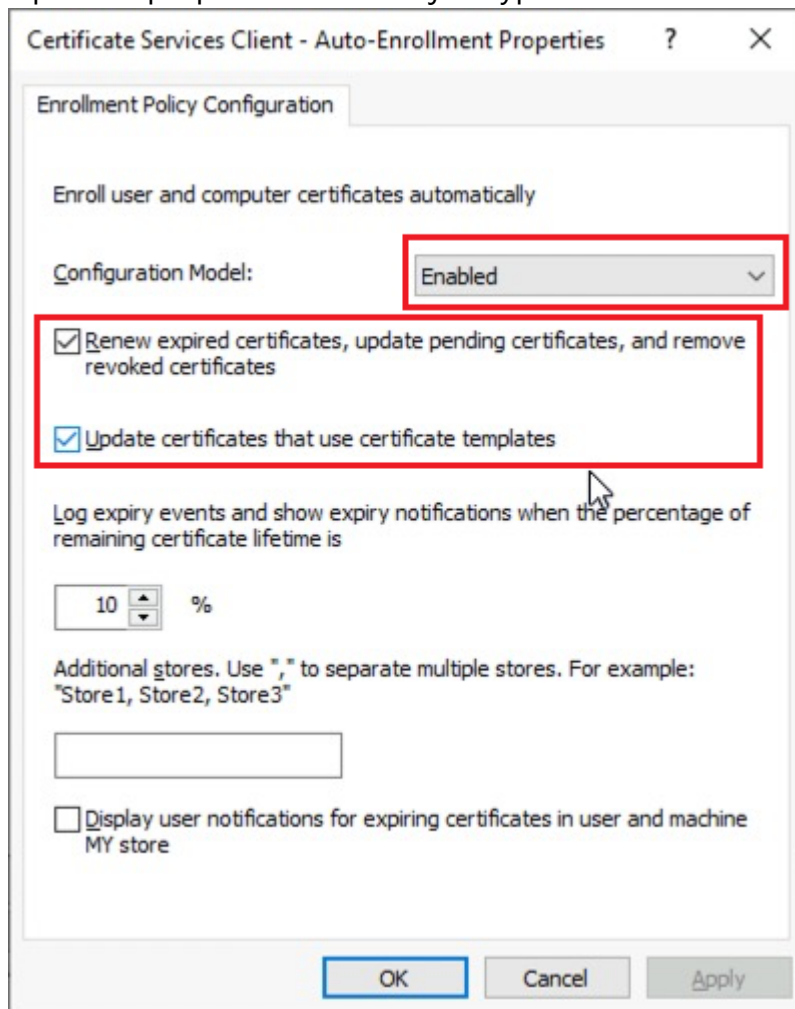
3. In order for the user certificate to roam to all computers on the network ("Certificate Credential Roaming"), enable **Credential Roaming**.

4. Open the corresponding object type and select the **Enabled** option on the **General** tab.
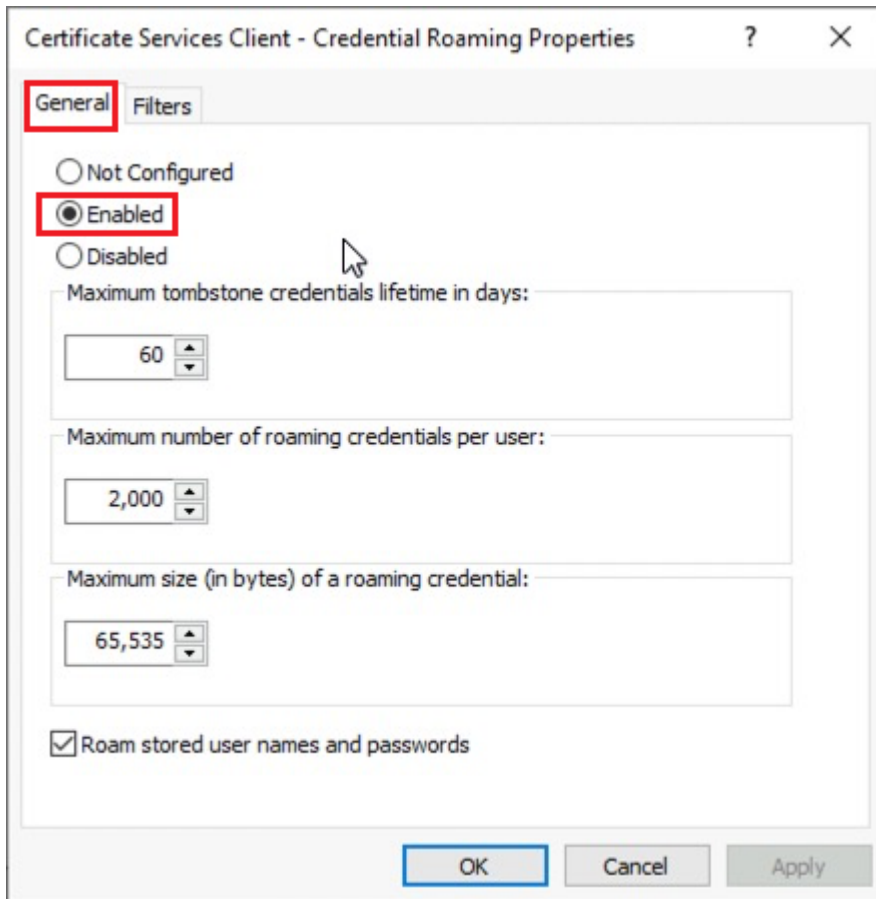
5. Confirm your settings with **OK** and close the Group Policy Editor.

6. Then link the GPO to the domain, OU or location. For example, you can link the GPO to the Employees OU, drag the object over that OU, and then release the mouse button.

17.6.2.1.1.5 Testing the automatic enrollment

To test, proceed as follows:

1. Start a Windows 11 client of the Active Directory domain and log on with a user.

2. To make sure that the newly set GPO definitely takes effect, you can run a Group Policy Refresh in a DOS box.

3. `gpupdate /force`: This is to verify that the GPO has been applied

4. `gpresult /r`

5. The certificate can be found in **certmgr.msc** under **Personal** - **Certificates**.
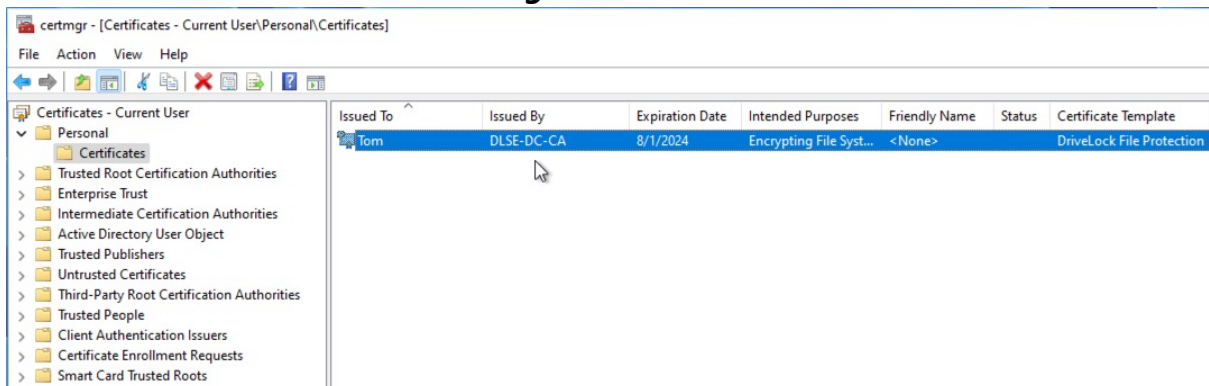
17.6.2.1.2 Creating certificates via the DES

> 📝 Note: You only need user certificate management via the DES if you are not using your own certificate management via a CA.

The integrated certificate management in DriveLock File Protection helps you to manage users and their associated certificates without an existing public key infrastructure (PKI). It is not required if

- You already have a Microsoft Active Directory environment and you are administering user certificates using this infrastructure

- You are already using a PKI that is compatible with Microsoft Windows

- You want to use exclusively passwords for encryption authentication. (Note that these passwords are different from Windows passwords).

DriveLock File Protection already integrates all the functions required for simple, fast and clear management of users and their certificates so that you do not have to set up your own PKI. Users can apply for their own certificates, these applications can be automatically approved and stored in the user's certificate store. When a user requests a certificate, DriveLock automatically creates a corresponding user account. As an administrator, you can approve, revoke or delete certificates.

> ❗ Warning: The DriveLock PKI does not store and manage the privat key of a user's certificate. Users should export the certificate including the private key (PFX file) from the windows certificate store using the DriveLock Application and keep it in safe place. You have to import it again to the windows certificate store to access their encrypted folder from a different computer.

17.6.2.1.2.1 Creating a Master Certificate for Key Management

To manage your own certificates using the DriveLock Enterprise Service, create a master certificate for each tenant that signs and issues all other user certificates.

How to create a master certificate for DriveLock File Protection:

1. Open DriveLock Enterprise Services / Tenants
   Right-click <tenant name> / All Tasks / **Configure root certificate**.
   If the certificate management has not been set up yet, a setup wizard appears. Click Next.

2. To use an existing certificate, select **Existing Master Certificate** and then select a certificate file. Then enter the password to access the certificate contained in the file.
   To create a new, self-signed certificate, select **Create new master certificate**.

3. Enter the details for the certificate completely in the following dialog.

4. The certificate will now be stored in the DriveLock database. Click **Finish** when the certificate saving is successfully completed. In case of an error, you will receive a corresponding error message instead of the success message. In this case, run the wizard again.

> ☑ Note: When the master certificate has been created and the wizard has finished, certificate and key management is initialized on the server running the DriveLock Enterprise Service and the DriveLock Enterprise Service is restarted.

17.6.2.1.2.2 Configuring Certificate Management

Creating or designating a master certificate automatically activates the certificate and key management functionality of the DriveLock Enterprise Service. You can deactivate or reactivate this functionality at any time.

Another setting used for certificate management is the configuration of how DriveLock File Protection issues the creation and renewal of user certificates. The following two methods are available:

- A user certificate is automatically generated and issued when a user applies for a certificate. (Default)

- An administrator must approve user certificates before they are issued to users.

To change settings for certificate management, perform the following procedure:

1. Open the tenant properties in the DriveLock Enterprise Services node -> double-click on <tenant name> -> Certificate management.

2. To activate certificate management, select the **Enable key and certificate management** checkbox.

3. To require an administrator to validate and approve all user certificates, select the **Certificate requests must be manually approved by an administrator** checkbox.

4. Enter the number of years the user certificate is valid for.

5. To save the settings, click Apply.

17.6.2.1.2.3 Manage certificates

Certificates are managed in the DriveLock Management Console. You can access DriveLock File Protection certificate management by clicking **DriveLock File Protection** in the navigation pane and then clicking **Certificates**.

DriveLock File Protection uses three categories of certificates that are displayed separately:

- **Certificate requests**: This includes user requests for certificates or certificate renewals that an administrator has not yet approved or denied. A certificate request can either be rejected or accepted here.

> Note: The approval of certificates is only necessary if you have activated the corresponding option in the Tenant settings. Otherwise, this list never contains certificates.

- **Active certificates**: This overview shows all currently active certificates stored in the DriveLock database. Here you can view certificates, export the public part and delete or revoke them.

- **Revoked certificates**: This list displays all certificates that have been revoked by an administrator. Revocation marks a certificate as invalid, but does not yet delete it from the database. Here you can view revoked certificates, export the public part and revoke the revocation (a certificate will then be marked as active again).

Click on one of the three categories to display all certificates stored for that category.

On the right side, you can see an overview of all certificates stored in the DriveLock database.

To sort the displayed entries by another column (default is object name), click one of the column headers. To change the order from ascending to descending or from descending to ascending, click this column heading once more.

To edit certificate requests, proceed as follows:

1. In the navigation pane, click **Certificate requests**.

2. Right--click the certificate request to manage

3. To approve the request and issue a certificate, click **All tasks**-> **Approve request**. The certificate's list entry is removed, the certificate is activated. To deny the request and not issue a certificate, click **Deny request**. The request is removed from the list and deleted.

To revoke an active certificate, perform the following procedure:

1. In the navigation pane, click **Active certificate**.

2. Right-click the certificate to revoke and then click **All tasks** -> **Revoke**.

3. Select the reason for the revocation from the list

4. Optional: In the **Comment** text box, enter additional information about the revocation of this certificate.

5. Click **OK** to revoke the certificate permanently. The certificate's list entry is removed and the certificate is marked as revoked.

To reactivate a revoked certificate, perform the following steps:

1. In the navigation pane, click **Revoked certificates**.

2. Select All tasks and then **Cancel Revocation**.

3. Click **Yes** to activate the certificate. The certificate's list entry is removed, the certificate is activated.

To export a certificate, perform the following procedure:

1. Click on **Active** or **Revoked certificates** in the navigation area.

2. Click **Export certificate...**.

3. Select a directory and a file name to save the public section of the certificate in a file (extension .cer).

> Note: This certificate file can be used by a user to authorize the certificate owner (i.e. the user this certificate was generated by) for a specific private directory. Further information can be found in the DriveLock user documentation (WebHelp on the DriveLock Agent).

To delete an active certificate, perform the following steps:

1. In the navigation pane, click **Active certificate**.

2. Click **Delete certificate**

3. Click **Yes** to delete the certificate permanently. The request is removed from the list and deleted.

> ⚠️ Warning: Please note that deleting certificates does not delete the user stored in the database. However, it is no longer possible to authorize this user to access a centrally managed directory. Permissions already set up remain unaffected as long as the user has his user certificate stored in the Windows certificate store. To invalidate permissions that have already been set up, please revoke the desired certificate.

17.6.2.2 Create and manage users

If certificates are created via the DES, the corresponding user is already created via the DES. If not, a user must be create first. In the DOC, the AD inventory is used for this, in the DMC this is done via querying the AD directly.

17.6.2.2.1 Users in the DOC

Configuration: Security Controls -> Encryption -> File Protection -> Centrally managed folders or Users

Once you have created centrally managed folders in your environment (either via the agent or in the DMC), these are displayed in the list in the DOC. You can also see the corresponding users in the details of the respective folders.

To add users to a folder (or to remove them or edit their permissions), the required permissions must be available. This is checked by the DOC Companion, which searches for the required certificate in the certificate store to ensure that the permission is available.

In the list of users, you will see all authorized users with their respective certificates. You can add users from the AD inventory to create 'File Protection users'. These are special users who have a certificate that is required when working with centrally managed folders.

In the user's detail view, you can also see which centrally managed folders the user has access to.

User certificate exchange in the DOC

It is also possible to swap certificates of File Protection users, i.e. to select a different certificate for a user. This is necessary, for example, if the user certificate has been updated in the AD and the new certificate is to be used in future. In the Certificate status column, the old certificate is then displayed as revoked and the new one as valid. The next time the user logs on to the agent, the DES checks the existing certificates and the agent automatically replaces them in the centrally managed folders.

> Note: We recommend exchanging the certificate only via the DOC and not via the DMC.

17.6.2.2.2 Users in the DMC

In the DriveLock Management Console, you will find the options for creating or managing users and groups under **DriveLock File Protection** and then **Users and groups**.

On the right side you can see an overview of all users or groups stored in the DriveLock database.

> Warning: Please note that you cannot create certificates here, only use existing ones.

To create a user or group with an existing certificate (i.e. import a certificate), perform the following steps:

1. Right-click on **Users and groups** in the navigation pane or on an empty space in the details pane to the right.

2. In the context menu, point to **New** and then click one of the following:
   - **User from Active Directory**: if you want to select a user with an existing certificate from Microsoft AD. In this case, the standard dialog for selecting objects from Active Directory appears and you can select a user.
   - **User from certificate**: if you have a certificate in the form of a certificate file (*.cer). In this case you can open this certificate file via the file selection dialog.

3. After scanning the certificate, the properties window of the user opens.

4. As long as the data could already be read from the certificate, the appropriate input fields are already filled with these values. Please fill in missing information such as email address or department.

5. Optional: In environments with more than one DES and different clients, the new user can be created for a specific client. In this case, select the correct client from the Client drop-down list. Otherwise, leave this entry unchanged.

6. Optional: You can also add any display image from a graphics file. Since this image is displayed in different places during user selection, it can make it easier to select the right user, especially if the names are the same. To do so, click Change picture and select a suitable graphic file. Click Open. If the file could be used as a display image,

this new image is now displayed in the upper left corner of the user properties.

7. Click OK to create the user and save the changes. The new user is now displayed in the detail view on the right.

To change or view the properties of a user, double-click the required entry:

- The **Centrally managed folders** tab displays all centrally managed folders that the user is authorized to access.

- The **Certificates** tab displays all certificates associated with the user that are stored in the DriveLock database.

17.6.2.2.3 Manage groups

> ☑ Note: This functionality is currently only available in the DMC.

DriveLock File Protection groups are a set of DriveLock users. DriveLock groups can be assigned to centrally managed encrypted folders. Once DriveLock users are added to or removed from a DriveLock group, the DriveLock Enterprise Server automatically updates the corresponding users in all centrally managed folders assigned to this DriveLock group.

> ☑ Note: DriveLock groups behave differently than Windows (AD) groups. For AD groups, the permissions are checked at the time of access. However, since groups cannot have certificates and cannot authenticate themselves, DriveLock must assign the corresponding users to the respective folders individually. It may take approximately 15 minutes for this assignment to be completed.

To create a new group right-click **Users and Groups** and then **New**.

You can either create a new DriveLock group and add the DriveLock users or import an existing group from the Active Directory (AD). When importing from AD, the AD group members are added to the DriveLock group under the following conditions:

- The AD user already exists as a DriveLock user => the user is simply added to the DriveLock group.

- the AD user has a valid certificate => a new DriveLock user is created and then added to the DriveLock group

- The AD user does not have a valid certificate => a hint is displayed and the user is not added

In the new group' properties dialog, you can now assign/customize the group name on the General tab and select the correct tenant. On the Users tab you can add/customize users of the tenant. You must mark at least one user as a group administrator. Click OK to save the new group.

> Note: Once the group is created, only a group administrator can add additional users and grant or revoke administrator permissions using the DriveLock application. This procedure is described in the DriveLock User Manual.

Open the properties dialog of a DriveLock group to get information about the group members and the assigned centrally managed folder. In exceptional cases, when the group administrator is not available, DriveLock Administrator can remove users or managed folders from the group.

17.6.3 Working with encrypted folders

17.6.3.1 Centrally managed folders

The DriveLock Enterprise Service (DES) manages administrative information, such as user permissions, centrally. This means that this information can be managed from both DriveLock consoles.

> Note: As centrally managed folders will only use certificates for authentication, you will need to distribute certificates and create File Protection users first.

How to create centrally managed folders

- Starting with version 2024.1, it is possible to specify that an encrypted folder is to be centrally managed directly when creating it on the agent. Doing so has the following advantages: Any existing files may also be encrypted and the centrally managed folder can be located anywhere.

- In DriveLock On-Premise environments, you can also create centrally managed folders in the DMC under DriveLock File Protection-> Centrally Managed Folders, although with this method you cannot encrypt existing files and the directory must be located on a network share to which the DES (primary server) has access.

Managing access permissions

Administrators can delegate the permissions to perform these tasks to others. This enables designated individuals to administer permissions for their departments and also makes it

possible to remove the permission to decrypt certain sensible files even from administrators.

To change the permissions, the following options are available:

- Via the agent on the encrypted folder

- In the DOC under *Security Controls -> Encryption -> File Protection -> Centrally managed folders*

- In the DriveLock Management Console (DMC) under DriveLock File Protection-> Centrally managed folders

In any of the above cases, users who are authorized as folder administrators can add or remove new users or change the permissions of existing users.

> ☑ Note: If a centrally managed folder in the DOC is deleted, the folder itself becomes an independent folder.

17.6.3.2 Independent folders

In addition to centrally managed folders, users can also define (or create) their own folders and store files there securely encrypted (e.g. as a private local directory, on a USB stick or as a directory at Dropbox or another cloud service provider). As with centrally managed folders, permissions to access data in such individual encrypted folders can be given to additional users.

In addition to certificates, passwords can also be used for authentication. This makes it easier to share files and use Mobile Encryption.

> ☑ Note: The management information is only stored in the respective folder, i.e. it is not available on the DES and the folder can therefore not be managed via the DOC.

17.6.3.3 Creating an encrypted folder via the agent

It is possible to create an encrypted folder directly from the DriveLock Agent and then manage it centrally or manage it yourself as a separate folder.

To do so, users either select

- the **Encrypt folder** command in the context menu of a folder in the Explorer or

- the **Create encrypted folder** menu command in the Start menu or DriveLock Tray icon in the File Protection context menu.

If the **My DriveLock File Protection user and certificate** option is selected as the authentication method, you can define whether the folder is managed centrally or remains independent. For centrally managed folders, the encryption information can also be saved in the folder itself so that the folder can also be used offline.

If the user opts for centrally managed, the folder is displayed in the DOC and can be further edited there by the administrator or another authorized person (e.g. by adding additional users).

17.6.3.4 Settings for enforced encryption

For the enforced encryption of external data volumes, you can also use file encryption instead of container encryption (see DriveLock Encryption 2-Go). For large volumes, this speeds up the initialization significantly, because a container does not have to be created first, but only the files to be copied are encrypted. It also allows you to have multiple folders created with different permissions, for example, a folder with a company certificate that can be transparently accessed by all certificate holders, a folder with username and password for the owner only, and a folder for unencrypted data.

Use forced encryption with DriveLock File Protection

1. Activate the enforced encryption with DriveLock File Protection in the policy at:
   Encryption / Settings / **Enforced encryption method for removable media**
   Select **DriveLock File Protection**. This will use file and folder based encryption for all new unencrypted drives that have enforced encryption enabled in a rule.
   If you want your users to choose between container-based or file and folder-based encryption, select **Let the user decide**.

2. Configure the encryption settings in the **Enforce encryption** sub-node.
   Open the context menu, then select **New** and create one or more new encryption rules for different user groups.
   a. In the rule configuration dialog, create a short description for the rule under **General**.

   b. In the **File System** tab, configure whether existing data should be preserved and moved/encrypted to the configured folder and specify whether the Mobile Encryption application should be copied to the drive. If you do not select Preserve existing data here, all existing data will be deleted before the stick is encrypted.

   c. In the **Settings** tab you specify the type of permissions and encryption and assign a name for the encrypted folder. Under **Advanced settings**, they can

assign the names for additional folders and specify whether they should instead include the existing unencrypted data during initialization.

d. In the tabs **Computer**, **Networks** and **Logged on users** you define to whom and where the rule should apply.

e. Set the **priority** with which the rule should be applied. The applicable rule with the highest priority is always used.

User selection of the encryption rule (Optional)

Similarly, create new user selection rules and add encryption rules if users are to select a suitable encryption rule themselves. Here you need to set the priority so that the rule is applied prior to the encryption rules.

> ✏ Note: If you have configured user decision, the encryption method selection dialog appears first, followed by the user selection rules dialog. Be sure to select the options available in both dialogs only once.

17.6.3.5 Recovering encrypted folders

If a user is no longer able to access an encrypted folder and decrypt the content, which can occur, for example, if the appropriate user certificates are lost or the password is not remembered, you can use recovery to restore access to these folders.

The following procedures are used to restore the data:

- Challenge-response procedure: this involves the user and the administrator (or support employee).
The challenge/response mechanism validates both the challenge (request code) that DriveLock creates for the user and the corresponding response code that is generated by the person performing the recovery. Only when both codes are valid for the drive or folder to be recovered, can access to the data be restored (for example enabling the user to select a new encryption password). The request code is generated by the user with the help of a wizard, transmitted to the administrator and checked for validity by the administrator in the DOC under *Security Controls -> Encryption -> Recovery -> File Protection Recovery*. The administrator checks that the request code is valid and then generates a response code that is in turn validated by the wizard running on the client computer.

- If the user has access to the certificate, it can be used directly (via online recovery)

514

- Direct recovery from the DOC under *Security Controls -> Encryption -> File Protection -> Centrally Managed Folders* using the menu command *Recover access to the folder*

The steps for recovery by the administrator (or support employee) in the DMC correspond to those for online or offline recovery with Encryption 2-Go.

17.6.3.5.1 Configuring recovery

To configure the recovery of encrypted folders in the DMC, open the sub-node **Recovery of encrypted folders** in the **File Protection** node.

> Note: When restoring encrypted directories, the appropriate recovery certificate must then be selected if certificates with multiple priorities have been created.

By default, there is initially one certificate entry which is used for all encrypted directories (if configured). This certificate has the **Lowest** priority and cannot be deleted.

To create a default recovery certificate, perform the following steps:

- Double-click **Certificate-based recovery (Lowest priority)** .

- Click **Certificate File** and select **Create New** from the drop-down menu. This will start the wizard for generating the main certificate.

- Next, either specify the folder where you want to save the certificate file or, alternatively, choose a smart card as the location.

- If you are using a smart card for storage, you will now be asked to insert and select the card, depending on the card you are using.

> Warning: Make sure that this file is saved in a safe place, as it is urgently needed for password recovery.

- Now enter the password for accessing the private key area of the certificate. You must enter the password twice for security reasons.

- To continue, click Next. It takes a few seconds to generate the main certificate. You will then be notified when the process is complete and the file has been saved to the previously specified location.

> Warning: Make sure you do not forget this password. You should likewise store this in another safe place (for example, in a safe).

- If a smartcard is used for storage, you will be prompted to enter the PIN for accessing the smartcard.

- Click Finish.

The certificate file you just created is now displayed.

> ⚠️ Warning: Once the certificate has been created and the first encrypted container has been generated, no new certificate may be created, as this will overwrite the old one and thus it can no longer be used for recovery.

If you click **Properties**, you will get additional information about the main certificate.

The certificate is also stored in the private certificate store of the current user. The public key of the certificate is also stored inside the local policy file store.

If you cancelled the creation wizard or there was a problem during the creation, DriveLock will display the corresponding message and you will have to create the main certificate again.

If you have used encrypted directories without a root certificate before, it is useful to enable the **Add recovery information to existing folders** option. In this case, each time a directory is connected, DriveLock checks whether recovery information already exists and generates this information if necessary. Subsequently, the data required for recovery is also transferred to the DriveLock Enterprise Service.

If DriveLock Enterprise Service is not used in your environment or you do not want the recovery data to be transferred to DriveLock Enterprise Service, you can disable this feature by enabling the **No offline recovery - do not upload recovery information to DES** option.

Right-click **Encrypted Folder recovery** and select **New** -> **Encryption recovery rule** from the context menu to create another certificate.

At the beginning there is no certificate file specified here. Click **Certificate File** and select **Create New** from the drop-down menu.

This will start the main certificate generation wizard again. Now the procedure is the same as when generating the certificate for the lowest priority.

Via Settings on the tabs **Computer**, **Networks** and **Logged on users** you can now specify for which of the areas with the same name this certificate should be used. The functionality is the same as in many other places in DriveLock and is therefore not described in detail here.

The new certificate is then displayed in the detail view on the right.

The first additional certificate is assigned priority 1, and each additional certificate is assigned a priority that is one higher than the highest existing priority.

Right-click an entry and select **Down** or **Up** to adjust the order of prioritization. Via **Delete** you can delete an existing certificate.

> ⚠ Warning: If you delete a certificate that has already been used, it is no longer possible to restore it.

In order to use the offline password recovery functionality, you have to generate a master certificate consisting of a public and private key pair before creating the first encrypted directory. For this purpose, it is also possible to create multiple certificates, which can be filtered via Computer / Networks / Logged on users. This is useful if the group of users who are allowed to perform recovery of encrypted data differs. However, at least the default recovery certificate with the lowest priority should be generated.

Example: Especially in large environments, it may be preferred to create a default certificate that is used for all. Only the management board has its own recovery certificate. The standard certificate is given to the IT helpdesk so that the password of encrypted directories can be reset for all employees except the management board. Only the IT Security Manager and the IT Enterprise Administrator receive the recovery certificate from the Management Board so that recovery is also possible here. This measure further restricted the group of people who potentially have access to confidential data (those on the Management Board).

17.6.3.5.2 Company Certificate

Encrypted folders containing a company certificate can be mounted by any user, who has access to the corresponding private key in the windows certificate store. If so, when the user mounts an encrypted folder, DriveLock first checks, whether the folder can be decrypted using the company certificate, then the folder will be mounted without any further user interaction. Otherwise, the user will be asked for his credentials.

> ⚠ Warning: The company certificate is not used for centrally managed folders.

DriveLock does not create company certificates but allows you to import the public key of any certificate (*.cer) you own. You have to store the private key (*.pfx) yourself in the Windows certificate store (user or computer account).

Technically a company certificate is very similar to a recovery certificate and configured in the same way.

Follow these steps to create a company certificate:

- To add a new company certificate in a policy open Encryption / **File Protection** / **Encrypted folder recovery** / **New** / **Company certificate...** On the General tab, add a description and import the certificate.

- Check **Enabled** to use the certificate when creating / updating encrypted folders.

- In the **Options** tab, select how to use the certificate.

> Note: For evaluation purposes you may use e.g. a DriveLock Recovery certificate as a company certificate.
> Import the DLFfeRecovery.cer to the policy and the DLFfeRecovery.pfx to the Windows certificate store.

Update a Company Certificate

DriveLock does not care about the expiration date of a company certificate but still allows you to access and create encrypted folders. Nevertheless you may add new company certificates to your policy at any time and you may remove the expired certificates from your policy.

> Note: If you delete a company certificate from the Windows certificate store, you will no longer be able to connect the encrypted folder with this key. If this has been the only key for a folder, a new company certificate cannot be added any more.

17.6.3.6 Use case: Accessing encrypted folders

In order for users and groups to have access to encrypted resources, you must define these groups and users from Active Directory.

For this purpose, go to **New** in the **Users and Groups** submenu and select a user or group from the Active Directory.
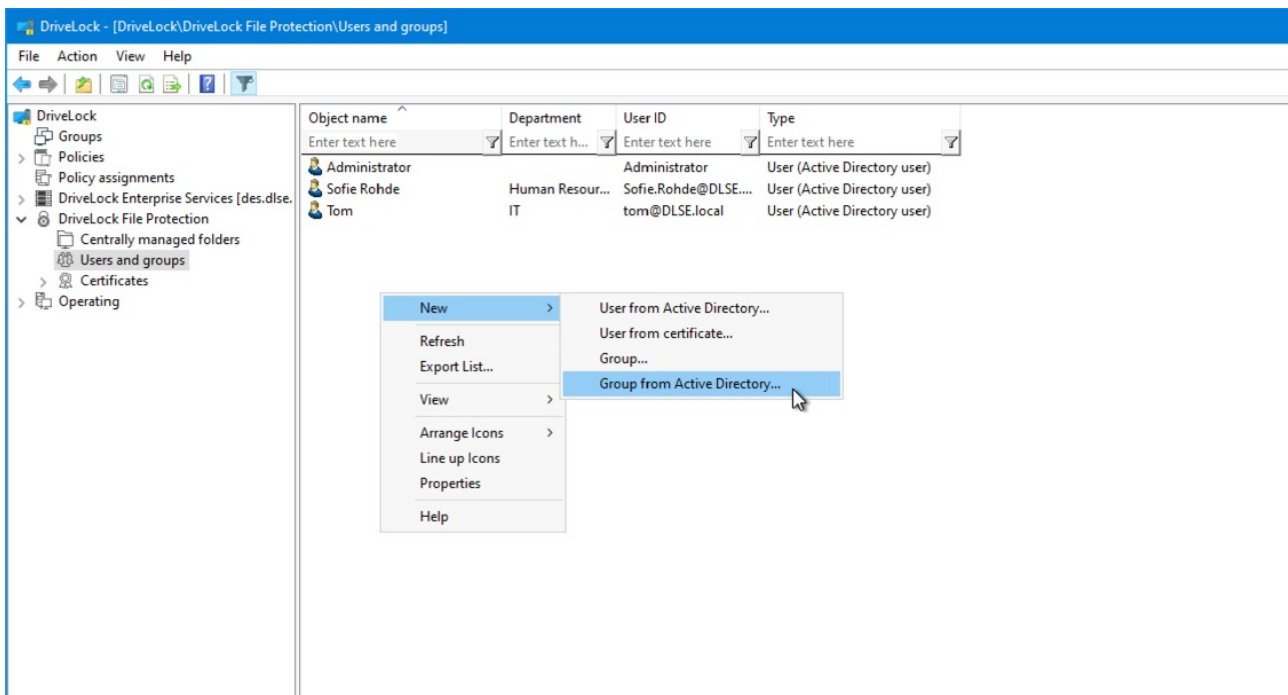
In this case, the group "Human Resources Users Munich" was selected.
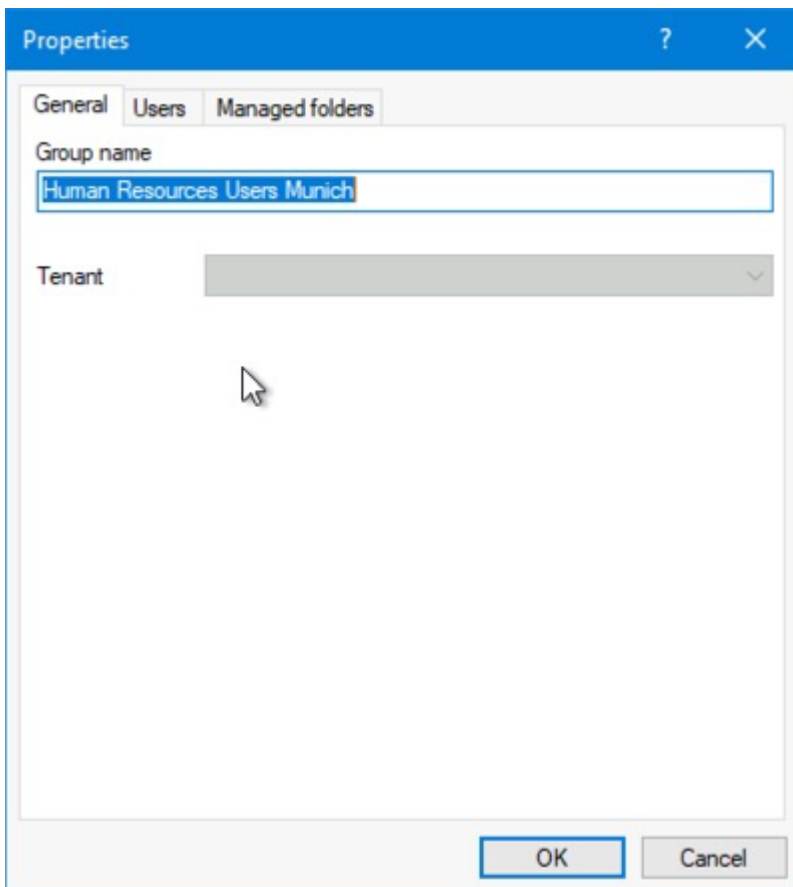
For groups, you must select a group administrator. This is configured on the **User** tab.
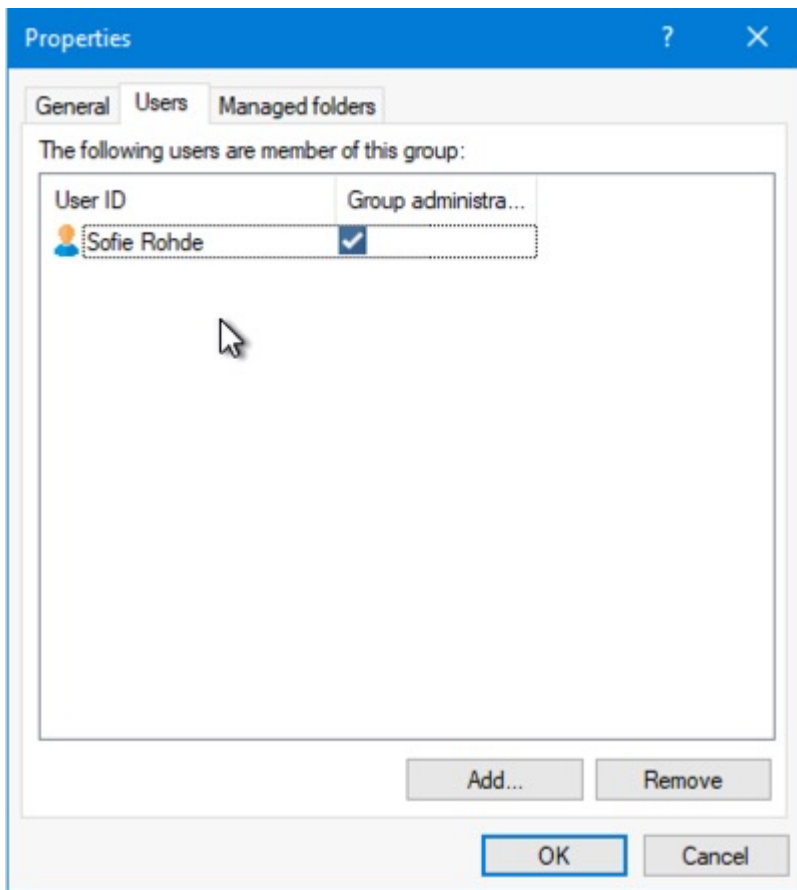
Now select the **Centrally managed folders** sub-node and configure a new centrally managed folder.
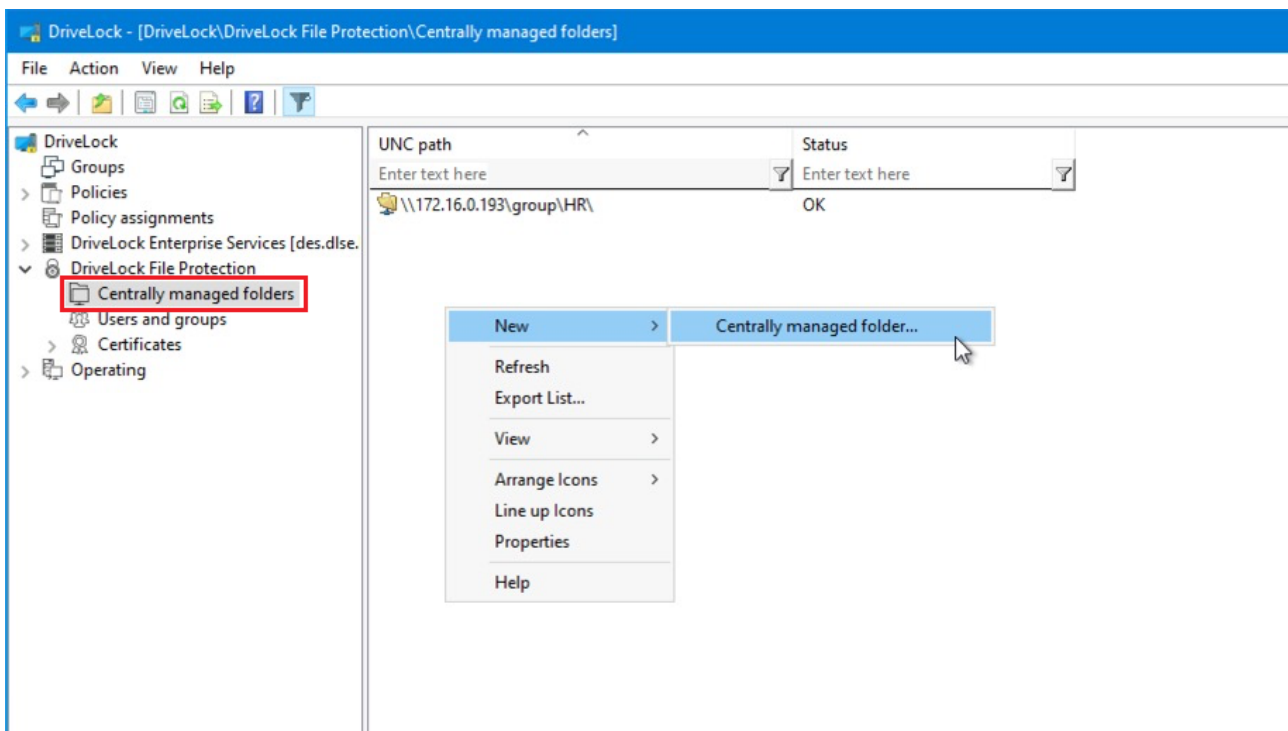
Specify here the UNC path to the network drive or the published folder to be encrypted with DriveLock File Protection.

Select the group or user added in the previous step.
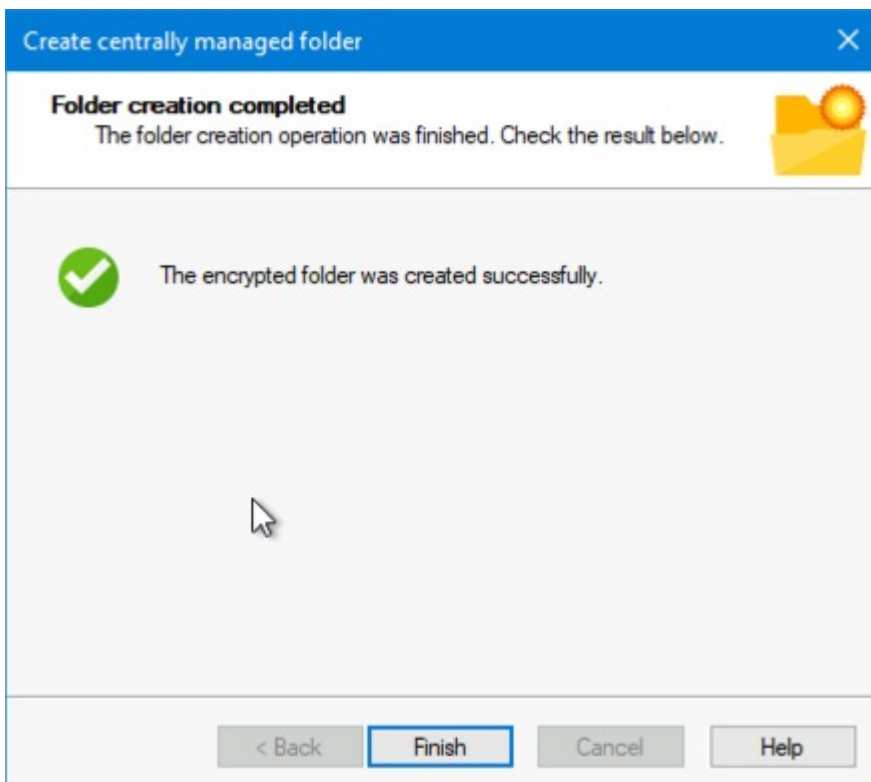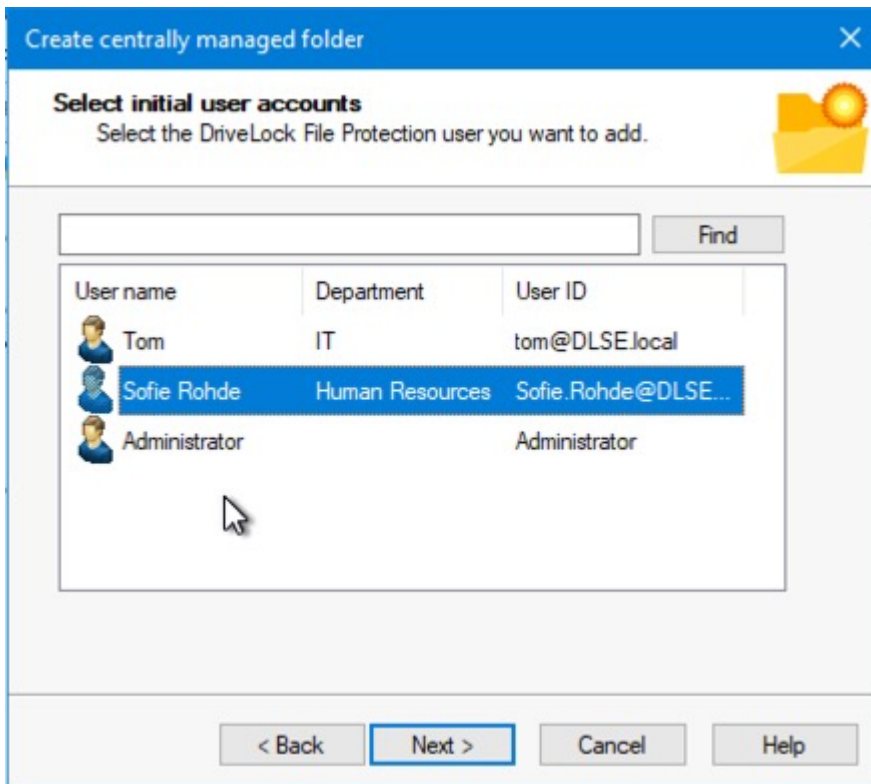
Click Finish. The folder is now encrypted.
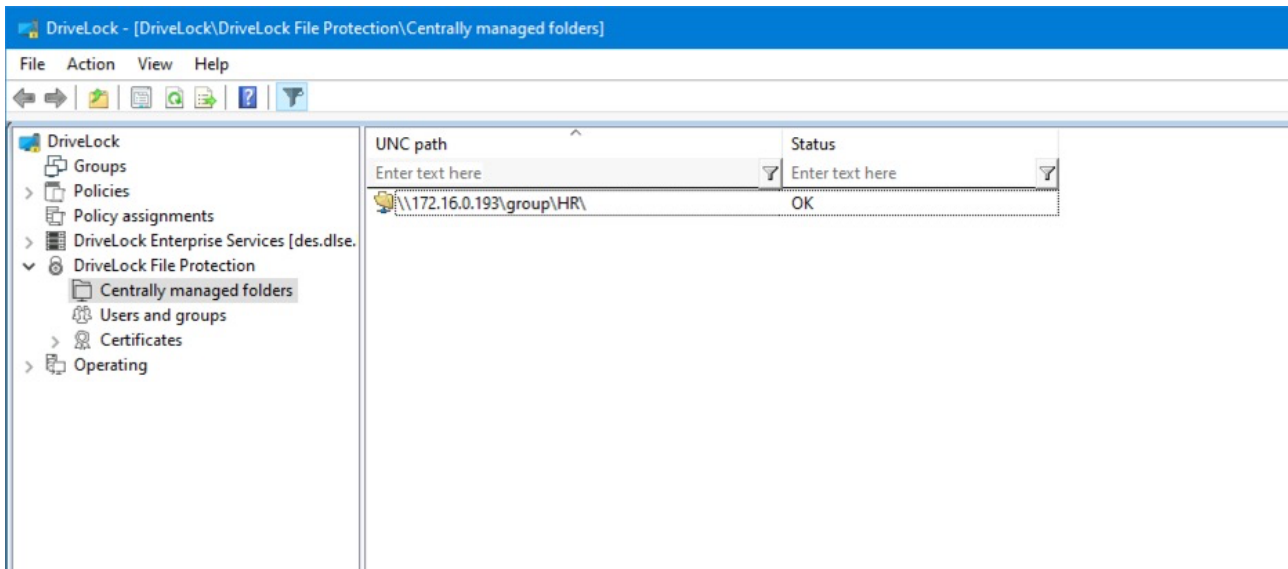
You can now log on to a computer that is a member of the domain. In this example we use "Sofie Rohde". Sofie is a member of the group "Human Resource Users Munich".
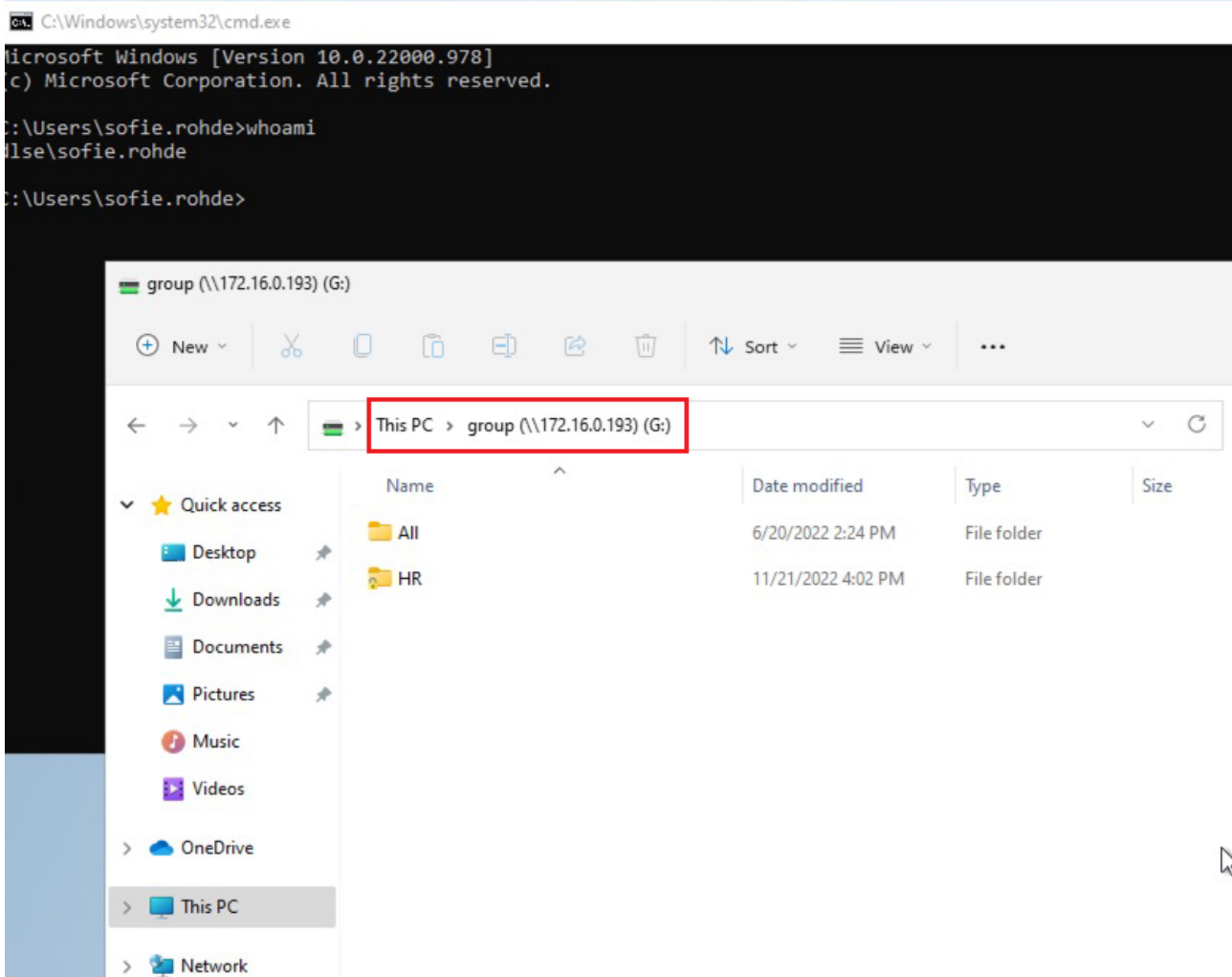
As soon as the user clicks on the folder in the network, it is decrypted and mounted by DriveLock Agent. A corresponding message will appear in the message area.
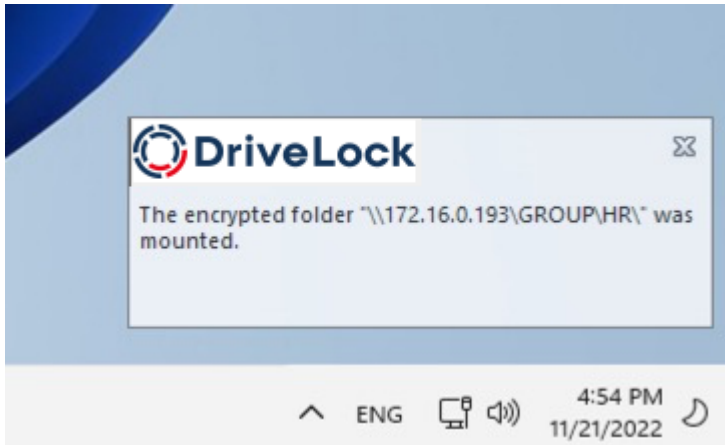
17.7 DriveLock Disk Protection

DriveLock Disk Protection is an integrated security and data encryption solution for hard drives. It can be used on the following operating system:

- UEFI BIOS: Windows 10 (64-bit only) or higher

DriveLock Disk Protection provides the following functions:

- Hard disk encryption

- Pre-boot authentication (PBA)

- Single sign-on or manual Windows authentication

- Emergency recovery of pre-boot users and token logins

- Emergency recovery and administration tools

17.7.1 Policy settings

17.7.1.1 Encryption certificates

Before installing Disk Protection, it is necessary to create certificates for data recovery. These files are required for performing emergency recovery and emergency logon procedures.

The following certificates have to be created:

- **Master Security Certificate (MSC):**

  The DLFDEMaster.cer and DLFDEMaster.pfx files produce a public/private key pair. DLFDEMaster.pfx is used to decrypt the hard disks. It has to be secret, stored securely, and available only to those who need to perform emergency recovery.

DLFDEMaster.cer is the public key component of the master certificate (MSC) and is automatically used for each installation.

- **Recovery Support Certificate (RSC):**
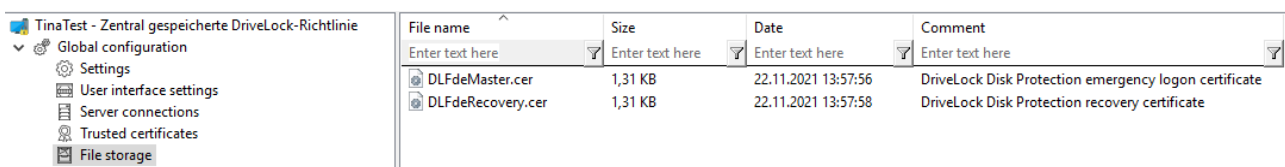
The DLFDERecovery.cer and DLFDERecovery.pfx files produce a public/private key pair.

DLFDERecovery.pfx is used for the emergency logon procedure. It should be secret, stored securely, and available only to those who perform password recovery (e.g., Help Desk / Support).

DLFDERecovery.cer is the public key component of the recovery certificate (RSC) and is automatically used for each installation.

> 📝 Note: Make sure that these files are saved in a safe place along with the password, as they will be used for emergency logon and data recovery. Recovery without this data is not possible.

Once the encryption certificates are created, the DriveLock Management Console shows the time and date of their creation.

File name	Size	Date	Comment
Enter text here	Enter text here	Enter text here	Enter text here
DLFdeMaster.cer	1,31 KB	22.11.2021 13:57:56	DriveLock Disk Protection emergency logon certificate
DLFdeRecovery.cer	1,31 KB	22.11.2021 13:57:58	DriveLock Disk Protection recovery certificate

Make sure to enable the Display sys**tem files setting so th**at these certificates appear:
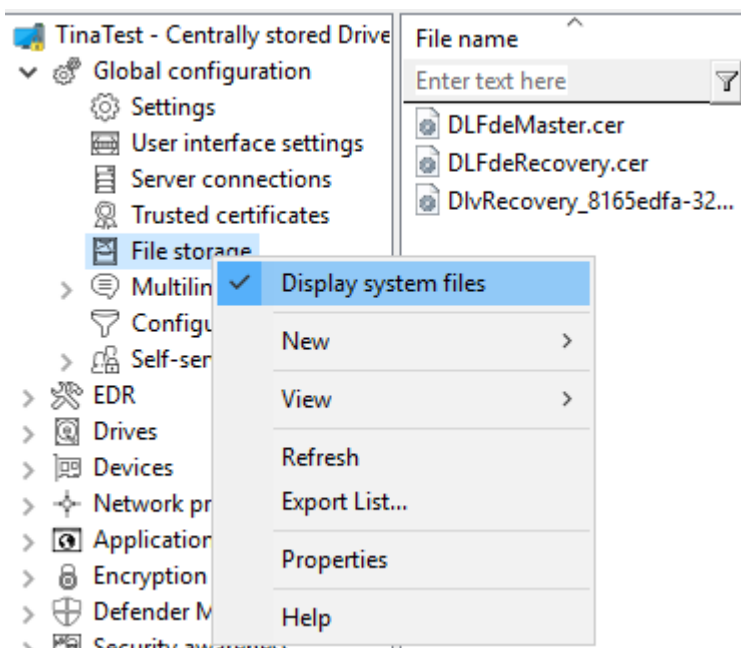
The certificates are also stored in the private certificate store of the current user:

17.7.1.1.1 Create encryption certificates

First, the central certificates must be generated, which are required for all recovery mechanisms. You can back them up on a smart card, for example, in addition to the options offered by DriveLock.

Please do the following:

1. In the Policy Editor, open the **Encryption** node.

2. Depending on which view you have selected, either go to the **DriveLock Disk Protection** section from the Taskpad view and select **Generate master certificates...** here. Or you can select the **Encryption certificates** option directly in the **DriveLock Disk Protection** sub-node.

3. In the dialog, click the **Generate certificates...** button. Then follow the instructions here from step 3.

> ⚠ Warning: Once the certificates have been generated and Disk Protection has been installed on the client computers, you must not create any new certificates, as this will overwrite the old ones making them unusable for recovery.

17.7.1.1.2 Recovery keys

Recovery information is stored in the database on DriveLock Enterprise Service (DES) by default. We recommend leaving this option enabled.

However, if you select one of the other two options **File server (UNC path)** or **Local folder on agent computers (not recommended)** on the **Recovery** tab, the following files will be created:

- **Recovery.env - Envelope file for emergency logon**

  DriveLock Disk Protection creates the envelope file and sends it to the location you configured immediately after the Agent has finished installing DriveLock Disk Protection on a client computer. The ZIP file containing the EFS recovery files is created and copied only after all drives have been fully encrypted.

- **DiskKeyBackup.zip - This ZIP file contains the EFS recovery file for the data recovery procedure.**

  The recovery files should be stored either on the DriveLock Enterprise Server or a central file share. Additionally, the files can be stored locally on the computer, but this is not recommended for security and recovery reasons.

If the files are stored on a central file share, the file names are as follows: <computer>.envelope.env and <computer>.backup.zip

> Note: Each client computer has its own corresponding envelope file that must be used for the emergency logon. If you have configured Disk Protection to automatically place the file on a central file share, the file name starts with the name of the client computer (e.g. DE2319WX.Envelope.env).

17.7.1.2 User-related agent settings

By default, DriveLock Agent users are notified of the installation of or encryption with Disk Protection and their client computer is restarted after 30 seconds. You can change these settings if necessary.

Agent settings tab

On this tab you can decide whether notifications are displayed or not, and you can also choose when they appear in the notification area: during configuration, during encryption and/or before installing updates.

The **Display user information / confirm computer restarts** option and the four options below it are enabled by default.

Select the **Do not restart computer (wait until manual restart)** option if you want to control it yourself. This allows you to start your own installation script, for example, with a shell command after the installation.

Two options are available:

- **Run as the currently logged on user**: The script runs with the rights of the user who is currently logged on. Normally it would run under the local system account.

- **Run also after uninstall**: The script runs during installation and uninstallation.

Appearance tab

On this tab you specify how Disk Protection or the DriveLock PBA is displayed to end users.
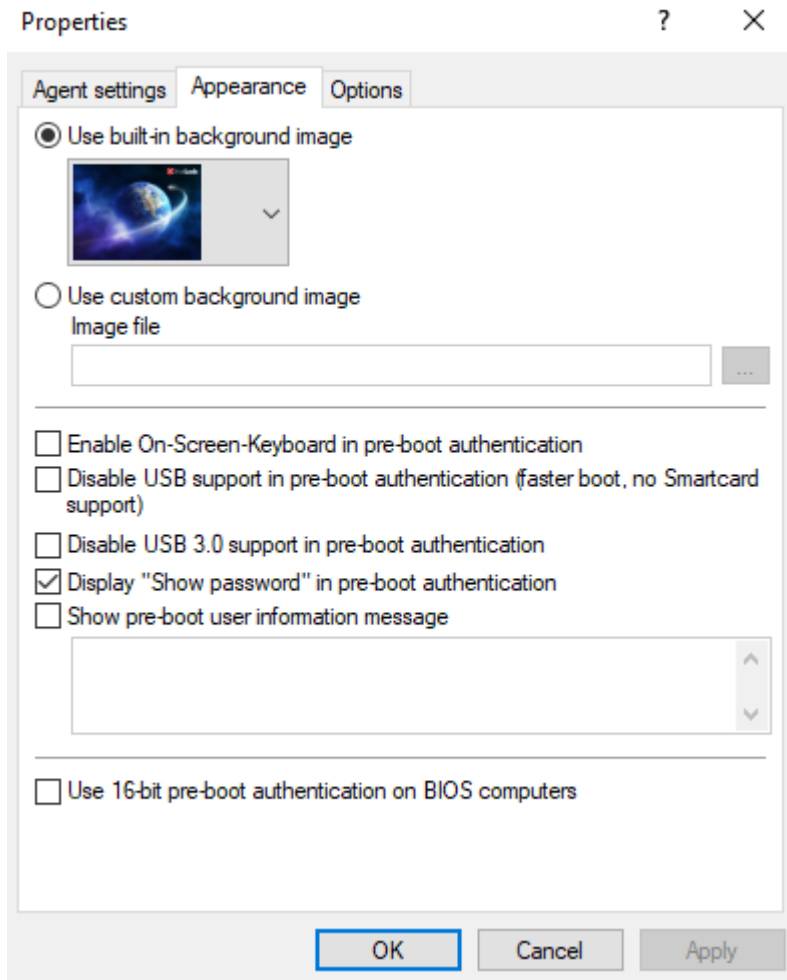
- **Use built-in background image**: Disk Protection comes with ready-made images from which you can select the image you want to use for pre-boot authentication.

- **Use custom background image**: you select the file from the policy's file storage or from the file system, format PNG, maximum 32 MB, optimal resolution 1024x768.

- **On-screen keyboard**: With the help of a virtual keyboard, user entries can be made even without an existing real keyboard

- **USB support**: If this is deactivated, the PBA can be loaded faster. Note that the USB interface will not work with devices such as a mouse or smartcard reader.

- **USB 3.0 support**: This option disables the support of USB 3.0 devices within the PBA

- **Show password**: This can be used to prevent an entered password from being displayed in plain text. This option is set by default.

- **Show pre-boot information message**: Enter your own user information in the text field, which is then displayed within the PBA, e.g. notes on use or contact persons

527

- The option **Use 16-bit pre-boot authentication on BIOS computers** is only possible if you still have BIOS computers in use. The 16-bit PBA is no longer supported for DriveLock pre-boot authentication under UEFI systems.

Options tab

Show DriveLock Disk Protection logon messages: Select this option if you want the pre-boot authentication logon information to be displayed in the client computer's notification panel after logging in to Windows.

A message with detailed information pops up on the client computer.

> 🖉   Note: The other options in this dialog are only relevant for BIOS systems.

17.7.1.3 Hard disk encryption settings

The following settings are available in this dialog.

On the **General** tab:

- Here you can enable Disk Protection encryption by selecting the **Encrypt local disks on agent computers** option.

- AES **is preset as encryption algo**rithm; you can use it as such. You can choose between different encryption algorithms, we recommend AES 256-bit.

- With **Configure encryption settings per drive** you can specify the encryption for each drive separately. The default setting is to encrypt all local hard disks.

- If you select **Enable FIPS compliant encryption library**, the FIPS library will be used. Performance is better if you do not select this option; a CC EAL-2 certified non-FIPS library automatically uses AES NI (Intel® Advanced Encryption Standard (AES) Instructions Set) hardware support if the client supports it.

- To display a warning to all users indicating incomplete disk encryption, you can enable the **Display warning when disks are not fully encrypted** option.

- **Encryption priority**: Specify the computer performance used for encryption. **Normal** is the default value. When set to **High**, other applications may run slower.

- **Perform hard disk check (ChkDsk) before encryption**: Use this option to ensure the integrity of the file system on all drives you want to encrypt. This will repair all bad sectors so that Disk Protection can encrypt them.

- Disk Protection manages a memory for some BIOS interrupt vector addresses (Legacy BIOS only). This allows Disk Protection to detect potential attacks launched by changing the interrupt vector addresses. If it detects a difference between the BIOS interrupt vector address and the previously saved copy, an error message is displayed.
If the interrupt vector address changes (e.g. due to a BIOS update), the error is still displayed. The system protection group provides a mechanism to accept authorized changes, by updating the copy of disk, keyboard, and clock tick interrupt vector addresses.
You can completely disable interrupt vector checks with the **Disable any interrupt vector protection** option.

- Enable the **Encrypt only if pre-boot login succeeded at least once** option to delay the encryption of the disks until a user has successfully logged in to pre-boot authentication once and has thus been stored in the user database of the PBA.

- If you want to delay decryption for some time, specify the number of days with the **On configuration changes, delay decryption by x days** setting. This may be useful so that the client computers and their users can be properly prepared for decryption. The default value is **3** days. This value provides additional protection against misconfiguration. If you want to perform decryption immediately, change the setting to 0 days.

On the **Recovery** tab:

Here you specify where to store the DriveLock Agent recovery keys for the challenge response procedure.

17.7.1.4 Pre-boot authentication settings

17.7.1.4.1 General

In the **Pre-boot authentication settings**, you can activate pre-boot authentication for DriveLock agents that are protected with Disk Protection.

On the General tab, select the **Enable pre-boot authenti**cation **option.**
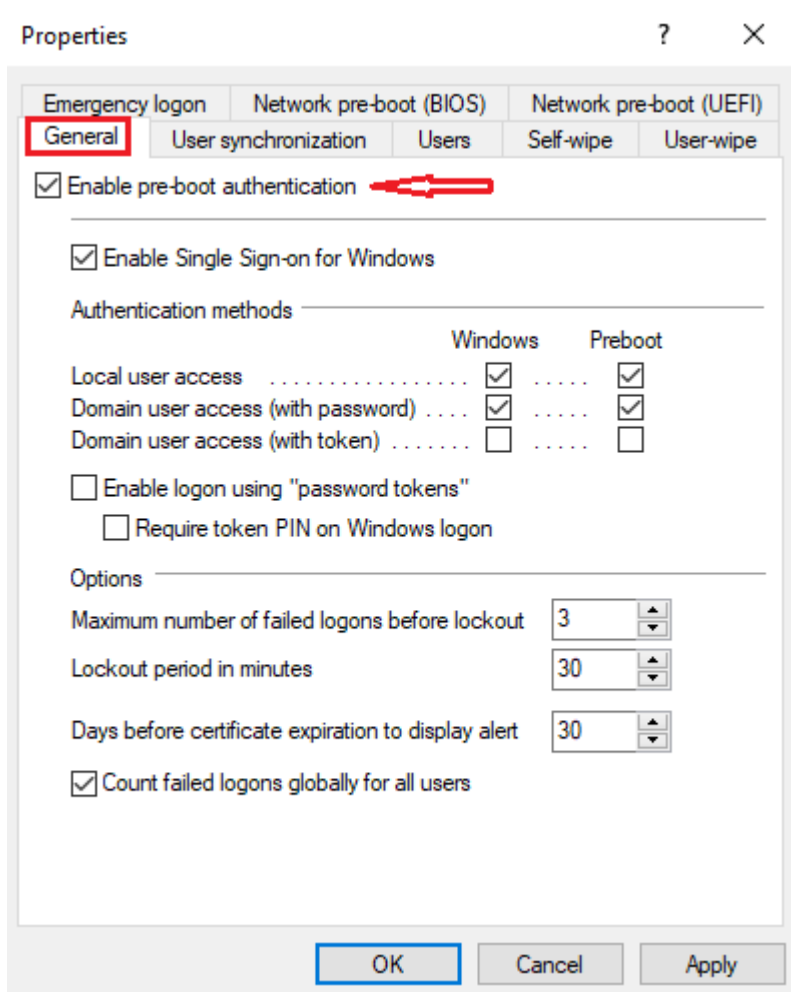
To access a system protected by Disk Protection, authentication is required at both the pre-boot authentication level and the Windows access level. In single sign-on mode, an end user only needs to log in once for both levels (pre-boot and Windows). That's why the option **Enable single sign-on for Windows** is set by default.

A combination of local users, domain users (with password) and domain users (with token) are available to the user for pre-boot and Windows authentication. Here, too, the top two options are set by default.

- **Local user access**: This default method allows local Windows users to authenticate to the system using their local Windows user name, password, and local system name.

- **Domain user access (with password)**: This method allows Windows domain users to authenticate to the system using their Windows domain username, password, and domain name.

- **Domain user access (with token)**: This method allows Windows domain users to authenticate themselves with a smartcard / token and PIN.

- **Enable logon using "password token"**: This method allows pre-boot authentication for a password token user. If you select this option, you have to select at least one Windows authentication method. If you check this option, then you need to select at least one more Windows authentication.

> 🗹 Note: Make sure there is a valid token for both PBA and Windows logon (unlock) before configuring Disk Protection for token access only.

- **Count failed logins globally for all users** is preset and causes failed attempts to be counted up regardless of the specified user.

> 🗹 Note: After a certain number of failed logins, a user can be locked out for a certain amount of time to protect the system from a brute force attack using automated login scripts. Change the default values according to your corporate security policies.

- If you use certificates for authentication you can also configure how many days before the expiration of a certificate DriveLock Disk Protection notifies the user of the upcoming expiration.

Once a policy with this setting takes effect on the DriveLock Agent, the PBA is enabled there and the end user is presented with a corresponding dialog.

17.7.1.4.2 Network pre-boot (BIOS)

> ⚠ Warning: Please note that since version 2022.2, DriveLock Legacy BIOS Pre-Boot Authentication is no longer supported and has been removed from the product. When installing an agent from version 2022.2, the system checks whether an active legacy BIOS PBA is present on the system. In this case, an update or installation of the agent will not be performed.

For some legacy BIOS systems, Disk Protection provides network-capable pre-boot authentication that can automatically detect whether a computer is part of a pre-defined corporate network and deactivates logon to the PBA (auto-boot).

This functionality is only available for some systems and can only be activated with the appropriate assistance of a DriveLock Professional Service Team member.

17.7.2 Decryption

Disk decryption may start for the following reasons:

- The **Encrypt local disks on agent computers** option is disabled within the policy (see below)

- The assignment of the policy containing the disk protection settings is removed or disabled

- The Disk Protection license option within an assigned policy is removed

> 📝 Note: You can monitor the decryption process, just like the encryption process, in the DriveLock Operations Center (DOC).

To start decrypting encrypted drives, proceed as follows:

1. Open the corresponding Disk Protection policy.

2. Open the **General** tab in the **Harddisk encryption settings** dialog.

3. Uncheck the **Encrypt local hard disks on Agent computers** option.

4. If you want to perform decryption immediately, change the **On configuration changes, delay decryption by x days** setting to 0 days.

5. Confirm your setting.

6. Decryption will be carried out on the DriveLock Agent with the corresponding messages.

17.7.3 Overwrite policy (Disk Protection)

If you want to make changes to Disk Protection configuration only on very specific computers (e.g. uninstall Disk Protection, decrypt hard disks), the setting can be overridden specifically for an individual agent, regardless of the central configuration.

You can achieve this with the help of the remote agent control. First connect to a DriveLock agent and select **DriveLock Disk Protection properties** from the context menu.

Click **Reconfigure agent**.

Activate **Override policy** to configure computer-specific settings in deviation from the central policy. The selected settings apply only to the currently connected computer.

You can see which users are stored in the computer's PBA on the **Users** tab. You can add or delete individual users here.

17.7.4 DriveLock Disk Protection Recovery and Tools

Disk Protection covers two different recovery methods:

- Emergency notification procedure
  The emergency logon procedures are used when a user is no longer able to log on to the pre-boot authentication (e.g. the user has forgotten his password or PIN).

- Recovery of encrypted drives (data)
  Recovery becomes necessary when local drives can no longer be accessed. This happens, for example, when data sectors of a drive are damaged and you can no longer log on to Windows.

Both procedures are performed via the Recovery Wizard. Right-click **Agent remote control** in the **Operating** node, and then select **DriveLock Disk Protection recovery and tools / Disk recovery / emergency logon** from the context menu.
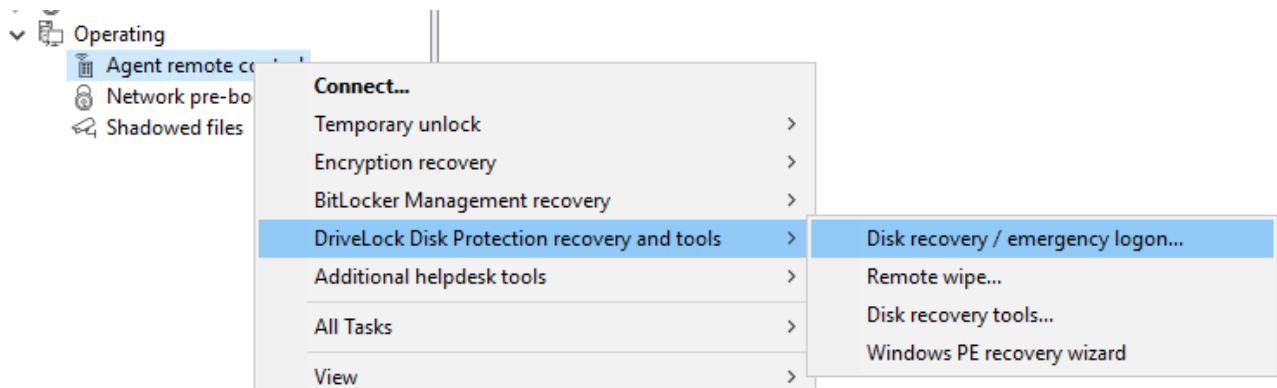
17.7.4.1 Retrieving diagnostic information

When DriveLock Disk Protection is installed, the DriveLock Agents sends the installation log file to the DriveLock Enterprise Services. You can retrieve this file from the DriveLock database to find out more details, if a Disk Protection installation has failed.

Please do the following:

1. Select **Retrieve diagnostic information** and select **DriveLock Enterprise Service**.

2. Select the DES Server connection from the list.

3. To search for Agents registered in the DriveLock database, type the computer name or part of the name and then click Find. DriveLock Disk Protection displays all registered computers that contain the text you typed as part of their names. To view a list of all registered computers, don't type any text and the click Find.

4. Select the appropriate computer from the list.

5. Select the path where to store the diagnostic file. Click Next to retrieve the file from the DriveLock database.

6. After the file has been retrieved, click Finish. A ZIP file containing the diagnostic information is created in the location you specified.

17.7.4.2 Settings for the emergency logon (challenge response)

The emergency logon procedures are configured in the Pre-boot authentication settings.

To assist the end user with the emergency logon, follow these steps:

1. Open the recovery wizard.

2. Select **Emergency logon**. If your recovery keys are sent to the DriveLock Enterprise Service, do not change the default setting **DriveLock Enterprise Service**. To specify the path to the required recovery keys later, select **Recovery files (copied by agent computer)**.

3. For the emergency logon procedure you need the private key of the recovery certificate. In the second dialog, specify the storage location, either Windows certificate store, a smart card or a PFX file together with the respective password. For more information on certificates, please click here.
If you are using a smart card, you will be prompted to insert and select the card you are using.

4. The third dialog provides a list of computers where you can select the computer to restore. Check the option **only show the most recent entry for each computer**. Click **Next**.

5. Next, you will see the dialog for entering the user's request/recovery code.

   > Note: For more information on the interaction between administrator and end user, click here.

   Enter the code in the appropriate text boxes (see figure). You can optionally specify the name of the user.

   > Warning: The recovery code provided by the user is mandatory.

6. Click **Next** to generate the response code.

7. Tell the user the **response code**.

8. Click **Finish**.

17.7.4.3 Recovering encrypted drives

Drive recovery is necessary when local drives can no longer be accessed (e.g. when data sectors of the drive are defective).

In order to restore (decrypt) an encrypted drive, you need to perform the following four steps:

1. Create the recovery files

2. Copy all the files necessary for decryption to a USB removable disk or to the recovery CD

3. Boot the computer with the recovery CD

4. Use the recovery files and tools to decrypt the desired hard drive(s) on the affected computer.

17.7.4.3.1 Disk key recovery

Please do the following:

1. Select **Disk key recovery** as the recovery type.

2. If you have configured Disk Protection to send the client recovery keys to DriveLock Enterprise Service, select the **DriveLock Enterprise Service** option. To specify a file as the location of the required recovery disk keys, select **Recovery files (copied from the agent computer)**.

3. In the next dialog, select where the certificates/recovery keys are stored. You can either enter the path to the DLFDEMaster.pfx file and the corresponding password (**File system** option). Or you can select **Smart card** to access a private key that was stored on a smartcard. If the certificate information with the private key was imported into the local certificate store of the currently logged in user, you can also select the first option **Windows certificate store**.

4. In the next dialog, either select the agents with DriveLock Disk Protection or specify the file for the recovery information.

> Note: Each client computer has its own corresponding EFS recovery file that must be used for drive recovery. If you configured DriveLock Disk Protection to upload this file automatically to a central shared folder, the file name is pre-fixed with the name of the client computer (for example: DE2319WX_ Backup.zip). The EFS disk recovery files are automatically generated by the DriveLock Agent when it starts encrypting hard disks.

5. In the next dialog you specify where the disc key will be stored. It is necessary that Disk Protection creates a special disk key. Specify a file name and path. Alternatively, you can specify the path and file name manually.

> Note: Make sure to specify the correct file extension (*.dke).

Specify a password to secure access to this file. The password must be at least six characters long It will be needed later for recovery.

Select the **Save full pre-boot authentication backup to folder** checkbox and type the path for the location of the Backup.zip file that contains all recovery data stored in the DriveLock database for this computer.

6. Click Next to create the disc key.
   If you selected a smartcard, you will be prompted for the PIN that is required to access the smartcard.

7. Now you can copy the created file to a USB drive or the recovery CD to use it in the next steps.

17.7.4.3.2 Creating a recovery medium

To recover a system that can no longer be booted, you need bootable recovery media (or a recovery CD) to boot the system.

Note: You only need one recovery medium for your system environment, because the individual recovery file is copied to another USB stick.

Before you start the wizard, make sure you meet the following requirements:

- You have administrative privileges on your computer to install the Windows Assessment and Deployment Kit (ADK) (if not already installed).

> ⚠️ Warning: The ADK must be installed in order to create a recovery image with the Windows PE Recovery Wizard.

- The latest DriveLock Management Console is installed on your computer.

- A USB stick (min. 1GB) or a writable CD for the Windows PE recovery medium is ready.

17.7.4.3.2.1 Windows PE recovery wizard

Invoke the wizard using the context menu commands **DriveLock Disk Protection recovery and tools**, and then **Windows PE Recovery Wizard** in the Agent Remote Control sub-node.

1. In the first dialog, simply click **Next**.

2. In the second dialog you accept the license.

3. In the third dialog, make sure that all preconditions are met and marked with a green check mark.

4. In the fourth dialog you specify the directory where the output files should be written, select the language and the target architecture of the Windows PE environment to be used.

> ⚠️ Warning: The amd64 architecture must be selected for UEFI systems.

   You can now specify additional drivers and other tools to be added to the Windows PE environment. These can be additional hard disk drivers or any other tools that can be run without an installation (e.g. antivirus scanners, backup tools, additional third-party tools, etc.).

5. In the following dialog, select whether you want to create a bootable ISO file or a bootable USB stick. If you do not make a selection, only a file structure is created, which you must copy manually to a bootable medium yourself. Start the automatic process by clicking **Create WinPe image**. As soon as the process is completed, a corresponding message appears.

6. When the process is finished, you will be shown the links to the respective directory. Click **Finish** to exit the wizard.

The recovery CD created in this way now contains all the tools, drivers and recovery files necessary for recovery.

17.7.4.3.3 Recovering disks

Before you can start the recovery, make sure you meet the following requirements:

- The *.dke file required for the computer was created and copied to a USB flash drive.

- You have created a bootable Windows PE recovery media.

Now boot the computer from the recovery medium.

Then you will see a command line window with a list of available disks (volumes). To display this list again, use this command: `echo lis vol | diskpart`

Encrypted volumes are displayed in the Fs column as RAW. Memorize the drive letter of the USB stick that contains the recovery file (if necessary, insert the stick and display the list again).
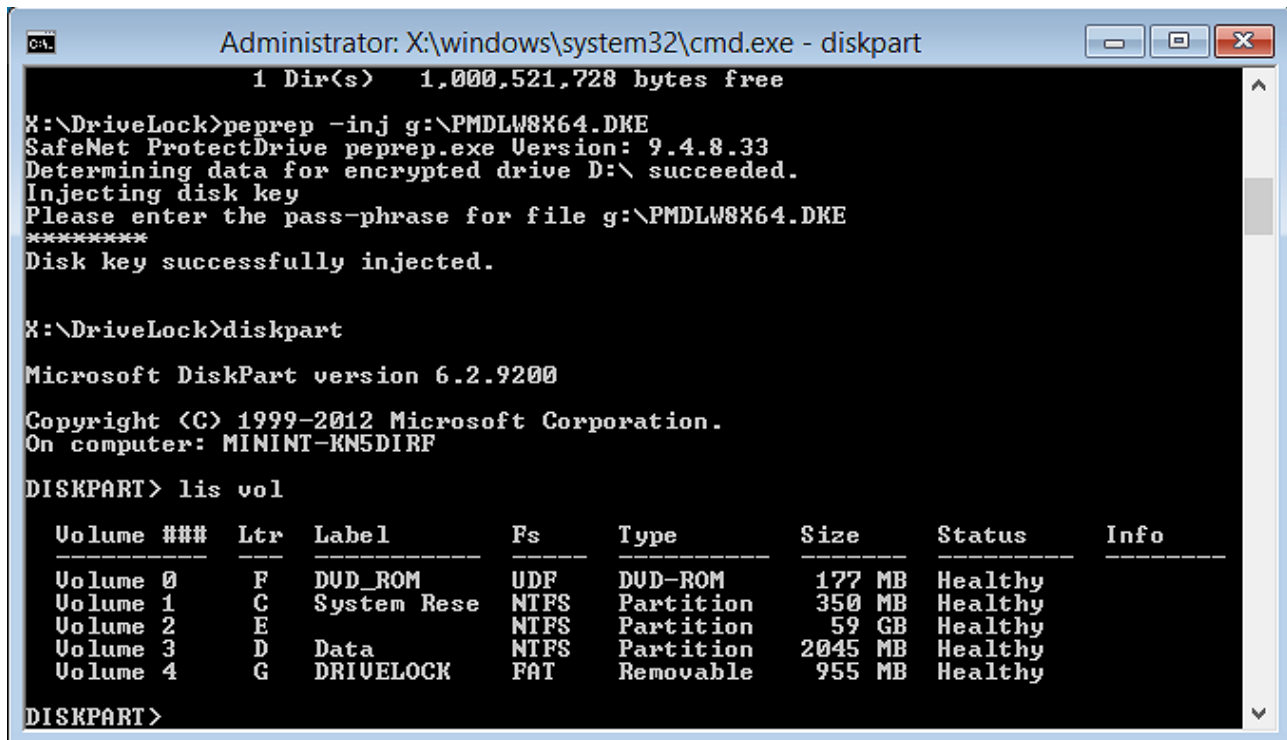
Enter the command `cd X:\DriveLock`

Use the following command to introduce the recovery key for decryption to the system:

```
peprep -inj <USB drive letter>:\<path to disk key file>
```

The command in this example is `peprep -inj G:\PMDLW8X84.DKE` Now enter the password that you used to create the DKE file.

Run the command `echo lis vol | diskpart` again to see if the recovery key was successfully added.

If the action was successful, the drive will no longer be displayed as RAW.
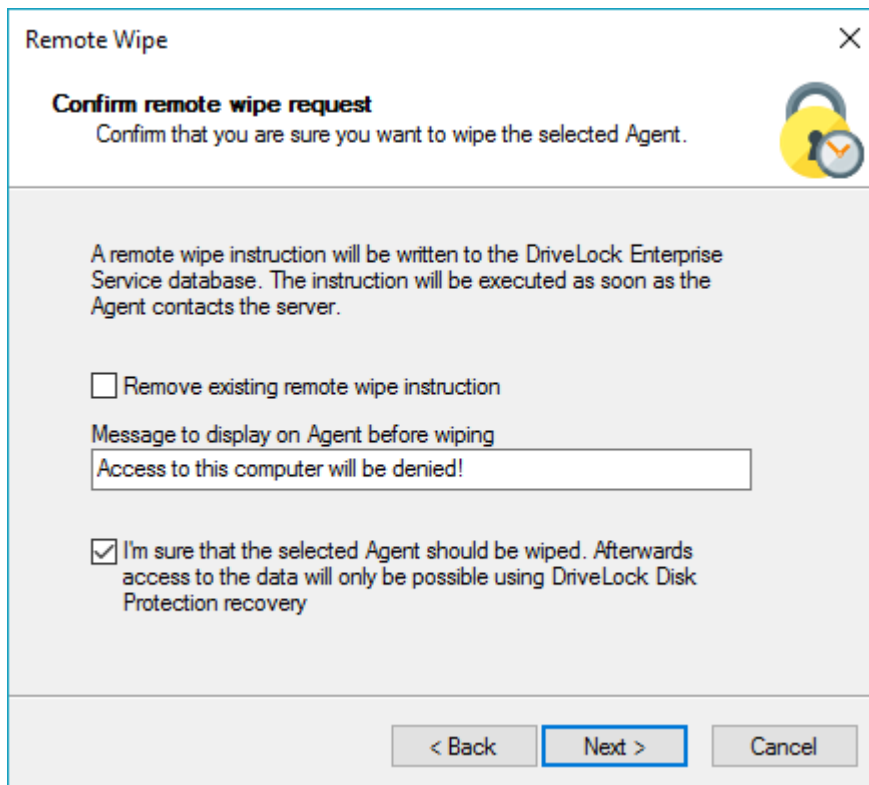
Enter `Exit` to leave DISKPART.

You can now access the drive (provided there is no other critical issue) and copy important files or try to repair the hard drive.

17.7.4.4 Remote wipe

An administrator is able to remove the DriveLock PBA. To initiate a remote wipe, in the DriveLock Management Console, select **Operating**, then **Agent remote control**. Open the context menu and select **DriveLock Disk Protection recovery and tools** and then **DriveLock Disk Protection remote wipe...**.

You are prompted to provide the private key of the recovery certificate. Enter the path to the DLFDERecovery.pfx file and the correct password. Then select the computer you want to delete. In the next dialog you have to **confirm the remote wipe request**. The settings made are activated as soon as the computer connects to the DES. The DES must be accessible from the Internet to enable remote wiping from outside the company network.

Configure the settings as shown in the dialog.

Select **Remove existing remote wipe instruction** to revoke a previously issued remote delete command (if the PBA database is not already deleted).

18 Defender Management

DriveLock allows you to configure Microsoft Defender via the Policy Editor and keep track of the current status of DriveLock Agents in the DriveLock Operations Center (DOC).

All existing Microsoft Defender Antivirus Group Policy (GPO) settings can be configured in the Policy Editor.

For quick configuration, selected settings are available from within the Taskpad view:

- Settings for scanning file accesses and response to detected malware

- Exceptions for file checks or processes

- Regular scans with date and time, frequency and type of response

- Type and content of end user notifications

In addition, you can configure settings for using Defender to scan external drives:

- Use virus scanner when connecting external drives and, if necessary, automatically block access if malware is detected

> 📝 Note: Due to a known limitation of the GPO ADMX format, only operating systems from Windows 8.1 and newer are supported.

The DriveLock Operations Center (DOC) allows you to view status reports on current threats and the status of DriveLock Agents. Any threats found can be analyzed precisely and, if necessary, false or irrelevant notifications can be suppressed.

> ⛔ Warning: A license is required for Defender Management.

18.1 Configuration in the Policy Editor

18.1.1 Overview in the DriveLock Management Console

Once licensed, the policy includes the new node **Defender Management**. Here you can configure the settings for Defender. From this overview, you can enable (or disable) Defender functionality and thereby integrate its control into DriveLock.
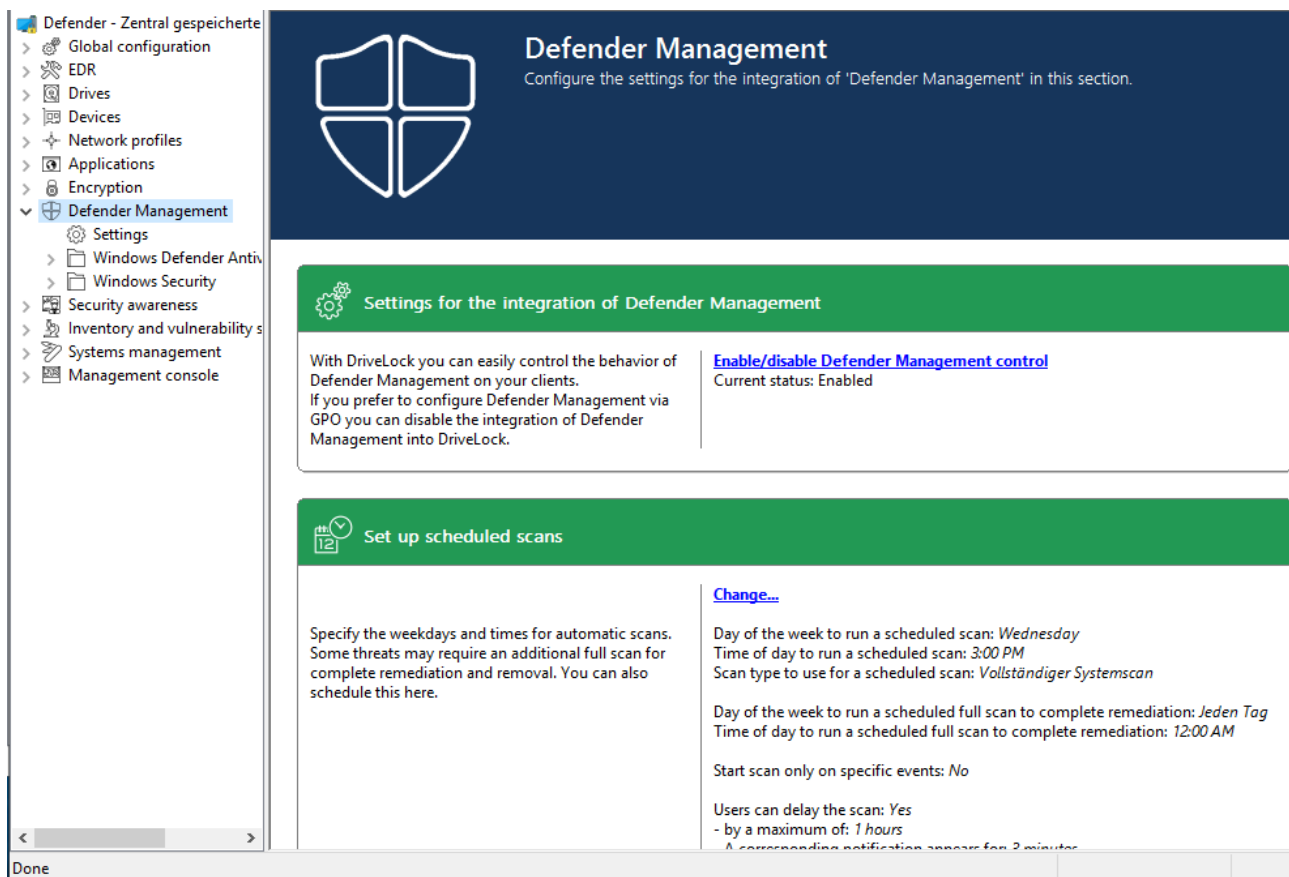
In case another view opens in your policy, you might have to change the **Show basic configuration** setting. To see the basic configuration options, make sure to enable this setting at the highest level of the policy, see figure:
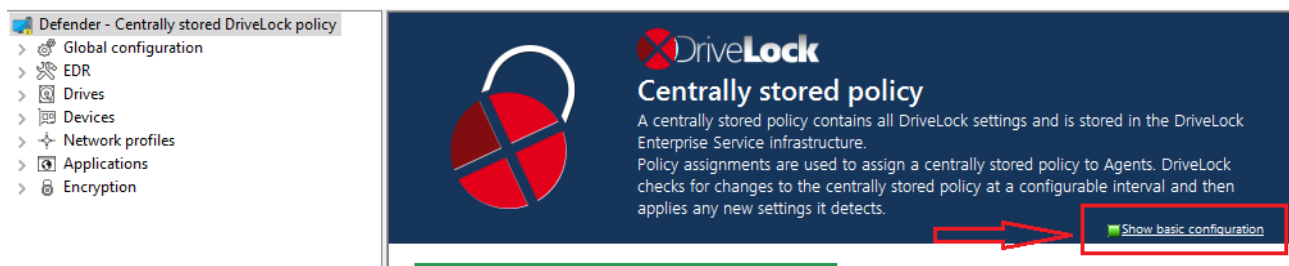
18.1.2 Easy configuration in the Taskpad view

In addition to enabling Microsoft Defender control, you can configure other basic settings in the Taskpad view of the **Microsoft Defender** node.

1. **Set up scheduled scans**
    Here you can configure the following:
    -   Time and type of scan: If you specify the time for the scheduled scan at this point, DriveLock uses its own scheduler to start the scan at the defined time. Microsoft Defender's own settings such as **Randomize scheduled task times**

544

or **Start the scheduled scan only when computer is on but not in use** are not considered.

- Time for complete remediation: This specification is necessary because some threats can be eliminated by Microsoft Defender only after another complete scan.

- Scan delay and scan events: When you set up scheduled scans, you can define that scans may only start under certain conditions and that users may delay scans.
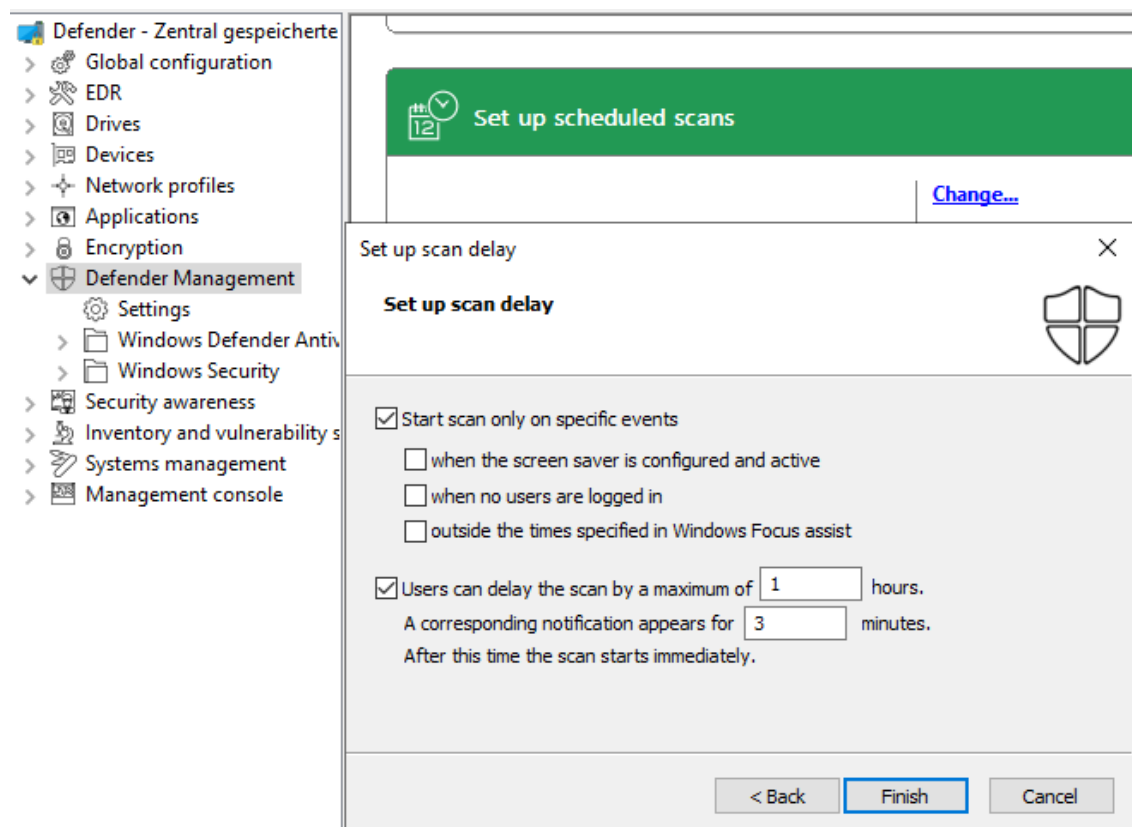
> Note: If you want to use Microsoft Defender's own scheduler, configure the appropriate settings in the **Windows Defender Antivirus** subnode in the **Scan** setting.

2. **Scanning options**:
   Configure the antivirus scanning options here.

3. **Exclusions**:
   Configure the exclusions here to exclude certain files from Microsoft Defender antivirus scans. For more information, see Microsoft.

4. **Automatic remediation action**:

Configure the automatic remediation action for each threat alert level.

The classification of individual threats according to threat alert level (low, medium, high, severe) is stored in the Defender signature definitions. For example, you can display this information using Powershell with the Get-MpThreatCatalog command. The SeverityID corresponds to the threat alert level:

1 = Low

2 = Medium

4 = High

5 = Severe

5. **Attack surface reduction**:
   Create rules for Attack Surface Reduction (ASR) here.

18.1.3 Settings

18.1.3.1 General settings

You can configure the following general settings to integrate Microsoft Defender into DriveLock:

- Enable/disable Microsoft Defender control

- Clear existing Microsoft Defender configuration

- Show advanced configuration options

18.1.3.1.1 Enable/disable Microsoft Defender control

To permit DriveLock to control Microsoft Defender on DriveLock Agents, you must activate the **Enable/disable Microsoft Defender control** setting in the policy. This is the default setting.

> Note: This setting only affects the control by DriveLock and not the actual functionality of Microsoft Defender.

18.1.3.1.2 Show advanced configuration options

If you select **Show advanced configuration options**, two additional configuration options appear in the configuration dialogs of the **Windows Defender Antivirus and Windows Security** nodes, which are invisible otherwise.

The example shows the dialog for the e-mail scan settings:
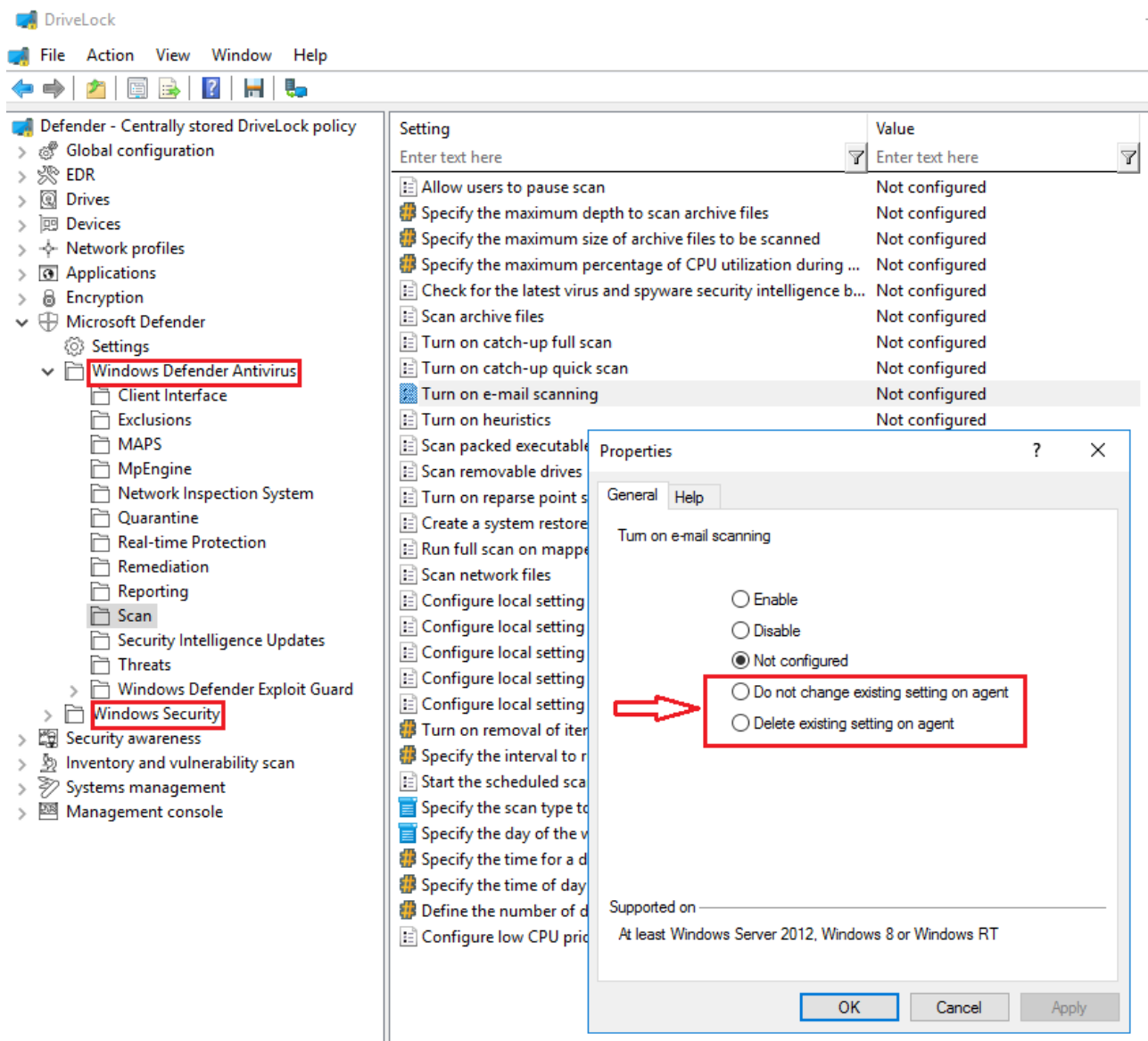
These configuration options provide the following benefits:

- **Do not change existing setting on agent**

  If a setting is already applied to the agent, DriveLock will not change it.

  > Note: In contrast to **Not configured**, DriveLock does not change such a setting, regardless of whether it is set in another assigned DriveLock policy or not. This applies to policies that come **before** this policy in the order of assignment.

  Example:

  You want to apply specific Defender settings to all DriveLock Agents. Create a

  DriveLock policy with the appropriate settings and assign them to your agents. You

want to allow one department to configure some of these settings independently (e.g., via Group Policy, manually or with another external tool). To avoid having to copy the entire policy and only change these few settings, you can create a new policy and set the relevant settings in this policy to **Do not change existing setting on agent**. Assign this new policy to the agents so that it appears after the existing Defender policy.

- **Delete existing setting on agent**
  If you specify this value for a Defender setting from the **Windows Defender Antivirus** node, the Defender setting is deleted from the DriveLock Agent. The Defender will then use its default setting.
  This option can be compared to the Clear existing Microsoft Defender configuration setting, except that it is used for a single setting, while **Clear existing Microsoft Defender configuration** will clear all settings.

18.1.3.1.3 Clear existing Microsoft Defender configuration

The **Clear existing Microsoft Defender configuration** setting determines whether DriveLock maintains existing Defender settings on the agent or deletes them before applying the policy.

By default, the DriveLock Agent maintains the existing Defender configuration and only applies those settings that are included in the DriveLock policy.

18.1.3.2 Settings for Defender scans with DriveLock Scheduler

The following settings apply to executing scheduled scans with DriveLock Scheduler:

- Scheduled scan day
- Scheduled scan time
- Start scan only on specific events
- Allow users to delay the scan
- Maximum number of hours to delay the start of the scan
- Time in minutes after which the notification is automatically closed

18.1.3.2.1 Scheduled scan day

This setting lets you specify a day when scanning will be performed.

You can change or delete the day of the week for the Defender scan by setting it to **Not Configured**.

18.1.3.2.2 Scheduled scan time

This setting lets you specify a time when scanning will be performed.

You can change or delete the time for the Defender scan by setting it to **Not configured**.

18.1.3.2.3 Start scan only on specific events

With this setting, you can specify that the Defender scan may start only when certain events occur. As a result, users will not be disturbed during their work.

> 📝 Note: The screen saver must be active and configured when selecting the corresponding option. Otherwise the option will be ignored.

You can specify a detailed setting of notification times in the Windows Focus Assist, which DriveLock will query. Use this option to run the scan (or display notifications) only outside of these configured times.

18.1.3.2.4 Allow users to delay the scan

To keep the CPU load on the respective client computers as low as possible, you can specify here that users are allowed to delay a Defender scan. Select **Enable** to do so.

You can configure how long the delay will last and whether a corresponding notification will be displayed to the user.

18.1.3.2.5 Maximum number of hours to delay the start of the scan

At times, users may want to postpone the start of a Defender scan, for example, to continue to work without interruption or when performing automated tasks. For this reason, a delay of up to 16 hours can be configured.

Enter an appropriate value in the dialog.

Once the delay expires, the notification dialog is closed on the client computer and the scan is then started immediately.

18.1.3.2.6 Time in minutes after which the notification is automatically closed

Use this setting to configure how long the notification dialog stays open for the user.

As soon as the notification dialog closes automatically without the user entering a delay, the scan is started. In this case, the shorter configured time (delay or display time) always applies.

18.1.4 Windows Defender Antivirus and Windows Security

The **Windows Defender Antivirus** and **Windows Security** subnodes contain all settings for Microsoft Defender that can be distributed using Group Policy as of June 2019.

The DriveLock Agent stores the settings from the DriveLock policy in the same location in the registry where Group Policy settings are stored. The Defender settings can then be found at

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender` and/or
- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center`

If the Clear existing Microsoft Defender configuration setting is disabled, you can use Group Policy or another external tool to distribute some of the Defender settings in addition to the DriveLock policy.

18.1.5 External drives

18.1.5.1 Scanning external drives

You can configure an external drive in policies to automatically start a virus scan when it is connected to the computer. This way, users can only access the drive when the scan is complete and no malware has been found.

18.1.5.2 Configure removable drive locking

Please do the following:

1. Open the **Drives** node in the policy, select the **Removable drive locking** subnode and select the relevant drive to edit it.

2. Switch to the **Options** tab in the dialog.

3. Check the option **Scan for malware with Microsoft Defender before granting access**.
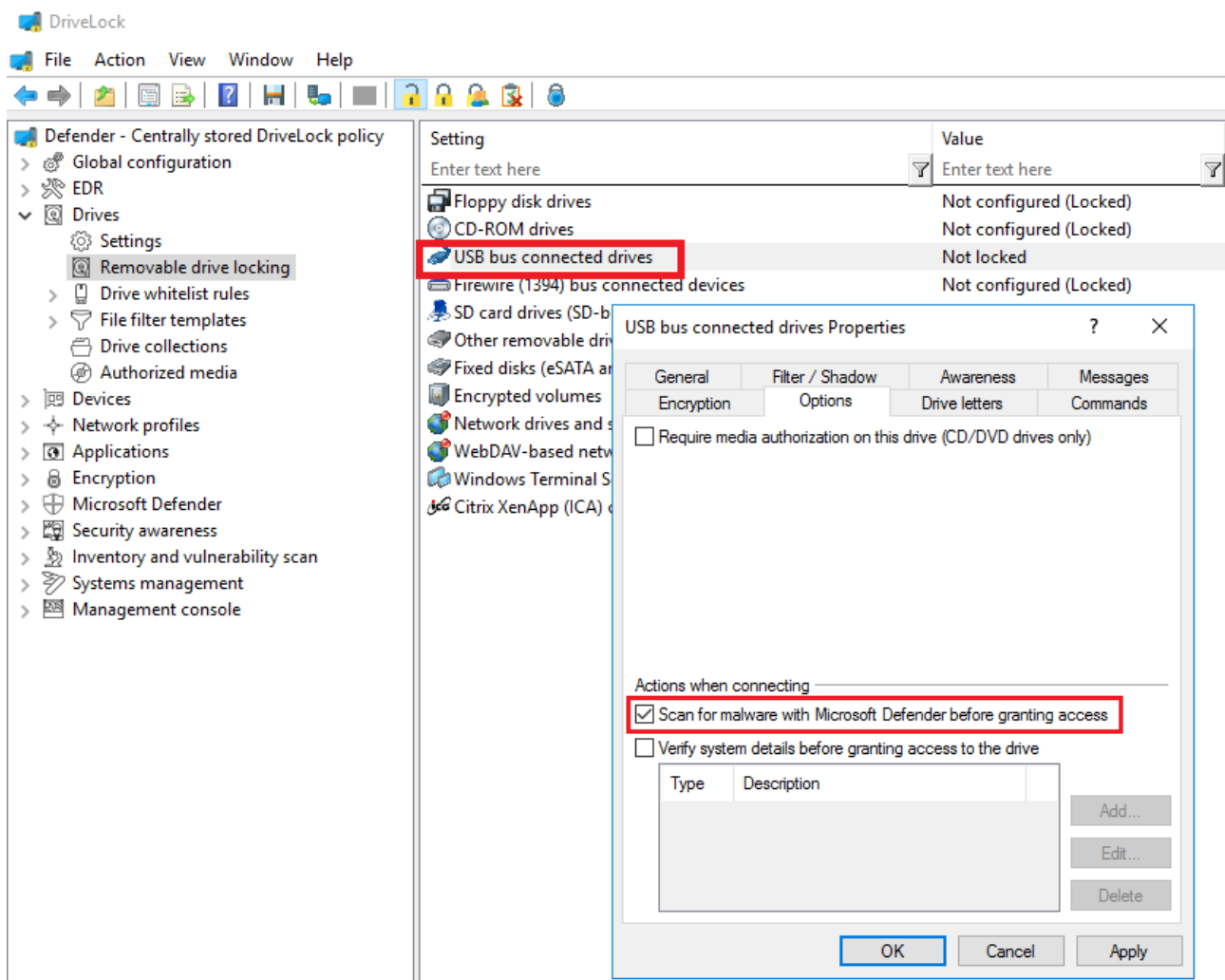
18.1.5.3 Configure drive whitelist rules

Please do the following:

1. Open the **Drives** node in the policy and select the **Drive whitelist rules** subnode. Create a new whitelist rule or open an existing one for editing.

2. Switch to the **Drive scan** tab in the dialog.

3. 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.

18.2 Agent remote control

18.2.1 Properties of the DriveLock Agent

Connect to a DriveLock Agent via **Agent remote control** and open its properties dialog by double-clicking on it.

On the **Defender** tab you can find current information about the Defender status on the respective agent.

18.2.1.1 Options in the Defender dialog

On this tab you can see the time of the last scan on the agent, check whether any errors occurred and, for example, whether antivirus protection is enabled or what version the signature has.
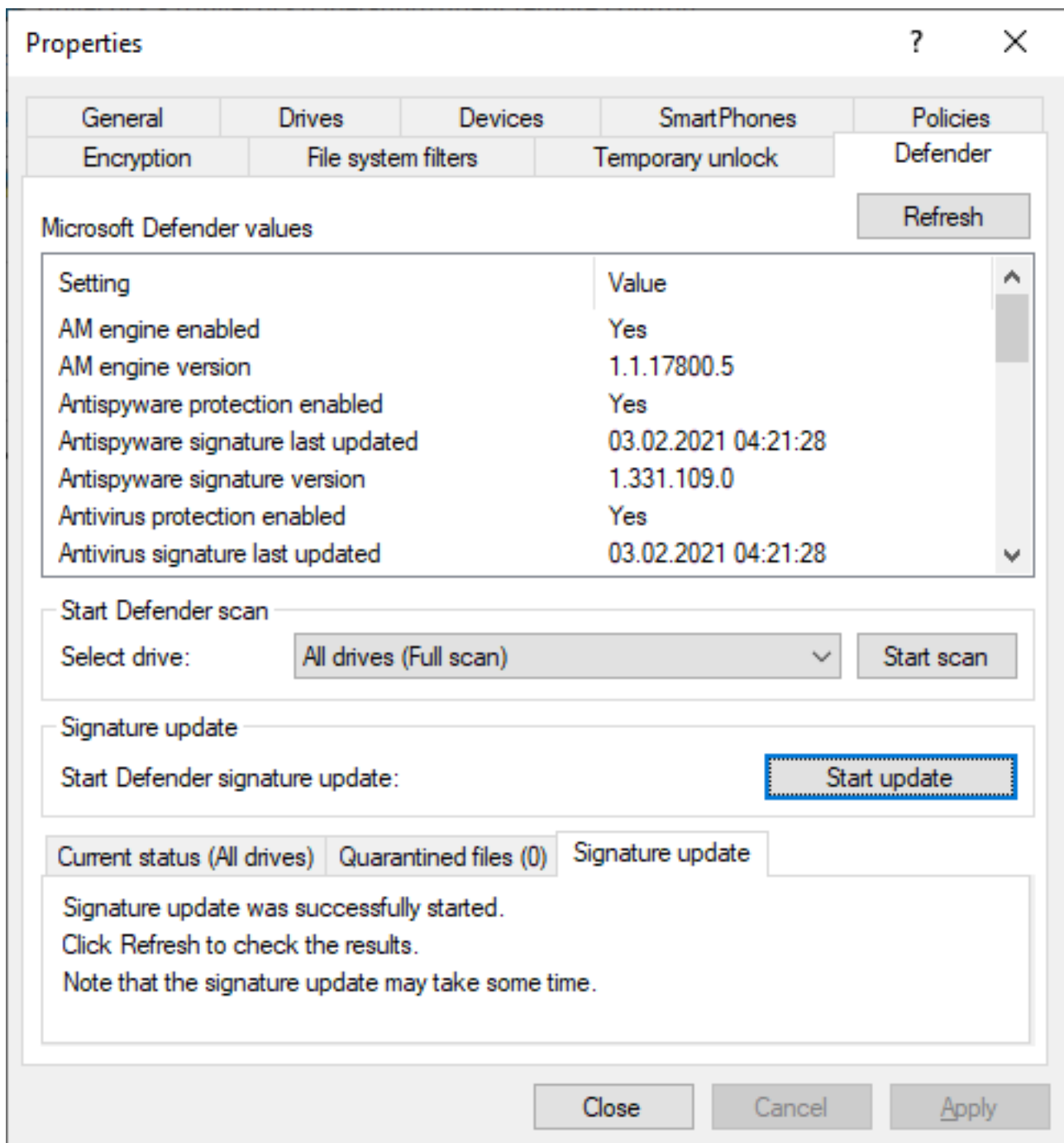
The following options are available:

- Click **Refresh** to reload the values.

- Click **Start Scan** to start a Defender scan immediately. Then if you click **Refresh**, the current status will appear on the corresponding tab.

- Click on **Start update** under Signature update to instruct Defender to renew the signature.

- The **Current status** tab provides an overview of the history and result of the last scan performed.

- The **Quarantined files** tab lists all the files in quarantine (not just those from the last scan).

- You can see the signature update history on the **Signature update** tab.

18.2.2 Disabling Defender in the Unlock Agent Wizard

DriveLock Defender Management can be temporarily disabled for individual agents in the unlock wizard. This is convenient if you want to change some Defender settings manually, for example, in order to analyze an agent's behavior, install specific software or remove viruses manually.

18.2.2.1 Enable/disable Defender Management control

Please do the following:

1. Select the DriveLock Agent you want to disable Defender control on.

2. Open the wizard for unlocking the agent by clicking the Unlock temporarily button.

3. Click **Next** until you get to the Defender options.

4. Disable the control for Microsoft Defender as shown below. You can also disable the real-time protection or the controlled folder access here.

5. On the last dialog page, specify how long you want your agent to be unlocked, and then click **Finish**.

> Note: Once the temporary unlock is over, DriveLock will reapply the policy assigned to the agent. Depending on the configuration, however, this may imply that manual changes are undone.
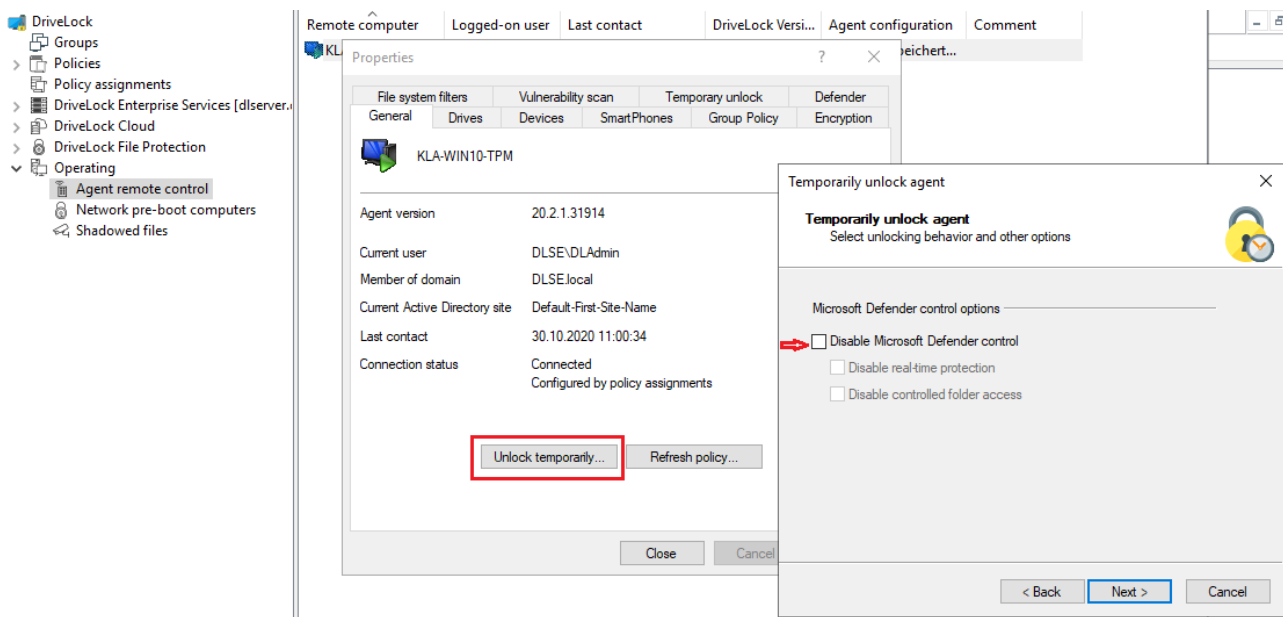
18.2.2.2 Disable Defender on the DriveLock Agent

If you have configured the agent user interface in your policy to allow users to use temporary self-service unlock, they can also temporarily disable Microsoft Defender control.

> ✏ Note: Further information can be found in Configuration of the agent user interface or temporary unlock.

18.3 Events

18.3.1 Status report and events

The DriveLock Agent regularly sends the current Defender status to the DriveLock Enterprise Service (DES). The status includes information such as definition version numbers, last scan times and threats found.

The status is sent after the start of the service and then every 24 hours. In addition, this also happens after configuration changes, after updating Microsoft Defender and when threats occur.

> ✏ Note: The status is always sent, regardless of whether the **Enable/disable Microsoft Defender control** option is set or not.

18.3.2 Microsoft Defender events

DriveLock Enterprise Service (DES) generates specific events for Defender. To specify in the policy that these events are sent to the DES and displayed in the DriveLock Operations

Center (DOC), go to the **Events and Alerts** node, **Events** sub-node and then **Microsoft Defender** in the **DriveLock Enterprise Service** column.

18.4 Microsoft Defender Management in the DOC

You can see the status of Microsoft Defender on the agents in the DriveLock Operations Center (DOC) in the **Microsoft Defender** view.

The Administrator or Threat Hunter role is required to be able to see the Micorsoft Defender view (see figure).

The DOC Dashboard also displays the Microsoft Defender status with various widgets. If the Microsoft Defender dashboard does not appear automatically, you can add it using the appropriate template.

18.4.1 Dashboard

Description of the widgets on the standard Microsoft Defender dashboard:

- **Protection** status shows the current status of the computers
    - Open threats
      Number of computers with open threats that could not be removed by
      Microsoft Defender.

    - Signatures or status not up to date
      Number of computers without open threats, whose Microsoft Defender sig-
      nature definitions have been updated, and whose last status report was no
      longer than 1 week ago.

    - Protected
      Number of computers whose Microsoft Defender signature definitions are older
      than 1 week or whose last status message was more than 1 week ago.

    - Inactive
      Number of computers not running Microsoft Defender Service

- **Service overview** shows the number of computers running the Windows Defender
  Antimalware Service or Windows Defender Antivirus Network Inspection Service.

- **Feature overview**
  Indicates the number of computers having individual Microsoft Defender features
  enabled.

- **Threats by severity**
  Displays all threats that have occurred and groups them by severity. We do not dis-
  tinguish between threats that have already been resolved and those that are still
  open.

- **Threats by category**
  Displays all threats that have occurred and groups them by category. We do not dis-
  tinguish between threats that have already been resolved and those that are still
  open.

- **Microsoft Defender state** provides an overview of the status of Microsoft Defender
  on the computers:
    - Not set: The status has not yet been reported

    - Active

    - Partly active: One or more Microsoft Defender components are not running, e.g.

        real-time protection

- Inactive: The Microsoft Defender Service is not running

- **Affected computer count history**
Shows the history of affected computers by number

- **Threat history by severity**
Shows threat history by severity

- **Threat history by category**
Shows threat history by category

18.4.2 View

The **Open threats** view is opened by default as a preconfigured view for the **Computer** list.
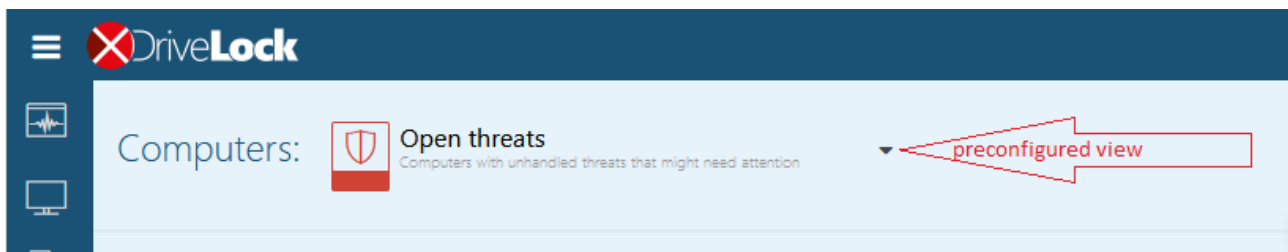
By clicking on the down arrow you can select more views from three different areas:

1. **Computer**
The Computers section will show the affected computers based on the view you choose.
For example, the preconfigured view **Features to enable** displays the number of computers where Microsoft Defender features are available but not active. Features that can be enabled include access protection, real-time protection, and behavior and tamper protection. Here the system checks whether the feature is actually available. For example, tamper protection is only available from Windows 10 1903 onwards.

    By clicking on ⊞ you can display the detailed view for each computer, which is composed of different blocks:

    - **Overall computer status** provides an overview of the status of Microsoft Defender, such as version numbers, available features and services, and the last update date. The lines that suggest an issue are highlighted in red in this view.

    - **Open/ resolved/ suppressed threats**
    Based on the status of existing threats, they are displayed under open, resolved or suppressed threats. Open threats can be suppressed for the selected computer or for all computers.

The **Open encyclopedia** link will take you to a Microsoft information page where you can get more information about the threat.

The **Show threat detection details** link opens the details view of the threat on the computer, where you can see which files are affected or when the threat was found.

- **Properties**

    The properties include general operating system information and the detailed status of Micrsosoft Defender, as displayed on a computer via the Powershell command Get-MpComputerStatus, for example.

    The Last update line shows when the DES was last updated by the agent.

2. **Detected threats**

    Here you can select how the detected threats are grouped (by category or by severity) or whether all suppressed threats are displayed as a preconfigured view.

3. **Threat detection details**

    Each threat can occur several times on the same computer, e.g. in different directories, on different USB sticks or several times in a row. The items shown in the list correspond to the occurrence of a threat on a computer. So several lines may contain the same computer with the same threat.

    The detail view shows affected files and the properties of the threat. In the properties you can see the status of the threat and when the last Defender action took place.

18.4.3 Quick Defender scan

To quickly scan an individual computer for viruses, open the context menu of the computer in the **Computer** view, then click on **Run action on computer** and select the menu command **Quick scan for viruses**. The start of this quick scan is displayed in the computer details under **Actions**. If a virus is found, it is displayed under **Detected threats**.

> ⚠ Warning: The quick scan can only work if a user is logged in to the system locally. Logging on via a remote desktop connection (RDP session) is not sufficient, as Defender Management tasks cannot be carried out from the DOC in RDP sessions or Terminal Server / Citrix sessions.

18.5 Troubleshooting

When tracing is enabled, the following log files are created on the agent:

- DlSvcDefender.log

- DES.log

You can also save the latest status sent by the agent to the DES to a file. To do so, you need to enable tracing and set the following registry key on the agent:

- Registry key: `HKLM\Software\CenterTools\TraceLog`

- DWORD-Wert: DlSvcDefender_LogStatus

- The file **DefenderStatus.json** is then saved in the trace directory.

19 Security Awareness

Raising employee security awareness is one of the most important tasks of a company today. With DriveLock Security Awareness, you can deliver event-driven campaigns and trainings with the following added value:

- Flexible security awareness trainings that are available online or offline continuously and can be administrated centrally,

- Interactive presentation of security-relevant information when needed, for example, when a USB flash drive is inserted,

- Event-driven campaigns, for example once a week or once a month automatically,

- Adaptive posting of actions to be taken following a security incident, and

- Implementation of security measures in line with the GDPR.

As part of the DriveLock Zero Trust platform, Security Awareness is a standard feature of DriveLock and does not require a separate license.

However, the Security Awareness Content AddOn does require a separate license and will provide you with a variety of external content you can use to create security awareness campaigns.

> Note: The Content AddOn packages can only be displayed correctly if Microsoft Edge WebView2 is installed on the agents.

19.1 Concepts

19.1.1 Campaigns

The security awareness campaigns used in DriveLock consist of texts in various formats (RTF, PDF, text), images, videos, web content, or e-learning modules. Campaigns provide users with targeted safety information, alert them to specific events, give instructions and assign the training they need.

You can configure security awareness campaigns so that they appear at specific times and events, for example when users log on to their computer or when connecting a smartphone, starting an application, plugging in a USB stick or connecting an external drive. You can also configure them to be displayed to users without any particular event or let the users decide when they want to watch the campaigns. The frequency of the display is also adjustable.

To ensure that the security information has reached its destination and the user has dealt with the content, a confirmation can be requested.

Campaigns can also be defined individually for drives, devices and applications within rules.

You can create campaigns in the Policy Editor and in the **Awareness** menu in the DOC.

> ☑ Note: The DOC only allows you to create campaigns with content packages, and only limited or reduced configuration options are available for these campaigns.

19.1.2 Content packages

The Content AddOn, which requires a license, contains multimedia content (for example, complete security trainings) and can be used to create campaigns. The content is updated regularly and automatically via the Internet on a subscription basis and can be accessed in the DOC.

Content is available in **English**, **French** and **German**.

Please note that some campaigns are only fully visible in certain resolutions. The resolution or scaling can be changed and adapted to the size of the respective window without having to restart the campaign.

> ☑ Note: If you are using DriveLock On-Premise, you will need to activate the content packages before you can include them in campaigns.

19.1.3 Assessments

A range of assessments are offered in the context of campaigns, and can be used in an audit, for example. Employee trainings, courses or tests and other measures relating to security-relevant issues can be precisely tracked and verified in this way.

Campaigns can be split into sessions for assessment purposes. Once a campaign has been assigned to a user group and presented to them on their respective endpoints, every single session can be assessed. This makes it easy to track whether a session failed to complete or was not passed, or whether there were any errors during completion.

The Assessments tab features the following:

- Predefined filters for previous, current and/or future campaigns

- Navigation view with campaigns and assigned groups as a child element

- Navigation view with groups and campaigns as a child element

- Assessment overview for all selected campaigns (stacked bar chart)

- Display of active and running campaigns for groups in the user-group detail view
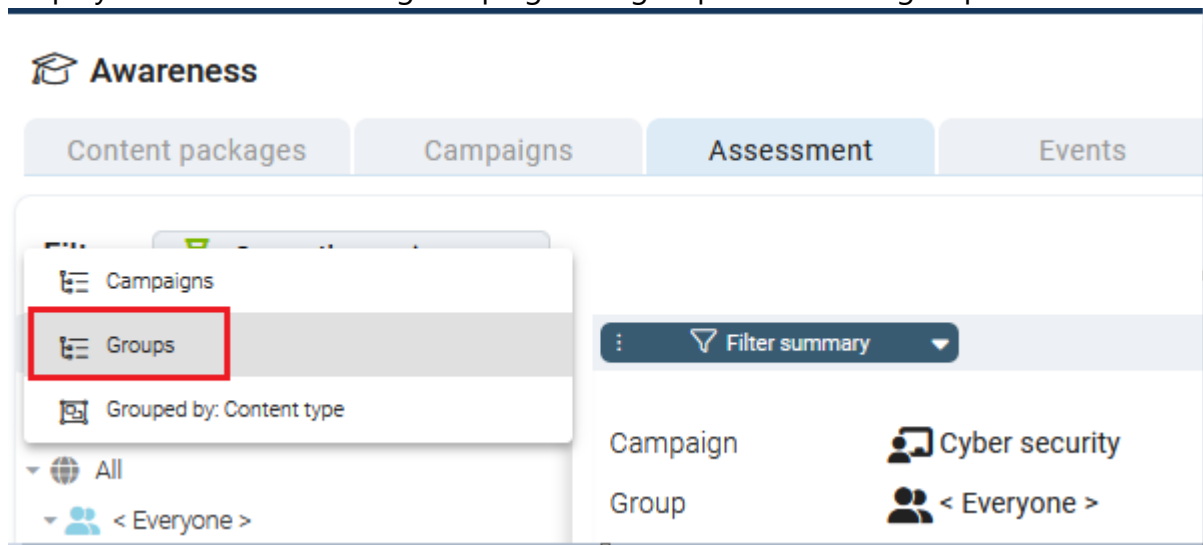
You can switch between the card and list view by clicking on the ![button] button.

In the diagrams, clicking on a specific area (e.g. the red Failed area) takes you directly to the individual assessment.

Assessment overview for 6 selected campaigns
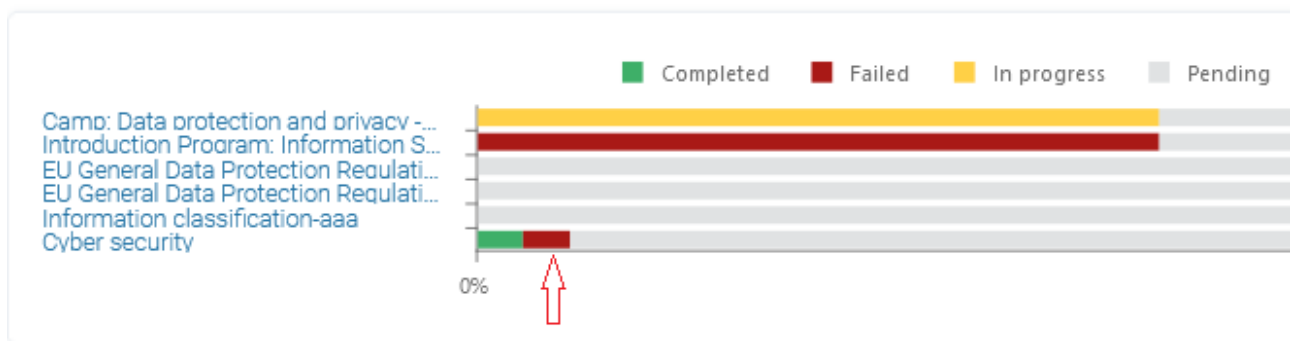
19.1.4 Events

The DOC lists the main security awareness events on the **Events** tab. They allow for a precise evaluation of how the campaign was executed and provide information about errors and warnings that occurred. It is also possible to trace back the objects associated with the event here.

In the Policy Editor, you can see a list of all security awareness events in the **Security Awareness** subnode under **DriveLock events** in the **Events and Alerts** node. Some of the events need to be activated before they can be transmitted from the DriveLock Agent to the DriveLock Enterprise Service (DES) and used for evaluation.

> Note: By default, key security awareness events are enabled for evaluation in the DOC.

19.2 Configuration in the DOC

19.2.1 Security awareness dashboard

In the DOC, you get an overview of your ongoing security awareness campaigns in the **Security Awareness** dashboard (see figure). The course of a campaign is referred to as a 'session'.

Each view is individual and depends on various factors, such as the number and type of campaigns you have already created.
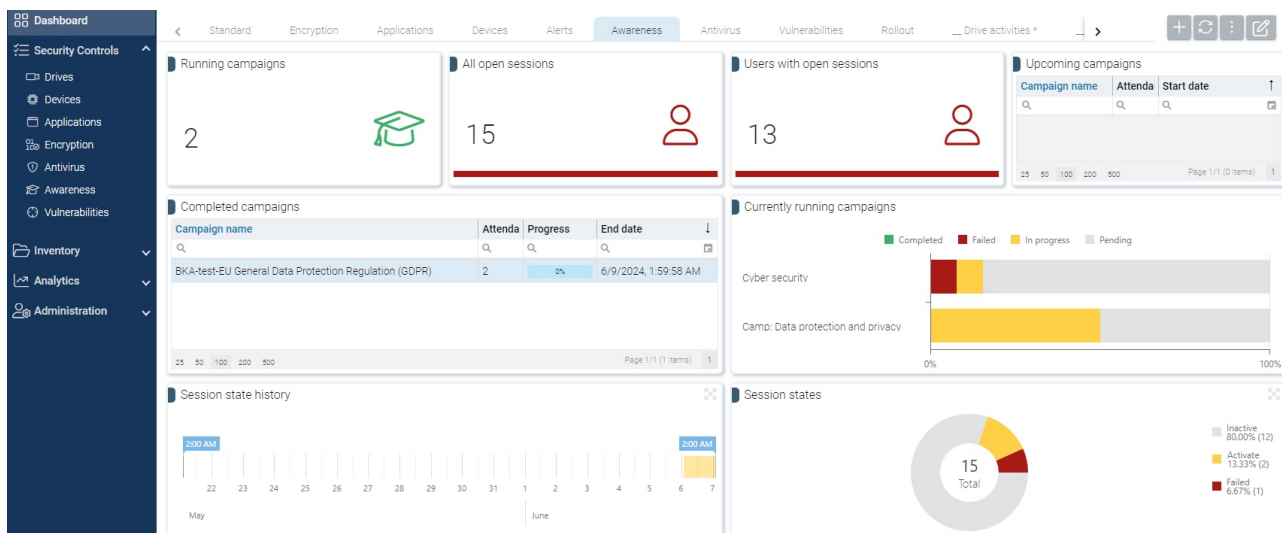
The sessions are grouped according to certain filters:

- For example, if you want to see which users still have open sessions, click the **Users with open sessions** widget to access the **Evaluations** tab. Here you will then see a list of all users with the respective number of open sessions (switch to the card view with the button ⬚). Highlight a session and then you will see the details: start and end dates, computer and user name and the status.

- In the **Completed campaigns** widget, for example, you can search directly for a specific campaign title.

- The **Session states** shows you the different states of the sessions in a pie chart. If you click the **Failed** segment, you can see, for example, who failed a session.

The following requirements are necessary so that campaigns or their sessions can be displayed in the DOC:

1. You have already created one or more security awareness campaigns. The content is not important.

2. The policies containing the campaigns have been assigned to the applicable DriveLock Agents. Campaigns are only displayed if they have already been started, are currently active or have already been completed on the agent.

> 📝 Note: Campaigns that you create in the DOC are automatically assigned.

3. The security awareness events must be enabled on the DriveLock Enterprise Service.

Campaign previews

You can view the content of a content package before assigning a campaign to users. The language can also be selected. To do this, click on the package on the **Content packages** tab to display its properties. The content is displayed in the **campaign preview** area.

19.2.2 How to create a campaign step by step

If you are creating a campaign for the first time and want to assign it to an agent followed by an evaluation, proceed as follows.

1. Open **Awareness** in the **Security Controls** menu.

2. If you have licensed the Content AddOn, all packages will automatically appear on the **Content Packages** tab. To see what kind of content a campaign has, select it and review the description on the right in the Details pane in the **Properties**. You can group the packages by content type or by name. The "Working in the cloud" training package is the example here.

> Note: Note that the packages must first be synchronized before they are assigned to campaigns if you are using DriveLock On-Premise. Then, the server downloads them so they can be redistributed to agents.

3. To create a campaign with this package, select **Working in the cloud**. Right-click to open the context menu or select the ⠿ button. Select **Create campaign**.

4. Enter a **name** and description for the campaign or accept the input. Next, specify the **priority** for the campaign execution order (settings from 1 - 10, order descending). Campaigns with the same priority will be displayed in random order.

5. In the next step, select who the campaign will be **assigned to**. Add a **user group** here, which you have to define beforehand.
   - If required, you can define a **start and end time** for the campaign.
   - Optionally, you can send all users an **invitation e-mail** to attend the campaign.

   > Warning: All automatically generated e-mails (for example, reminder or invitation e-mails) are sent by DriveLock according to an internal schedule (once a day).

   - Optionally, you can specify when you want users to be reminded of the campaign.

6. Once you click **Finish** , the new campaign will appear on the **Campaigns** tab.

7. Here you can edit, delete, deactivate the campaign or reduce or increase its priority. Once the campaign has been executed, you can already see the status in the **Detail view** at **Assessment overview**.

> ✎ Note: Note that the total number may increase as additional users log in to their DriveLock agents who are not previously registered as members.
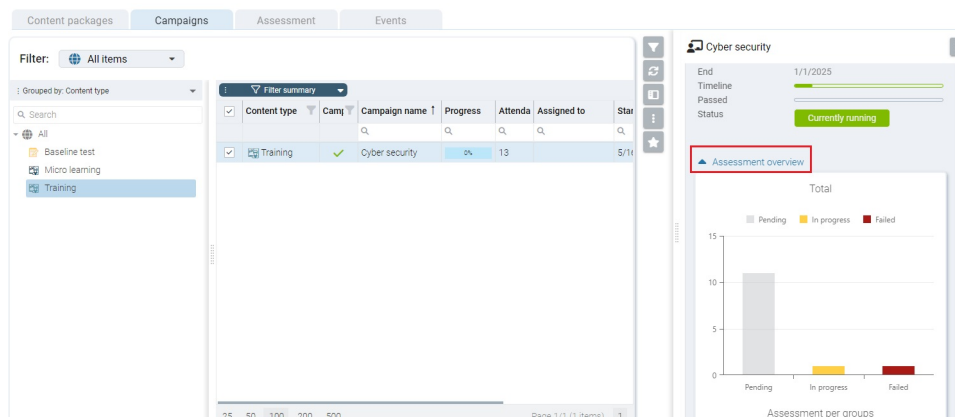
> ✎ Note: In the display, the campaigns can take on different text colors. Dark gray if the current date is outside the start and end range. Light gray when the campaign is disabled. Black is the normal text color.

8. If you click on the green area, the tab **Evaluations** opens automatically with further information
   Here you can take a closer look at individual sessions of campaigns using various filters and groupings.

9. The **Events** tab displays the relevant security awareness events.

19.2.3 Share campaign

If you want to share a specific campaign directly with members of a group, you can send the respective end users (members) an e-mail or a link to this campaign, e.g. via Teams from the DOC.

> ✎ Note: It works even if end users are not receiving campaigns via the Security Awareness Library, that is, from the DriveLock Agent on their end device.

You can use different templates and languages for e-mails.

This approach is practical in cases where you can tell that a user has not yet responded to a campaign by looking at their user status, for example. They might not have received a notification yet because they were inactive, or they may have overlooked an important campaign.

Proceed as shown in the figure:
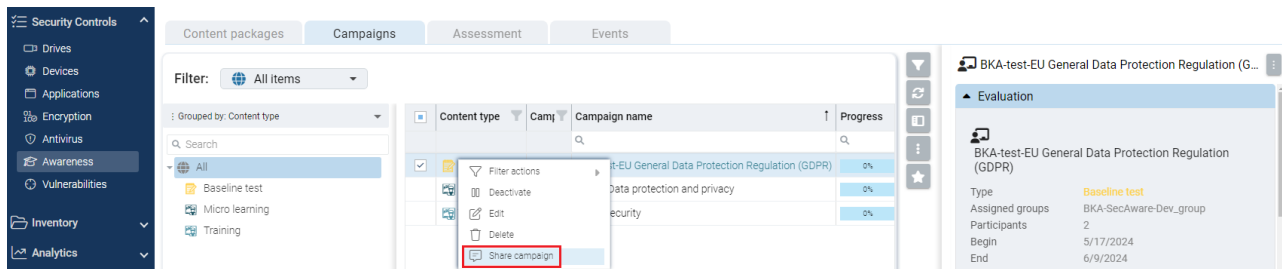
In the dialog that follows, you see a list of users who have been assigned this campaign but have not yet carried it out. The standard display shows users whose status is 'no activity'. You can also see when the user was last connected to the DriveLock Agent in the **Last login** column.

Next, simply copy the link to the campaign and send it by e-mail, or send an e-mail directly by clicking on the **Share by e-mail** button. These links can be sent to end users regardless of end devices, browsers or operating systems.

If you are missing a valid e-mail address, you can add it via the button or edit an existing one.

Send e-mails off schedule

You can use this menu command to bypass DriveLock's internal schedule for sending e-mails. All notification and invitation emails are 'collected' by DriveLock and sent to their respective recipients within the next hour.

19.2.4 Creating a security awareness report

In the **Assessments** view, you can generate reports for different areas of assessment. Depending on the filter and grouping selected, you can generate different reports that are geared more towards the type of content or users, for example. The reports are not static, but always show the current status. They are saved under *Analytics -> Reports* and can be configured just like other reports.

To create a report, proceed as shown below.
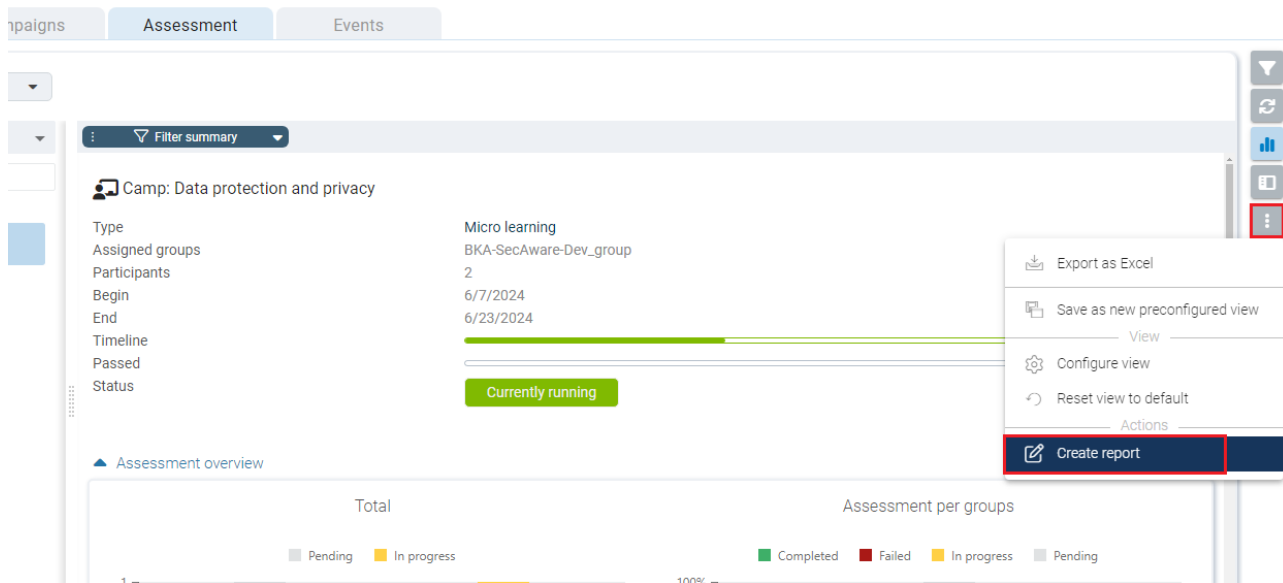
19.3 Configuration in the Policy Editor

19.3.1 Creating campaigns

In the **Security Awareness** node in your policy, you can create new campaigns in **Campaigns** as shown in the figure:
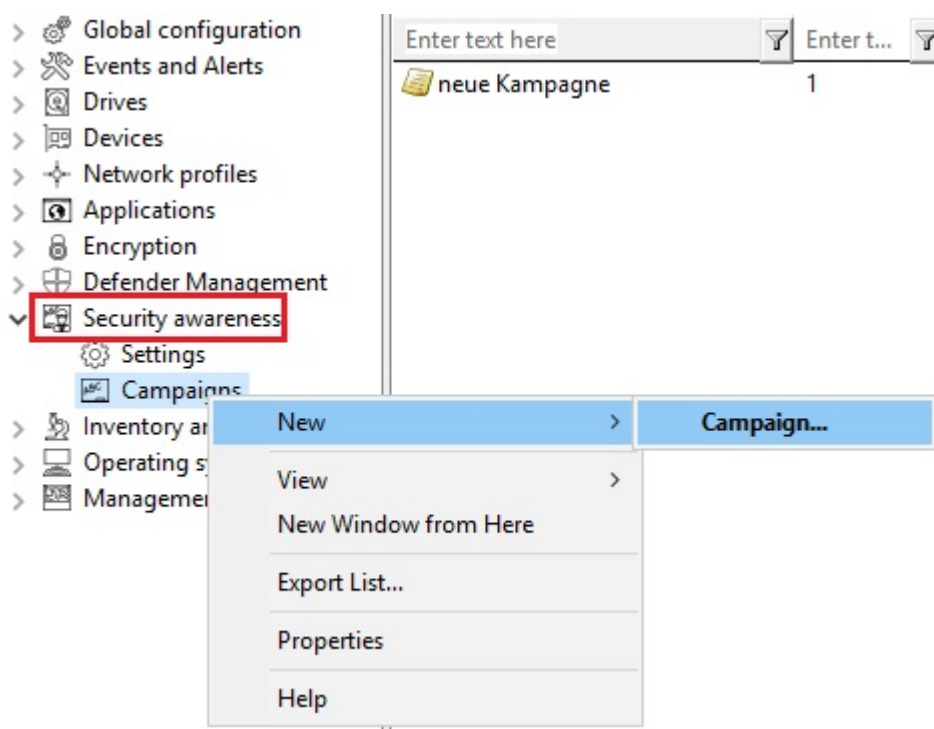
From the **campaign** context menu, select **New** and then **Campaign....** The **New Campaign** Wizard will open and you will go through the following dialog pages:

1. Content of a new campaign

2. Trigger for a new campaign

3. Recurrence of a new campaign

4. General settings

> ☑ Note: To assign the new campaign to specific computers, users, and network connections, open the Security Awareness Campaign Properties. Here you can also change all the settings you made in the **New Campaign** Wizard.

19.3.1.1 General

The **General** tab allows you to specify the following:

- **Description** of your campaign and an optional **Comment**. A description is needed so that you can find your campaign in the campaign listing. It is also used later on for reporting.

- **Priority** according to which the execution order of the campaigns is set (settings from 1 - 10, order descending). Campaigns with the same priority will be displayed in random order.

- Select the **Language** in which the campaign is presented. For example, if you select Brazilian, your campaign will only appear on agent computers whose operating system language is Brazilian. Leaving the language on Neutral includes all operating system languages.

> 🖉 Note: If you select a security awareness package from the Security Awareness Content AddOn, the language is already predefined by this selection (German, English or French only).

- Specify how long the campaign remains visible before the user has to confirm or is allowed to close the campaign.

- Specify whether the user must confirm that the campaign content has been read. You can enter a confirmation text for all of your campaigns in the general security awareness settings.

- The **User can watch the campaign on demand in the Security Awareness Library** option is enabled by default. A user can select campaigns from the Security Awareness Library and watch or complete them whenever it is convenient.

- Full screen mode:
Select **Yes** if you want to show the campaign in full screen mode on the agent computer.
Select **General settings** if you want to use the security awareness settings that apply to all campaigns for this specific campaign.
Select **No** if you do not want full screen mode.

> 🖉 Note: This option is not available at all if you selected the **Ignore full screen mode settings on campaign level** option earlier for all campaigns.

19.3.1.2 Content

The **Contents** dialog page allows you to determine which contents (elements) your campaign should contain.

- **Image**

  Select any image from your file system or policy file storage. DriveLock supports the usual image formats (*.png, *.jpg, *.bmp).

- **Content AddOn Package**

  Choose a package that suits your needs. This could be a training, a security flash or a knowledge test.

  > Note: Please note that Content AddOn packages are only displayed in this list if you have purchased the license for the DriveLock Content AddOn. If not, only the demo packages will appear.

- **Built-in image:**

  Select one of the images DriveLock provides.

- **PDF file:**

  Select a PDF file here that will be displayed to the user. Please make sure that the content is displayed correctly, as not all PDF features are supported.

- **RTF file**

  Select an RTF file here that will be displayed to the user. This may be plain text only, Unicode or ANSI character code.

- **Text**

  Enter any text for your campaign.

- **URL (web content):**

  Enter a URL here that points to Web content you want to use for your campaign.

- **Video file**

  Select a video file (in *.mp4 or *.avi format) which will be displayed to the user in Windows Media Player.

  > Note: The window size always adjusts to the content, except for Content AddOn packages and URLs where the window size is 1280x1024.

19.3.1.3 Trigger

The **Trigger** dialog page allows you to specify in which event your campaign will appear.

> ✎ Note: Examples of **events** include users logging in to their computer, plugging in an external drive, connecting a device, such as a smartphone, or updating a policy that uses rules to control the display of a campaign.

The following options are available:

- **Independent of an event**
  Choose this option to display a campaign directly to users at the nearest possible time, regardless of the usual events that trigger the display of a campaign. In this case, the DriveLock Agent checks at certain intervals (every 30 minutes) whether independent campaigns are pending and then displays them to the user accordingly.

  > ✎ Note: Select this option if you want to send ('push') users a security awareness campaign as quickly as possible, for example important company-internal information or warnings.

- **When a user logs on**
  Select this option to display a campaign to users as soon as they log on to their computer.

- **If used in rules**
  Select this option if you want to use a campaign in a rule. The campaign is displayed to users as defined in the corresponding rule for drives, devices or applications on the **Awareness** tab.

  > ✎ Note: This option is only available if you are using the full range of DriveLock features.

The last two options are only available if you are using DriveLock Security Awareness alone (without Device Control):

- **When connecting a device**
  Select this option to show a campaign to users as soon as they plug a device into their computer.

- **When connecting a drive**
  Select this option to show a campaign to users as soon as they connect a drive to their computer.

19.3.1.4 Recurrence

On the **Recurrence** tab, you specify how often you want your campaign to be displayed or repeated.

You can set the following here:

- **Show campaign x times**
  Here, you can define how often you want your campaign to be displayed by specifying a certain number of times, or you can select **Never** or **Indefinitely** from the drop-down list.
  Selecting **Never** makes sense if you do not want to display your campaign at first. At a later time, you can change this in the campaign's properties.

- **Every time the event occurs**

- **Once per day/week/month/year**

- You can also specify that your campaign is **displayed once every** few days (e.g. every third day).

- In case a campaign was displayed partially or an error occurred, you can specify that it will be displayed again after a certain time.

19.3.1.5 Deploy the campaign to users

To roll out a new security awareness campaign to the target users (computers running DriveLock Agents), you must first publish the policy.

1. Open the policy's context menu and select the **Publish** menu item. Or select the **Publish** button from the menu bar.

2. Optionally, you can enter a comment.

3. If you want to sign the policy, enable the corresponding option and select the certificate.

4. The policy is now published and used by DriveLock agents

19.3.2 General settings

In the **Security Awareness** node in your policy, you can configure general details for all campaigns in **Settings**.

Please do the following:

1. Under **Security Awareness**, select the **Settings** menu item.

Application Control - Zentral gespeiche	Setting	Value
> Global configuration	Enter text here	Enter text here
> Events and Alerts	Security awareness user interface settings	Configured
> Drives	Custom usage policy texts and options	Not configured
> Devices	Get executed campaigns from DES	Not configured (Disabled)
> Network profiles		
> Applications		
> Encryption		
> Defender Management		
∨ Security awareness		
Settings		
Campaigns		
> Inventory and vulnerability scan		
> Operating system management		
> Management console		

2. Click the **Security awareness user interface settings** option to specify the following settings:

- **All campaigns**
   On this tab you make general settings that affect **all** campaigns.
   - Here you can determine whether the window in which security awareness campaigns are displayed is always visible to the user.

   - If you want all campaigns to be displayed in full-screen mode, check the corresponding option.

   > Note: In full-screen mode, your campaigns come out especially well.

   - Select the **Ignore full-screen mode settings on campaign level** option if you want to override the settings in individual campaigns (full-screen mode can be set in the campaign properties).

   - If you have not yet created multilingual notification texts for your policy, you can use this dialog to enter headings and texts for your campaigns that are specifically tailored to your company.

   - Alternatively, you can specify languages in the **Multilingual notification messages** section of the **Global configuration** node and define corresponding notification texts here.

> ☑ Note: Further information on creating multilingual notification texts can be found here.

3. Select **Custom usage policy texts and options** to show customized content when a user attempts to access a drive and/or a device. The option only applies to a usage policies. In the Properties dialog, specify the following:

   - Select the file that contains the usage policy or enter text for the usage policy

   - Enter text for the buttons (if you don't want to use Accept or Decline)

   - Enter a caption

   - Select a video to show the users and specify settings for this video

> ☑ Note: You can configure DriveLock in such a way that an external drive or device can only be accessed after the user has confirmed reading a usage policy by clicking the "Agree" button.

4. Select **Get executed campaigns from DES** to specify that users can "take" their completed campaigns with them when they log on to another computer, i.e. the completed campaigns are no longer displayed there. A request is sent to the DriveLock Enterprise Service (DES).
   The default setting is **Disable** because most users work at their own computer.

19.3.2.1 Custom usage policy texts and options

Usage policies are used to inform the user of security-related behavioral measures or corporate policies before actually accessing a drive or device.

You can configure DriveLock in such a way that an external drive or device can only be accessed after the user has confirmed reading a usage policy by clicking the "Agree" button.

You can freely define a heading, the texts for the two buttons, as well as the text itself via this configuration item. To do so, check the **Display custom content** option.

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

es

there. You can use the policy store to distribute this file along with the DriveLock configuration.

An AVI video can also be played within the usage policy which can also be configured via this dialog as a special option. You can define the options the user has while the video is displayed.

The option **Show x times per user and session** will not display the message more than the specified number of times.

You can also define when and how long it takes for the Accept button to become available to the user.

19.3.3 Enabling security awareness events in the Policy Editor

In the Policy Editor, security awareness events are enabled as follows:

1. In the **Events and Alerts** node, under **Events**, open the **Security Awareness** subnode.

2. Select all the events you want to have displayed in the DOC and open the context menu.

3. Select **'Enable DriveLock Enterprise Service'** to allow events to be uploaded to DES.

19.4 Synchronize Content AddOn packages

If you are using the DOC, you can also synchronize the content packages manually by using the **Synchronize content packages** menu command under Awareness on the **Content packages** tab as shown in the figure.
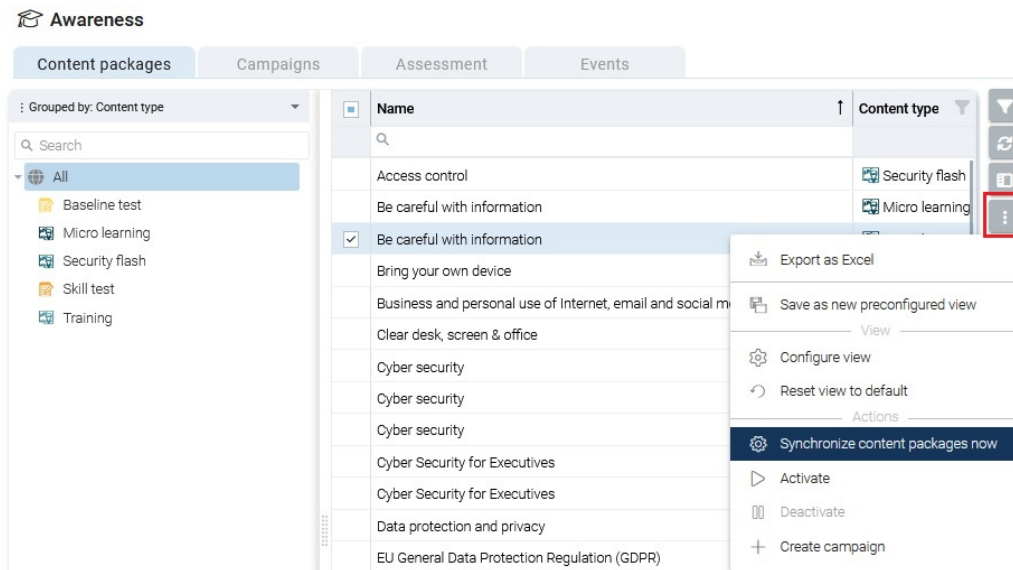
If you are using DriveLock On-Premise, you can also synchronize your content packages manually from the DriveLock Enterprise Service (DES) by proceeding as follows:
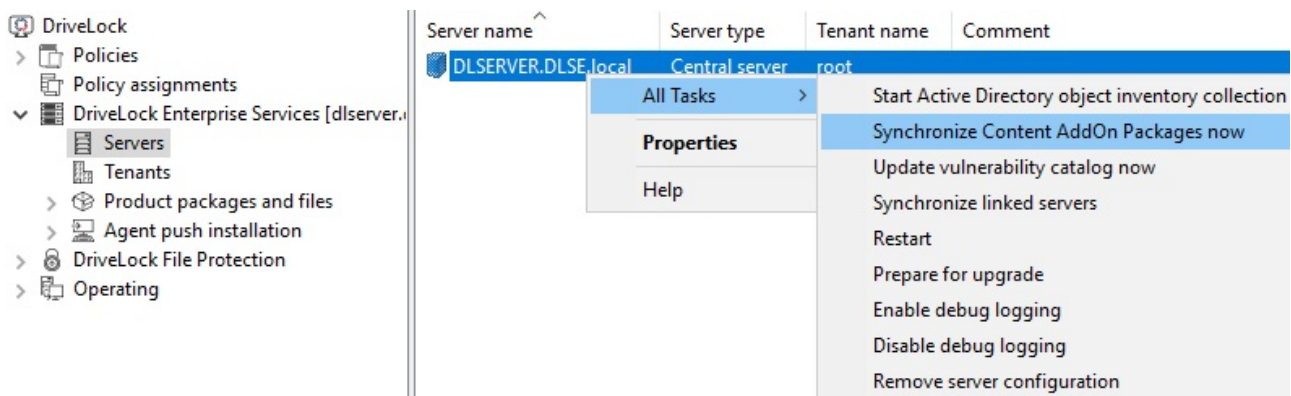
1. In the DriveLock Management Console (DMC), open the **DriveLock Enterprise Services** node.

2. Select the **server** that is 'responsible' for your Content Add-on packages.

3. Open the context menu and then the **All Tasks** menu command.

4. Click **Synchronize Content AddOn packages**.

5. All Content AddOn packages are now up to date.

19.4.1 Synchronization overview
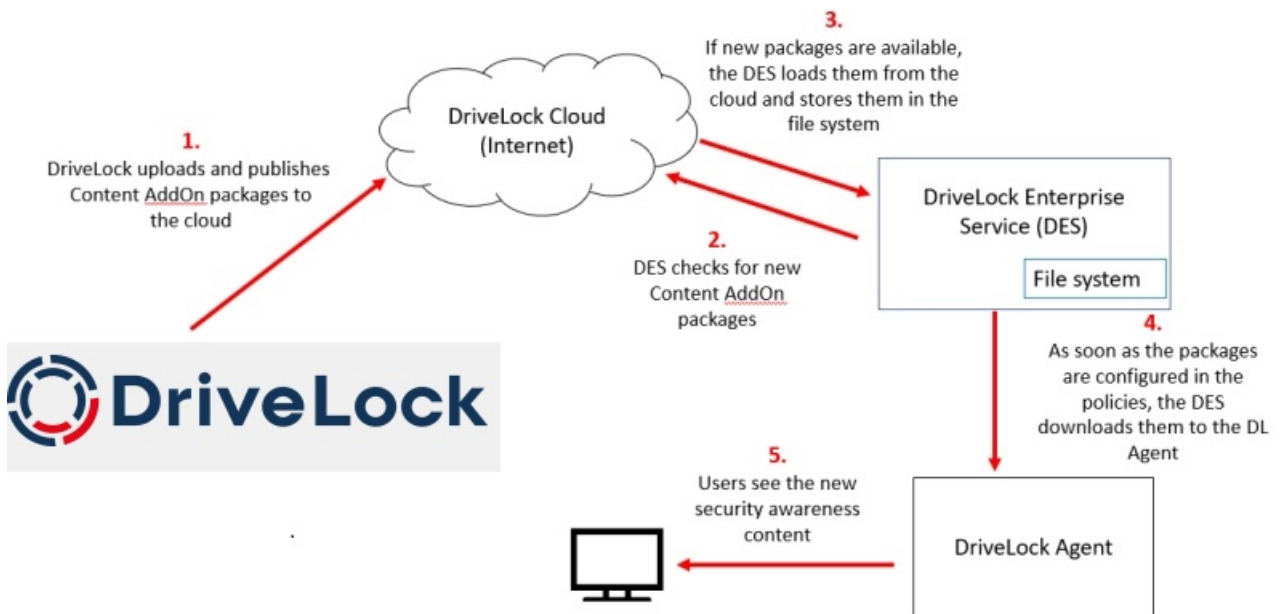
19.5 Usage of security awareness campaigns

Campaigns created in DriveLock Operations Center (DOC) can only use content packages. They are automatically configured so that they are shown when a user logs in or they can be accessed from the Security Awareness library. Configuring in the DOC is faster and easier, but offers fewer configuration options.

19.5.1 When calling up an application

To trigger security awareness campaigns when users launch applications, follow the steps below. This procedure applies to all application rules.

> ☑ Note: DriveLock Application Control requires a separate license and is not part of the standard DriveLock product range.

> ☑ Note: Please note that the display of a security awareness campaign depends on the higher-level **Scanning and blocking mode** that you have defined for your application launch. For example, in whitelist mode, the parent rule unblocks a particular application, while in blacklist mode, the parent rule blocks the application. Only if the system has checked and applied the rule already configured, the rule for displaying the security awareness campaign is applied. This mechanism is also described here.

1. Select the **Applications** node in the policy configuration.

2. Select the **Application rule** (see figure below) where you want to set security awareness and open the context menu.

3. Click **New**, then the rule and open the **Awareness** tab in the Properties dialog.

4. Select **Show security awareness campaign** and add the campaign you created earlier.

   > ☑ Note: The DriveLock agent will show the campaign according to the settings you specified when creating the campaign (e.g. how often and at what times it should be displayed or repeated). Campaigns with the same priority appear in random order.

5. Confirm your settings.
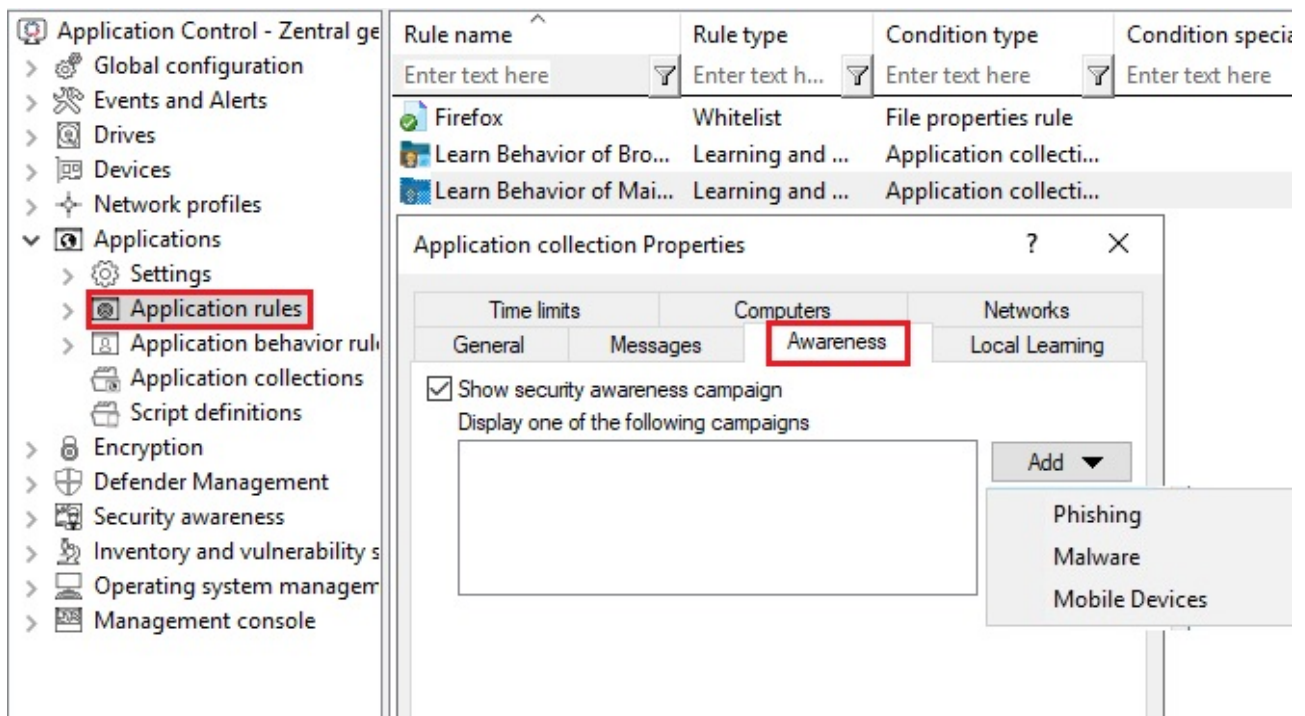
19.5.2 When connecting a drive

To configure Security Awareness so that a campaign is displayed when a drive is connected, use the Policy Editor as shown in the figure. This procedure applies to all types of drives.

1. Select the **Drives** node in the policy configuration.

2. Select the drive type you want to make security awareness settings for in the **Removable drive locking** section. In the example below, this is a USB bus connected drive.

3. Double-click the drive to open the Properties dialog.

4. On the **Awareness** tab, you can specify the following:
   - If you want to **Show a usage policy**, select this option. You can also specify passwords that must be entered when accepting the policy or check the **Launch self-service unlock after accepting usage policy** option so that the user can use the device after having confirmed the policy.

   - If you want other users than the user logged on to Windows to confirm the policy, select **Require Windows password for accepting usage policy** and **Allow authorized user login**. Click **Authorized users** to enter these users in a list and check **Enable "login as user" option by default**. The self-service wizard will "run as" the authorized user.

   > Note: Click here to find out how you can create a usage policy.

- You want to **display an awareness campaign** when a user attempts to connect to the device. Now you can add a campaign you created earlier.
  Select it from the list that opens after you click **Add**.

5. Confirm your settings.
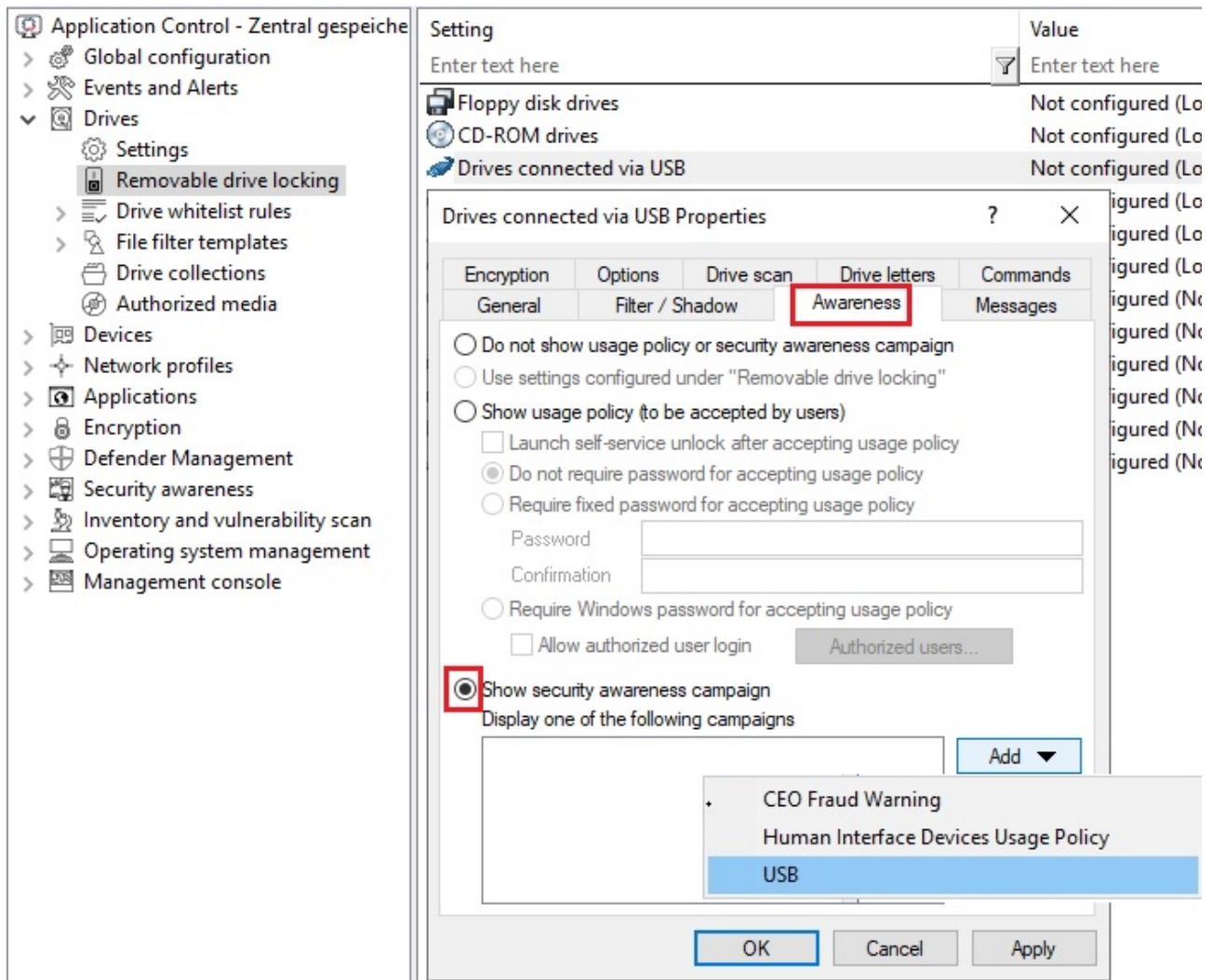
For **drive whitelist rules**, security awareness campaigns can be included with all rules except the following: network drive rules, WebDAV network drive rule, and terminal services rules.

19.5.3 When connecting devices

To configure security awareness when a device is being used, follow the steps illustrated below. This procedure applies to all devices and all smartphones, plus all adapters and interfaces except COM and LPT, and also to all device whitelist rules.

The example below shows how an awareness campaign will be displayed once a user tries to connect an input device (HID) to their computer at work.
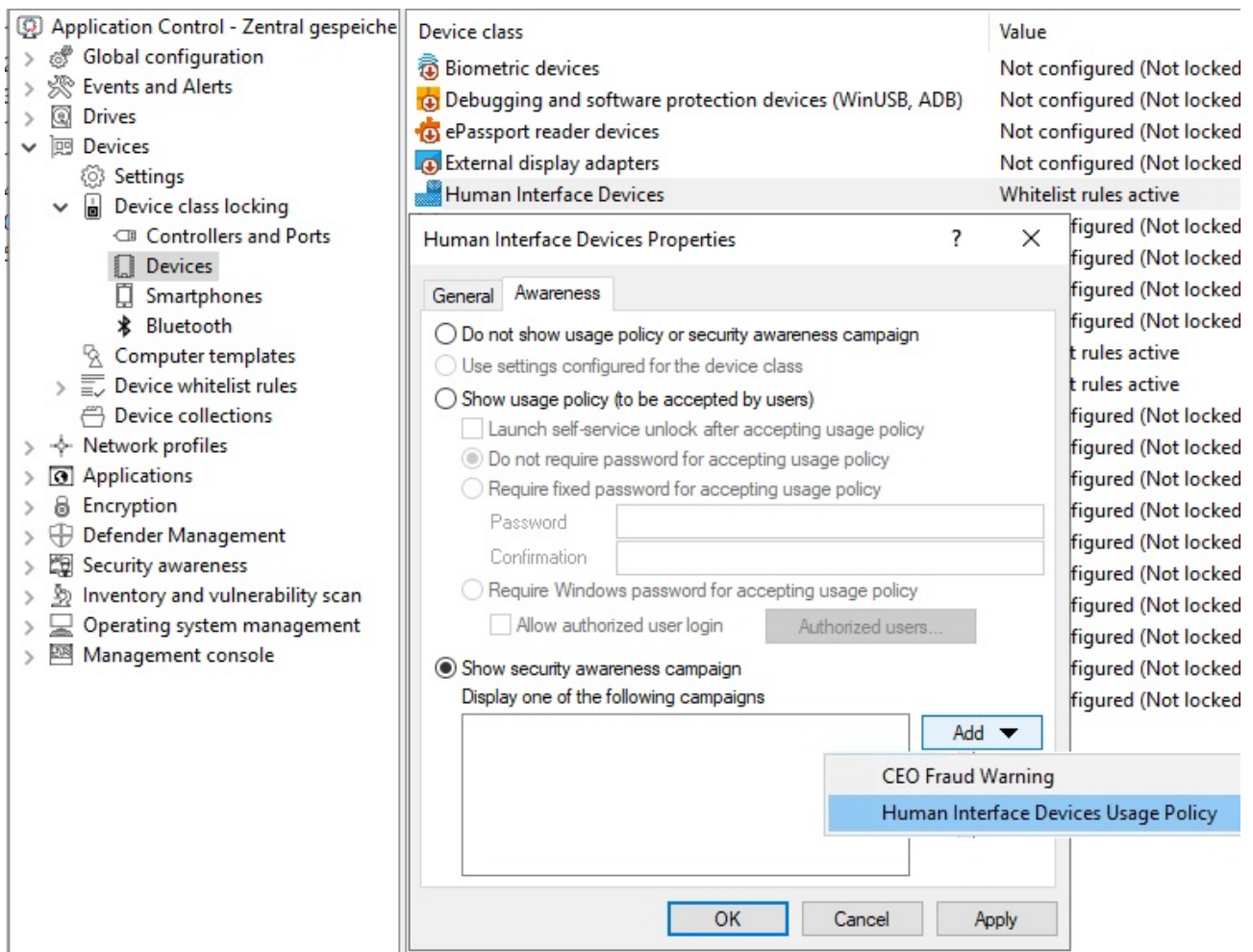
1. In the policy configuration, select the **Devices** node.

2. In the **Device class locking** section, select the device class you want to specify security awareness settings for.

3. On the **Awareness** tab you can configure the same settings as for the drives.

4. Confirm your configuration.

19.6 DriveLock Agent

19.6.1 Display on the DriveLock Agent

Campaigns are displayed on the DriveLock Agent according to the settings in the policy.

- Users can open the security awareness library in the agent user interface:
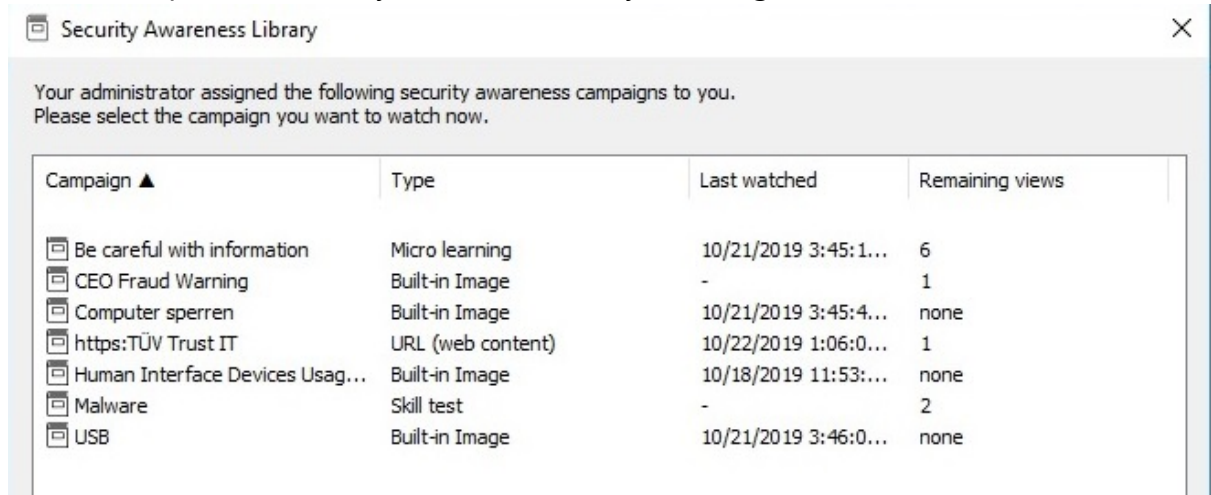
- The security awareness library can also be accessed via the tray icon on the agent:

In order for this to work, select **Taskbar notification area settings** in the policy in **Agent user interface settings** beforehand.

On the **Options** tab, add the option **Select a security awareness campaign...**(see figure).

Then the user can select a campaign on the agent.

20 Vulnerability Management

DriveLock Vulnerability Management enables you to automatically and regularly scan a computer system for previously known Windows and third-party vulnerabilities.

To do so, DriveLock accesses a database that is updated several times a day. The DriveLock Operations Center (DOC) then displays the findings in a separate new view with a risk and impact assessment, including missing patches, outdated software or libraries of known vulnerabilities.

You need a separate Vulnerability Management license to use it.

20.1 Vulnerability scan in the DOC

In the DriveLock Operations Center (DOC), the status of the vulnerability scan on the agents is displayed in the **Security Controls** under **Vulnerabilities**.

To indicate the criticality of a vulnerability, the Common Vulnerability Scoring System is used as a rating system. The base score reflects how critical a vulnerability is. It ranges from S1 (uncritical) to S10 (highest criticality).

- The filter on the **Computer** tab is set to **Computer with high risk** by default. This includes all computers that have open vulnerabilities with a base score >= S7. This filter displays the open or suppressed vulnerabilities for a computer and allows the vulnerability to be suppressed for one or all computers

- The **CVEs** (Common Vulnerabilities and Exposures (CVE®)) tab shows which CVEs exist and allows them to be suppressed for all computers. Shows the vulnerable computers in the detailed view of a CVE and allows navigation to the vulnerable computers (opens the list of detected vulnerabilities)

- The **Vulnerabilities** tab provides a vulnerability overview and shows for specific computers when a specific vulnerability was detected and allows suppression for one or all computers

20.2 Configuration in the Policy Editor

20.2.1 Vulnerability catalogs

Vulnerability scanning is based on catalogs that are first uploaded from the cloud to the central DriveLock Enterprise Service (DES) and then distributed to DriveLock Agents.

There are separate catalogs for operating system and third-party vulnerabilities.

In order to load the catalogs, the DES accesses

- a web service at https://service.drivelock.cloud and

- a configuration at https://download.drivelock.com/vulnerability-defin-
tions/catalogs.json.

When setting up the vulnerability scan for the first time, it may take a while until the catalog is completely loaded on the DES. Any later updates only transfer the modifications and are thus considerably faster.

> Note: After entering the license, either restart DES or update the catalogs in the Management Console.

20.2.1.1 Updating the vulnerability catalogs

Please do the following:

In the context menu of the respective DES, click **All Tasks** and then **Update vulnerability catalog now** (see figure).
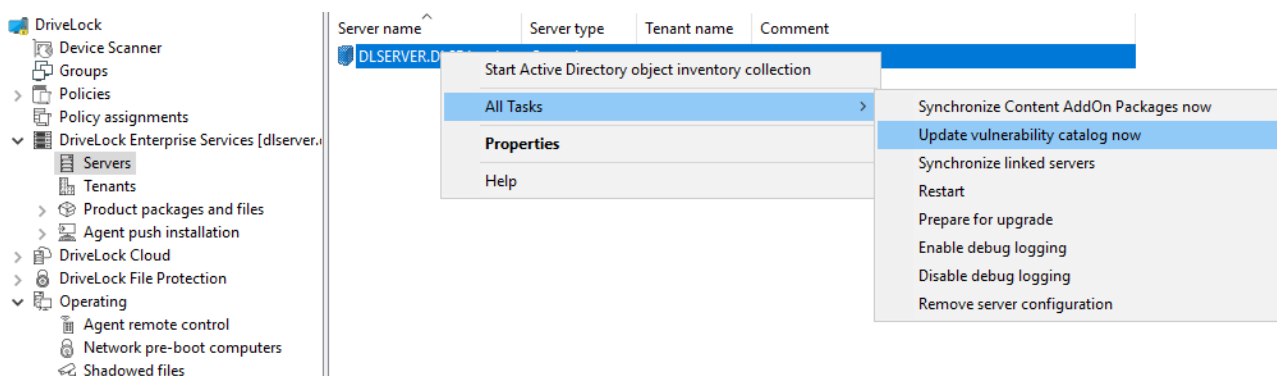
20.2.2 Configure vulnerability scan

Vulnerability scanning is disabled by default; you must first enable and configure it in the policy where you licensed Vulnerability Scanner.

Please do the following:

1. Go to the **Inventory and vulnerability scan** node and open the **Settings**.

2. Open **vulnerability scan**.
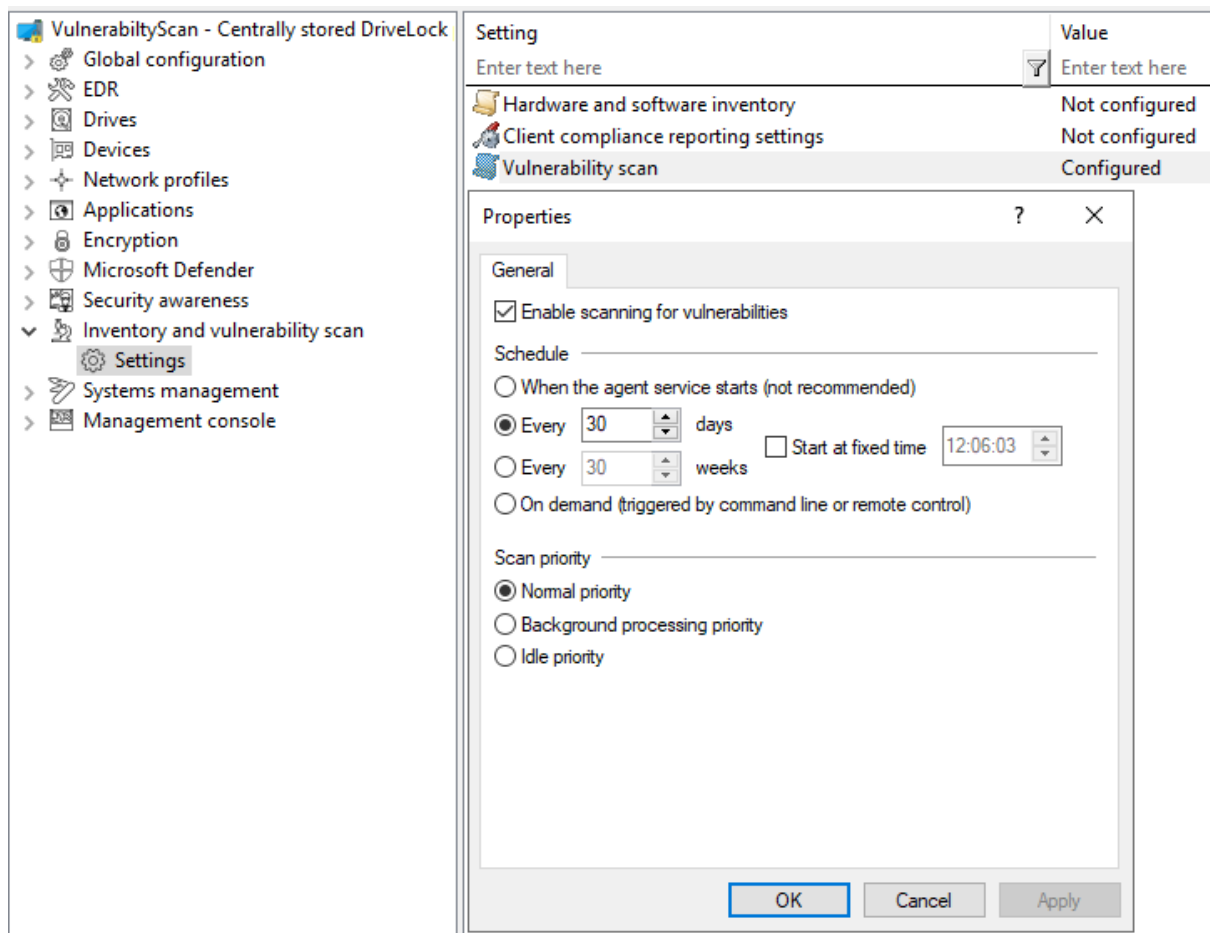
3. Check **Enable scanning for vulnerabilities**.

4. If you select the **On demand (...)** option, the vulnerability scan must be started via the agent remote control or alternatively via the agent command line.

5. Using the options to **Scanner priority** you can set the process priority of the scanner on the agent. If you want to reduce CPU usage and accept a longer runtime, you can select **Background processing priority** or even **Idle priority** here.

20.3 DriveLock Agent

20.3.1 Vulnerability scan on the DriveLock Agent

The vulnerability catalogs are downloaded from the DriveLock Enterprise Service (DES) to the DriveLock Agent and are updated on a regular basis.

You can find the catalogs on the agent under:

- C:\ProgramData\CenterTools DriveLock\VulScan\3P and

- C:\ProgramData\CenterTools DriveLock\VulScan\OS.

The actual vulnerability scan is performed by **DLVulScan.exe**. The **DLOvalHelper.exe** is also involved in transferring the catalogs to the agent. Both are located in the DriveLock directory on the agent.

20.3.1.1 Start vulnerability scan via agent remote control

Please do the following:

1. Connect to the respective agent via the **agent remote control**.

2. Click the **Start scanning** button.
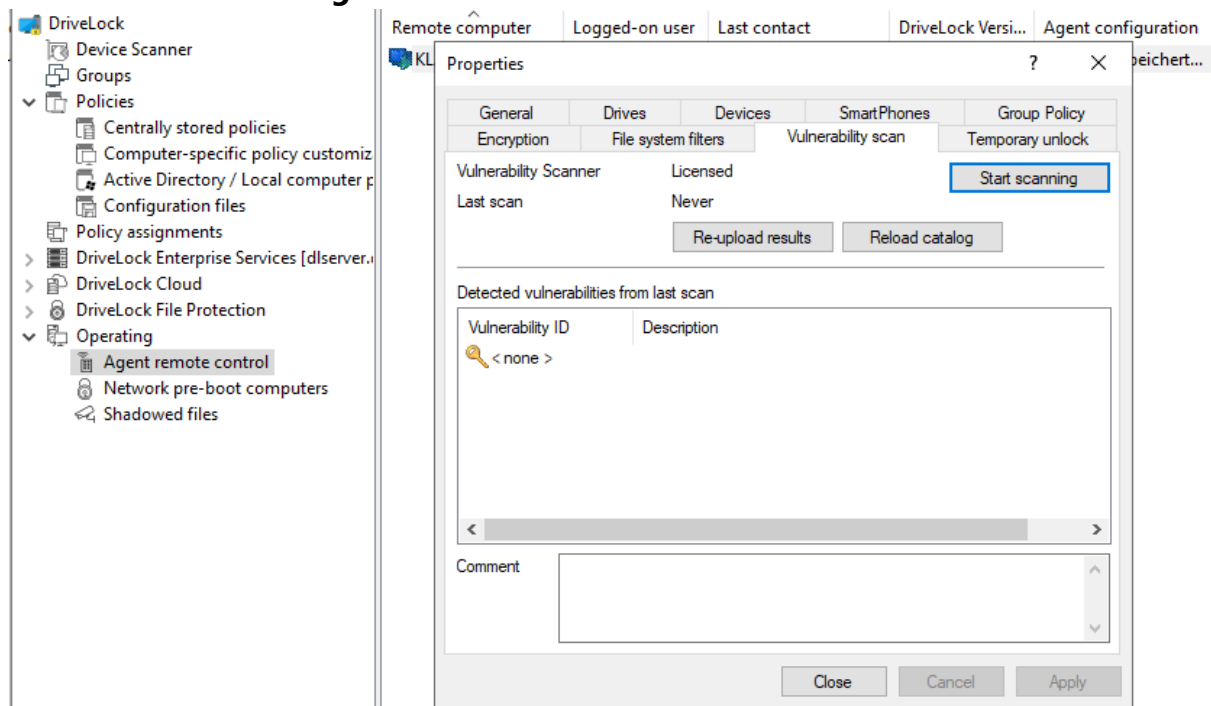
3. Click the **Re-upload results** button reload the scan results.

4. Or click **Reload Catalog** to reload the scan catalog.

> Note: These two options are intended mainly for troubleshooting.

5. If vulnerabilities were detected during the last scan, they will be displayed with ID and description in the dialog.

20.3.1.2 Start vulnerability scan from the command line

Actions can be triggered on the agent via command line.
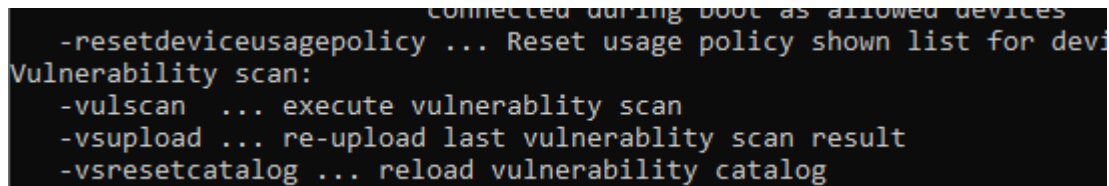
Trigger actions via the following command lines:

`drivelock -vulscan`: Start scanning for vulnerabilities

`drivelock -vsupload`: Reload results

`drivelock -vsresetcatalog`: Reload or reset catalogs

The options are also documented via `drivelock /?`"

20.4 Inventory

The DriveLock Agent retrieves information about the current hardware or software of the client computer regularly or at specified times; this information is then transmitted to the DriveLock Enterprise Service. The collected data can be analyzed centrally via the DriveLock Control Center (DCC) or the DriveLock Operations Center (DOC). That way, you get a quick overview of the programs or software patches that are installed on your computers.

20.4.1 Hardware and software inventory

Here you can specify when the DriveLock Agent collects certain information, and whether this feature stays disabled or not.

Please do the following:

1. Go to the **Inventory and vulnerability scan** node, open the **Settings** sub-node, and then click **Hardware and software inventory**.
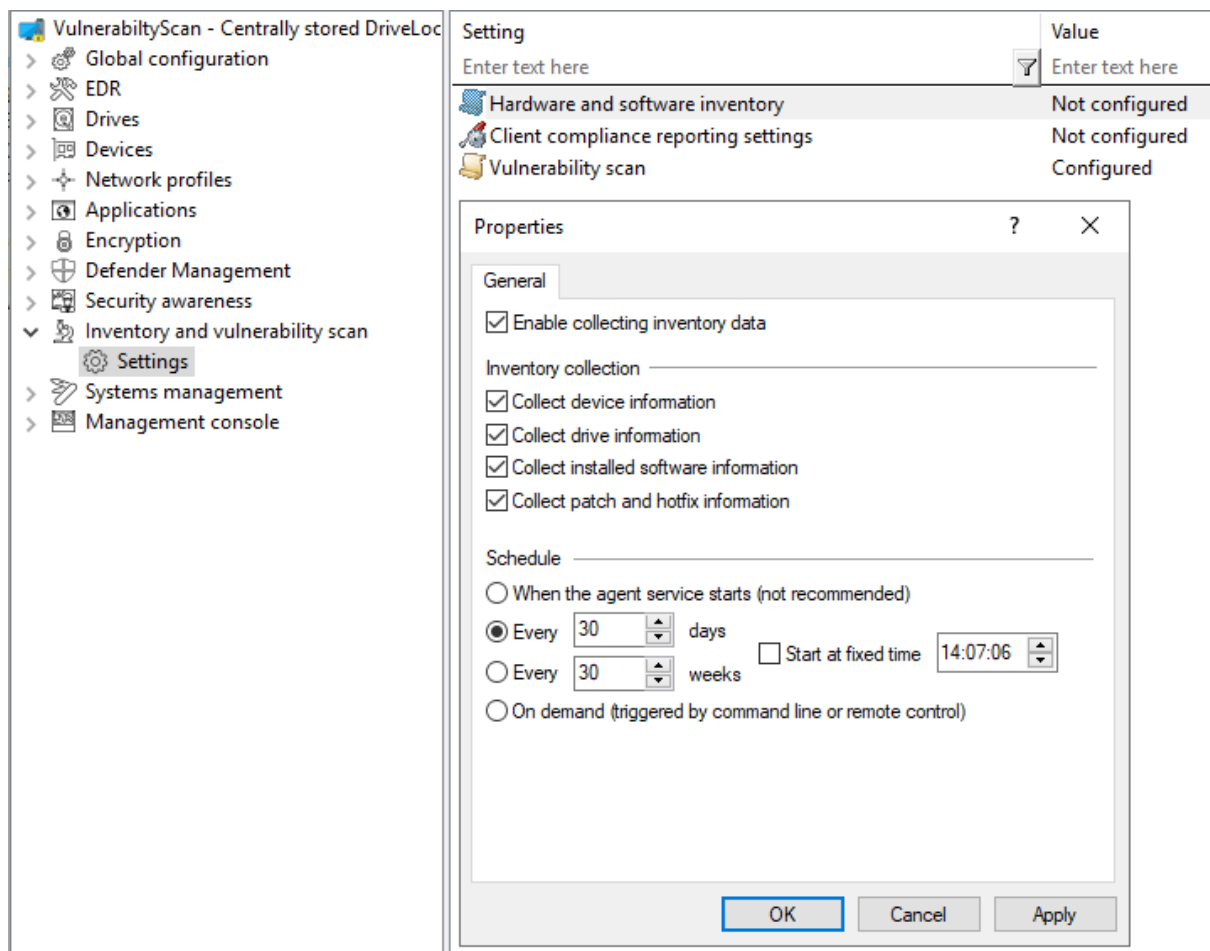
2. To allow the agent to collect information about the computer, select **Enable collecting inventory data**.

3. Choose which data you want the agent to collect and send to the DriveLock Enterprise Service.

4. Next, define the time when the agent starts gathering information and when the data is sent to the DriveLock Enterprise Service.

> Note: Please note that it takes some time for the agent to collect the data and the workload on the system is slightly higher than it would be otherwise. Therefore, the scan will also be delayed for a few minutes after the agent is started (if you have selected this option).

20.4.2 Client compliance

This option allows you to specify the parameters that will be checked on the computer for the client compliance status.

20.4.2.1 Client compliance settings

Please do the following:

1. Go to the **Inventory and vulnerability scan** node, open the **Settings** sub-node, and then click **Client Compliance Settings**.
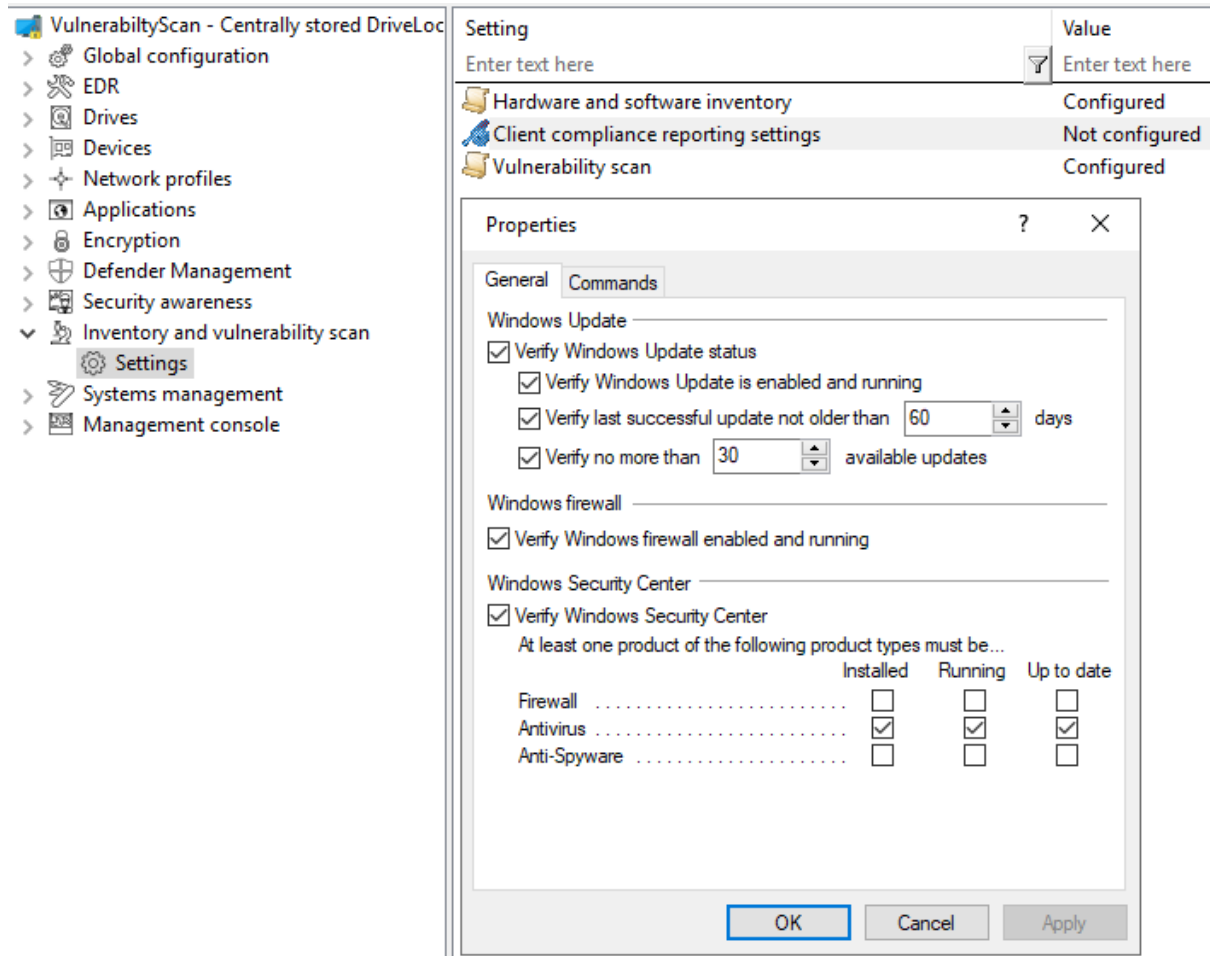
2. Select the required settings.

3. On the **Commands** tab you can configure executable programs or scripts of your choice.
   Add them to the policy file store first and select them from there. The DriveLock Agent calls the programs or scripts on the clients; they must return 1 for compliant and 0 for non-compliant.

21 Operating system management

In this section, you configure settings for DriveLock Agent operation and system management.

21.1 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.
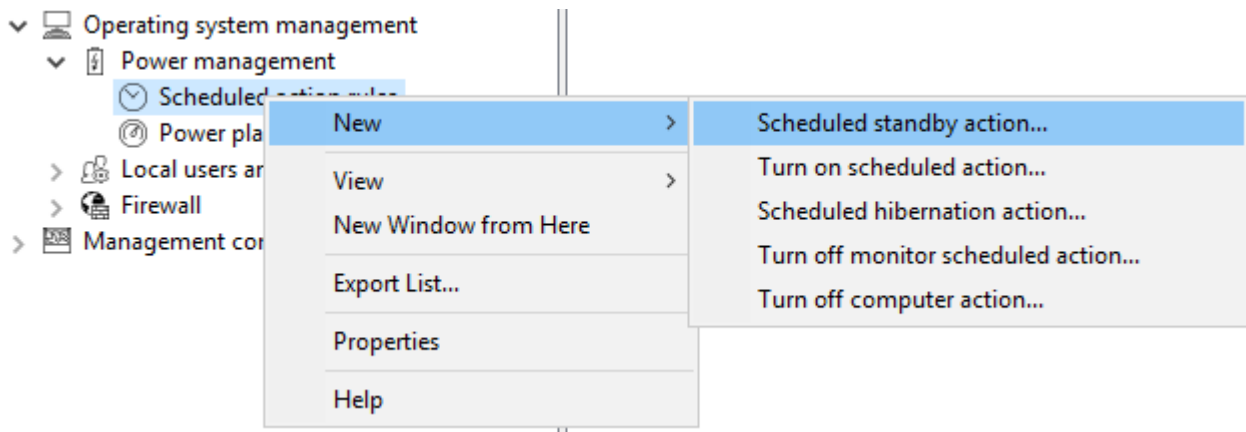
21.2 Local users and groups

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, you can add specific users to the local administrators group so that you can have different local administrators for a specific group of computers. This involves specifying who gets local admin rights on particular systems. Users with these local admin rights will be able to make changes to their computers. To get these permissions (temporarily), a user is issued a password that is valid only on that specific computer for a certain period of time. Passwords remain stored in the system, they are protected by certificates and have an expiration date.

How it works:

Role-based permissions: The functionality is based on a role that allows specific users to temporarily work with elevated permissions.

Password with expiration date: The provided passwords have an expiration date, so users can work with elevated permissions only for a limited time.

Local password limitation: The temporary password is valid only on the user's own endpoint and cannot be used on other endpoints.

Passwords in DriveLock: Passwords are stored in DriveLock. Administrators with the appropriate role have access to the passwords and can view them in plain text in order to give them to users.

Workflow:

Administrator actions:

- The Administrator role is assigned to a user to grant temporary local administrator privileges.

- A user who requires elevated privileges on a temporary basis contacts the administrator and requests a temporary password.

End user actions:

- The end user enters the temporary password received to work with elevated privileges for the specified period of time.

- Once the time expires, the elevated privileges are automatically revoked.

Offline functionality:

If the end user is offline, the policy is still applied locally and the elevated privileges remain active until the set time expires.

21.2.1 Settings

The following settings are available:

Local account data storage

This setting allows you to specify where user names and passwords are stored - certificate based locally or on the DES.

Management mode settings

Local user administration mode:
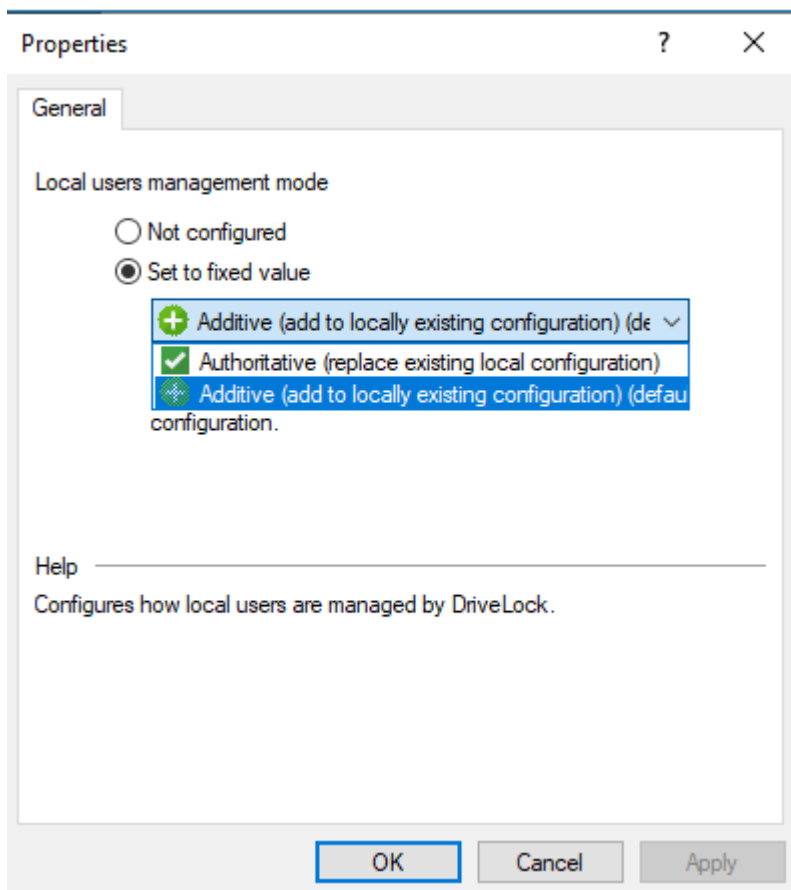
With the **Local users and groups management mode** you can specify how users and groups are managed by DriveLock.

- 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.

21.2.2 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:
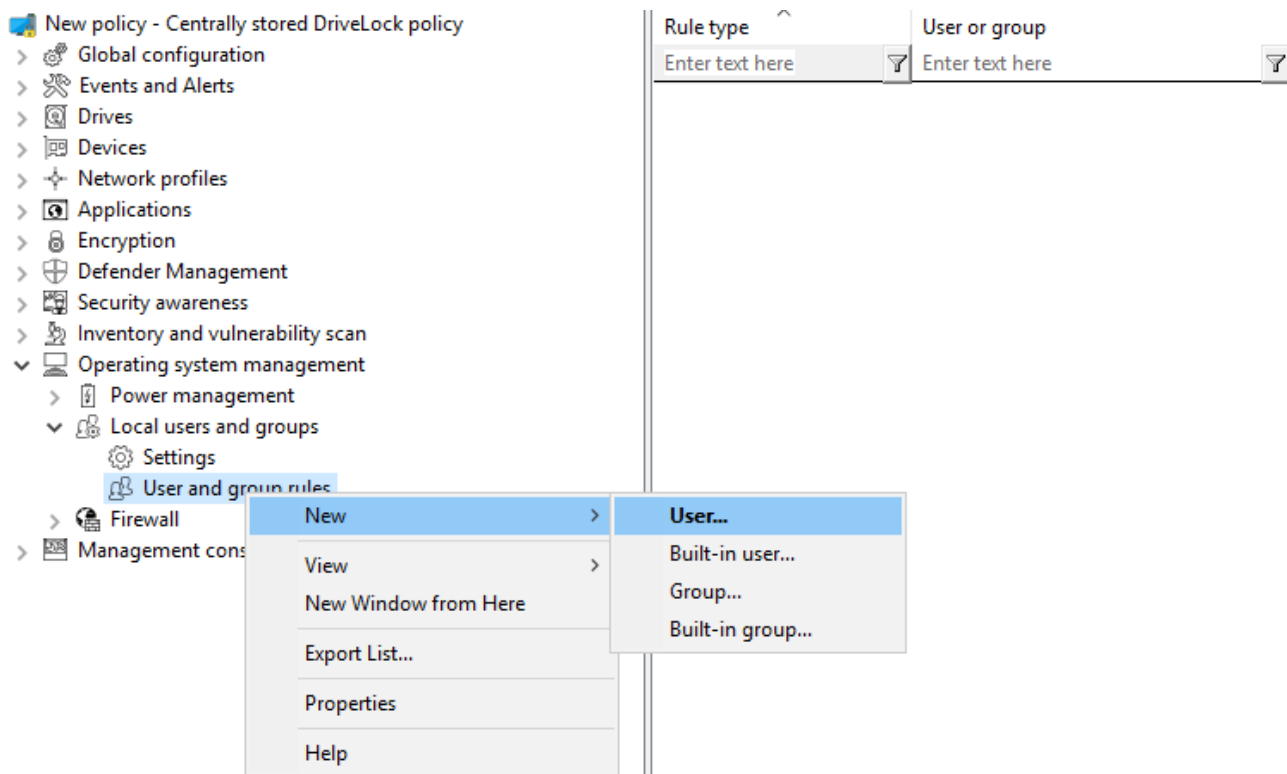
The difference between built-in and custom accounts is the username.

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.
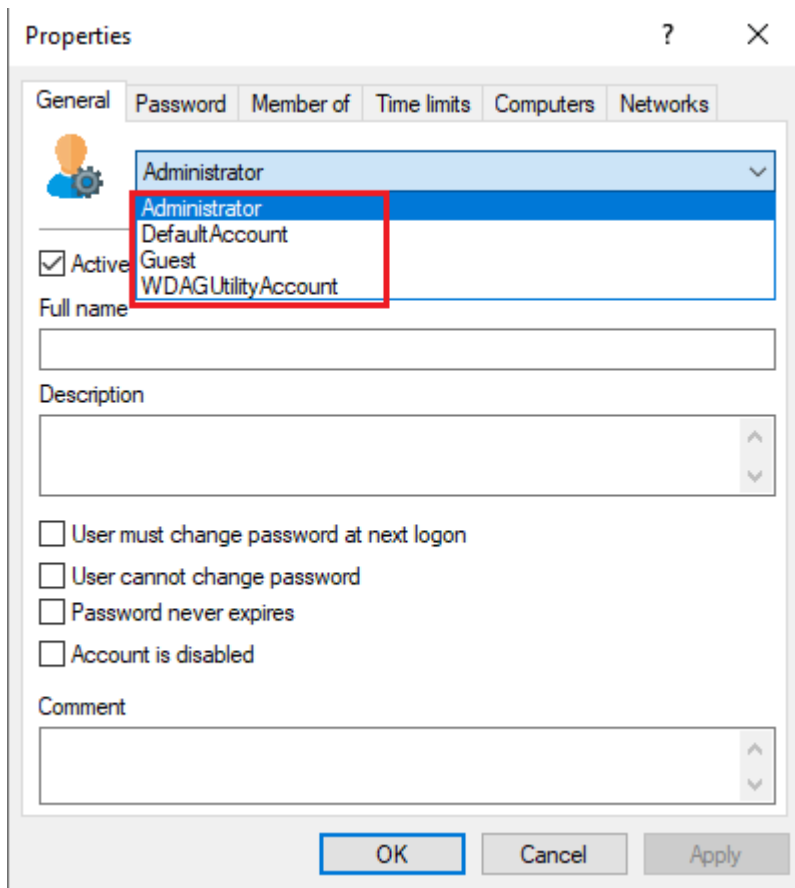
On the **Password** tab you specify whether a fixed, a calculated or a random password should be used for the account. Also, for built-in users, you can specify whether to change the fixed user name:

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.

21.2.2.1 Local account retrieval

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, that is, if data is uploaded to the 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.

As of version 2023.1, passwords can now also be retrieved via the DOC. This also includes a history of passwords.

21.2.2.1.1 Show password of local users (DOC)

In the context of a computer in the DriveLock Operations Center (DOC), a user (for example, a help desk employee) with the appropriate permission can provide an end user with the local account password.

> 📝 Note: You must have the user names and passwords stored on the DES to do this.

To get the password, open the **Computers** view in the DOC, select the computer, open the **Advanced** context menu, and then click **Show password of local users**.
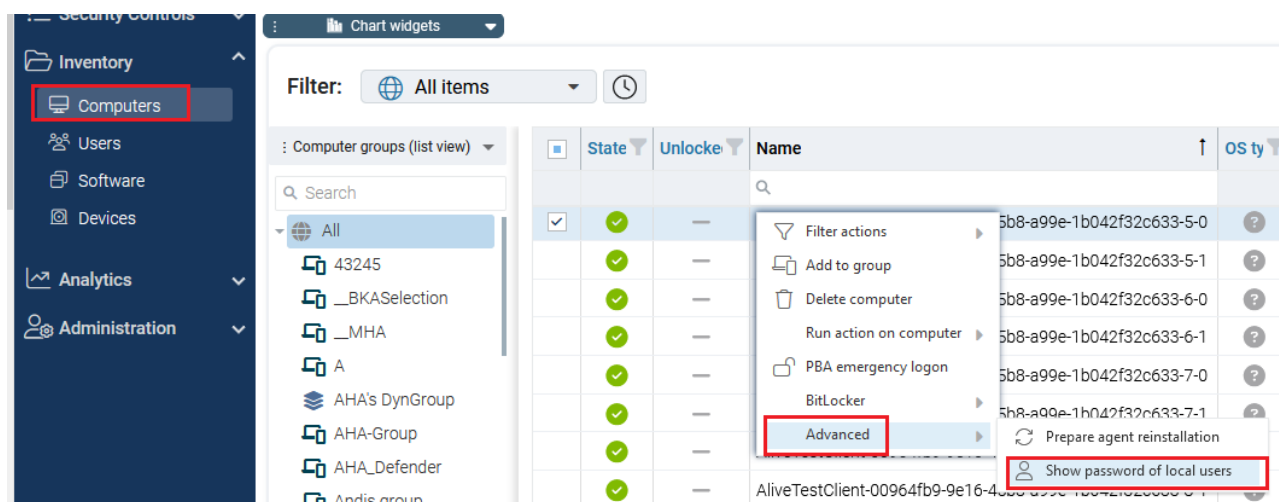
21.2.2.2 Local users and groups in agent remote control

In the Agent remote control, a new dialog was added to the Agent properties dialog, which shows 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.

21.3 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.

21.3.1 Settings

You can configure the following options:

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.
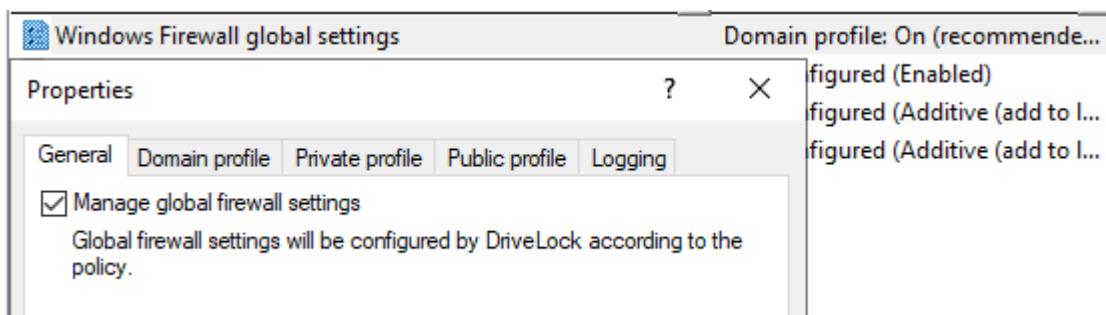
- **General** tab: If you want DriveLock to configure the Windows Firewall according to the settings in this dialog, check **Manage Global Firewall Settings**. This setting does not affect the actual firewall rules. The rules are managed according to the policy, even if this setting is disabled.

- **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.

602

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.

603

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 local rules are replaced by the rules in the policy. Firewall rules predefined by Windows are only deactivated by DriveLock and not deleted.

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.

21.3.2 Inbound and outbound rules

In the policy you are able to define inbound and outbound rules. To do so, select **Inbound rules** or **Outbound rules** and open the context menu.
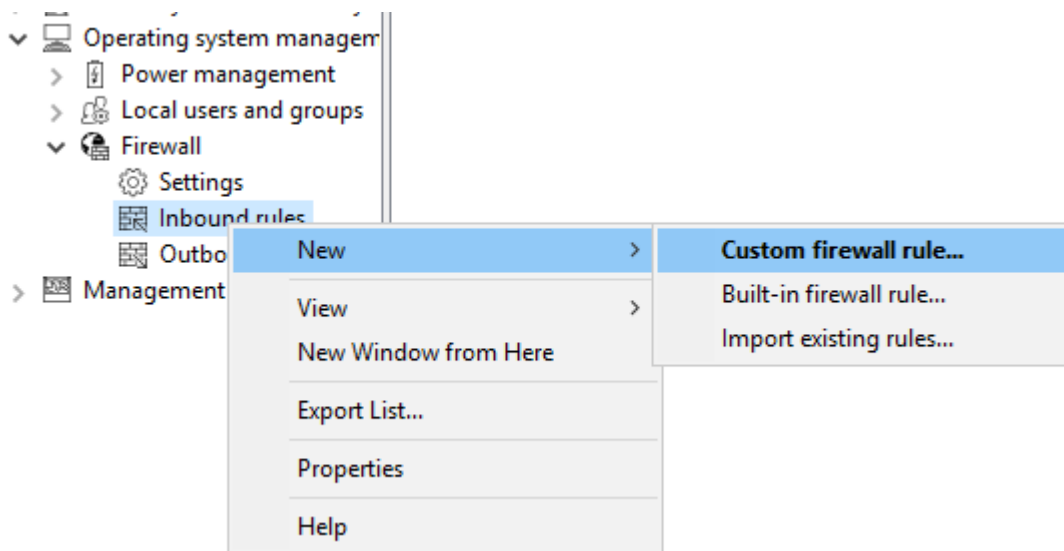
The following configuration options are available:

- **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 preceded 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):
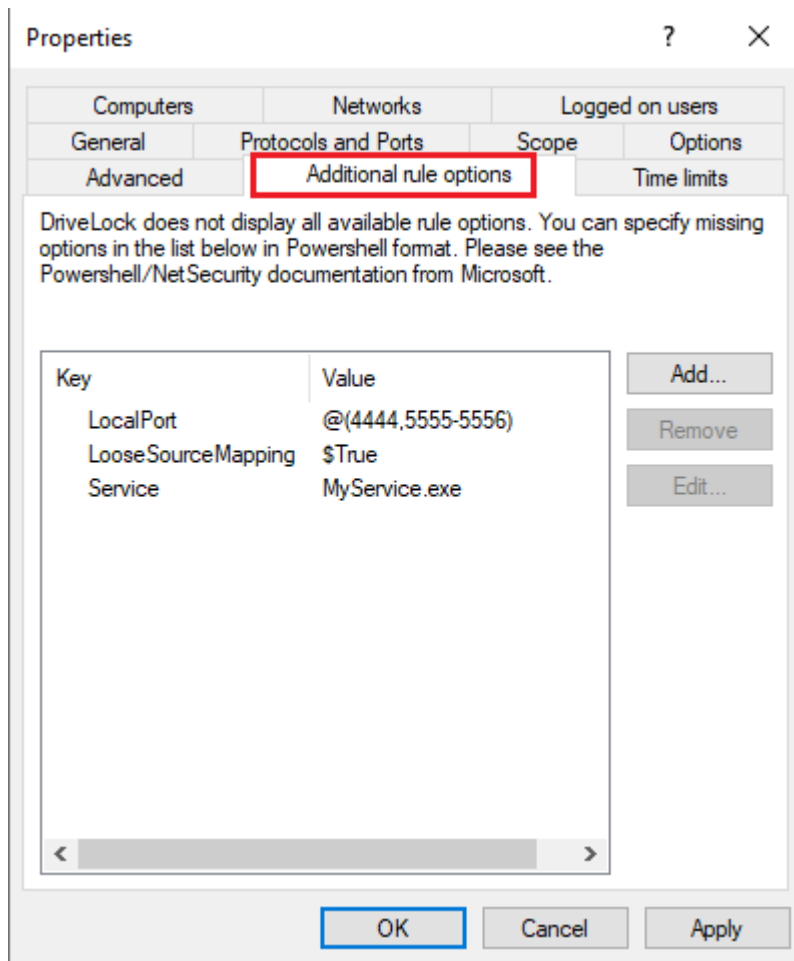
> 📝 Note: Note that these options only work with Windows 8.1 or later. Older operating systems will ignore these options.

- **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.

22 Events and alerts

This DriveLock functionality lets you

- monitor and configure all events related to DriveLock and its modules,

- submit DriveLock events to the DES,

- monitor third-party events, and

- Define and use event filters, alerts, and responses.

When combined with Application Behavior Control, you can use parts of the MITRE Attack Framework, which is provided as importable DriveLock rules. For this you need the Application Control license.

> Note: A comprehensive list of all events including a description can be found in the separate event documentation at DriveLock Online Help.

22.1 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.

22.1.1 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.

22.1.2 Event message transfer settings

Each of the possible targets to which events can be sent require different settings. To configure destinations for the transmission of events, open the **Events and alerts** node in the console structure on the left-hand side and select **Settings**. Then click **Event message transfer settings** in the right pane to open the settings dialog. The following tabs are available: Event log, SMTP, SNMP, Server, Options and Computer name.

609
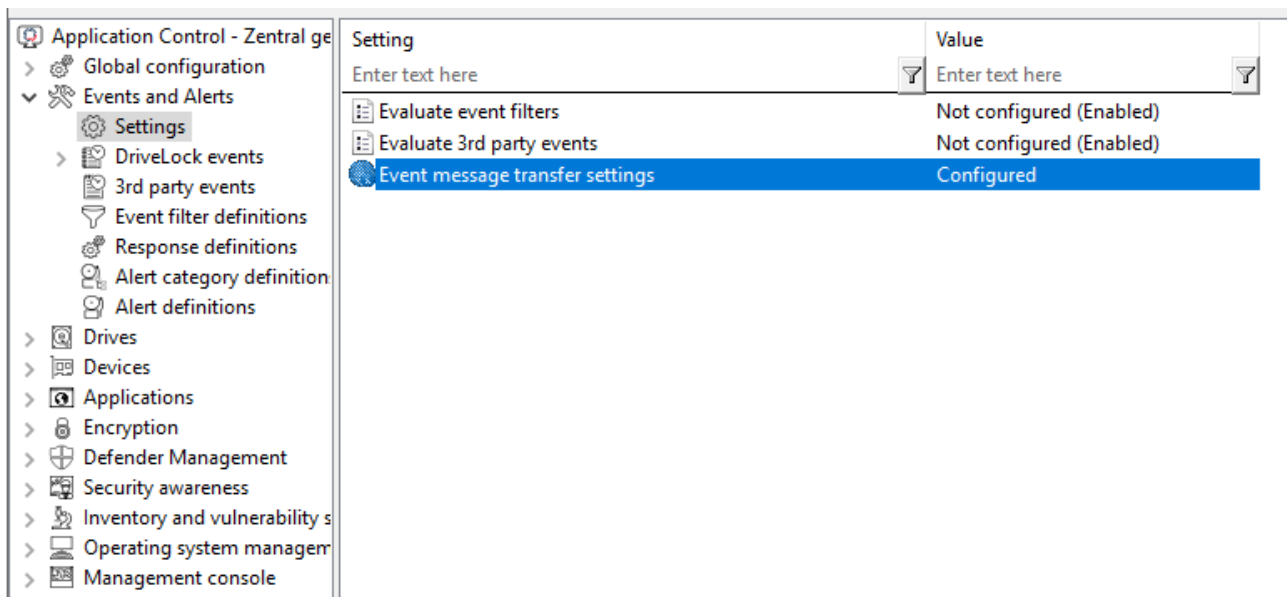
22.1.2.1 Event log

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.

22.1.2.2 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.

22.1.2.3 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.

22.1.2.4 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.

22.1.2.5 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.

22.1.2.6 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.

22.1.3 3rd party events

Use this functionality to collect and process third-party events. You can select a third-party event provider in the DriveLock Management Console and import its events. Then, the events can be forwarded from the agent to DriveLock Enterprise Service (DES) or used in event filters.

Third-party events are also registered if the DriveLock Agent is not active. As soon as the agent reports back to the DES, these events are processed.

The global setting **Evaluate 3rd party events** can be used to enable or disable this functionality.

> Note: Note that you can use this feature only if the events of the corresponding event provider are available for query. If this is not the case an empty list will appear instead.

22.1.4 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 trans-

mits 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.

22.1.5 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 various instances of the event are to be filtered. Click **Add** , to add criteria and logical operators 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.

The global setting **Evaluate event filters** allows you to specify whether event filters or alerts are evaluated.

22.1.6 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.

22.2 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. Using the **Is system user** filter property, you can filter for them.

After selecting the individual data masking mode for user or computer data in events, you can quickly configure the data masking setting in the context menu of any individual event ID.

22.3 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** tab in the DOC in the **Analysis** menu under **Events** (see figure).
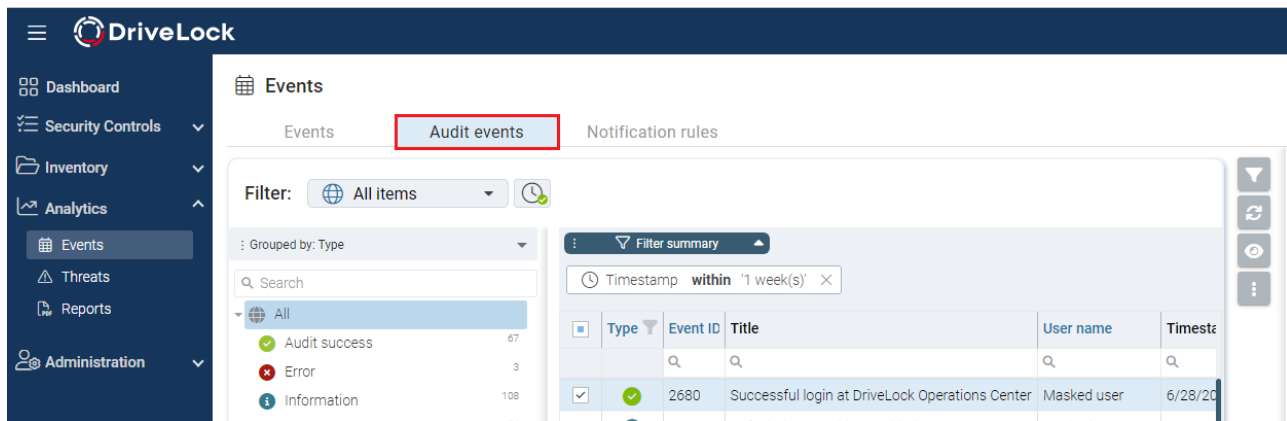
A list of all events and audit events can be found in the DOC.

22.4 Notification rules in the DOC

Configuration: DOC -> Analytics -> Events -> Notification rules

You can define notifications for all events that the DriveLock Agent reports to the DriveLock Enterprise Service (DES) via e-mails to one or more recipients. For example, if you want to be notified that DriveLock Agent has detected a virus on an agent, you can associate the corresponding event with an action. For this you will create a **notification rule**.
Please do the following:

1. Once you have assigned a name, choose the events you want to be notified about. Click **Select...** in the **Selected events** section. For example, select **Event 684: Microsoft Defender detected a threat**.

2. The notification rule is enabled by default. You can uncheck **Enable** if you want to temporarily disable the rule but not delete it.

3. Under **Actions** , click **Create new action** and enter the appropriate information in the dialog. If you click **Configure e-mail templates**, you can create different templates with custom texts, either in English or German.

> Note: If you have already created actions, you can select them again and again (even in different rules) and have them sent to the appropriate recipient groups.

Configuring the e-mail server

To configure an e-mail server to receive the notifications, click the ⋮ button and select **Configure e-mail server**.

> 📝 Note: The mail server is configured in the Tenant settings under e-mail and mail server.

The default setting is **DriveLock**, with e-mails sent via the DriveLock mail server. This option works only for Managed Security Services in the cloud. Alternatively, you can select **SMTP** if you are using DriveLock On-Premise. In this case, you must specify the configuration of your SMTP server yourself.

22.4.1 Variables in email notifications

The following variables are used when configuring e-mail templates:

Variable	Description
{name}	Rule name
{text}	Short name of the event that triggered the rule
{longtext}	Resolved event text with parameters
{id}	Event ID
{tenant}	Tenant name

23 MacOS support

DriveLock supports the assignment of centrally stored policies to DriveLock agents with operating system Ventura (13) and higher on Intel and ARM architectures.

> Note: For DriveLock On-Premise customers, the macOS Agent(DriveLock Agent.dmg or DriveLock Agent.pkg) is available on the DriveLock ISO file. Managed services customers can download the macOS Agent package from the installation area in the DriveLock Operations Center (DOC).

> Note: From version 2024.1, the Package Installer (*.pkg format) can be used for software distribution.

macOS support currently includes targeted blocking of external drives that are connected to the macOS clients via a USB interface, plus encryption of USB drives. This gives administrators the chance to control the usage of external drives on DriveLock macOS Agents so that clients are reliably protected against malware attacks. In addition, it is possible to evaluate some DriveLock events and create corresponding event filter definitions.

> Note: Please note that data masking is not yet implemented for the macOS agent.

In addition, command line parameters can be used to define a proxy server that is used for downloads and DES communication.

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

23.1 Installing the DriveLock macOS Agent

23.1.1 Installation with disk image file

Proceed as follows to install the DriveLock macOS Agent on macOS clients using a disk image file. Click here for information on how to install the agent with the Package Installer.

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

1. Double-click the **DriveLock Agent.dmg** disk image file.

2. Drag and drop the **DriveLock Agent** app into the **Applications** folder.
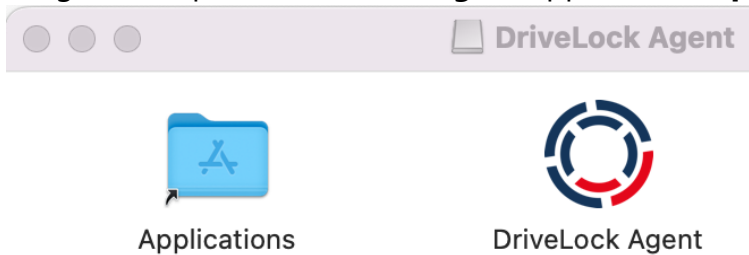
3. Now, configure the DriveLock Agent by running the following command line:
   ```
   % sudo /Applications/DriveLock\ Agent.ap-
   p/Contents/MacOS/dlconfig -t tenant_name -s DES_server_url -d
   debug_level
   ```
   Example:
   ```
   % sudo /Applications/DriveLock\ Agent.ap-
   p/Contents/MacOS/dlconfig -t root -s https://DES_HOSTNAME:6067
   -d 3
   ```

4. Start the DriveLock Agent system extension activation process from the DriveLock Agent app.

   1. Open the **DriveLock Agent** app in the **Applications** folder.

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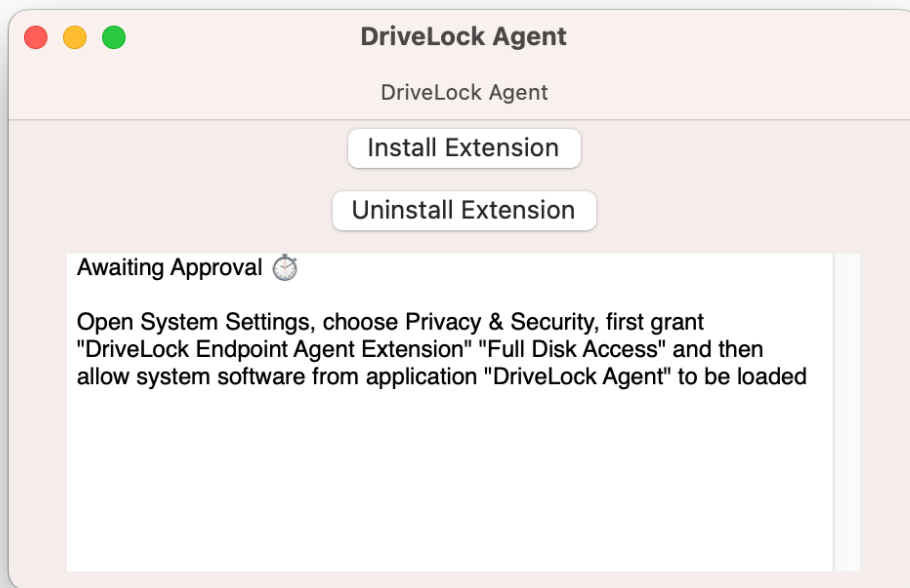
> Note: Alternatively, you can enable the system extension from the command line by entering the following command: `% /Applications/DriveLock\ Agent.app/Contents/MacOS/DriveLock\ Agent -a`

5. Then, in the **System Preferences/Settings** -> **Privacy & Security** section, enable **full disk access** for **DriveLock Endpoint Agent Extension**.
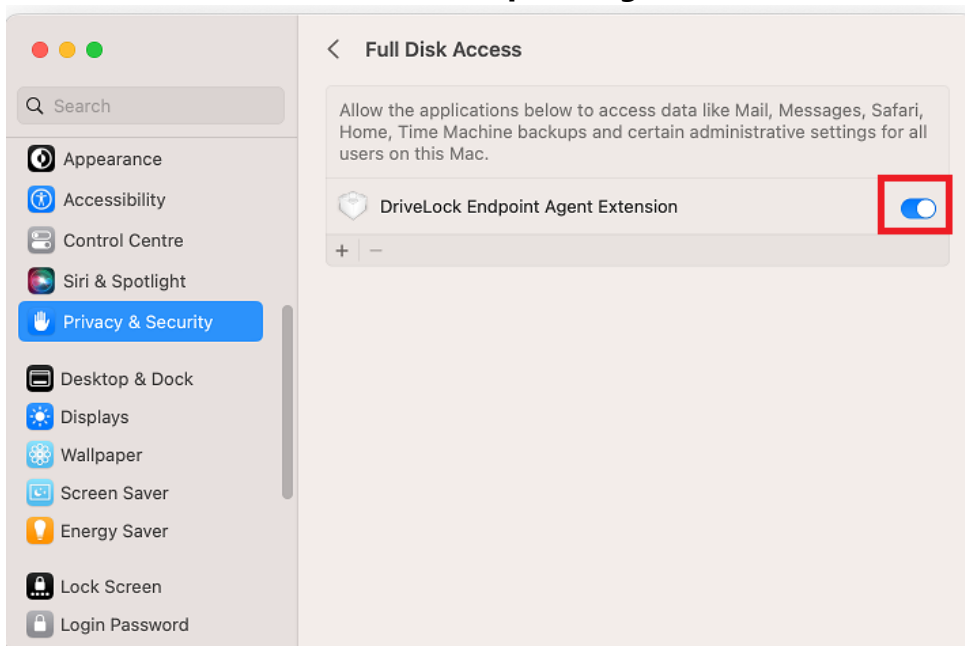
6. Next, allow the system software to load.
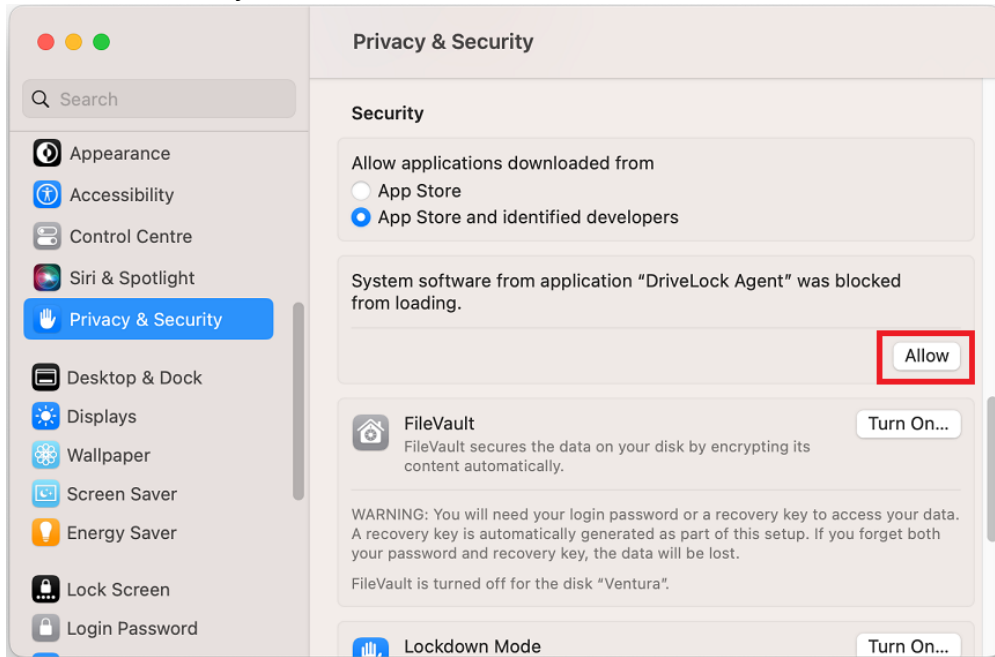
7. The installation is completed successfully as soon as the following message appears:
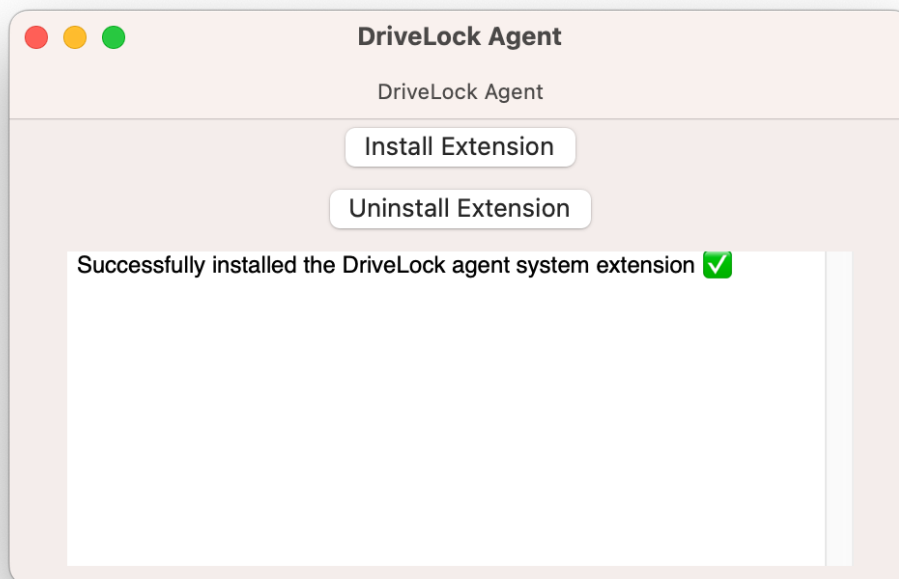
8. If necessary, you can check the process status of the DriveLock Agent in the activity display.

23.1.1.1 Use join token

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

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

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

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

23.1.1.2 Update

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

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

23.1.1.3 Uninstall

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

- **Uninstalling with the DriveLock Agent app**

    1. Open the app under **Programs**.

    2. Click the **Uninstall extension** button.

    3. Enter your password to delete the system extension.

    4. After the message **Successfully uninstalled the extension** appears in the app's dialog box, quit the DriveLock Agent app and delete it from the **Applications** folder.
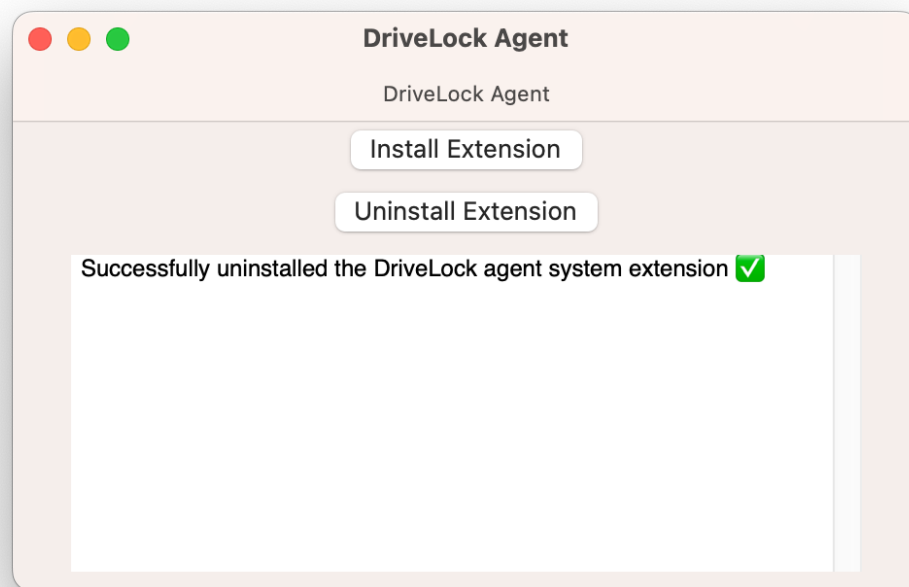
> 📝 Note: Alternatively, you can disable the system extension from the command line by entering the following command:
> ```
> % /Applications/DriveLock\ Agent.ap-
> p/Contents/MacOS/DriveLock\ Agent -d
> ```

- **Delete DriveLock Agent app directly from Programs.**

    1. Enter your password to delete the DriveLock Agent system extension.

    2. If the DriveLock Agent program is not completely removed the first time, you may have to delete it twice.

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

23.1.2 Manual installation with the Package Installer

Installation: DOC -> Settings ⚙ *-> Installation -> macOS -> Section "Installation of the MAC-Agent with the Package Installer" -> Download Package Installer*

The DriveLock Agent can also be installed using the Package Installer.
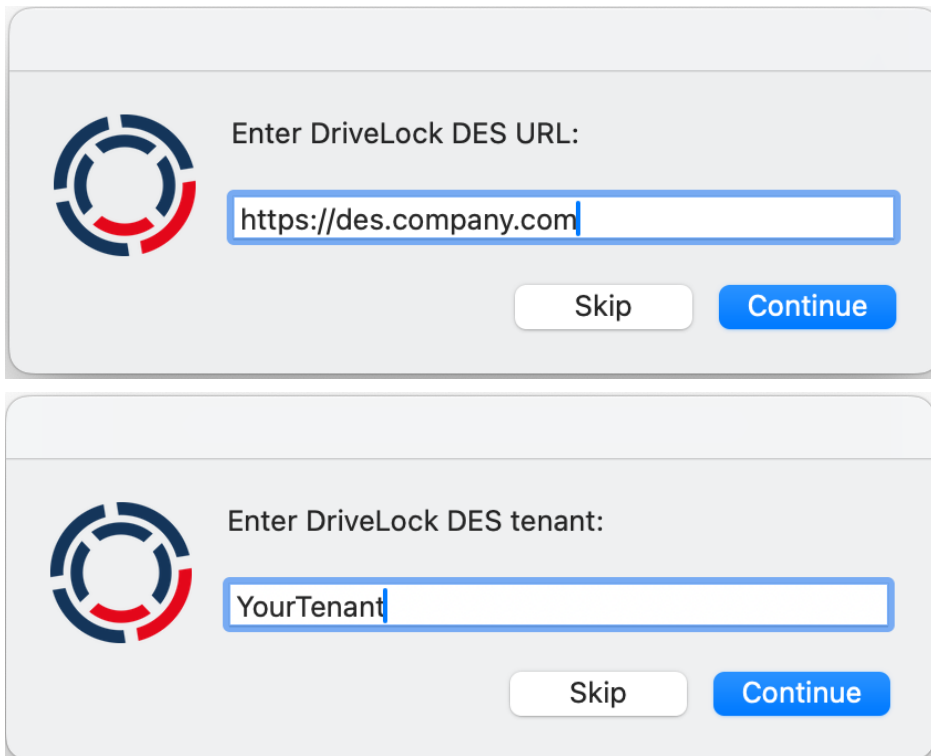
> Note: Before you start installing, make sure to have the following information available: URL for your own DriveLock Enterprise Service (DES) and the name of the tenant. You will receive both from your administrator.

Please do the following:

1. Double-click the downloaded **DriveLock Agent.pkg file**.

2. Follow the instructions in the welcome dialog and click **Continue**.
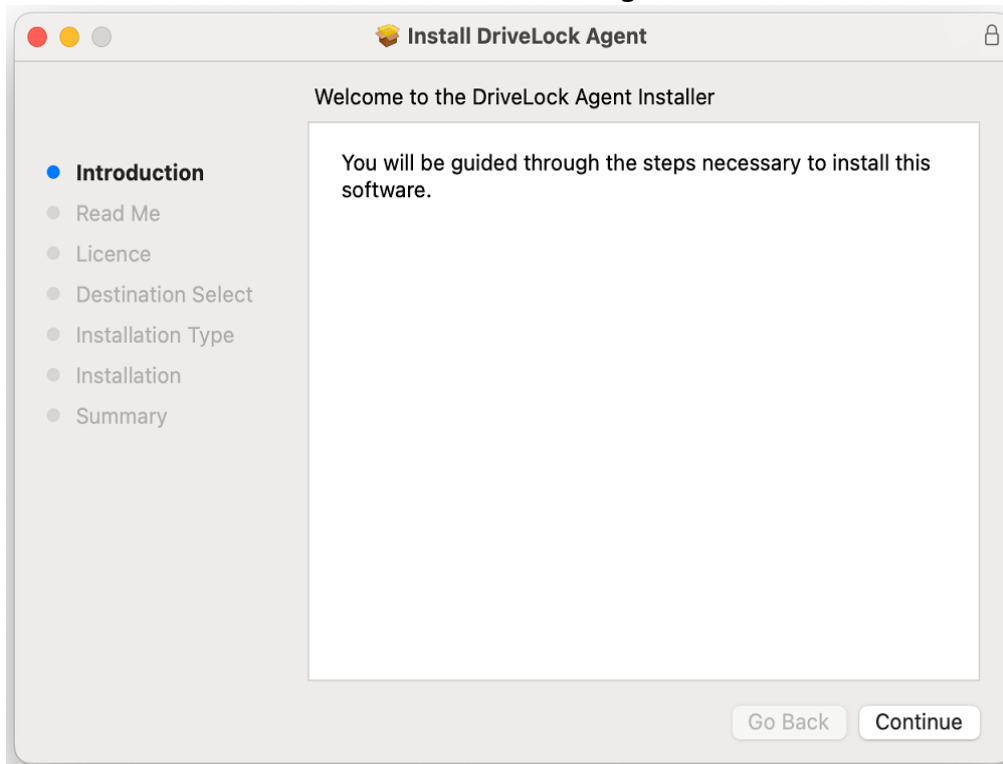
3. The **Read Me** section provides more information on the installation. Please read them carefully.

4. Agree to the **license** agreement under **License** and go to the next dialog.

5. Next, install the DriveLock Agent on the system you are currently running.
Continue by entering your password in the **Installer** .
Click **Install software**. During this process, you must enter the URL for your DES and the client name.

Next, **Open System Settings**.
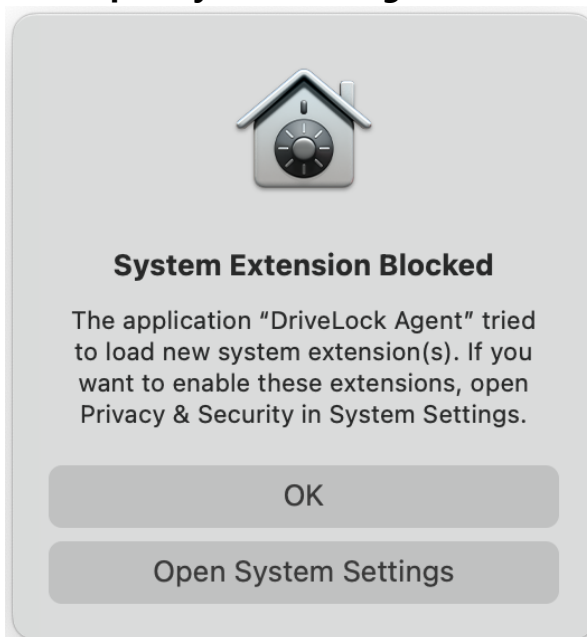
6. Then follow **steps 5 and 6** of the Installation with disk image file topic.

7. The last step shows the successful installation.
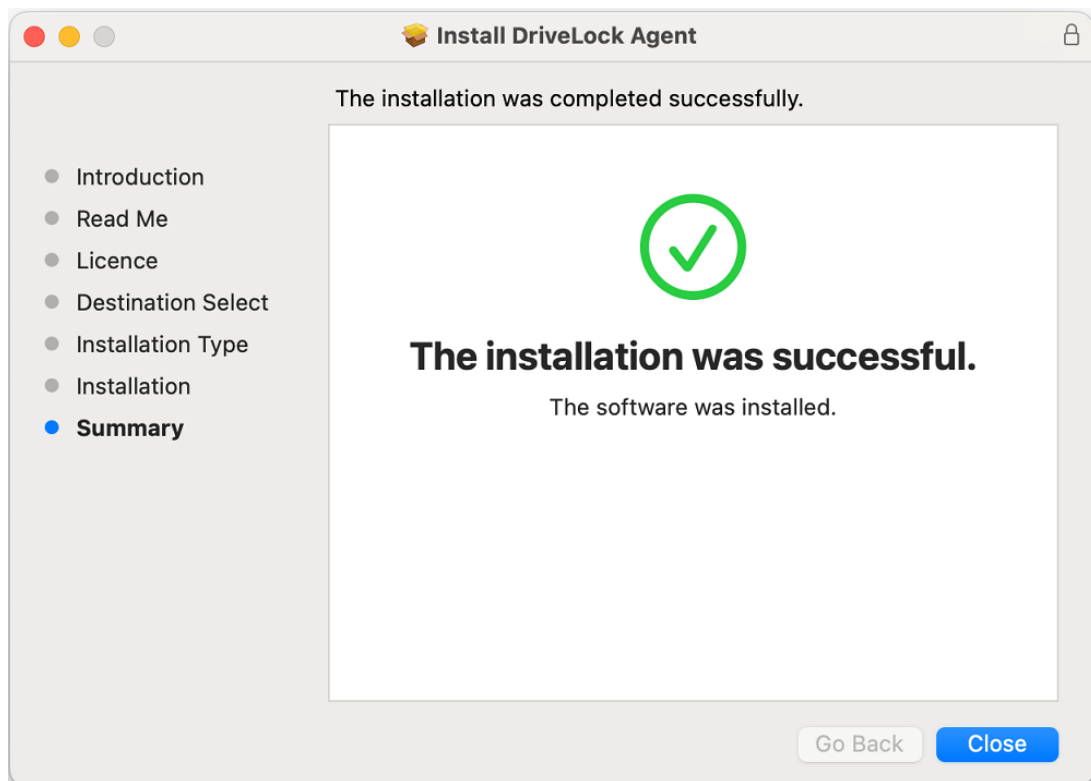
23.1.3 Unattended installation of the DriveLock Agent

From version 2024.1, the Package Installer can be used for software distribution with an MDM system.

The following guidelines explain how to configure the MDM system and how to create installation and uninstallation scripts.

> Note: For some MDM systems (e.g. JAMFNow), the installation package differs from this.

Requirements for the MDM settings (Microsoft Intune, JAMF or others):

- The DriveLock Endpoint Agent Extension must be given "Full disk access".

- Allow the DriveLock system extension with the bundle identifier `com.drive-lock.agent.extension` to be installed unattended.

Installation:

1. Install the DriveLock Agent App:
   ```
   % sudo installer -pkg "path/to/DriveLock Agent.pkg" -target /Applications
   ```

2. Configure the DriveLock Agent with user-specific settings:

```
% sudo /Applications/DriveLock\ Agent.ap-
p/Contents/MacOS/dlconfig --server 'https://y-
our.drivelock.cloud' --tenant 'your_tenant'
```

Uninstallation:

1. Unload the DriveLock system extension
   ```
   % sudo /Applications/DriveLock\ Agent.ap-
   p/Contents/MacOS/DriveLock\ Agent -d
   ```

2. Delete the DriveLock Agent App
   ```
   % sudo rm -R /Applications/DriveLock\ Agent.app
   ```

23.1.3.1 Repackage the DriveLock Agent package manually

Some MDM systems, such as JamfNow, do not support software distribution with scripts. To enable a fully automated installation with these MDM systems, an MDM administrator must configure the specific (organizational) settings for the DriveLock Agent within the Package Installer before the software can be distributed via the MDM system.

Prerequisites:

- Xcode command line tools has been installed

- Developer ID Installer certificate of the company has been installed in Keychain

Please do the following:

1. Unpackage the DriveLock Agent Package Installer:
   ```
   % pkgutil --expand /path/to/drivelock/agent.pkg /folder-
   /to/extract/to
   ```

   > ![note icon]   Note: Ensure that the folder you want to extract to does not exist beforehand.

2. Open the postinstall file with an editor. Such as:
   ```
   % vi /extracted/folder/DriveLock_Agent.pkg/Scripts/postinstall
   ```
   The postinstall file can also be opened by right-clicking on the **DriveLock_Agent.pkg** within the extracted folder, select **Show Package Contents** from the context menu, right-click on file Scripts/postinstall, and open it with your appropriate application, such as Visual Studio Code.

3. Configure agent settings.

Fill in DES_URL, DES_TENANT, DES_JOINTOKEN (optionally) according with your company settings and save the file.

4. Pack the modified Package Installer.
```
% pkgutil --flatten /extracted/folder path/of/-
modified/drivelock/agent.pkg
```

5. Sign the modified Package Installer with Developer ID Installer certificate.
```
% productsign --sign "Developer ID Installer: Your Company
(XXXXXXXXX)"path/of/modified/drivelock/agent.pkg
path/of/signed/drivelock/agent.pkg
```

6. Check signature of the newly signed Package Installer
```
% pkgutil --check-signature path/of/signed/drivelock/agent.pkg
```
The output should be similar to the following:

```
 1  Status: signed by a developer certificate issued by Apple for distribution
 2     Signed with a trusted timestamp on: 2024-10-01 14:06:22 +0000
 3     Certificate Chain:
 4      1. Developer ID Installer: Your Company (XXXXXXXXX)
 5         Expires: 2025-01-21 10:22:41 +0000
 6         SHA256 Fingerprint:
 7             1A C4 ED 34 AB DA BE 30 BC 79 72 3C 19 BC 74 19 96 07 9A 3C B6 B0
 8             24 23 7C 2B B6 1C DD 5A B5 D4
 9             ------------------------------------------------------------------
10      2. Developer ID Certification Authority
11         Expires: 2027-02-01 22:12:15 +0000
12         SHA256 Fingerprint:
13             7A FC 9D 01 A6 2F 03 A2 DE 96 37 93 6D 4A FE 68 09 0D 2D E1 8D 03
14             F2 9C 88 CF B0 B1 BA 63 58 7F
15             ------------------------------------------------------------------
16      3. Apple Root CA
17         Expires: 2035-02-09 21:40:36 +0000
18         SHA256 Fingerprint:
19             B0 B1 73 0E CB C7 FF 45 05 14 2C 49 F1 29 5E 6E DA 6B CA ED 7E 2C
20             68 C5 BE 91 B5 A1 10 01 F0 24
```

7. Once the repackaged Package Installer is properly signed, it is ready to be deployed through a MDM system. The admin can decide if this repackaged Package Installer should be notarized, but it is not mandatory for the further MDM deployment.

23.2 System requirements

23.2.1 Supported macOS versions

DriveLock supports macOS from version Ventura (version 13) with Intel (x86_64) and Apple Silicon (arm64) architectures.

23.2.2 DriveLock configurations

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

- DriveLock Management Console (DMC) and Policy Editor or DriveLock Operations Center (DOC) with DOC Companion

- DriveLock Enterprise Service (DES)

- DriveLock macOS Agent (on macOS clients)

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

23.3 Settings in the DriveLock Policy Editor

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

- **Global configuration**: Settings, Server connections, Trusted certificates

- **Events and alerts**: events (general events, device and drive events), event filter definitions

- **Drives**: Removable drive locking, Drive whitelist rules
  Example: If you want to generally block the usage of USB drives, but allow specific USB flash drives, you will set the appropriate blocking settings first and then create a drive rule for the allowed USB flash drives (whitelist mode).

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

23.3.1 Global configuration

1. Open the **Settings** section to configure the following:

   - **License**: Add here the licenses you have purchased for your macOS agents.

   - **Remote control settings and permissions**: On the **Permissions** tab, you specify the users who are explicitly allowed to perform actions on the macOS agent, such as making changes to the configuration.

   - **Event message transfer settings**: Make sure to check the **Enable event forwarding to the DriveLock Enterprise Service** option on the **Server** tab. The second option, **Report agent status to server**, allows you to specify the intervals for sending agent alive messages to the DES.

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

   - Settings for logging: **Logging level**, **Maximum log file size in MB** and **Time until automatic deletion of old log files**.

2. In the **Server connections** section you can add a new server, if required.

3. In the **Trusted certificates** section you select the certificates for the secure communication between the DriveLock Management Console and/or the DriveLock macOS Agents and the DES.

23.3.2 Drives

23.3.2.1 Drive settings

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

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

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

1. Select the default option **Deny (lock) for all users (default)**:
   This setting blocks the use of all drives connected via the USB interface for all users. You will need to define a whitelist rule that allows specific drives to be used.

2. Select **Allow** (for all users):
   This option allows users to connect all drives over the USB interface. You will need to specify the drives you want to block in your drive rule.

23.3.2.2 Drive whitelist rules

To block drives, the macOS Agent supports:

- Windows hardware ID of the parent USB device (optionally with serial number)

- Numerical USB IDs for vendor, product and revision (optionally with serial number)

- Windows rules for vendor, product and revision names; from version 2024.2 optionally with serial number

- All three rule types are also supported in drive collections.

- From version 2024.2, the drive events are reported with Windows-compatible vendor, product and revision names.

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

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

2. On the **General** tab, please enter the drive's hardware ID. This ID consists of the vendor ID (VID), product ID (PID) and revision number (REV).

3. On the **Permissions** tab, specify whether to deny (lock) or allow the drive (depending on your removable drive settings).

> ⚠ Warning: Note that locking with access for defined users/groups is not possible on macOS agents.

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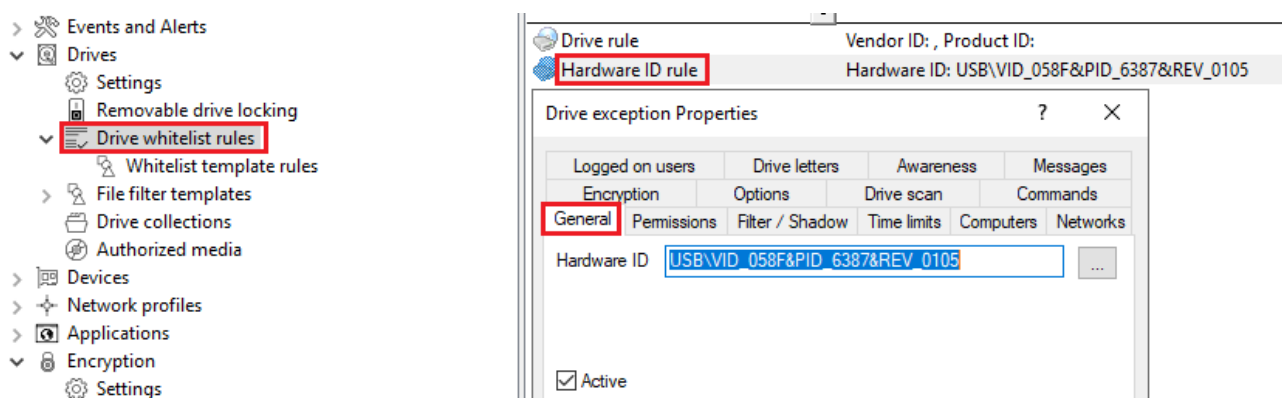
23.3.3 Agent remote control

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

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

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

1. **Disconnect** the Linux agent.

2. **Unlock temporarily...** : more information here.

3. **Show RSOP...**
   Click this option to view a summary of the policy assigned to the macOS agents. You can not change any settings here.

4. **Agent configuration...**
   Click this option to open a dialog with information on the agent's configuration. It shows you the server your macOS Agent receives the centrally stored policy from and, if necessary, you can add another server or enter another tenant on the **Options** tab.

5. **Display inventory data**
   Click here to get inventory information on your macOS Agent (on the **General**, **Drives**, **Networks** tabs)

23.3.3.1 Temporary unlock

Use the temporary unlocking feature to quickly and temporarily allow a connected DriveLock macOS Agent to access blocked drives via agent remote control in the DriveLock Management Console (DMC). This can also be done from the DriveLock Operations Center (DOC).

Please do the following:

1. From the macOS Agent context menu, choose the menu command **Unlock temporarily....**

2. Specify the drive types you want the unlock to apply to.

3. Then, specify the time period and reason for unlocking the drive.

23.4 macOS Agents in the DOC

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

The following DOC views are relevant for macOS agents:

- **Inventory/Computers**: Filter by **OS type**, for example, to have your macOS agents grouped by their operating system. Select any macOS agent to view its details.

- **Inventory/User**: In this view you can see a listing of all user accounts that are allowed to access the DOC. It also shows information on status and roles along with name and logon details.

- **Administration/Groups**: If you have defined a DriveLock group for your macOS agents, it will be displayed here with information about the respective members and the assigned policies.

- **Analysis/Events**: The events that a macOS agent sends to the DES are listed in this view.

- **Analysis/Threats**: The **Alerts** tab provides ongoing monitoring and configurable response to safety-related events.

23.4.1 Creating a DriveLock group in the DOC

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

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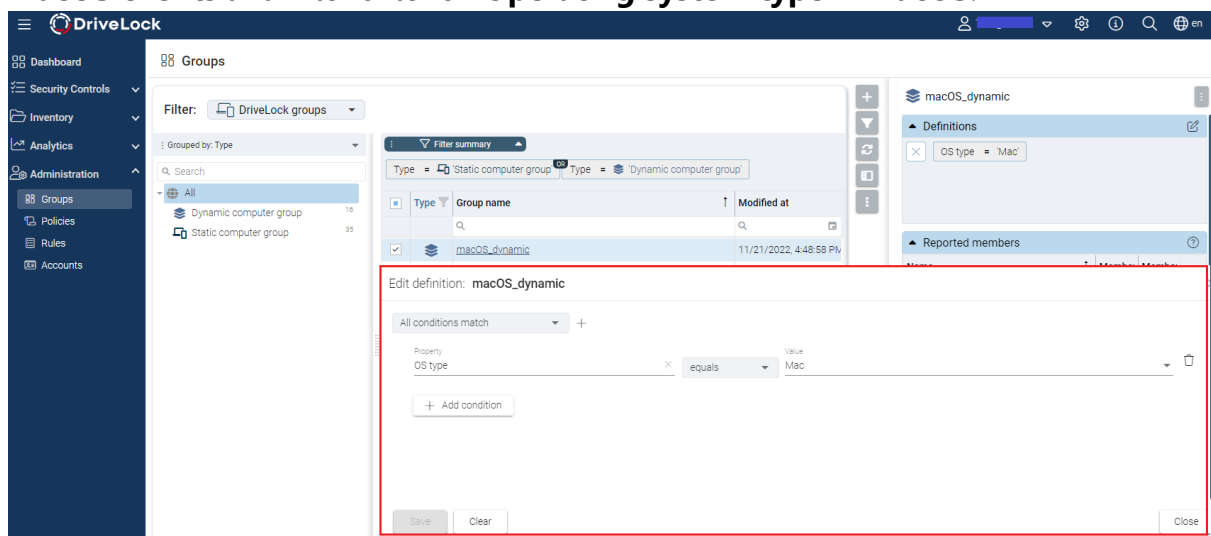
2. Further information on DriveLock groups can be found here.

3. If you want to use a different tenant for your DriveLock macOS agents, you must explicitly select it. Further information on using tenants can be found here.

4. Create a new centrally stored policy for your macOS clients, name it accordingly (for example 'macOSpolicy') and start with Global configuration settings.

5. Assign the 'macOS policy' to your DriveLock group. You can also assign to All Computers if you do not want to use a group.

23.4.2 Temporary unlock from the DOC

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

The example shows the macOS agent to be unlocked.

The temporary unlock ends after the configured time limit. If an absolute time is specified, the temporary unlock will survive a restart if the time is still within the configured period.

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

All USB drives can be unlocked at once for drive control.

23.4.3 Display license status in DOC

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

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

23.5 Events

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

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

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

23.5.1 Event settings

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

1. In the **Events and Alerts** node, open the **Events** sub-node. Doubleclick the event in the **Drive events** section. For macOS agents, only the settings on the **General** tab are currently possible (see figure).
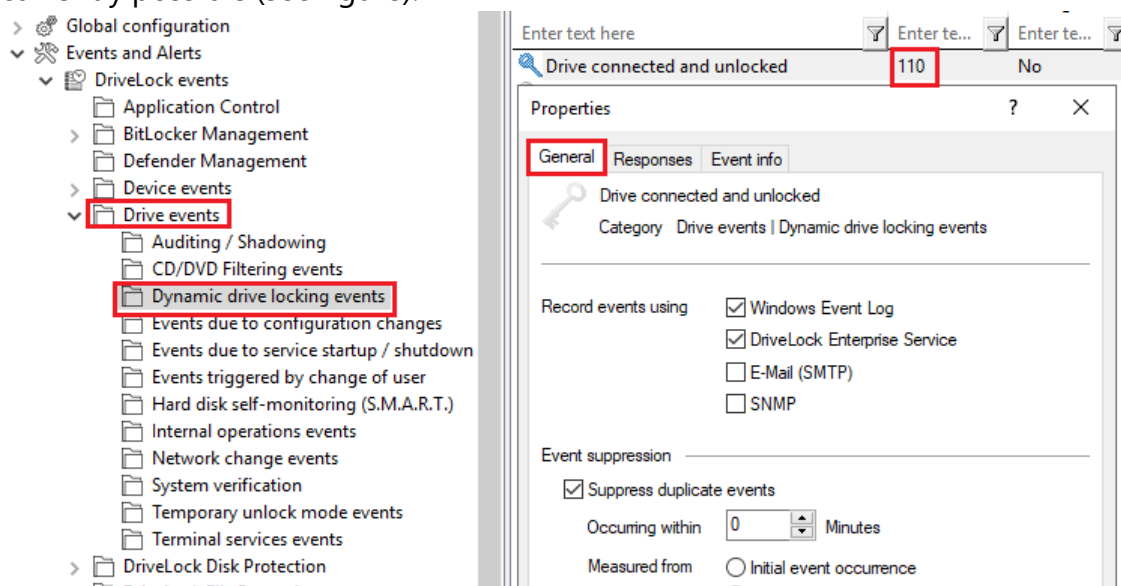
2. The System Event Log (**Windows Event Log**) option is the default, but you can also select **DriveLock Enterprise Service** to save the events in the event log on the DES.

3. If required, you can also check the **Suppress duplicate events** option.

23.5.1.1 Event filter definitions

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

You can filter

- by filter criteria,

- by computers (with computer names or Drivelock groups)

- and by times.

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

23.5.1.1.1 Create event filter definitions

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

Please do the following:

1. Right-click the **Event Filter Definitions** sub-node in the **Events and Alerts node** and select **New.**.. from the menu. A list of available events is displayed. Select the event 238.

2. On the **General** tab, check the **Windows Event Log** and **DriveLock Enterprise Service** options.

3. On the **Filter criteria** tab, select the parameters to filter by. By clicking the **Add** button you can select the appropriate criteria and the operators.
   In the example above, one criterion would be the **function name** GetAgentStatus. Then the DriveLock Agent will send only the relevant events.

23.5.2 List of events

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

Eine Auflistung aller Ereignisse, die in Zusammenhang mit DriveLock wichtig sind, finden Sie im DOC.

The DriveLock macOS agent reports the following events to the DES:

Event ID	Event level (Information, Warning, Error)	Event text	Description
105	Information	Service started	The [name] service was started.
108	Information	Service stopped	The service [name] was stopped.
110	Audit	Drive connected and unlocked	The drive [name] ([category]) was added to the system. It is a [type] bus device. The drive is [locked/unlocked] for this event's user account. Device Id: [ID] [ID] (Rev. [rev]) (Serial number [number]) Applied whitelist rule: [rule] Screen state (keyboard [Win]-[L]): [state]
111	Audit	Drive connected and locked	The drive [name] ([category]) was added to the system. It is controlled by {Product} because of company policy. As an ACL was applied to the drive, some users may no longer be able to access it. It is a [type] bus device. The drive is [locked/unlocked] for this event's user account.

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

Event ID	Event level (Information, Warning, Error)	Event text	Description
			Agent ended because the unlock time elapsed.
152	Warning	Policy storage extraction failed	The policy storage container [name] cannot be unpacked to the local computer. Some functions relying on files stored in this container may fail.
153	Warning	Configuration file applied	The configuration file [name] was successfully applied.
154	Error	Configuration file download error	The configuration file [name] could not be downloaded. Error code: [code] Error: [error]
158	Error	Configuration file error	The configuration file [name] could not be read. Error code: [code] Error: [error]
191	Warning	{PrefixEnterpriseService} selected	The {PrefixEnterpriseService} [name] was selected by {Product}. Connection ID: [ID] Used for: [Invent-

Event ID	Event level (Information, Warning, Error)	Event text	Description
			ory/Recovery/Events]
192	Warning	{Pre-fixEnterpriseService} not available	No {Pre-fixEnterpriseService} is available because no valid server connection is configured.
199	Warning	Drive temporarily unlocked	Drive types temporarily unlocked by administrative intervention are [DriveType1] [DriveType2] [DriveType3] [DriveType4] [DriveType5] [DriveType6] [DriveType7] [DriveType8] [DriveType9] [DriveType10]
235	Error	SSL: Cannot set up	The encrypted communications layer (SSL) could not be set up. Error: [error]
236	Error	Remote control: Cannot set up server	The remote control server component coud not be set up. Agent remote control will be unavailable. Error: [error]
237	Error	Remote control:	Agent remote control: An

Event ID	Event level (Information, Warning, Error)	Event text	Description
		Internal error	internal SOAP communications error occurred. Error: [error]
238	SuccessAudit	Remote control: Function called	An Agent remote control function was called. Calling IP address: [IP address] Called function: [function]
243	Error	Cannot open database	A database could not be opened. Database file: [name] Error code: [code] Error: [error]
246	Error	Cannot store configuration status	The Agent cannot store the configuration status used by other {Product} components. Error code: [code] Error: [error]
247	Error	Cannot initialize configuration store	{Product} Agent cannot initialize the configuration database stores.
249	Error	Configuration file: Fallback configuration applied	A configuration using configuration files was detected but no settings could be retrieved from a configuration database.

Event ID	Event level (Information, Warning, Error)	Event text	Description
			{Product} will fall-back to a configuration where all removable drives are blocked.
250	Warning	Configuration file: Using cached copy	The configuration file [name] could not be loaded from its original location. A locally cached copy was used.
251	Error	Configuration file: Cannot extract	A {Product} configuration file could no be extracted.%rSettings from this file will not be applied. Database file: [name] Error code: [code] Error: [error]
264	Error	Cannot merge configuration database with RSoP	Cannot merge the configuration database [name] into the resulting set of policy.
287	Error	No server defined for inventory	No server is defined for uploading collected inventory data.
288	Information	Inventory collection successful	Hard- and software inventory data was successfully

Event ID	Event level (Information, Warning, Error)	Event text	Description
			collected and uploaded. DES server: [server name] Connection ID: [ID]
289	Information	Inventory collection failed	An error occurred while collecting hard- and software inventory data.DES server: [server name] Connection ID: [ID] Error: [error]
294	Error	Cannot download centrally stored policy	The centrally stored policy [name] could not be downloaded. Server: [name] Error: [error]
295	Error	Centrally stored policy: Cannot extract	A centrally stored policy could no be extracted. Settings from this file will not be applied. Configuration ID: [ID] Error code: [code] Error: [error]
297	Error	Centrally stored policy: Fall-back configuration applied	A configuration using centrally stored policies was detected but no settings could be retrieved from a server. {Product} will fall-back to a configuration where all removable drives

Event ID	Event level (Information, Warning, Error)	Event text	Description
			are blocked.
299	Information	Centrally stored policy downloaded	The centrally stored policy [name] was successfully downloaded. Configuration ID: [ID] Version: [version]
443	Error	Component start error	A {Product} system component could not be started on this computer. Error code: [code] Error: [error] Component ID: [ID]
520	Error	All {PrefixES} not reachable	Cannot load company policy. All configured {PrefixEnterpriseService}s are not reachable.
521	Error	Cannot determine computer token	Cannot determine the computer token. Error code: [code] Error: [error]
522	Error	Error loading policy assignments	An error occurred while loading policy assignments from server [name]. Error: [error]
523	Error	Policy integrity check	The integrity of an assigned

Event ID	Event level (Information, Warning, Error)	Event text	Description
		failed	policy could not be verified.%rPolicy ID: [ID] Policy name: [name] Actual hash: [value] Expected hash: [value]
533	Warning	No policy - wiped	No valid policy available - the company policy was wiped because the computer was offline for a long period of time.
584	Information	Inventory started	Inventory generation was triggered by DES.
639	Error	Server certificate error	Server certificate error detected. Certificate: [name]. Error message: [text]

23.6 DriveLock configuration tool

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

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

Parameter details:

Parameter	Description
-s, --server serverurl	Specifies the DES the macOS client communicates with
-t, --tenant tenantname	Specifies the tenant for your macOS agent
-j, --jointoken token	Specifies the join token set during installation
-p, --set-proxy<type>;<proxy>	Specifies the proxy server to be used for downloads and DES communication. <type> can be system, none, named or pac with the following meaning:

Parameter	Description
	• `system` = use system proxy settings • `none` = no proxy • `named;<proxy>:<port>` = explicit proxy • `pac;<pac url>` = use proxy configuration script Example: `% sudo ./dlconfig -p "pac;https://www.company.com/proxy.pac"`
`-x, --setproxyaccount <proxy-user>;<proxypassword>`	Sets the credentials for the proxy server.
`-m, --removeproxy`	Deletes all proxy settings.
`-d, --debug off|<0-7>`	Enables or disables tracing to log files located in the installation directory in the log subfolder. (Larger number means more detailed tracing. Standard is 4 - info. The value 0 or off disables tracing).
`-u, --update`	Updates your configuration, e.g. if you have made changes to your policies The macOS Agent then connects to the DES immediately and loads the changes
`-a, --status`	Shows the current status of the macOS client and informs when, for example, the DES was last contacted, which policies are assigned or which DriveLock modules are licensed (see fig-

Parameter	Description
	ure below)
`-r, --recre-atebootdevices`	Creates a new list of currently connected USB devices that should always be allowed at boot time

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

23.7 macOS tools

The following command line tools are available for macOS.

1. To check the status of the process:

   `% sudo launchctl list 6GZR4TWXD2.com.drivelock.agent.extension:` Allows you to view the details of the DriveLock agent system extension history.

2. To display all system extensions:

   `% sudo systemextensionsctl list:` Displays all system extensions that are installed on the corresponding client.

24 Linux support

DriveLock supports assigning centrally stored policies to DriveLock agents running the Linux operating system.

The functionality of Linux support is currently limited to locking external devices and drives connected to Linux clients via a USB interface, plus some application control functions. This gives administrators control over the usage of devices, drives and applications, on DriveLock Linux agents as well, so that these client computers are reliably protected from malware attacks. In addition, it is possible to evaluate some DriveLock events and create corresponding event filter definitions.

> ⊗ Warning: Please note the restrictions for Linux in the system requirements for the DriveLock Agent in the current release notes at DriveLock Online Help.

24.1 System requirements

24.1.1 Supported Linux distributions

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

- Debian 12
- Fedora 40
- IGEL OS 11.05
- Red Hat Enterprise Linux 5
- SUSE 15.4
- Ubuntu 24.04
- AlmaLinux OS 9.4

24.1.2 DriveLock configurations

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

Complete installation and configuration of DriveLock with the current version

- DriveLock Management Console (DMC)
- DriveLock Enterprise Service (DES)
- DriveLock Linux agent (on the Linux clients)

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

24.2 Installing the DriveLock Agent

24.2.1 Installation instructions

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

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

1. Copy and extract the **drivelock.tgz** file on your Linux clients. It is included on the DriveLock ISO image.

2. The file contains the **drivelockd-install.sh** installation script . Run this script (see also Installation parameters).

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

   ```
   test@testub:~$ sudo ./drivelockd-install.sh
   [sudo] password for test:
   Drivelock self extract installer
   extracting archive...
   install to path [suggest: '/opt/drivelock']:
   drivelock server url [format: http(s)://<server>:<port>]: https://192.168.8.249:6067
   drivelock tenant [default: root]: kav
   drivelock tenant join token [default: none]:
   installing drivelock linux agent to: '/opt/drivelock'
   setting server to: 'https://192.168.8.249:6067'
   setting tenant to: 'kav'
   starting agent ...
   ```

3. Enter the following:
   - Installation path: The default is `/opt/drivelock`, but you can also specify a different path.
   - DES and port: Enter the server URL in the format '`https://<Server->:<Port>`' here.
   - Tenant: The default is 'root', but you can also specify a different tenant (in the figure `kav`).
   - Join token: a join token can be specified here or the line can be left empty.

4. The DriveLock Service starts as soon as the DriveLock Linux Agent has been completely installed.

5. If you experience errors during installation, we recommend restarting the Linux client to ensure that all DriveLock messages are displayed in the Linux client's user interface.

> ✎ Note: The Linux client only displays messages when devices are connected or disconnected (as popups), the DriveLock Agent does not have its own user interface here.

24.2.2 Installation parameters

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

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

 options:
  -h|--help                        print this help message
  -c|--custom-part                 create a custom partition package
  -i|--install <PATH>              install into path
  -s|--server <SRV>                server
  -t|--tenant <TENANT>             tenant
  -j|--jointoken <TOKEN>           tenant join token
  -d|--debug                       set debug logging level
  -r|--remove                      unintall drivelock
```

You can specify the following installation parameters:

- `-h`: Displays help for the installation parameters

- `-c`: This parameter only applies to IGEL clients. Here you enter the Custom Partition Package you want to use.

- `-i`: Enter the path to the DriveLock installation directory. The default is the current working directory, but you can also specify a different path.

- `-s`: Enter the server here in the format `https://<server>:<port>`'. See figure above.

- `-t`: Enter the tenant, the default is 'root'.

- `-j`: Set a join token during the installation. More information here.

- `-d`: Sets the local log level

- `-r`: Uninstalls the Drivelock agent

651

24.2.3 Installing the DriveLock agent via the IGEL app

As of version 2024.1, the DriveLock Agent for IGEL OS 12 will be available for download in the IGEL App Portal.

There are different procedures to follow depending on whether you are installing the DriveLock app in an IGEL UMS environment or locally (without UMS).

After installation, you can view the status of the DriveLock Agent on a client by searching for the client computer in the DES inventory.

You can query the current status of the DriveLock agent locally on the client with the command `drivelock-ctl -showstatus`. Further command line parameters can be found here.

24.2.3.1 Installing the DriveLock IGEL App in the UMS environment

To import the DriveLock IGEL app from the Igel App Portal into your UMS, proceed as follows:

1. Installing and configuring the DriveLock app
   Open the **App Portal menu**, select the **DriveLock app** in the **Security** category and click **Import**.
   If you are using an offline UMS, you must export the app from the app portal and upload it to your UMS.
   Please find further information in the IGEL Knowledge Base

2. Assign the app to your devices
   After installation, assign the app to your devices. See IGEL Knowledge Base.

3. Configure the app in UMS
   You can save the app configuration in an IGEL profile in order to distribute it to the cli-

ents. See IGEL Knowledge Base.
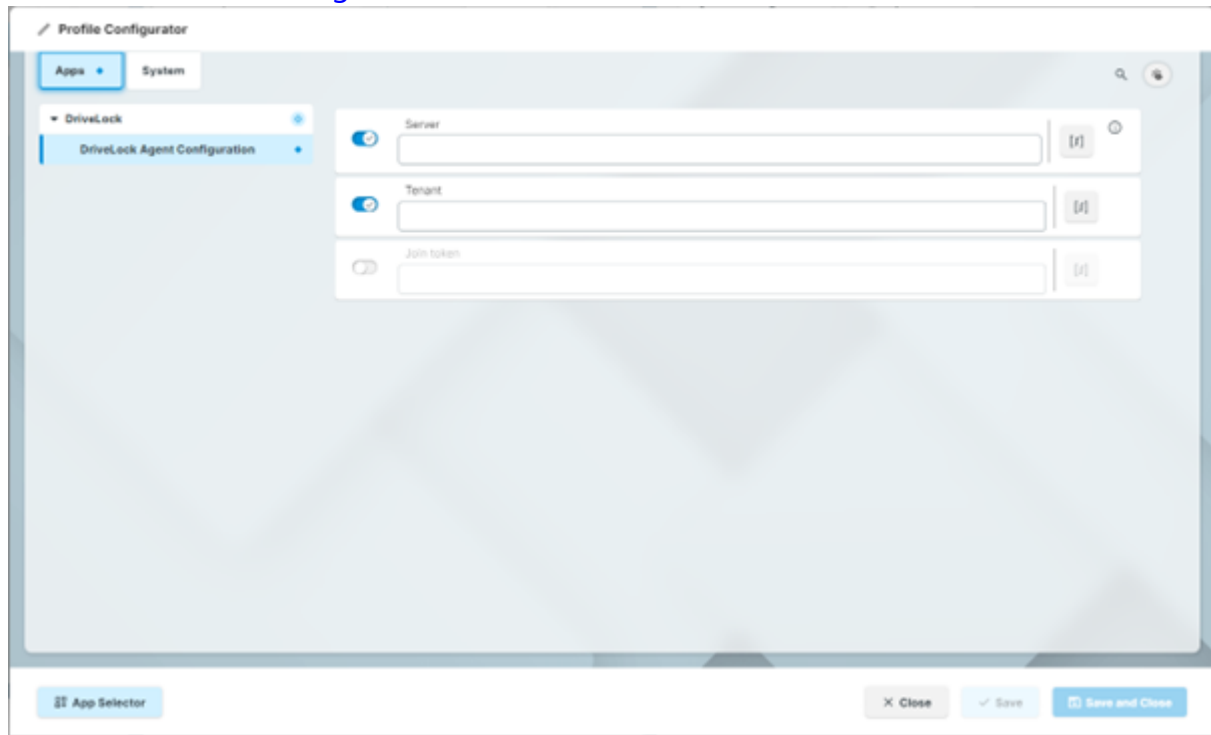
24.2.3.2 Installing the DriveLock IGEL App locally

It is also possible to install the DriveLock App locally direct from the Igel App Portal without an UMS environment. This requires local installations of apps to be allowed on the client.

Please do the following:

1. Open the App Portal and search for the **DriveLock app** in the **Security** category and select **Install**. See IGEL Knowledge Base article .

2. Configure the app locally by first opening the **IGEL Setup** after installation.

3. Go to the **Apps** menu and select **DriveLock**.

4. Select **DriveLock Agent Configuration** to set the **DES server**, the **tenant** and, if necessary, a **join token**.

5. After making the changes, click **Save** at the bottom of the setup window and the con-

653

figuration will become active for the DriveLock Agent.
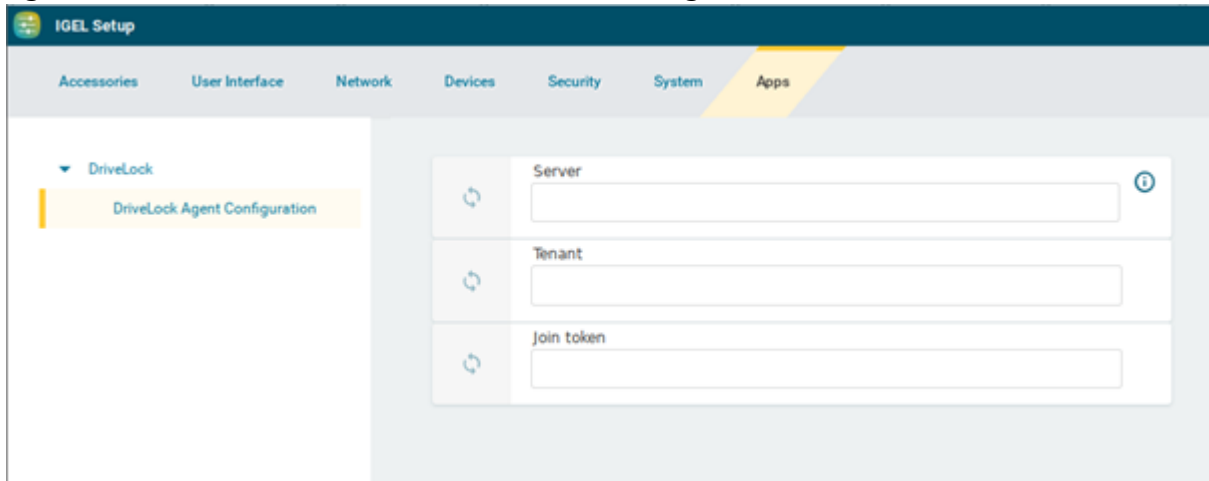
24.2.4 Installation for IGEL versions older than version 12

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

1. Copy and extract the **tar -xzf drivelock.tgz** file on your Linux clients. It is included on the DriveLock ISO image.

2. The tar file contains the **drivelockd-install.sh** installation script.
   Run this script with the parameter `-c` (see figure).

See Installation parameters for more information.

3. Enter the following:
   - Installation path: The default is the current working directory, but you can also specify a different path (in the figure `/home/test/igel_custom_par-tition`).

   - DES and port: Enter the server URL in the format '`https://<Server->:<Port>`' here.

   - Tenant: The default is `root`, but you can also specify a different tenant.

   - Path and name for the user-defined IGEL OS partition files. By default, these files are created in the current working directory.

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

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

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

5. Next, configure the UMS server.

24.2.4.1 Configuring the UMS server

Please do the following:

1. Upload the **drivelock.inf** and **drivelock.tar.bz2** files to the UMS server.

2. Open the UMS Console.

3. In the UMS Console, navigate to **Files** -> **New File** -> **Upload local file to UMS server**.

4. Set **Root** as **Owner** (see figure).

5. Repeat the same for the **drivelock.tar.bz2** file.

6. In the UMS system, create a new profile, e.g. drivelock.

7. In the UMS Console, navigate to **Profiles** -> **New Profiles** -> **Profile Name**.

8. Edit the created profile and activate the Custom Partition as follows (see figure):

   1. Navigate to **System** -> **Firmware Customization** -> **Custom Partition** -> **Partition**

   2. Unlock **Enable Partition**

   3. Check **Enable Partition**

   4. Set size of the partition to 150 or 200 MB

5. Keep /custom as **Mount Point**.
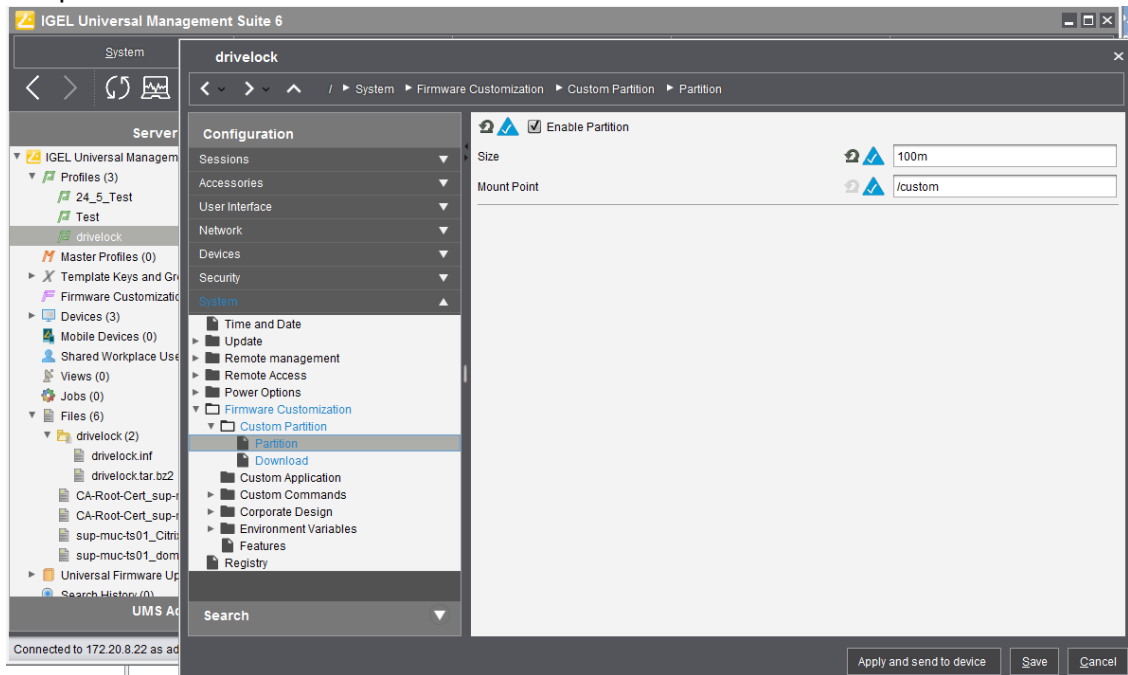
9. Specify the download source.

   1. Navigate to **System** -> **Firmware Customization** -> **Custom Partition** -> **Download**

   2. Click [**+**] to add a **Partition Download Source**.

   3. Add the download URL **http(s)://<server>:8443/ums_file-transfer/drivelock.inf**

   4. Enter the **user name** and **password** to download the file. To confirm the user has access, test in browser.
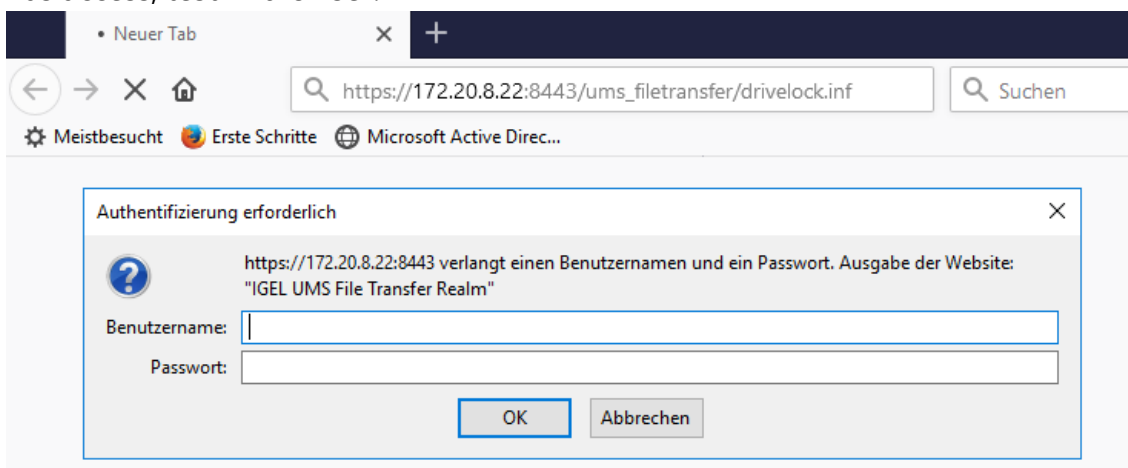
10. In the next step, enter the following (see figure):

    Set **Initializing Action** to /custom/drivelock/drivelock-ctl start.

    Set **Finalizing Action** to /custom/drivelock/drivelock-ctl stop.
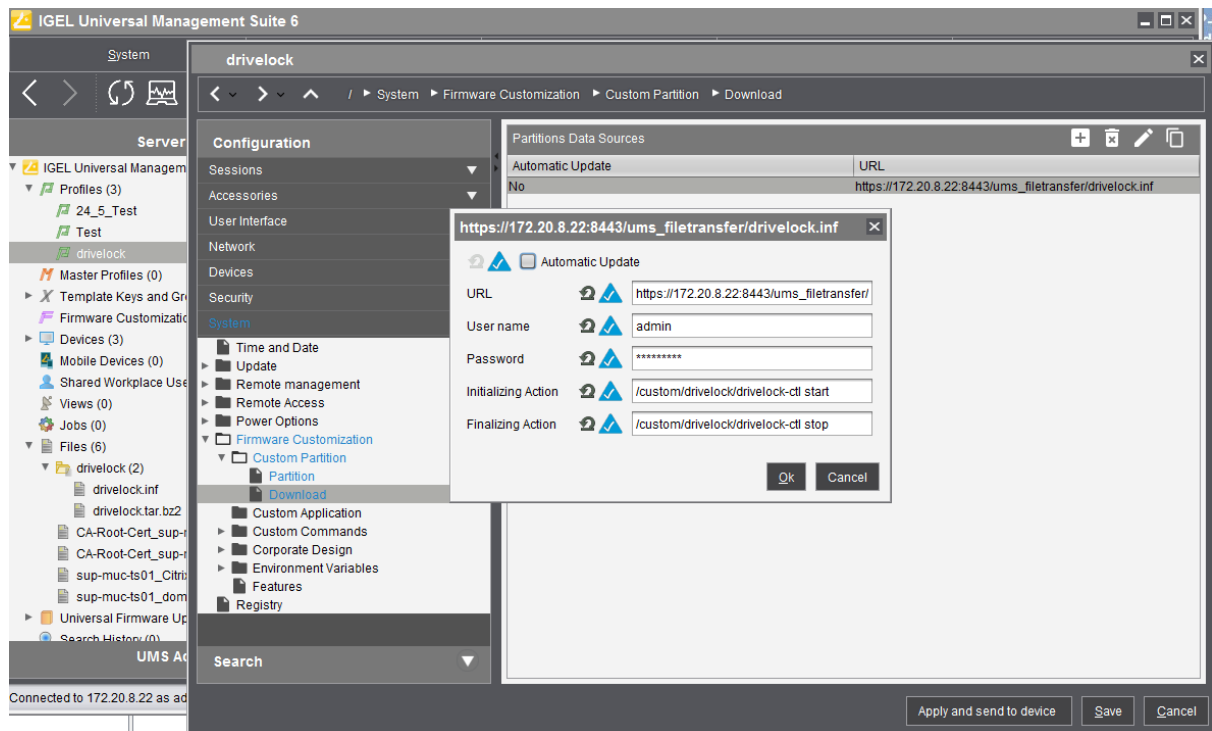
> **Note:** Please note that the Mount Point matches the mount point configured in step 8.

11. Disable **USB access control** on Thin Clients.

    Navigate to **Devices** -> **USB access control** -> uncheck **Enable**.
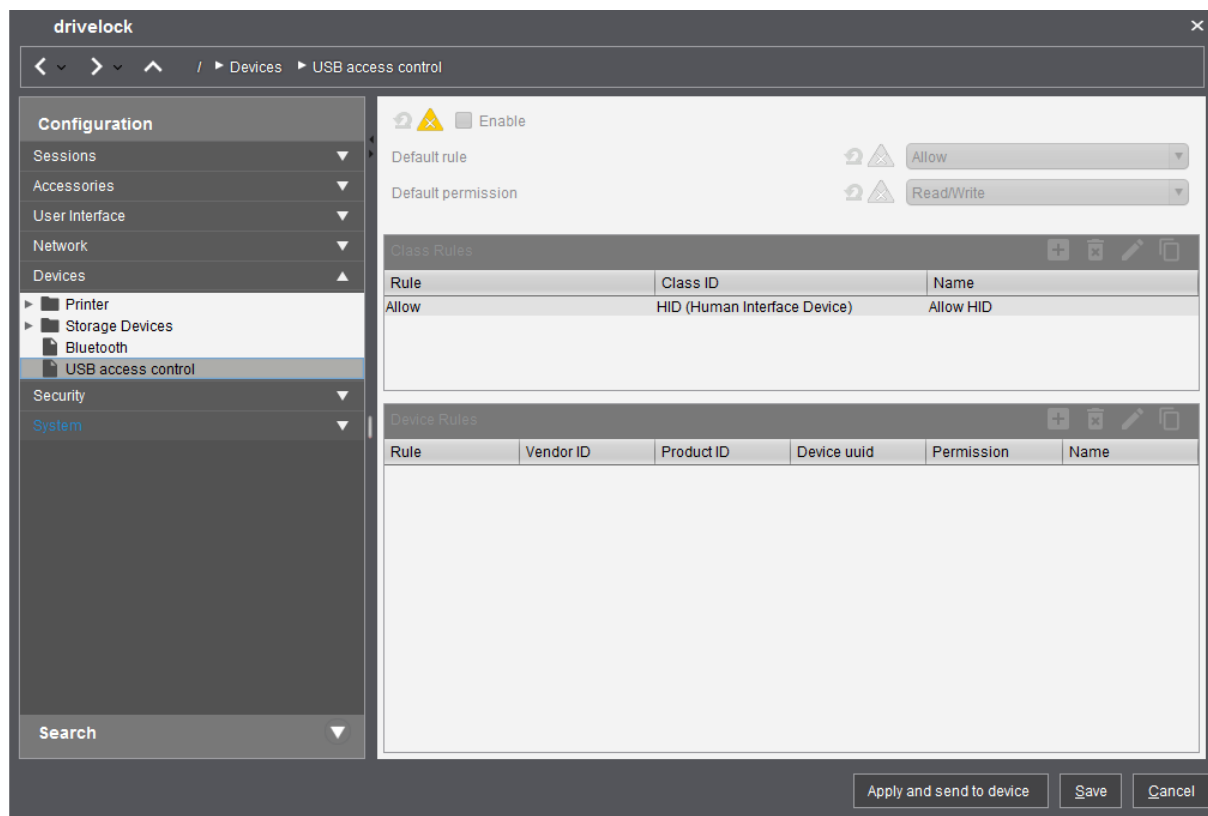
12. Assign the DriveLock profile to the Thin Clients.

    1. Navigate to **Devices** -> **Client**. Drag and drop the DriveLock profile icon to the Thin Client.

    2. As per requirement, select **Now** or **By next reboot** to activate the changes.

24.3 Configuration settings

24.3.1 Recommended procedure

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

1. Start by creating a DriveLock group (static or dynamic) that includes your Linux agents.
   This makes it easier to assign the policy you configure for your Linux agents later.
   Select the filter criteria **OS type Linux** as group definition.
   The figure below shows the dynamic **Linux** group with description **All Linux clients** and filter criterion **OS type = Linux**.
   Further information on DriveLock groups can be found here.

2. To use a different tenant for your DriveLock Linux agents, select another one.

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

4. Depending on whether you want to control the use of devices, drives or applications, set the appropriate settings.

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

24.3.2 Policy settings for DriveLock Linux Agents

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

- **Global configuration**: Settings, Server connections, Trusted certificates

- **EDR**: Events (General Agent events, Device and Drive events), Event filter definitions

- **Drives**: Removable drive locking, Drive whitelist rules

- **Devices**: Device class locking, Device whitelist rules, Device collections

- **Applications**: scanning and blocking mode setting, local whitelist learning settings, special rule, file properties and application hash rule

⚠ Warning: Please note that the settings for drives and devices for DriveLock Linux agents are limited to controlling the USB interface.

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

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

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

- You want to block the usage of USB drives, e.g. USB flash drives, but want to allow specific USB flash drives: create a drive rule where you specify the allowed USB flash drives (whitelist mode).

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

24.3.2.1 Global configuration

1. Open the **Settings** section to configure the following:
   - **License**: Add the licenses you have purchased for your Linux agents.

   - **Remote control settings and permissions**: On the **Permissions** tab you can add the users that are allowed to take action on the Linux agent, such as changing the configuration.

   - **Event message transfer settings**: Make sure to check the **Enable event forwarding to the DriveLock Enterprise Service** option on the **Server** tab. The second option, **Report agent status to server**, allows you to specify the intervals for sending agent alive messages to the DES.

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

   - Settings for logging: **Logging level**, **Maximum log file size in MB** and **Time until automatic deletion of old log files**.

2. In the **Server connections** section you can add a new server, if required.

3. In the **Trusted certificates** section you select the certificates for the secure communication between the DriveLock Management Console and/or the DriveLock Linux Agents and the DES.

24.3.2.2 Events and alerts

The Risk & Compliance feature offers an optimized display of individual events combined with various filter options.

For DriveLock Linux agents, the following event categories are important: **Application control**, **General agent events** and **Device** and **Drive** events. See Events for a detailed list.

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

The following settings are currently available for Linux agents.

24.3.2.2.1 Event settings

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

1. In the **Events and Alerts** node, open the **Events** sub-node. Doubleclick the event in the **Drive events** section. Currently only the settings on the **General** tab are available for Linux agents (see figure).

2. The System Event Log (**Windows Event Log**) option is the default, but you can also select **DriveLock Enterprise Service** to save the events in the event log on the DES.

3. If required, you can also check the **Suppress duplicate events** option.

24.3.2.2.2 Event filter definitions

On Linux agents it is possible to apply event filter definitions to the events available for Linux.

You can filter

- by filter criteria,

- by computers (with computer names or Drivelock groups)

- and by times.

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

24.3.2.2.2.1 Create event filter definitions

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

Please do the following:

1. Right-click the **Event filter definitions** subnode in the **EDR** node and select **New...** from the menu. A list of available events is displayed. Select the event 238.

2. On the **General** tab, check the **Windows Event Log** and **DriveLock Enterprise Service** options.
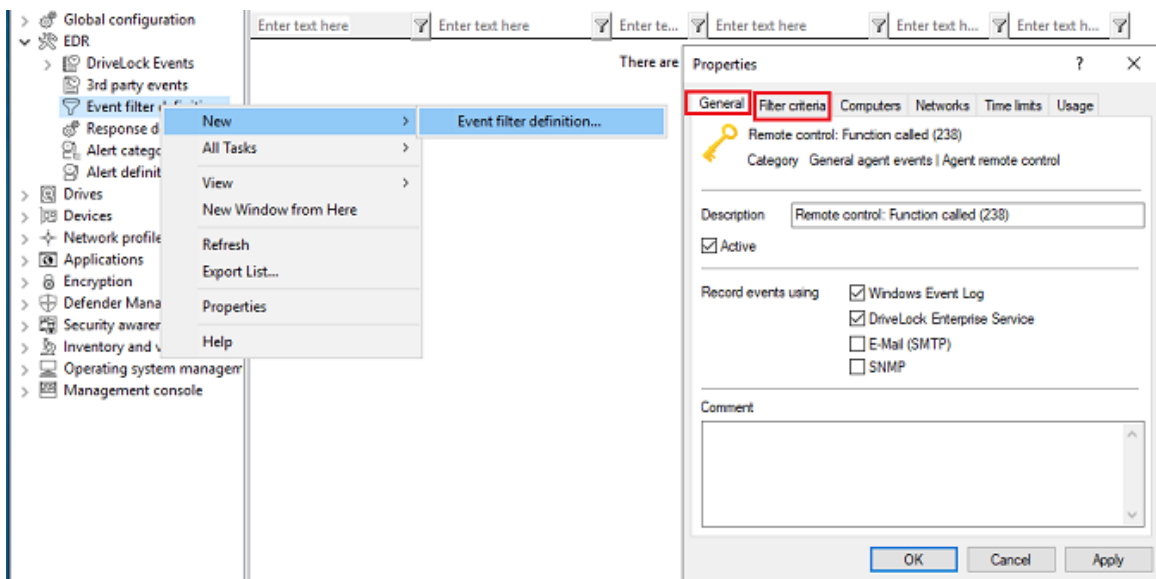
3. On the **Filter criteria** tab, select the parameters to filter by. By clicking the **Add** button you can select the appropriate criteria and the operators.
   In the example above, one criterion would be the **function name** GetAgentStatus.
   Then the DriveLock Agent will send only the relevant events.
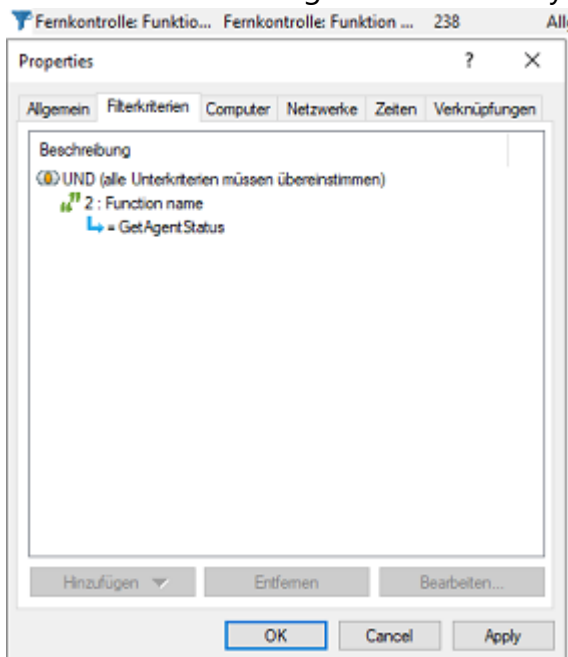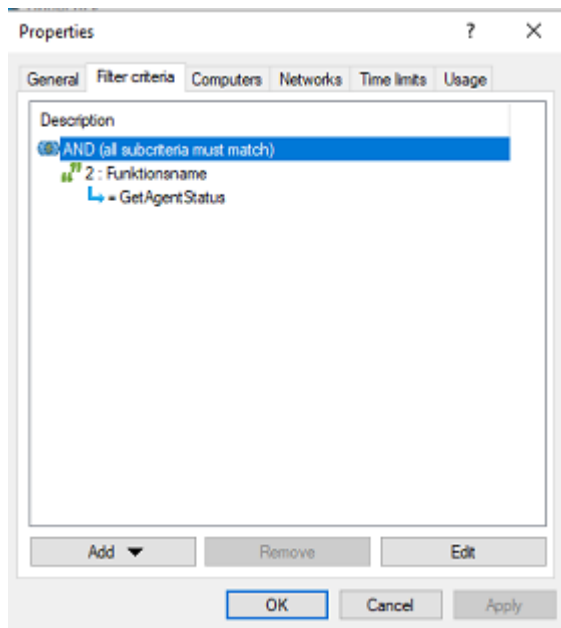
24.3.2.3 Drives

24.3.2.3.1 Drive settings

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

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

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

1. Select the default option **Deny (lock) for all users (default)**:
   This setting blocks the use of all drives connected via the USB interface for all users. You will need to define a whitelist rule that allows specific drives to be used.

2. Select **Allow** (for all users):
   This option allows users to connect all drives over the USB interface. You will need to specify the drives you want to block in your drive rule.

24.3.2.3.2 Drive whitelist rules

As of version 2024.2, drive rules based on vendor or product ID can also be used on Linux agents.

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

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

2. Enter the corresponding IDs on the **General** tab. You can also select a drive by searching for it using the **...** button.
   For a drive rule, enter a **vendor ID**, the name of the drive vendor and a **product ID** (this is the unique ID assigned to the product by the vendor).
   The hardware ID of the drive is required for a **hardware ID rule** . This ID consists of the vendor ID (VID), the product ID (PID) and the revision number (REV).

   > Note: You can use wildcards for both options: * for several characters, ? for exactly one character.

3. On the **Permissions** tab, specify whether to deny (lock) or allow the drive (depending on your removable drive settings).

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

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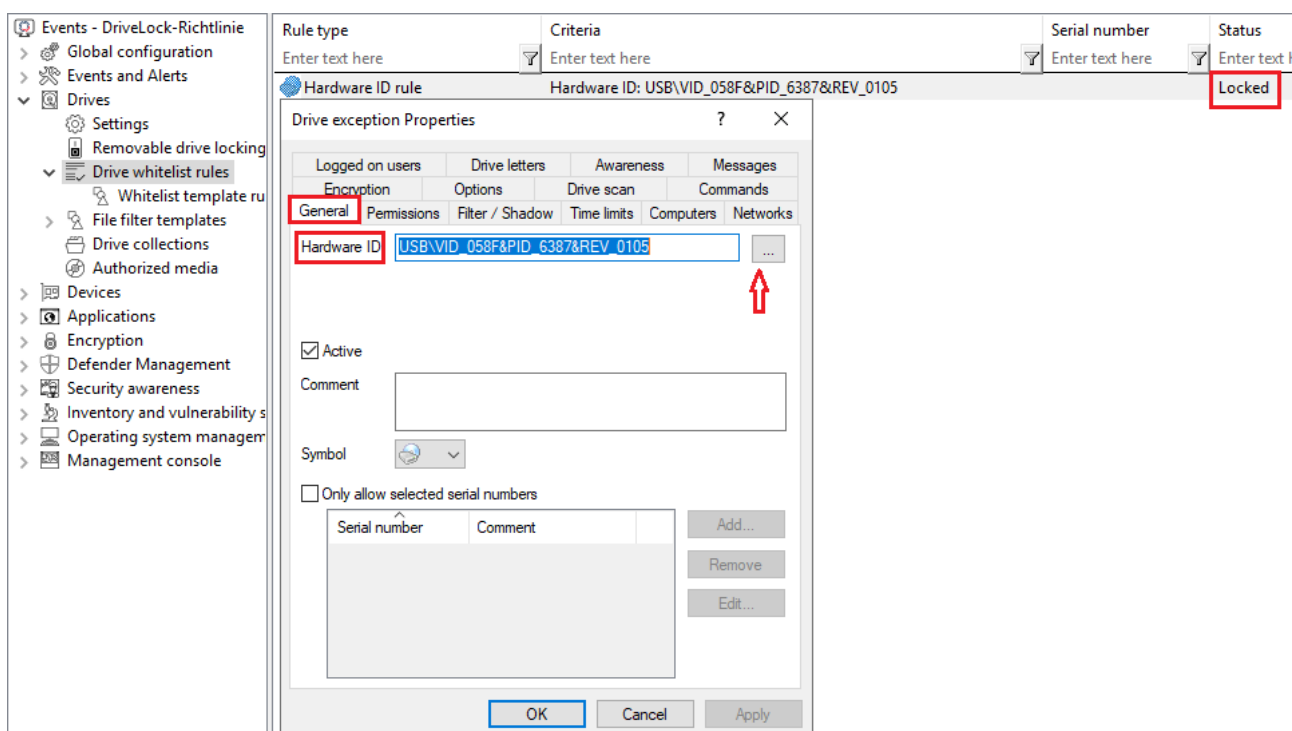
24.3.2.4 Devices

24.3.2.4.1 Supported device classes for Linux agents

The following DriveLock device classes are currently supported for Linux:

- **Devices:**
  - Debugging and software protection devices (WinUSB, ADB) -> corresponds to Linux "Diagnostic Device class" (DC)

  - Printers -> corresponds to Linux "Printers class" (07)

  - Human Interface Devices (HID) -> corresponds to Linux "Human Interface Devices class" (03)

  - Modems, network adapters -> corresponds to Linux "Communications & CDC control class" (02)

  - Scanners and cameras -> corresponds to Linux "Image class" (06)

  - Smartcard readers -> corresponds to Linux "Smart Card class" (0B)

  - Sound, video and game controllers -> corresponds to Linux "Audio/Video/Audio&Video classes" (01|0e|10)

  - Unknown Linux device (new device class from version 24.2 for devices that were found by Linux Agents and for which no classification is possible)

- **Controllers and Ports:**
  - Bluetooth adapters -> corresponds to Linux "Wireless Controller Class" (e0)

  - USB controllers -> corresponds to Linux "Hub class" (09)

- ## USB classes:

USB classes	USB class description	Windows class	Windows class name
"00"	Composite devices	"{36FC9E60-C465-11CF-8056-444553540000}"	USB Host controllers
"01"	Audio	"{4D36E96C-E325-11CE-BFC1-08002BE10318}"	Sound video and game controllers (Multimedia)
"02"	Communications & CDC control	"{4D36E978-E325-11CE-BFC1-08002BE10318}"	Ports
"0202"	Communications & CDC control	"{4D36E96D-E325-11CE-BFC1-08002BE10318}"	Modems
"020d"	Communications & CDC control	"{4D36E972-E325-11CE-BFC1-08002bE10318}"	Network
"020e"	Communications & CDC control	"{4D36E972-E325-11CE-BFC1-08002bE10318}"	Network
"03"	Human Interface Devices	"{745A17A0-74D3-11D0-B6FE-00A0C90F57DA}"	Human Interface Devices
"05"	Physical	no match	
"06"	Image	"{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}"	Imaging devices
"060101"	Image / PTP	"{EEC5AD98-8080-425f-922A-DABF3DE3F69A}"	Portable Devices (Media player)
"07"	Printer	"{4D36E979-E325-11CE-BFC1-08002BE10318}"	Printers
"08"	Mass Storage	"{4D36E97B-E325-11CE-BFC1-08002BE10318}"	SCSI and RAID controllers
"09"	Hub	"{36FC9E60-C465-11CF-8056-444553540000}"	USB Host controllers
"0a"	CDC Data	no match	
"0b"	Smart Card	"{50DD5230-BA8A-11D1-BF5D-0000F805F530}"	Smart card readers
"0d"	Content Security	no match	
"0e"	Video	"{ca3e7ab9-b4c3-4ae6-8251-579ef933890f}"	Imaging devices (camera)
"0f"	Personal Healthcare	no match	
"10"	Audio / Video	"{4D36E96C-E325-11CE-BFC1-08002BE10318}"	Sound video and game controllers
"11"	Billboard	no match	
"12"	USB-Type-C Bridge	no match	

USB classes	USB class description	Windows class	Windows class name
"13"	USB Bulk Display Protocol	no match	
"14"	MCTP over USB Protocol	no match	
"3c"	I3C	no match	
"58"	XBox	"{4D36E96C-E325-11CE-BFC1-08002BE10318}"	Sound video and game controllers
"dc"	Diagnostic Device	no match	
"e0"	Wireless Controller	no match	
"e00101"	Wireless / Bluetooth	"{E0CBF06C-CD8B-4647-BB8A-263B43F0F974}"	Bluetooth radios (Microsoft)
"e00103"	Wireless / RNDIS	"{4D36E972-E325-11CE-BFC1-08002bE10318}"	Network
"e00104"	Wireless / Bluetooth AMP Ctrl	"{E0CBF06C-CD8B-4647-BB8A-263B43F0F974}"	Bluetooth radios (Microsoft)
"ef"	Miscellaneous	no match	
"ef0201"	Miscellaneous /Interf. association	"{36FC9E60-C465-11CF-8056-444553540000}"	USB Host controllers
"ef0401"	Miscellaneous / Net	"{4D36E972-E325-11CE-BFC1-08002bE10318}"	Network
"fe"	Application Specific	no match	
"ff"	Vendor Specific	no match	

24.3.2.4.2 Device settings

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

This section provides two choices for your Linux policy:

1. Open the **Controllers and Ports** section and doubleclick **USB controllers**. This setting lets you block or allow the complete USB interface of the Linux Agent.
   The following options are available:

a. Leave the setting as it is.

You do not check the **Enable controlling devices of this device class** option. This is the default setting: **Not configured (not locked)**.

b. Lock the USB interface.

Check the **Enable controlling devices of this device class** option and then select **Block device**. This means that you will need to configure appropriate whitelist rules for the devices you want to allow.

c. Allow the USB interface.

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

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

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

> Note: Please note that only some of the device classes available for Windows policies have a counterpart on the Linux side.

Input devices (HID) are selected in the figure.
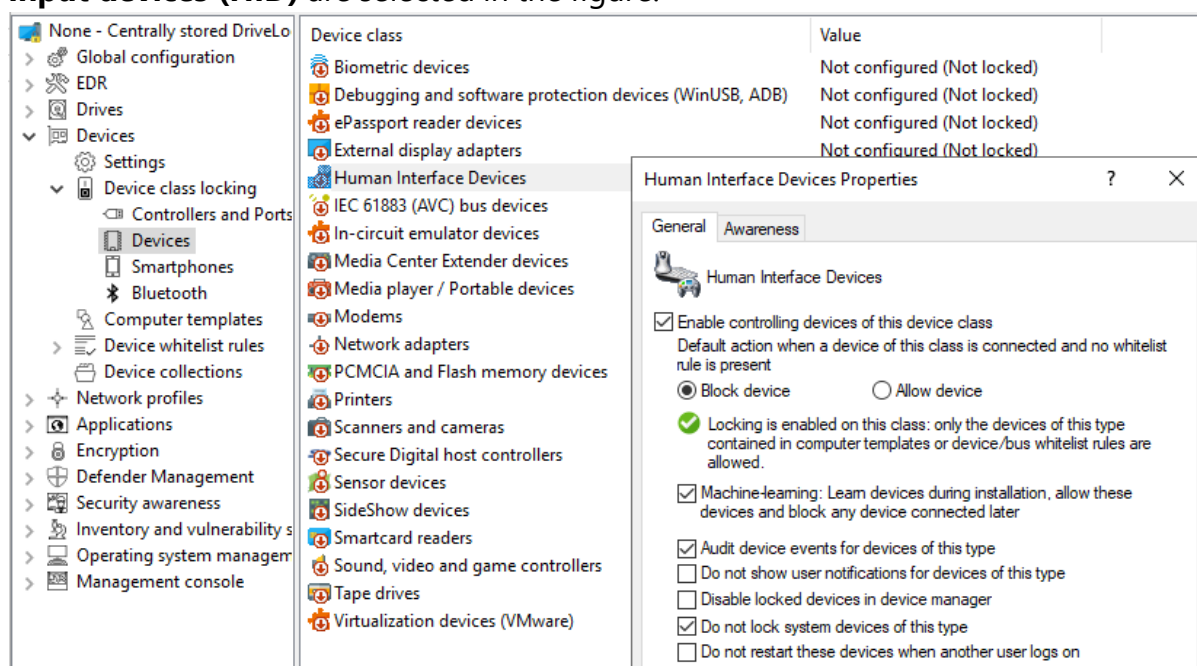
The same dialog is displayed as described above:

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

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

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

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

24.3.2.4.3 Android and Apple devices

Creating rules for Android and Apple devices is also supported, see the figure. Similar to other device categories, you need the hardware ID or serial number of the device to do so. On the **Permissions** tab, you can set the appropriate blocking settings.
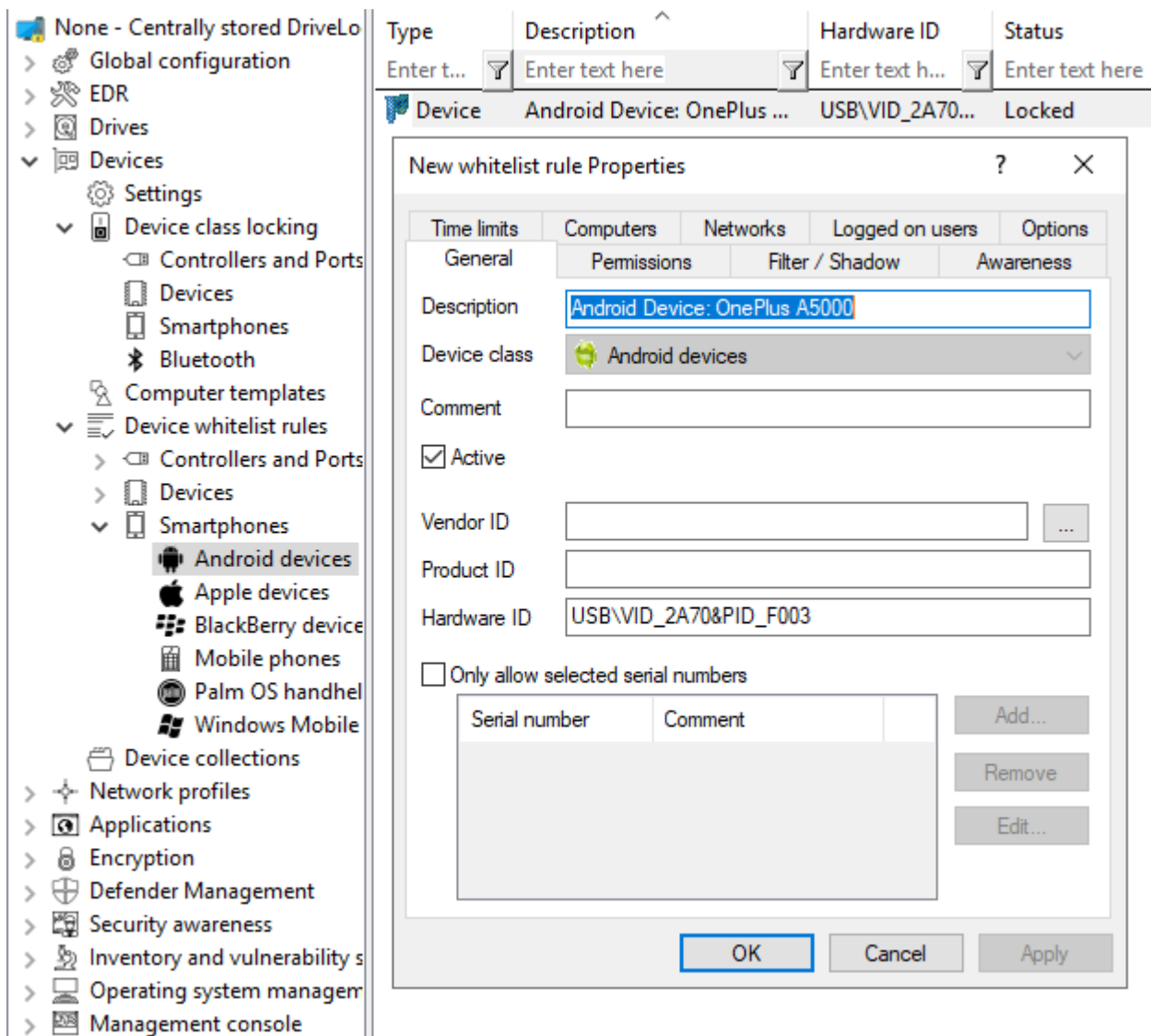
The agent identifies a device as an Android or Apple device if it appears in the list of devices that is installed with the Drivelock Agent. The list contains the product and vendor IDs (or serial numbers); when connecting the respective device, the IDs are compared.

This list is located in the system in the /etc/udev/rules.d/ directory in the **51-drivelock-apple.rules** and **51-drivelock-android.rules** files.

> Note: The list can be extended. If you need assistance with this, please contact our support.

24.3.2.4.4 Device whitelist rules (for devices)

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

All other steps are identical.

In the figure below, the USB device with the hardware ID **USB\VID_0E0F&PID_0003&REV_0102&MI_00** has the status **Not locked**.
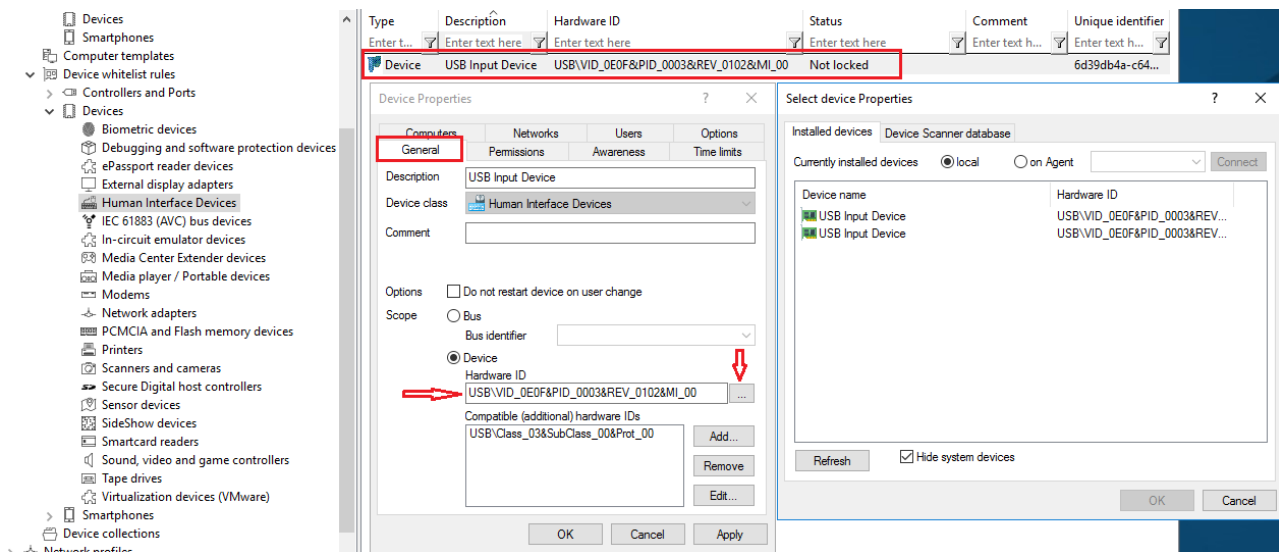
24.3.2.4.5 Device whitelist rules (for USB controllers)

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

1. In the **Devices** node, open the **Device whitelist rules** subnode; select **Controllers and Ports** and then **USB controllers** (see figure).

2. Open the context menu, select **New** and then **Device or bus...**.
   None of the other options are relevant for Linux agents.

3. On the **General** tab, select the **Device** radio button and find the device you want to lock or allow (depending on whitelist or blacklist mode).

4. In the **Select devices** dialog you can display the devices that are installed **locally** or the devices that are currently connected to the DriveLock Linux Agent (**on Agent**). Note that the DriveLock Linux Agent must be online if you choose the 'on Agent' option.

5. On the **Permissions** tab, specify the appropriate **Device locking behavior**.

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

671

In the figure below, the USB controller with the ID **USB\VID_15AD&PID_0770&REV_00** is permitted and has the status **Enabled**.
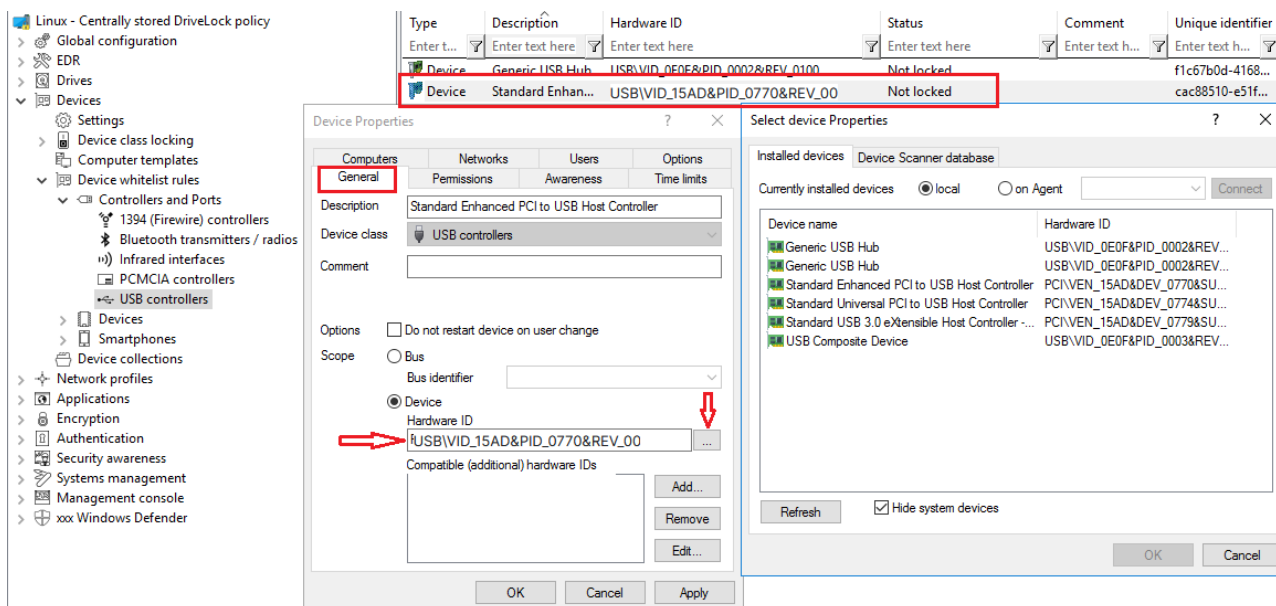
24.3.2.4.6 Device collections

You can use device collections on Linux agents. They simplify managing devices of the same type when the same settings apply to them, while reducing the number of whitelist rules needed. Device collections may contain several similar devices and can be used in whitelist rules.

Note that only some device classes are supported on Linux agents. By specifying the corresponding hardware ID, the class could be ignored during comparison.

Here you will find information on how to create device collections.

24.3.2.5 Applications

DriveLock includes some application control options for Linux agents.

> ⚠ Warning: Please note that Application Control is currently not available for IGEL clients.

1. The following settings can be used for Linux agents:
   - Use Scanning and blocking mode to activate the Application Control functionality
   - Set **Hash algorithm for hash-based rules** to specify the hash algorithm used in all rules

- Use Start learning the local whitelist automatically to automatically create a local hash database

- By using Local whitelist and predictive whitelisting, you can use the hash database as a whitelist

- With Directories learned for local whitelist (Linux) you specify the directories that may be used for the learning process.

2. Three application rules can be used for Linux:

   - File properties rule

   - Special rule

   - Hash database rule

> ⊘ Warning: To be able to use Application Control for Linux, specific requirements regarding the Linux kernel must be met.

> ☑ Note: General information on application control and application rules can be found here.

24.3.2.5.1 Prerequisites for Application Control on Linux Agents

To support the full functionality of Application Control with whitelisting, the following requirements must be met:

- The fanotify API must be active in the Linux kernel

- The Linux kernel must be greater than 5.0.
  In kernel versions smaller than 5.0, only the fanotify flag FAN_OPEN_PERM is available and only blacklisting is possible.

- The file system must support fanotify events.
  Current list of supported file systems:
    - bfs

    - btrfs

    - cifs

    - ecryptfs

    - ext2

    - ext3

- ext4

- fuseblk

- fuse.vmhgfs-fuse

- iso9660

- jfs

- minix

- msdos

- nfs

- nfs4

- nssvol

- ncpfs

- overlay

- overlayfs

- ramfs

- reiserfs

- smbfs

- squashfs

- tmpfs

- udf

- vfat

- xfs

- zfs

⚠ Warning: Running Application Control on Linux systems alongside other fanotify-based security solutions is not supported. This can have unforeseen consequences, such as the failure of the operating system.

📝 Note: Due to the limitations of fanotify, it is not possible to use Application Control inside containers.

24.3.2.5.2 Scanning and blocking mode

Use this setting to select the mode DriveLock uses to scan applications on the Linux agent and/or to initiate appropriate actions.

Please do the following:

Select **Set to fixed value**, and then select one of the following options from the list:

- **Audit only**: events are generated only; you can analyze them later
- **Whitelist**: applications may only be executed if a corresponding whitelist rule exists. All other applications will be blocked.
- **Blacklist**: applications are blocked only if there is a corresponding blacklist rule. All other applications are allowed.
- **including DLLs**: this addition also checks the shared libraries
- **(simulate)**: this addition means that the effects of your rules are tested in advance and corresponding events are generated.

24.3.2.5.3 Local whitelist and predictive whitelisting

If this setting and the Automatically start learning local whitelist setting are enabled, the Linux agent scans the file systems and automatically creates a local hash file at startup if it does not already exist, and uses it as a local whitelist to allow files to be executed if the corresponding file hash is included in the list.
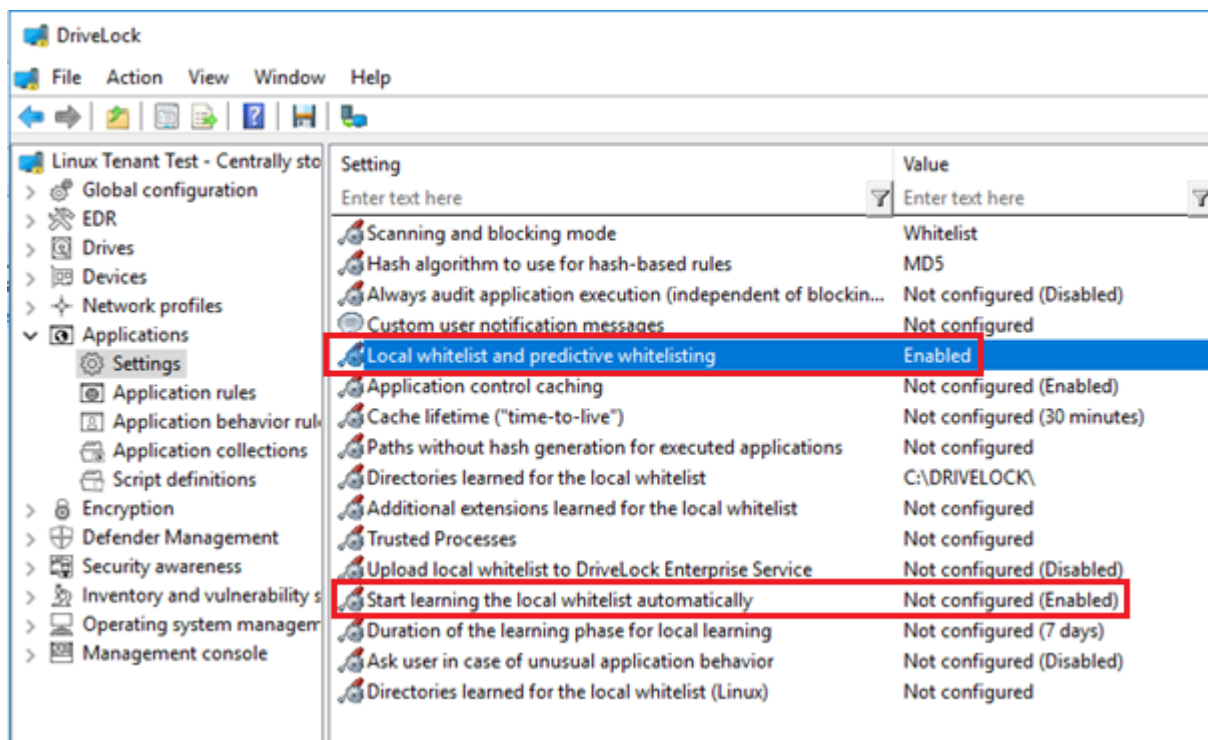
The scan processes all ELF binaries and scripts starting with #! start, in all or in the specified directories configured with the setting Directories learned for local whitelist (Linux).

Limitation:

The Linux agent is not notified of system or software updates, so if updates are made during or after the local whitelist scan, these new hashes are not included in the hash database and cannot be executed unless a new hash scan is started. If the local whitelist is used to whitelist important files of the operating system, it is recommended to disable automatic updates.

24.3.2.5.4 Start learning the local whitelist automatically

Use this setting to define whether local whitelist learning is started automatically (i.e. as soon as the corresponding policy is assigned to the DriveLock Agent) or by users.

The default option is **Enabled**.

24.3.2.5.5 Directories learned for the local whitelist (Linux)

If you want to limit learning to specific directories, you can specify them in the dialog under **Set to fixed list**.

The default list of directories to learn is:

/bin,

/sbin,

/lib64,

/lib,

/etc,

/usr,

/snap/* for Ubuntu,

/.snapshots for Suse.

24.3.2.5.6 File properties rule

This rule allows you to specify different file properties to filter by. This rule can be created as a whitelist or blacklist rule.

Please do the following:

In the **Applications** node, under **Application Rules for Linux Agents**, open the **File properties rule....** context menu item.

1. On the **General** tab, the first thing you do is set the rule type. Then you have the following choices:
   - **Path**: Specify a path in Linux format (e.g. /home/test/) if you want to allow (or block) applications from a specific path. Wildcards are allowed.
   - **Hash**: This option verifies that the hash value of the file contents matches the specified value. The system stores this value when creating the rule and compares it with the currently calculated value at runtime. If both match, the rule is activated. Use this option, for example, for a single application that you want to allow or block via whitelist or blacklist.
   - **Owner**: Use this option to restrict the starting of an application to a specific file owner. For example, you can use this setting to allow all programs installed by an administrator or by a trusted installer account, while blocking all applications that were installed by other users. This also allows for automatically blocking all applications that can be run without prior installation.

   A combination of the options is possible.

2. On the **Permissions** tab, you can specify specific Linux users or groups for which this rule is active. Users or groups can be included or excluded. You can specify not only the names in Linux format, but also numeric IDs.

3. On the **Time limits** tab you can specify the times when the rule should be active.

4. On the **Computers** tab you can specify the computers where the rule will be active.

24.3.2.5.7 Special rule

The special rule can be used only as a whitelist rule.

Please do the following:

1. In the **Applications** node, under **Application Rules for Linux Agents**, open the **Special Rule** context menu item....

2. On the **General** tab you have three options to choose from:
   - **Program file is part of the operating system**:
     This option automatically allows operating system programs from the following system directories:
       - /bin, /sbin, /lib, /lib64, /usr, /etc
       - Ubuntu: /snap
       - Suse: /.snapshots

   - **Program file is part of DriveLock**
     Here binaries are allowed in the Drivelock installation folder and the "bin" folder below it.
     The custom installer drivelockd-install.sh is not included, the user must add a rule to run the script in case of upgrades.

   - **Any program is started**:
     All started applications are allowed here, regardless of the directory.

3. On the **Time limits** tab you can specify the times when you want the rule to be active.

4. On the **Computers** tab you can specify the computers where the rule will be active.

24.3.2.5.8 Application hash database rule

With this rule it is possible to create a hash database file or add an existing file previously created on the Linux computer. Application hash database rules can be defined as blacklist or whitelist.

Please do the following:

1. In the **Applications** node, under **Application Rules for Linux Agents**, open the **Application hash database rule....** context menu item.

2. First, select the **rule type**.

   > Note: Note that whitelist is supported only if the Linux kernel is greater than 5. For example, only binaries that have a hash in the list are allowed as a whitelist.

3. Then enter a **rule name**.

4. Under **Database file** you can choose to create a new file or select a file that has already been created.

   > Note: The hash database file is a text file with the format `<Hash> <Dateipfad>` for each line. It can be created on the Linux client using one of the supported hash algorithms with the supplied tool **dl-hash**.

24.3.3 Agent remote control

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

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

DriveLock
> DriveLock File Protection
∨ Operating
     Agent remote control
     Network preboot computers
     Shadowed files

Remote computer	Logged-on user
debian10	test
ITC000C299043DD	
TESTUB	
TEST-VIRTUAL-MACHINE	
UBUNTU	
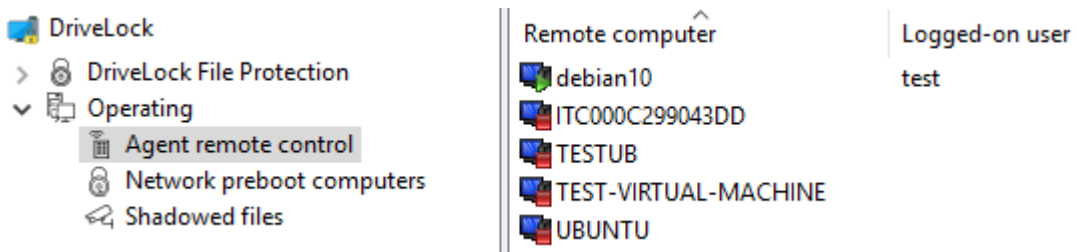
The following agent remote control actions are relevant for Linux agents:
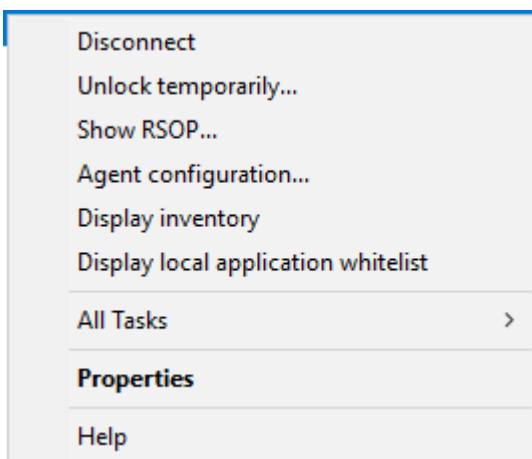
Disconnect
Unlock temporarily...
Show RSOP...
Agent configuration...
Display inventory
Display local application whitelist
All Tasks   >
Properties
Help

1. **Disconnect** the Linux agent.

2. **Unlock temporarily...** : more information here.

3. **Show RSOP...**
   Click this option to view a summary of the policy (Resultant Set of Policy) assigned to the Linux agent. You can not change any settings here.

4. **Agent configuration...**
   Click this option to open a dialog with information on the agent's configuration. It shows you the server your Linux agent receives the centrally stored policy from and, if necessary, you can add another server or enter another tenant on the **Options** tab.

5. **Display inventory**
   Click here to get inventory information on your Linux agent (on the **General**, **Drives**, **Devices**, **Applications** and **Networks** tabs).

DriveLock
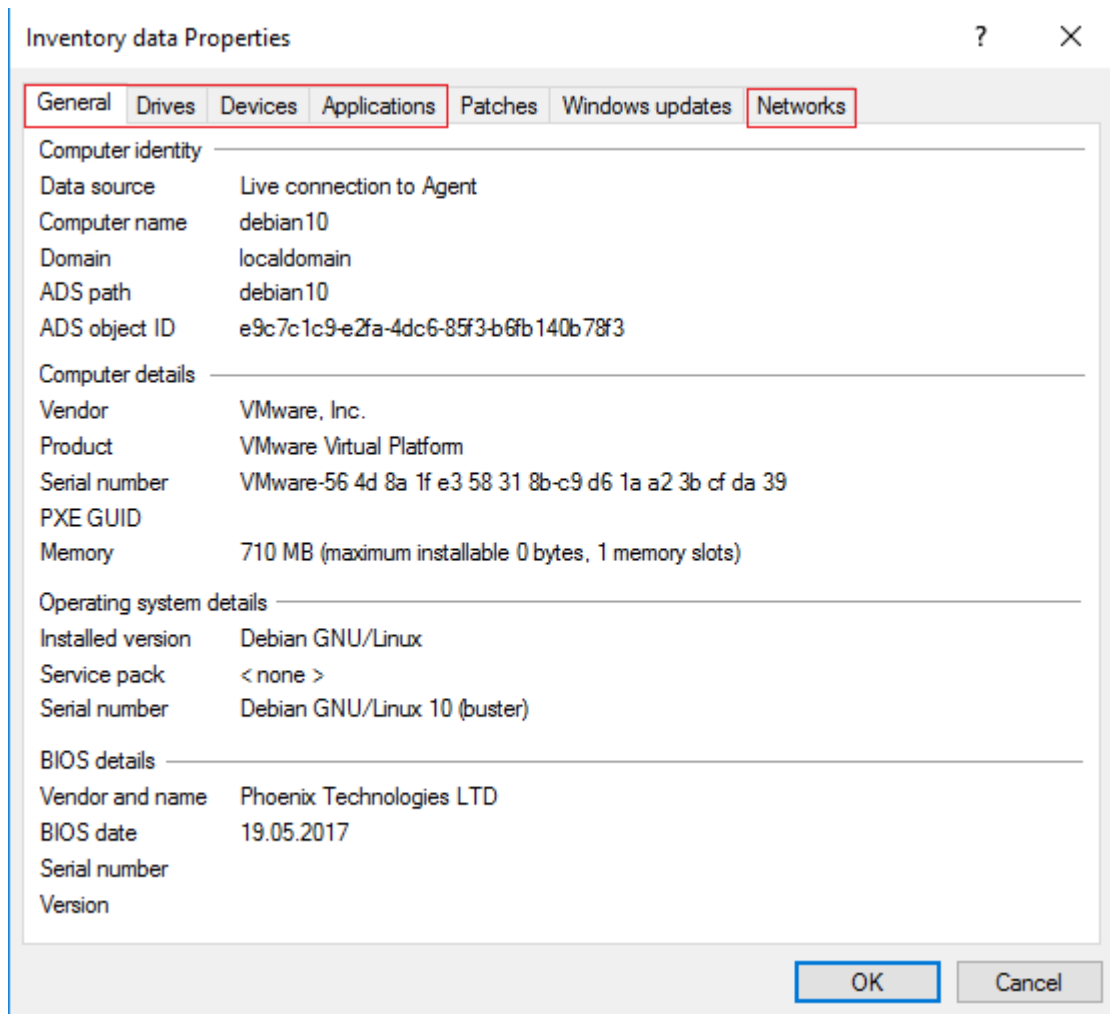
6. **Display local application control whitelist...**: Click here to view the current contents of the application hash database.

24.3.3.1 Application control in the agent properties

It is possible to trigger a rescan of the local whitelist via the agent remote control or via the Drivelock command line utility `drivelock-ctl -rescanapps` (this requires administrator privileges).

Please do the following:

1. Open the agent properties dialog by double-clicking the respective Linux agent.

2. Select the **Application Control** tab.
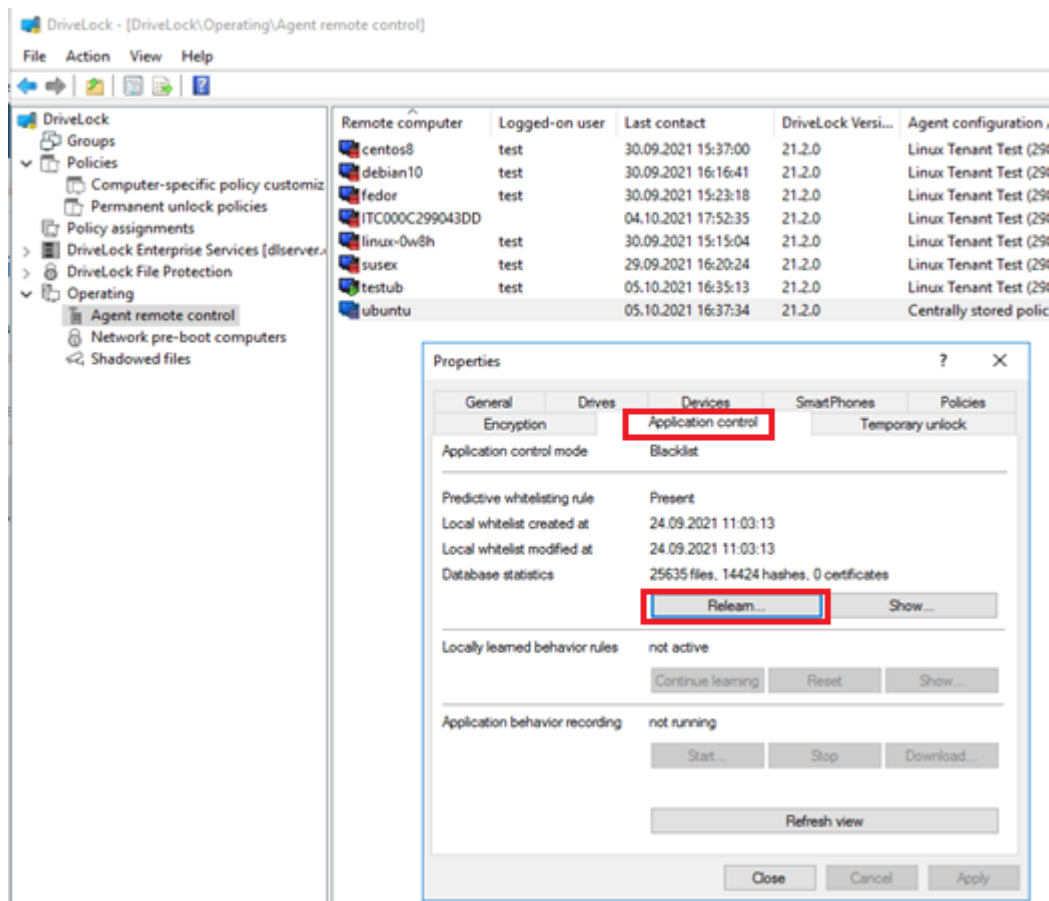
3. Click the **Re-learn**... button to initiate a scan. This may take some time.

4. Click **Show...** to view the current contents of the application hash database.
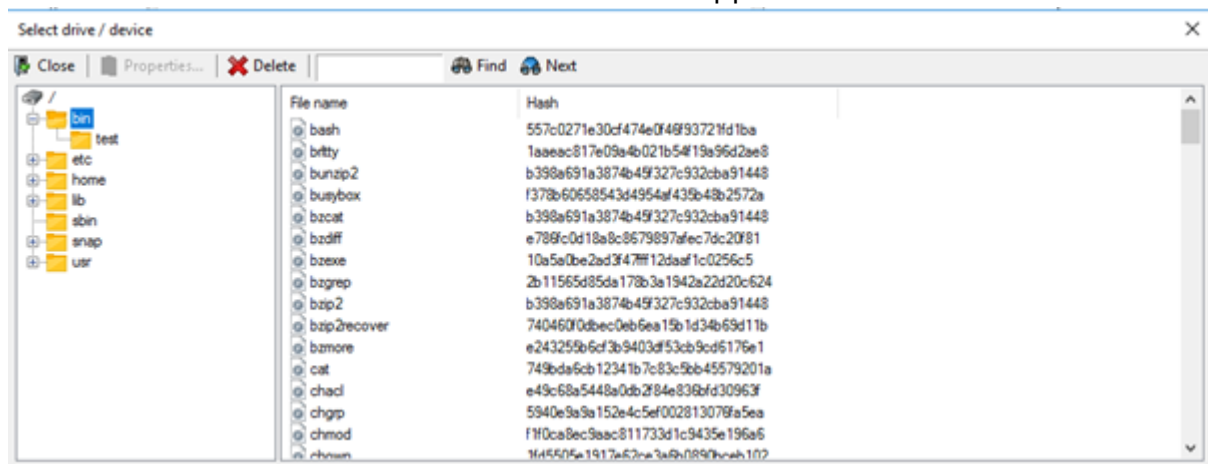
24.3.3.2 Temporary unlock from the DMC

Using temporary unlock, you can quickly and temporarily allow a connected DriveLock Linux agent to access locked drives, devices, or applications via remote agent control in the DriveLock Management Console (DMC).

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

DriveLock

Please do the following:

1. In the context menu of the Linux agent, select the menu command **Unlock temporarily...**.

2. Specify where to apply the unlocking to (drive types or device types or both).
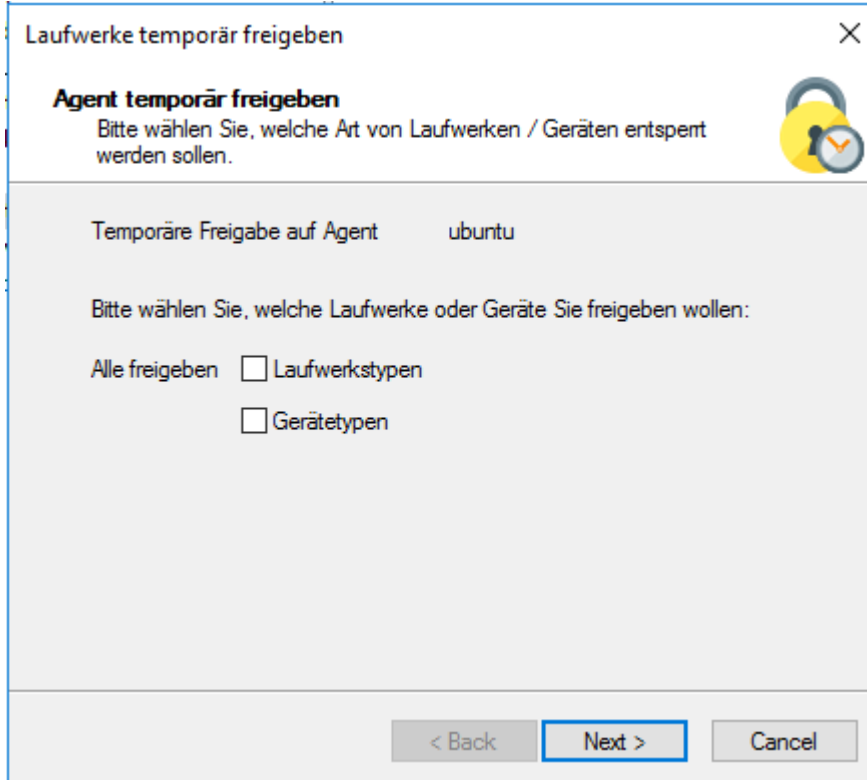
3. If you want to unlock applications, select **Disable application control during sharing** in the dialog.
   To add the applications used during the unlock period to the local hash database, you can also select the corresponding option and also specify exactly which files or applications should be learned.

4. Lastly, define the time period and specify a reason for the unlock.

24.4 Linux agents in the DOC

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

The following DOC views are relevant for Linux agents:

- **Computer**: Filter by **OS Type** (icon), for example, to group your Linux agents by their OS type. Select any Linux agent to check details.

- **Groups**: If you have defined a DriveLock group for your Linux agents, it is displayed here with information about the respective members and the assigned policies.

- **Events**:This view lists the events that a Linux agent sends to the DES.

- **EDR**: The Endpoint Detection & Response view provides continuous monitoring and allows you to configure your response to security alerts.

- **Accounts**:This view provides a list of all user accounts that are allowed to access the DOC. It also shows information on status and roles along with name and logon details.

24.4.1 Display license status in DOC

The Linux Agent supports Drivelock licenses for the following components, as configured via policy: Application Control and Device Control (drive and device control).

The agent activates the components according to the license and reports the correct license status to DriveLock Enterprise Service (DES). You can check this in the details of the computer in DOC (see figure).
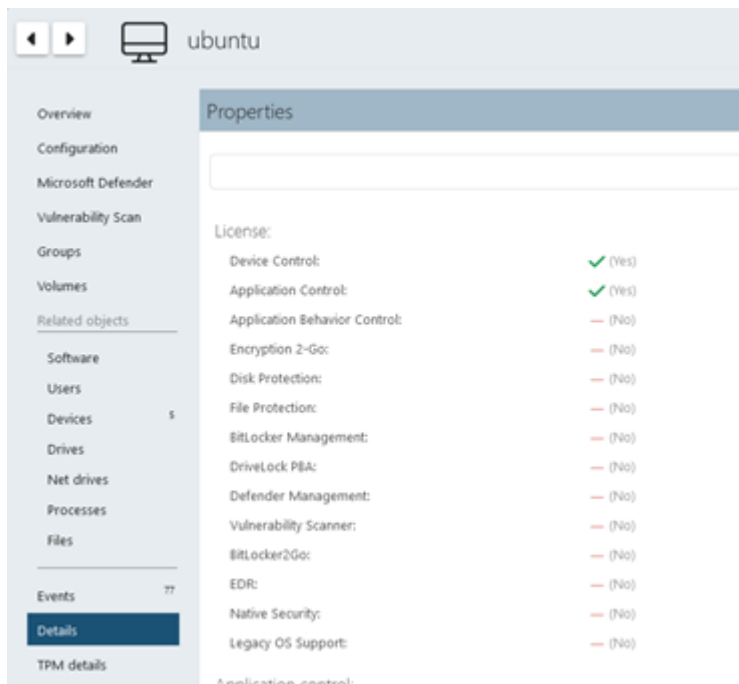
Using the command line tool "drivelock-ctl -showstatus" it is possible to check the current license status on the client.

24.4.2 Temporary unlock from the DOC

It is possible to temporarily unlock the application or drive accounts on the Linux agents from DriveLock Operations Center (DOC) using the **Unlock computer online** action.
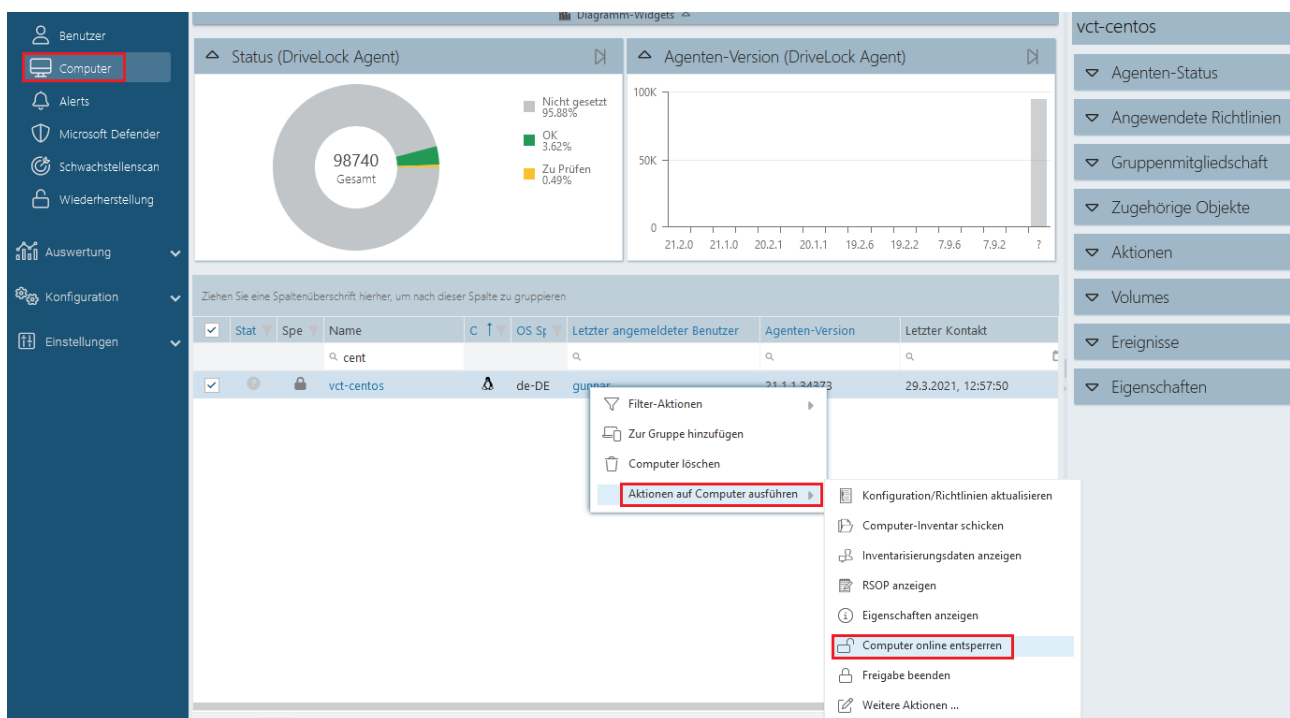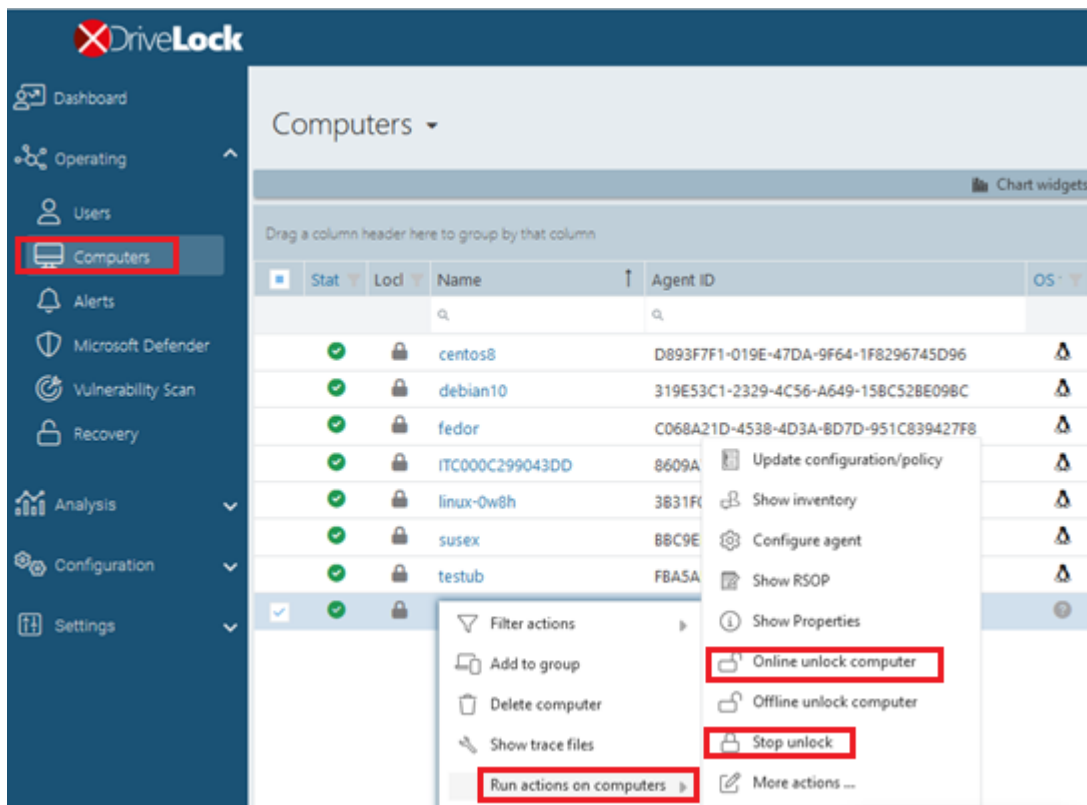
686

The temporary unlock ends after the configured time limit. If an absolute time is specified, the temporary unlock will survive a restart if the time is still within the configured period.

You can use the `drivelock-ctl -showstatus` command line command to display the current status of the temporary share.

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

In application control, the agent allows execution of all binaries and can also detect started or written binaries and add them to the local whitelist if required in the configuration.

For device control, all USB drives or devices can be unlocked at once.

24.4.3 Use join token

The functionality for securely adding agents using a join token can also be used for Linux agents. During installation, a join token is set for this purpose with the `-j` option.

Example: `#sudo ./drivelockd-install.sh -t root -s` `https://192.168.8.75:6067 -i /opt/drivelock -j fa173c1e-6403-439d-8850-f0a71a2fbea7`

You can set the join token later with the `drivelock-ctl -setjointoken` command.

You can find a Linux client's join token in the computer details in the DOC.

24.5 List of events

The following table shows the Linux-related events that are displayed in the DriveLock Operations Center (DOC). All events below are triggered by DriveLock:

A list of all events that are important in connection with DriveLock can be found in the DOC.

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

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

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

Event ID	Event level (Information, Warning, Error)	Event text	Description
131	Audit	Temporarily unlocked	{Product} Agent was temporarily unlocked by an administrator. Administrator computer: [ComputerName] (unique ID [ComputerGuid]). Administrator account: [UserName] (domain [Domain], SID [SID])
132	Audit	Temporary unlocked cancelled	The temporary unlock mode of the {Product} Agent was canceled by an administrator. Administrator computer: [ComputerName] (unique ID [ComputerGuid]). Administrator account: [UserName] (domain [Domain], SID [SID]
139	Warning	Temporary unlock ended	The temporary unlock mode of the {Product} Agent ended because the unlock time elapsed.
152	Warning	Policy storage extraction failed	The policy storage container [name] cannot be unpacked to the local com-

Event ID	Event level (Information, Warning, Error)	Event text	Description
			puter. Some functions relying on files stored in this container may fail.
153	Warning	Configuration file applied	The configuration file [name] was successfully applied.
154	Error	Configuration file download error	The configuration file [name] could not be downloaded. Error code: [code] Error: [error]
158	Error	Configuration file error	The configuration file [name] could not be read. Error code: [code] Error: [error]
191	Warning	{PrefixEnterpriseService} selected	The {PrefixEnterpriseService} [name] was selected by {Product}. Connection ID: [ID] Used for: [Inventory/Recovery/Events]
192	Warning	{PrefixEnterpriseService} not available	No {PrefixEnterpriseService} is available because no valid server connection is con-

Event ID	Event level (Information, Warning, Error)	Event text	Description
			figured.
199	Warning	Drive temporarily unlocked	Drive types temporarily unlocked by administrative intervention are [DriveType1] [DriveType2] [DriveType3] [DriveType4] [DriveType5] [DriveType6] [DriveType7] [DriveType8] [DriveType9] [DriveType10]
200	Warning	Devices temporarily unlocked	Device classes temporarily unlocked by administrative intervention are: [DeviceTypes]
221	Warning	Application hash database missing	The application hash database [FileName] is missing from the policy file storage. Please check if the group policy or configuration file is correctly applied. Rule: [ObjectID]
222	Warning	Cannot open application hash database	The application hash database [FileName] cannot be opened. Please verify the file using Management Console. The underlying

Event ID	Event level (Information, Warning, Error)	Event text	Description
			application rule will not function. Rule: [ObjectID]
235	Error	SSL: Cannot set up	The encrypted communications layer (SSL) could not be set up. Error: [error]
236	Error	Remote control: Cannot set up server	The remote control server component coud not be set up. Agent remote control will be unavailable. Error: [error]
237	Error	Remote control: Internal error	Agent remote control: An internal SOAP communications error occurred. Error: [error]
238	SuccessAudit	Remote control: Function called	An Agent remote control function was called. Calling IP address: [IP address] Called function: [function]
243	Error	Cannot open database	A database could not be opened. Database file: [name] Error code: [code] Error: [error]

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

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

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

Event ID	Event level (Information, Warning, Error)	Event text	Description
			was blocked by company policy. Process: [ProcessName] File Hash: [ProcessHash] Applied rule: [ObjectID] Rule type: [WlType] File owner (user name): [UserName] File owner (user sid): [SID] File version: [FileVersion] Certificate issuer: [CertIssuer] Certificate subject: [CertSubject] Certificate serial: [CertSerNo] Certificate thumb print: [CertThumbprint] Description: [VerDescription] Product: [VerProduct] Command line: [CmdLine] Parent Process: [ProcessName] ([ProcessGuid]
474	Audit	Process started	A process was started. Process: [ProcessName] File Hash: [ProcessHash] Applied rule: [ObjectID] Rule type: [WlType] File owner (user name): [UserName] File owner (user sid): [SID] File version: [FileVersion] Certificate issuer: [Cer-

Event ID	Event level (Information, Warning, Error)	Event text	Description
			tIssuer] Certificate subject: [CertSubject] Certificate serial: [CertSerNo] Certificate thumb print: [CertThumbprint] Description: [VerDescription] Product: [VerProduct] Unique Process ID: [ProcessGuid] Command line: [CmdLine] Parent Process: [ProcessName] ([ProcessGuid]
520	Error	All {PrefixES} not reachable	Cannot load company policy. All configured {PrefixEnterpriseService}s are not reachable.
521	Error	Cannot determine computer token	Cannot determine the computer token. Error code: [code] Error: [error]
522	Error	Error loading policy assignments	An error occurred while loading policy assignments from server [name]. Error: [error]
523	Error	Policy integrity check failed	The integrity of an assigned policy could not be verified.%rPolicy ID: [ID] Policy

Event ID	Event level (Information, Warning, Error)	Event text	Description
			name: [name] Actual hash: [value] Expected hash: [value]
533	Warning	No policy - wiped	No valid policy available - the company policy was wiped because the computer was offline for a long period of time.
546	Warning	Application control temporarily disabled	Application control was temporarily disabled by administrative intervention. Learn written files: [LearnWrittenFiles] Learn executed files: [LearnExecutedFiles]
584	Information	Inventory started	Inventory generation was triggered by DES.
593	Information	Machine learning completed	Machine learning for local application whitelist was completed.
594	Error	Error during machine learning	An error occurred during machine learning of the local application whitelist. Step: [StepName] Error

Event ID	Event level (Information, Warning, Error)	Event text	Description
			code: [ErrorCode]
595	Error	Error during machine learning	An error occurred during machine learning of executable file "[FileName]". Error code: [ErrorCode] Error: [ErrorMessage]
596	Information	Machine learning completed	Machine learning of executable file "[FileName]" completed. Reason: [AlfLearnReason]
597	Error	Application control license required	The company policy contains settings for application control features requiring a special license which is not present on the system. Error: [ErrorMessage]
639	Error	Server certificate error	Server certificate error detected. Certificate: [name]. Error message: [text]
648	Audit	DLL blocked	The loading of a DLL was blocked by company

Event ID	Event level (Information, Warning, Error)	Event text	Description
			policy. Process: [ProcessName] ([ProcessGuid]) Applied rule: [ObjectID] Rule type: [WlType] DLL File Name: [ProcessName] DLL File Hash: [ProcessHash] File owner (user name): [UserName] File owner (user sid): [SID] File version: [FileVersion] Certificate issuer: [CertIssuer] Certificate subject: [CertSubject] Certificate serial: [CertSerNo] Certificate thumb print: [CertThumbprint] Description: [VerDescription] Product: [VerProduct]
649	Audit	DLL loaded	A DLL was loaded. Process: [ProcessName] ([ProcessGuid]) Applied rule: [ObjectID] Rule type: [WlType] DLL File Name: [ProcessName] DLL File Hash: [ProcessHash] File owner (user name): [UserName] File owner (user sid): [SID] File version: [FileVersion] Certificate issuer: [Cer-

Event ID	Event level (Information, Warning, Error)	Event text	Description
			tIssuer] Certificate subject: [CertSubject] Certificate serial: [CertSerNo] Certificate thumb print: [CertThumbprint] Description: [VerDescription] Product: [VerProduct]
679	Information	Machine learning started	Machine learning for local application whitelist was started.

24.6 Command line tool

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

The following commands are available (see figure):

```
test@testub:~$ /opt/drivelock/drivelock-ctl h
-----------------------------------------------------------------------
Drivelock Linux Agent- Command line tool
-----------------------------------------------------------------------
DriveLock, 21.2.0.36779
Usage: drivelock-ctl [Option]

Options:
    -enabletracing <level>                Enable service logging. Parameter is optional.
    -disabletracing                       Disable service logging
    -updateconfig                         Trigger a configuration update
    -showstatus                           Show drivelock configuration status
    -setjointoken <join token>            Set join token
    -settenant <tenantname>               Set tenant name
    -setserver [http(s)://<server>:<port>]  Set one or more server(DES) URLs,
                                          URLs should be delimited by ;
    -recreatebootdevices                  Re-load boot devices
    -rescanapps                           Re-create local whiteliste
```

- `enabletracing`: Enables tracing to the **Drivelock.log** file residing in the installation directory in the **log** child directory.

- `disabletracing`: Disables tracing

- `updateconfig`: Updates your configuration, e.g. if you have made changes to your policies. The Linux agent then immediately connects to the DES and loads the changes

- `showstatus`: Shows the current status of the Linux client and informs when, for example, the DES was last contacted, which policies are assigned or which DriveLock modules are licensed (see figure)

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

Agent Identity:
----------------------------
Agent version:          21.2.0.36779
Computer Name:          testub
Computer GUID:          16e49a3e-19da-4707-8456-f11bdcdf6680
Domain Name:            localdomain
OS Name:                Ubuntu
OS Version:             21.04 (Hirsute Hippo)

Component licensing status:
----------------------------
Device control:         Licensed
Application control:    Licensed

Agent Configuration & Status:
----------------------------
Tenant:                 kav
Server URL(s):          https://192.168.8.249:6067
Last server contact at: 05.10.2021 16:45:14
Last inventory at:      unknown

Temporary unlock:       Not active

Assigned Policies:
----------------------------

1  CSP ID: 55f8de53-9444-4151-979b-8895c2cdc6da
   ConfigName: Linux Tenant Test
   Version: 298
   Target: LinuxGroupUben
   Status: CSP Successfully Applied
```

- `setjointoken <join token>`: Specify here the join token that will be set during the installation.

- `settenant`: Specifies the tenant for your Linux agent

- `setserver`: Specifies the DES that communicates with the Linux agent

- `recreatebootdevices`: Creates a new list of currently connected USB devices that should always be allowed at boot time

- `rescanapps`: Creates a new local whitelist

25 Other

25.1 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 program "dlcmd.exe" is installed in the DriveLock program directory (Programs -> CenterTools -> DriveLock MMC -> Tools). 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.

25.1.1 Check 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:
Computer GUID:        {              df-4ab8-97f8-7ce69013e8e7}
Domain DNS name:      D
ActiveDirectory site: D      -First-Site-Name
Logged-on user name:  D
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)
```
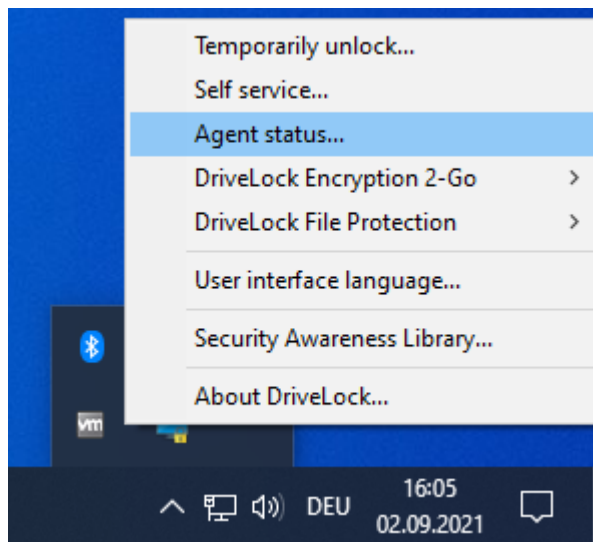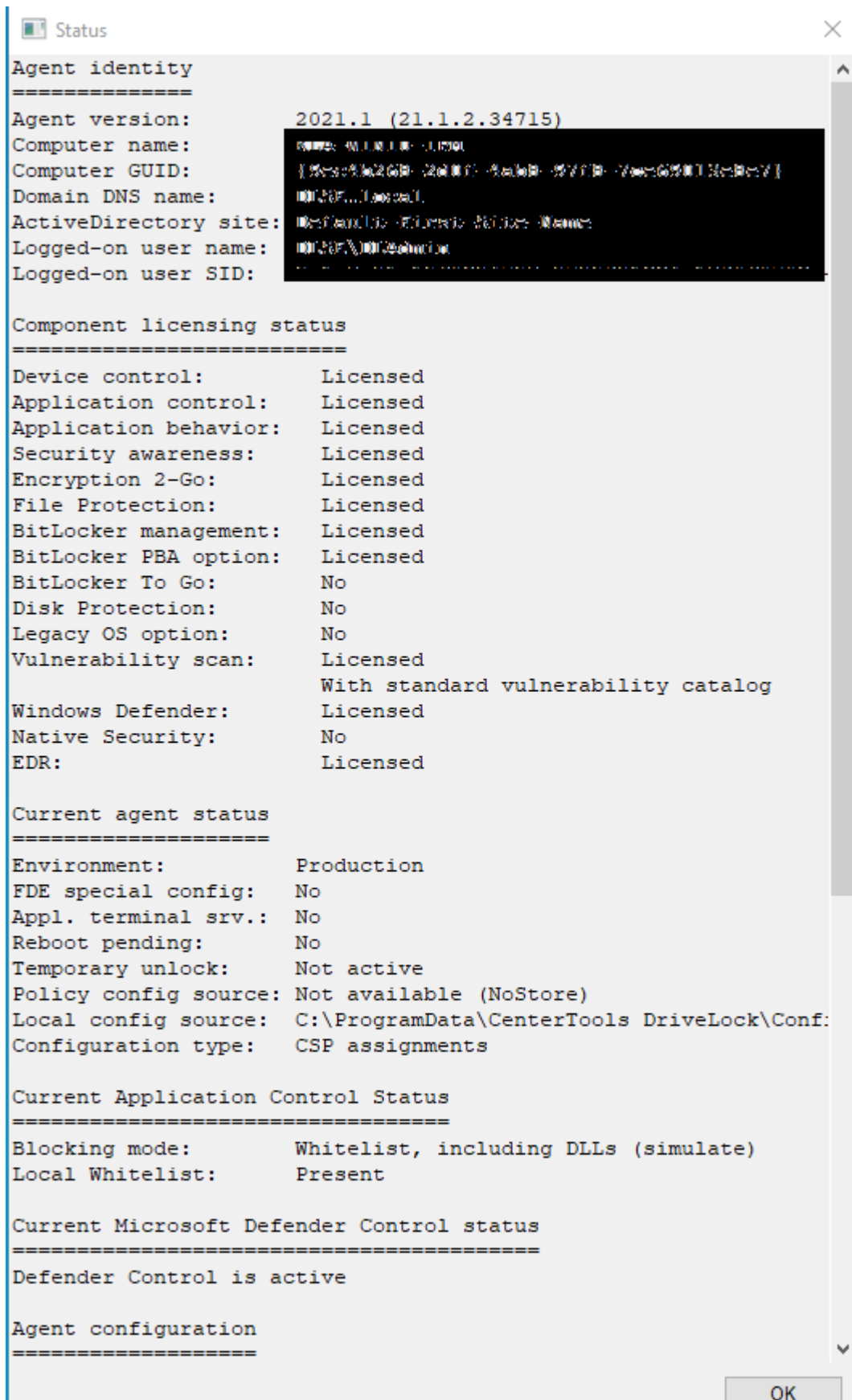
You will receive detailed information about the licenses, configuration and status of the individual components.

2. Via the tray icon on the DriveLock Agent:

Select **Agent status**....

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

```
Status                                                                    ✕

Agent identity
==============
Agent version:          2021.1 (21.1.2.34715)
Computer name:          ▮▮▮▮▮▮▮▮▮▮▮
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
===================

                                                              OK
```

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

25.1.2 DriveLock Support Companion

Start the DriveLock Support Companion by calling up one of the following files directly on the client computer:

- Dlsupport.exe: Is installed with the DMC.

- Dlsupportagent.exe: Installed with the DriveLock Agent. As a rule, use this file.

You can use the Support Companion to create trace or diagnostic files or test the connection to the client.

- You can use the **Test connection** option to 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.

The functionality for displaying the trace files can also be found in the DOC under *Settings* ⚙ *-> Trace files*. To create or activate trace files, go to the respective computer in the DOC and click *Run actions on computer -> Request trace files from agent* in the context menu.

Copyright