



DriveLock Encryption

Documentation 2022.2

DriveLock SE 2022



Table of Contents

1 ENCRYPTION WITH DRIVELOCK	8
1.1 License settings	8
2 DRIVELOCK DISK PROTECTION	10
2.1 Policy settings	10
2.1.1 Encryption certificates	10
2.1.1.1 Generate encryption certificates	11
2.1.1.2 Recovery keys	12
2.1.2 User-related agent settings	13
2.1.3 Hard disk encryption settings	15
2.1.4 Pre-boot authentication settings	16
2.1.4.1 General	16
2.1.4.2 Network Pre-Boot (BIOS)	18
2.2 Decryption	19
2.3 Overwrite policy (Disk Protection)	19
2.4 DriveLock Disk Protection recovery and tools	21
2.4.1 Retrieving diagnostic information	22
2.4.2 Settings for the emergency logon (challenge response)	22
2.4.3 Recovering encrypted drives	23
2.4.3.1 Disk key recovery	24
2.4.3.2 Creating a recovery medium	25
2.4.3.2.1 Windows PE recovery wizard	26
2.4.3.3 Recovering disks	27
2.4.4 Remote wipe	28
3 DRIVELOCK BITLOCKER MANAGEMENT	30
3.1 General information	30
3.1.1 System Requirements	31

3.1.2 Algorithms for DriveLock BitLocker Management	33
3.2 Policy settings	34
3.2.1 Encryption certificates	34
3.2.1.1 Create encryption certificates	34
3.2.2 User-related agent settings	37
3.2.3 Hard disk encryption settings	39
3.2.3.1 The General tab	39
3.2.3.2 The Encryption protection tab	42
3.2.3.3 The Recovery tab	44
3.2.3.4 The Execution options tab	46
3.2.4 Pre-boot authentication settings	47
3.2.4.1 Authentication type	48
3.2.4.1.1 Option: DriveLock pre-boot authentication	50
3.2.4.2 Password options	51
3.2.4.3 Logon methods	53
3.2.4.4 Appearance	54
3.3 Decryption	55
3.3.1 Decrypting encrypted drives	55
3.4 Override policy settings (BitLocker)	56
3.5 Sample configuration	58
3.6 Recovery	59
3.6.1 Recovering encrypted hard disks	59
3.6.2 Recovery process	61
3.7 Taking over native BitLocker	65
3.7.1 Integrating existing BitLocker environments	65
3.7.2 Additional modifications of BitLocker policies	66
3.8 DriveLock Agent	67

3.8.1 BitLocker pre-boot authentication	67
3.8.2 BitLocker Management on client computers (DriveLock Agent)	68
3.8.3 Encrypting client computers	69
3.8.3.1 Delay encryption	71
3.8.4 Integrating data partitions with existing BitLocker	73
3.9 Tracing BitLocker actions	76
4 DRIVELOCK PRE-BOOT AUTHENTICATION	77
4.1 Pre-boot authentication settings	78
4.1.1 Users	79
4.1.2 User synchronization	79
4.1.3 User wipe	80
4.1.4 Network pre-boot (UEFI)	80
4.1.5 Emergency logon	80
4.1.6 Self-wipe	81
4.2 PBA settings in the list view	81
4.2.1 Allow local PBA configuration changes	82
4.2.2 Select PBA keyboard driver	82
4.2.3 Load SmartCard drivers in PBA	82
4.3 PBA settings in the DriveLock Operations Center (DOC)	83
4.4 Override policy settings (DriveLock PBA)	84
4.5 Network pre-boot authentication (UEFI)	86
4.5.1 Network pre-boot (UEFI)	87
4.5.2 Use case 1: Automatic logon	89
4.5.3 Use case 2: Network login for all AD users	90
4.5.4 Network PBA settings in the DOC	92
4.6 Settings for emergency logon	93
4.7 DriveLock Agent	96

4.7.1 Installing the DriveLock PBA on the DriveLock Agent	96
4.7.2 Login to the DriveLock PBA	96
4.7.3 Network pre-boot authentication	99
4.7.4 Emergency logon with recovery code	101
4.7.5 Windows authentication	103
4.7.6 BIOS pre-boot authentication	104
4.8 DriveLock PBA command line tool	107
4.9 Shortcut and function keys	109
5 DRIVELOCK BITLOCKER TO GO	111
5.1 Requirements for BitLocker To Go	111
5.2 Policy settings	112
5.2.1 General settings for BitLocker To Go	113
5.2.2 Recovering encrypted drives	114
5.2.2.1 Administrative password	114
5.2.2.2 Certificate-based recovery	115
5.2.3 Settings for enforced encryption	115
5.3 Sample configuration for BitLocker To Go encryption	116
5.3.1 Create drive whitelist rule	118
5.4 BitLocker To Go recovery	119
5.4.1 Recovery procedure	120
5.4.2 Recovery in the DriveLock Operations Center (DOC)	120
5.5 DriveLock Agent	121
5.5.1 BitLocker To Go on the DriveLock Agent	121
5.6 Use cases	124
5.6.1 Administrative password rules	124
5.6.2 Encryption rules	125
6 DRIVELOCK ENCRYPTION 2-GO	127

6.1	General information	127
6.1.1	Encryption methods	127
6.2	Policy settings	128
6.2.1	Settings	128
6.2.1.1	General encryption settings	128
6.2.1.2	Enforced encryption settings	129
6.2.1.3	Password recovery settings	130
6.2.1.4	Advanced settings	130
6.2.2	Recovering encrypted containers	136
6.2.2.1	Administrative password	136
6.2.2.2	Certificate-based container recovery	137
6.2.3	Enforced encryption	137
6.2.3.1	Encryption rule	138
6.2.3.2	User selection rule	140
6.3	Offline recovery process	141
6.4	Online recovery process	142
6.5	Recovery in the DriveLock Operations Center (DOC)	144
7	DRIVELOCK FILE PROTECTION	145
7.1	How does DriveLock File Protection work?	145
7.1.1	Supported Encryption Mechanism	146
7.2	Configuring File Protection	147
7.2.1	Creating a Master Certificate for Key Management	148
7.2.2	Configuring Certificate Management	148
7.3	Policy settings	149
7.3.1	Configuring encryption settings	149
7.3.2	Configuring the encryption user interface	150
7.3.3	Configure encrypted drives settings	152

7.3.4 Configure additional settings	153
7.3.5 Applied encryption format	153
7.4 Settings for enforced encryption	154
7.5 Configure encrypted drive recovery	156
7.5.1 Company Certificate	158
7.6 Managing User Accounts and Certificates	159
7.6.1 How User Administration works	159
7.6.2 Manage users	160
7.6.3 Manage groups	162
7.6.4 Manage certificates	163
7.7 Managing encrypted drives centrally (Centrally managed folders)	165
7.7.1 Preparations in Active Directory	166
7.7.1.1 Duplicating the certificate template	166
7.7.1.2 Issuing the template	169
7.7.1.3 Creating a group policy	171
7.7.1.4 Automatic registration	172
7.7.1.5 Testing the automatic enrollment	174
7.7.2 Creating a new encrypted drive	177
7.7.3 Change access permissions	177
7.8 Use case: Accessing encrypted folders	179
7.9 Restore encrypted folders	184
7.10 File Protection in the DOC	185
COPYRIGHT	186

1 Encryption with DriveLock

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: [DriveLock Pre-Boot Authentication \(PBA\)](#) is used in 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

1.1 License settings

To use the different encryption modules, you need different licenses. You can find the license settings in the Global Settings section of the Policy Editor.

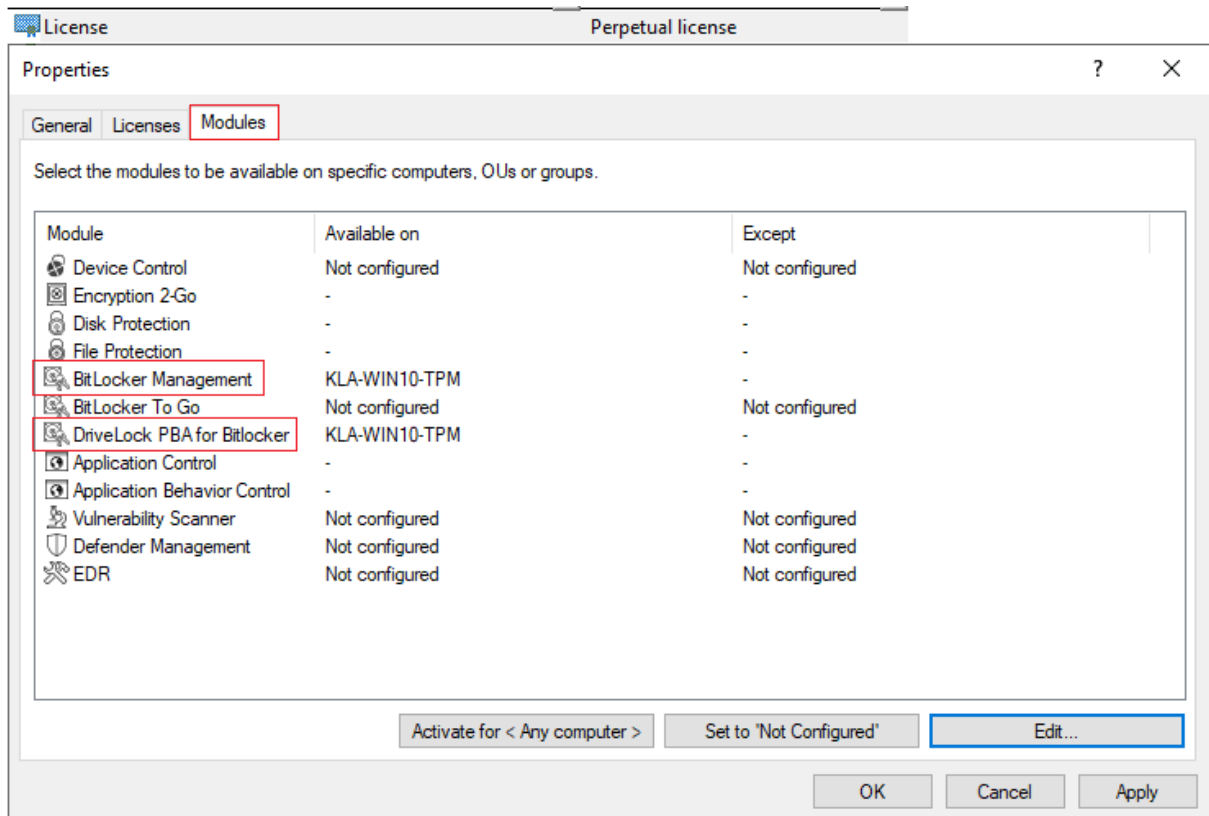


Note: Please refer to the DriveLock installation and administration documentation for general licensing information at [DriveLock Online Help](#)..

The example of licensing BitLocker Management and DriveLock PBA for BitLocker illustrates the process:

1. In **Global Settings**, go to **Settings** and then double-click **License**.
2. Open the **Licenses** tab.

3. Select **Add License File...** or **Add License Key...** and follow the License Activation Wizard.
4. On the **Modules** tab, select the **BitLocker Management** and **DriveLock PBA for BitLocker** licenses.



5. Either activate the license for **<All computers>** or click the **Edit...** button and select specific AD computers, groups OUs where you want to deploy BitLocker Management.
6. Confirm your settings.

Warning: It is not possible to assign the Disk Protection and BitLocker Management license in one policy at the same time!

2 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

2.1 Policy settings

2.1.1 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):**

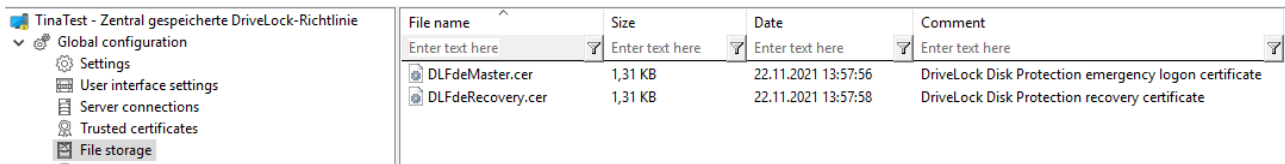
The DLFDERecovery.cer and DLFDERecovery.pfx files produce a public/private key pair.

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.

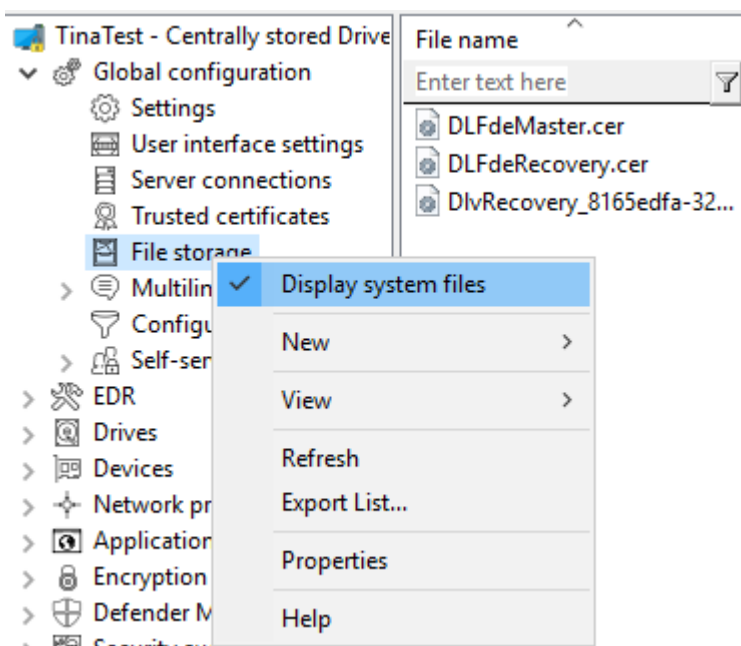
 **Note:** Make sure that these files are saved in a safe place along with the password, as they will be used for emergency logon and data recovery. Recovery without this data is not possible.

Once the encryption certificates are created, the DriveLock Management Console shows the time and date of their creation.




File name	Size	Date	Comment
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 system files** setting so that these certificates appear:



The certificates are also stored in the private certificate store of the current user:



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	S...	Certificate Template
ProtectDrive Recovery Support	ProtectDrive Recovery Support	22.11.2051	1.2.840.113556.1.80...	<None>		DL Recovery Support
ProtectDrive Master Security	ProtectDrive Master Security	22.11.2051	1.2.840.113556.1.80...	<None>		DL Master Security

2.1.1.1 Generate 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.

2.1.1.2 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 auto-

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).

2.1.2 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.

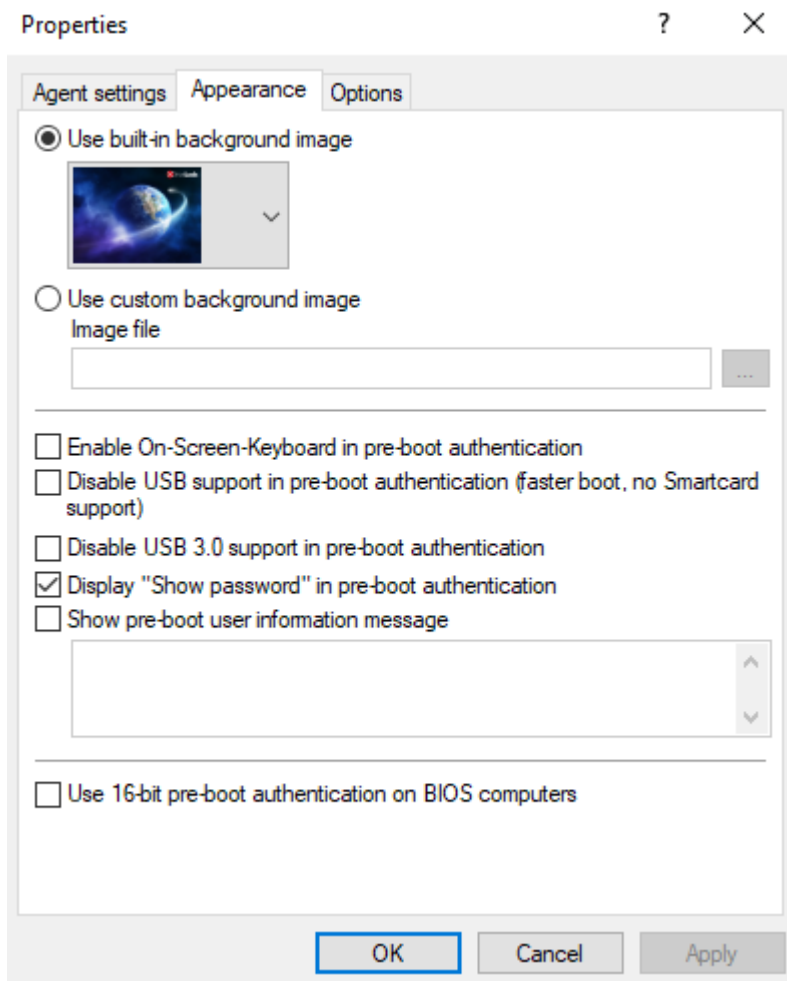
Select the **Do not restart computer (wait until manual restart)** option if you want to control it yourself. This allows you to start your own installation script, for example, with a shell command after the installation.

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

- 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.

2.1.3 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 algorithm**; 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:

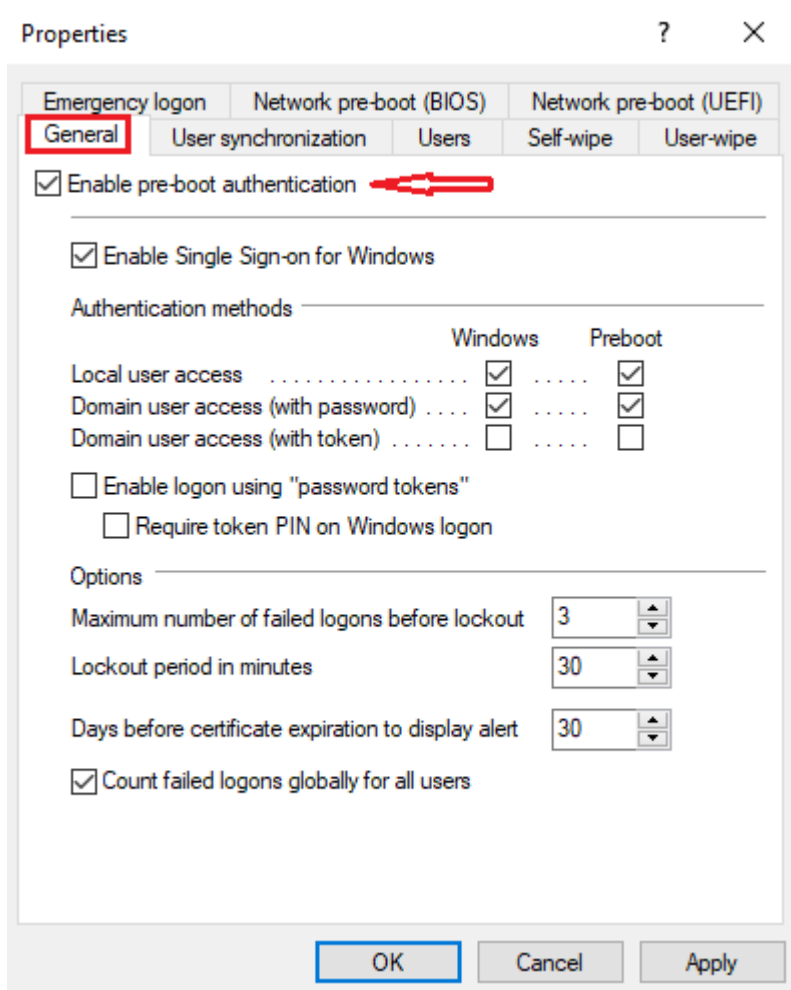
Here you specify where to store the DriveLock Agent [recovery keys](#) for the challenge response procedure.

2.1.4 Pre-boot authentication settings

2.1.4.1 General

In the **Pre-boot authentication settings**, you can enable the [pre-boot authentication](#) for DriveLock agents that are protected with Disk Protection.

On the **General** tab, select the **Enable pre-boot authentication** 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 use a smartcard / token and PIN for authentication.

- **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.

 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. Adjust the values to match your organization's security policy.


- 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 the following dialog:



2.1.4.2 Network Pre-Boot (BIOS)

 Note: Note that as of version 2022.2, DriveLock Legacy BIOS pre-boot authentication is no longer supported and will be removed from the product. When you

 install a version 2022.2 agent, the system checks whether there is an active legacy BIOS PBA 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.

2.2 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).

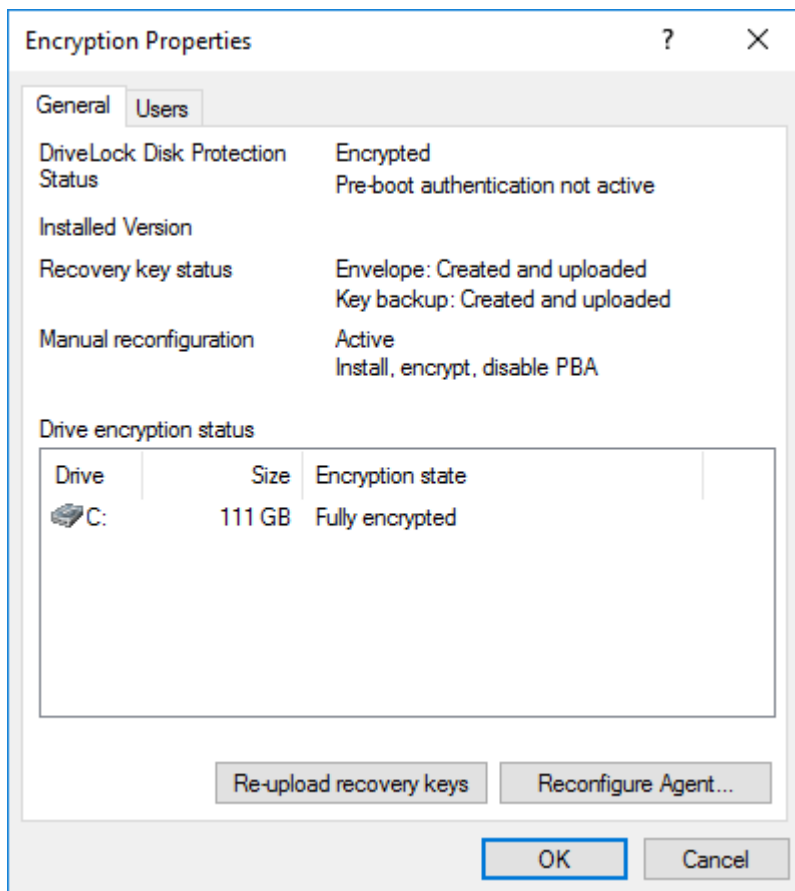
To start decrypting encrypted drives, proceed as follows:

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.

2.3 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**.

Reconfigure DriveLock Disk Protection

You can override DriveLock Disk Protection settings in your company policy on Agents. This replaces the settings configured here with the company policy that is applied to the Agent computer.

☒ **Override policy settings**

☒ **Override general deployment settings**

- ☒ Install DriveLock Disk Protection
- ☐ Enable pre-boot authentication
- ☒ Encrypt local hard disks

Pre-boot authentication settings

- ☒ Disable 32-bit pre-boot authentication
- ☒ Enable On-Screen-Keyboard in pre-boot authentication
- ☒ Disable USB support in pre-boot authentication

☐ **Override authentication methods**

	Windows	Preboot
Local user access	<input type="checkbox"/>	<input type="checkbox"/>
Domain user access (with password)	<input type="checkbox"/>	<input type="checkbox"/>
Domain user access (with token)	<input type="checkbox"/>	<input type="checkbox"/>

☐ Enable logon using "password tokens"

☐ Require token PIN on Windows logon

☐ **Override emergency access methods**

- ☐ Allow emergency logon with user name
- ☐ Single Sign-on after emergency logon
- ☐ Allow emergency logon without user name
- ☐ Allow emergency logon for token users

OK **Cancel**

Activate **Override policy** to configure computer-specific settings in deviation from the central policy. The selected settings apply only to the currently connected computer.

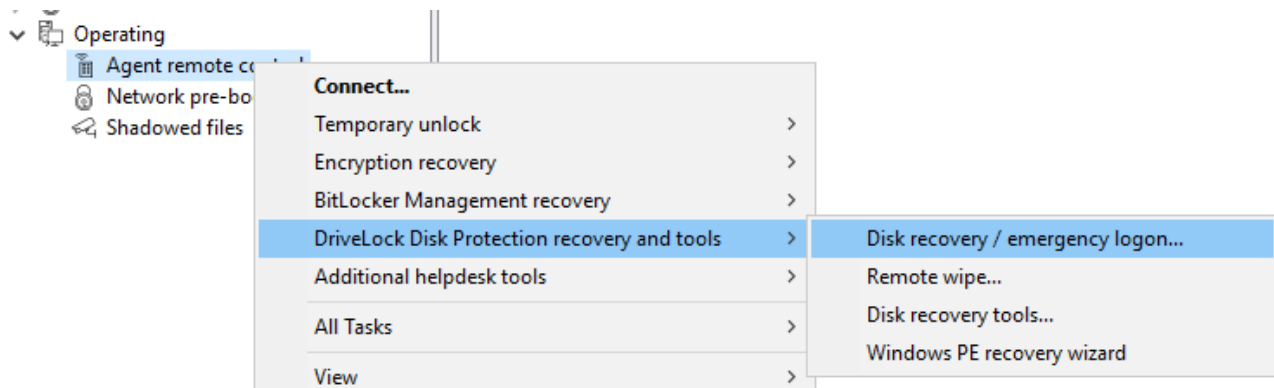
You can see which users are stored in the computer's PBA on the **Users** tab. You can add or delete individual users here.

2.4 DriveLock Disk Protection recovery and tools

Disk Protection covers two different recovery methods:

- [Emergency logon procedure](#)
The emergency logon procedures are used when a user is no longer able to log on to the pre-boot authentication (e.g. in case the user forgets the password or PIN).
- Recovery of encrypted drives (data)
Drive 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.



2.4.1 Retrieving diagnostic information

When DriveLock Disk Protection is installed, the DriveLock Agents send 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 then 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.

2.4.2 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. On the first page, select the **Emergency logon** option. If your recovery keys are sent to DriveLock Enterprise Service, keep the default setting **DriveLock Enterprise Service**. If you want to specify the path to the required recovery keys later, select **Recovery files (copied from agent computer)**.
3. For the emergency logon procedure, you need the private key of the recovery certificate. In the second dialog you specify the location, either Windows certificate store, a smart card or a PFX file together with the respective password. You can find more information about certificates [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 displays a list of computers allowing you to select the computer you want to restore. Check the option **Show only the newest entry per computer**. Click **Next**.
5. Next, the page for entering the user's request / recovery code appears.



Note: For more information on the interaction between administrator and end user, [click here](#).

Enter the code in the appropriate fields (see figure). You can optionally specify the name of the user.



Warning: Now, the recovery code that the user must provide you with is mandatory.

6. Click **Next** to have the response code generated.
7. Tell the user the **response code**.
8. Click **Finish**.

2.4.3 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.

2.4.3.1 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.



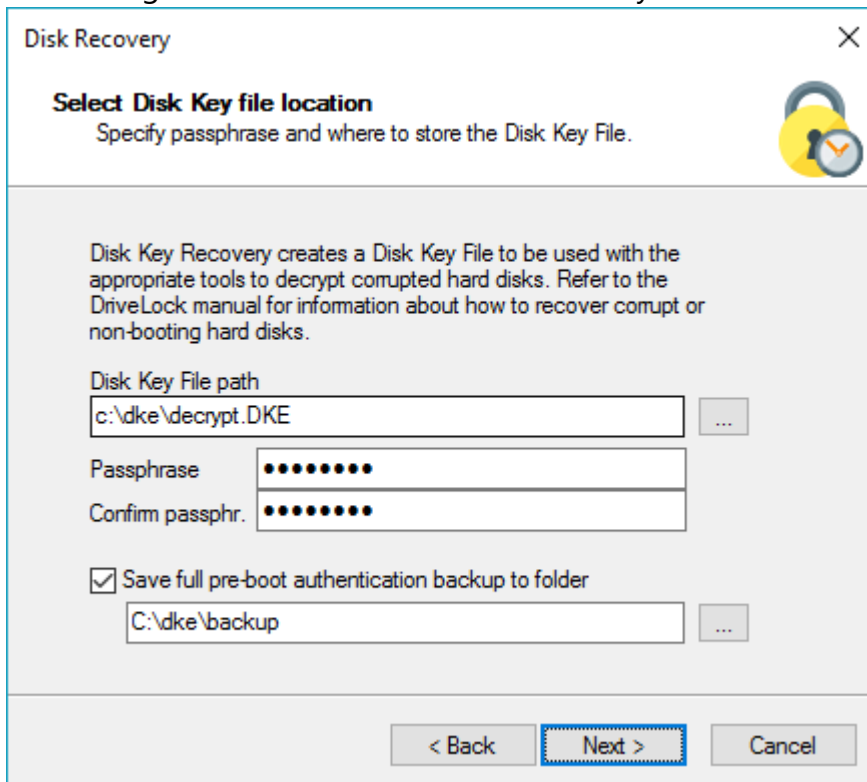
Note: Each client computer has its own corresponding [EFS recovery file](#) that must be used for drive recovery. If you configured DriveLock Disk Protection to upload this file automatically to a central shared folder, the file name is prefixed with the name of the client computer (for example: DE2319WX_Backup.zip). 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.

2.4.3.2 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.

2.4.3.2.1 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. The wizard is only available in English.

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 to write the output files, 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 flash drive. If you don't select anything, the system simply creates a file structure that you have to 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 see the links to the respective directory. Click **Finish** to exit the wizard.

The Recovery CD contains all tools and drivers that are required to perform a disk recovery.

2.4.3.3 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`

```

Administrator: X:\windows\system32\cmd.exe - diskpart

X:\windows\system32>wpeinit
X:\windows\system32>cd ..\..\DriveLock
X:\DriveLock>peprep.exe /usb
SafeNet ProtectDrive peprep.exe Version: 9.4.8.33
USB support installed.
X:\DriveLock>diskpart

Microsoft DiskPart version 6.2.9200

Copyright (C) 1999-2012 Microsoft Corporation.
On computer: MININT-KN5DIRF

DISKPART> lis vol

   Volume ###  Ltr  Label          Fs      Type          Size      Status       Info
   -----
   Volume 0      F    DUD_ROM        UDF     DVD-ROM       177 MB    Healthy
   Volume 1      C    System Rese    NTFS    Partition     350 MB    Healthy
   Volume 2      E                    NTFS    Partition     59 GB     Healthy
   Volume 3      D                    RAW     Partition     2045 MB   Healthy
   Volume 4      G    DRIVELOCK      FAT     Removable     955 MB    Healthy

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.

```

Administrator: X:\windows\system32\cmd.exe - diskpart
1 Dir(s) 1,000,521,728 bytes free

X:\DriveLock>peprep -inj g:\PMDLW8X64.DKE
SafeNet ProtectDrive peprep.exe Version: 9.4.8.33
Determining data for encrypted drive D:\ succeeded.
Injecting disk key
Please enter the pass-phrase for file g:\PMDLW8X64.DKE
*****
Disk key successfully injected.

X:\DriveLock>diskpart

Microsoft DiskPart version 6.2.9200

Copyright (C) 1999-2012 Microsoft Corporation.
On computer: MININT-KN5DIRF

DISKPART> lis vol

  Volume ###  Ltr  Label          Fs      Type          Size      Status       Info
  -----
  Volume 0      F   DVD_ROM        UDF     DVD-ROM       177 MB     Healthy
  Volume 1      C   System Rese    NTFS    Partition     350 MB     Healthy
  Volume 2      E   Data           NTFS    Partition     59 GB      Healthy
  Volume 3      D   Data           NTFS    Partition     2045 MB    Healthy
  Volume 4      G   DRIVELOCK      FAT     Removable     955 MB     Healthy

DISKPART>

```

If the action was successful, the drive will no longer be displayed as RAW.

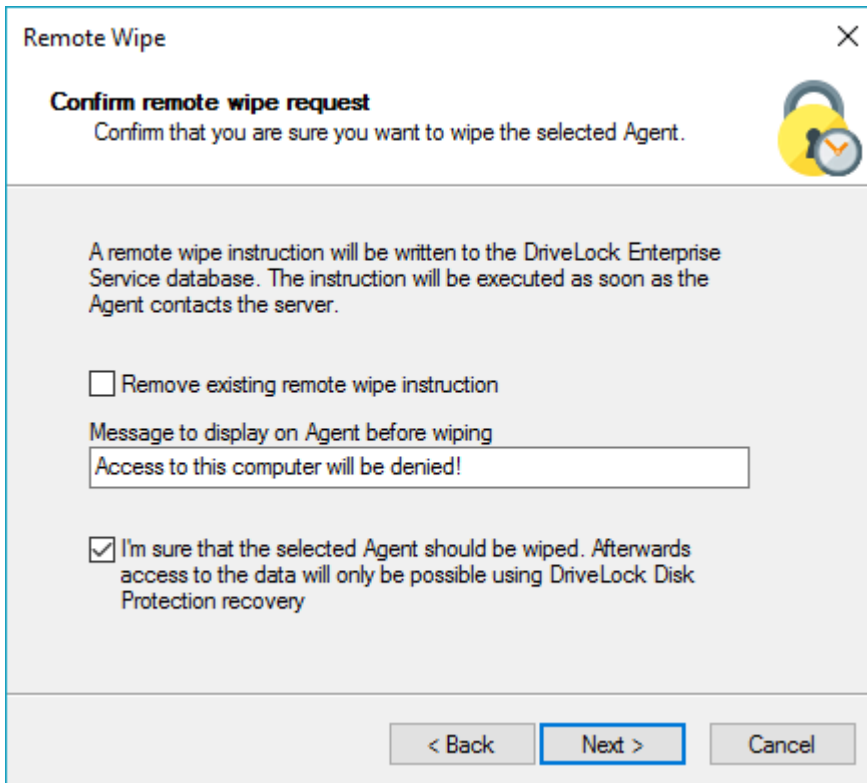
Enter `Exit` to leave DISKPART.

You can now access the drive (provided there is no other critical issue) and copy important files or try to repair the hard drive.

2.4.4 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.



Remote Wipe

Confirm remote wipe request
Confirm that you are sure you want to wipe the selected Agent.

A remote wipe instruction will be written to the DriveLock Enterprise Service database. The instruction will be executed as soon as the Agent contacts the server.

☐ Remove existing remote wipe instruction

Message to display on Agent before wiping
Access to this computer will be denied!

☒ I'm sure that the selected Agent should be wiped. Afterwards access to the data will only be possible using DriveLock Disk Protection recovery

< Back Next > Cancel

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).

3 DriveLock BitLocker Management

DriveLock BitLocker Management offers you a number of advantages when compared to the native 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
- Use smartcard and token in addition to common BitLocker authentication methods
- Monitor the encryption and decryption states of individual client computers in the DriveLock Control Center
- 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
- [DriveLock pre-boot authentication](#) for BitLocker allows you to unlock the system partition using your Windows login. This eliminates the need to enter the computer-specific BitLocker password.

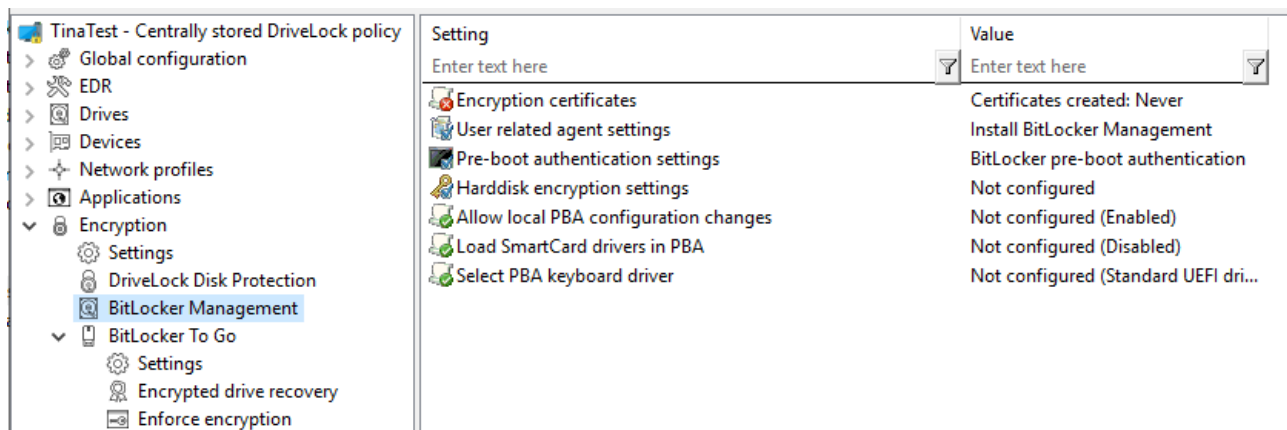
3.1 General information

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.



3.1.1 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**
 - 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)

3.1.2 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	<ul style="list-style-type: none">• AES 128 bit with diffuser• AES 256 bit with diffuser• AES 128 bit• AES 256 bit
Windows 8.1	<ul style="list-style-type: none">• AES 128 bit• AES 256 bit
Windows 10 and higher	<ul style="list-style-type: none">• 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.

3.2 Policy settings

3.2.1 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 adds the encryption certificates to the Windows Certificate Store where it also stores the passwords.



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](#).

3.2.1.1 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 generated 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** button.

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 otherwise 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.

Encryption Certificate Creation ✕

Certificate protection
Type the password to protect the private keys for the certificate.



 Private keys for the certificates are protected by passwords. Passwords are not stored as part of the DriveLock policy. You will need the passwords to access private keys for emergency logon and recovery.
Please save these passwords in a secure location.

Emergency logon certificate password _____

Password

Confirm password

Recovery certificate password _____

Password

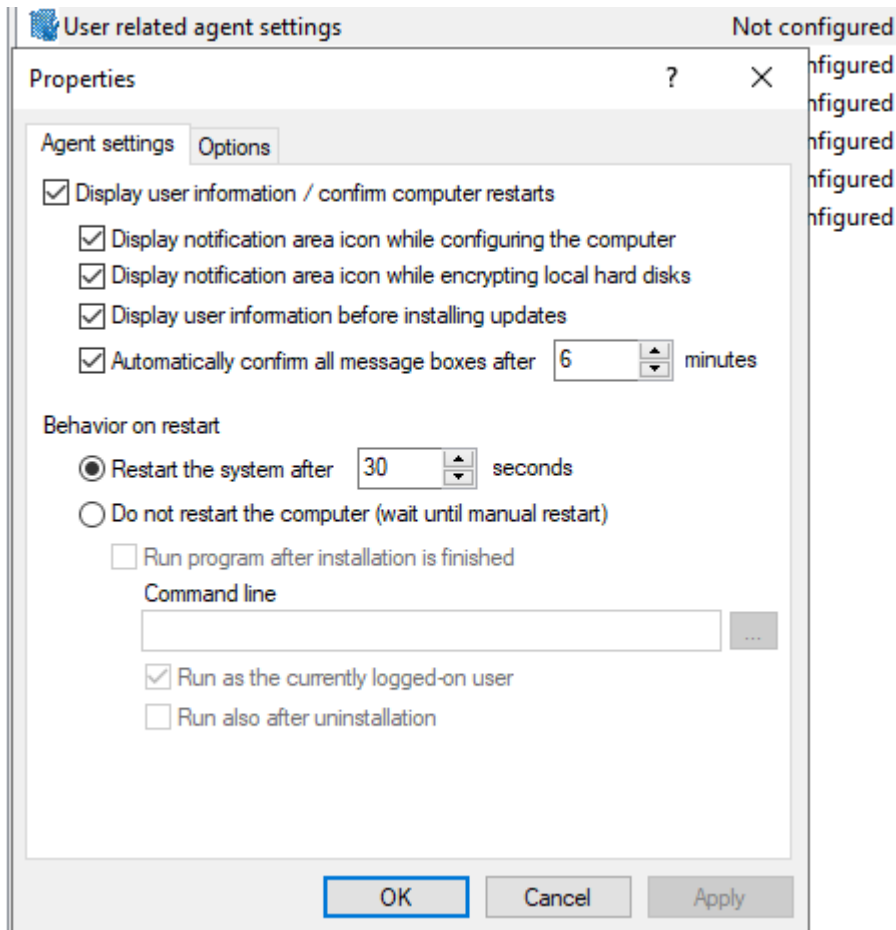
Confirm password

- Next, DriveLock generates the encryption certificates in the location you specified.

3.2.2 User-related agent settings

When BitLocker Management or the DriveLock PBA for BitLocker is installed on a DriveLock agent, the users are informed by default and their client computer is restarted after 30 seconds after the installation. 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.

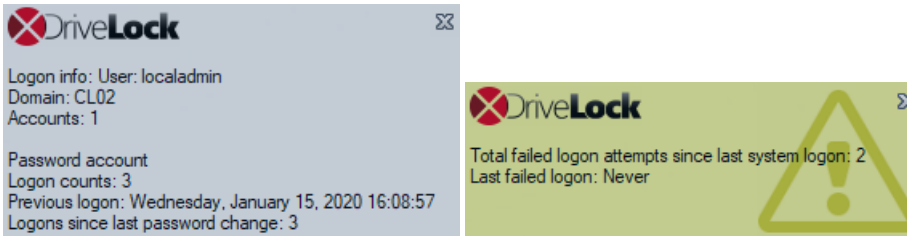
Two options are available:

- **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.

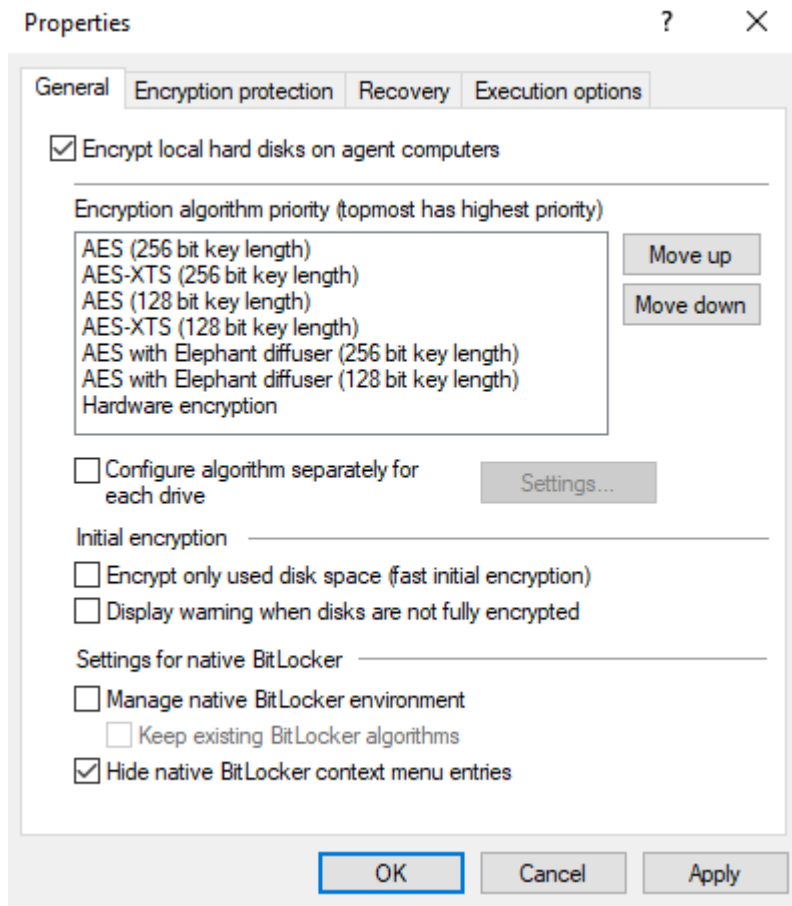
A message with detailed information will appear on the client computer (see figure):



3.2.3 Hard disk encryption settings

3.2.3.1 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, make sure 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 chapter [decryption](#)), uncheck the option and, if necessary, specify a [delay in days](#).

 Warning: Once you uncheck the option and do not specify a delay (and the policy is assigned and synchronized by the client), the decryption process will start.

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.

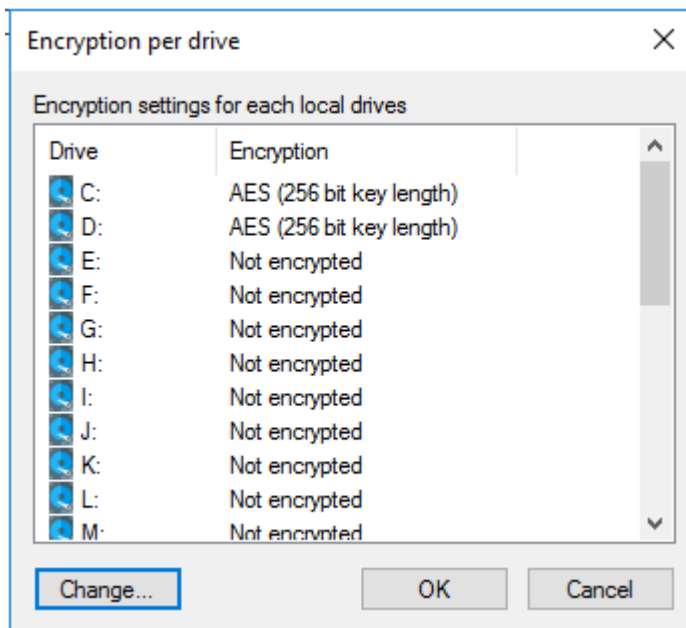
 Note: We recommend placing the strongest algorithm at top level.

- 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. 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.

3.2.3.2 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.

3.2.3.3 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.

Properties

General Encryption protection **Recovery** Execution options

Recovery key rotation

Maximum BitLocker recovery key age: 5 days

Recovery Disk Keys will be stored on

☒ DriveLock Enterprise Service
Server connections are configured under Global configuration | Server connections

☐ File server (UNC path)

☐ Local folder on agent computers (not recommended)

☐ Login to File server (UNC path)

User name

Password

Confirm password

OK Cancel Apply

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.

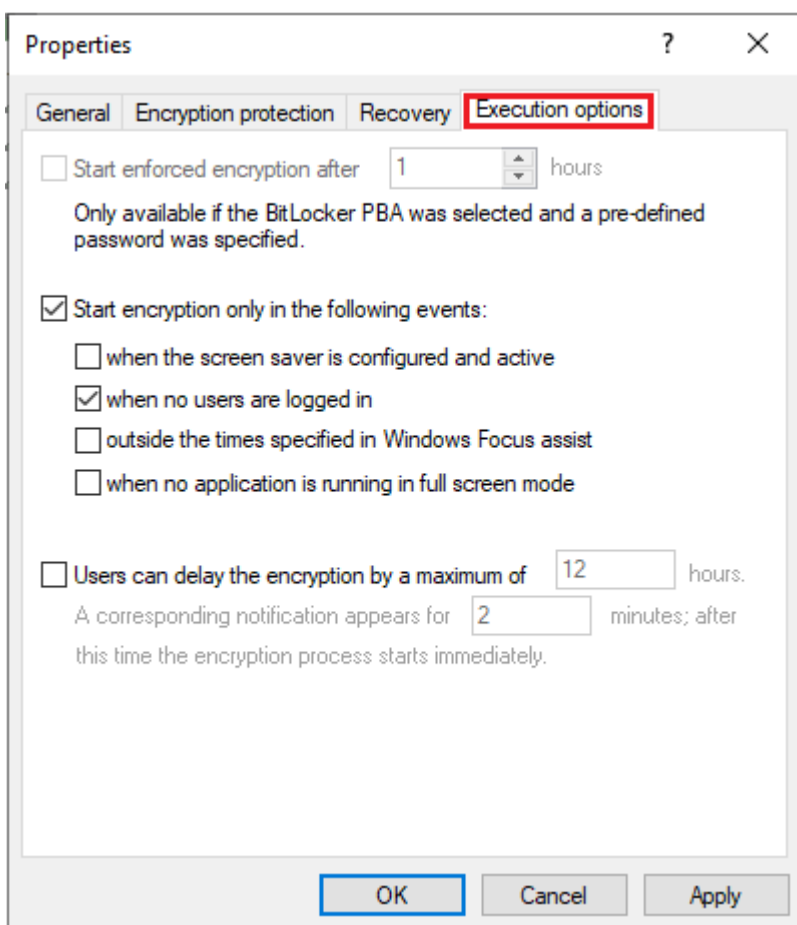
3.2.3.4 The Execution options tab

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.

The **Start enforced encryption after x hours** option is available only if you have selected BitLocker PBA in the [Pre-boot authentication settings](#) and specified a password. 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 option **Start encryption only in the following events:** 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.

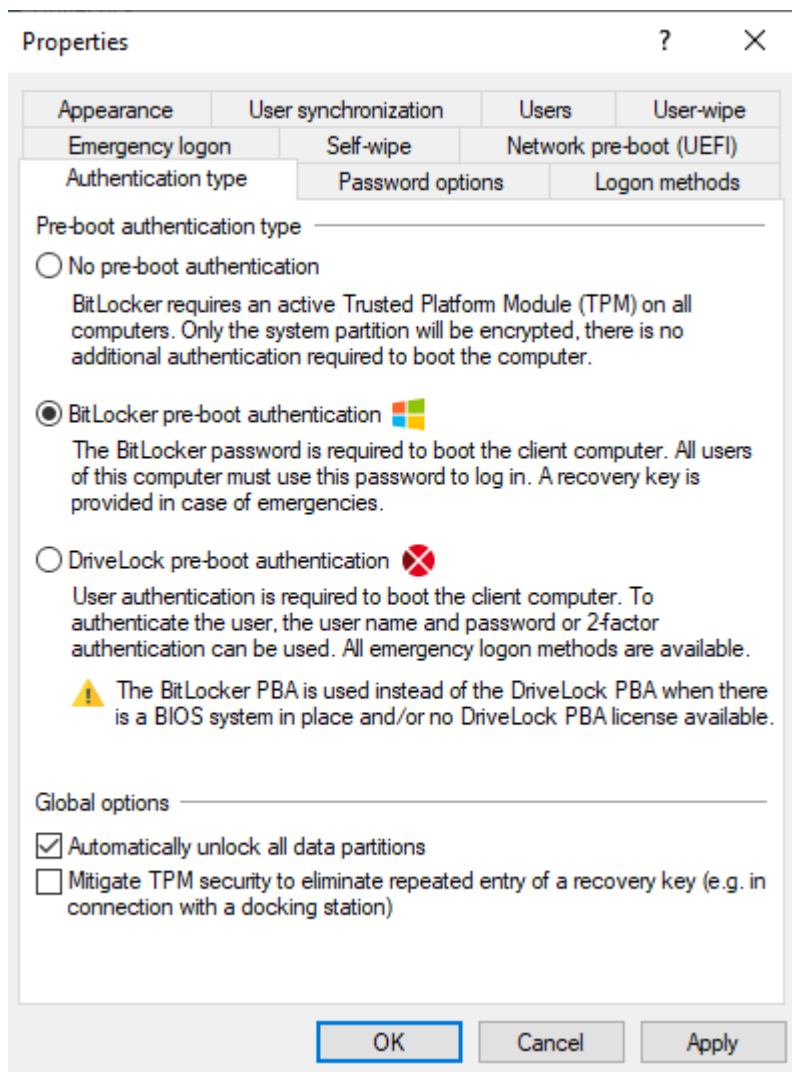
3.2.4 Pre-boot authentication settings

3.2.4.1 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**,
 - 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.
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 specify a password or to 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.

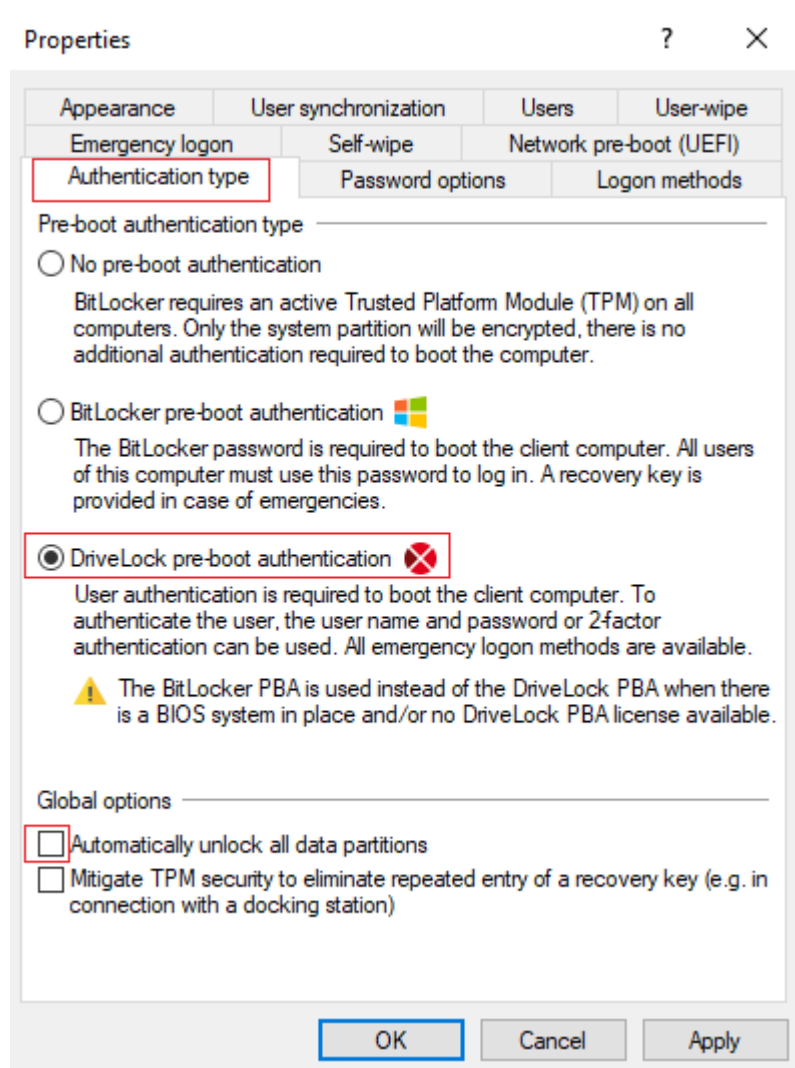
 Note: Unlike Microsoft, DriveLock unlocks the data partitions automatically for all users of a computer. The unlocking process by DriveLock BitLocker Management works independently of the Windows Bitlocker functionality; this means, for example, that the call `manage-bde -status` still returns "Automatic Unlock: Disabled" for drives that DriveLock unlocks.


4. The **Mitigate TPM security ...** option can be used to customize the TPM platform validation. 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.

3.2.4.1.1 Option: DriveLock pre-boot authentication

Open the **Pre-boot authentication settings** and select **DriveLock pre-boot authentication** 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.

3.2.4.2 Password options

There are different options available:

The screenshot shows the 'Properties' dialog box with the 'Password options' tab selected. The 'Valid for:' section shows 'BitLocker pre-boot authentication' is selected. Below this, there are fields for 'Predefined BitLocker password' with 'Password' and 'Confirm' input boxes. There are checkboxes for 'User cannot change password' (unchecked) and 'User must change password at first encryption' (checked). Below the second checkbox is a 'Maximum password age' spinner set to '0' days. A yellow warning icon and text state: 'The user must enter a password before the encryption will start.' Below this is a section for 'Back up user related recovery information' with an unchecked checkbox. Another section for 'Password must meet the following requirements:' is checked, containing sub-options: 'Allow only numbers' (unchecked), 'Allow numbers and Latin based characters' (unchecked), and 'Minimum password length' spinner set to '8' characters. Below this, it states 'A valid password must contain at least...' followed by four spinners: 'lower case letters' (1), 'upper case letters' (1), 'numbers' (1), and 'special characters' (1). There is also an unchecked checkbox for 'Treat numbers as special characters'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

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. You check the option **User must change password at first encryption** (see figure):
 - The user can specify a password, you do not enter a password here.
 - 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.

The options below **Password must meet the following requirements:** provide precise 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.

3.2.4.3 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 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 user name, 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.
- The option **Disable pre-boot authentication until first Windows logon** disables the PBA until the first user logs 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.

3.2.4.4 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 choose 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 text in the text box below the **Show pre-boot user information message** option.

3.3 Decryption

Decryption is triggered with a single [setting](#) that is specified in the **Harddisk encryption settings** on the **General** tab.

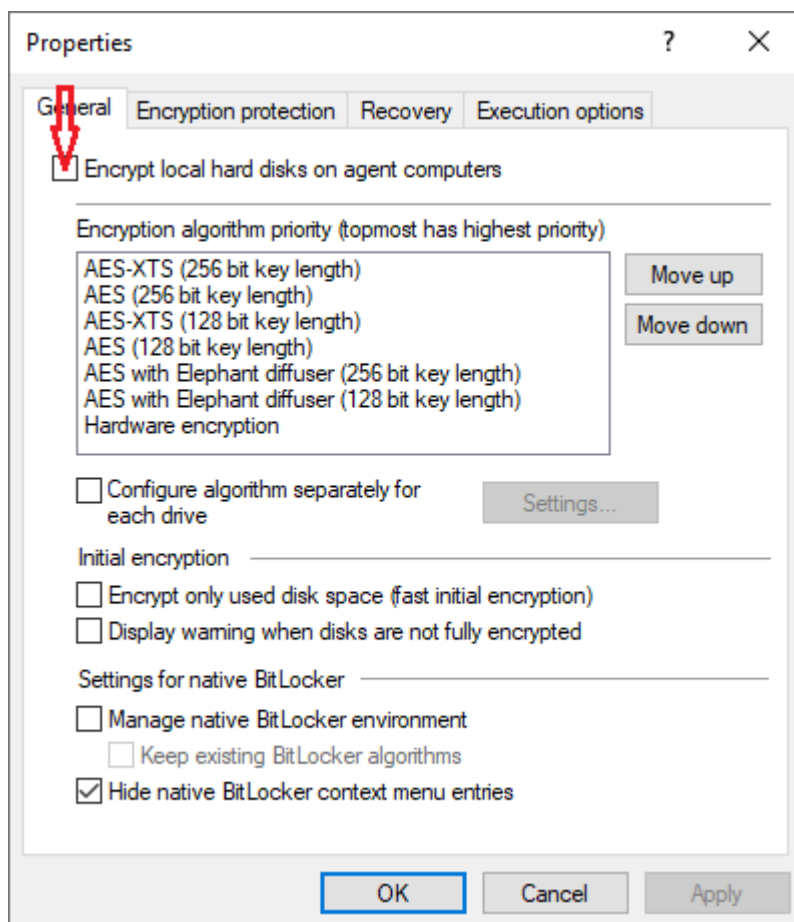
You can monitor the decryption process, just like the encryption process, in the DriveLock Operations Center (DOC).

The [Event report](#) (BitLocker events) also provides information on the decryption/encryption of individual computers.

3.3.1 Decrypting encrypted drives


To start decrypting encrypted drives, proceed as follows:

1. Open the respective BitLocker policy.
2. Open the **General** tab in the **Harddisk encryption settings** dialog.
3. Uncheck the **Encrypt local hard disks on Agent computers** option.

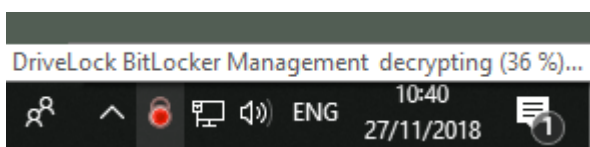


4. On the **Encryption protection** tab, set a value for the **Delay decryption by x** days setting. The default value is **3**, which means that decryption starts after 3 days.

Depending on the value you enter, the decryption will be 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.




3.4 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.

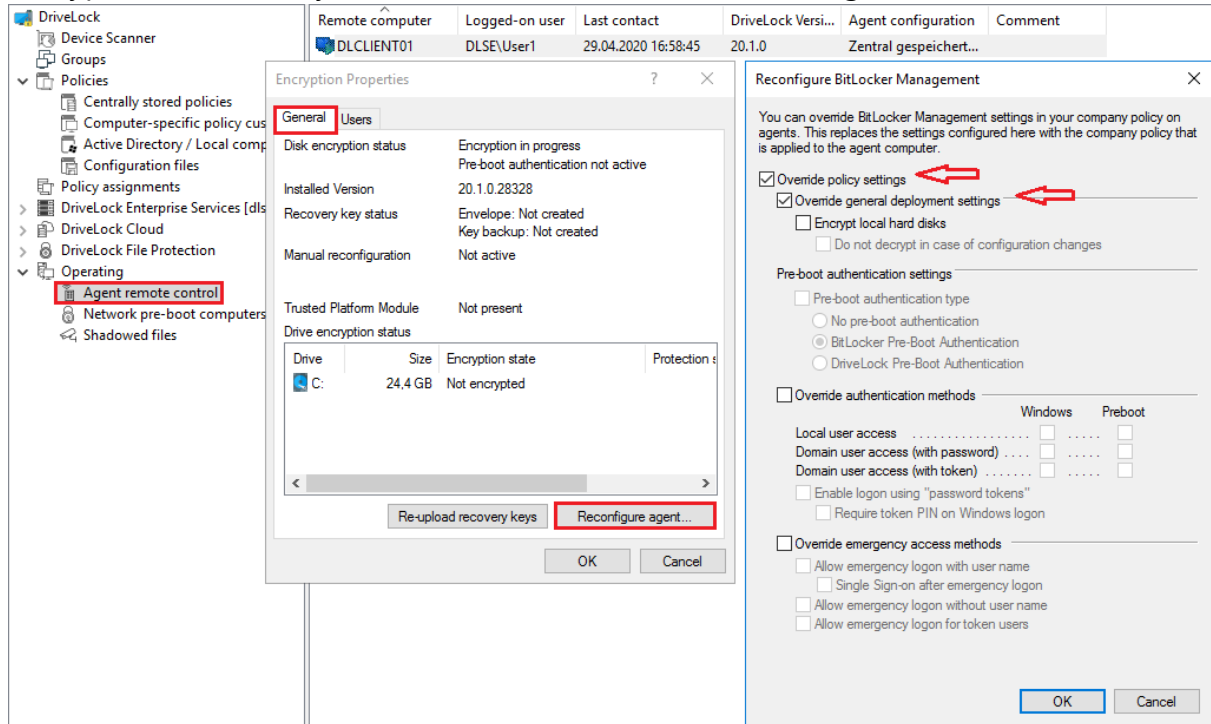
Please do the following:

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 checking the **Encrypt local hard disks** option, the encryption settings from the policy (e.g. algorithm or fast encryption) are applied.
7. If you select the **Do not decrypt in case of configuration changes** option, the corresponding policy option (Do not decrypt) is overwritten.
8. If you click **OK** now, your settings will be applied to the selected client computer with immediate effect.

3.5 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.
11.  Note: For more information on installing the DriveLock Agent or on policy management in general, please refer to the DriveLock Installation or Administration Guide at <https://drivelock.help/>.

3.6 Recovery

3.6.1 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.

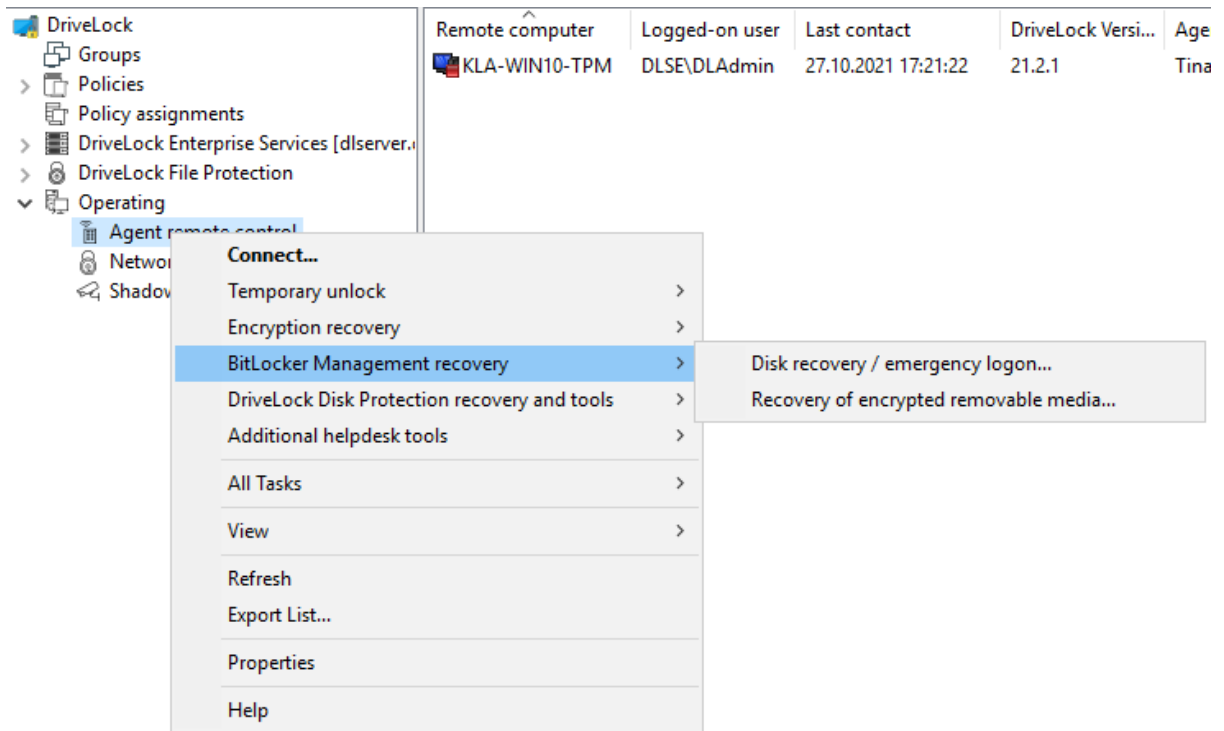


Note: The upload of the recovery data starts when all drives that are needed for encryption have begun encrypting.

In this case, please start the [recovery process](#). For this purpose, DriveLock offers you two possibilities:

1. In **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**.
Enter the certificate or certificate file information and the corresponding password.

2. In the **DriveLock Management Console**, select the **Operating** node and open the context menu for **Agent remote control** to select the **BitLocker Management recovery** menu item (see figure).

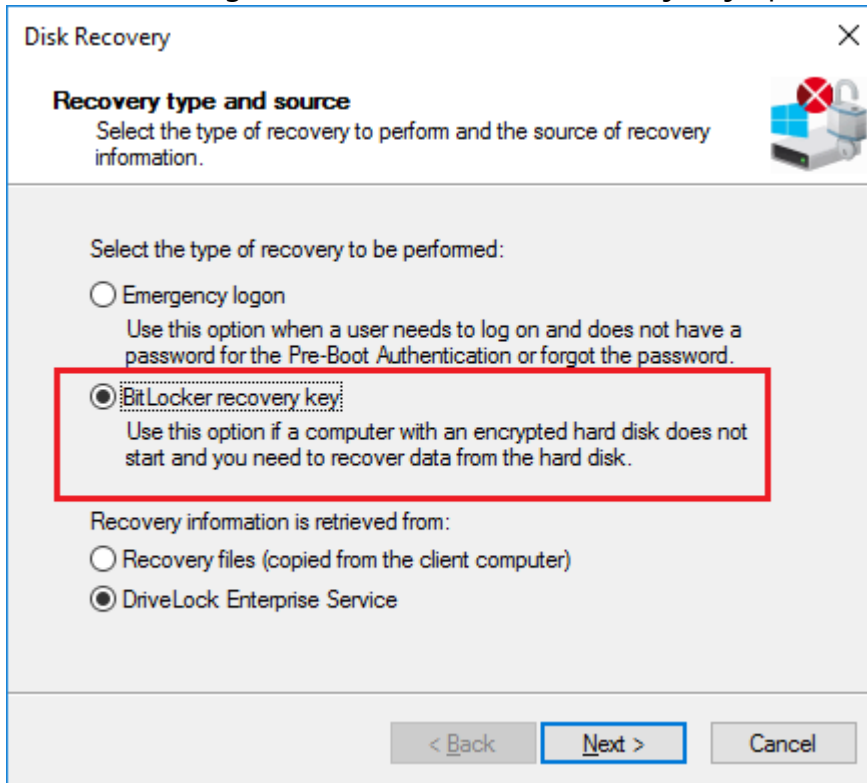


Here, the [recovery wizard](#) opens and guides you through the respective steps.

3.6.2 Recovery process


To recover access to an encrypted hard disk, Please do the following::

1. Open the Recovery Wizard (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**.

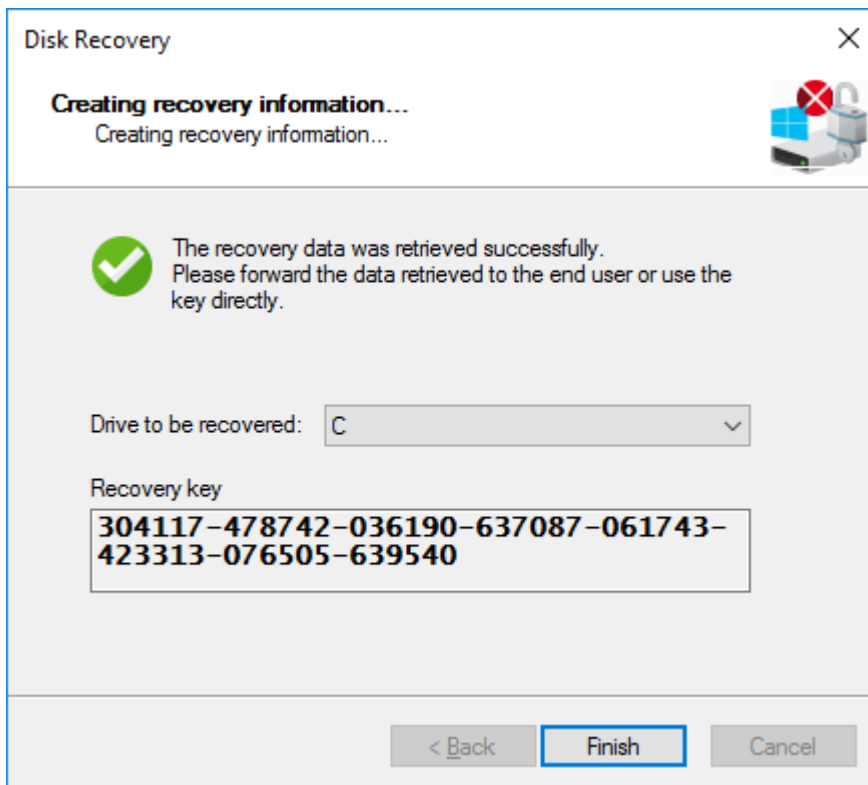
 Note: If you specified earlier in the encryption settings dialog that the recovery information resides in the file system, please enter the matching password for the private key here.

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.


 Note: The challenge-response feature will be fully available in the next version.

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.



8. Provide the user with 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.

3.7 Taking over native BitLocker

3.7.1 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. Note that a password entry is only required if the **User must change password** option has been enabled in the **Password options** dialog before. 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 creates new recovery keys when it integrates the native 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.

3.7.2 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.

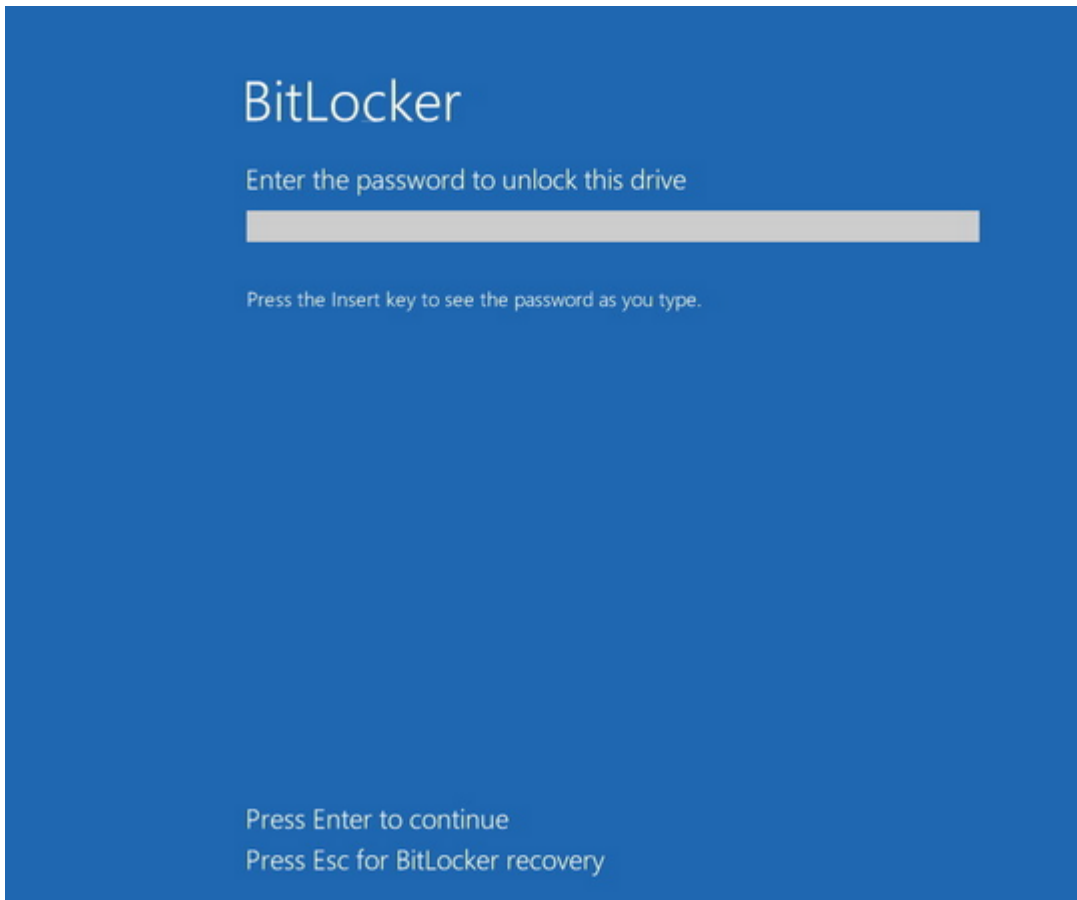
3.8 DriveLock Agent

3.8.1 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.



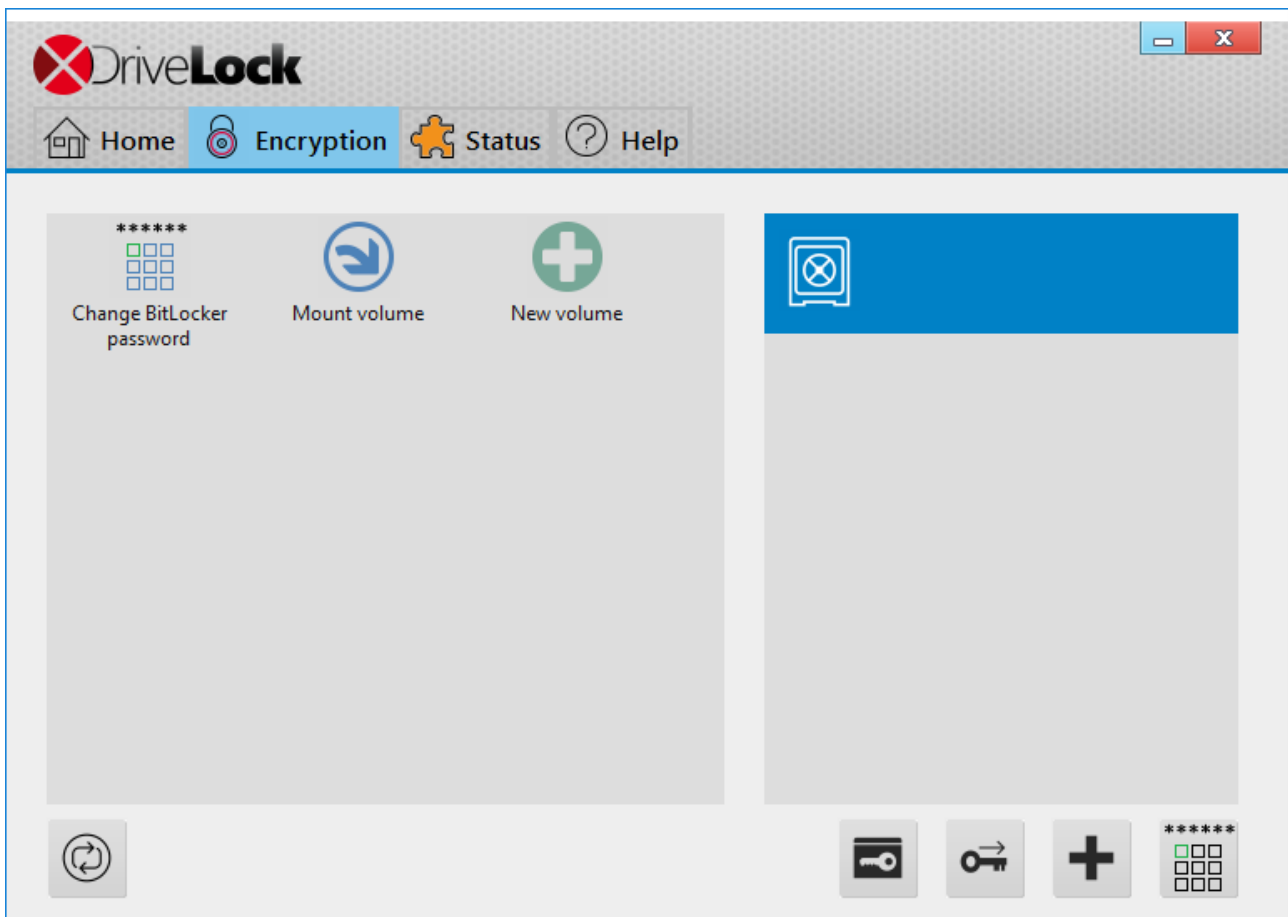
3.8.2 BitLocker Management on client computers (DriveLock Agent)

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.

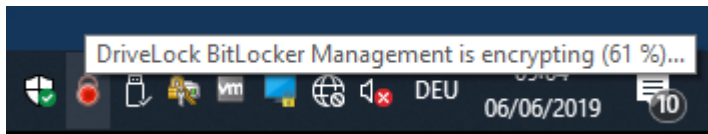


3.8.3 Encrypting client computers

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.

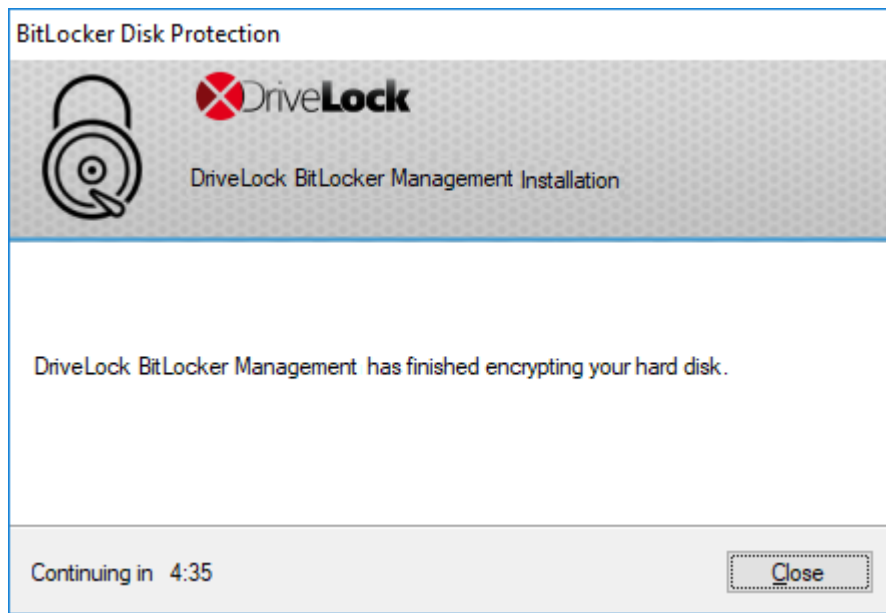


When the encryption process is finished, DriveLock issues the message described in item 5.

- 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.

3.8.3.1 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**.



3.8.4 Integrating data partitions with existing BitLocker

There are two settings in the **Password options** of the BitLocker policy that determine how to unlock data partitions that have been encrypted with native BitLocker and that are to be integrated in DriveLock BitLocker Management:

- 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.

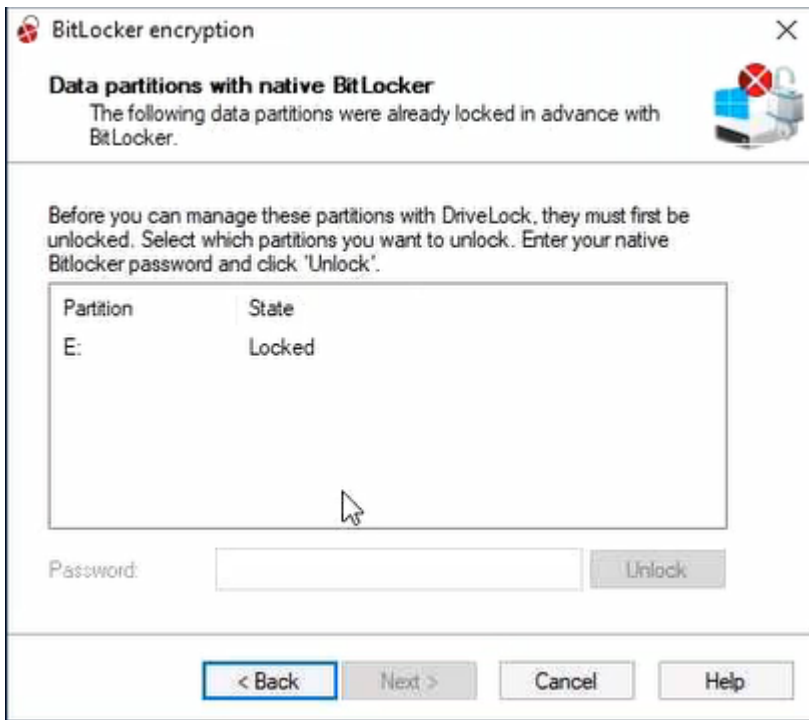


- The other wizard only contains information on how to integrate the native BitLocker environment:



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.

3.9 Tracing BitLocker actions

In the DriveLock Operations Center (DOC), [events](#) can be used to track all BitLocker actions.

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.

```

DlSvcBitLocker.log - Notepad
File Edit Format View Help
16.05.2019 10:29:55.318 1656 3540 Exit      0 CBitLockerController::GetLockedNativeBIDriveString (BitLockerWorkflow.cpp @2772)
16.05.2019 10:29:55.318 1656 3540 Entry    CBitLockerController::GetVolumeIndexDelta (BitLockerWorkflow.cpp @1315)
16.05.2019 10:29:55.318 1656 3540 Entry    CBitLockerController::GetSystemStatus (BitLockerController.cpp @2085)
16.05.2019 10:29:55.318 1656 3540 Entry    CBitLockerController::GetBUMStatus (BitLockerController.cpp @1888)
16.05.2019 10:29:55.475 1656 3540 Exit      1 CBitLockerController::GetBUMStatus (BitLockerController.cpp @2074)
16.05.2019 10:29:55.475 1656 3540 Exit      CBitLockerController::GetSystemStatus (BitLockerController.cpp @2113)
16.05.2019 10:29:55.475 1656 3540 Entry    CBitLockerController::VerifyBitLockerAlgorithm (BitLockerController.cpp @3716)
16.05.2019 10:29:55.475 1656 3540 Exit      1 CBitLockerController::VerifyBitLockerAlgorithm (BitLockerController.cpp @3758)
16.05.2019 10:29:55.475 1656 3540 Msg      CBitLockerController::GetVolumeIndexDelta: Drive C: is BitLocker encrypted but not managed by DriveLock. It will be adopted now. (BitLockerWorkflow.cpp @1461)
16.05.2019 10:29:55.475 1656 3540 Msg      CBitLockerController::GetVolumeIndexDelta: Protector TpmAndPin needs to be replaced by TpmAndPin for drive C:. (BitLockerWorkflow.cpp @1515)
16.05.2019 10:29:55.475 1656 3540 Entry    CBitLockerController::VerifyBitLockerAlgorithm (BitLockerController.cpp @3716)
16.05.2019 10:29:55.475 1656 3540 Exit      1 CBitLockerController::VerifyBitLockerAlgorithm (BitLockerController.cpp @3758)
16.05.2019 10:29:55.475 1656 3540 Msg      CBitLockerController::GetVolumeIndexDelta: Drive E: is BitLocker encrypted but not managed by DriveLock. It will be adopted now. (BitLockerWorkflow.cpp @1461)
16.05.2019 10:29:55.475 1656 3540 Msg      CBitLockerController::GetVolumeIndexDelta: Protector Passphrase needs to be replaced by Passphrase for drive E:. (BitLockerWorkflow.cpp @1515)

```

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).

4 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: Please also note: When installing a version 2022.2 agent, a check is made to see if there is an active Legacy BIOS PBA on the system. In this case, no update or installation of the agent will be performed.

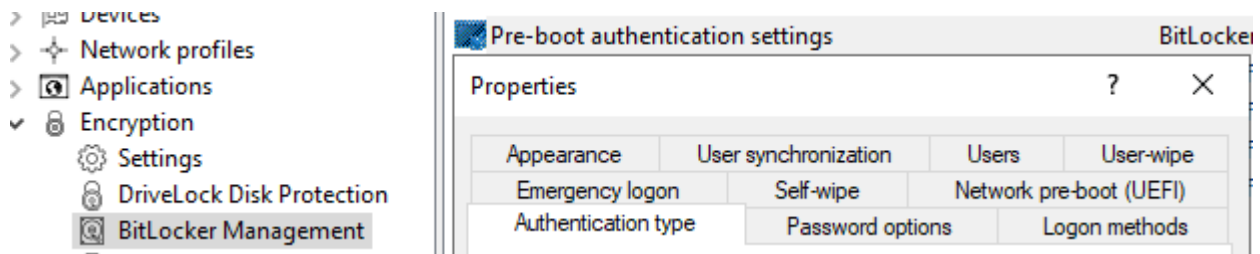
DriveLock pre-boot authentication offers you a number of benefits:

- 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

4.1 Pre-boot authentication settings

Pre-boot authentication 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:



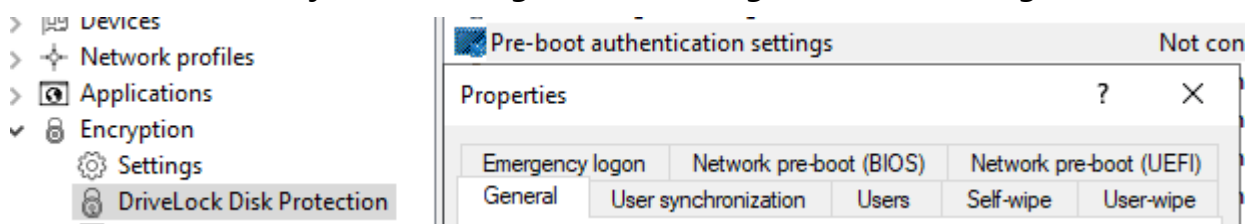
[Logon methods](#)

[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](#)

4.1.1 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 option **Automatically add Windows users to pre-boot authentication on logon** 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.

4.1.2 User synchronization

The option **Synchronize Active Directory users to pre-boot authentication** is not enabled by default because AD users are automatically entered into the PBA database when 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 <code>DlFdeUser.exe</code>
Policy	User was created via policy - and will be synchronized/removed with policy changes.
Windows login	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.

4.1.3 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.

4.1.4 Network pre-boot (UEFI)

For more information on this tab, please click [here](#).

4.1.5 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.

4.1.6 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 connect to the corporate network on a regular basis.

To configure self-wipe, select the **Self-wipe** tab, check **Enable self-wipe when computer is offline** and configure the appropriate settings as described in the dialog.

After the specified offline time expires, DriveLock deletes the PBA database.

4.2 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](#)

4.2.1 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.

4.2.2 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.

4.2.3 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: Note that 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.

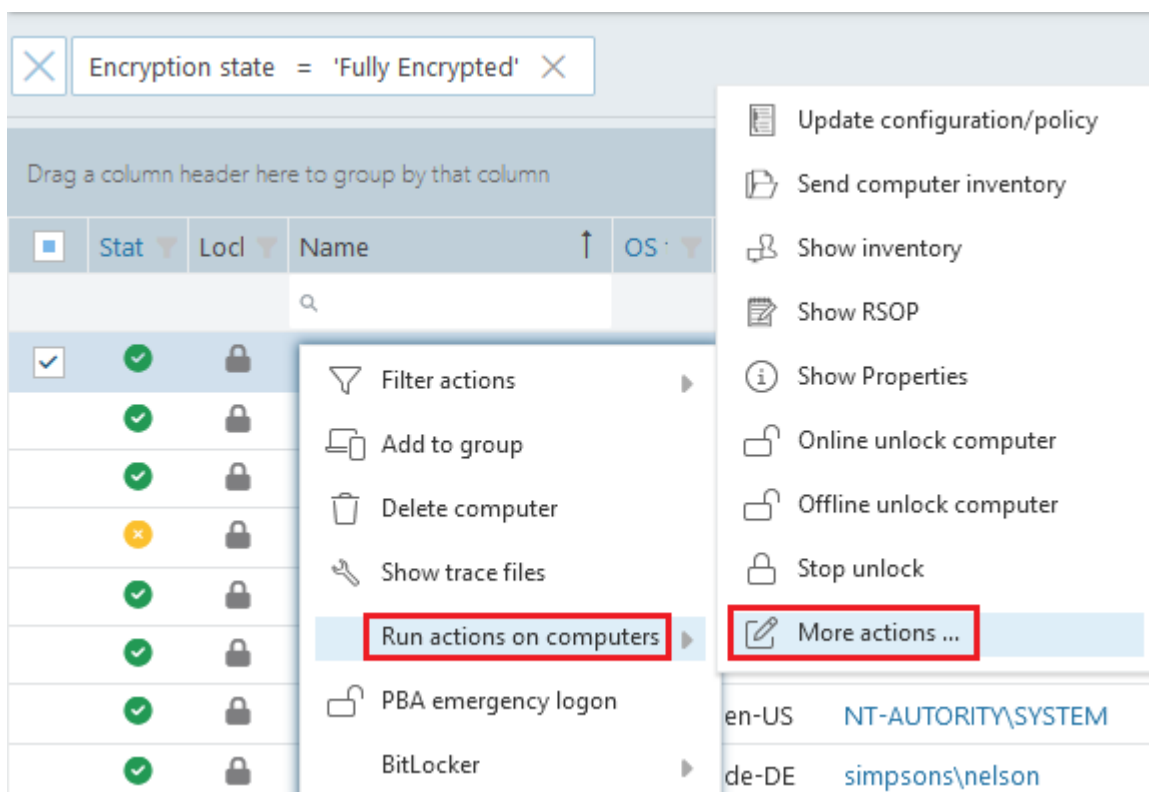
4.3 PBA settings in the DriveLock Operations Center (DOC)

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.

In the DOC, open the **Encryption** dashboard. 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 **Computers** 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:

Pre-boot authentication (PBA)

☒ Suspend PBA☐ In the time from

-

☐ For specified number of restarts

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.

4.4 Override policy settings (DriveLock PBA)

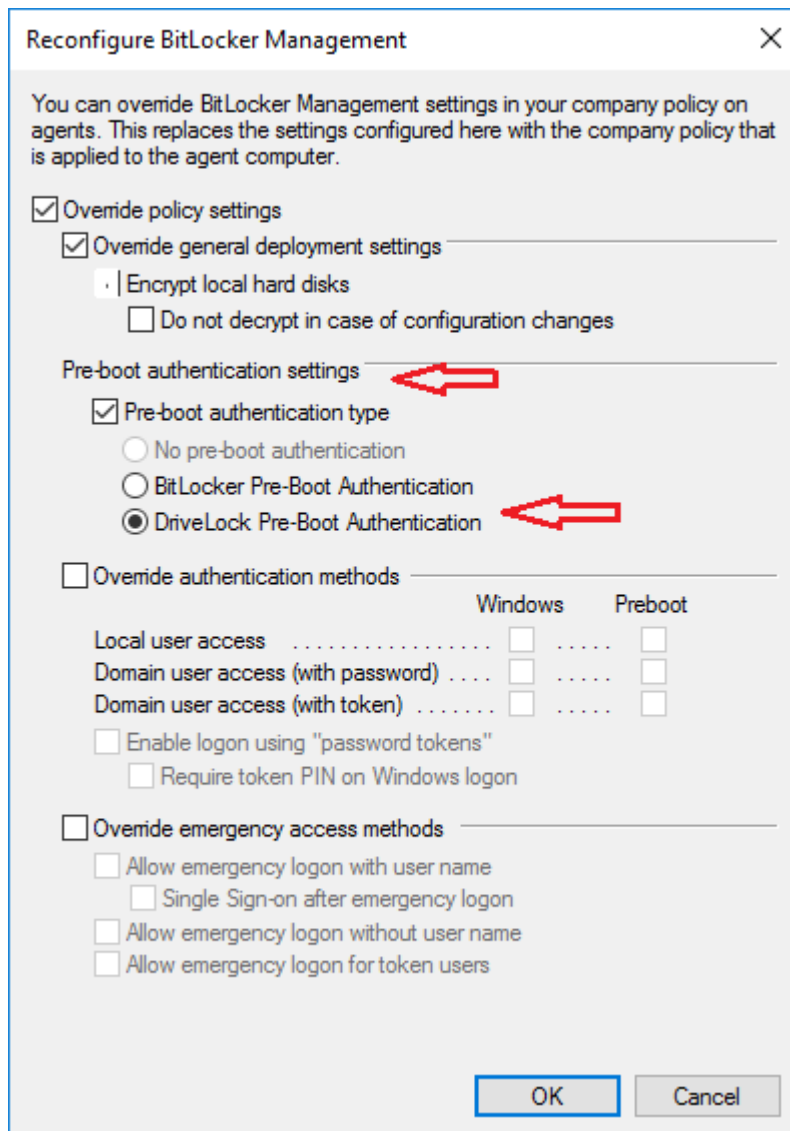
To disable specific pre-boot authentication settings on individual client computers, you can override the respective policy settings.




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 menu item **Disk encryption properties....**
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.

4.5 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 **Server connections** subnode in the **Global settings**.

4.5.1 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 the DriveLock pre-boot authentication is used for both features.

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 auto-logon.



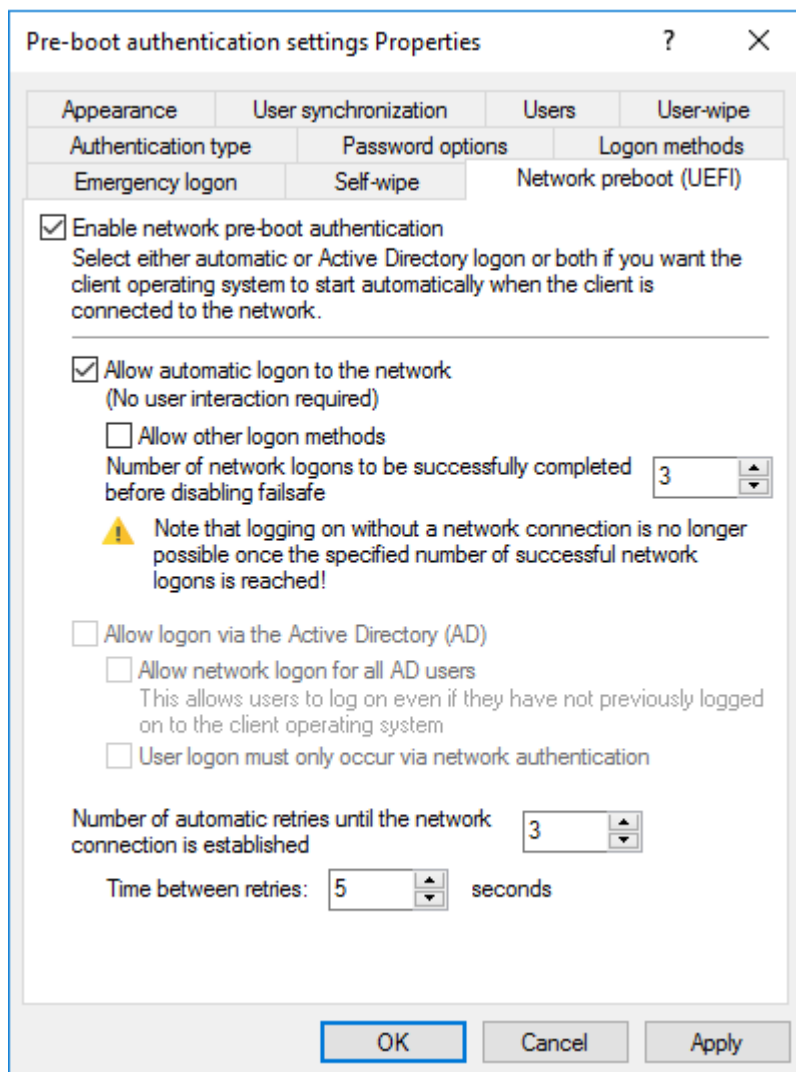
Warning: This option can only be set initially, it has no effect on systems that are already running. For safety reasons, make sure not to select a number too high.

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.

4.5.2 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**.

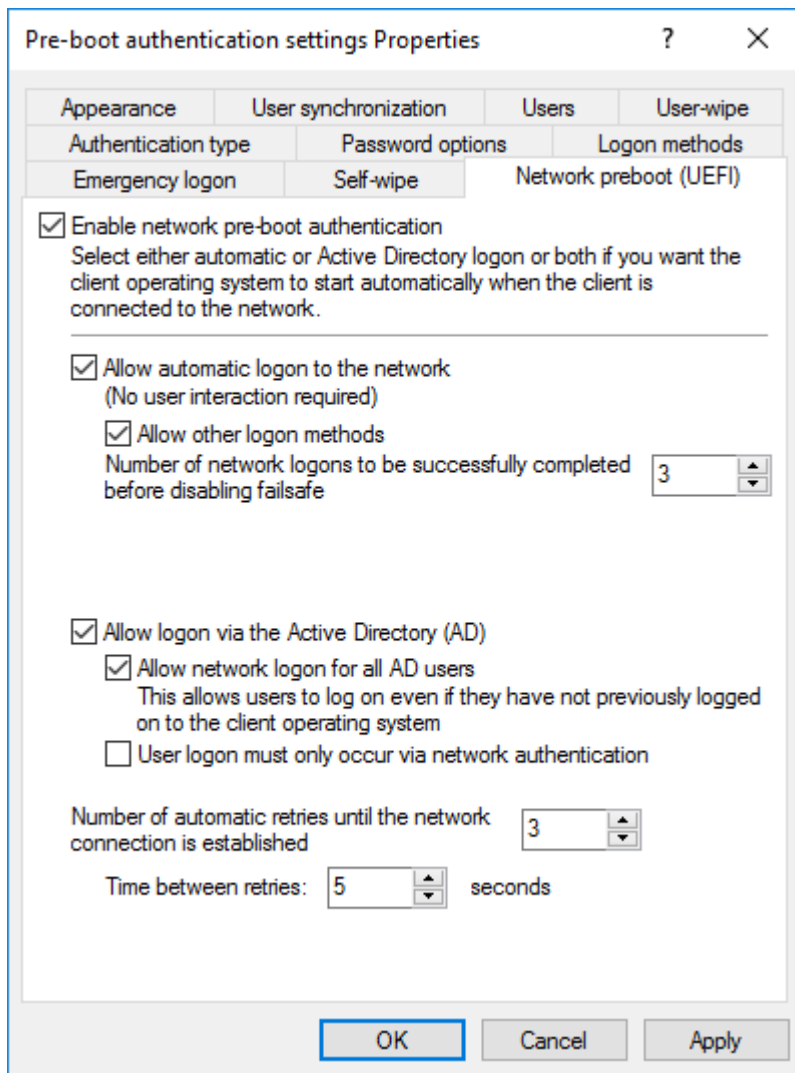
4. Leave the default value for failsafe at 3. This way you can make sure that only after 3 successful network logins there is no other way to log on. This option is intended for both testing purposes and as a failsafe.
5. Leave the default value 3 at **Number of automatic retries until network connection is established**.
6. Likewise, you can leave the pauses between retries at 5 seconds.
7. **Apply** your changes by clicking **OK**.

4.5.3 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):



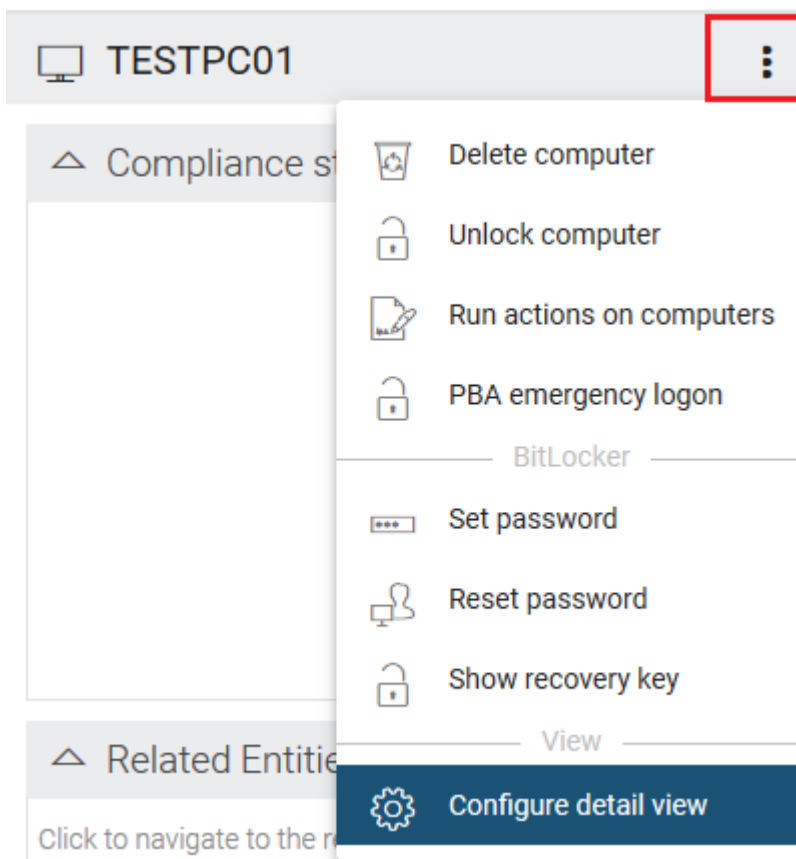
1. Select the basic setting **Enable network pre-boot authentication**.
2. Select **Allow automatic logon to the network**.
3. Keep the check mark at **Allow other logon methods**.
4. Leave the default value for failsafe at 3. This way you can make sure that only after 3 successful network logins there 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**.


4.5.4 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 view.




4. Select **Network Pre-Boot Authentication** and check **Show** and optionally **Expand** (depending on whether you want to display the item open right away).
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.

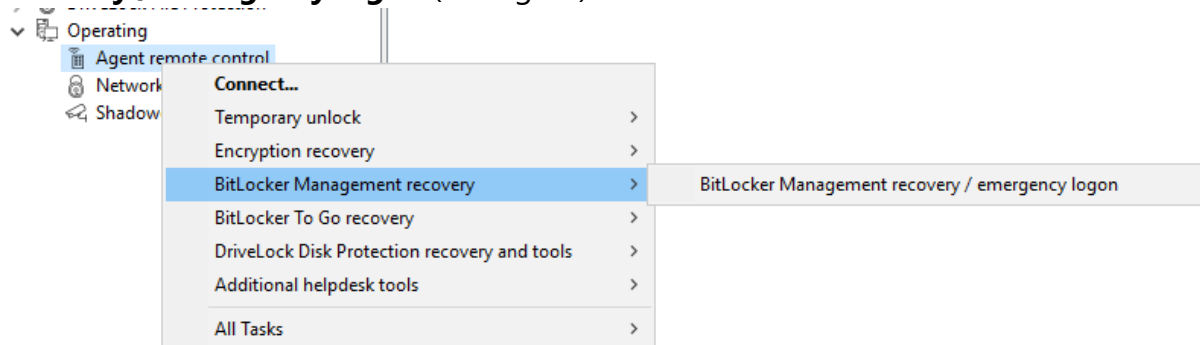
4.6 Settings for emergency logon

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.

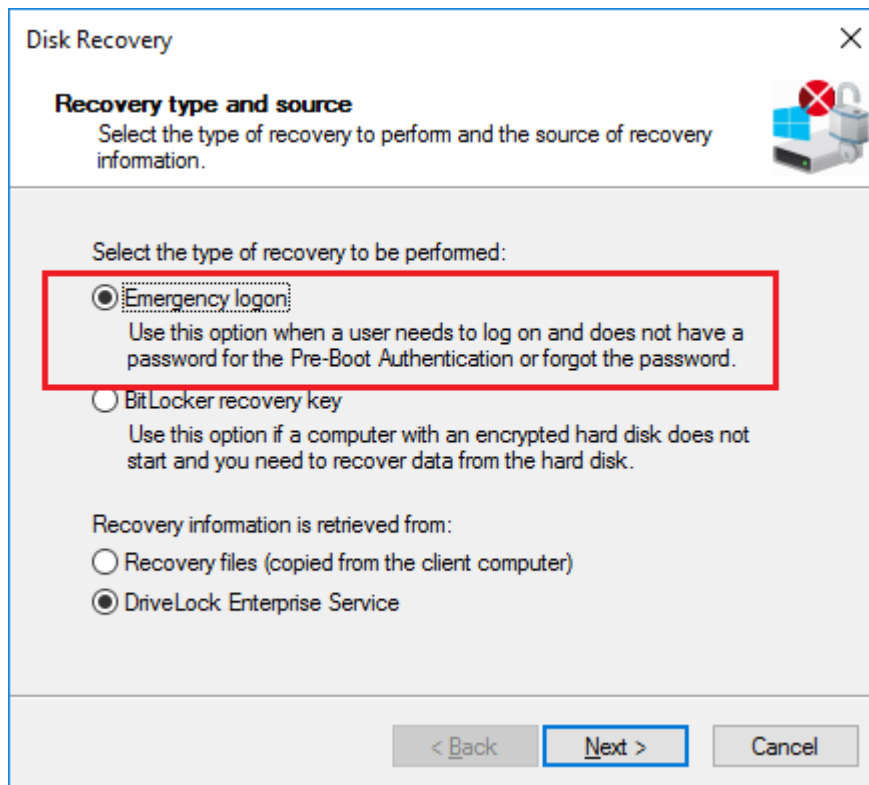
 Note: For more information on the interaction between administrator and end user, click [here](#).

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 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](#). 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.

Disk Recovery

Specify recovery code
Select user to enable to log on and type the recovery code from the PBA screen.

Users must initiate a request for a one-time password from the Pre-Boot Authentication (PBA) screen by selecting "Emergency" or pressing F3. Then after entering the user name a recovery code is generated.

☐ Recovery for specific user

Recovery code as specified by the user


Z+SGJ **N4G-R** **Y+3**

< Back **Next >** Cancel

7. Click **Next** to generate the response code.

Disk Recovery

Recovery completed
Please review the results of the recovery operation.

 The user must enter the Response Code on the Pre-Boot Authentication screen in the "Enter response below:" field and then press ENTER.

Response code

CZ2C. NQ60F RZ* K+ JW3VR KF*CK 3 ...

< Back **Finish** Cancel


8. Tell the user the **response code**.
9. Click **Finish**.

4.7 DriveLock Agent

4.7.1 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.

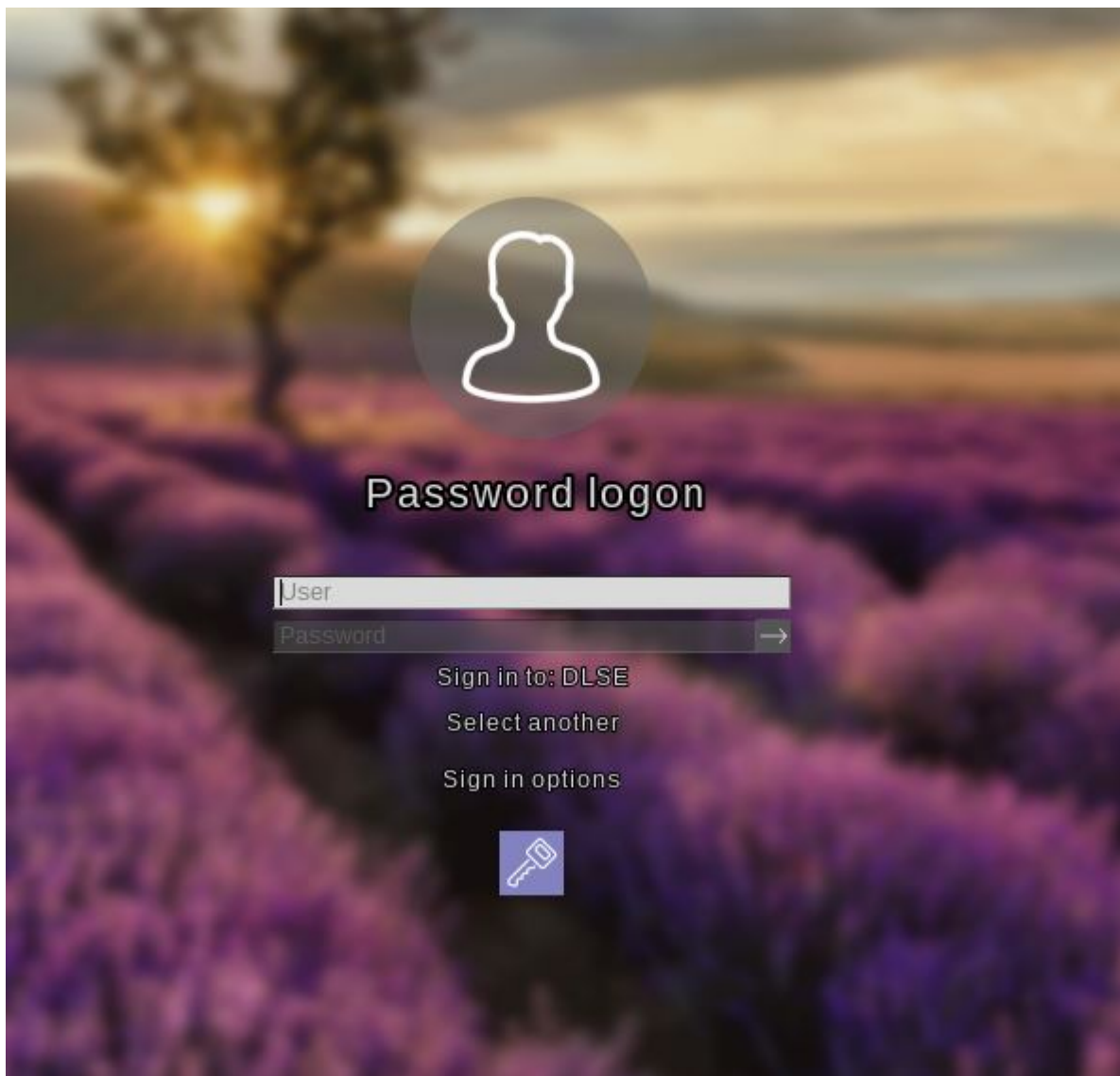


4. At the same time the encryption starts; restarting or shutting down the computer is now possible at any time.

4.7.2 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 to ensure successful authentication 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.

4.7.3 Network pre-boot authentication

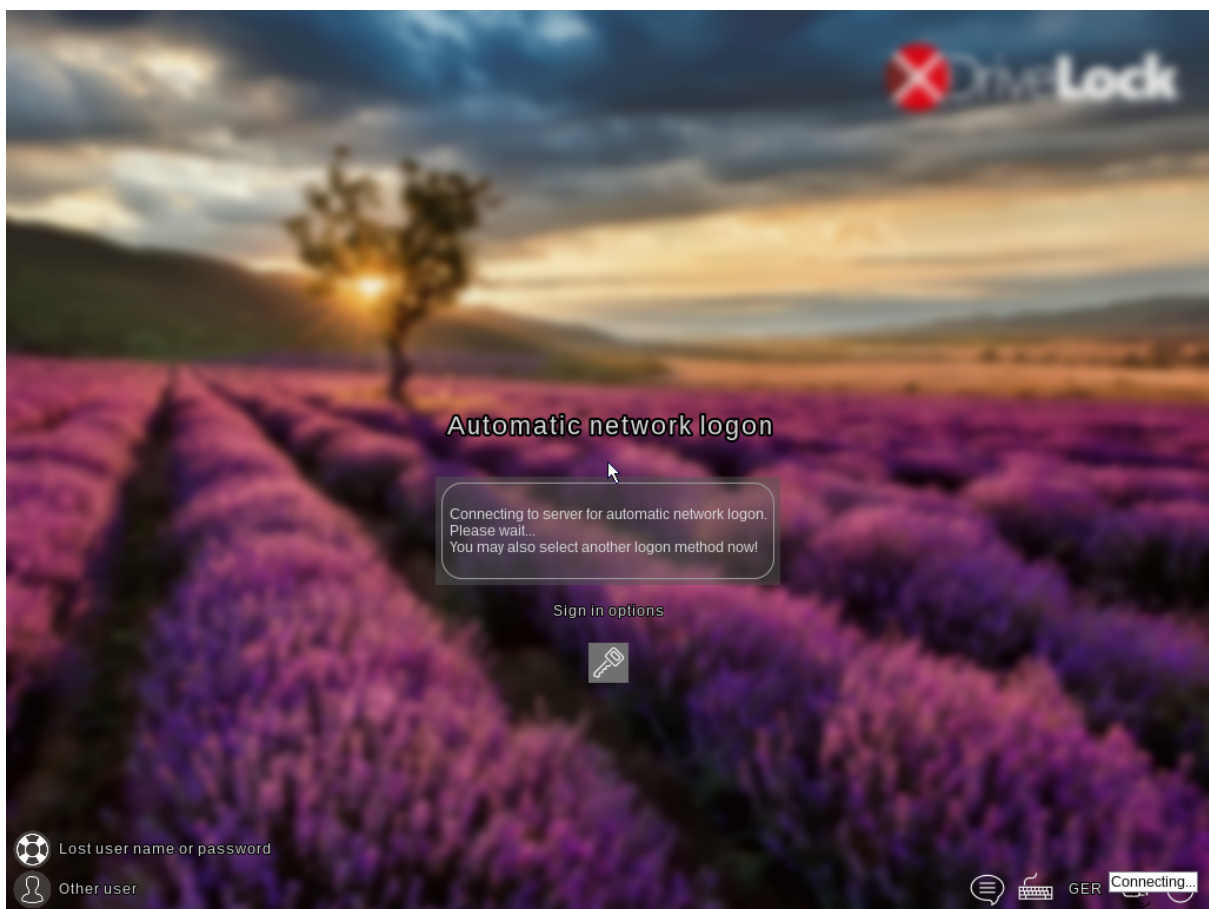
Once the policy containing the [network PBA settings](#) is assigned to the client computer and the computer is started, the following scenarios are possible:


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.

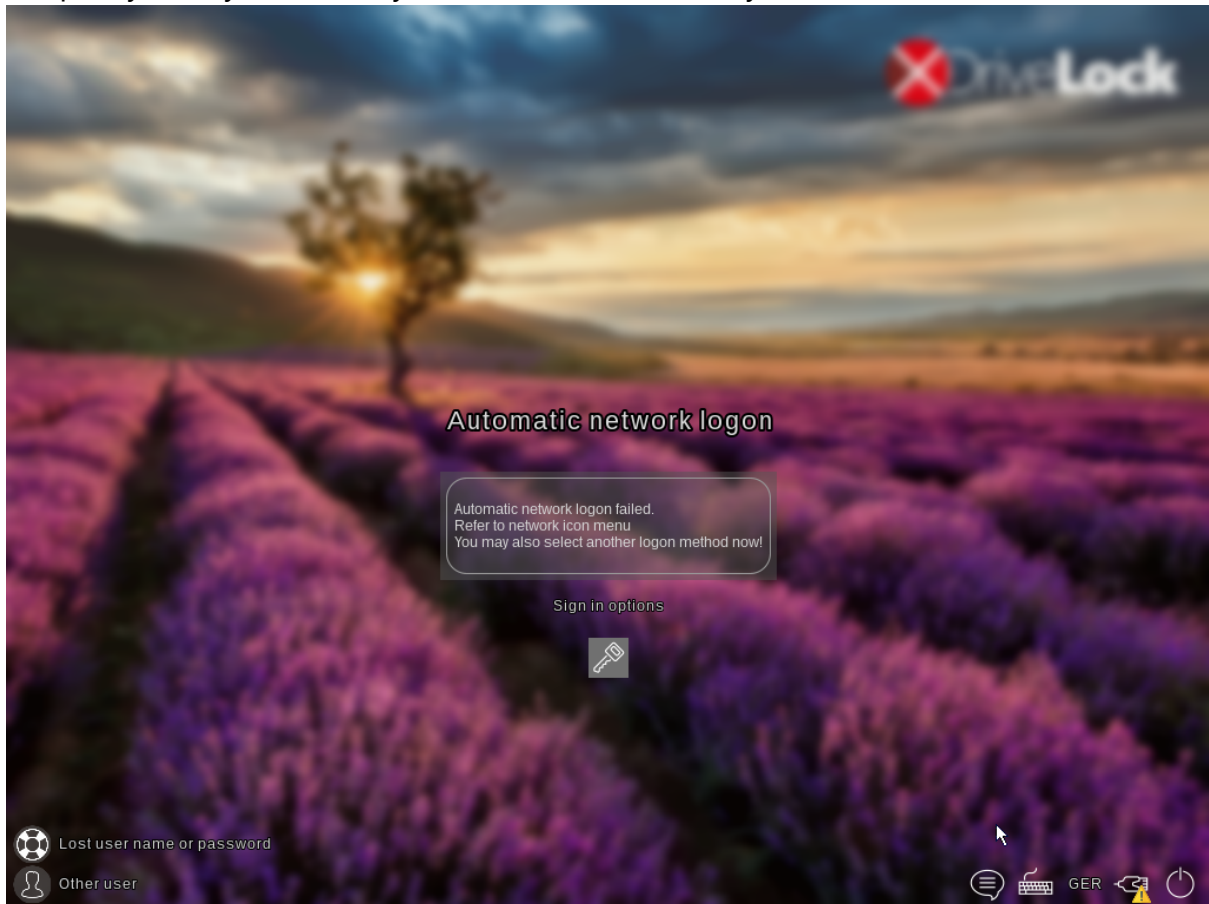


 Note: By clicking the key icon within 10 seconds it is possible to switch to the PBA login mode with user name and password entry, if enabled.

The next step shows the Windows login screen where the Windows credentials are entered.

2. The client computer cannot connect to the corporate network

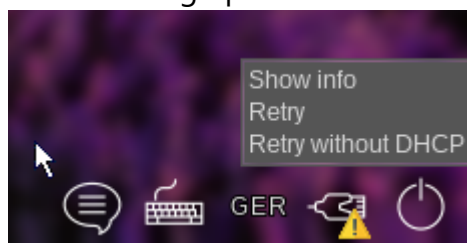
As soon as the client computer is booted, the notification indicating that DriveLock pre-boot authentication is active also appears. However, the login screen now indicates that the automatic network login has failed. Depending on the configuration in the policy, the system will try to connect automatically 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.

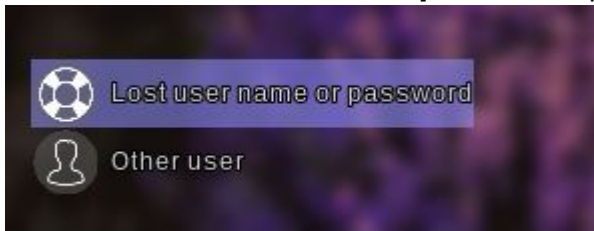
4.7.4 Emergency login with recovery code

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.

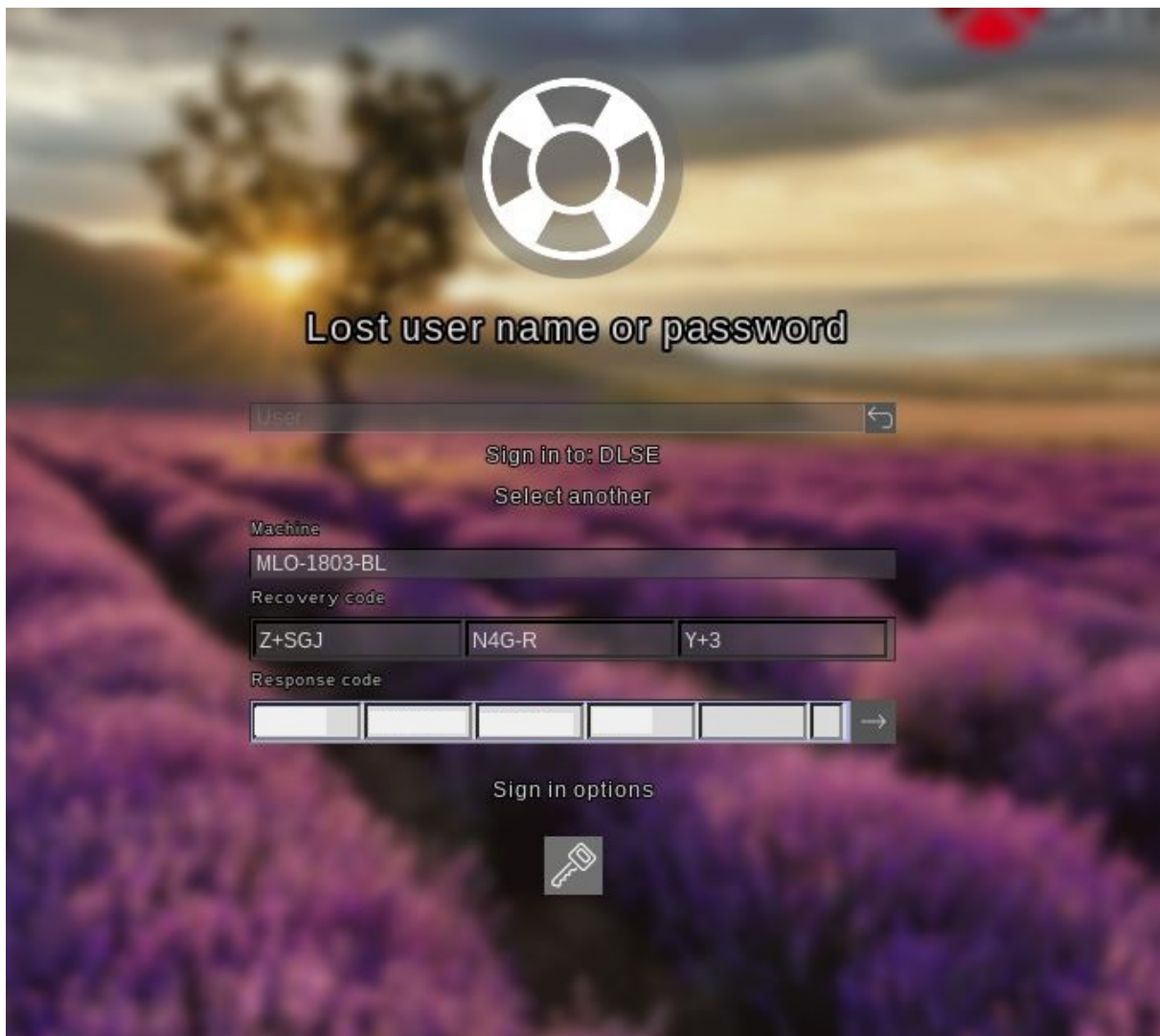
User and administrator now perform the following actions:

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.



Lost user name or password

User


Sign in to: DLSE
Select another

Machine
MLO-1803-BL


Recovery code
Z+SGJ N4G-R Y+3

Response code

Sign in options



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!

4.7.5 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:

- Automatically: **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.

4.7.6 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:

The screenshot shows a pre-boot authentication window with a header bar containing five buttons: 'Passwort [F1]' (with a key icon), 'Smartcard [F2]' (with a smartcard icon), 'Notfall [F3]' (with a lifebuoy icon), 'Einstellungen [F4]' (with a gear icon), and 'Hilfe [F5]' (with a question mark icon). Below the header, the text 'Anmeldung mit Benutzername, Domäne und Passwort.' is displayed. The main area contains three input fields: 'Benutzername:' with an empty text box, 'Passwort:' with an empty text box and an 'Anzeigen' button to its right, and 'Domäne:' with a dropdown menu showing 'PMCT'. At the bottom right, there is an 'Anmelden' button.

Passowrd [F1] Smartcard [F2] Emergency [F3] Settings [F4] Help [F5]

Login using user name, domain name and password.

User name:


Password: Show

Domain name: PMCT

Login

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: Note that in the 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:		<input type="text"/>		
<input type="button" value="Anmelden"/>				

 Password [F1]	 Smartcard [F2]	 Emergency [F3]	 Settings [F4]	 Help [F5]
Login using smart card (token) and PIN.				
Pin:		<input type="text"/>		
<input type="button" value="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.

4.8 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 about the encryption status, such as the number of encrypted 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>
```

4.9 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 and/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

5 DriveLock BitLocker To Go

DriveLock BitLocker To Go includes the following features:

- Enforced encryption of external USB storage media with BitLocker To Go
- 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

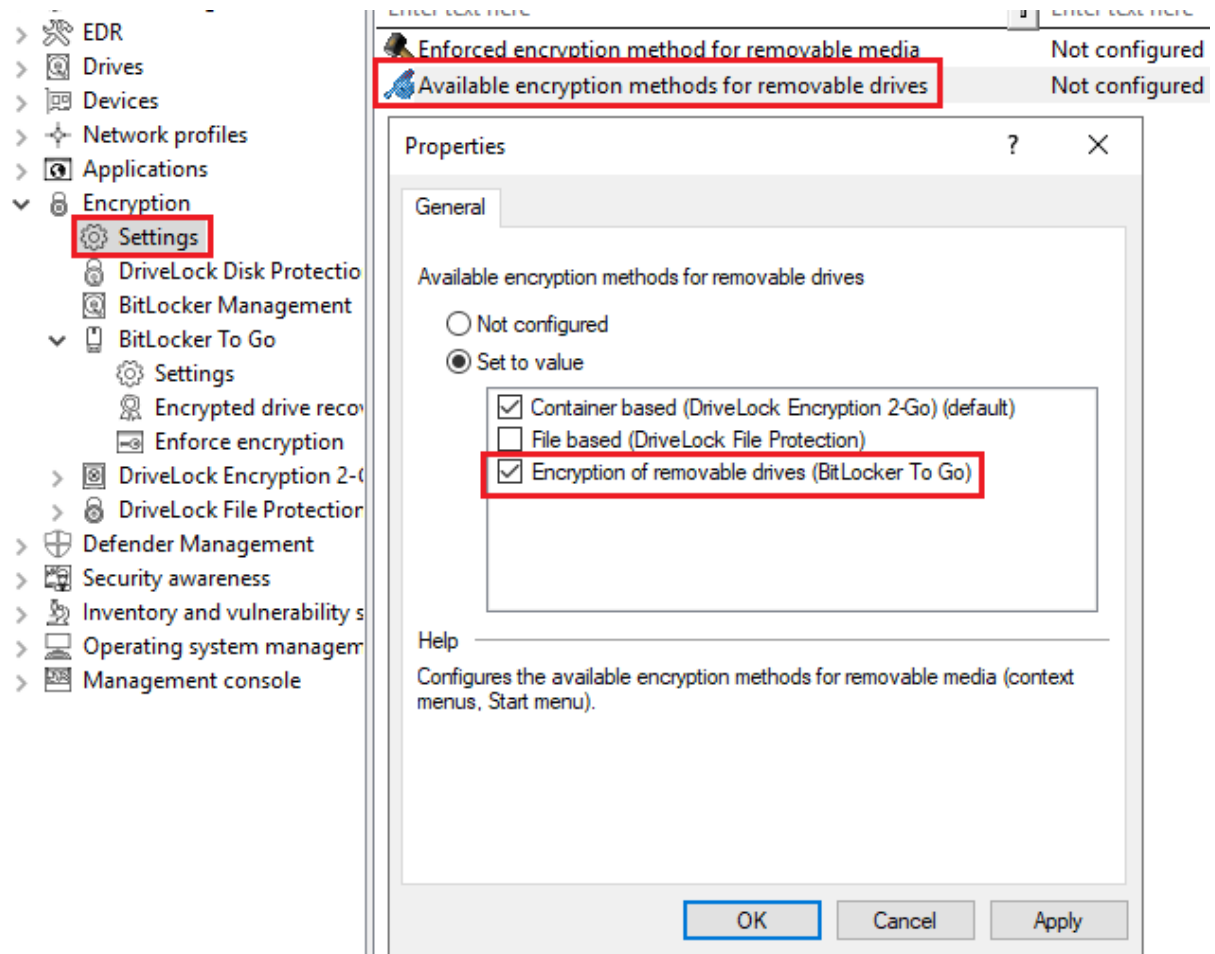
5.1 Requirements for BitLocker To Go

Before you can use BitLocker To Go to encrypt external USB storage devices or drives, two conditions must be met:

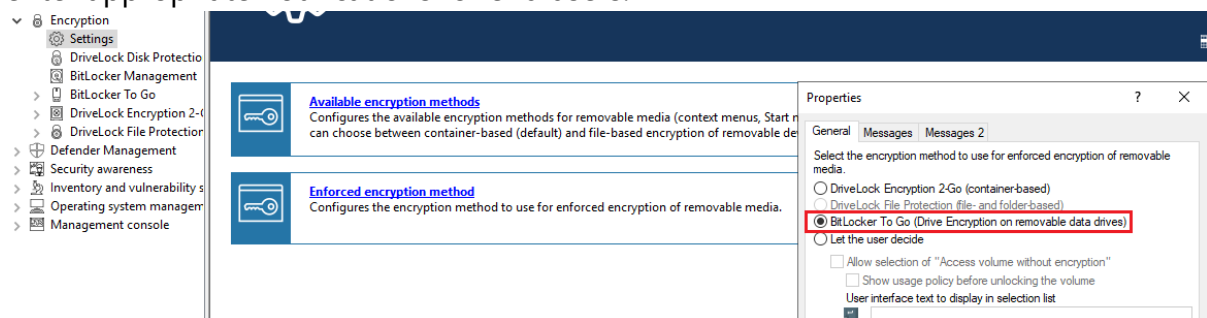
1. You have a valid license for the product. For licensing, proceed as described in the chapter [Licensing BitLocker Management](#).
2. You select BitLocker To Go as the encryption method in the general encryption settings.

Proceed as illustrated in the figure.

Under **Available encryption methods for removable drives**, select the **Encryption of removable drives (BitLocker To Go)** option.



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.



5.2 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 \(certificate-based recovery\)](#)
- [Administrative password rule](#)

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.

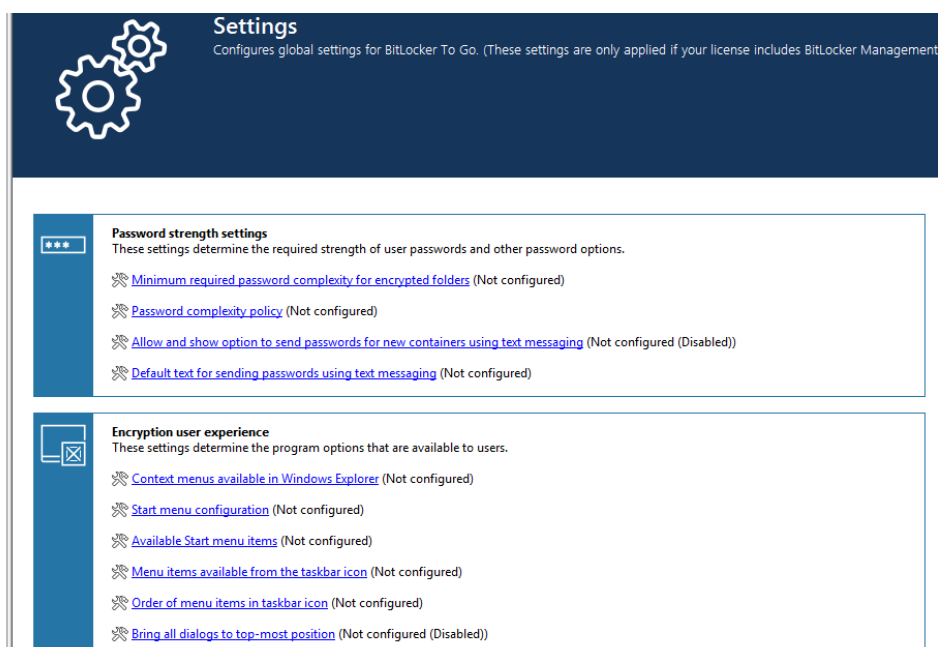
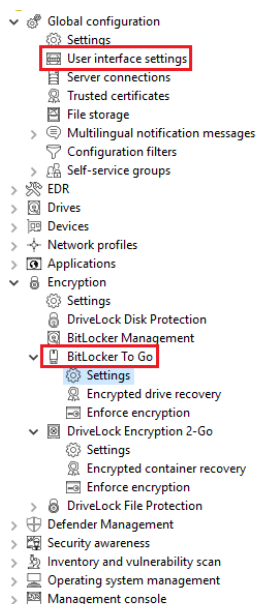
The next time a user connects a USB storage device to the DriveLock Agent, an unencrypted drive is immediately encrypted. DriveLock walks users through the encryption process. USB storage devices that have been encrypted before will be recognized in the corporate network, won't be re-encrypted and can 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\$)

5.2.1 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.
 - For more settings, see **Password strength** and **Encryption user experience:**
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.

For information about the effects of the settings, see [BitLocker To Go on the DriveLock Agent](#).

5.2.2 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

5.2.2.1 Administrative password

Use a central administrative password for accessing encrypted removable storage devices.

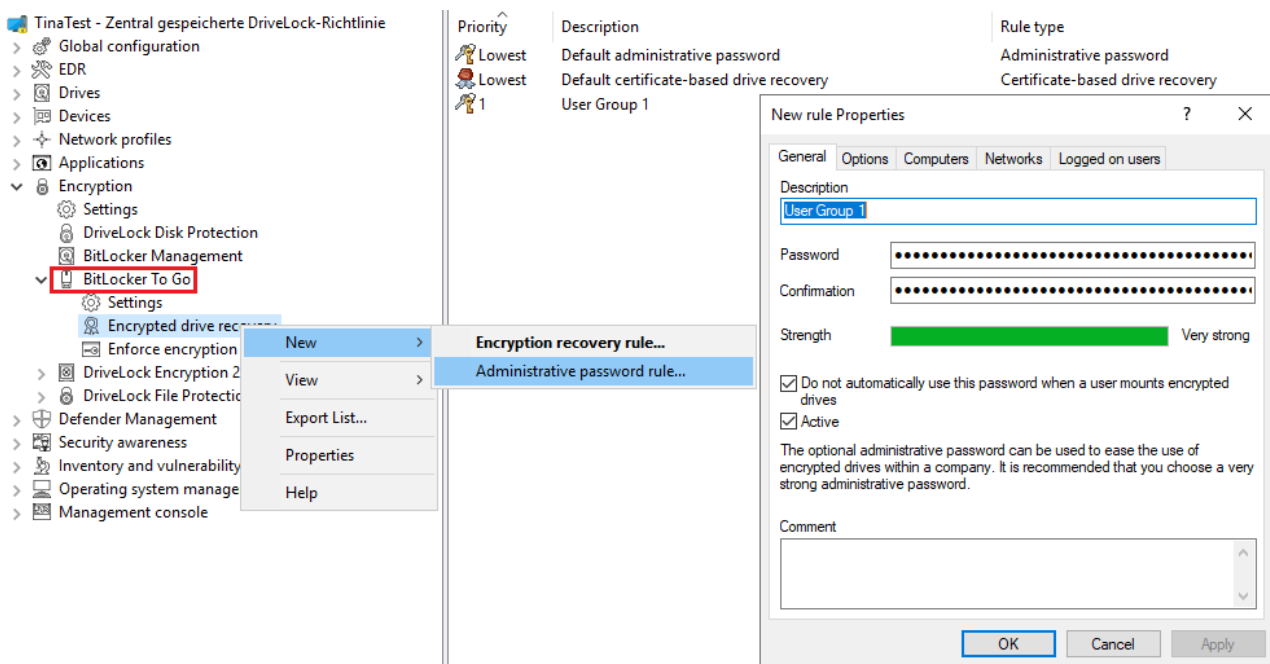


Note: Ensure that the administrative password is complex enough.

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 administrative password rule, select **Encrypted drive recovery**, open the context menu, click New and then **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.



5.2.2.2 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. See chapter [Create encryption certificates](#) for more information.

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.

5.2.3 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.
- **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: Note that this option only works if you have specified an administrative password in the **Encrypted drive recovery** section.

- **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.

5.3 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.

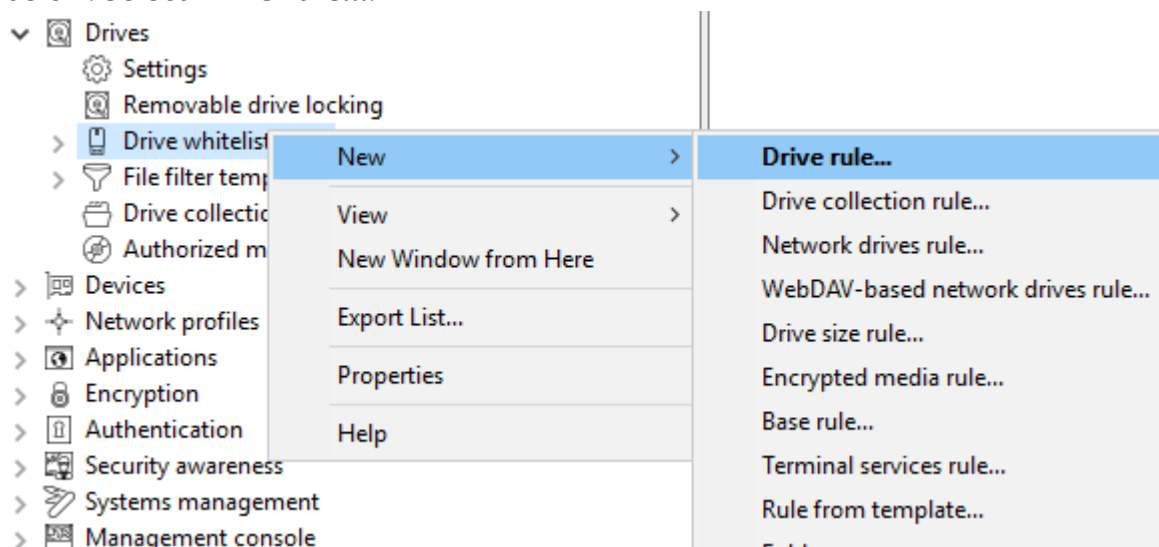
1. Create a policy (or open an existing one) that contains the settings related to BitLocker To Go.

 Note: Verify that you have licensed BitLocker Management in this policy and that the option is selected in the **Licensed Computers** section.

- 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.

- Select **Available encryption methods**.
- 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.
- Open the **Drives** node. Keep the default value **Not configured (locked)** in the **Removable drive locking** settings for **USB bus connected drives**.
- Open the context menu from the **Drive whitelist rules** sub-node, see the figure below. Select **Drive rule...**



- Create a drive rule for the corresponding USB drive. To see how this works, click [here](#).
- Next, open the **Encryption** node again and then the **BitLocker Management** sub-node. Here you go directly to **BitLocker To Go** and select the **Encrypted drive recovery** option.
- Here we have already created two standard rules that cannot be deleted.
 - First, open the **Administrative password** rule. Specify a complex administrative password.

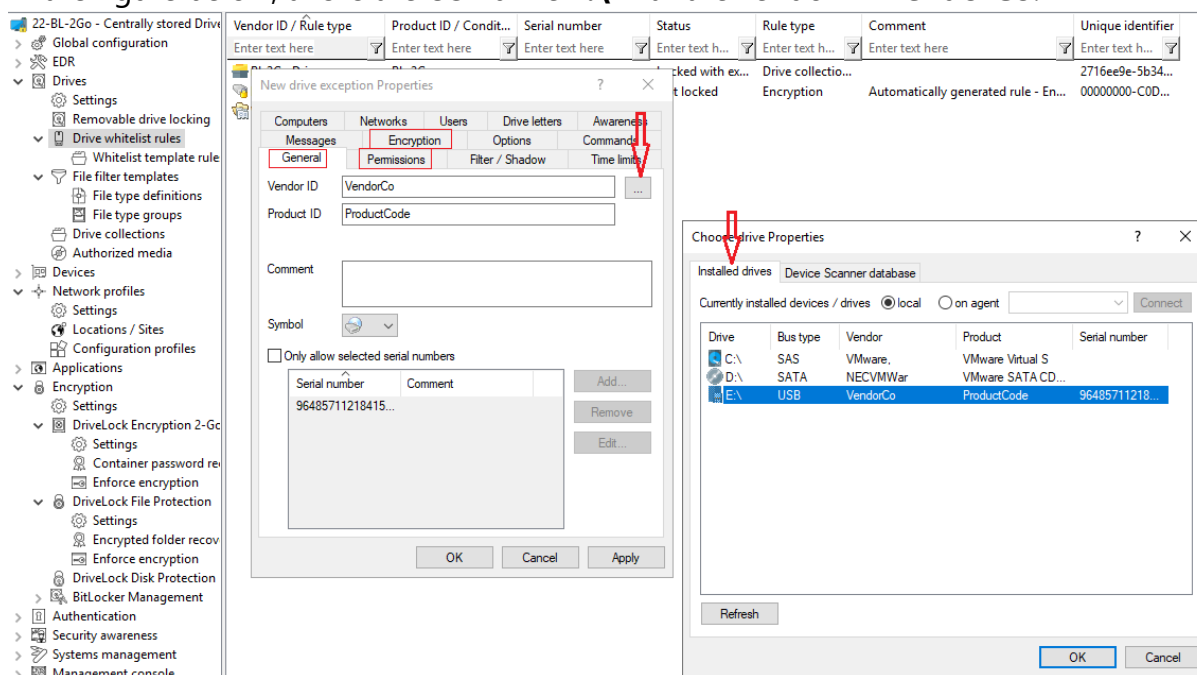
- Second, open the rule for **certificate-based recovery**. You will need to specify a certificate, as this is required for recovery. Either create a new certificate or select an existing one. Save your settings and close the dialog.
- Next, open the context menu of the **Enforce encryption** option, 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.
 - Last, assign your policy to all or to specific DriveLock Agents.

5.3.1 Create drive whitelist rule

Please do the following:

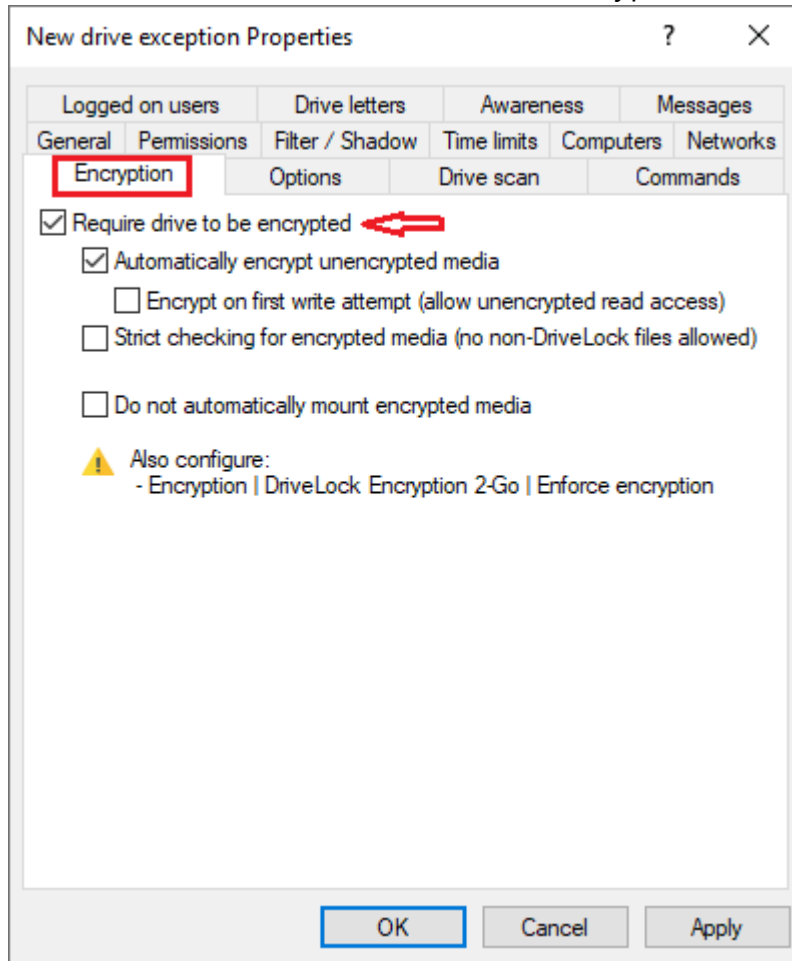
- On the **General** tab, select the USB drive from the list of **Installed drives**.


In the figure below, this is the USB drive **E:** with the vendor ID **VendorCo**.



- On the **Permissions** tab, specify that you want to allow this USB drive.
For more information on creating whitelist rules, please refer to the administration guide at [DriveLock Online Help](#).
- The **Encryption** tab has nothing selected by default.

- Check the **Require drive to be encrypted** option. This ensures that the connected and allowed USB drive must be encrypted before it can be used.



 Note: With this option, the access rights may be modified to enable the intended 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 wizard 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.

5.4 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.

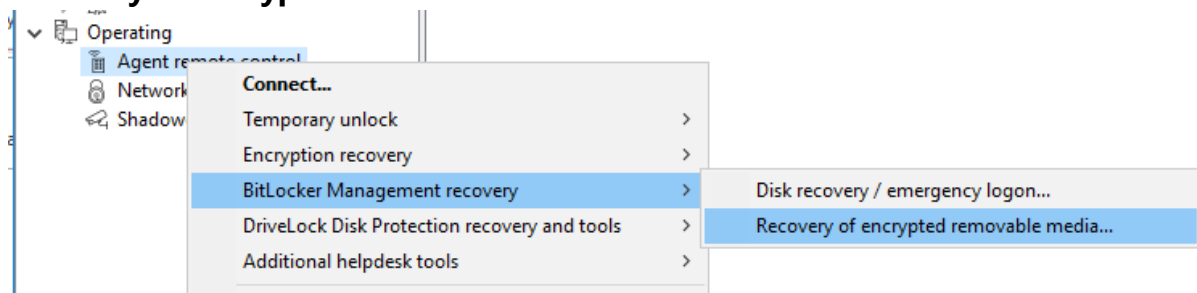
The password may be reset even if the client computer is currently not on the corporate network.

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.

5.4.1 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.

5.4.2 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** (from the DriveLock Control Center or from a browser).
2. Select the **Tasks** section and choose **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.

The screenshot shows the DriveLock web interface. On the left is a sidebar with navigation links: Dashboard, Computers, Groups, SecAware, Events, EDR, Tasks (highlighted), Accounts, and MAIN PERMIS. The main content area is titled 'Tasks' and has three sub-sections: 'File Protection recovery', 'Encryption 2-Go recovery', and 'BitLocker To Go recovery' (which is selected). The 'BitLocker To Go recovery' section displays a form titled 'Recover data protected with BitLocker To Go'. The form contains the following elements: a text input field for the recovery code with the value 'UGWTD-OUQTB-4IBYA'; a message box stating 'Recovery data was found. Select the certificate you want to use to generate a response code. The certificate is not transferred over the internet!'; a 'Select a certificate' dropdown menu showing 'DLB2GoRecovery.pfx'; a 'Password for certificate' field with masked characters; a 'Generate response code' button; and a text input field for the response code with the value 'RBVQC5-7RUP7L-XPNBZD-N7LBOW-YWD3FZ-P3VBBH-C7ZABG-BD43VN'.

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.

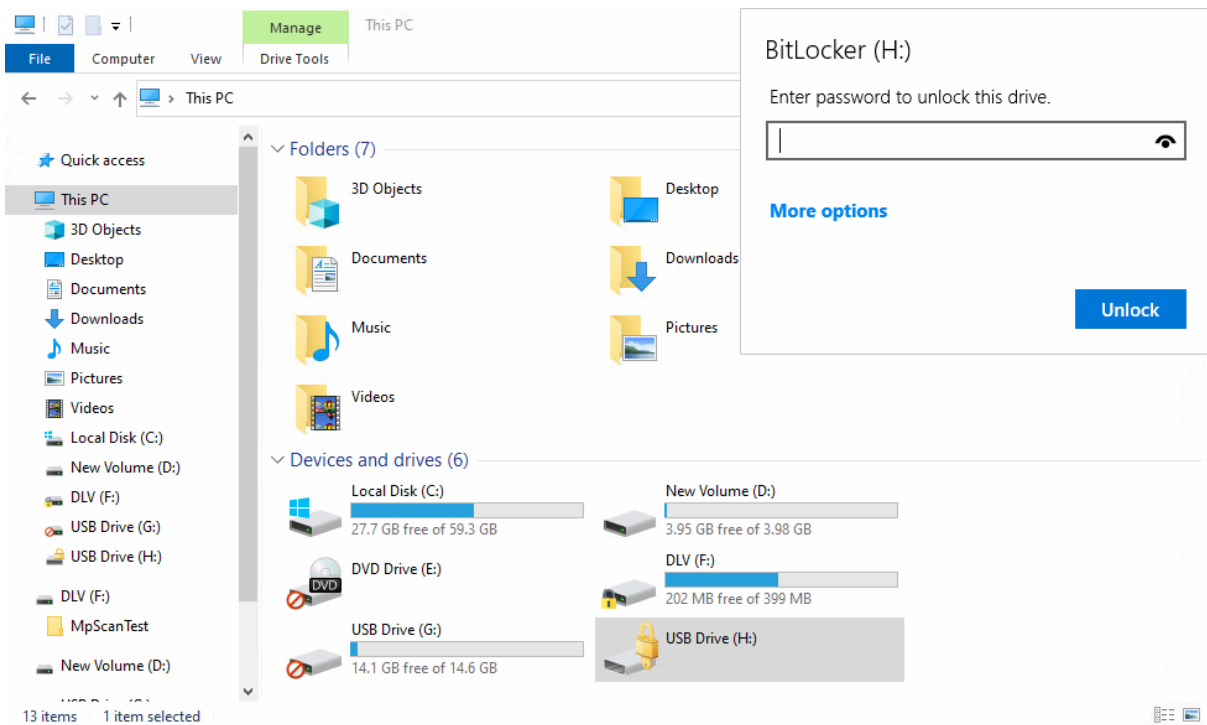
5.5 DriveLock Agent

5.5.1 BitLocker To Go on the DriveLock Agent

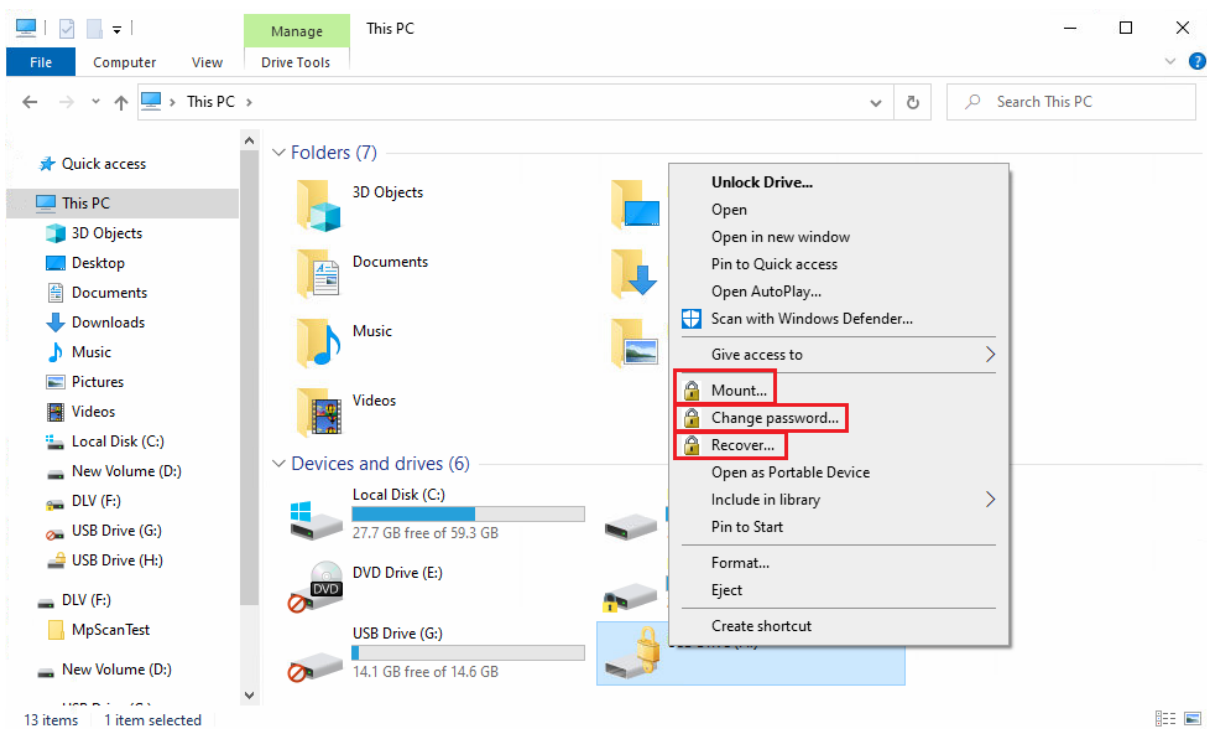
When the user plugs in an external USB storage device or external drive to the DriveLock Agent, the following options are available, depending on the policy [settings](#):

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...**

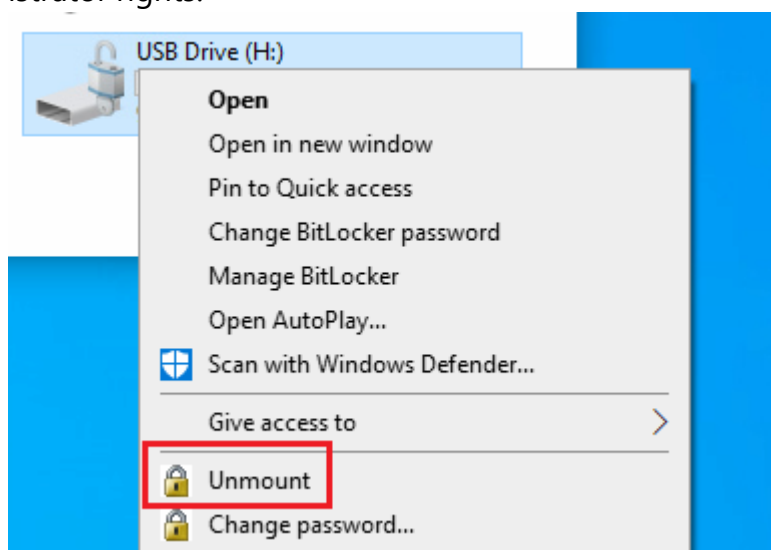
To change the password of an encrypted drive, click this menu item. Again, a wizard will open where you can first enter your old password and then your new password.

- **Recover...**

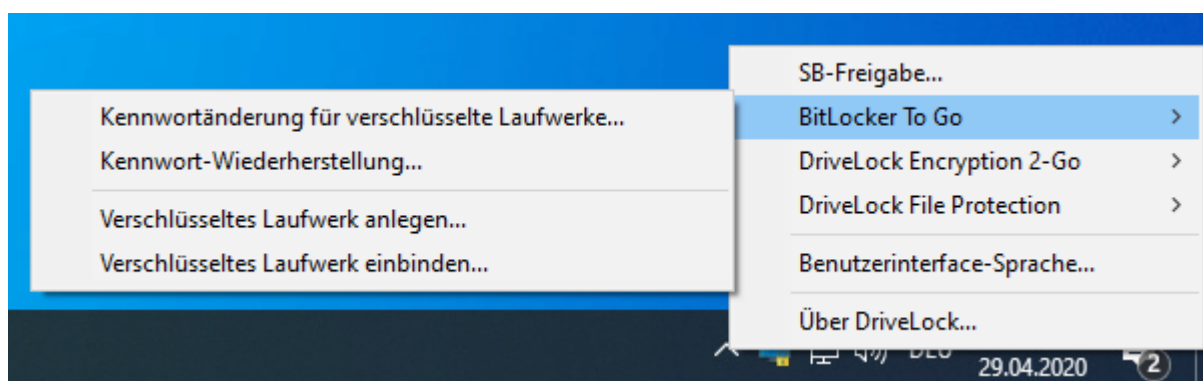
Use this menu command to restore the password. The recovery process of an encrypted drive takes place between the administrator and the user. For more information, please visit [here](#).

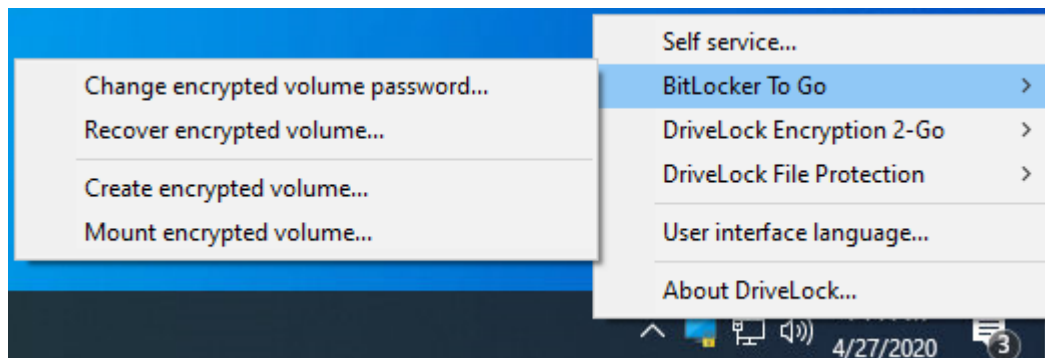
- **Unmount**

Use this menu command to unmount the drive, even without having administrator rights.



3. **If specified, the different options for BitLocker To Go can also be selected from the taskbar, see the figure below:**





5.6 Use cases

Please see the use cases for the following DriveLock BitLocker To Go options:

- [Administrative password](#)
- [Enforced encryption](#)

5.6.1 Administrative password rules

- 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.
- 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.
- 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.

5.6.2 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.

6 DriveLock Encryption 2-Go

DriveLock Encryption 2-Go lets you securely encrypt external drives or storage media, such as USB flash drives or SD cards. You can also use DriveLock Encryption 2-Go to securely and irreversibly delete sensitive data using one of several standard methods.

6.1 General information

DriveLock recognizes two different types of drives:

- Drives based on a file (container file)
- Drives based on an existing partition

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.

6.1.1 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 are performed by 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

6.2 Policy settings

6.2.1 Settings

In the Taskpad view, you can configure settings for Encryption 2-Go in the following sections:

- [General settings](#) for removable media encryption
- [Enforced encryption settings](#)
- [Password recovery](#) configuration for encrypted media

If you click **Advanced Configuration**, all existing settings will be displayed.

Encryption
Configure settings for the DriveLock encryption components in this configuration section.

General settings for DriveLock Encryption 2-Go

DriveLock Encryption 2-Go lets users encrypt removable drives and media and create encrypted containers. To simplify this process for users and to ensure that certain encryption settings are used, you can pre-configure several settings. Users cannot change any settings that are defined by company policy.

There are more options available in [Advanced configuration](#)

[Configure general settings...](#)

- Enforcement of FIPS 140-2-validated cryptography: Not configured (Off)
- Preconfigured encryption algorithm: Not configured
- Preconfigured password hash algorithm: Not configured
- Method to securely delete files: Not configured
- Allow quick format: Not configured (Disabled)
- Password complexity policy: Not configured

Enforced encryption settings for DriveLock Encryption 2-Go

When using enforced (automatic) encryption for removable media, you need to predefine certain settings, such as encryption algorithms, because users are not prompted to select these settings when a drive is encrypted.

There are more options available in [Advanced configuration](#)

[Configure enforced encryption settings...](#)

- Space usage: Use complete drive for encrypted container
- Encryption algorithm: AES
- Password hash algorithm: SHA-1
- Use quick format: Disabled
- Preserve existing data: Enabled
- Copy Mobile Encryption Application: Disabled

Password recovery (for DriveLock Encryption 2-Go)

DriveLock can perform recovery of passwords when a user no longer has access to a container's encryption password. This recovery is also available offline, without physical access to the encrypted container. To enable password recovery a recovery certificate is required.

There are more options available in [Advanced configuration](#)

[Show recovery certificate...](#)

Status: Default certificate-based container recovery

6.2.1.1 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 methods 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**

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.

6.2.1.2 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.

6.2.1.3 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.

6.2.1.4 Advanced settings

Below is an overview of all available settings for Encryption 2-Go.

Setting	Functionality
Encryption strength settings	

Setting	Functionality
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 algorithm to be used for encrypted drives	Specify the hash algorithm here.
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

Setting	Functionality
	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 (and display) of random passwords for new containers	An additional option is displayed in the creation wizard that allows users to generate random passwords.
Allow and show option to send passwords for new containers using text messaging	<p>When enabled, this option generates an additional wizard page when creating containers and allows passwords to be sent via text message (SMS).</p> <p>The SMS gateway required for this is configured in the Global configuration node in the Text messaging (SMS) gateway settings. For more information, see the DriveLock Administration documentation at DriveLock Online Help.</p>
Default text for sending passwords using text messaging	Sets the default text for sending passwords via text message.
Password recovery settings	

Setting	Functionality
Encrypted volume password recovery methods	<p>DriveLock provides two methods for recovering lost passwords for encrypted containers:</p> <ul style="list-style-type: none"> • 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 on the corresponding computer.
User contact information for offline container recovery	<p>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.</p>
Encryption user experience	
Context menus available in Windows Explorer	<p>These settings define all the options available from the context menu. The "Not configured" setting activates all options</p>
Start menu configuration	<p>You can define whether the DriveLock Start menu items are displayed and how they are arranged.</p>
Available Start menu items	<p>This option defines the start menu items to be displayed</p>
Menu items avail-	<p>You can define whether all menu items are displayed when</p>

Setting	Functionality
able from the taskbar icon	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.
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.

Setting	Functionality
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 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

6.2.2 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.

6.2.2.1 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 administrative password rule, select **Encrypted drive recovery**, open the context menu, click New and then **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:

- **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.

6.2.2.2 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.

6.2.3 Enforced encryption

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'.

6.2.3.1 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 the [Use cases](#) for more information.

To create new rules, select **New** and then **Enforced encryption rule...** in the **Enforce encryption** subnode.

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.

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: Note that this option only works if you have specified an administrative password in the **Encrypted drive recovery** section.

- **Disable any administrative password for new drives:** Once a user has set a personal password, the administrative password is deleted when encrypting the USB stor-

age 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.
- **Encryption:** Select the appropriate encryption method.
- **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.

On the **Encryption** tab, specify the [encryption and hash algorithm](#), file system and cluster size.

On the **Volume creation** tab you can specify the following:

- **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. 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 portion:** You also have the option to specify whether the Mobile Encryption application should be copied to

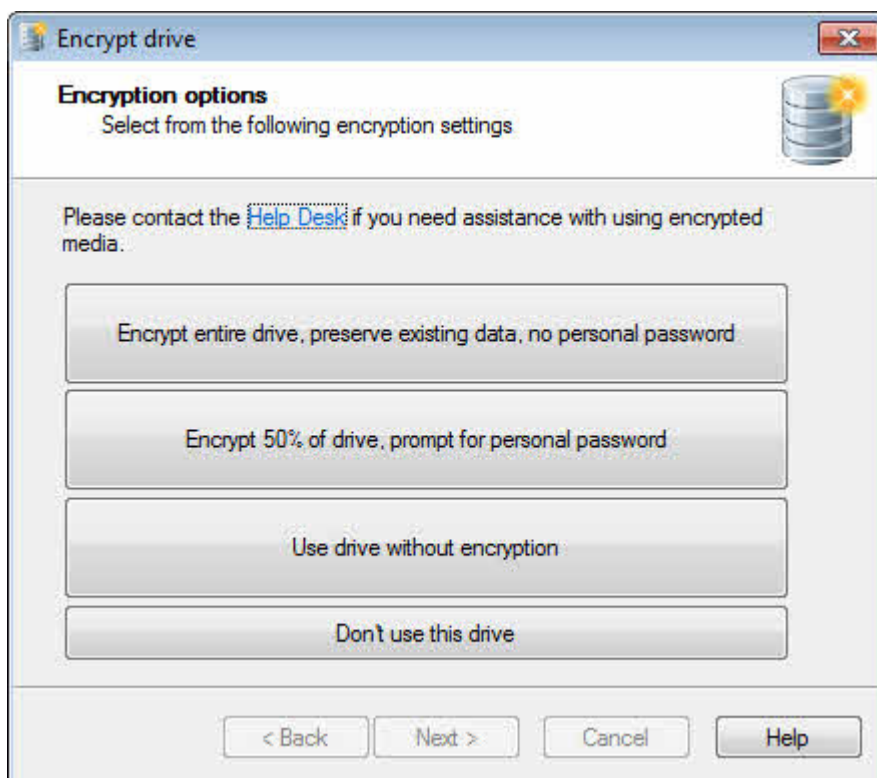
removable media during automatic encryption. This allows using it even on computers where DriveLock is not installed. In addition, an Autorun.inf file can be created, in which user-specific contents can also be configured.

- **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**

6.2.3.2 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.

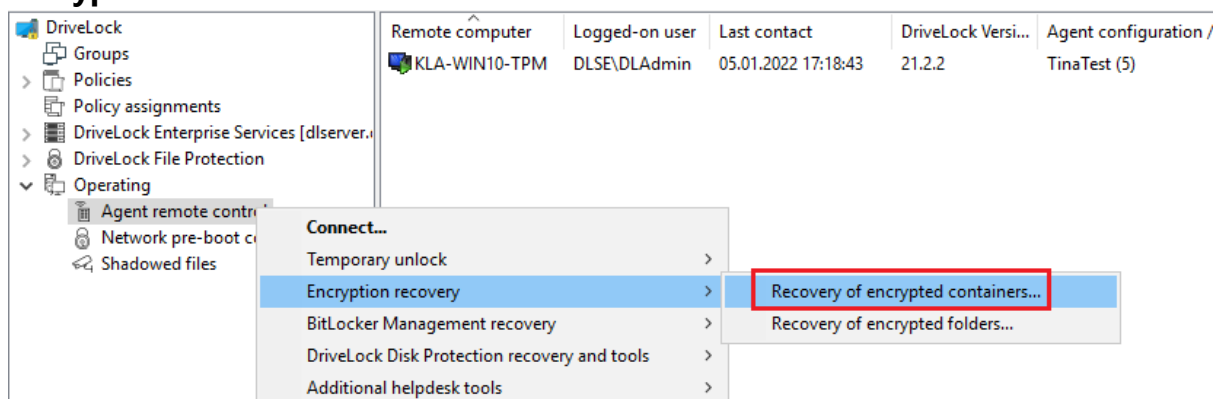
On the **Messages** tab you define the texts that will then appear in the user selection dialog. Here you can configure the title, subtitle and help text elements. You can enter all texts either directly or select a multilingual notification message you defined earlier.

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.

6.3 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.

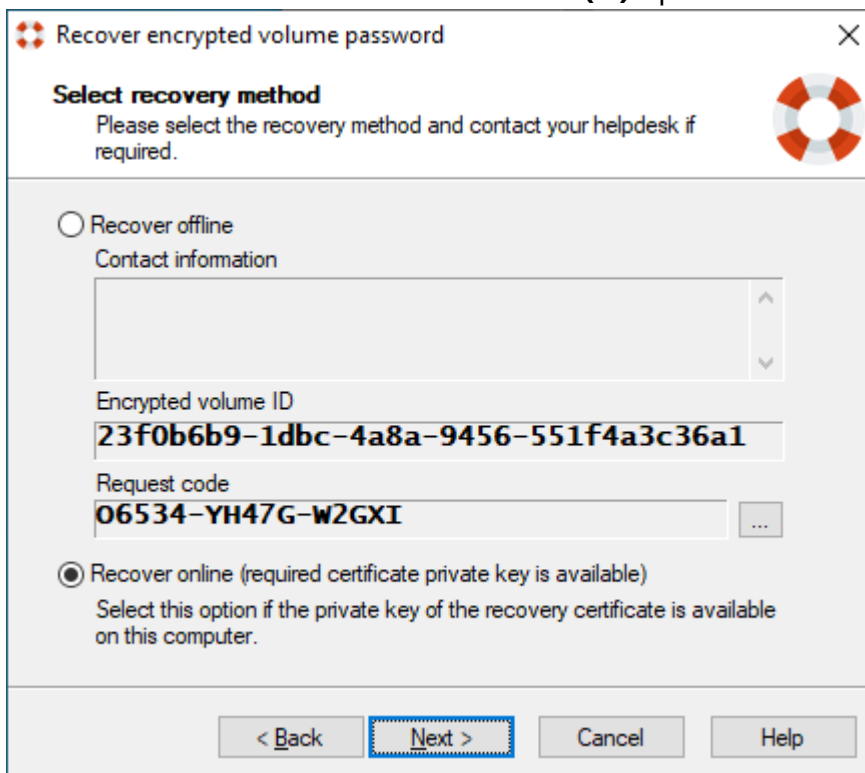
6.4 Online recovery process

 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.



Recover encrypted volume password

Select recovery method
Please select the recovery method and contact your helpdesk if required.

☐ Recover offline
Contact information

Encrypted volume ID
23f0b6b9-1dbc-4a8a-9456-551f4a3c36a1

Request code
06534-YH47G-W2GXI

☒ Recover online (required certificate private key is available)
Select this option if the private key of the recovery certificate is available on this computer.

< Back Next > Cancel Help

2. Select recovery certificate

The user will either provide the path to the certificate file along with the correct password or refer to a smart card or the certificate in the certificate store.

Recover encrypted volume password

Select recovery certificate and private keys
Please select the location of the password recovery certificate and private key.

Please select the location of the password recovery certificate and private key.

☒ Certificate file (PFX)
PFX file
C:\Users\user1\Documents\DLDivRecovery.pfx
Password
.....

☐ Smart card
☐ Certificate store of current user

< Back Next > Cancel Help

3. Enter new password

A new password can then be assigned in the last dialog.

Recover encrypted volume password

Enter the new password
The encrypted volume password will be changed to the new password.

Please type the new encrypted volume password. After the password has been changed you can use the new password.

Password
Confirm password
Password strength

The password must contain at least 8 characters including 1 lower case letter, 1 upper case letter, 1 number, 1 special character.

< Back Next > Cancel Help

6.5 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.

7 DriveLock File Protection

DriveLock File Protection enables you to encrypt files and directories independent of or beyond the control of privileged users. It contains:

- File encryption on local computers, central directories of a server, external USB data carriers or cloud-based services (e.g. Dropbox, Microsoft OneDrive, Google Drive)
- AES-NI support (hardware-assisted fast encryption)
- Authentication when accessing encrypted directories with user name/password or via X.509-based certificates
- Integrated, fully functional public key infrastructure



Note: A license is required to use File Protection.

With version 2022.2, DriveLock introduces a new encryption format that will be applied by default to new DriveLock agents starting with this version. Existing agents will keep using the old format. There is now a special [policy setting](#) in the DMC that allows you to specify different encryption formats if needed.



Warning: New and old encryption formats are not compatible and must be handled in separate policies.

7.1 How does DriveLock File Protection work?

First, a folder is marked as “encrypted”, which indicates that all data in this folder is to be encrypted. Next, authorized users are designated for whom DriveLock File Protection will automatically and transparently encrypt and decrypt files as they are read and saved.

On a computer where DriveLock File Protection is active, it checks every time a folder is accessed whether that folder is marked as encrypted. 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.

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.

To use certificates for authentication, an existing Public Key Infrastructure (PKI) is not required. Instead you can use the certificate functionality built into DriveLock itself.



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.

All encryption and decryption operations take place in the background and are completely transparent to users. This process is performed by encryption algorithms already included in the processor (AES NI).

Administration of the encryption of centralized file resources, such as shared folders and network-attached storage (NAS), can be performed by IT administrators using the DriveLock Management Console. 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.

In addition to centrally managed folders, users can also create their own encrypted folders and securely store data in them, for example as a private local directory, on a USB drive, 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.



Note: For more information about creating and using private directories, see the DriveLock User Guide at [DriveLock Online Help](#).

7.1.1 Supported Encryption Mechanism

DriveLock File Protection supports the following encryption algorithms:

- AES (recommended): The Advanced Encryption Standard (AES) is a symmetric encryption mechanism that was chosen by the National Institute of Standards (NIST) as successor to DES and 3DES in October 2000. It is also called the Rijndael algorithm for its developers Joan Daemen and Vincent Rijmen. DriveLock uses AES-256, which is considered sufficient also for top secret information.

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-1:** This algorithm was developed by NIST (National Institute of Standards and Technology) in cooperation with the NSA (National Security Agency) as the secure signing hash function of the digital signature algorithm (DSA) for the Digital Signature Standard (DSS). The function was released in 1994. Secure Hash Standard (SHS) specifies a secure hash-algorithm (SHA) with a hash value of 160 bits for messages with a size of up to 264 bits. S SHA is similar to the MD4 algorithm developed by Ronald L. Rivest. The secure hash algorithm initially exists in two variants, SHA-0 and SHA-1, which differ in the number of rounds passed in generating the hash value. NIST published three more variants ("SHA-2") of the algorithm in August 2002 that produce larger hash values. These are the SHA-256, SHA-384 and SHA-512 where the appended number indicates the length of the hash value (in bits) in each case.

7.2 Configuring File Protection

Before you can use DriveLock File Protection you need to determine your exact requirements and perform the configuration steps that match these requirements.

You need to determine the following requirements:

- How will you administer the user certificates that will be used for authentication?
- What settings will apply to the encryption and decryption of data?
- What functionality will be available to users on their computers?
- What will be the folder structure that you will use for storing encrypted data and files?

For administering [user certificates](#) you can use the following methods:

- 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 administered in an existing PKI using Microsoft Active Directory without any involvement by DriveLock.
- User certificates are administered in a third-party Windows compatible-environment without any involvement by DriveLock

For the various options for encryption, decryption, and user option configuration, see the [Policy settings](#) chapter.

The chapter [Manage encrypted drives centrally](#) describes how to create and manage centrally managed directories.

7.2.1 Creating a Master Certificate for Key Management

Before you can create and manage any user certificates using the DriveLock Enterprise Service, you need to create or import a master certificate for tenant root or per tenant which can be used to sign and issue all other user certificates.

You may use the master certificate of tenant root for all tenants or create a master certificate for each tenant.

- Open DriveLock Enterprise Services / Server / double-click <Server Name> / Options and check or uncheck **Enable tenant-aware certificate management**.

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. When prompted, type the password used to protect the private key, click Next Continue with Step 5 of this procedure.
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.

7.2.2 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. Navigate to DriveLock Enterprise Service / double-click <tenant name> / Certificate mgmt.
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.

7.3 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:

- [Configure settings for encryption](#)
- [Configure the encryption user interface](#)
- [Configure encrypted drives settings](#)
- [Configure additional settings](#)
- [Create encryption certificate](#)
- [Use forced encryption](#)
- [Specify forced encryption](#)

7.3.1 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:** Select the encryption algorithm to be used for encryption and decryption (see ["Supported Encryption Algorithms"](#)).
- **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 look for this file in the location you specify.

You can also place dictionary files into the policy file storage and select "Policy file storage..." as the dictionary location. 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).

7.3.2 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 entries 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.
- **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.

7.3.3 Configure encrypted drives settings

To configure the settings for encrypted drives, the following options are available:

- **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 smart-cards 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.

7.3.4 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.

7.3.5 Applied encryption format

Future development for DriveLock File Protection is built on the new format for encrypted files.

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 you assign the two formats in separate policies, as they are not compatible.

The following options are available as fix adjustable values:

- **Automatic (default):**

Depending on the existing version on the agents, DriveLock uses either the new or the old format.

- **New format:**

Use this option if compatibility with encrypted folders in the old format is not required.

- **Old format:**

If there are already encrypted folders on your agents from older DriveLock versions, we recommend this option.

- **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 (old driver):**

If your agents are clients that are still using Windows XP, this option will be used automatically. Otherwise, it is a fallback option in case of compatibility issues with the old driver.



Warning: Please note that combining the different encryption methods can lead to data corruption, for example if "Old format (old driver)" is active although folders created with the "New format" exist. These folders should not be accessed (with the old driver).

The two lower settings are only fallback options.



Note: Please also note that the **Old Format** and **Old Format (old driver)** encryption formats do not support the Distributed File System (DFS).

7.4 Settings for enforced encryption

For forced encryption of external disks, you can 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. Enable the forced encryption with DriveLock File Protection in the policy under: Encryption / Settings / **Forced Disk Encryption Method**
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 to let your users choose between container-based or the file and folder-based encryption, check **Decision by user**.
2. Configure the encryption settings in the **Forced 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.

7.5 Configure encrypted drive recovery

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).

To configure the settings for restoring encrypted drives, open the **Encrypted folder recovery** sub-node 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.

7.5.1 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.

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.

Open tab Options and check the desired type of encryption.



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.

7.6 Managing User Accounts and Certificates

Before you can administer users and their certificates you need to configure several settings. These settings are described in the sections [Creating a Master Certificate for Key Management](#) and [Configuring Certificate Management](#).

7.6.1 How User Administration works

User administration in DriveLock File Protection allows you to issue and administer certificates for users without the need for an existing public key infrastructure (PKI).

The integrated user administration 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).

One main advantage of using user certificates for authentication with DriveLock File Protection is that encryption and decryption processes can be performed completely transparent to users and without requiring users from changing anything about how they access and use files and folders. Each time an encrypted folder is accessed, DriveLock File Protection checks whether the user's certificate store contains a user certificate and automatically uses this certificate for authentication.

To make it easy for administrators to use certificates without having to become familiar with the details of a public key infrastructure (PKI), all functionality for quick and easy administration of users and their certificates is integrated into DriveLock File Protection. Users can apply for their own certificates, these applications can be automatically approved and stored in the user's certificate store. Administrators can add or remove users, modify, revoke and delete certificates and import existing certificates from Active Directory or other sources.



Note: In DriveLock File Protection a user and the user's certificate are closely linked. Every DriveLock File Protection user needs a certificate and each certificate is linked to one user. The two therefore form a unit. When a user requests a certificate, DriveLock automatically creates a corresponding user account. Similarly, if an administrator creates a user account, DriveLock File Protection automatically creates a certificate for the user.



Warning: The DriveLock PKI does not store and manage the private 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.

7.6.2 Manage users

Users are managed using the DriveLock Management Console. You can access DriveLock File Protection certificate management by clicking **DriveLock File Protection** in the navigation pane and then clicking **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 as an administrator you cannot generate certificates using this user management. You can merely import existing certificates from a PKI here, for which the corresponding user is then also created. Only a user can create DriveLock File Protection certificates. This procedure is described in the DriveLock User Manual.

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.



Note: If a user requests/creates a certificate himself, a corresponding user is created automatically.

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.

To delete a user, right-click the user and then click Delete user.

7.6.3 Manage groups

DriveLock File Protection groups are a set of DriveLock users. DriveLock groups can be assigned to centrally managed encrypted folders. Each time DriveLock users are added to or removed from a DriveLock group, DriveLock Enterprise Server silently adjusts the corresponding users at all centrally managed folders that have that DriveLock group associated with them.



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 required DriveLock users or import an existing group from Group from 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.

7.6.4 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: Certificate approval is only necessary if you have activated the corresponding option in the DES 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. In the navigation pane, click **Active certificates** or **Revoked certificates**.
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. This procedure is described in the DriveLock User Manual.

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.

7.7 Managing encrypted drives centrally (Centrally managed folders)

Using the DriveLock Management Console (DMC), you manage encrypted directories in a central location. Access directory management by clicking **DriveLock File Protection** in the Navigation Pane and then clicking **Centrally managed folders**.

An overview of all directories stored in the DriveLock database and their status is displayed on the right side.

This is where you can create new directories and set up user permissions just once, change or view permissions on existing directories (provided you have directory administrator permissions as a user yourself), or delete directory entries.

When you create a new centrally managed directory, please note the following:

- Existing directories cannot be centrally managed and encrypted. Firstly, there is usually no DFP service installed on a server that could provide asynchronous encryption, and secondly, conflict situations that occur during the initial encryption period cannot be resolved sufficiently from a technical point of view (e.g. if only a part of the files is already encrypted or a larger file is currently being encrypted and another user accesses this file from his computer).
- When creating the directory, the users who are authorized for access are given administration rights for this directory. Administration rights allow to authorize additional users or to remove authorizations. Thus, as an IT administrator, you can hand over the management of authorized users to one or more users from the business department when creating the directory.

7.7.1 Preparations in 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:

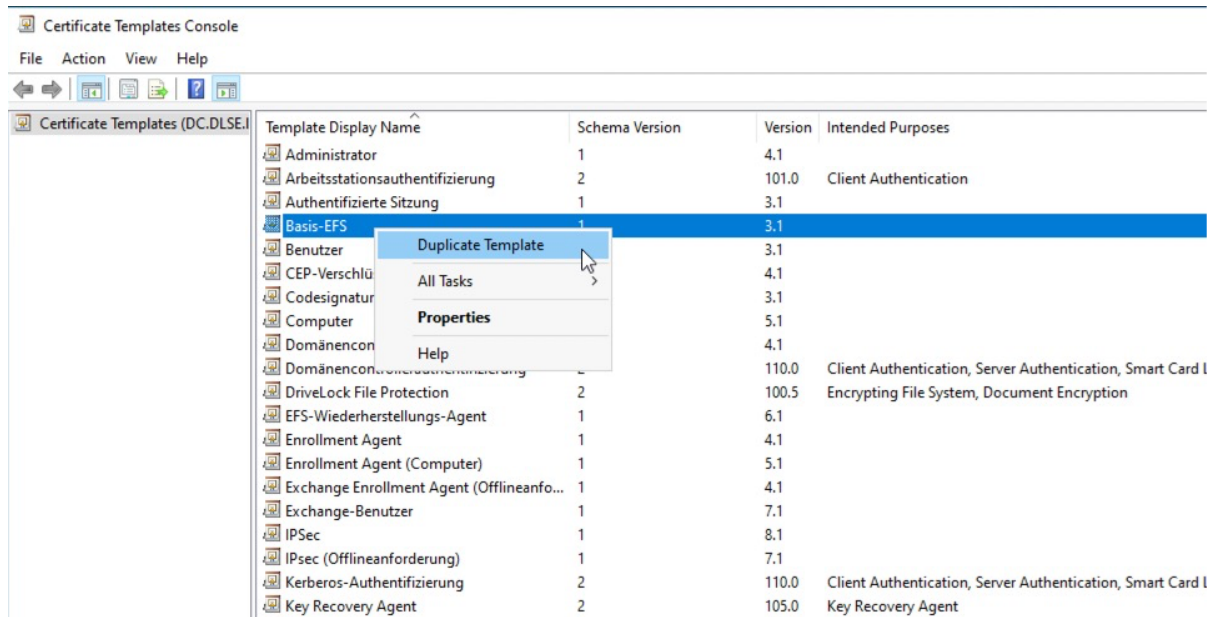
1. [Duplicating the certificate template](#)
2. [Issuing the template](#)
3. [Creating a group policy](#)
4. [Auto enrollment and policy activation](#)
5. [Testing the automatic enrollment](#)

Once this is done, the configuration can be performed in the DriveLock Management Console (DMC). You can find a concrete use case [here](#).

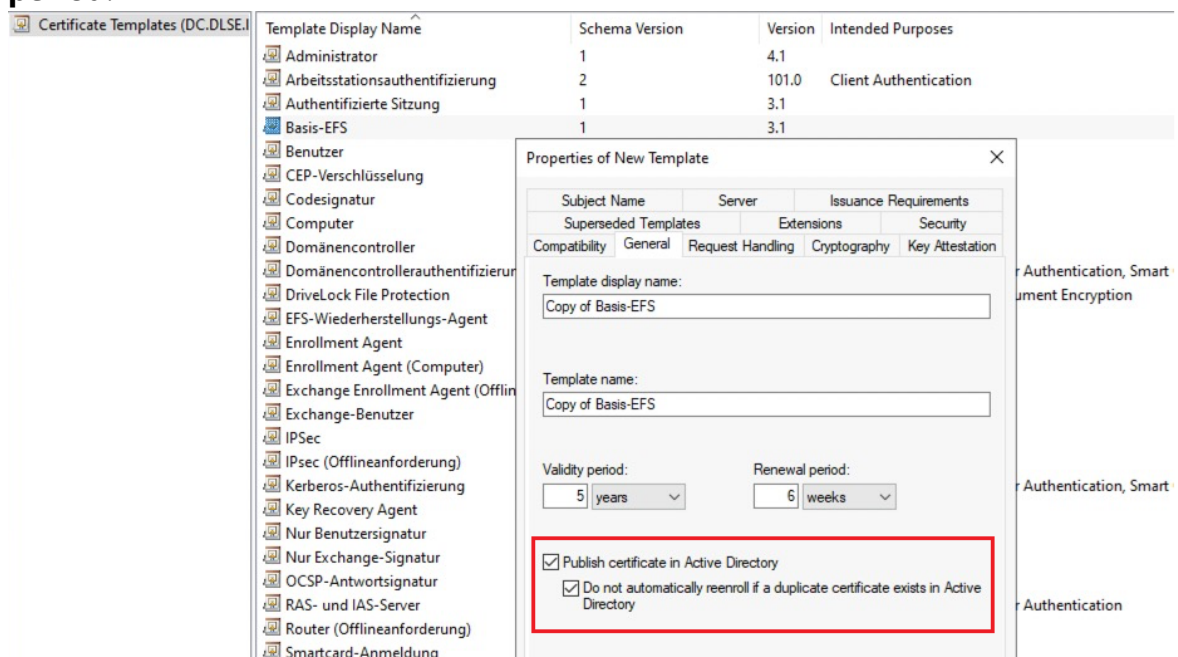
7.7.1.1 Duplicating the certificate template

To duplicate the certificate template, follow these steps:

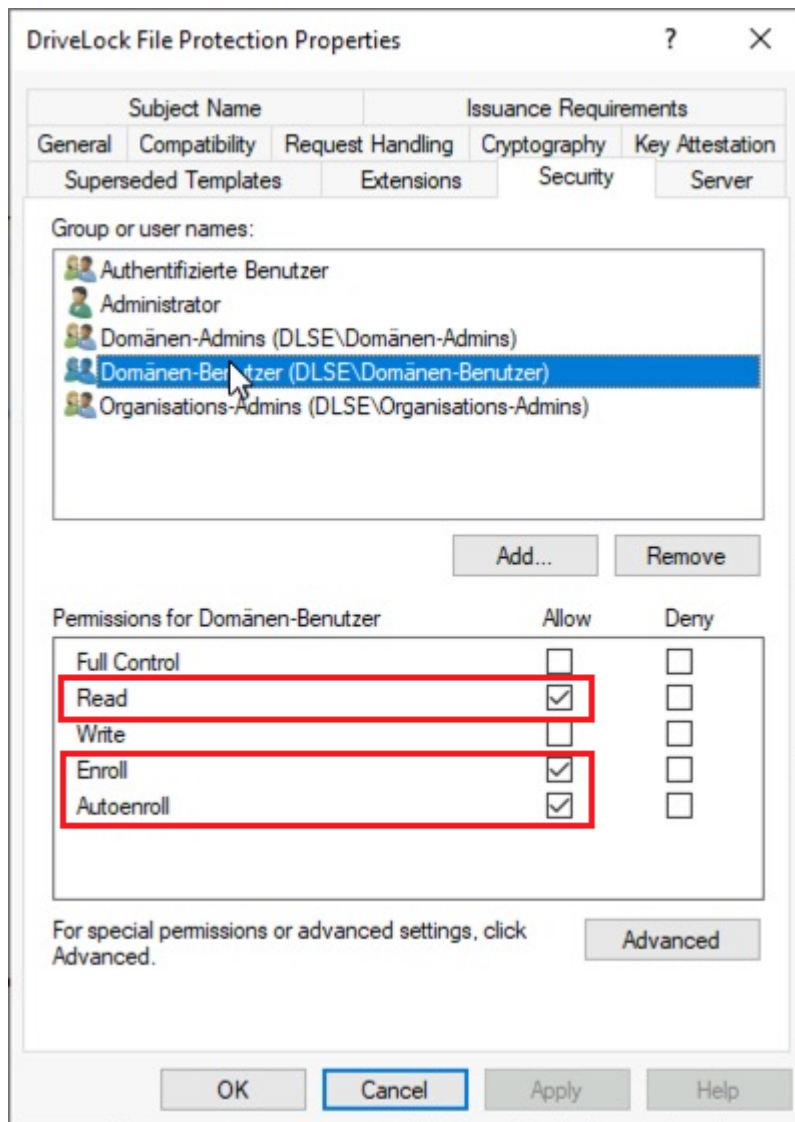
1. On the CA server, open the Certificate Template Console **certtmpl.msc** and right-click **Basis-EFS**.
2. Select **Duplicate Template**.



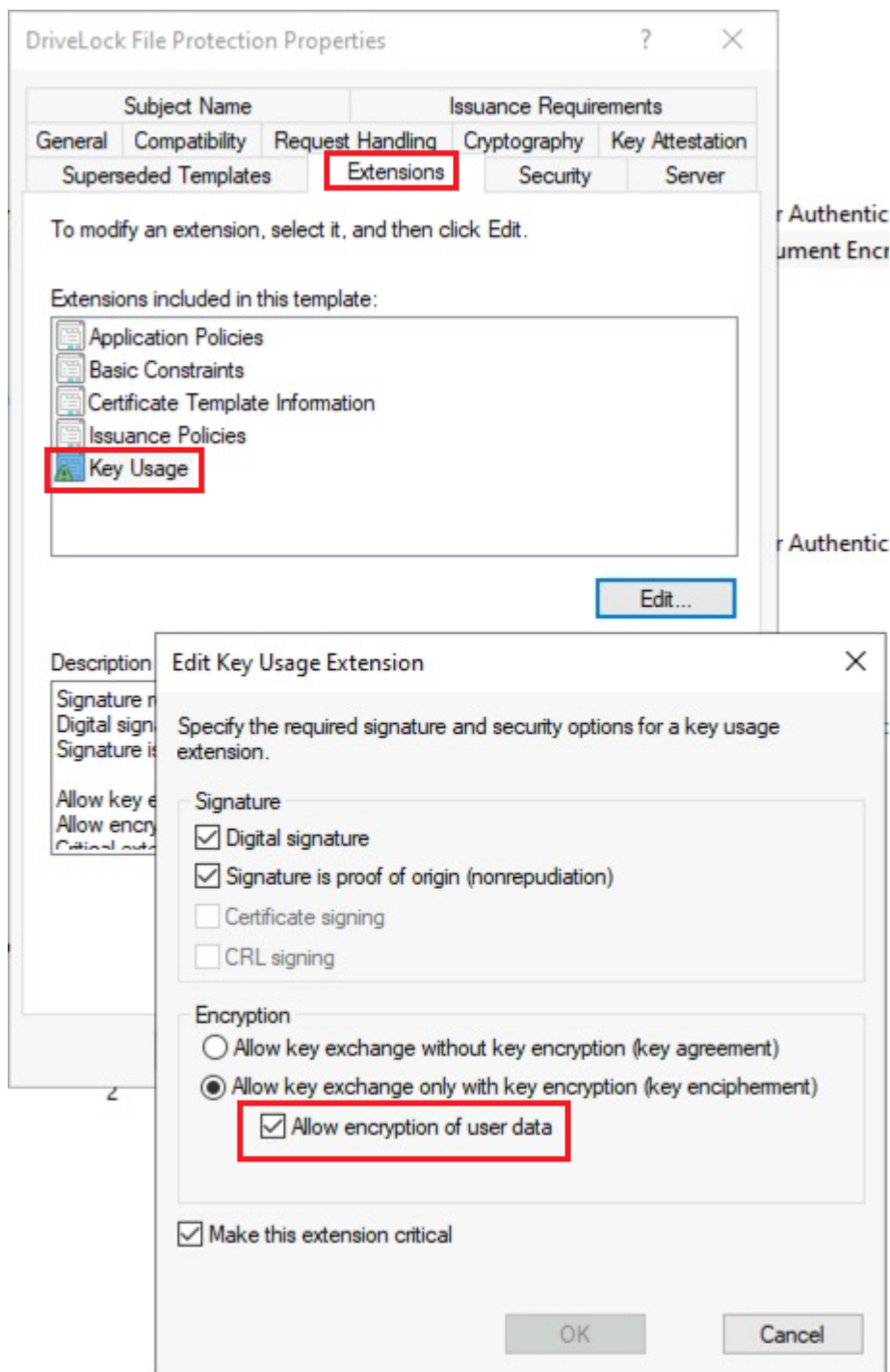
3. On the **General** tab, specify a suitable **Template display name** and the **validity period**.



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.



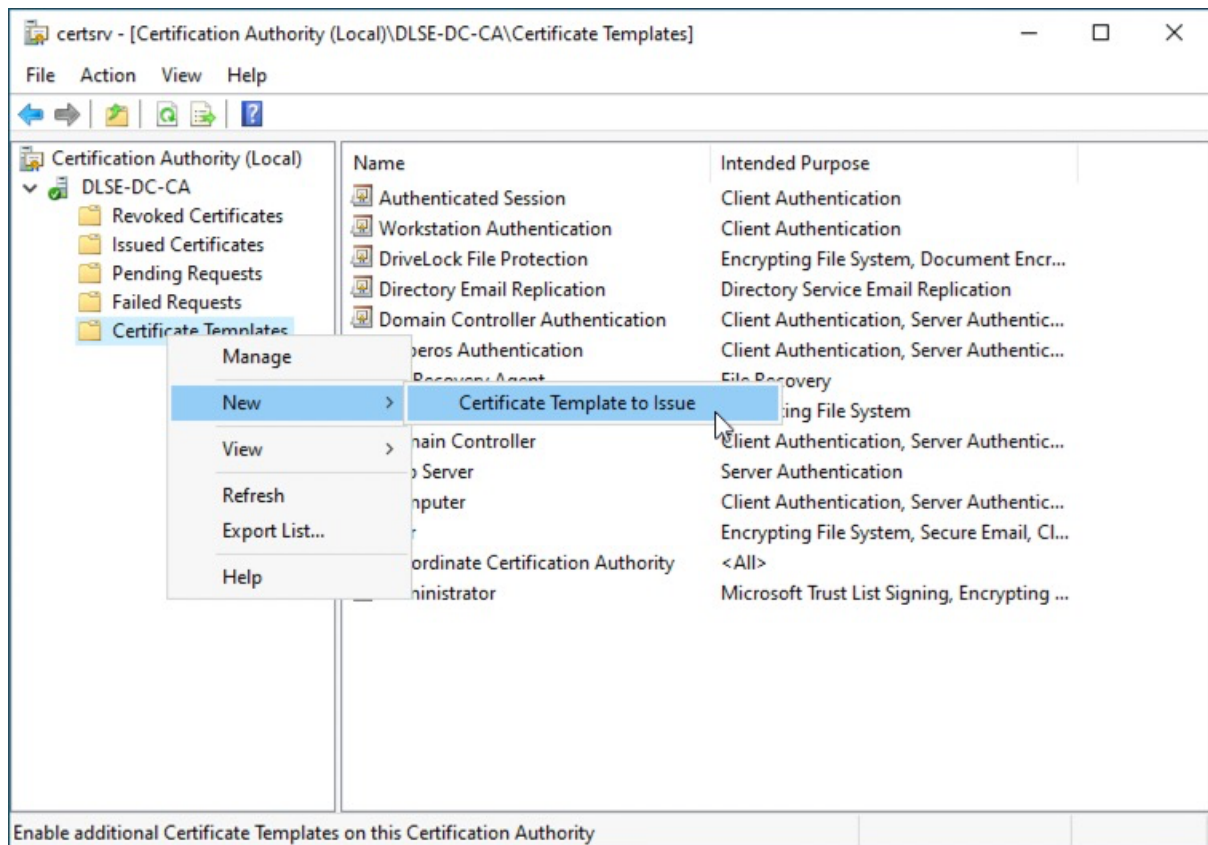
7. On the **Extensions** tab in **Key Usage**, place a check mark next to the **Allow encryption of user data** option and confirm with **OK**.



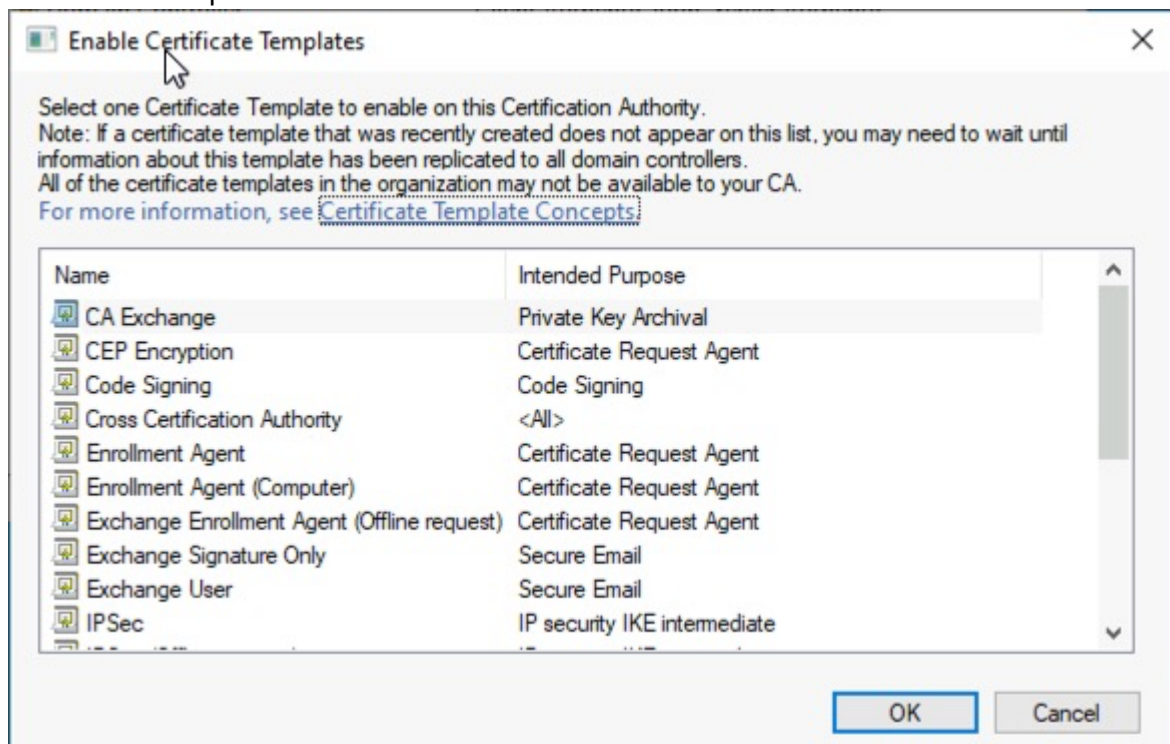
7.7.1.2 Issuing the template

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.

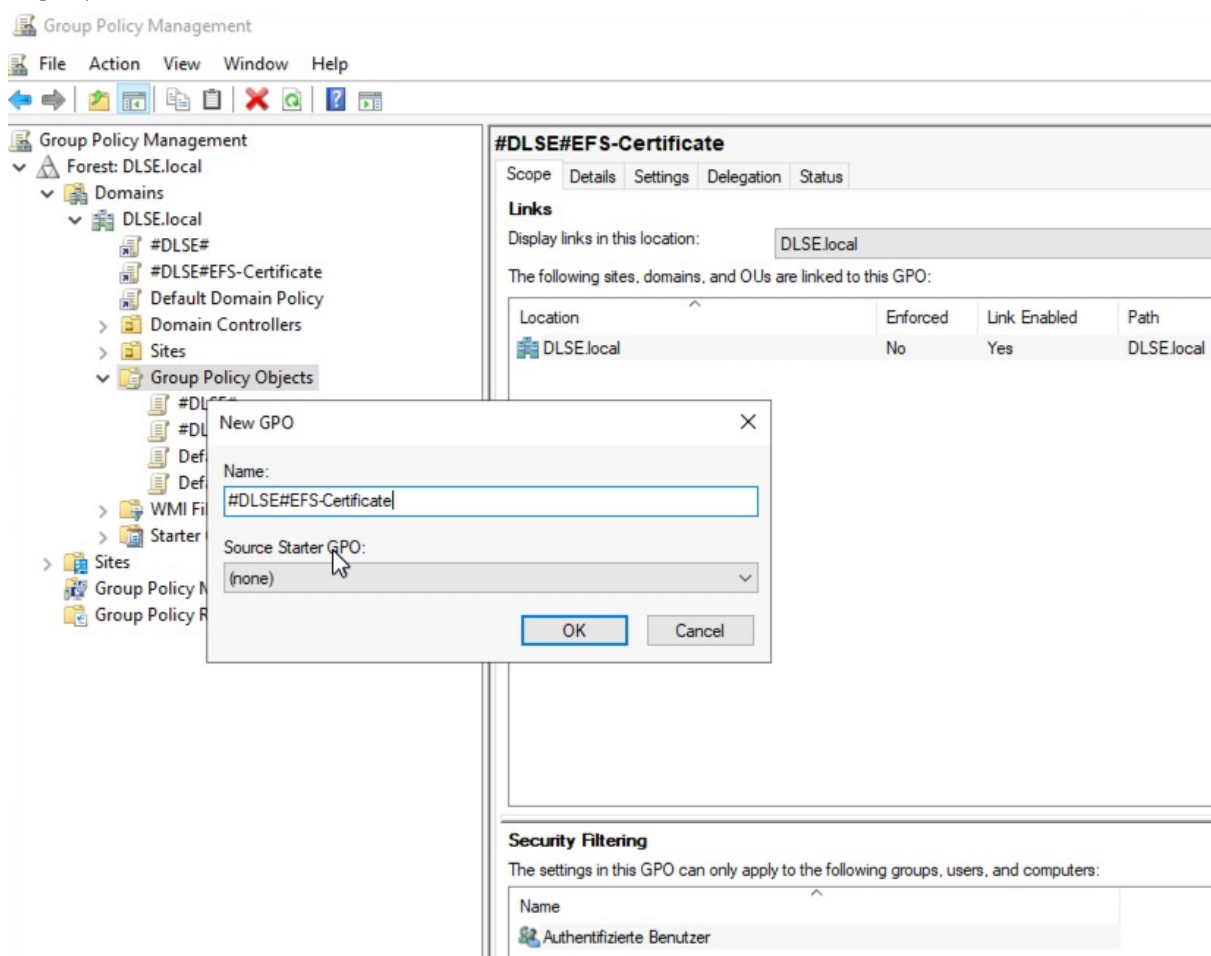
Name	Intended Purpose
Authenticated Session	Client Authentication
Workstation Authentication	Client Authentication
DriveLock File Protection	Encrypting File System, Document Encr...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...

4. Next, set up a group policy.

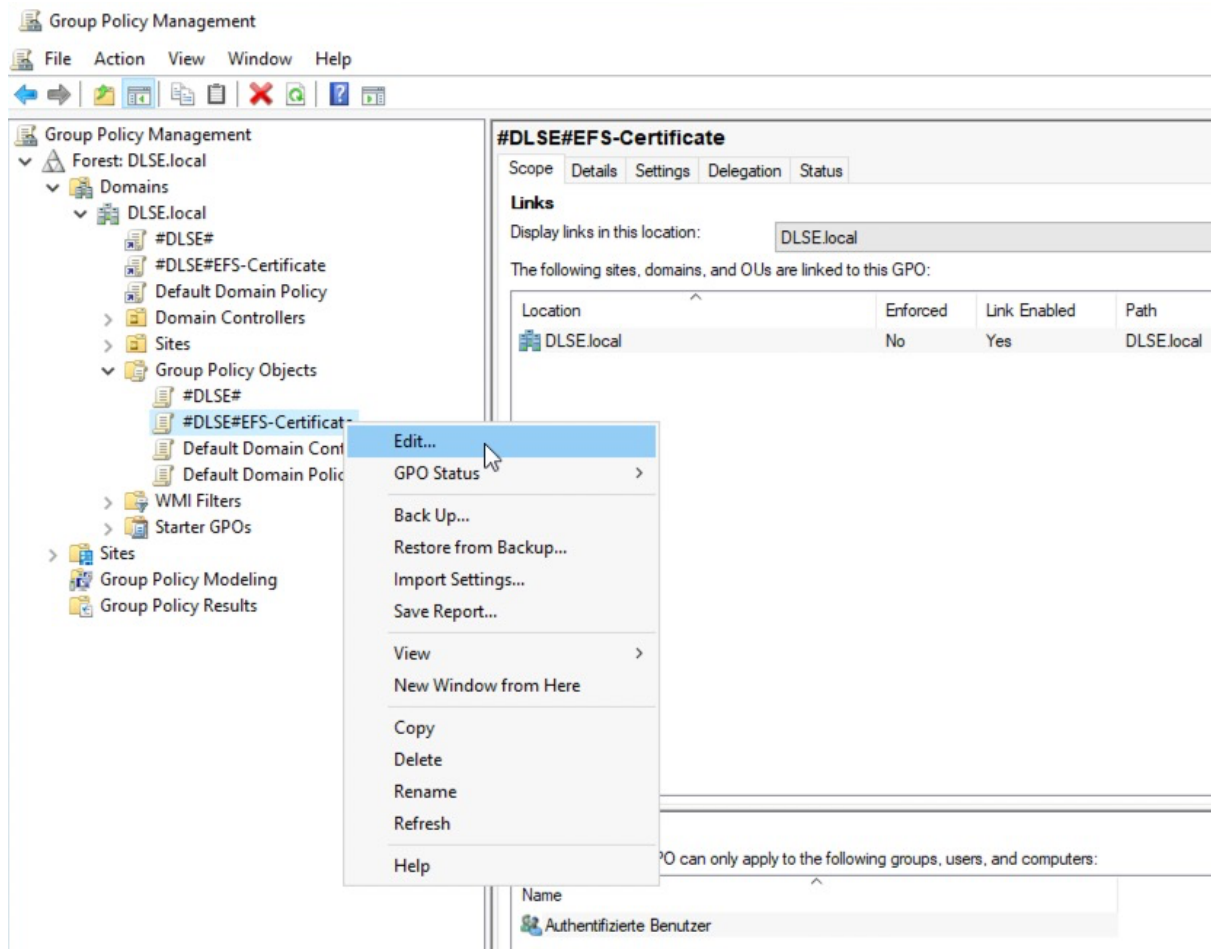
7.7.1.3 Creating a group policy

To create a group policy, follow these steps:

1. Open **gpmc.msc** on a domain controller, select the **Group Policy Objects** and then **New**.



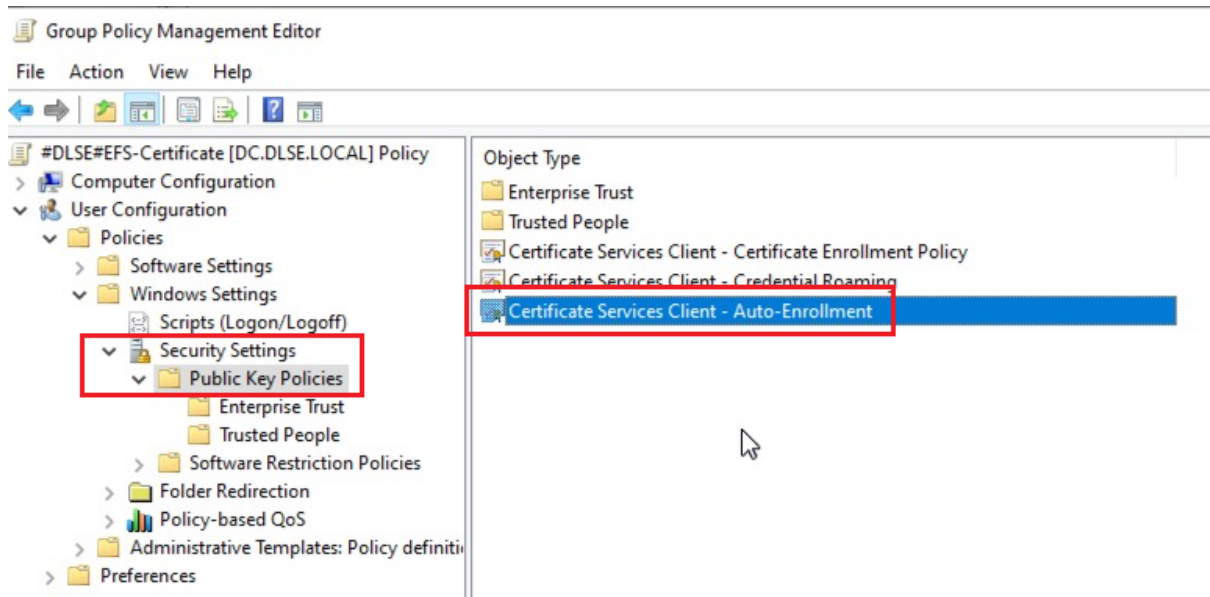
2. Open the context menu of the GPO and select Edit...



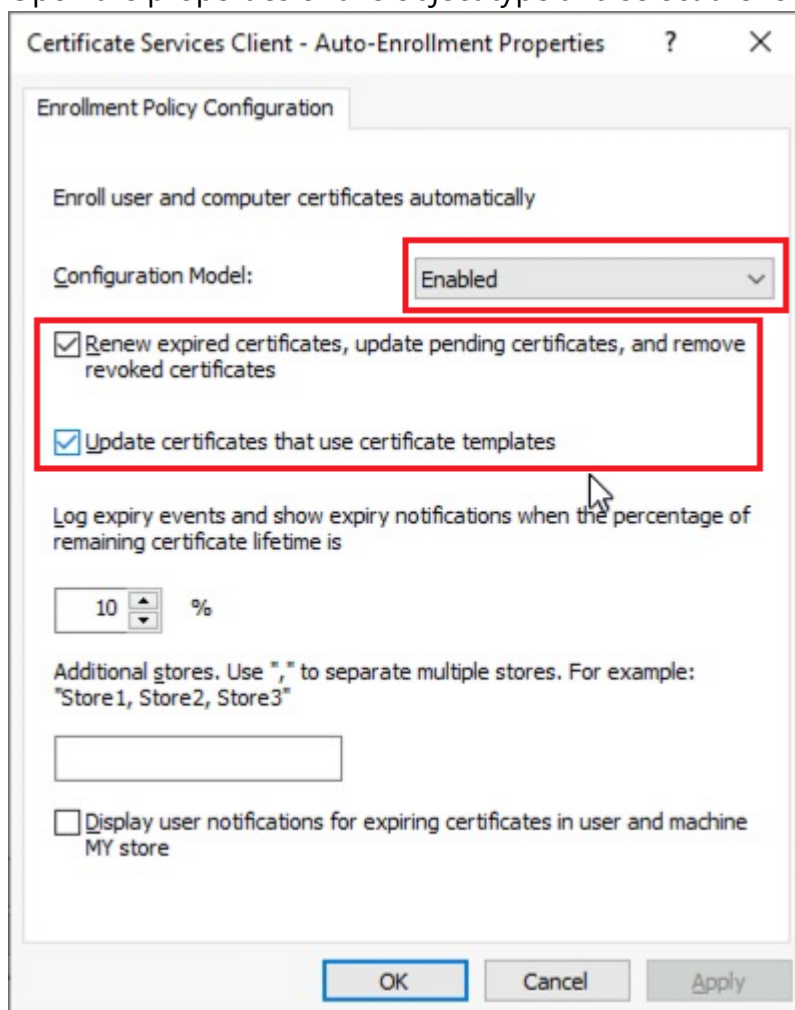
7.7.1.4 Automatic registration

To automatically register and activate the GPO, follow these steps:

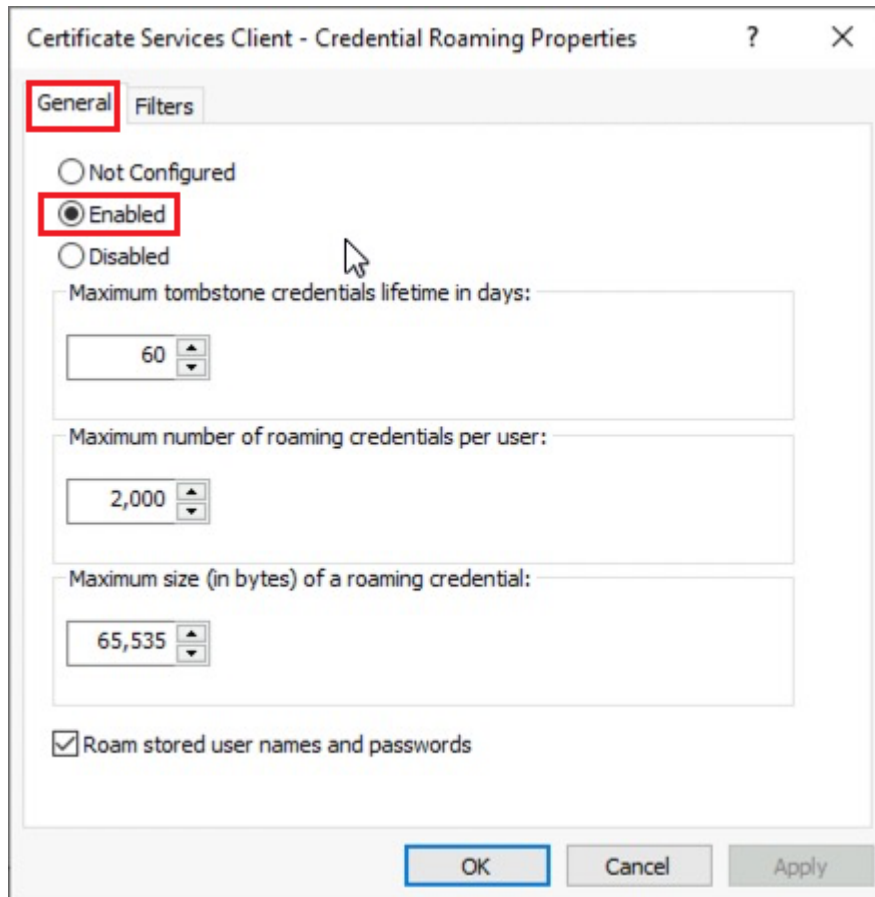
1. Under **User Configuration**, open **Policies**, then click **Windows Settings** and **Security Settings**.



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.

7.7.1.5 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`


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.652]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\tom>gpupdate /force
Die Richtlinie wird aktualisiert...

Die Aktualisierung der Computerrichtlinie wurde erfolgreich abgeschlossen.
Die Aktualisierung der Benutzerrichtlinie wurde erfolgreich abgeschlossen.

C:\Users\tom>gpresult /r

Betriebssystem Microsoft (R) Windows (R) Gruppenrichtlinienergebnis-Tool v2.0
© Microsoft Corporation. Alle Rechte vorbehalten.

Am 23.06.2022 um 16:56:39 erstellt

RSOP-Daten für DLSE\tom auf CLIENT01: Protokollmodus
-----

Betriebssystemkonfiguration: Mitglied der Domäne/Arbeitsgruppe
Betriebssystemversion: 10.0.22000
Standortname: Nicht zutreffend
Roamingprofil: Nicht zutreffend
Lokales Profil: C:\Users\tom
Langsame Verbindung? Nein

BENUTZEREINSTELLUNGEN
-----
CN=Tom,OU=Users,OU=IT,OU=Munich,OU=Sites,DC=DLSE,DC=local
Letzte Gruppenrichtlinienanwendung: 23.06.2022, um 16:55:43
Gruppenrichtlinienanwendung von: DC.DLSE.local
Schwellenwert für langsame Verbindung: 500 kbps
Domänenname: DLSE
Domänentyp: Windows 2008 oder höher

Angewendete Gruppenrichtlinienobjekte
-----
Default Domain Policy
#DLSE#
#DLSE#EFS-Zertifikat

Folgende herausgefilterte Gruppenrichtlinien werden nicht angewendet.
-----
Richtlinien der lokalen Gruppe
Filterung: Nicht angewendet (Leer)

Der Benutzer ist Mitglied der folgenden Sicherheitsgruppen
-----
```

```

C:\Windows\system32\cmd.exe

C:\Users\tom>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\tom>gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on 11/ 16/ 2022 at 1:06:45 PM

RSOP data for DLSE\tom on CLIENT01 : Logging Mode
-----

OS Configuration:      Member Workstation
OS Version:            10.0.22000
Site Name:              N/A
Roaming Profile:        N/A
Local Profile:          C:\Users\tom
Connected over a slow link?: No

USER SETTINGS
-----
CN=Tom,OU=Users,OU=IT,OU=Munich,OU=Sites,DC=DLSE,DC=local
Last time Group Policy was applied: 11/16/2022 at 1:06:28 PM
Group Policy was applied from:      DC.DLSE.local
Group Policy slow link threshold:   500 kbps
Domain Name:                        DLSE
Domain Type:                        Windows 2008 or later

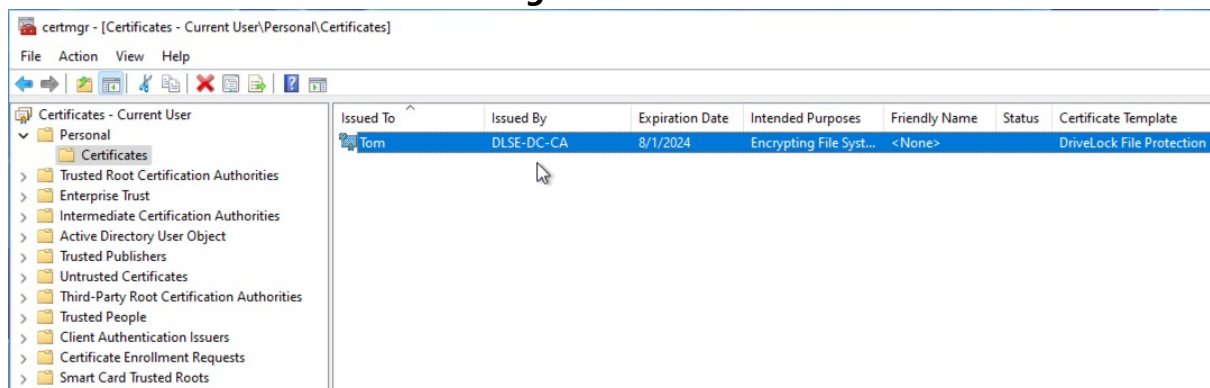
Applied Group Policy Objects
-----
Default Domain Policy
#DLSE#
#DLSE#EFS-Certificate

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups
-----

```

5. The certificate can be found in **certmgr.msc** under **Personal - Certificates**.



7.7.2 Creating a new encrypted drive



Note: You need to have write permissions to the directory or network drive where you want to create the new encrypted directory.

To create a new encrypted directory, perform the following steps:

1. Right-click on **Centrally Managed Folders** in the navigation pane or on an empty space in the details pane to the right
2. Select **New** and **Centrally Managed Folder...**
3. Optional: The settings **Generate for Tenant** and **Primary Server** only need to be adjusted if there is more than one DES available in your environment and you want to use a different DES than the central service, or you have set up more than one tenant and you do not need to use the default root tenant. In most cases, no change to these specifications should be necessary.
4. Enter the UNC path for the new directory in the **Path of new centrally managed folder** text box.

Alternative:

1. Click on the button ... and select the required directory via the selection dialog. Click **New Directory** to create a new directory in the previously selected folder and select it.
2. Be sure that the UNC path that is now displayed is correct.
3. To search for a specific user, enter a search text in the upper search field.
4. Now select one or more displayed users. These are given administrative permissions for this directory after setup.
5. Click **Next**. The new folder is now created and the permissions entered. You will then receive feedback whether this process was completed successfully.
6. Click **Finish**. The folder is now encrypted.

You can find a concrete use case [here](#).

7.7.3 Change access permissions

Access permissions for an encrypted folder can be changed either through the DriveLock user interface, via the context menu in Windows Explorer, or via the DriveLock Management

Console. To make changes, the executing user needs administrative permissions for this directory.

To change the access permissions as an administrator via Windows Explorer, right-click the Directory and select Properties and Users of the encrypted folder.

To change access permissions for an existing centrally managed directory as an administrator using the DriveLock Management Console, follow these steps:

1. Click Centrally Managed Folders in the Navigation Pane.
2. Right-click the required directory in the details pane and select Manage Folders.

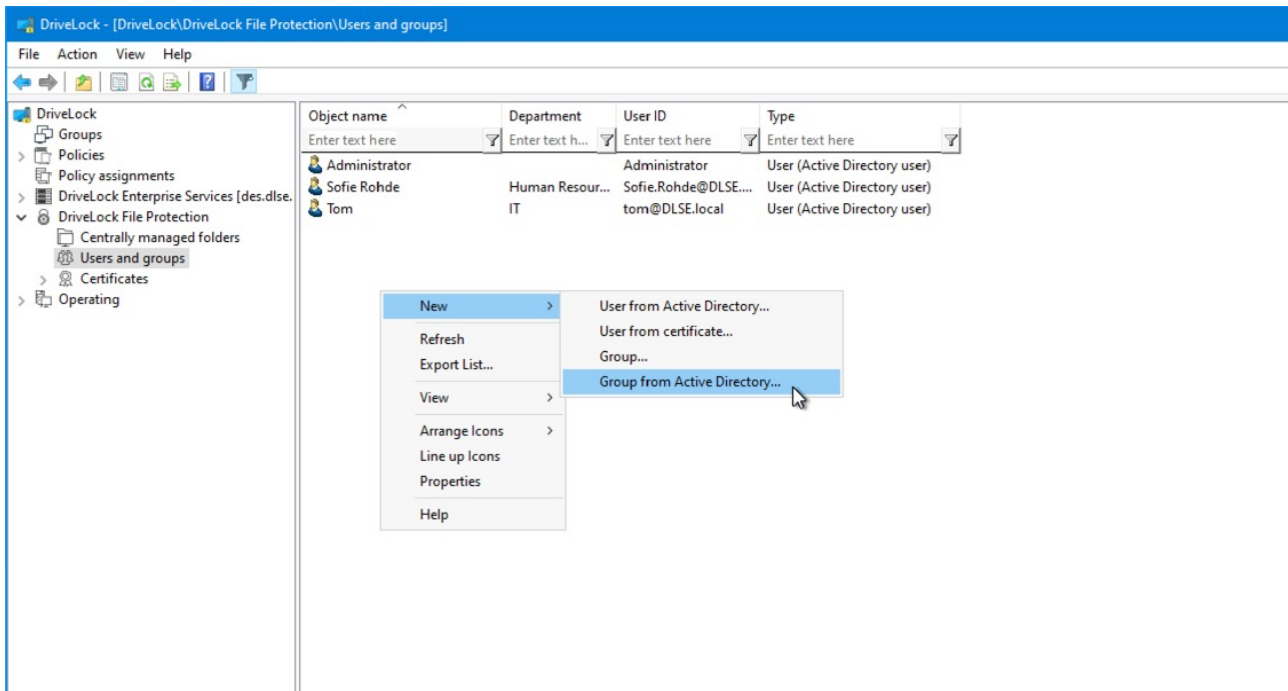
Alternative:

1. Double-click the required directory, select the **User** tab and click **Manage**.
2. If <Log on to view data> is displayed in the information, you still have to authenticate yourself first. To do this, click **Log in** and select the certificate that is needed for access.
3. Select the **User** tab.
4. To revoke a user's access, select the required user and click **Remove**.
5. To authorize a new user, click **Add**.

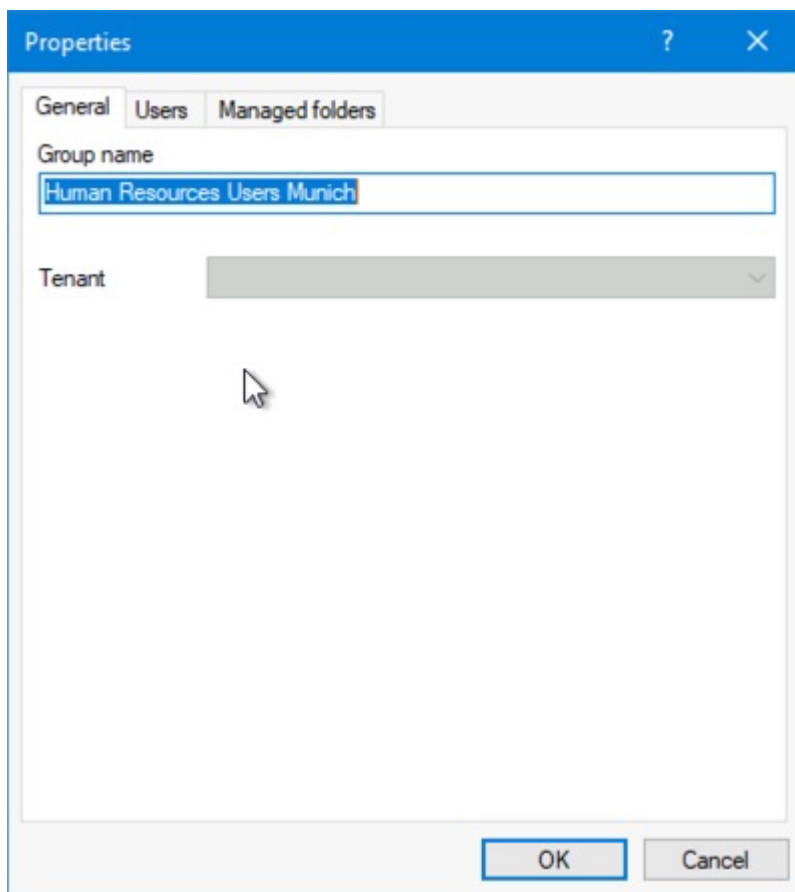
7.8 Use case: Accessing encrypted folders

In order for users and groups to have access to encrypted resources, you must define these groups and users from Active Directory.

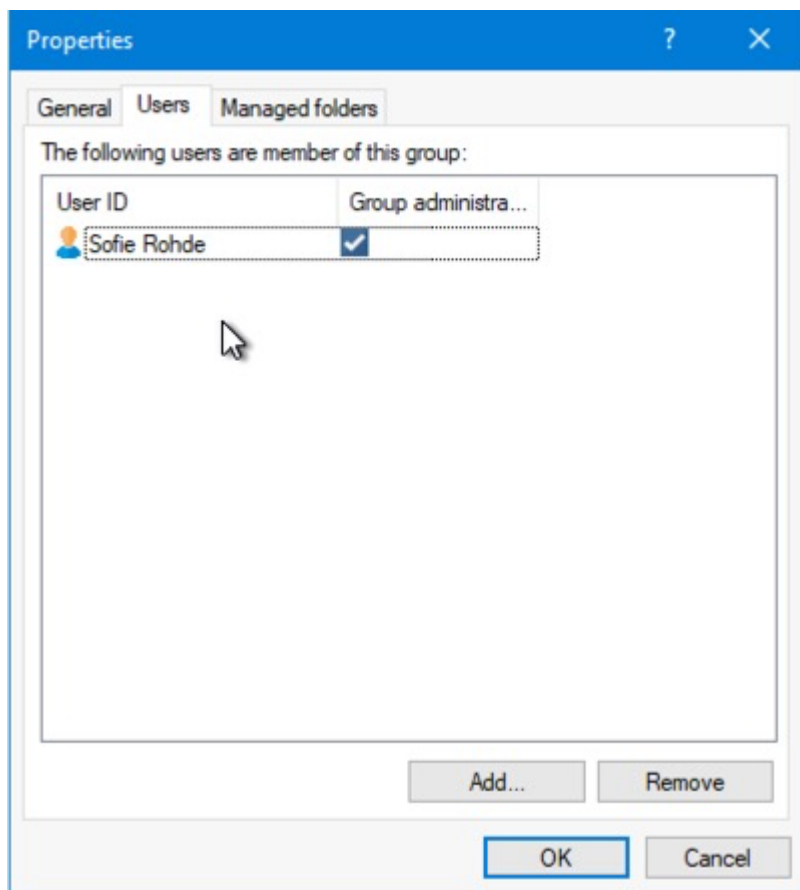
For this purpose, go to **New** in the **Users and Groups** submenu and select a user or group from the Active Directory.



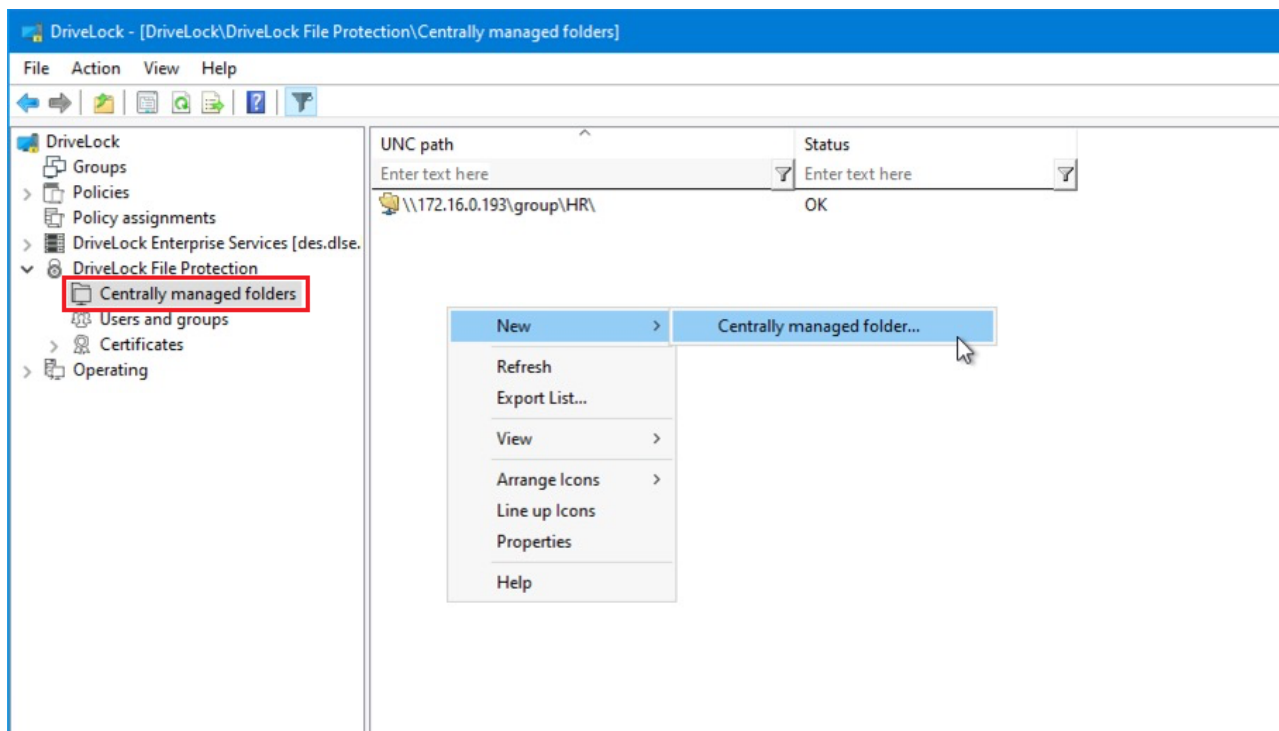
In this case, the group "Human Resources Users Munich" was selected.



For groups, you must select a group administrator. This is configured on the **User** tab.

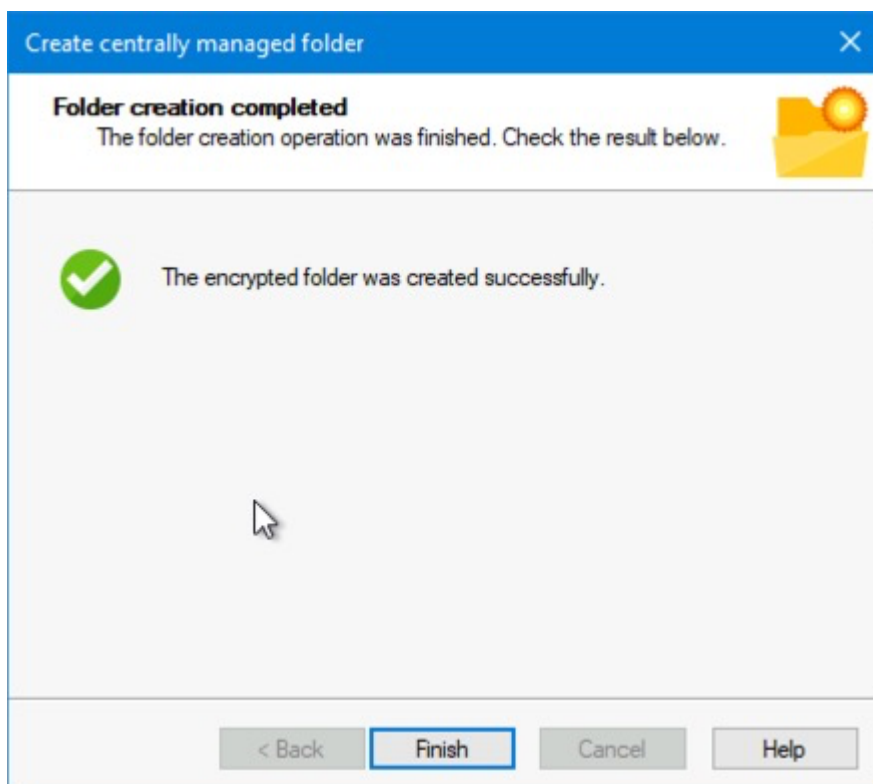
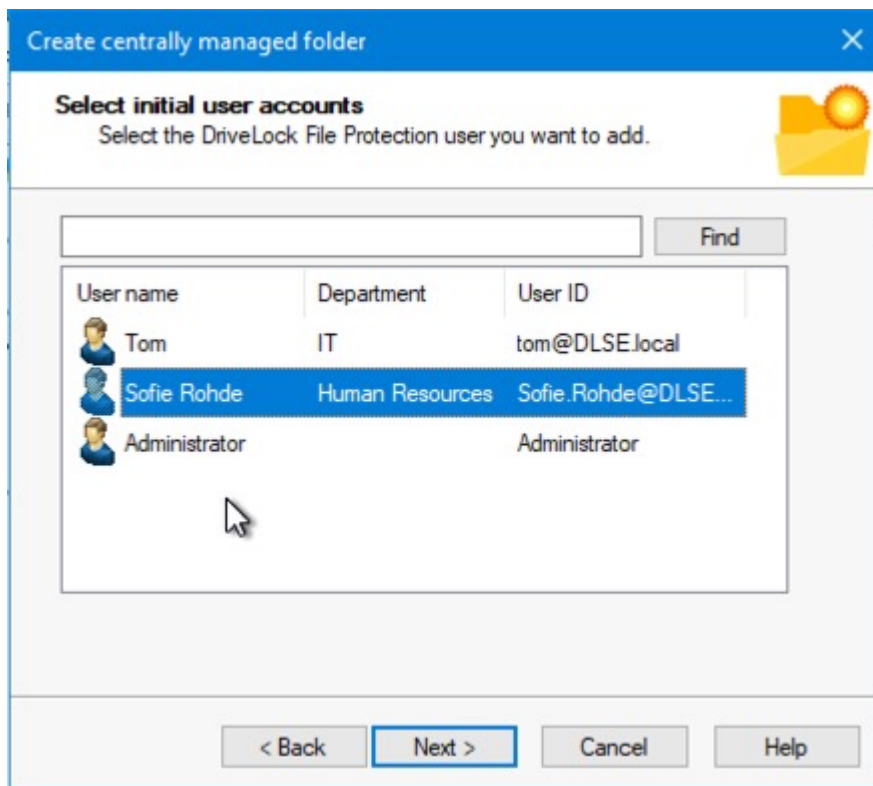


Now select the **Centrally managed folders** sub-node and configure a new centrally managed folder.

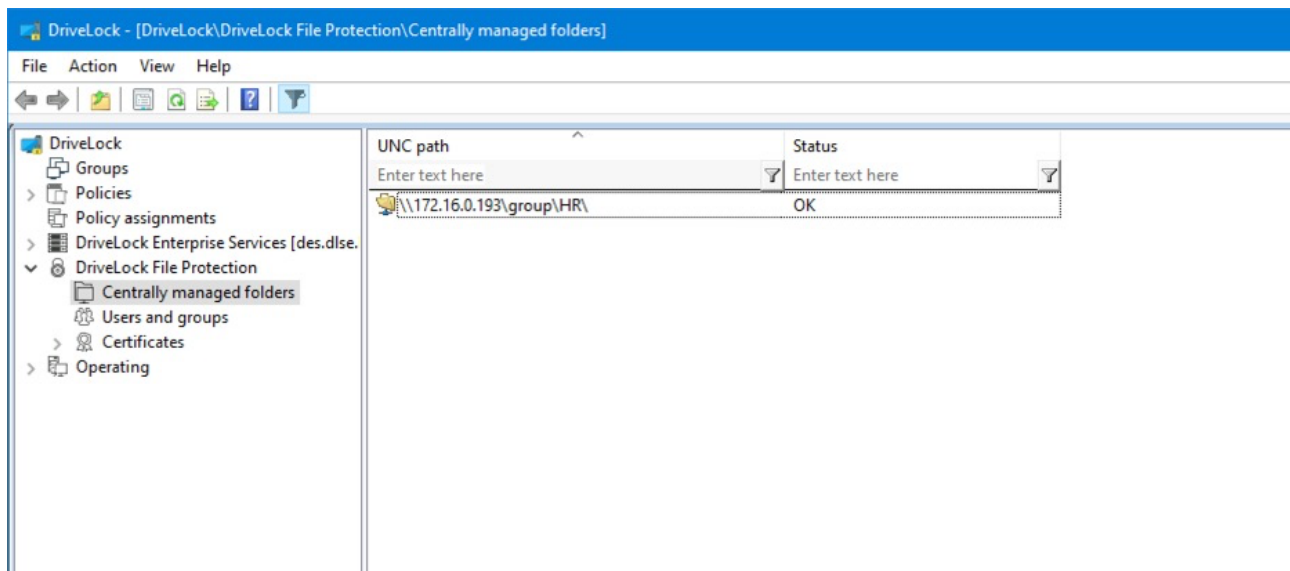


Specify here the UNC path to the network drive or the published folder to be encrypted with DriveLock File Protection.

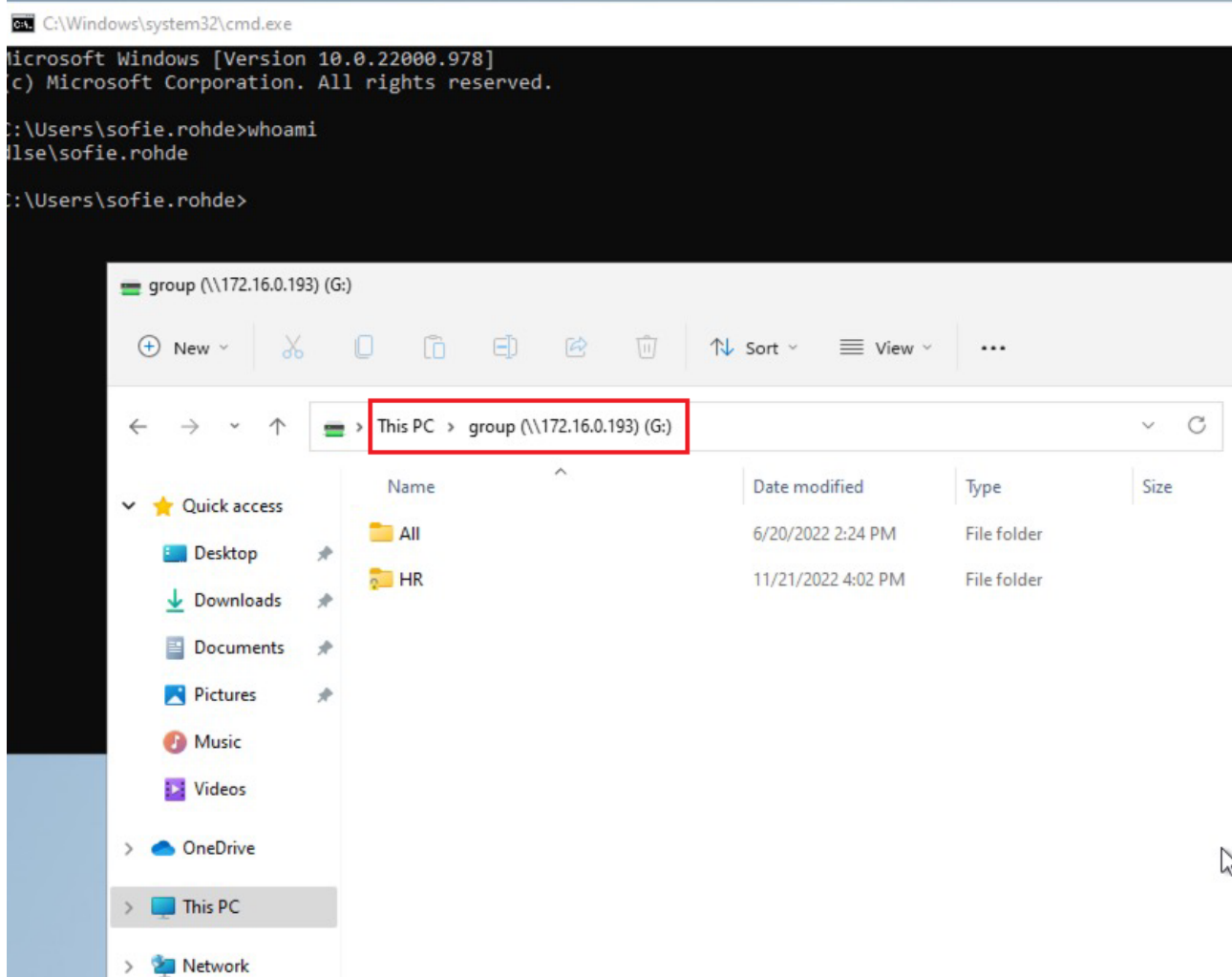
Select the group or user added in the previous step.



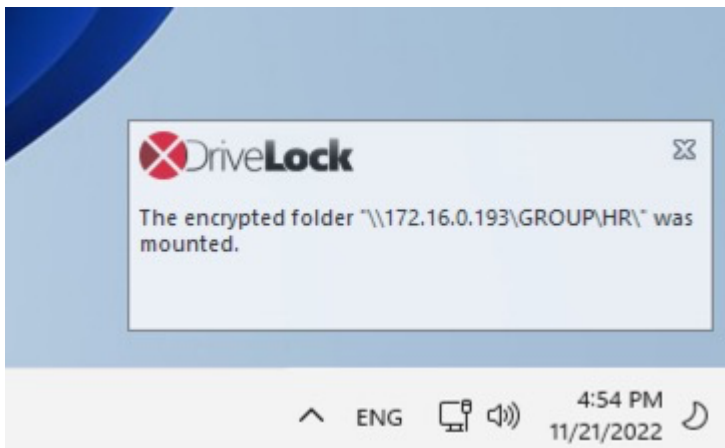
Click Finish. The folder is now encrypted.



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.



7.9 Restore encrypted folders

Recovery may become necessary when a user has lost access to encrypted drives or folders. This may either happen due to the loss of access to a certificate's private key or the forgetting of the password.

To restore access to encrypted drives after forgetting a password or losing a certificate, a so-called offline recovery is performed using a challenge-response method. This involves the user, the administrator or helpdesk personnel.

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 user generates the challenge code using a wizard and provides this code to an administrator. 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.

The procedure a user must complete to initiate recovery are described in the DriveLock User Manual.

The procedure an administrator or helpdesk employee must perform to complete recovery is identical as for drives/containers and described in Recovering Encrypted Drives and Folders.

7.10 File Protection in the DOC

Evaluations, reports and statistics can be performed using the DriveLock Operations Center (DOC). Additionally, the recovery of encrypted folders can be performed using the **File Protection Recovery** view in the DOC.



Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2022 DriveLock SE. All rights reserved.

DriveLock and others are either registered trademarks or trademarks of or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

