



DriveLock Installation

Installation Guide 2021.2

DriveLock SE 2021




Table of Contents

1 WELCOME TO THE DRIVELOCK SETUP	4
2 OVERVIEW OF THE DRIVELOCK INFRASTRUCTURE	5
3 BEFORE INSTALLING DRIVELOCK	7
4 INSTALLING THE DRIVELOCK COMPONENTS	8
4.1 Selecting the components	8
4.2 Installing the server	10
4.3 Installing the database	12
4.3.1 Different procedures for different types of environments	12
4.3.2 Database Installation Wizard	13
5 INITIAL CONFIGURATION IN THE DRIVELOCK MANAGEMENT CONSOLE	18
5.1 First configuration steps	18
5.2 First settings on the DES	19
5.3 First upload of the agent packages to the DES	20
5.4 First steps for creating policies	21
5.4.1 First centrally stored policy	21
5.4.1.1 Licenses	23
5.4.1.2 Agent user interface settings	24
5.4.2 Saving and publishing a policy	25
5.4.3 Assigning a policy	25
5.5 First login to DriveLock Operations Center	26
6 INSTALLING THE DRIVELOCK AGENT	27
6.1 Installation requirements for the DriveLock Agent	27
6.2 Deploying agents via MSI	28
6.2.1 Installation via command line	28
6.3 Push installation via the DOC	30
6.4 Blocked drives on the agent after installation	31

6.5	Checking the DriveLock Agent	31
7	UPDATING DRIVELOCK	33
7.1	Updating the DriveLock Enterprise Service	33
7.2	Updating the database	34
7.3	Updating the DriveLock Agent	35
8	APPENDIX	37
8.1	DriveLock architecture	37
8.2	Communication structure and ports	38
8.3	Files, directories and services for DriveLock	39
8.4	More information about installing the database	40
COPYRIGHT	42

1 Welcome to the DriveLock Setup

DriveLock's mission is to protect enterprise data, devices and systems. With the latest technologies, experienced security experts and solutions based on the Zero Trust model, DriveLock ensures the highest level of security for your data and systems.

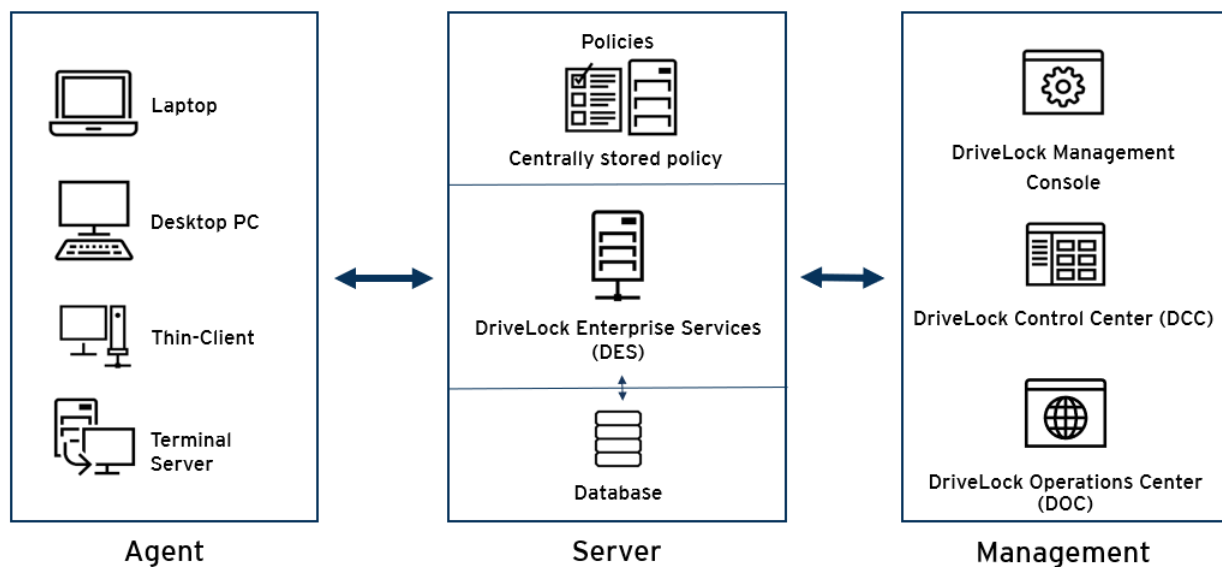
Designed to help you install DriveLock for the first time, this Installation Guide provides instructions on how to quickly and easily install DriveLock's management components on your server and the DriveLock Agent on the client computers in your network.

As an alternative to installing and setting up your environment on your own, DriveLock also offers a comprehensive security solution through our cloud-based Managed Security Service. The service includes hosting the entire solution, managing it with security experts, and tailoring security standards to individual requirements. A separate documentation is available for this solution; you will get it automatically as a Managed Service customer.

2 Overview of the DriveLock infrastructure

The following illustration shows the main components of DriveLock. They interact with each other as illustrated below.

Click [here](#) to see a detailed illustration of the DriveLock architecture with central and linked DES, and [here](#) for information on how communication works and which ports are required.



1. DriveLock Enterprise Service (DES)

The DriveLock Enterprise Service is installed on a server. It is the central component of DriveLock, responsible for distributing the configuration and storing the feedback from the DriveLock Agents.

2. DriveLock Management Components

- The **DriveLock Management Console (DMC)** is a MMC (Microsoft Management Console) snap-in and is used to configure DriveLock.
- The **DriveLock Operations Center (DOC)** is a web console and is responsible for monitoring, reporting or unlocking.
The web version of the DOC is automatically installed with the DES. The DOC is also available as a Windows application (DOC.exe). This must be installed additionally and is required for extended agent remote control functions.
- The **DriveLock Control Center (DCC)** is the predecessor of the DOC. Like the DOC, it provides complete monitoring and management of DriveLock Agents, generating dynamic reports and forensic analysis based on the collected data.

3. DriveLock Agent

The DriveLock Agent is the component of the DriveLock infrastructure that is installed on the end users' computers (client computers). The agent controls such actions as usage of removable media, devices, applications and encryption and security settings.

3 Before installing DriveLock

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

Necessary:

- Create an account that is used to access the DriveLock Enterprise Service (DES). This account does not need to have administrator rights.
- Use Windows Server 2016 for installing the DES.

Optional:

1. If you are using your own certificate authority (CA), create a server certificate for client-server authentication with the following properties:
 - Advanced use:
 - Server authentication (1.3.6.1.5.7.3.1)
 - Use of the key: digital signature, key ciphering, key exchange protocol (a8)
 - When importing to the certificate store, it is essential that the option **Mark the certificate's private key as exportable** is set.
 - DNS alias: if a DNS alias is used for the DES server, the certificate must also be issued for this DNS alias
 - Please note that DriveLock does not support wildcard certificates for the DES.
2. If you do not want to use the provided Microsoft SQL Express Server (for small environments and test environments), you need a Microsoft SQL Server.
3. If the user installing the DES does not have the necessary permissions on the database server, the database administrator should make the following preparations:
 - Create a Microsoft SQL Server database for DriveLock
 - The login used during installation requires only the **public** SQL Server role and must be a member of the **db_owner** role in the DriveLock database.
4. If you want multiple users to be responsible for DriveLock administration, it is useful to create an AD group for the users that will have administrative permissions for DriveLock.



Note: For more information on these topics, see the latest release notes or the Administration Guide at [DriveLock Online Help](#).

4 Installing the DriveLock components

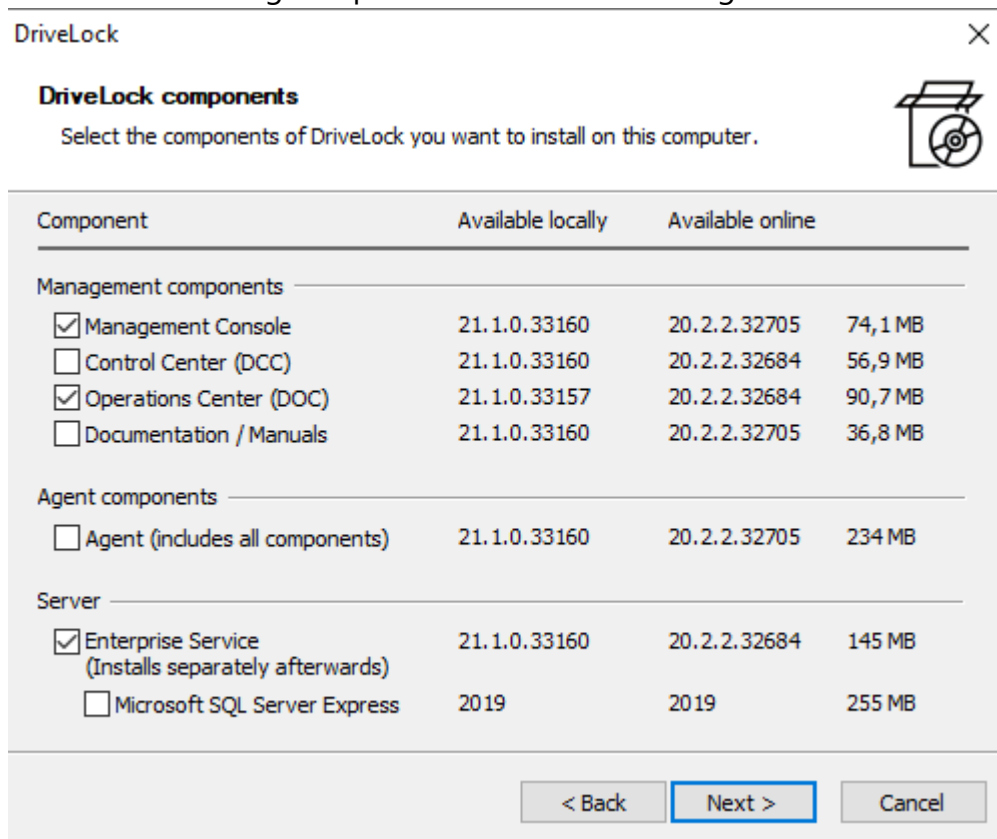
We recommend that you install the management components on the server as well.

However, you can also install the management components separately on individual client computers, for example, in a scenario where you want different users to work with the management components on these computers.

4.1 Selecting the components

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


1. Run the **DLSetup.exe** file from the ISO image.
2. Choose your language and accept the DriveLock EULA.
3. Select the following components as shown in the figure:



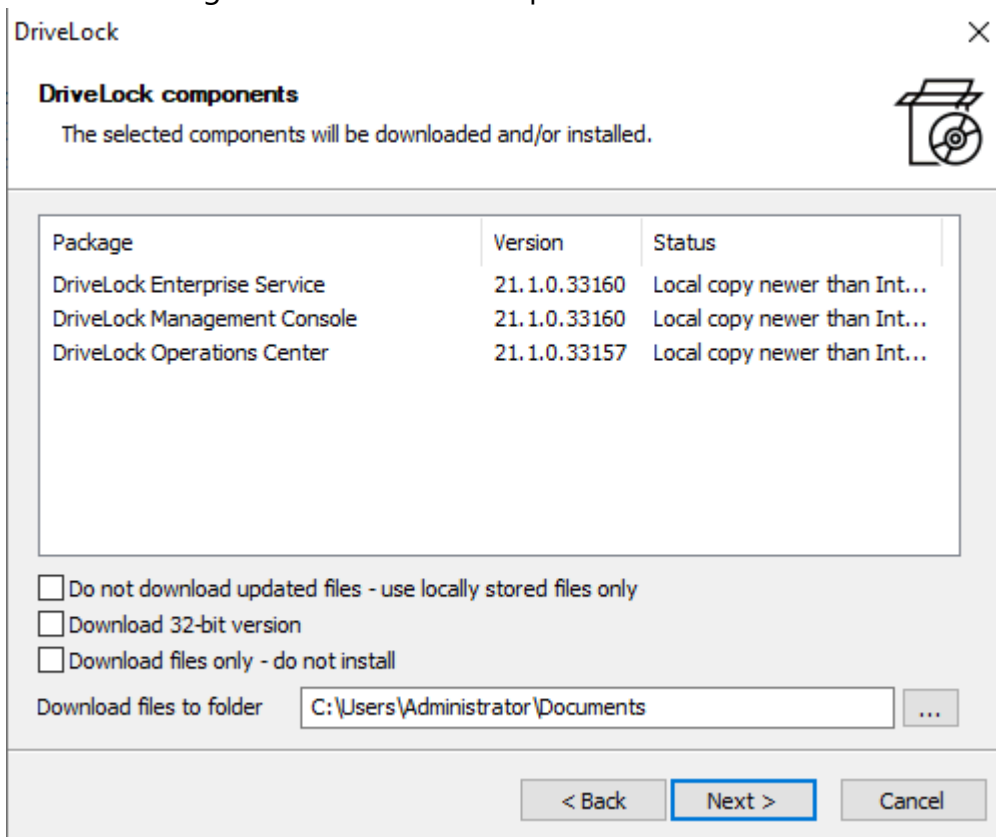
- **DriveLock Management Console**
- **Operations Center (DOC):** This is where the local Windows application (DOC.exe) is installed with advanced agent remote control features.
- **Enterprise Service**

Optionally, you can install a **Microsoft MS SQL Express** Server as a database server.

Beyond 200 devices (enterprise environment), a fully featured SQL Server is recommended.

 Note: You do not necessarily need the options **Control Center (DCC)** and **Documentation / Manuals**. The DCC functionalities come with the DOC and the complete up-to-date DriveLock documentation is available on [DriveLock Online Help](#).

4. The next dialog lists the selected components:



The following options are available:

- The **Do not download updated files- use locally stored files only** option allows you to install the versions stored in the current directory.
- If you do not want to install the previously selected components immediately but only download them over the Internet, you can select the **Download files only - do not install** option.

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

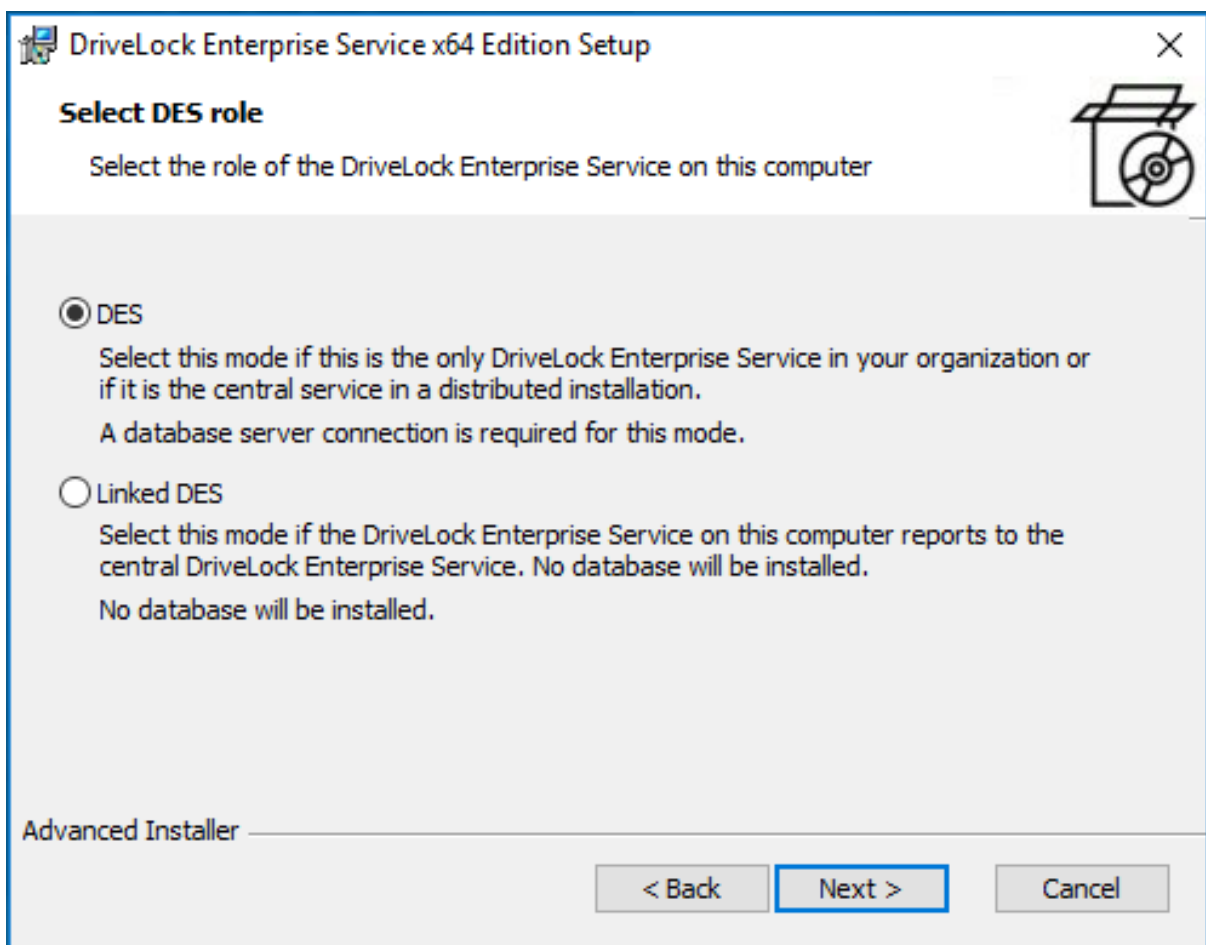
6. The wizard to [install the DriveLock Enterprise Service](#) pops up next.

4.2 Installing the server

Please do the following:

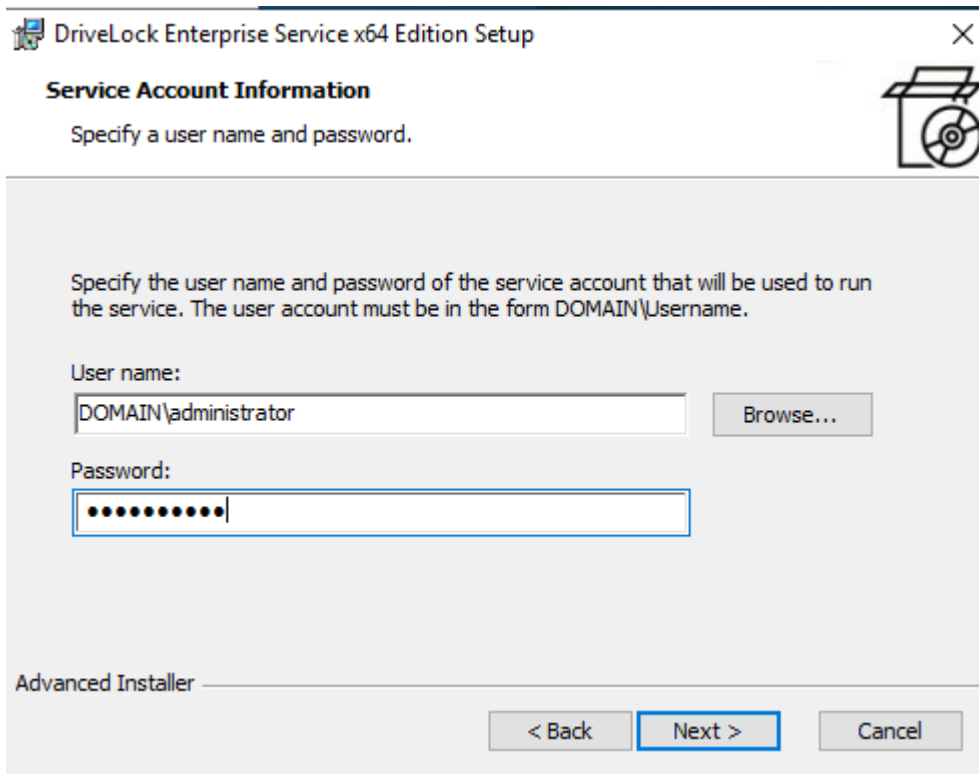
1. In the welcome dialog, click **Next** and then confirm the End User License Agreement (EULA) in the following dialog.
2. Now indicate the role your new DriveLock Enterprise Service (DES) will take. Here, select the **DES** option.

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

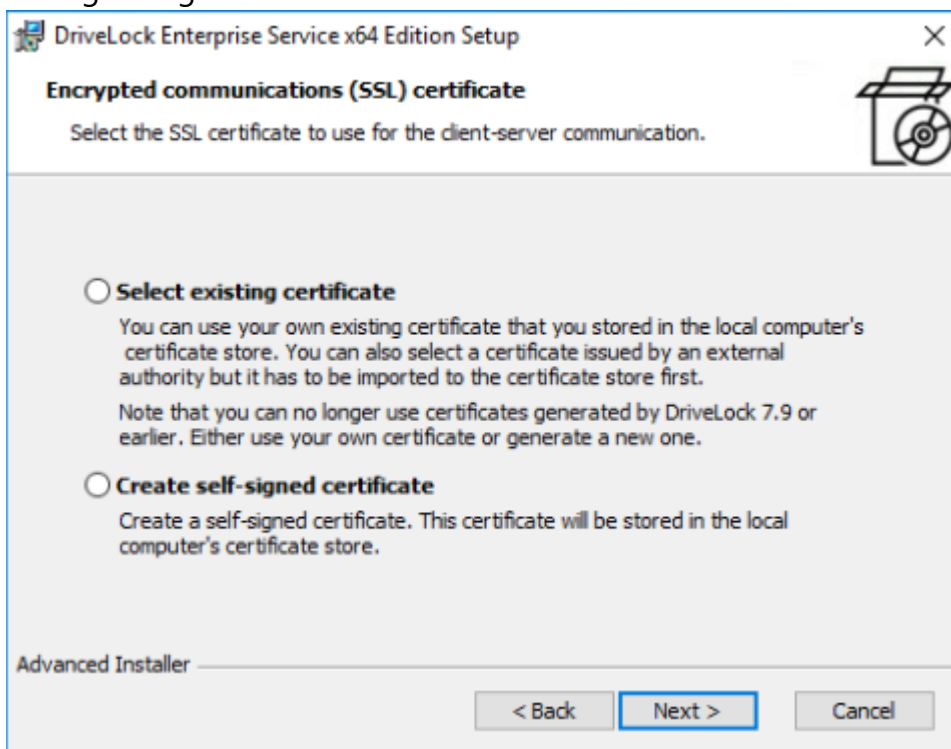


You may select the **Linked DES** option if your infrastructure is already set up with a central DES and you want to add [linked DES](#). In this case, you don't have to create a database again.

3. In the next dialog, enter the service account and the corresponding password you want to use for running the DriveLock Enterprise Service. Click **Browse...** to select an existing account.



4. After you have entered the account and password for the new DES, you will see the following dialog:



Here you have two options:

- Choose **Select existing certificate** if you have your own certificate in the computer's certificate store and want to use it.

Click **Next** and then select the certificate from the list below **More choices** in the next dialog.

- Select **Create self-signed certificate** if you want DriveLock to create an SSL certificate for you. This option may be recommended if you are using DriveLock in test environments.

For more information on certificates, please see the respective section [here](#).

5. Click **Install** in the next dialog to continue installing the DES.
6. Click **Finish** to complete the installation. The [Database Installation Wizard](#) will then start automatically.

4.3 Installing the database

DriveLock supports Microsoft SQL Server and Microsoft SQL Server Express as database system. For exact specifications, please refer to the latest release notes on [DriveLock Online Help](#).

4.3.1 Different procedures for different types of environments

Overview of the scenarios for database installation:

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

	SQL Express data- base.		
Required options for database install- ation:			
Create database	yes	yes	no
Create database login	yes	yes	no
Make DES service account the owner of the database	yes	no	no
Database main- tenance, data cleans- ing and backups	via DES	set up via SQL Server	set up via SQL Server

 Note: For more information, please visit [here](#) and/or see the DriveLock Database Guide in Technical Articles at [DriveLock Online Help](#).

4.3.2 Database Installation Wizard

Follow these steps to install the database:


1. Click **Next** in the **Welcome to DriveLock Database Installation Wizard** dialog.
2. In the following dialog, select the **Central DriveLock Enterprise Service** option if you want to create a new database.
It is the default option if you chose the DES option when installing the server.

Select DES role

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

- Central DriveLock Enterprise Service (default)**
Select this mode if this is the only DriveLock Enterprise Service in your organization or if it is the central service in a distributed installation. A database server connection is required for this mode.
- Linked DriveLock Enterprise Service**
Select this mode if the DriveLock Enterprise Service on this computer reports to the central DriveLock Enterprise Service. No database will be installed.
- Linked DriveLock Enterprise Service connected to the DriveLock Cloud**
Select this mode if the DriveLock Enterprise Service on this computer is part of the managed DriveLock Cloud environment. No database will be installed.

- Use the **Linked DriveLock Enterprise Service** option for creating [linked DES](#). No database will be created.
 - Use the **Linked DriveLock Enterprise Service connected to the cloud** option if you have the DriveLock Managed Service solution and are dealing with agents that do not have a direct Internet connection. In this case, the connection to DriveLock Cloud can be established using the linked DES as an intermediary. For more information about linked DES, refer to the Administration Guide at [DriveLock Online Help](#).
3. Next, specify the connection details for the database server.
- Here you can optionally specify a different user for database access. Windows and SQL Server authentication are possible. This data is not stored and is used exclusively for the installation / update.

 Note: In case you want to specify the port, the Database Installation Wizard supports the following notation: FQDN,Port\Instance (e.g.: myDLServer,14330\SQLEXPRESS)

- After entering the server name, click the **Test connection** button. The connection is established when the green check mark appears. If connection issues occur, they will be displayed in the area under **Messages**. You can then find an

appropriate solution.

- Select **Install a new DriveLock database** as installation action.

The screenshot shows the 'Connect database and select installation action' step of the DriveLock installation wizard. The title bar reads 'Connect database and select installation action.' Below the title, instructions state: 'Enter the connection parameters, run the connection test and select an installation action.'

The form contains the following fields and controls:

- Server:** A text input field with a placeholder value. Below it, a note says: 'Type the full Microsoft SQL Server instance name, for example: localhost\DRIVELOCK'.
- Use a different login to access database during installation**
- User:** A text input field containing 'sqllogin'.
- Password:** A text input field containing '*****'.
- Radio buttons for login type: Windows Login and SQL Login.
- Test connection:** A button that has been clicked, resulting in a green checkmark icon and a text box displaying '15.0.4083.2'.
- Select an installation action:** A section with two radio buttons: Install a new DriveLock database (highlighted with a dashed border) and Check / Update an existing DriveLock database.
- Navigation buttons at the bottom: '< Back', 'Next >', and 'Cancel'.
- A 'Messages' section at the very bottom with a downward arrow icon.

4. There are several solutions for creating the database, based on different [scenarios](#).

- **Create database:**

This option is set by default. The database is created on the SQL server. The account performing the installation must have [appropriate permissions](#) on the SQL Server (dbcreator role). If you deselect this option, you must provide a database. The schema is then installed into this database.

- **Create database login on SQL Server:**

This option is also set by default. A login is created for the **service account of the DES**. The account performing the installation must have appropriate permissions on the SQL Server (securityadmin role).

- **Give DES service account full permission on the database (db_owner). Recommended for SQL Express:**

This option is not set by default. It gives the [DES service account](#) maximum rights to the DriveLock databases, allowing it to perform tasks such as

maintenance (index maintenance), cleaning up old records and backing up the database.

For larger environments or when running on a full SQL Server, we recommend disabling this option.

Configure installation action

Create database

Database name:

Database collation:

Create database login on SQL Server

DES service account:

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

< Back Next > Cancel

Messages

- Next, specify the user accounts for the DOC or DCC and the Management Console. As a rule, this is the user under which the installation is performed.
 - DOC / DCC Administrator:** this user or group will be allowed to access DriveLock Operations Center and DCC later (full access). Other permissions can be customized later.
 - MMC Administrator:** this user or group will later be allowed to configure DriveLock Enterprise Service settings within the DriveLock Management Console. Additional permissions can be assigned later in the DriveLock Management Console

Set up accounts

This step will set up the DriveLock Control Center and DriveLock Management Console administrator accounts.

DOC / DCC administrator: ...

This account manages reports, operation and permissions for DriveLock Operation Center (DOC) and DriveLock Control Center (DCC).

DriveLock Management Console administrator: ...

This account manages DES (DriveLock Enterprise Server) settings, policies, permissions and installation packages.

< Back **Next >** Cancel

Messages

6. Execute actions: The database installation will be executed. Click **Next**.
7. In the next dialog, specify whether you want to enable database maintenance or backup. Accept the default options.
If you want to change the settings at a later time, you can do so in the DES properties. For more information, see the Maintenance and Cleanup chapter of the Administration Guide at [DriveLock Online Help](#).
8. The last dialog provides a summary of your settings. Click **Finish**.

5 Initial configuration in the DriveLock Management Console

Once you have completed the installation of the DriveLock components, DES and database, the new **DriveLock** entry will appear in your Start menu. Start the **DriveLock Management Console** here.

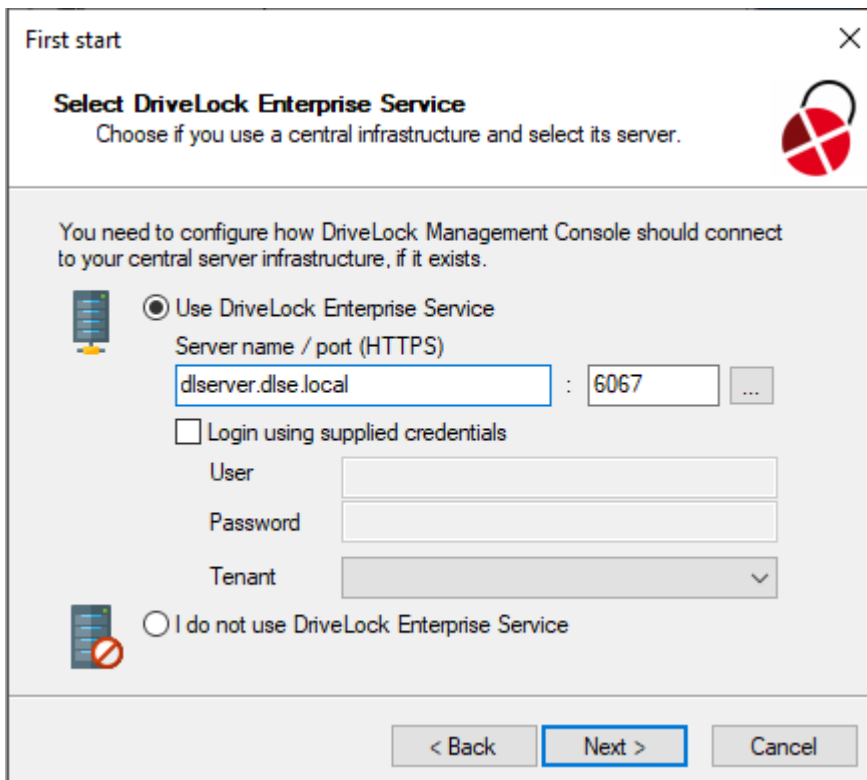
Tip: Pin this entry to your taskbar.

5.1 First configuration steps

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

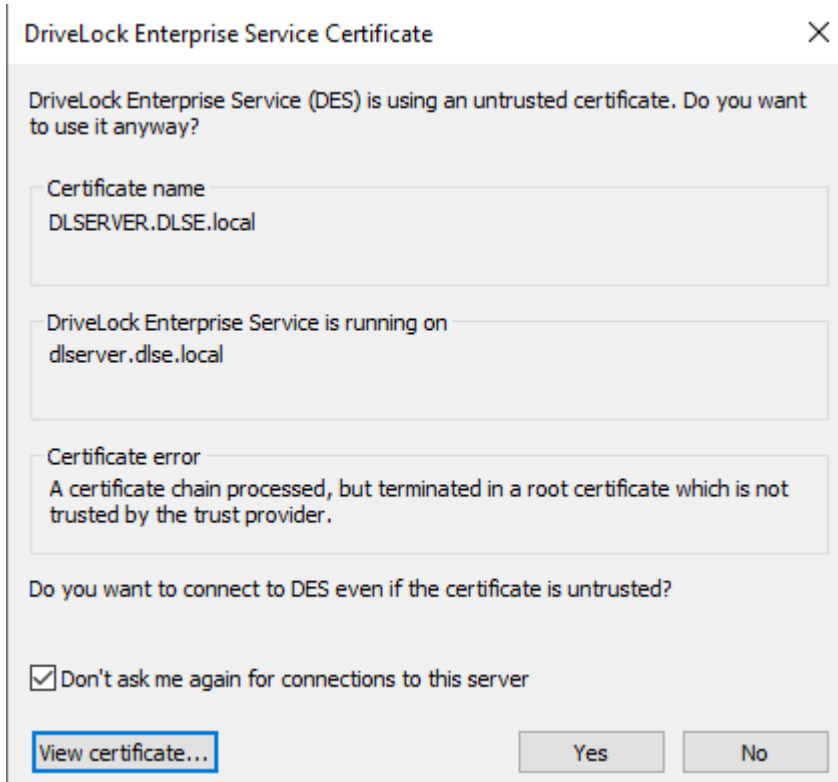
Please do the following:

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



The screenshot shows a dialog box titled "First start" with a close button (X) in the top right corner. The main heading is "Select DriveLock Enterprise Service" with a sub-instruction: "Choose if you use a central infrastructure and select its server." A DriveLock logo is in the top right. Below this, a message states: "You need to configure how DriveLock Management Console should connect to your central server infrastructure, if it exists." There are two radio button options: "Use DriveLock Enterprise Service" (selected) and "I do not use DriveLock Enterprise Service". Under the selected option, there are fields for "Server name / port (HTTPS)" containing "dlserver.dlse.local" and "6067", a "Login using supplied credentials" checkbox (unchecked), and fields for "User", "Password", and "Tenant" (a dropdown menu). At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

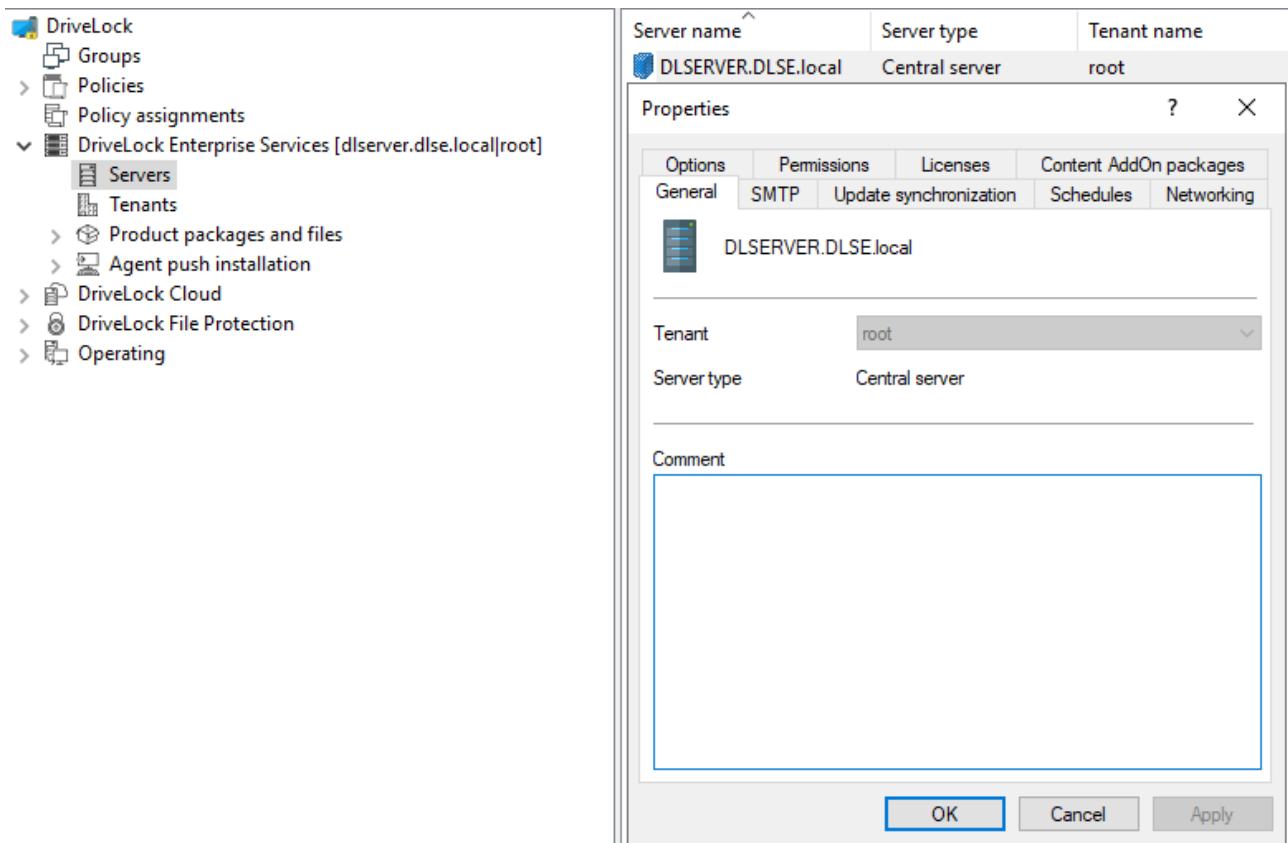
- If the DES uses a self-signed certificate, you will need to confirm the certificate as trusted afterwards.
 - Click the **View Certificate...** button to verify that it is indeed the certificate that the DES is using.
 - Check the option **Don't ask me again for connections to this server.**
 - Confirm with **Yes** to use the certificate.For more information on certificates, please click [here](#).



- In the final dialog, you specify how often you want to check for new versions of the DriveLock Management Console. The version status is verified directly via the DriveLock Cloud.
- Click **Finish** to confirm your entries.

5.2 First settings on the DES

Once you have completed the initial configuration steps, your central server is registered in the **DriveLock Enterprise Services** node.



In the Properties dialog, start by entering the following settings:

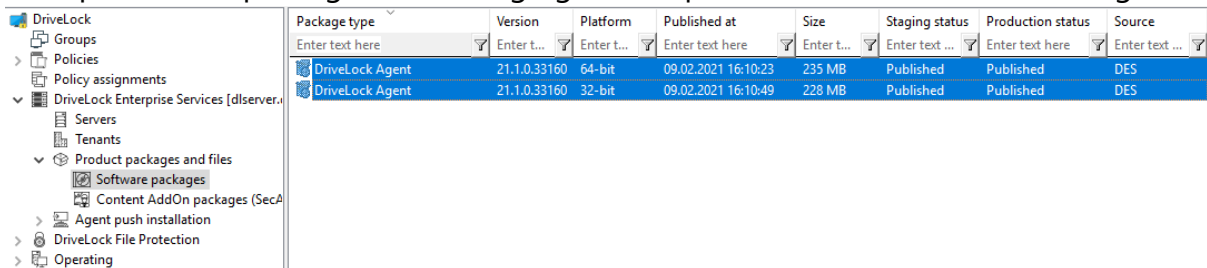
1. On the **Network tab**, check **Enforce HTTPS**. This option ensures that communication only takes place via HTTPS and not via HTTP. For more information, please click [here](#).
2. On the **Update synchronization** tab, leave the option **Download software updates from the Internet** enabled so that the software packages for your DriveLock components are always up to date.
3. On the **Permissions** tab you can add additional users who are allowed to access the DES and the management components. By default, the account specified during installation is granted full access to the server configuration, centrally stored policy configuration, and DriveLock File Protection.
At this point you can enter the AD group for the users who will have administrative permissions.
4. Once you have completed your settings, you will be prompted to restart DES.

5.3 First upload of the agent packages to the DES

We recommend uploading and publishing the agent packages to DES to ensure that the automatic update and [push installation](#) work.

Please do the following:

1. The DriveLock ISO image contains the two msi packages for the DriveLock Agent. Copy it to any place on your computer.
2. Then go to the **Product packages and files** node in the DriveLock Management Console, select **Software packages** and choose **Upload package** from the context menu.
3. Select the appropriate package or the two agent packages and upload them to DES. They will then appear in the list of software packages.
4. Now publish the packages in the staging and/or production environment, see figure:



Package type	Version	Platform	Published at	Size	Staging status	Production status	Source
DriveLock Agent	21.1.0.33160	64-bit	09.02.2021 16:10:23	235 MB	Published	Published	DES
DriveLock Agent	21.1.0.33160	32-bit	09.02.2021 16:10:49	228 MB	Published	Published	DES

For more information on push installation, see the corresponding chapter in the Administration Guide at [DriveLock Online Help](#).

5.4 First steps for creating policies

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

Using centrally stored policies (CSP) is a good practice because...:

- CSPs are stored in the DriveLock database; from there, the agents receive them via the DriveLock Enterprise Service
- CSPs are automatically subject to versioning; administrators can edit or publish them separately
- it is possible to create any number of policies (or even just one) and assign them to agents. Please also refer to the note in the [Licenses](#) section.

You can find more details about how to create and employ CSPs in the Administration Guide at [DriveLock Online Help](#).

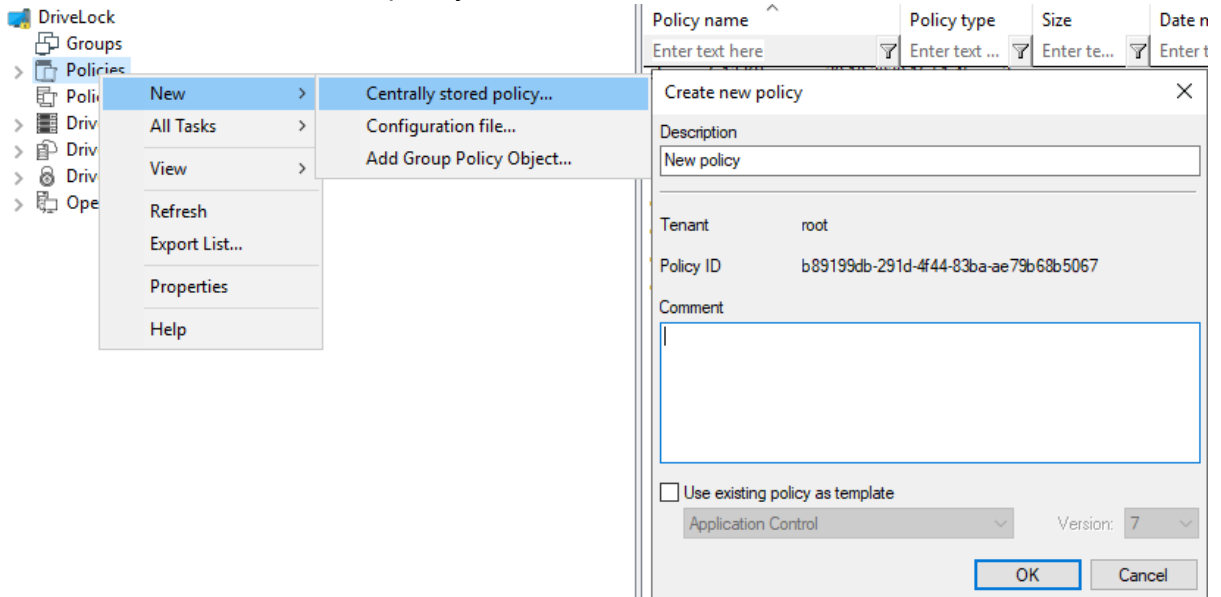
Now we will help you create your first centrally stored policy step by step, apply some basic settings, and then assign the policy.

5.4.1 First centrally stored policy

Here are the steps:

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

2. Enter a name and store the policy.




3. The new policy now appears in the list.

4. Then go to the **Global configuration** node first. The settings described below are basic settings and provide a minimum configuration. All other settings are explained in the Administration Guide.

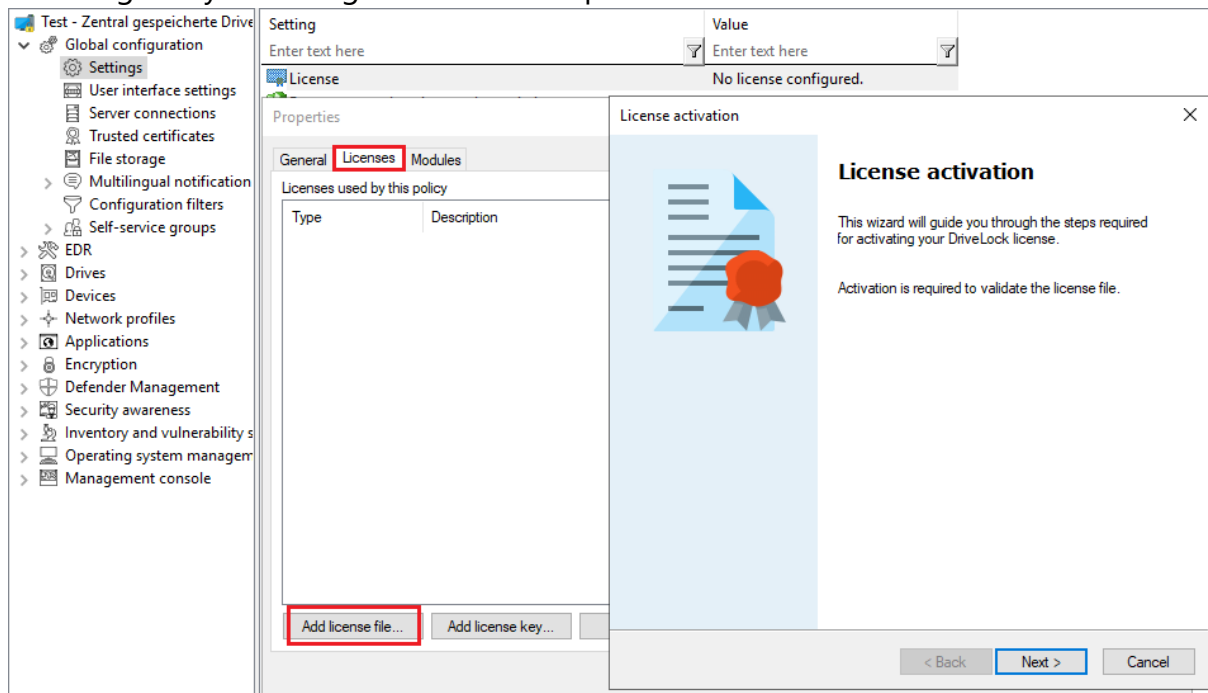
5.4.1.1 Licenses

First, enter your DriveLock licenses directly into the policy.

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

Please do the following:

1. Go to the **Settings** subnode and select **License**.
2. On the **Licenses** tab, you will enter your purchased licenses. You can do this directly by adding a license file or a license key, depending on what you have available. A wizard will guide you through the activation process.



3. Once the license is entered into the system, your licensed DriveLock modules will be displayed on the **Modules** tab.
4. Select all of them here and click the **Edit** button.
5. Now you can specify the computers where the modules will be available. Click **Add** and select **< Any computer >** from the list.

Note: You can also specify other settings here and restrict the modules to individual computers, groups or OUs. For more information, see the Administration Guide at [DriveLock Online Help](#).

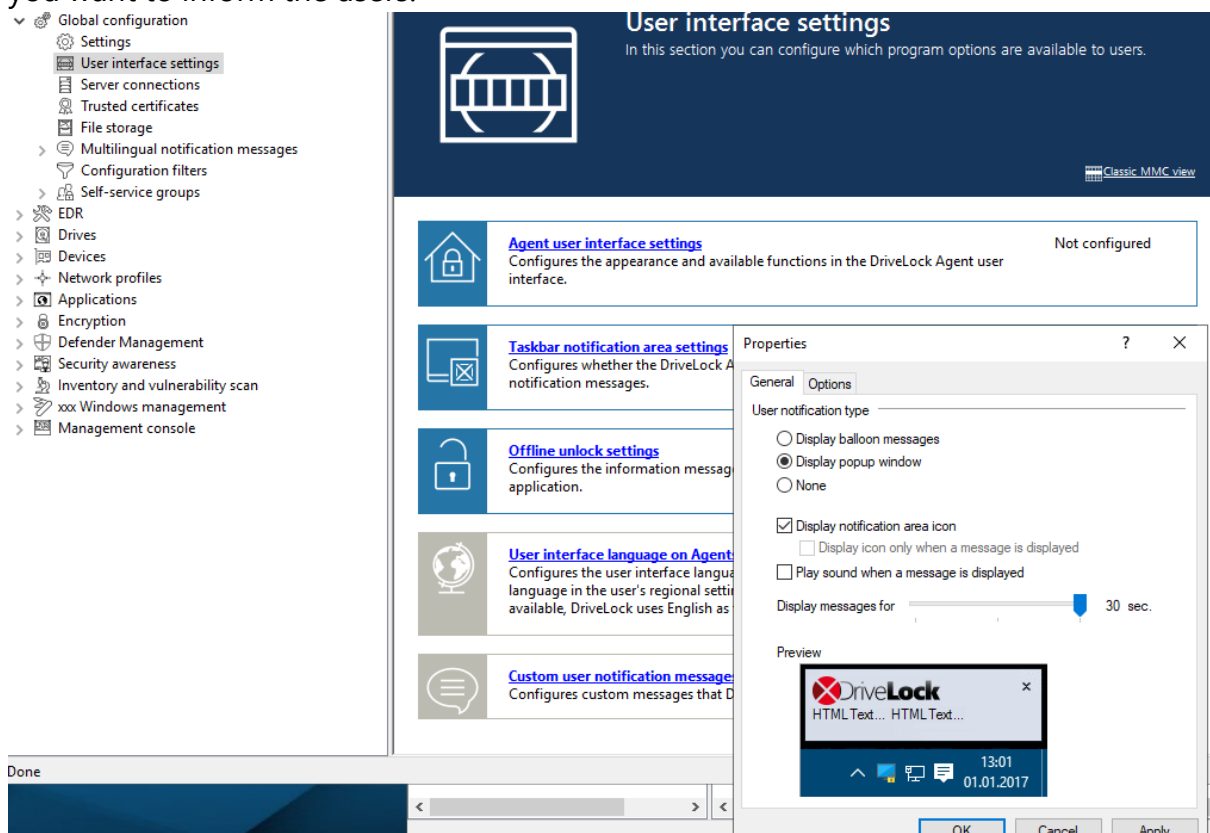
6. Confirm your selection and save your license settings.

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

5.4.1.2 Agent user interface settings

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


1. In the Global configuration node, open the **User interface settings** and the **Taskbar notification area settings**.
2. On the **General** tab, select **Display notification area icon** and then one of the two options **Display popup window** or **Display balloon message**, depending on how you want to inform the users.



3. Confirm your settings with **Apply** and **OK**.

5.4.2 Saving and publishing a policy

Any changes to policies should always be saved and published.

Save : Changes are saved for DriveLock administrators.

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

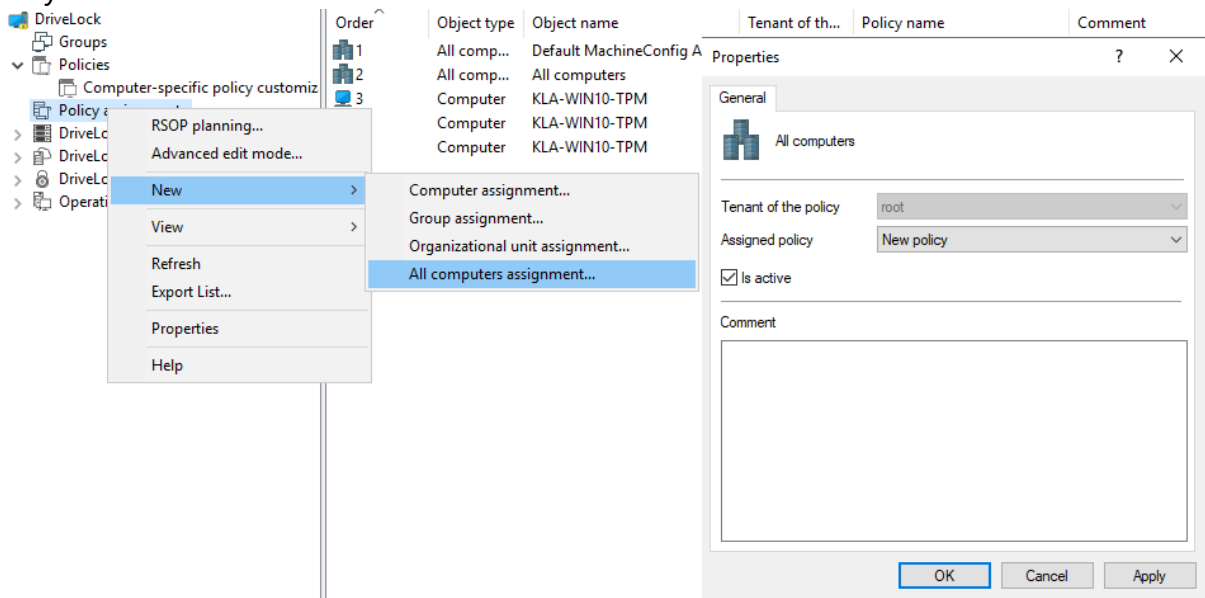
5.4.3 Assigning a policy

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

See the Administration Guide for more detailed information. During the initial installation, you will first assign your new policy to all computers.

Please do the following:

1. Go to the **Policy assignments** node and open the **New** command from the context menu.
2. Select **All computers assignment...**
3. Select the policy you have just created as **Assigned policy**, enter a comment if necessary and confirm with **OK**.



4. Your policy is now ready to be assigned to agents.

5.5 First login to DriveLock Operations Center



Note: For more information on the DOC, see the DriveLock Control Center manual at [DriveLock Online Help](#).

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

Please note the following:

- Only AD users can log in.
- Warnings may be issued in certain cases because SSL certificates are used.
- You can set or change the language at this point.
- Any DriveLock user who has full Helpdesk privileges can log in with their respective password.
- The AD group for the administrative users can be entered in the Settings view under Accounts.

6 Installing the DriveLock Agent

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



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

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

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

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

- By creating a [modified Windows installation package \(MSI file\)](#) or a Windows Installer transform (MST file).
- By using [Windows Installer command line parameters](#).

6.1 Installation requirements for the DriveLock Agent

For details on supported versions and installation requirements for the DriveLock Agent, see the latest release notes at [DriveLock Online Help](#).

6.2 Deploying agents via MSI

Please do the following:

1. Go to the **Policies** node in the DriveLock Management Console, open the **All Tasks** context menu and select **Deploy centrally stored policy....**
2. Start the Agent Deployment Wizard. The wizard queries all required parameters and generates the corresponding output.
3. In the second dialog, select the centrally stored policy you have created for use by DriveLock Agents and the server where the central DriveLock Enterprise Service is installed.
4. In the next dialog, select the type of installation package you want the wizard to create:
 - **Microsoft Installer File (MSI):** Creates a new Microsoft Installer package that contains the previously specified settings.
 - **Microsoft Installer Transform file (MST):** Creates a Microsoft Installer Transform (MST) file with the selected settings. You can use a MST file together with the original MSI package that is included in the DriveLock installation.
 - **Command line:** Displays the command line syntax with the selected settings for the Microsoft Installer.
5. Specify the path and name of the original DriveLockAgent.msi file and the new MSI file.
6. Start the agent deployment.

6.2.1 Installation via command line

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

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

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

The following example shows an installation with custom parameters:

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

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

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

USESERVERCONFIG=1	Indicates that a centrally stored policy is being used.
CONFIGID=<GUID>	<GUID> is the GUID of the centrally stored policy in the form: XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX
CONFIGSERVER=<name>	<name> is the server name on which the DriveLock Enterprise Service has been installed and from which the policy is to be loaded
TENANTNAME=<tenant>	<tenant> is the tenant name the policy is to apply to. If you have not configured any tenants, please use "root" as tenant name.
USEPROXY=1	Indicates that a proxy is to be used
PROXY=named;<proxy>:<port> PROXY=pac;<pac url> PROXY=netsh	<named>: use specific proxy <pac>: use Proxy Auto Configuration Script with URL <netsh>: use system proxy set with netsh
PROXYACCOUNT=<authscheme>; <proxyuser>;<proxypassword>	Specify an account if the proxy requires authentication. <proxyuser>: User <proxypassword>: Password

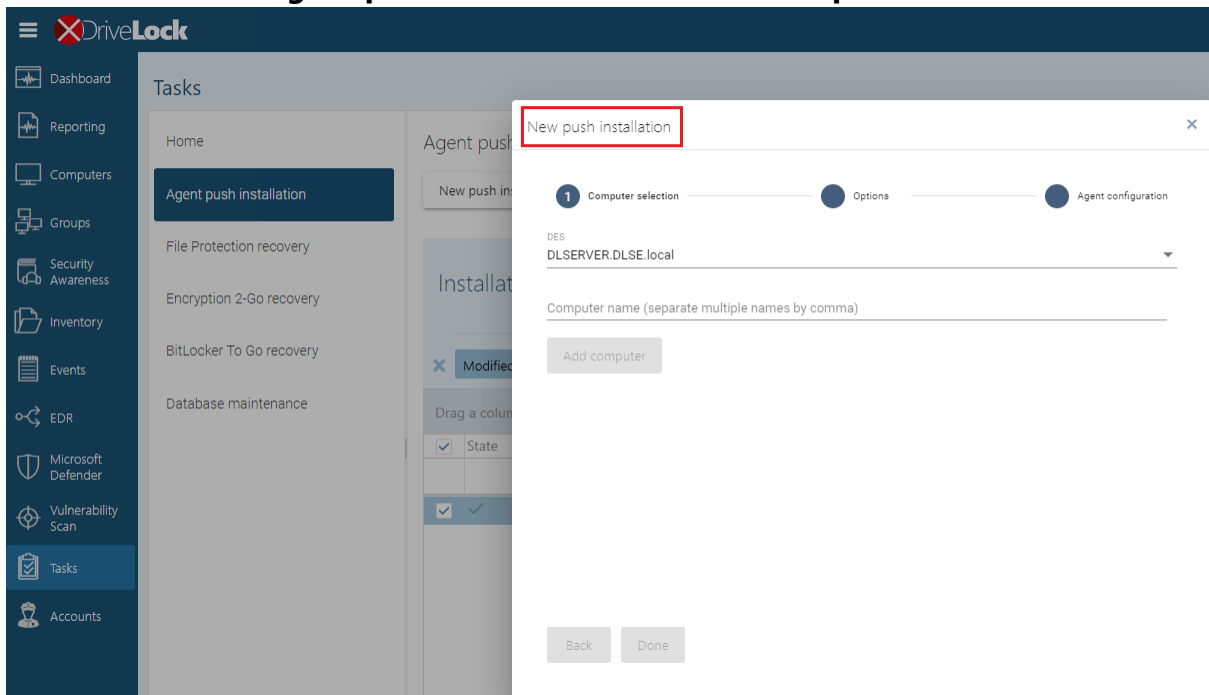
<authscheme>: possible values for the authentication scheme are basic, ntlm, passport, digest, negotiate.

6.3 Push installation via the DOC

This type of installation is especially suited for trial installations and maintenance.

Please do the following:

1. Open the DriveLock Operations Center (DOC).
2. From the menu on the left, select the **Tasks** view.
3. In this view, select **Agent push installation** and then **New push installation**.



4. Enter your DES and the name of the client computer where you want to install the agent. Repeat the process to add multiple computers.
5. The push installation may take some time. Once it has been successfully performed, the status of the computer is indicated with a green check mark.

6.4 Blocked drives on the agent after installation

Note that in the default settings of a new policy, access to the following drives is blocked on the DriveLock Agent. You can change these settings at any time.

Warning: Once the DriveLock Agent is installed on client computers, and thus the policy with these settings is in effect, users will no longer be able to connect USB sticks or other drives.

Setting	Value
Enter text here	Enter text here
Floppy disk drives	Not configured (Locked)
CD-ROM drives	Not configured (Locked)
USB bus connected drives	Not configured (Locked)
Firewire (1394) bus connected devices	Not configured (Locked)
SD card drives (SD-bus)	Not configured (Locked)
Other removable drives	Not configured (Locked)
Fixed disks (eSATA and other non-removable, non-system h...	Not configured (Not locked)
Encrypted volumes	Not configured (Not locked)
Network drives and shares	Not configured (Not locked)
WebDAV-based network drives	Not configured (Not locked)
Windows Terminal Services (RDP) client drive mappings	Not configured (Not locked)
Citrix XenApp (ICA) client drive mappings	Not configured (Not locked)

Using drive whitelist rules, access to certain drives can be allowed. Alternatively, you can configure access rights in the Drives section of the policy. See the Administration Guide at [DriveLock Online Help](#) for details.

6.5 Checking the DriveLock Agent

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

- Check for the DriveLock Agent icon in the Windows system tray.



If you open the context menu, you can also display the **agent status** here.

- Open the DriveLock Agent user interface. On the **Status tab** you can view the configuration status of the agent by clicking on the corresponding icon.
- Check whether DriveLock and DriveLock Health Monitor are active in the Services list. Both services must be running.

You can also use the following command line:

- `sc query drivelock` and/or `sc query dlhm`: to search for DriveLock services
- `drivelock -showstatus`: to check what is licensed on the agent and what server agents are connected to


When using the push installation:

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

Verification in the DOC

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

7 Updating DriveLock

 Note: Refer to the latest release notes at [DriveLock Online Help](#). for additional information on updating DriveLock.

It is not necessary to uninstall an older version of DriveLock, the update is performed automatically by installing a newer package "on top" of the older version. When updating, perform the same steps described in the chapters [Installing the components](#), [Installing the server](#) and [Installing the database](#).

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

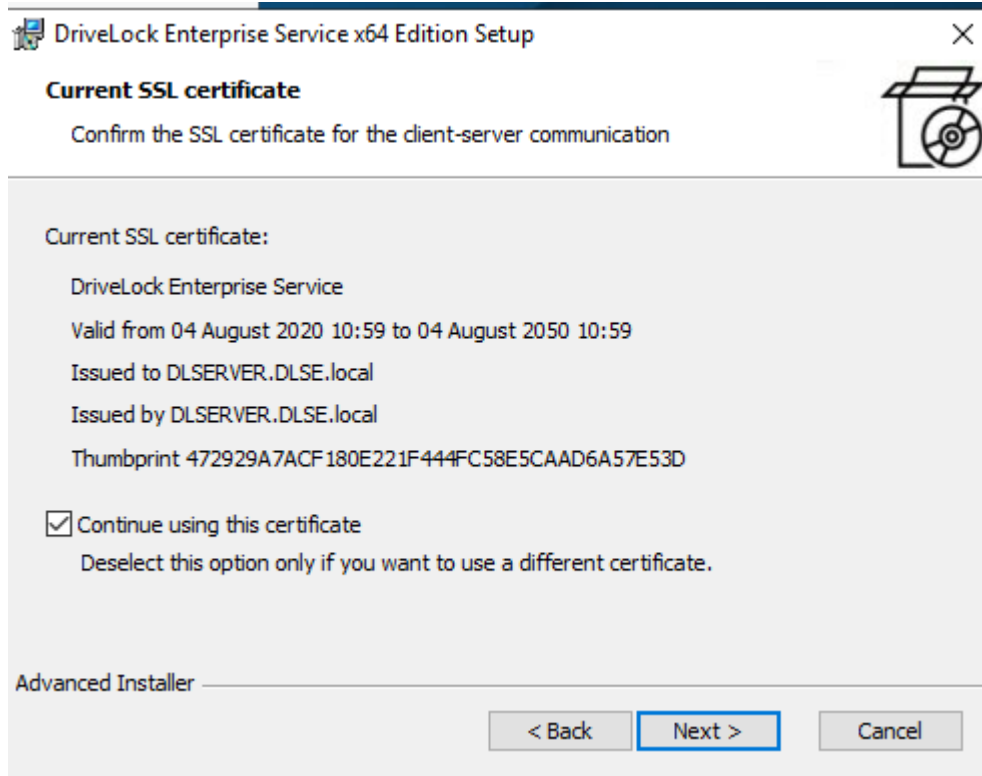
Note the following differences:

7.1 Updating the DriveLock Enterprise Service

Please note the following:

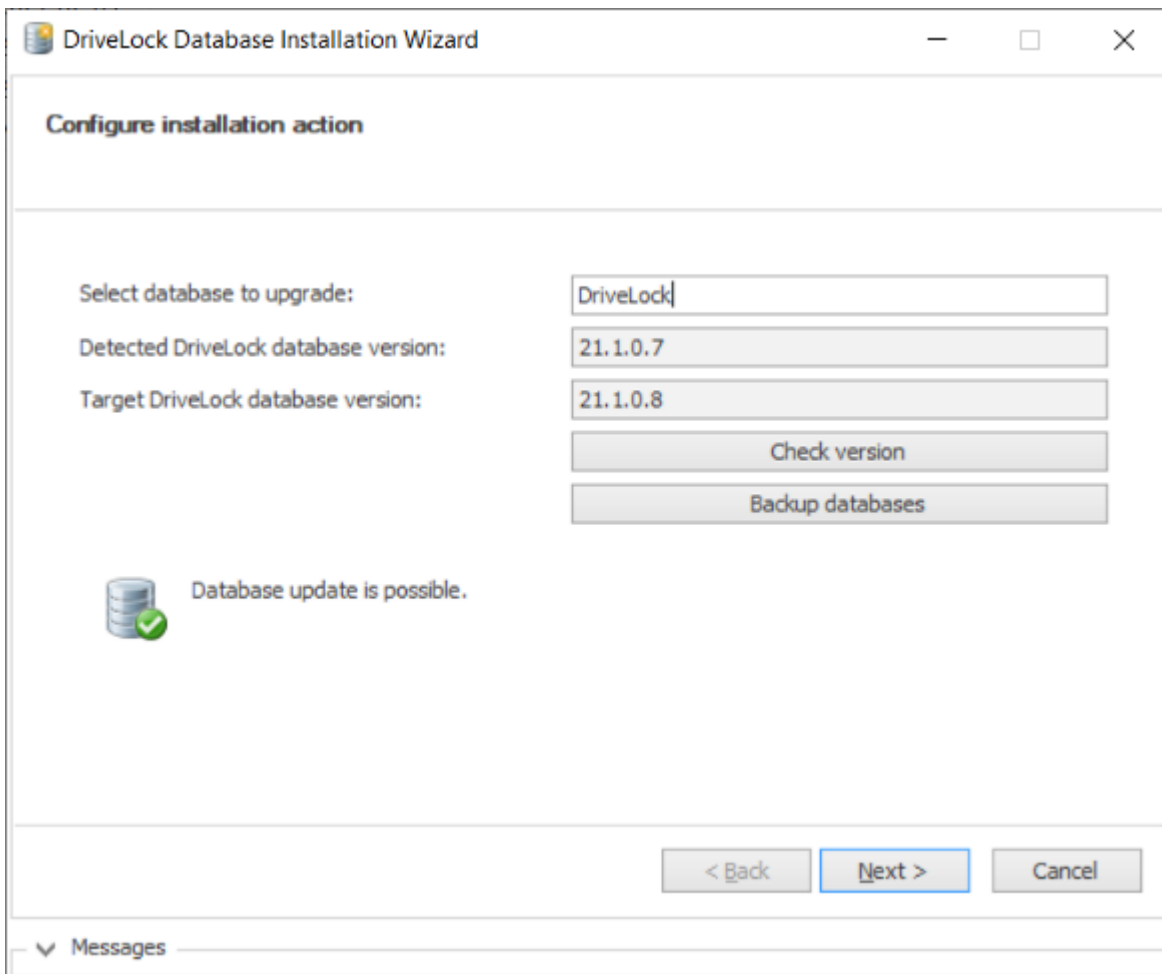
1. Update the DriveLock Enterprise Service (DES) before updating the DriveLock management components.
2. Before you start the update, you need a valid license including maintenance. You can renew it in your current DriveLock Operations Center (DOC). If you have any questions about your license, please contact DriveLock Support.
3. When updating the DES, you must confirm the certificate you have selected for communication between DriveLock Management Console or DriveLock Agents and the

DES. An additional dialog in the DES Setup Wizard shows you the certificate:



7.2 Updating the database

When updating the database, you will first go through the Database Installation Wizard as well. However, after the connection test, select the option **Check / update an existing DriveLock database**. The following dialog will then appear, displaying the database versions:



7.3 Updating the DriveLock Agent

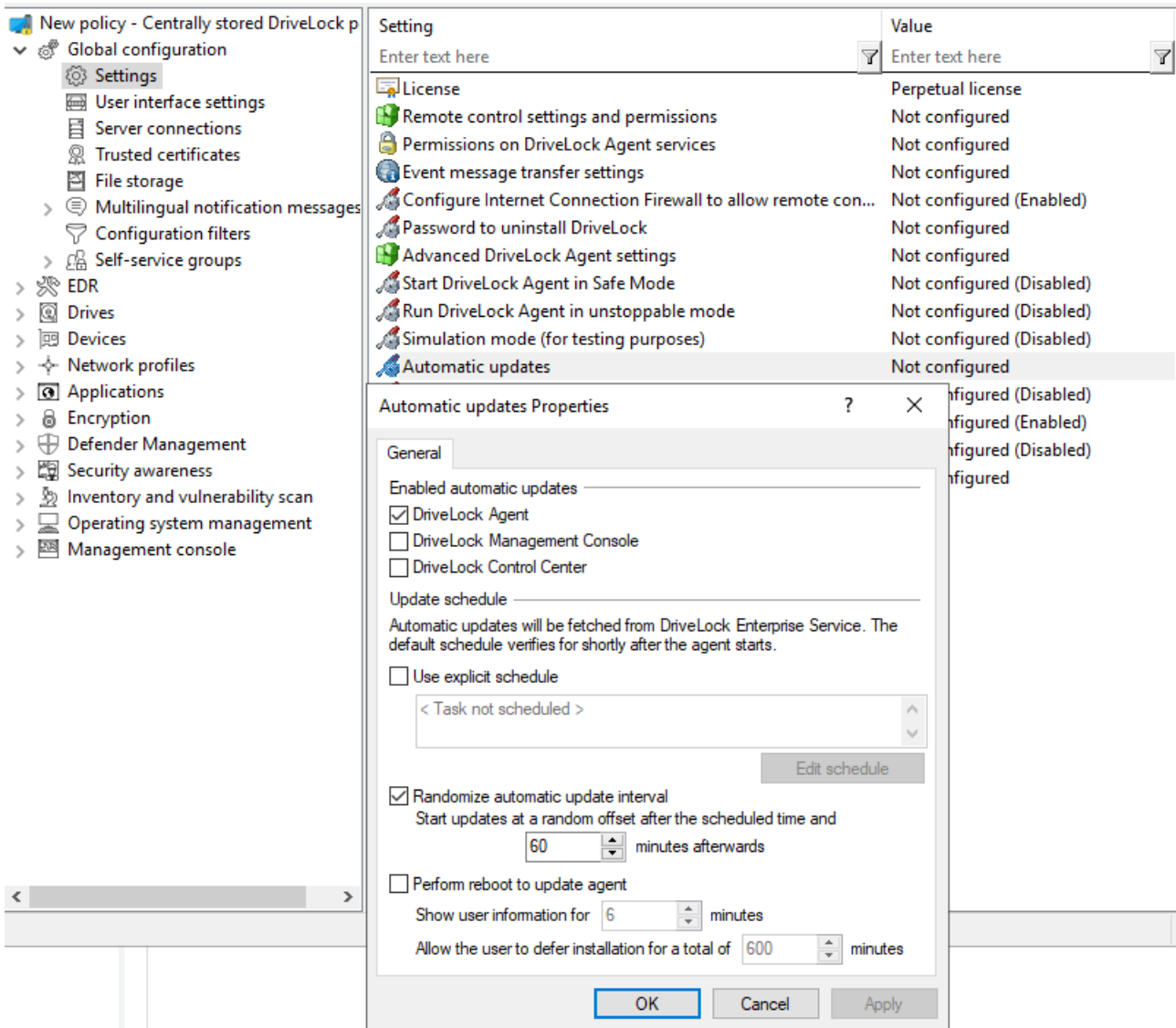
Note: The version of the DriveLock Agent may be lower, but never higher than the version of the DriveLock Enterprise Service. We recommend that all DriveLock components have the same version.

Manual installation

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


Automatic installation

The DriveLock Agent can perform automatic updates. This option is enabled by default in the following setting in the DriveLock policy:



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

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

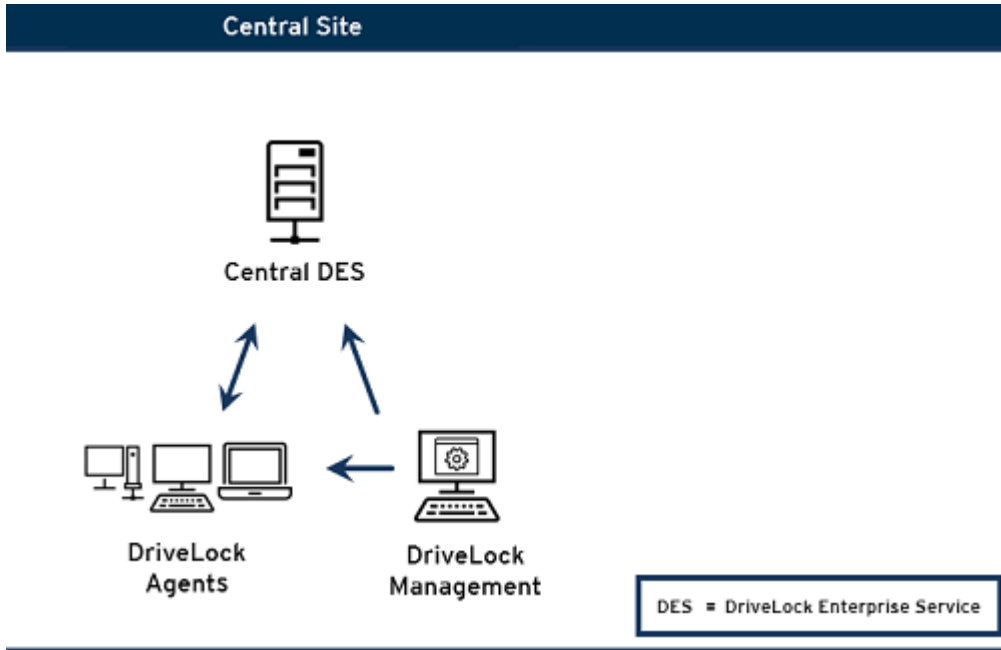
 Note: Please also refer to the notes on updating the agent in the current release notes at [DriveLock Online Help](#).

8 Appendix

8.1 DriveLock architecture

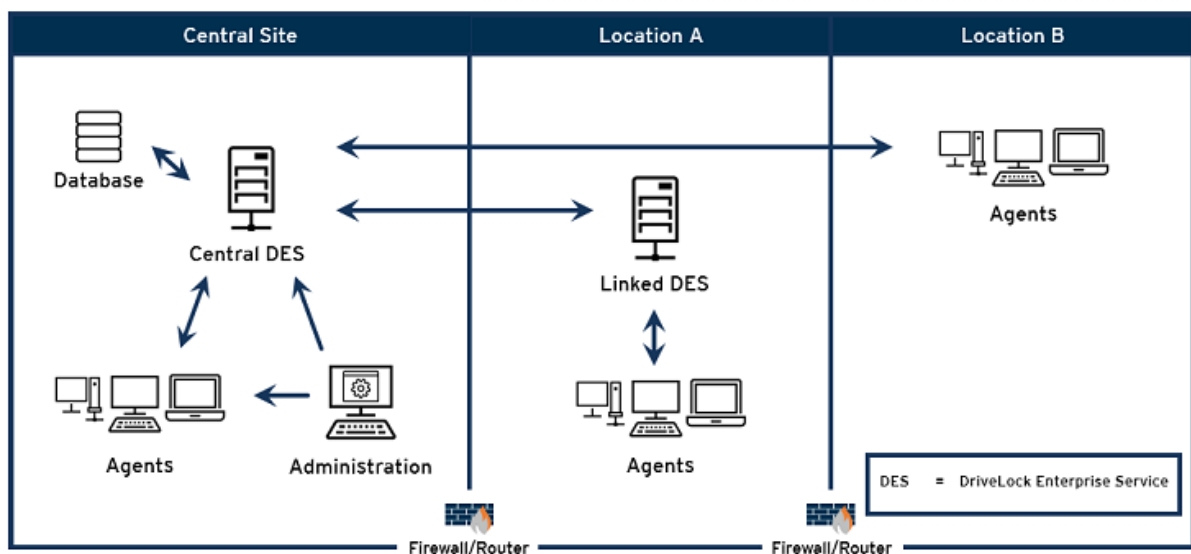
The central DriveLock Enterprise Service (DES) relies on a database for storing the configuration and feedback from the agents.

- Architecture with central DES:



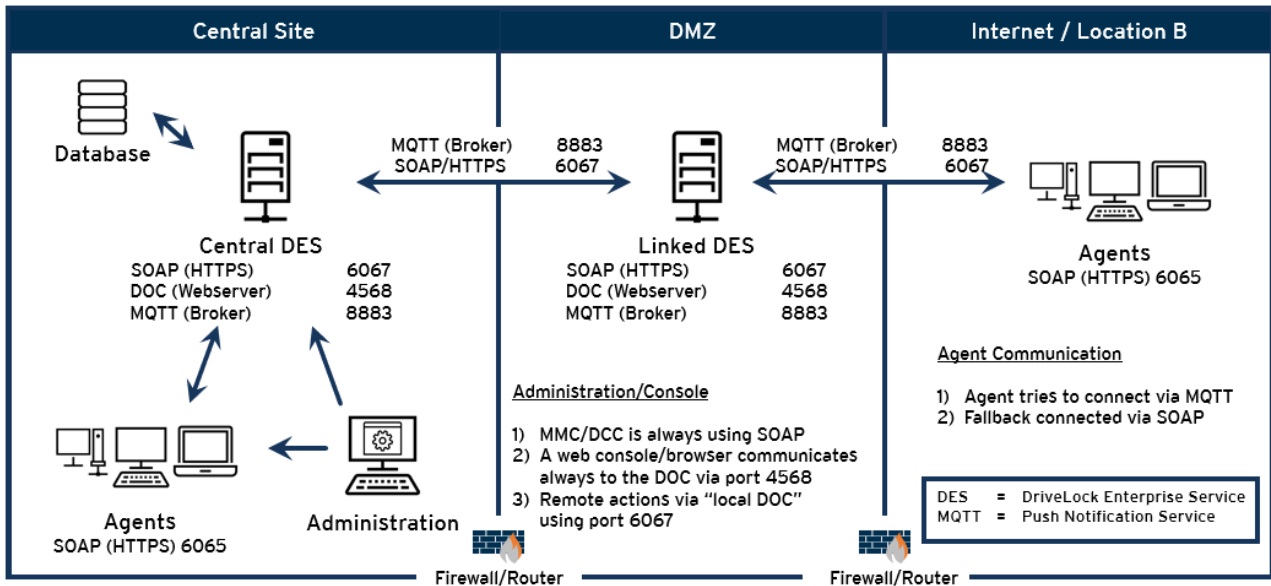
You can also use linked DES that do not access the database directly, but interact with it via the central server. In large DriveLock environments, this can reduce the use of system resources and network bandwidth of the central DES.

- Architecture with linked DES:



8.2 Communication structure and ports

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



List of ports required:

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

DOC (Webserver)	4568
LDAP	389

8.3 Files, directories and services for DriveLock

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

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

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

Files and directories:

- "C:\SECURDSK" (EFS).
- "C:\Program Files\CenterTools\DriveLock" (application directory).
- "C:\ProgramData\CenterTools DriveLock" (cache/working directory)

Processes/Services:

- **DriveLock**
Display name: DriveLock
Executable path: "C:\Program Files\CenterTools\DriveLock\DriveLock.exe"
- **dlhm**
Display name: DriveLock Health Monitor
Executable path: "C:\Program Files\CenterTools\DriveLock\DLHM.exe"
- **StorageEncryptionService**
Display name: DriveLock Full Disk Encryption Encryptor
Executable path: "C:\Program Files\CenterTools\DriveLock\DIFdeEncSvc.exe"
- **ClientDataManager**
Display name: DriveLock Full Disk Encryption Manager
Executable path: "C:\Program Files\CenterTools\DriveLock\DIFdeMgr.exe"
- **dlupdate**
Display name: DriveLock Update and Installation
Executable path: "C:\Windows\DLUpdSvc.exe"
- **dessvc**

Display name: DriveLock Enterprise Service

Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DES.exe"

- **DESTray**

Function: Displayed in the taskbar with the DES icon

Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DESTray.exe"

- **DesRestarter**

Function: Restarts the DES service

Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DesRestarter.exe"

8.4 More information about installing the database

The following accounts are involved in the installation:

- The DES service account is the Windows account used to run the DES service. This is specified during installation and gains access to the database through the installation.
- The Windows account that installs the DES and has local administrator rights. This is usually the logged-in user who performs the installation.
- By default, the account used to access the database is the same account that performs the installation. However, you can specify a different Windows or SQL Server authentication in the installation wizard.

Permissions for the database installation

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

SQL server roles:

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

Alternatives for enterprise environments:

- A SQL Server administrator can arrange for creating the database and the login for the DES service account. The login used during installation requires only the **public** SQL Server role and must be a member of the **db_owner** role in the DriveLock database.
- During the installation, you can choose whether to create the database or use a prepared database. You can also specify whether to create the login for the DES service account or not. This will allow customizing the required permissions on the SQL Server

for the installation login.


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

Permissions of the DES service account on the database

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

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

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



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.

© 2021 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.

