Manual

DriveLock Quickstart Guide

DriveLock SE 2019

DON'T GAMBLE WITH YOUR DATA

Content

1 Introduction

1.1 Purpose of this document

This document describes the procedure to install DriveLock and deploy your security policies within 2 hours.

Compared to other solutions you will get your desired security level with DriveLock faster than with any other solution. Even in daily business DriveLocks' simple architecture and the flexibility helps to save time and money.

The security of sensible and confidential data today is getting more and more important. To master the complex requirements in this are a secure and flexible solution is needed.

This flexible solution doesn't have to be complex to handle. Data security can be simple. With DriveLock you raise the security level of your data and protect your environment from open USB-ports and other uncontrolled interfaces.

With this manual, you can implement device security and encryption within 2 hours.

Afterwards you can download different whitepapers from the DriveLock Support portal to get an overview over the different use-cases and best-practices and their configuration.

2 Requirements

- ✓ DriveLock Software: Download the DriveLock-ISO:

  http://drivelock.support/hc - Release & Release Notes

- ✓ You find the system requirements in the file:

  Manual\DriveLock Release Notes EN.pdf

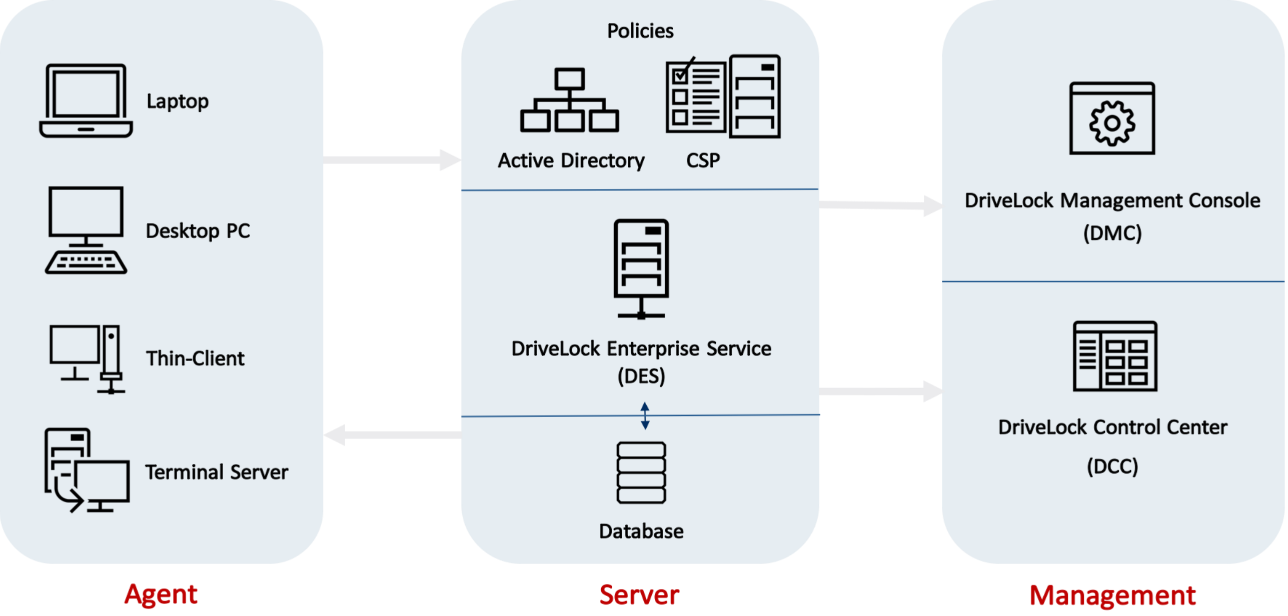
- ✓ One management PC to install the DriveLock Management Console (DMC) and the DriveLock Control Centers (DCC). The DriveLock-ISO-File should be mounted to upload the installation packages for the DriveLock Enterprise Service (DES) from this computer.
- ✓ One PC (for installations in a productive environment Windows Server is recommended) to install the DriveLock Enterprise Service (DES) and the DriveLock database (The ISO contains the sources of Microsoft SQL Express 2014 SP1). The DMC and DCC can also be installed on the server.
- ✓ A user with local admin rights to run the DriveLock Enterprise Service
- ✓ A user with local admin rights on the test clients to install the agent.
- ✓ The push installation requires that the file- and printer share is active.
- ✓ Recommended: An AD group where all PCs are members to install the agent via push-installation.

3 Installation DriveLock Server

A new installation of DriveLock and an update to a newer version of DriveLock require the same steps. If you do an update, do not select the components, which should not be updated (e.g. the Microsoft SQL Server). It is strongly recommended, always to use a same version of the DriveLock Enterprise Service (DES) and the management components. The version of the DES should be newer or equal to the most current version of the DriveLock Agents. When updating, you should always start with the DES and DMC/DCC consoles, before you publish the new DriveLock Agent.

DriveLock consists of four components:

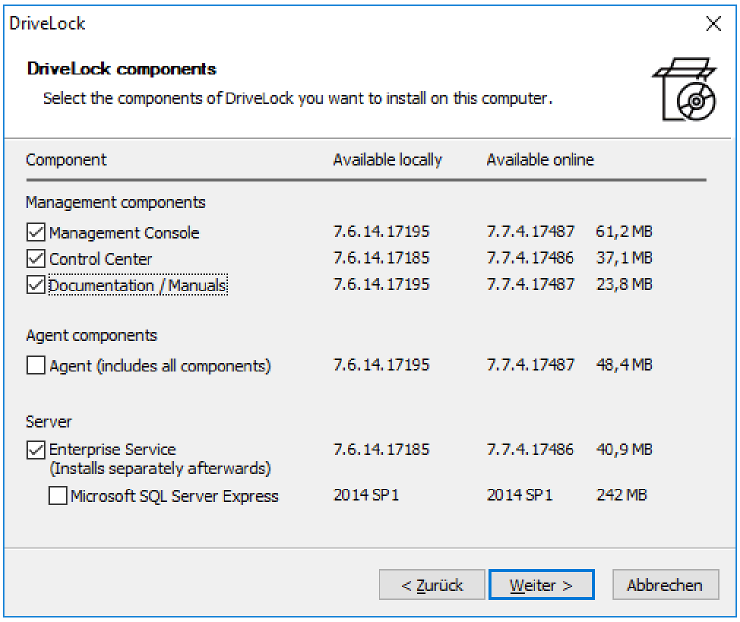
- DriveLock Enterprise Service
  - The DriveLock Enterprise Service (DES) is the central component of the DriveLock product and will be installed on a server.
- DriveLock Management Console
  - The DriveLock Management Console (DMC) is used for the configuration of the DES. Also, the policy creation management will be performed with the DMC.
- DriveLock Control Center
  - The DriveLock Control Center (DCC) is the tool for the helpdesk users. You can observe and interact with managed clients. You can create and evaluate your reports and you can perform forensic analysis.
- DriveLock Agent
  - The DriveLock Agent is a local service, which needs to be installed on all computers, which should be managed by DriveLock.


Laptop
Desktop PC
Thin-Client
Terminal Server
Agent
Policies
Active Directory
CSP
DriveLock Enterprise Service (DES)
Database
Server
DriveLock Management Console (DMC)
DriveLock Control Center (DCC)
Management

3.1 Installation DMC, DCC und DES

The installation wizard will guide you through the installation.

- Execute DLSetup.exe from the ISO-file
- Choose your language and accept the DriveLock EULA



DriveLock

DriveLock components

Select the components of DriveLock you want to install on this computer.

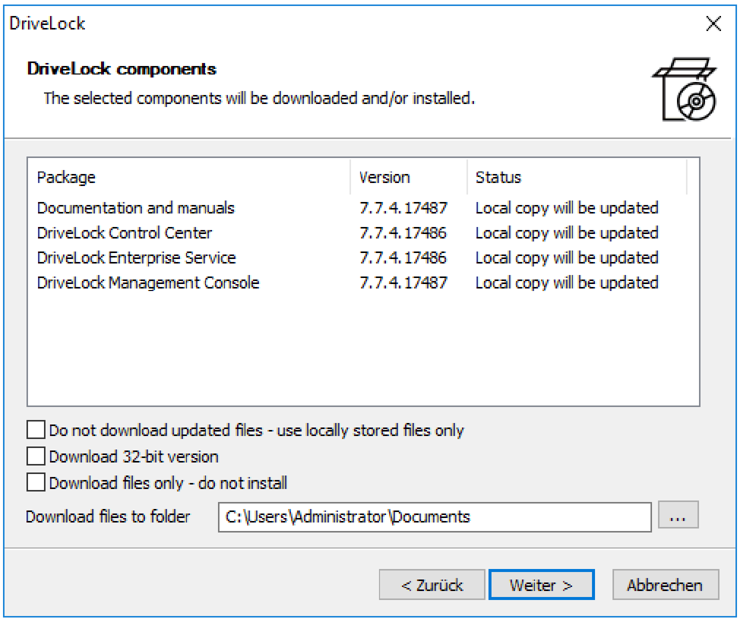
Component	Available locally	Available online	
Management components			
☑ Management Console	7.6.14.17195	7.7.4.17487	61,2 MB
☑ Control Center	7.6.14.17185	7.7.4.17486	37,1 MB
☑ Documentation / Manuals	7.6.14.17195	7.7.4.17487	23,8 MB
Agent components			
□ Agent (includes all components)	7.6.14.17195	7.7.4.17487	48,4 MB
Server			
☑ Enterprise Service (Installs separately afterwards)	7.6.14.17185	7.7.4.17486	40,9 MB
□ Microsoft SQL Server Express	2014 SP1	2014 SP1	242 MB

Choose these components:

- Management Console
- Control Center
- Documentation / Manuals
- Enterprise Service

Optionally you can install a Microsoft SQL Express Server.

For more than 200 devices a full SQL server is recommended!



DriveLock

DriveLock components

The selected components will be downloaded and/or installed.

Package	Version	Status
Documentation and manuals	7.7.4.17487	Local copy will be updated
DriveLock Control Center	7.7.4.17486	Local copy will be updated
DriveLock Enterprise Service	7.7.4.17486	Local copy will be updated
DriveLock Management Console	7.7.4.17487	Local copy will be updated

☐ Do not download updated files - use locally stored files only

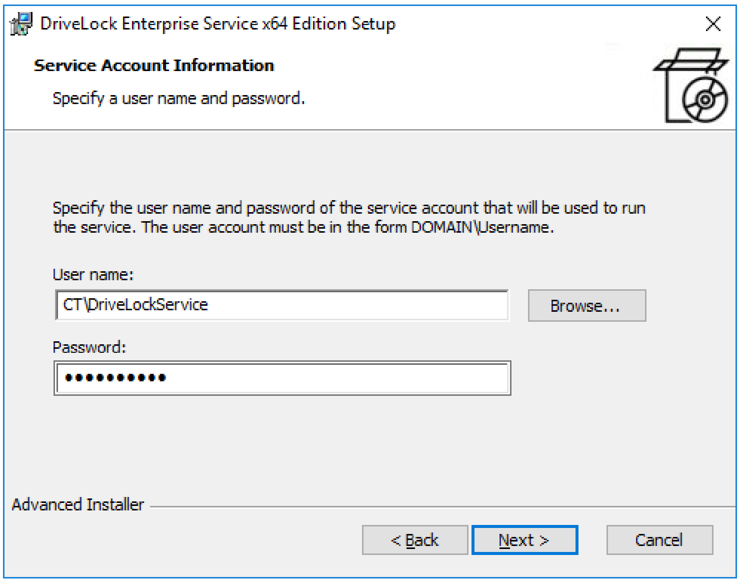
☐ Download 32-bit version

☐ Download files only - do not install

Download files to folder: C:\Users\Administrator\Documents

If there is an online connection the installation wizard will check the DriveLock Cloud for the most recent DriveLock version. You can automatically download the newer version and install it.

Right after the installation of the management components (DMC/DCC) the wizard for the DriveLock Enterprise Service will start an installation wizard.



DriveLock Enterprise Service x64 Edition Setup

Service Account Information

Specify a user name and password.

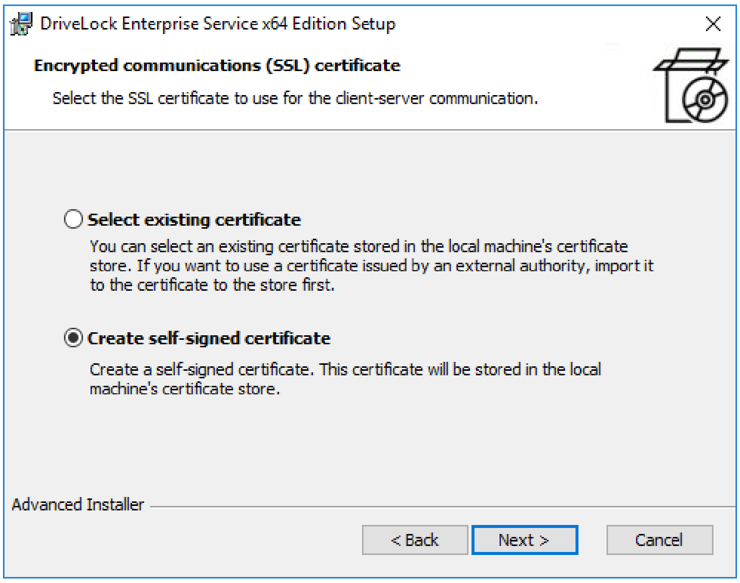
Specify the user name and password of the service account that will be used to run the service. The user account must be in the form DOMAIN\Username.

User name: CT\DriveLockService

Password: ••••••••••

Specify the user account and password for the DriveLock Enterprise Service.

Click browse to choose an existing one.



DriveLock Enterprise Service x64 Edition Setup

Encrypted communications (SSL) certificate

Select the SSL certificate to use for the client-server communication.

○ **Select existing certificate**

You can select an existing certificate stored in the local machine's certificate store. If you want to use a certificate issued by an external authority, import it to the certificate to the store first.

● **Create self-signed certificate**

Create a self-signed certificate. This certificate will be stored in the local machine's certificate store.

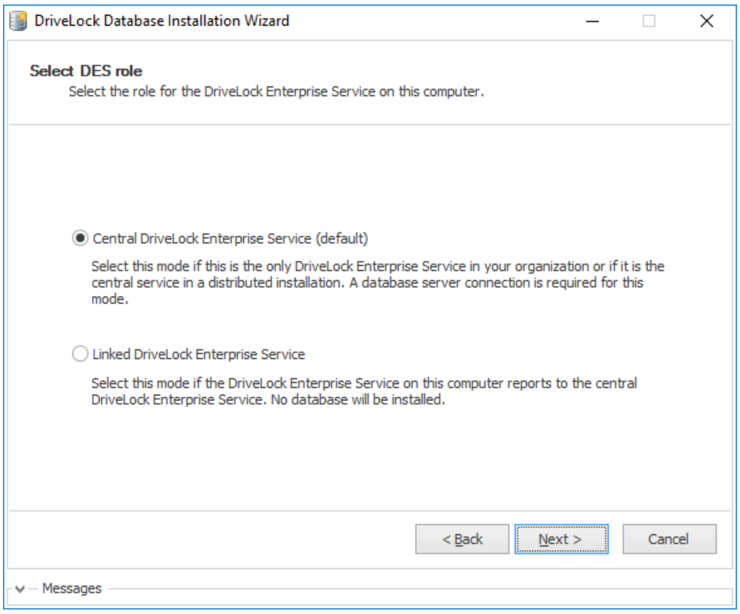
Create a self-signed certificate for the client server communication.

If you already have a DriveLock SSL-certificate in the local certificate store you can use this instead.

- The installation wizard may configure the Windows firewall.
- Complete the installation

3.2 Database installation

DriveLock supports Microsoft SQL Server and Microsoft SQL Server Express. For detailed system requirements see Release Notes *(See 2. System requirements)*.



DriveLock Database Installation Wizard

Select DES role

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

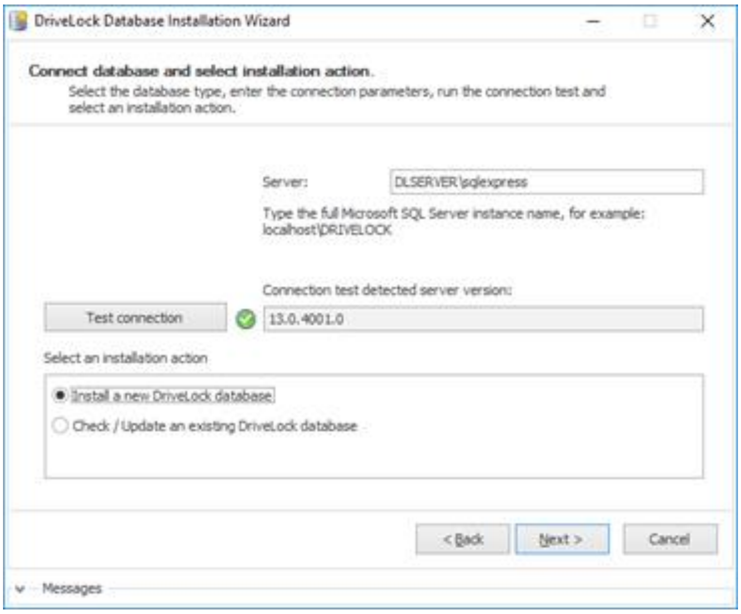
● Central DriveLock Enterprise Service (default)

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.

Check „Central DriveLock Enterprise Service“ to create a new database.



DriveLock Database Installation Wizard

Connect database and select installation action.

Select the database type, enter the connection parameters, run the connection test and select an installation action.

Server: DLSERVER\sqlexpress

Type the full Microsoft SQL Server instance name, for example: localhost\DRIVELOCK

Connection test detected server version: 13.0.4001.0

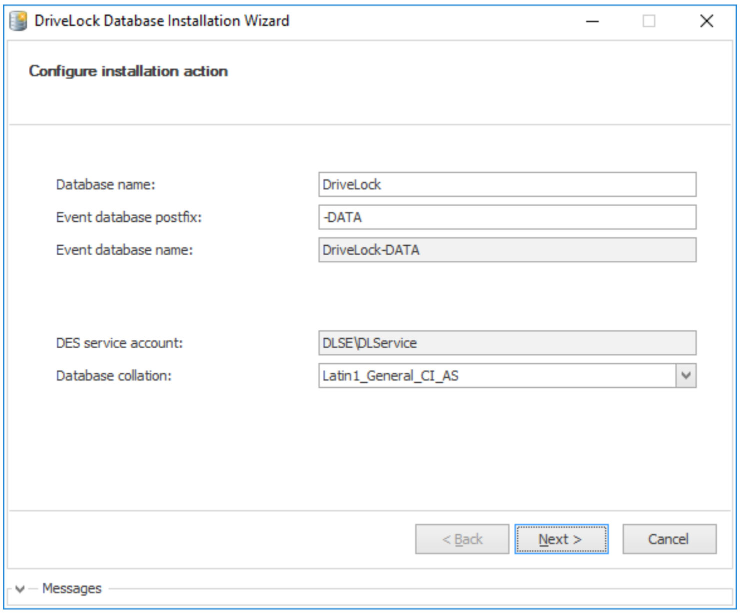
Select an installation action

● Install a new DriveLock database

○ Check / Update an existing DriveLock database

Select your SQL server.

Check „Install a new DriveLock database“



DriveLock Database Installation Wizard

Configure installation action

Database name: DriveLock

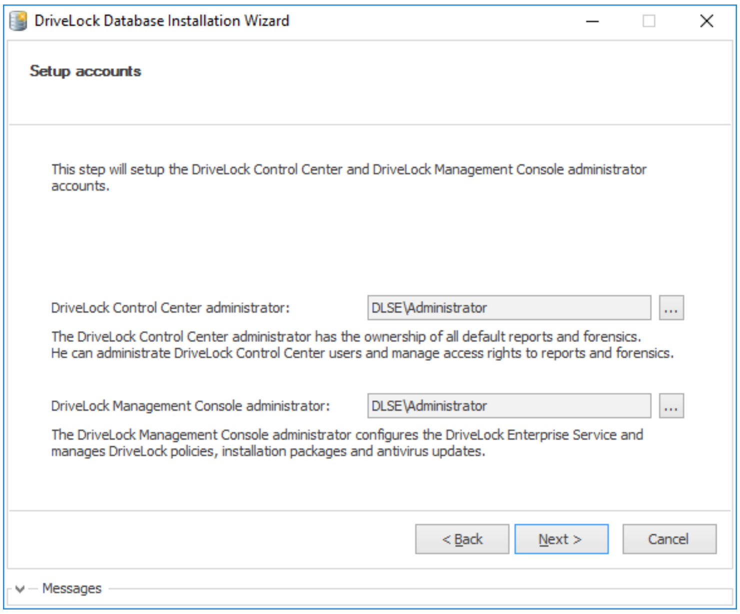
Event database postfix: -DATA

Event database name: DriveLock-DATA

DES service account: DLSE\DLService

Database collation: Latin1_General_CI_AS

Next



DriveLock Database Installation Wizard

Setup accounts

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

DriveLock Control Center administrator: DLSE\Administrator

The DriveLock Control Center administrator has the ownership of all default reports and forensics. He can administrate DriveLock Control Center users and manage access rights to reports and forensics.

DriveLock Management Console administrator: DLSE\Administrator

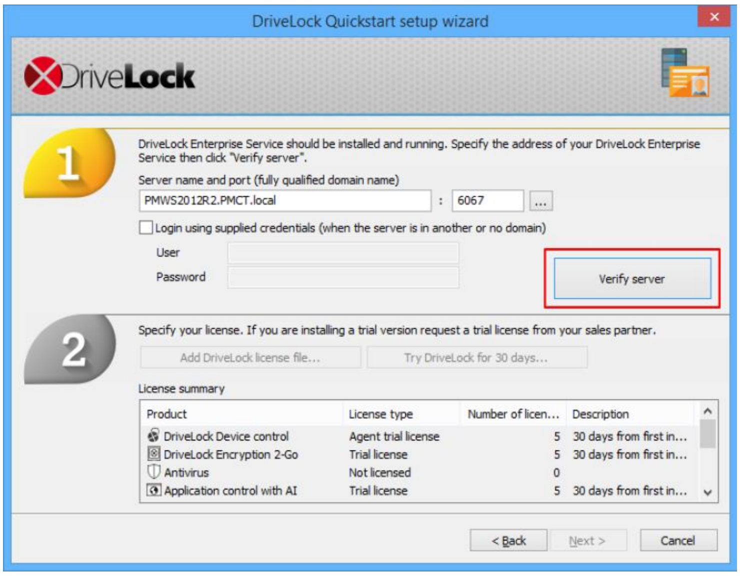
The DriveLock Management Console administrator configures the DriveLock Enterprise Service and manages DriveLock policies, installation packages and antivirus updates.

Here you can configure the administrator for the DMC and the DCC.

The installation user will be used by default.

4 DriveLock configuration

After the installation of the DriveLock Management Console has finished, the DriveLock Quick-start setup wizard appears. You may cancel the wizard at any time and restart it from the windows start menu again.



DriveLock Quickstart setup wizard

1 DriveLock Enterprise Service should be installed and running. Specify the address of your DriveLock Enterprise Service then click "Verify server".

Server name and port (fully qualified domain name)

PMWS2012R2.PMCT.local : 6067

□ Login using supplied credentials (when the server is in another or no domain)

User

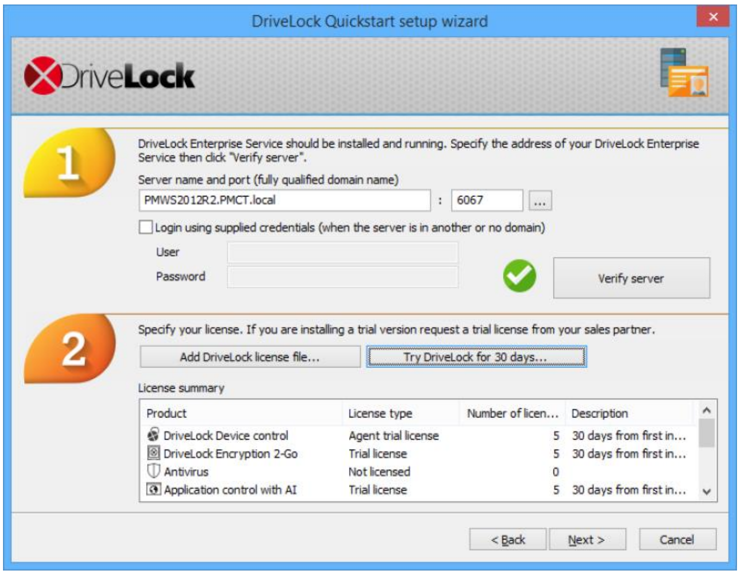
Password

2 Specify your license. If you are installing a trial version request a trial license from your sales partner.

License summary

Product	License type	Number of licen...	Description
DriveLock Device control	Agent trial license	5	30 days from first in...
DriveLock Encryption 2-Go	Trial license	5	30 days from first in...
Antivirus	Not licensed	0	
Application control with AI	Trial license	5	30 days from first in...

Enter the data to access the DriveLock Enterprise Service and click verify server. The checkmark becomes green, if the server can be connected.



DriveLock Quickstart setup wizard

1 DriveLock Enterprise Service should be installed and running. Specify the address of your DriveLock Enterprise Service then click "Verify server".

Server name and port (fully qualified domain name)

PMWS2012R2.PMCT.local : 6067

□ Login using supplied credentials (when the server is in another or no domain)

User

Password

2 Specify your license. If you are installing a trial version request a trial license from your sales partner.

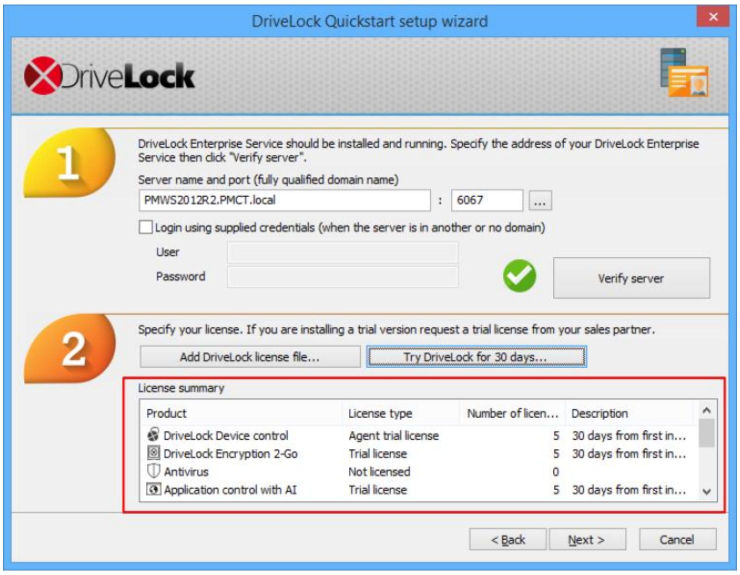
License summary

Product	License type	Number of licen...	Description
DriveLock Device control	Agent trial license	5	30 days from first in...
DriveLock Encryption 2-Go	Trial license	5	30 days from first in...
Antivirus	Not licensed	0	
Application control with AI	Trial license	5	30 days from first in...

Click „Add DriveLock license file", if you already have a test license provided by your reseller/partner.

In the license wizard enter the path to your license file.

Click "Try DriveLock for 30 days..." and a trial license will be generated and stored in your new policy automatically.



DriveLock Quickstart setup wizard
DriveLock
1
2
Verify server
Add DriveLock license file...
Try DriveLock for 30 days...
< Back
Next >
Cancel

DriveLock Enterprise Service should be installed and running. Specify the address of your DriveLock Enterprise Service then click "Verify server".

Server name and port (fully qualified domain name): PMWS2012R2.PMCT.local : 6067

□ Login using supplied credentials (when the server is in another or no domain)

User

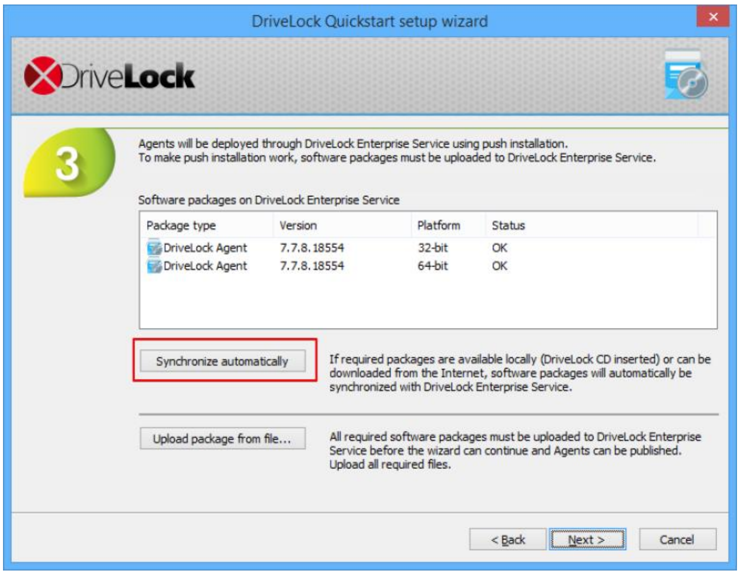
Password

Specify your license. If you are installing a trial version request a trial license from your sales partner.

License summary

Product	License type	Number of licen...	Description
DriveLock Device control	Agent trial license	5	30 days from first in...
DriveLock Encryption 2-Go	Trial license	5	30 days from first in...
Antivirus	Not licensed	0	
Application control with AI	Trial license	5	30 days from first in...

In the license overview, you can see all active licenses



DriveLock Quickstart setup wizard
DriveLock
3
Synchronize automatically
Upload package from file...
< Back
Next >
Cancel

Agents will be deployed through DriveLock Enterprise Service using push installation. To make push installation work, software packages must be uploaded to DriveLock Enterprise Service.

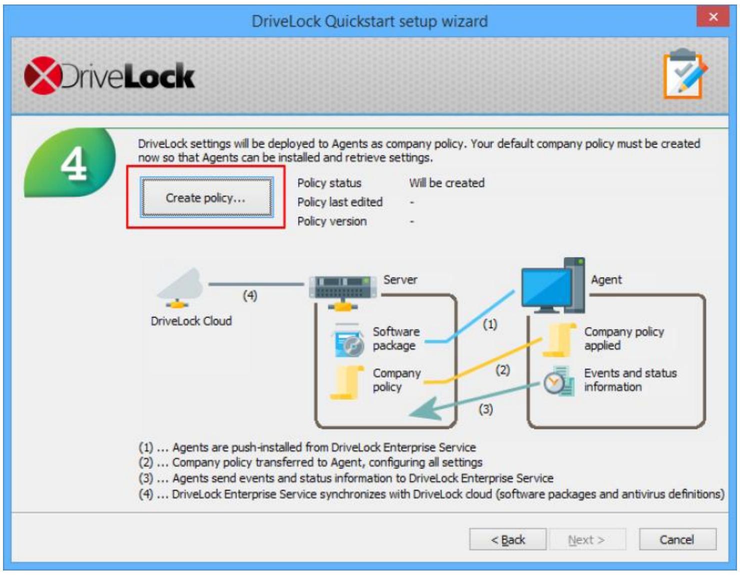
Software packages on DriveLock Enterprise Service

Package type	Version	Platform	Status
DriveLock Agent	7.7.8.18554	32-bit	OK
DriveLock Agent	7.7.8.18554	64-bit	OK

If required packages are available locally (DriveLock CD inserted) or can be downloaded from the Internet, software packages will automatically be synchronized with DriveLock Enterprise Service.

All required software packages must be uploaded to DriveLock Enterprise Service before the wizard can continue and Agents can be published. Upload all required files.

Prepare Deployment – the DES downloads the most current software packages from the Internet. If not yet available, you can synchronize the files from the ISO or upload packages manually.

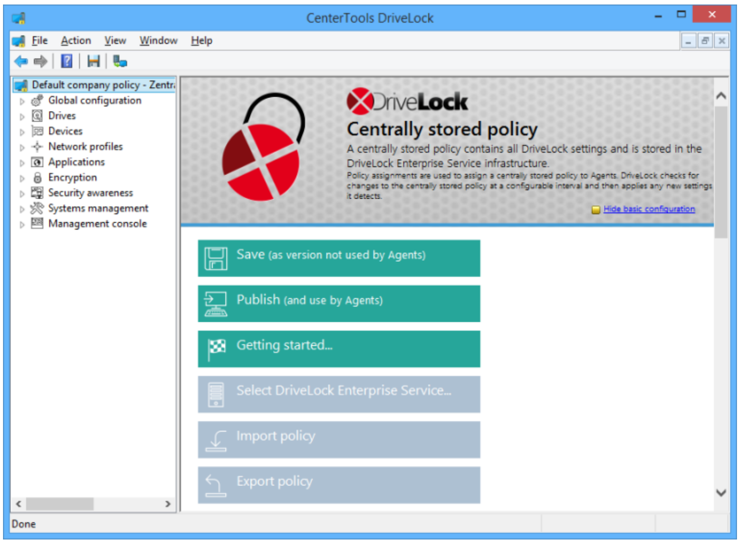


DriveLock settings will be deployed to Agents as company policy. Your default company policy must be created now so that Agents can be installed and retrieve settings.

Policy status	Will be created
Policy last edited	-
Policy version	-

(1) ... Agents are push-installed from DriveLock Enterprise Service
(2) ... Company policy transferred to Agent, configuring all settings
(3) ... Agents send events and status information to DriveLock Enterprise Service
(4) ... DriveLock Enterprise Service synchronizes with DriveLock cloud (software packages and antivirus definitions)

Create a default company policy.



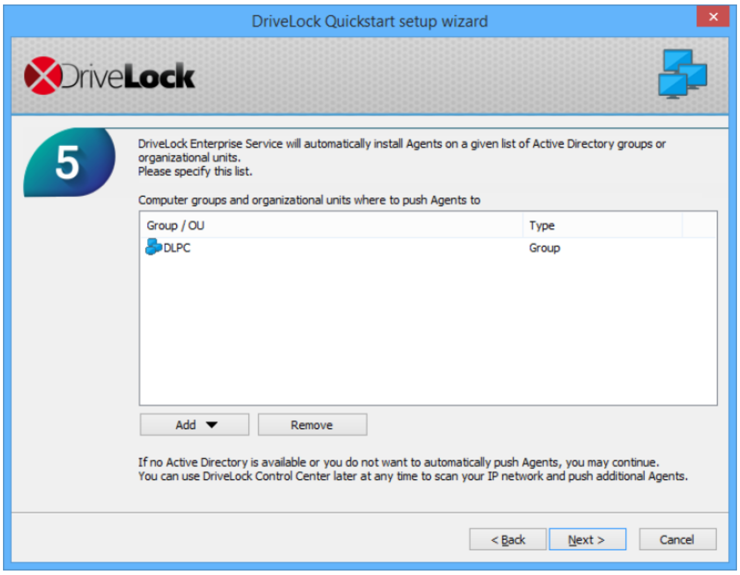
Centrally stored policy

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

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

Hide basic configuration
Save (as version not used by Agents)
Publish (and use by Agents)
Getting started...
Select DriveLock Enterprise Service...
Import policy
Export policy
Done

Safe and publish the unchanged policy to start with the basic configuration.



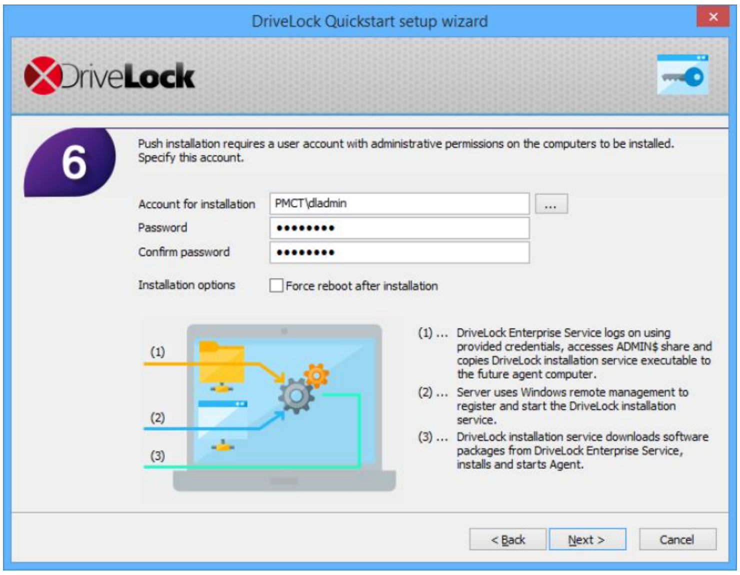
DriveLock Enterprise Service will automatically install Agents on a given list of Active Directory groups or organizational units.
Please specify this list.

Computer groups and organizational units where to push Agents to

Group / OU	Type
DLPC	Group

If no Active Directory is available or you do not want to automatically push Agents, you may continue.
You can use DriveLock Control Center later at any time to scan your IP network and push additional Agents.

Add groups and/or OUs from the Active Directory (AD), where the DES automatically shall install the DriveLock Agent and assign the default company policy.
If you don't use an AD you may initiate a manual push installation from the DriveLock Control Center later or deploy the Agent via a MSI package.

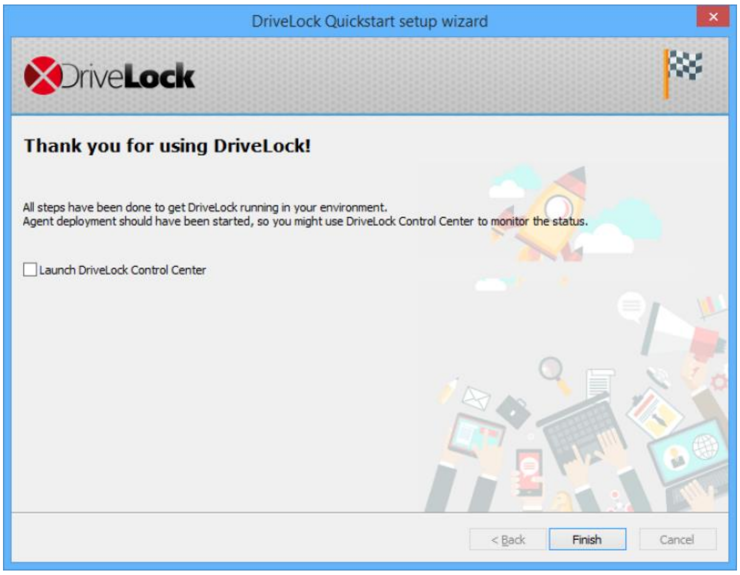


Push installation requires a user account with administrative permissions on the computers to be installed.
Specify this account.

Account for installation: PMCT\dladmin
Password: ••••••••
Confirm password: ••••••••
Installation options: □ Force reboot after installation

(1) ... DriveLock Enterprise Service logs on using provided credentials, accesses ADMIN$ share and copies DriveLock installation service executable to the future agent computer.
(2) ... Server uses Windows remote management to register and start the DriveLock installation service.
(3) ... DriveLock installation service downloads software packages from DriveLock Enterprise Service, installs and starts Agent.

Add the credentials for the user with local administration rights on the PCs where the agent shall be installed



Thank you for using DriveLock!

All steps have been done to get DriveLock running in your environment.
Agent deployment should have been started, so you might use DriveLock Control Center to monitor the status.

☐ Launch DriveLock Control Center

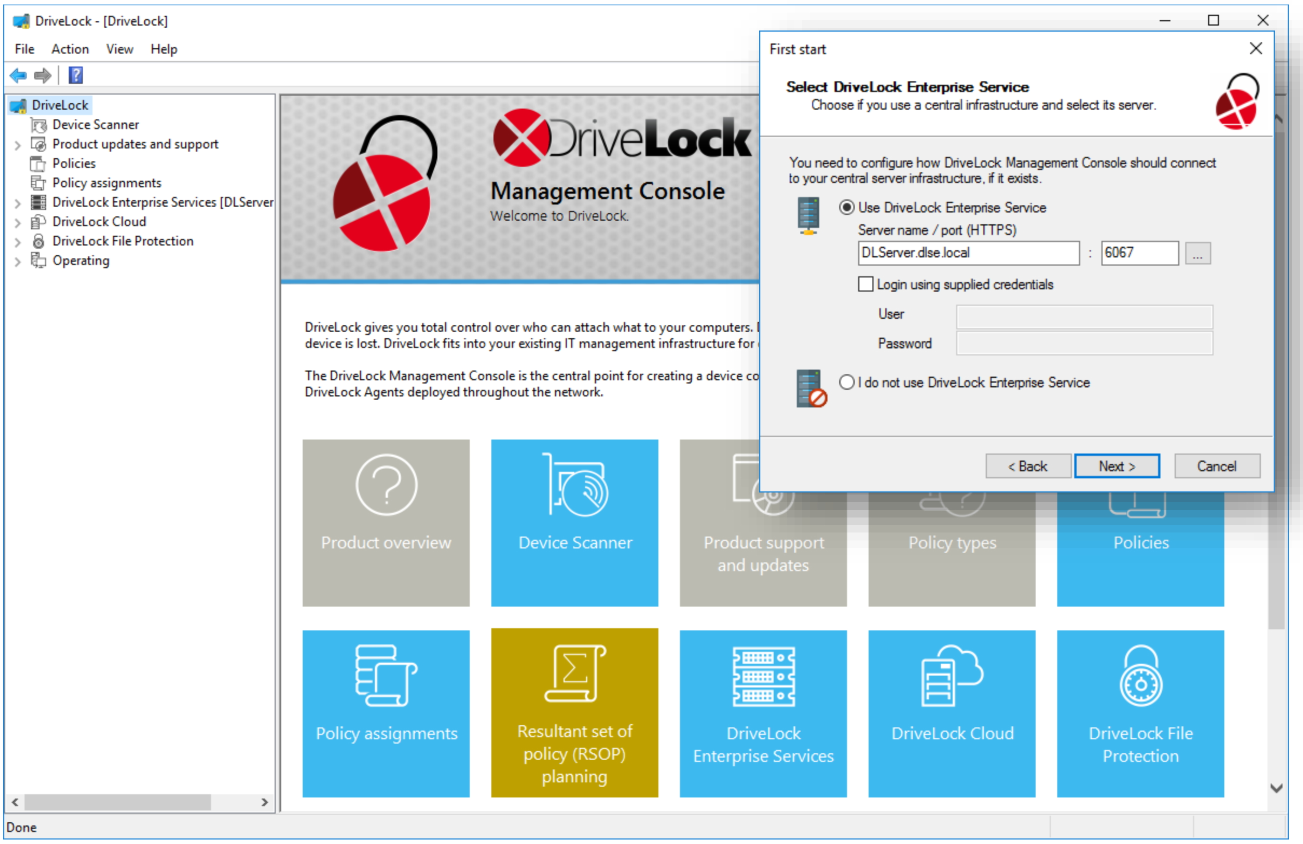
Finish the wizard. You don't need to start the DCC.

The system is now ready to use.

5 Policy configuration

5.1 Working with the DMC

You use the DriveLock Management Console to configure the security settings for your clients, manage your environment and access other DriveLock components. This console is a Microsoft Management Console (MMC) snap-in so you can easily integrate it into existing MMC console files that administrators may have already configured.



DriveLock gives you total control over who can attach what to your computers. I
device is lost. DriveLock fits into your existing IT management infrastructure for

The DriveLock Management Console is the central point for creating a device co
DriveLock Agents deployed throughout the network.

Select DriveLock Enterprise Service
Choose if you use a central infrastructure and select its server.

You need to configure how DriveLock Management Console should connect to your central server infrastructure, if it exists.

● Use DriveLock Enterprise Service
Server name / port (HTTPS)
DLServer.dlse.local : 6067
□ Login using supplied credentials
User
Password
○ I do not use DriveLock Enterprise Service

A detailed description of how to use the DMC can be found in the DriveLock Admin Guide.

5.2 Policy types

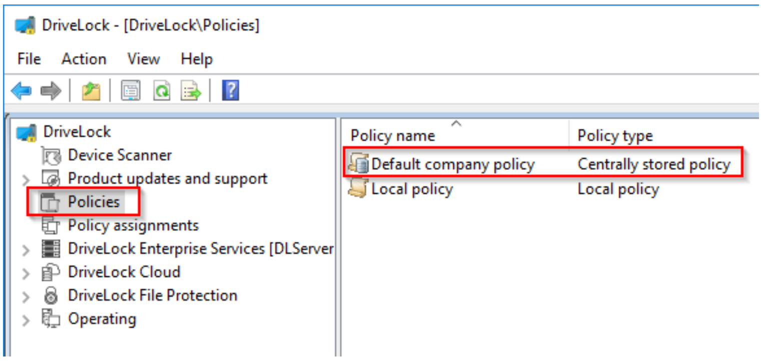
DriveLock can use different types of central policies to secure your endpoints. There are four types of policies:

- Configuration File
    - You can centrally install and configure DriveLock even in networks without Active Directory, like networks using Novell NetWare. In network environments without Group Policy or a DriveLock Enterprise Service you can distribute central DriveLock configuration settings by using a configuration file. This file can be placed on a central network drive (using a UNC path) or it can be accessed by using HTTP/HTTPS or FTP.
- Centrally Stored Policy
    - As an alternative to group policies you can distribute DriveLock settings using a Centrally Stored Policy (CSP). CSPs are similar to group policies, but they are stored in the DriveLock database by the DriveLock Enterprise Service (DES). Use CSPs if you don't have an Active Directory in place or if you cannot use Active Directory Group Policies for any other reason. For Managed Security Service Provider (MSSP), CSPs may also be the best choice to separate CSPs for different tenants. CSPs support versioning and change tracking, and administrators can selectively publish CSPs. They can be used in almost any network environment, including Active Directory, Novell Directory Service and workgroups.
- Group Policy
    - The easiest way to configure the DriveLock Agent on multiple computers in a network is by using an Active Directory Group Policy. DriveLock can be configured by using the Group Policy Object Editor in conjunction with the DriveLock Management Console (MMC) snap-in. This snap-in is automatically installed as part of the DriveLock installation.
      DriveLock can use Group Policy to deploy settings to computers that belong to an Active Directory domain. The DriveLock Agent running on these computers automatically applies all settings that are contained in the Group Policy Object.

	Central Configuration	Requires DES	Uses Existing Infrastructure	History or Versioning	Scalability	Quick Configuration
Local Policy	No	No	No	No	-/-	No
Group Policy	Yes	No	Yes (AD)	No	Very good	No
Centrally Stored Policy	Yes	Yes	No	Yes	Good	Yes
Configuration File	Yes	No	Yes (UNC,http(s),ftp)	No	Acceptable	No

5.3 Basic configuration

In this Quick-start guide a Centrally Stored Policy is used to deploy your settings. These settings can be made in the DriveLock Management Console. You can start it anytime from the start menu.



Open the default company policy to edit it.

Global settings:

Turn down the agent polling interval:

- Settings
  - Advanced DriveLock Agent settings
    - Intervals – Enable periodic reloading of configuration file / Centrally Stored Policy: 1 Min.

Activate the tray-icon:

- User interface settings:
  - Taskbar notification area settings
    - Display notification area icon: check

Configure a user or a user group for agent remote control:

- Settings
  - Remote control settings and permissions
    - Permissions
      - Add: User or user group (E.g.: DriveLock-Admin account)

DriveLock locks some drives by default settings:

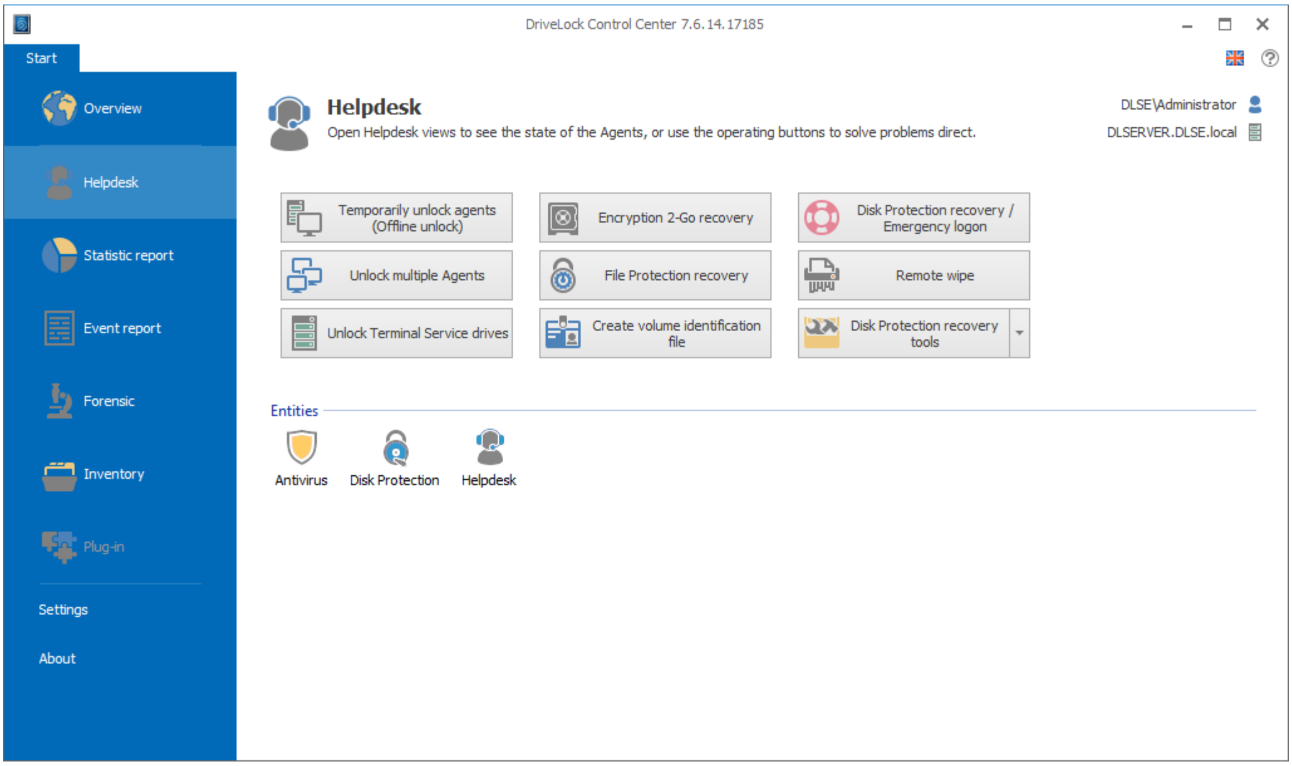
- Floppy disk drives
- CD-ROM drives
- USB bus-connected drives
- Firewire (1394) bus connected drives
- SD bus-connected drives
- Other removable drives

With drive whitelist rules or global removable drive locking settings you can grant access to all kinds of drives.

6 Installation of the DriveLock Agent

6.1 Overview DCC

You can use the DriveLock Control Center (DCC) to monitor the status of DriveLock Agents, to investigate events and incidents and create reports and statistics. The DCC communicates directly with the DriveLock Enterprise Service (DES), which retrieves information reported by DriveLock Agents from the database server where it stores this data.



DriveLock Control Center 7.6.14.17185

Helpdesk

Open Helpdesk views to see the state of the Agents, or use the operating buttons to solve problems direct.

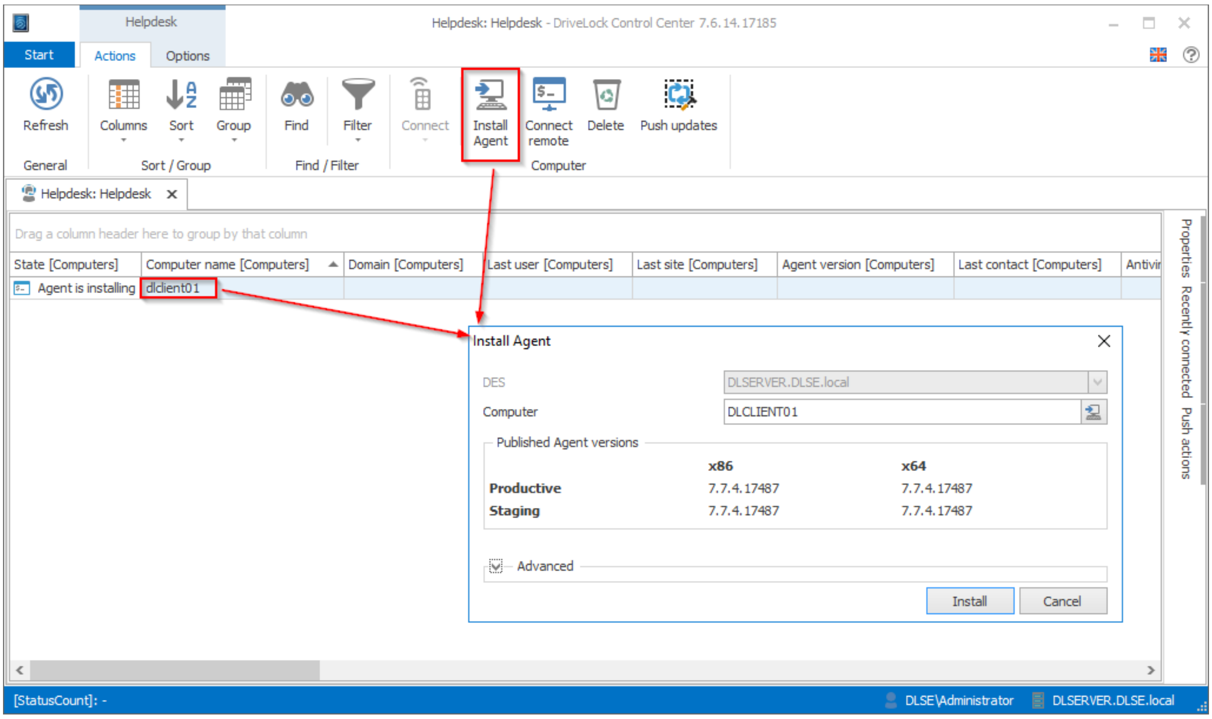
DLSE\Administrator

DLSERVER.DLSE.local

A detailed description of all functions and possibilities can be found in the DriveLock Control Center User Guide.

6.2 Push-Installation via DCC

With the DriveLock Control Center you can perform agent push installations or agent repair installations. In the Helpdesk view you can start Agent Push installation via the context menu of one or more computers or you click on the ribbon icon "Install Agent". Add computers, groups or OUs from Active Directory, a IP network or your network environment in the wizard to the list.



State [Computers]	Computer name [Computers]	Domain [Computers]	Last user [Computers]	Last site [Computers]	Agent version [Computers]	Last contact [Computers]	Antivir
Agent is installing	dlclient01						

Install Agent

DES: DLSERVER.DLSE.local

Computer: DLCLIENT01

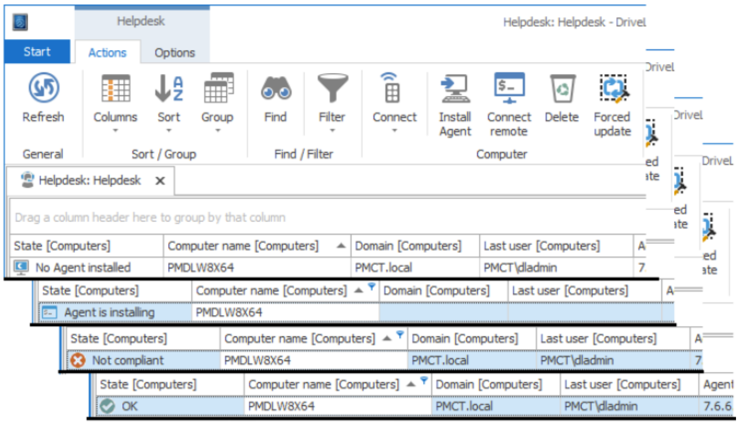
Published Agent versions

	x86	x64
Productive	7.7.4.17487	7.7.4.17487
Staging	7.7.4.17487	7.7.4.17487

Advanced

Install | Cancel

[StatusCount]: -   DLSE\Administrator   DLSERVER.DLSE.local



State [Computers]	Computer name [Computers]	Domain [Computers]	Last user [Computers]	A
No Agent installed	PMDLW8X64	PMCT.local	PMCT\dladmin	7

State [Computers]	Computer name [Computers]	Domain [Computers]	Last user [Computers]	A
Agent is installing	PMDLW8X64			

State [Computers]	Computer name [Computers]	Domain [Computers]	Last user [Computers]	A
Not compliant	PMDLW8X64	PMCT.local	PMCT\dladmin	7

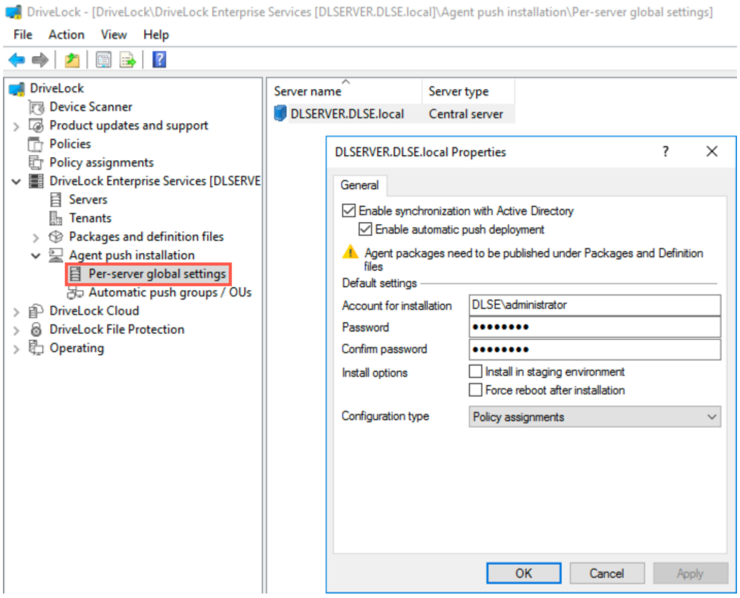
State [Computers]	Computer name [Computers]	Domain [Computers]	Last user [Computers]	Agent
OK	PMDLW8X64	PMCT.local	PMCT\dladmin	7.6.6

You see can see the status of an installation next to the computer object.

6.3 Automatic Agent-Push-Installation via DMC

You can configure the automatic push installation in the DriveLock Management Console

Configure the settings: DriveLock Enterprise Services – Agent-Push-Installation:



DriveLock - [DriveLock\DriveLock Enterprise Services [DLSERVER.DLSE.local]\Agent push installation\Per-server global settings]

Server name	Server type
DLSERVER.DLSE.local	Central server

DLSERVER.DLSE.local Properties

General

☑ Enable synchronization with Active Directory
☑ Enable automatic push deployment

Agent packages need to be published under Packages and Definition files

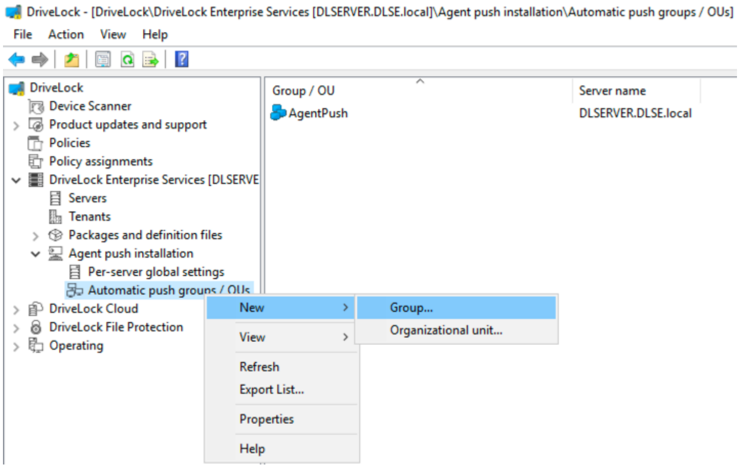
Default settings

Account for installation: DLSE\administrator
Password: ••••••••
Confirm password: ••••••••
Install options: □ Install in staging environment □ Force reboot after installation
Configuration type: Policy assignments

File
Action
View
Help
DriveLock
Device Scanner
Product updates and support
Policies
Policy assignments
DriveLock Enterprise Services [DLSERVE
Servers
Tenants
Packages and definition files
Agent push installation
Per-server global settings
Automatic push groups / OUs
DriveLock Cloud
DriveLock File Protection
Operating
?
OK
Cancel
Apply

Enter a user with local admin rights on the clients, where you want to push the DriveLock agent.

(Per server global settings – Server properties)



DriveLock - [DriveLock\DriveLock Enterprise Services [DLSERVER.DLSE.local]\Agent push installation\Automatic push groups / OUs]

Group / OU	Server name
AgentPush	DLSERVER.DLSE.local

Configure an installation target

(Automatic Push-Groups / OUs – Action– New)

The DriveLock Enterprise Service will perform the automatic push installation on every computer where no DriveLock agent is installed periodically. You can see the installation status in the DCC.

6.4 MSI package

There is a MSI package to install the DriveLock Agent on endpoints manually. This package ("DriveLockAgent.msi" / "DriveLockAgent X64.msi") installs the DriveLock Agent service without the creation of start menu entries or any user interaction (silent installation).

The MSI file is located on the DriveLock installation media or you can download them within the DMC (**DMC – DriveLock Enterprise Services – Packages and definition files – Software packages**).

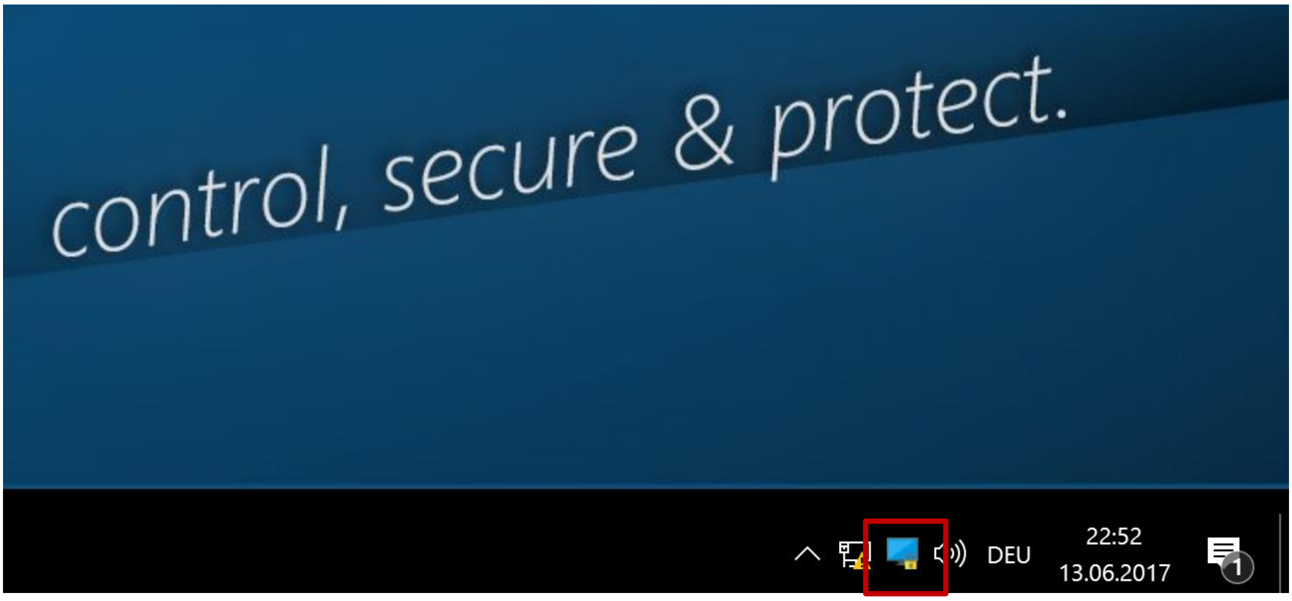
How the MSI file is prepared for the different kinds of policies and more detailed information about command line parameters you can find in the DriveLock Admin Guide in chapter 5.4.

7 Check the agent

If the agent installation was successfully there are two started services:

- DriveLock
- DriveLock Health Monitor

Like configured, there must be a tray icon in the notification area:


control, secure & protect.
DEU
22:52
13.06.2017
1