DriveLock Installation Guide 7.5

© 2015 CenterTools Software GmbH

DON'T GAMBLE WITH YOUR DATA

Table of Contents

Part I Document Conventions 4

Part II Securing Your Data with DriveLock 6

1 The DriveLock Components 7

DriveLock Agent 7
DriveLock Management Console 7
DriveLock Control Center 8
DriveLock Enterprise Service 8

2 Service Communications 8

Service Communications in Mixed Mode with Legacy Agents 10
Linked DES Servers 11

Part III Preparing to Install DriveLock 14

1 Quick Configuration Using mDNS / DNS-SD 15

Deactivating mDNS/DNS-SD 16

Part IV System Requirements 18

Part V Installing DriveLock 21

1 Evaluation Installation 21
2 Installing the DriveLock Enterprise Service 21
3 Installing the DriveLock Management Components 29
4 Installing the DriveLock Agent 31

Installing DriveLock by using Active Directory Group Policy 32
Installing the Agent by Using Configuration Files 34
Installing the Agent with a Centrally Stored Policy without Quick Configuration 39
Installation from a Command Prompt (Silent Installation) 44
Installing the DriveLock FDE Component 45

Part VI Updating DriveLock 47

1 Updating the DriveLock Enterprise Service 47
2 Updating the DriveLock Control Center 50
3 Updating DriveLock Management Components 50
4 Updating the Agent 50

Updating the DriveLock FDE Component 51

Part VII Uninstalling the DriveLock Agent 53

Part VIII Migrating a Legacy Database 55

 © 2015 CenterTools Software GmbH

Part I

Document Conventions

1 Document Conventions

Throughout this document the following conventions and symbols are used to emphasize important points that you should read carefully, or menus, items or buttons you need to click or select.

Caution: This format means that you should be careful to avoid unwanted results, such as potential damage to operating system functionality or loss of data

Hint: Useful additional information that might help you save time.

Italics represent fields, menu commands, and cross-references. **Bold** type represents a button that you need to click.

A `fixed-width typeface` represents messages or commands typed at a command prompt.

A plus sign between two keyboard keys means that you must press those keys at the same time. For example, ALT +R means that you must hold down the ALT key while you press R. A comma between two or more keys means that you must press them consecutively. For example 'ALT, R, U' means that you must first press the Alt key, then the R key, and finally the U key.

 © 2015 CenterTools Software GmbH

Part II

Securing Your Data with DriveLock

DON'T GAMBLE WITH YOUR DATA

2 Securing Your Data with DriveLock

CenterTools DriveLock is a lightweight software solution that helps you secure your desktop computers. It has a Multilingual User Interface (MUI), allowing you to select the desired language during installation or when running the program.

DriveLock offers dynamic, configurable access control for mobile drives (floppy disk drives, CD-ROM drives, USB memory sticks, etc.). DriveLock also lets you control the use of most other device types, such as Bluetooth transmitters, Palm, Windows Mobile, BlackBerry, cameras, smartphones, media devices and many more. By configuring whitelist rules based on device type and hardware ID you can define exactly who can access which device at which time. Removable drives can be controlled based on the drive's manufacturer, model and even serial number. This lets you define and enforce very granular access control policies. Additional features let you unlock specific authorized media and define time limits or computers for whitelist rules. Authorized administrators can even temporarily suspend device blocking on a computer, if required, even when the computer is offline and not connected to a network.

Installation of the client software (the DriveLock Agent) and policy deployment can be achieved easily by using existing software deployment mechanisms or by using the Group Policy feature of Active Directory. Alternatively, you can distribute policies using configuration files for standalone computers or in environments without Active Directory (for example Novell).

The auditing capabilities of DriveLock, coupled with its file shadowing functionality give you the information you need to monitor and enforce policy compliance. By using the DriveLock Device Scanner you can detect any drive or device that has been used in your network, even if it is no longer connected to the computer. The DriveLock Agent doesn't need to be installed on the target computers to use the Device Scanner.

Encryption is another main feature of DriveLock. DriveLock that can help you secure sensitive information by enforcing encryption when data is copied to removable drives. You can use the DriveLock Full Disk Encryption option to encrypt hard disks, including the system partition and to perform pre-boot authentication with single sign-on to Windows. DriveLock can also erase sensitive data permanently and securely by overwriting data multiple times using one of several industry-standard algorithms.

DriveLock's application control enables easy control over which applications run on a computer. You can allow or deny the starting of applications based on several criteria, such as the current user, network connection or computer.

DriveLock Antivirus adjusts to the current environment and your security policies. For example, you can enforce the most thorough scanning for removable drives before a user is allowed access to such a drive.

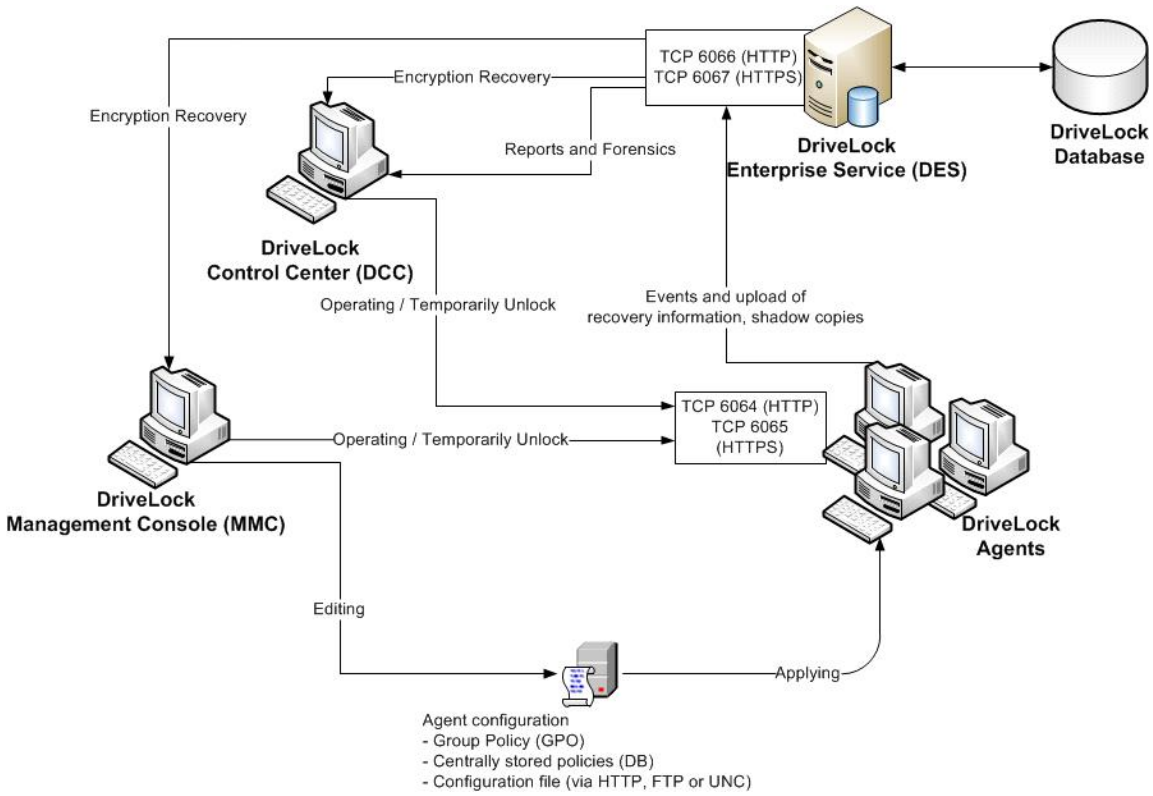
The DriveLock Enterprise Service (DES) is a central component that consolidates all DriveLock events and Device Scanner results in a central database. Administrators can then use this data to create dynamic reports for auditing and management purposes.

A single, unified console is used to configure all DriveLock components, which simplifies administration tasks.

 © 2015 CenterTools Software GmbH

2.1 The DriveLock Components

The section describes the DriveLock components and how they communicate with each other.



2.1.1 DriveLock Agent

The DriveLock Agent is the most important component of the DriveLock infrastructure. It implements and enforces your policy settings and must be installed on every computer where you want to control removable drives, devices or other settings. The Agent is a lightweight Windows service that runs in the background and maintains control over hardware ports and interfaces and enforces your security policy. To prevent unauthorized access or bypassing of the security settings, regular users can't stop the service; only users who are specifically authorized by you can access and control the service.

2.1.2 DriveLock Management Console

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.

The DriveLock Management Console lets you create a local configuration for the computer the console is running on, to define configurations by creating and changing Active Directory Group Policy settings or to save your settings to a configuration file that you can import on another computer. You can also monitor the status of clients or access the DriveLock Agent on clients. You can use the Management Console to remotely unlock an Agent by accessing it remotely, or— if the Agent is not connected to a network— by creating an offline access code that a user can enter on the client computer. In addition, the Device Scanner is integrated into the DriveLock Management Console.

 © 2015 CenterTools Software GmbH

2.1.3 DriveLock Control Center

The DriveLock Control Center (DCC) let you create dynamic reports and forensic analysis reports from events that were reported by DriveLock Agents data to a central server running the DriveLock Enterprise Service (DES). You can use the DCC to monitor the use of mobile drives, devices and data transfers in aggregate or in detail. The DCC includes the option to assign granular permissions for data queries and report creation.

For example, you can create reports about the use of removable media and device connection attempts (both allowed and blocked). In addition, you can create reports about which files have been written to or read from removable media and execute a forensic analysis by using the data drill-down capabilities of the DCC. The settings in your DriveLock policy determine what types of data are recorded.

The DCC also lets you monitor your current DriveLock Agent environment and view the status of clients. For example, you can identify computers that don't have the Agent installed or that have not recently reported their status. If you use the Full Disk Encryption option, you can view the current status of the drive encryption (for example, "Not installed" or "Currently encrypting"). You can also easily group and filter the list of Agents. All of these functions and the ability to view statistics as graphs make the DCC a very powerful monitoring and reporting tool.

2.1.4 DriveLock Enterprise Service

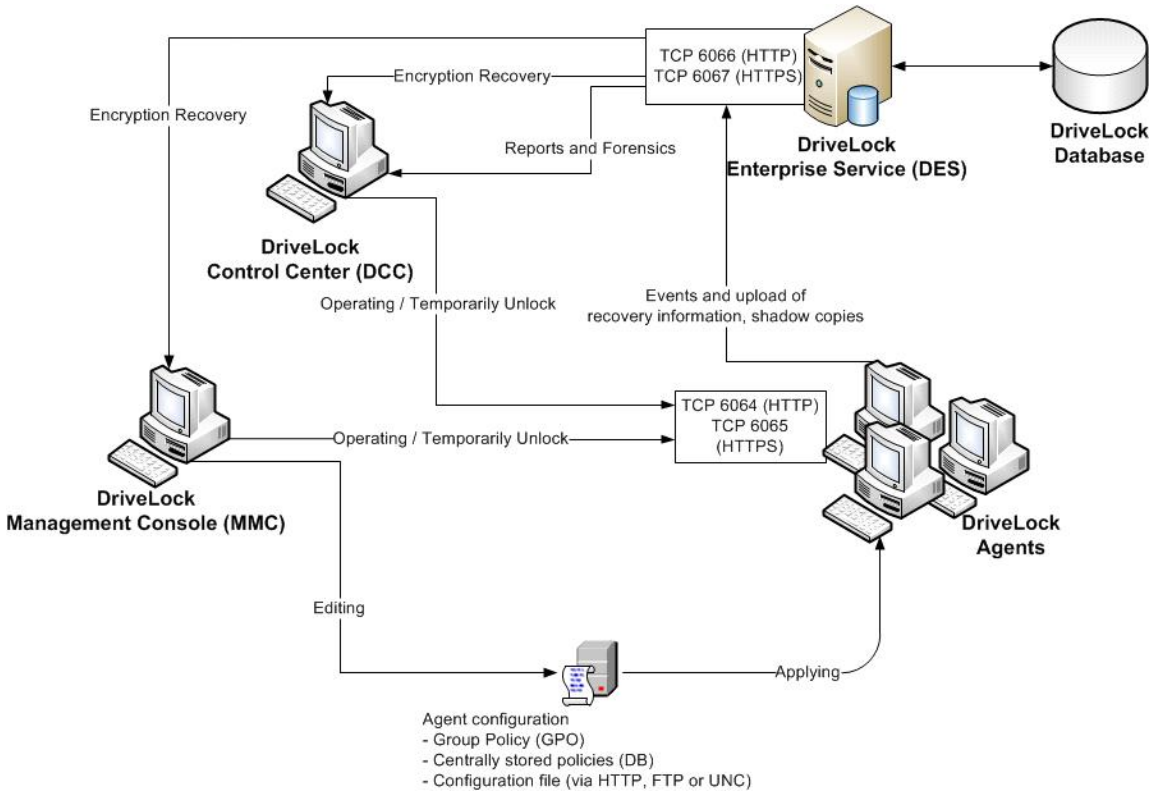
The DriveLock Enterprise Service (DES) centrally stores events from all DriveLock Agents. This service is not required for DriveLock to operate, but it lets administrators easily monitor all DriveLock operations and user activities in the entire organization. The DES replaces the Security Reporting Centers (SRC), which performed similar functions in DriveLock 5. The DES uses a new architecture and database structure to improve performance and add new functionality. The DriveLock Control Center (DCC) is the reporting console that enables administrators to view events that are stored in the DES and create reports from the event data.

Organizations that use one or both encryption modules (Encryption 2-Go or Full Disk Encryption) can use the DES to centrally store recovery data to simplify and streamline data recovery operations.

2.2 Service Communications

The following diagram illustrates communications paths and the role of the DriveLock Enterprise Service in the operations of DriveLock:

 © 2015 CenterTools Software GmbH



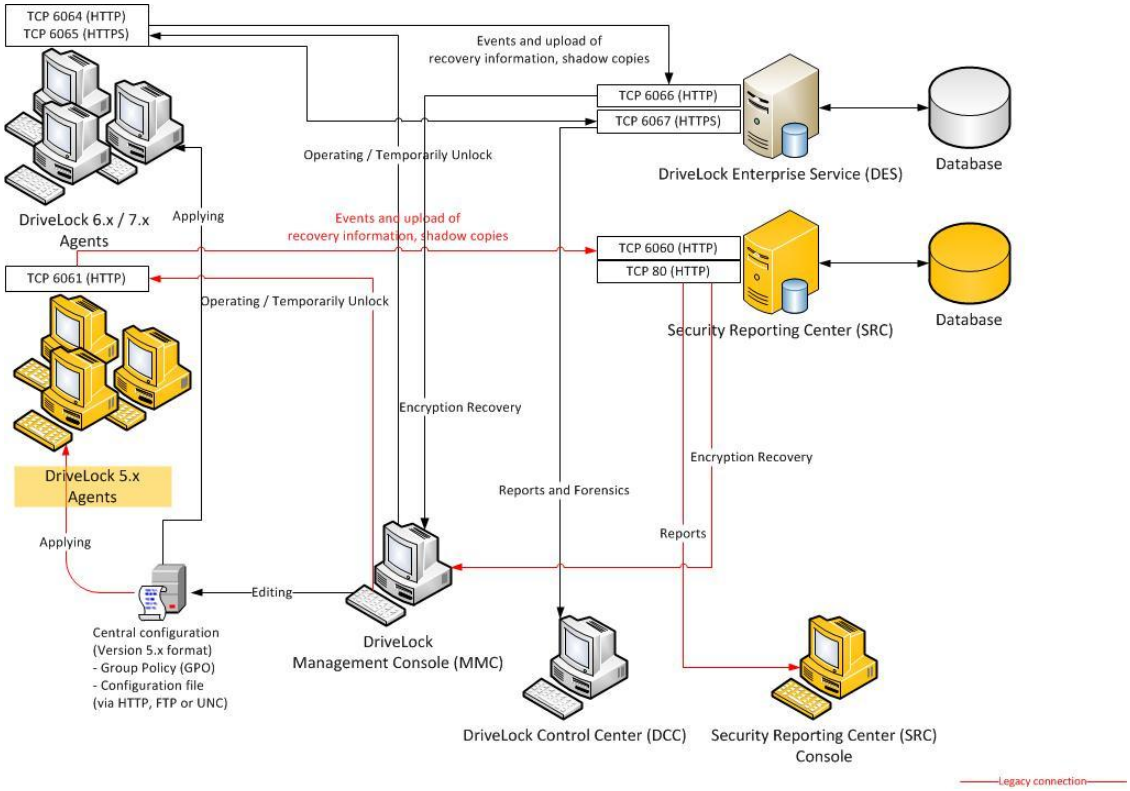
Default communications ports (These ports can be customized, if required)

Port	Direction	Protocol	Usage
6064 TCP	Incoming	HTTP	DriveLock Agent
6065 TCP	Incoming	HTTPS	DriveLock Agent
6066 TCP	Incoming	HTTP	DES
6067 TCP	Incoming	HTTPS	DES
135 TCP	Outgoing	RPC	(optional) MMC (GPO editing)
80 TCP	Incoming	HTTP	(optional) Access to configuration file on a server using HTTP
21 TCP	Incoming	FTP	(optional) Access to configuration file on a server using FTP
445 TCP; 139 TCP, 137 UDP, 138 UDP	Incoming	SMB; NetBIOS	(optional) Access to configuration file on a server using UNC

 © 2015 CenterTools Software GmbH

2.2.1 Service Communications in Mixed Mode with Legacy Agents

The following diagram illustrates communications paths and the role of the DriveLock Enterprise Service in the operations of DriveLock. In addition to the DriveLock 6 / DriveLock 7 environment, the diagram contains a legacy SRC server and an SRC console. During the migration from DriveLock 5 to DriveLock 6 or DriveLock 7, additional communications channels are used. Legacy communications channels are displayed in red or orange in the diagram.



Default communications ports (Ports can be customized, if required).

Port	Direction	Protocol	Usage
80 TCP	Incoming	HTTP	SRC
6060 TCP	Incoming	HTTP	SRC
6061 TCP	Incoming	HTTP	DriveLock 5.x Agent
6064 TCP	Incoming	HTTP	DriveLock Agent
6065 TCP	Incoming	HTTPS	DriveLock Agent
6066 TCP	Incoming	HTTP	DES
6067 TCP	Incoming	HTTPS	DES
135 TCP	Outgoing	RPC	(optional) MMC (GPO editing)
80 TCP	Incoming	HTTP	(optional) Access to

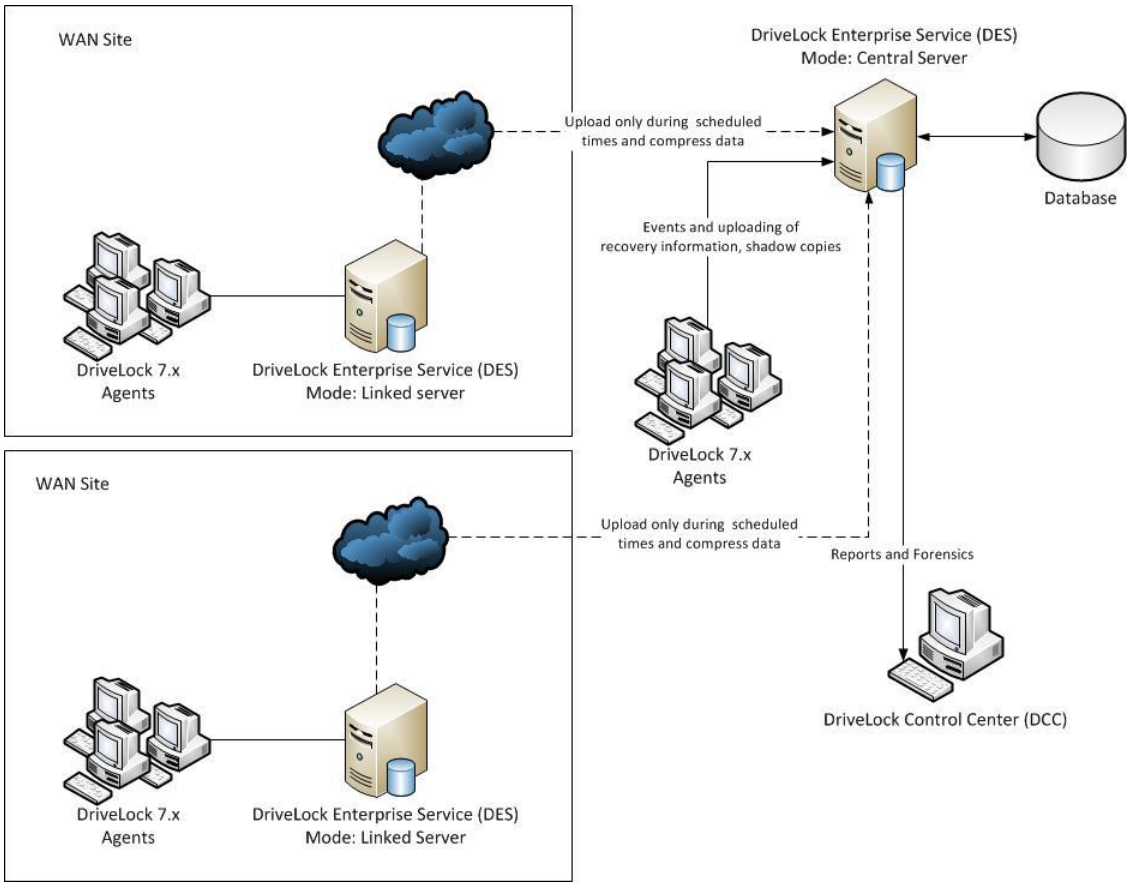
 © 2015 CenterTools Software GmbH

			configuration file on a server using HTTP
21 TCP	Incoming	FTP	(optional) Access to configuration file on a server using FTP
445 TCP; 139 TCP, 137 UDP, 138 UDP	Incoming	SMB; NetBIOS	(optional) Access to configuration file on a server using UNC

For additional information about the upgrade process, refer to the DriveLock Technical Article „Upgrading to DriveLock 6".

2.2.2 Linked DES Servers

In large DriveLock deployments you can minimize the use of system resources and network bandwidth by linking DES servers. In a linked deployment, one or more DES servers at branch offices are running in "Cache & Linked" mode. These servers collect events from DriveLock Agents but don't write the events to the database. Instead DES servers in Cache & Linked mode forward the event data in compressed form to a central DES server at preconfigured intervals. The central DES Server, which is running in the standard "Cache & Process" mode, is connected to a database server and writes the event data it receives from linked servers and clients to the DriveLock database.



To change the mode in which a DES Server is running, use the "Database Installation Wizard" which is included with

 © 2015 CenterTools Software GmbH

the DES.

 © 2015 CenterTools Software GmbH

Part III

Preparing to Install DriveLock

DON'T GAMBLE WITH YOUR DATA

3 Preparing to Install DriveLock

You can install DriveLock from compact disc or using files downloaded from the CenterTools Web site. All DriveLock components are available as separate 32-bit and 64-bit Microsoft Installer (MSI) packages. A separate installation package is available for the DriveLock documentation.

The easiest way to install DriveLock components is by using the DriveLock Installer (*DLSetup.exe*). This program can check whether the most current installation packages for all components are already present and download missing packages from the Internet. The DriveLock Installer runs both on 32-bit and 64-bit computers.

As an alternative you can download an ISO image containing the DriveLock Installer, all installation packages, documentation and additional information from www.drivelock.com. You can burn a CD from this ISO image.

Before starting the installation it is recommended that you decide which type of configuration you will be using to deploy DriveLock settings to clients because this will determine how you will deploy DriveLock Agents to client computers. The following configuration matrix can help you decide which of these methods is the most appropriate for your environment:

	Central Configuration	DES Required	Uses Existing Infrastructure	History / Versioning	Scalability	Quick Configuration
Local Configuration	No	No	No	No	-	No
Group Policy	Yes	No	Yes (AD)	No	Very good	No
Centrally Stored Policy	Yes	Yes	No	Yes	Gut	Yes
Configuration File	Yes	No	Yes (UNC, http, ftp)	No	Limited	No

> When using DriveLock for the first time, it is recommended to use a local configuration to become familiar with DriveLock before deploying configuration settings to multiple clients across your network.

- *Local configuration*: When using a local configuration, policy settings are only applied to the computer where you configure settings using the DriveLock Management Console. A local configuration is only appropriate for evaluating DriveLock or testing a policy before deploying it. The advantage of using a local configuration is that all changes take effect immediately on the local computer.
- *Group Policy*: You can store DriveLock configuration settings in a Group Policy Object in Active Directory. Policy settings are deployed to client computers using the native Group Policy mechanism in Windows.
- *Configuration Files*: Configuration settings are stored in a file. This file is stored in a shared folder or on an HTTP or FTP server from where it is retrieved by client computers. When using HTTP, client computers can retrieve the configuration settings over the Internet.
- *Centrally Stored Policies*: Centrally Stored Policy (CSP). CSPs are similar to configuration files, but they are stored by the DriveLock Enterprise Service (DES) and retrieved from there by Agents. Unlike other types of

 © 2015 CenterTools Software GmbH

policies, CSPs also automatically support versioning and change tracking and support Quick Configuration for effortless deployment.

A typical DriveLock deployment consists of four steps:

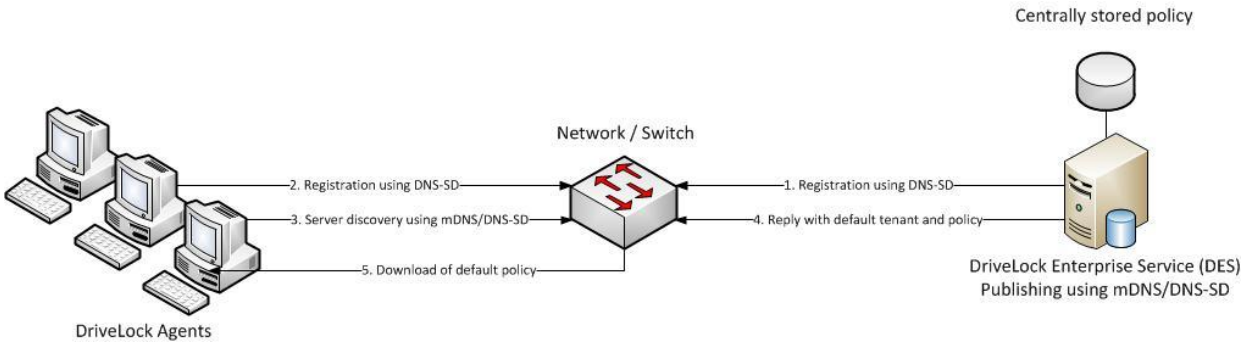
1. Installing the DriveLock Management Console on one or more administrator workstations
2. Installing the DriveLock Enterprise Service on a central server (database required)
3. Creating an initial DriveLock policy (for example, an initial policy that blocks no access until further testing is complete)
4. Installing the DriveLock Agent on selected client computers according to the selected deployment method

This document describes these steps in detail. Additional sections cover manually updating DriveLock, de-installing DriveLock and migrating from an older version (Version 5.5 R2 or older).

3.1 Quick Configuration Using mDNS / DNS-SD

The easiest and quickest option for configuring DriveLock is by using the multicast DNS (m-DNS) and DNS based Service Discovery (DNS/SD) protocols. These complementary technologies enable servers and clients to register themselves in the network using multicasts. This allows a DriveLock Agent to dynamically discover its DES server and to download its policy that has been configured by an administrator and stored in the DES. Only minimal configuration is required to enable this, but it requires that a DES server is running in the network environment.

The process of DES server discovery and downloading of the policy is illustrated in the following diagram:



The process of registration and discovery includes the following steps:

1. DES — Registration using DNS-SD
2. Agent — Registration using DND-SD
3. Agent — DES server discovery using mDNS/DNS-SD
4. DES — Reply with default tenant and policy
5. Agent — Download of default policy

> In a network that is connected using routers it is possible that the routers are not configured to forward multicast traffic between network segments. This prevents the use of mDNS/DNS-SD. If you cannot change the router configuration you need to use one of the other methods that are available for distributing the DriveLock policy to Agents.

 © 2015 CenterTools Software GmbH

For additional information about configuring centrally stored policies and assigning a standard policy, refer to the *DriveLock Administration Guide*.

3.1.1 Deactivating mDNS/DNS-SD

In some instances you may want to deactivate mDNS/DNS-SD and the associated multicast traffic. This will disable Quick Configuration, but it minimizes network traffic, which may be more important in large networks. To deactivate mDNS/DNS-SD, configure the following settings using the DriveLock Management Console:

- In the Agent configuration, for example in a Group Policy Object (GPO), under Extended configuration -> Global configuration -> Settings -> Agent remote control settings and permissions, deselect the checkbox *Enable automatic agent discovery (using DNS-SD)*.
- Under DriveLock Enterprise Services -> Servers -> <DES server> -> Properties, on the Options tab, select the checkbox *Disable automatic server discovery (using DNS-SD)*.

 © 2015 CenterTools Software GmbH

Part IV

System Requirements

DON'T GAMBLE WITH YOUR DATA

4 System Requirements

CenterTools DriveLock works in the background and therefore only uses minimal hardware resources. The DriveLock Agent runs on all recent versions of the Windows operating system and requires no additional infrastructure. The DriveLock Enterprise Service also requires a database (Microsoft SQL Server or Oracle).

CenterTools recommends that you install all available service packs and hotfixes for your operating system.

Detailed information of supported platforms and hardware requirements can be found in the DriveLock Release Notes.

Windows XP

- Microsoft Native WLAN API für Windows XP (wird für die Funktion „WiFi sperren wenn mit LAN verbunden")
- Microsoft IMAPI 2.0 (für CD/DVD Verschlüsselung)

Fulldisk Encryption

Supported Storage Hardware

DriveLock FDE can encrypt all fixed (non-removable) hard disk partitions that have been assigned a drive letter, including all IDE/EIDE, SATA and SCSI drives. There is no support for hidden partitions or software RAID arrays.

- DriveLock FDE does not interfere with the normal operation of the storage subsystem, with the following exceptions:
- It is not possible to format any partition on the system drive after DriveLock FDE has been installed.
- DriveLock FDE does not support post-installation addition, removal or substitution of hard drives.

During installation, DriveLock FDE examines all partitions present on the computer. Repartitioning, resizing, converting or activating partitions after DriveLock FDE has been installed is not supported, including any manipulation of the Master Boot Record.

DriveLock FDE supports the use of FAT16, FAT32, and NTFS file systems.

DriveLock FDE does not support multi-boot environments.

> MS-DOS can be used to start a computer to run DriveLock FDE disaster recovery tools. Computers running DriveLock FDE with a hard disk that is inaccessible or corrupt can be booted to MS-DOS from a floppy disk or a CD. Drives that require special DOS drivers, such as SCSI drives or TSRs are only accessible to the DriveLock FDE recovery tools if the required drivers are loaded.

Supported Networks

DriveLock FDE fully supports Active Directory and Windows domains. It does not interfere with normal operation of any Windows network services, including Remote Desktop connections. Windows domain users and local Windows users can authenticate to computers that are secured by DriveLock FDE. All hard disk partitions encrypted with DriveLock FDE can be shared on a network at the discretion of the system administrator.

 © 2015 CenterTools Software GmbH

Software Compatibility

DriveLock FDE has been tested and does not interfere with normal operation of most Windows-compliant software, applications, services and utilities. Some care needs to be taken, however, when using the following.

- *DOS Drivers and TSRs*: When booted from a DOS floppy disk or CD, DriveLock FDE can access hard disks that require DOS drivers and TSRs only if the appropriate drivers have been loaded.
- *Windows and Third-Party Boot Managers*: At system start-up, DriveLock FDE manipulates the Master Boot Record (MBR) and verifies its integrity. All software that needs to manipulate the MBR for its own purposes is incompatible with DriveLock FDE. This includes the standard Windows boot manager.
- *Windows Disk Management Utility*: No disk repartitioning, resizing, and mirroring configuration changes can be performed after DriveLock FDE has been installed. If any of the above operations are required, decrypt all disks and uninstall DriveLock FDE before proceeding.
- *Windows File Compression*: Windows file compression is fully supported, with the following exception: The DriveLock FDE system files directory (C:\Securdsk) must not be compressed.

Do not install DriveLock FDE to a compressed system drive. Doing this leads to compression of the C:\Securdsk directory, interfering with normal operations of DriveLock FDE.

The directory C:\Securdsk is a hidden system directory that can't be viewed by regular users.

- *Windows System Restore Utility*: After DriveLock FDE has been installed, Windows system-restore points that were created prior to the installation can no longer be used to restore a computer to a previous state. You can only restore the system to a restore point created following the installation of DriveLock FDE.
- *Windows Fast User Switching*: DriveLock FDE disables the standard Windows Welcome screen along with its fast user switching functionality.

 © 2015 CenterTools Software GmbH

Part V

Installing DriveLock

DON'T GAMBLE WITH YOUR DATA

5 Installing DriveLock

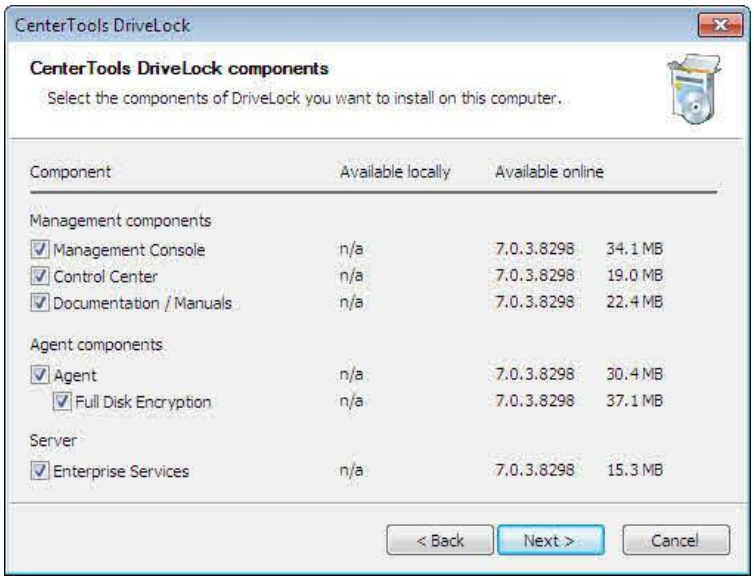
The following sections describe the steps that are required to install the DriveLock components:

- Evaluation Installation
- Installing the DriveLock Enterprise Service
- Installing the DriveLock Management Components
- Installing the DriveLock Agent

5.1 Evaluation Installation

In this type of installation all DriveLock components are installed on a single computer running (Windows Vista or later). This is the recommended installation type for evaluating DriveLock. The use of Microsoft SQL Server Express 2008 is recommended to support this installation type.

To start the installation, run the DriveLock Installer (*DLSetup.exe*) to first download all installation packages from the Internet and then install them on the local computer. For a complete installation on a computer where you want to evaluate DriveLock, simply select all components.



The DriveLock Installer is described in more detail in the section Installing DriveLock Management Components. More details about installing the DriveLock Enterprise Service are available in the section Installing the DriveLock Enterprise Service.

5.2 Installing the DriveLock Enterprise Service

The DriveLock Enterprise Service (DES) is the central component of the DriveLock product family that needs to be installed on a central server. The DES requires a database server where the DriveLock databases are created and maintained.

Before you start the DES installation, create a service account that the DES will use for database access. Unless the DES server is also the database server, this must be a domain

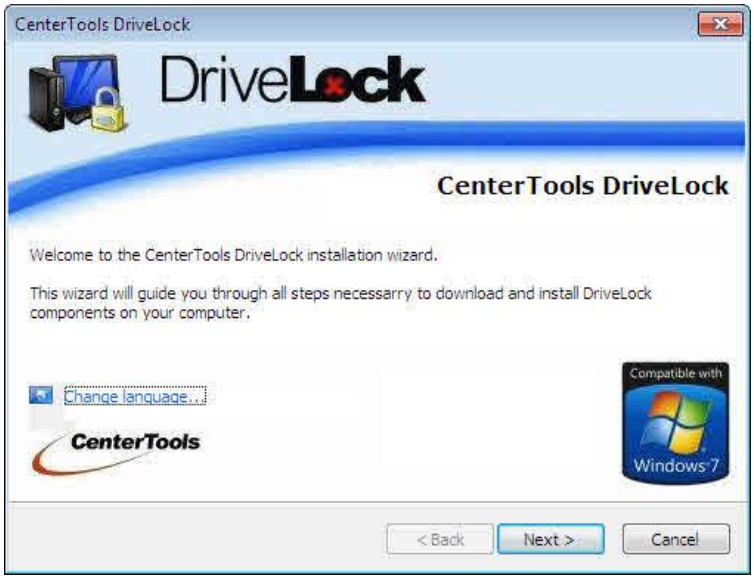
 © 2015 CenterTools Software GmbH

account with the password set to never expire. You don't need to assign any special permissions or rights to the account.

You can install DES using the DriveLock Installer, which can check whether a more recent version is available via the Internet.

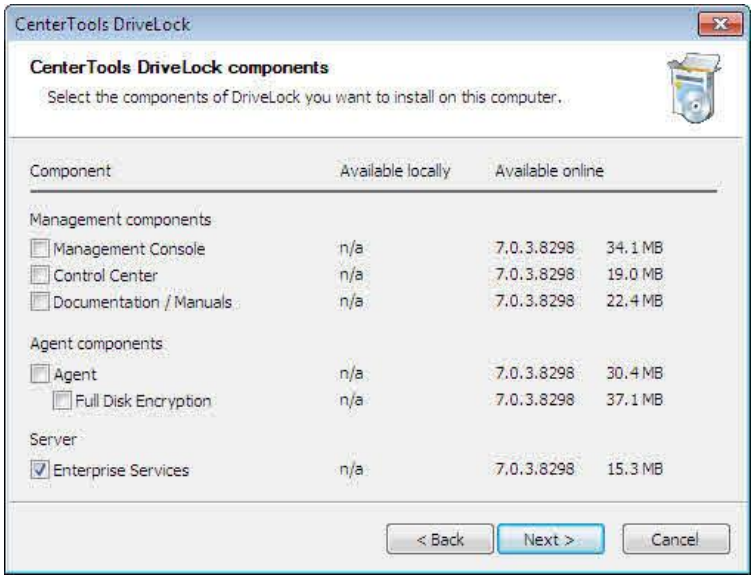
To start the installation, copy the DriveLock Installer (*DLSetup.exe*) to a folder on your hard drive. All installation packages that the Installer downloads will be stored in the same folder and can later be used for additional installations.

To start the DriveLock Installer, double-click it in Windows Explorer.



If a newer version of the Installer is available, a notification appears and you can select to download the newest version.

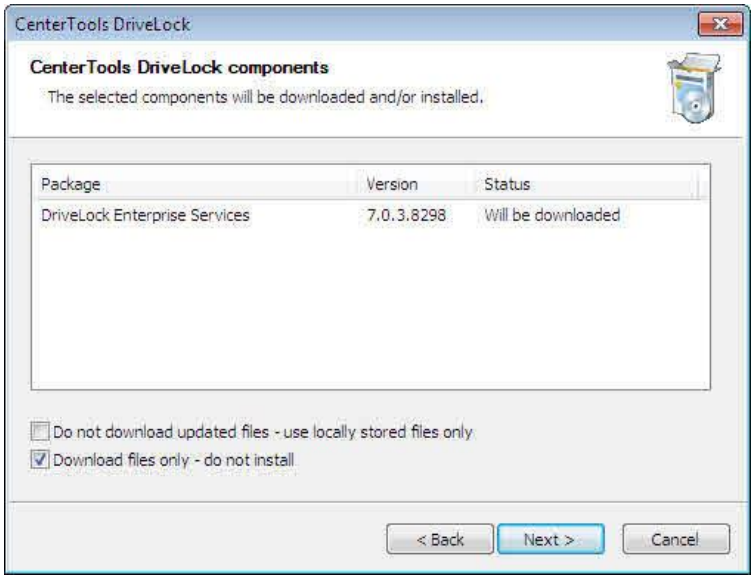
Click **Next**, accept the license agreement and then click **Next** again.



To install DES, select the last checkbox. The Installer will check whether an installation package is already present and whether a newer version is available.

 © 2015 CenterTools Software GmbH

Click **Next**.



To only download the selected components but not install them, select the checkbox *Download files only*.

To use local versions of the selected components without downloading newer versions, select the checkbox *Do not download files*.

Click **Next** to start the download or installation. When the process has complete, a notification is displayed.

Click **Finish** to complete installation. Unless you selected the option to only download the installation package, the DriveLock Enterprise Service Setup Wizard starts.

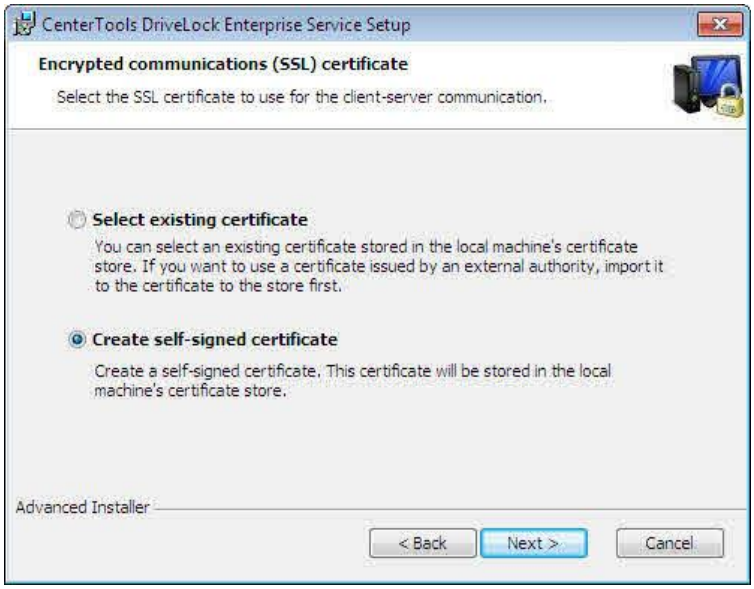
Click **Next**.

 © 2015 CenterTools Software GmbH

Type the user name and password of the service account used to run the DriveLock Enterprise Service or click **Browse** to select an existing account.

Click **Next** to continue installation.

> Use the Continue without validation checkbox only if the user account can't be verified but you are certain that the account exists and that you want to proceed with the installation.

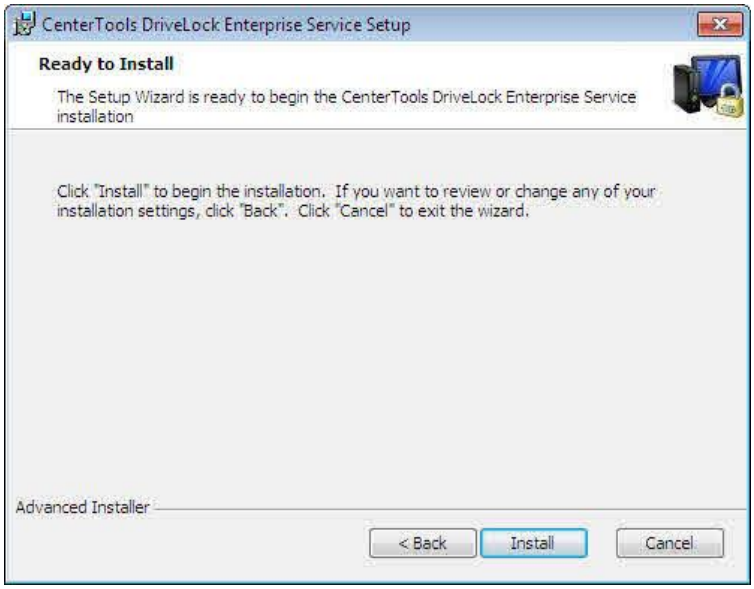


A certificate is required for the encrypted client-server communication.

Click **Select existing certificate** if the SSL certificate you want to use is already in the computer's certificate store and select the "*DriveLock Enterprise Service*" certificate. Click **Next**, select the certificate from the list, and then click **OK** to confirm.

To have DriveLock create a certificate, click **Create self-signed certificate** and then click **Next**.

 © 2015 CenterTools Software GmbH

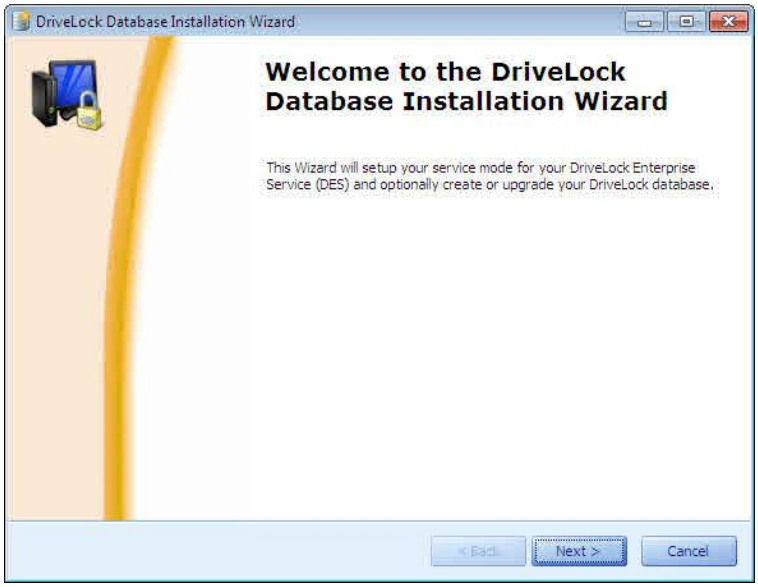


Click **Install**.

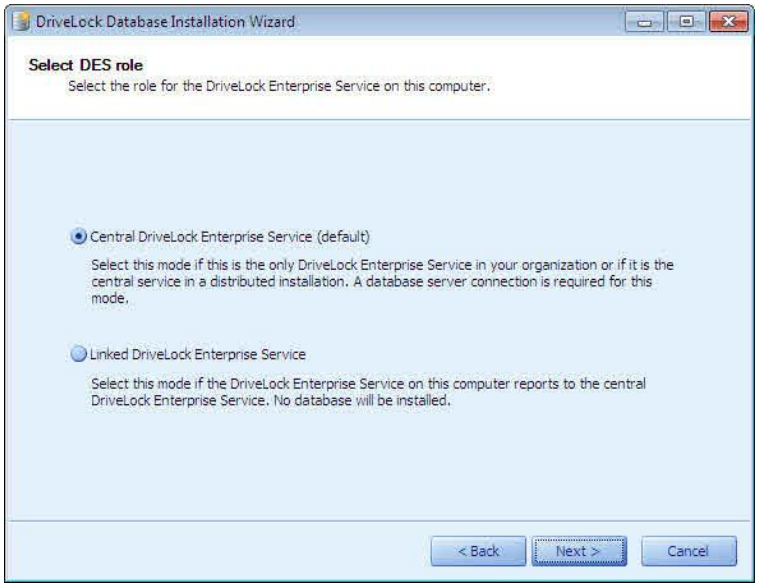
When the installation has completed, click **Finish** to close the wizard.

When the installation is complete, the Database Installation Wizard starts. This wizard guides you through the process of installing, configuring or updating the DES database. You can also use the wizard to change the DES mode for branch offices deployments.

 © 2015 CenterTools Software GmbH



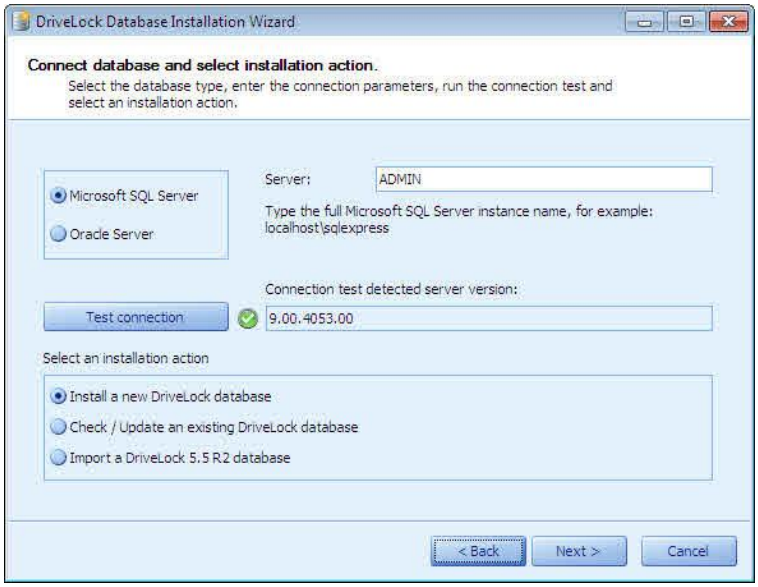
Click **Next**.



Select the server role and then click **Next**.

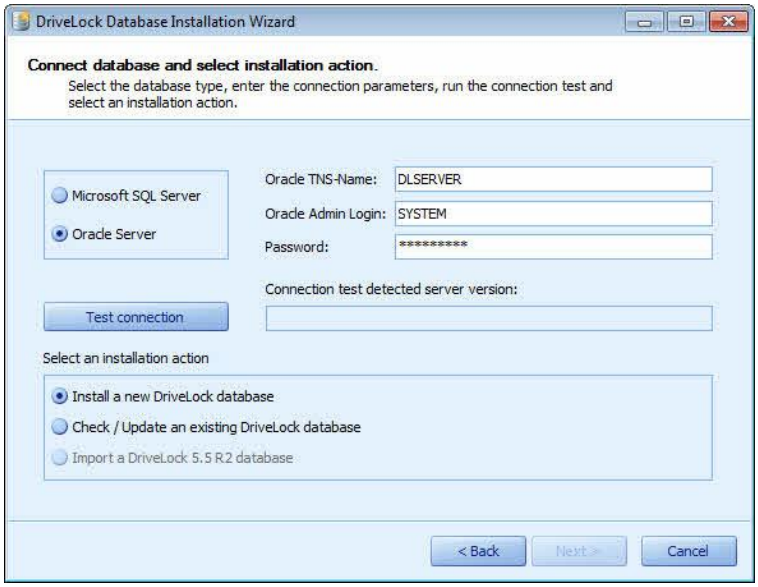
> If you are installing the first DES-Server in your organization, select the *Central DriveLock Enterprise Service* mode. For more information about server modes, refer to the *Architecture* chapter in the *DriveLock Enterprise Service* manual.

 © 2015 CenterTools Software GmbH



Select the database server type, Microsoft SQL Server or Oracle. Type the name of the database server and, if required, the name of the database instance.

If you use an Oracle database select *Oracle Server.*

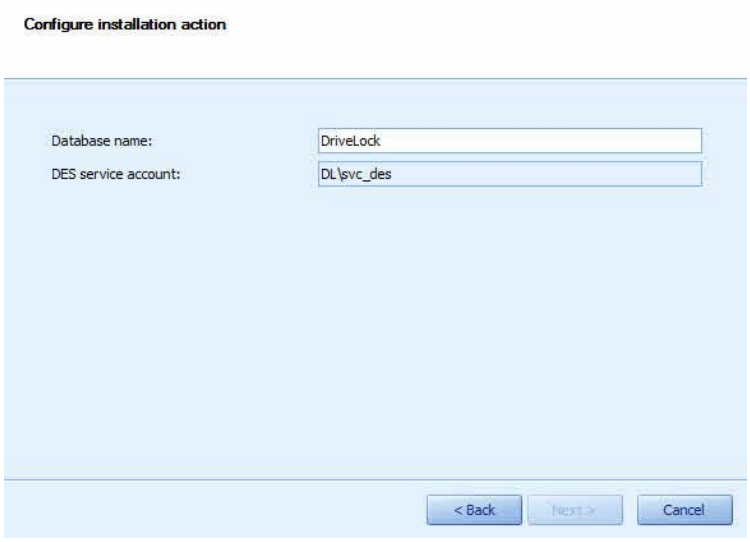


Specify the Oracle TNS name, administrator login and password. The login will be used to create the DriveLock databases on the server.

To confirm that DES can connect to the server, click **Test Connection**. Finally select whether to create a new DriveLock database, update an existing DriveLock database or to import an existing DriveLock 5.5 R2 database, and then click **Next**.

An upgrade of an existing DriveLock 5.5 R2 database cannot be performed in place. Instead you need to create a new database and import the contents of the old database. For more information about such an upgrade, refer to the section Migrating a Legacy Database.

 © 2015 CenterTools Software GmbH

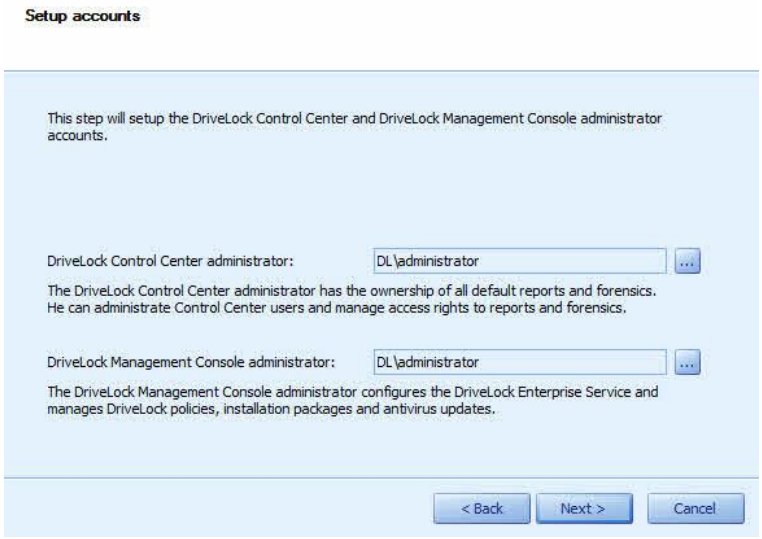


Type the following information:

- *Database name* (If using an Oracle server, also specify the tablespace, which needs to match the name of the database files. During the installation the database user and tablespace (name = user+" TS") will be created using scripts.
- Path to the database files on the server (Oracle only)

The service account that the DES services use to connect to the database was specified during the installation.

Click **Next** to continue.



Select the initial accounts for the following two security roles:

- DriveLock Control Center administrator and SID: A group or user and corresponding security identifier (SID) that will initially be assigned Full Control permissions to use the DriveLock Control Center. You can change this account or add additional users and groups in the Control Center after the database installation has completed.
- DriveLock Management Console administrator and SID: A group or user and corresponding security identifier (SID) that will initially be assigned permissions to configure the DriveLock Enterprise Service using the

 © 2015 CenterTools Software GmbH

Management Console. You can change this account or add additional users and groups in the DriveLock Management Console after the database installation has completed.

Click **Next** to continue.

A summary of the installation settings is displayed. Review these settings and then click **Next** to start the installation.

The configuration procedure may take several minutes, depending on the database server you are using. The installation wizard creates two databases based on the information you provided (for example, *DriveLock* and *DriveLock-Data* if you use Microsoft SQL Server).

When the installation is complete, click **Next**.

To complete the installation, click **Finish**.

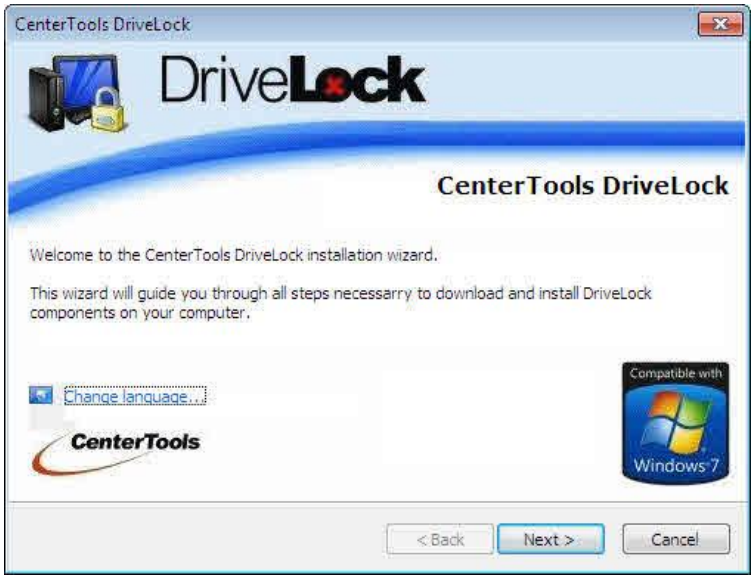
5.3 Installing the DriveLock Management Components

You can install all DriveLock management components using the DriveLock Installer, which can check whether a more recent version is available via the Internet.

To start the installation, copy the DriveLock Installer (*DLSetup.exe)* to a folder on your hard drive. All installation packages that the Installer downloads will be stored in the same folder and can later be used for additional installations.

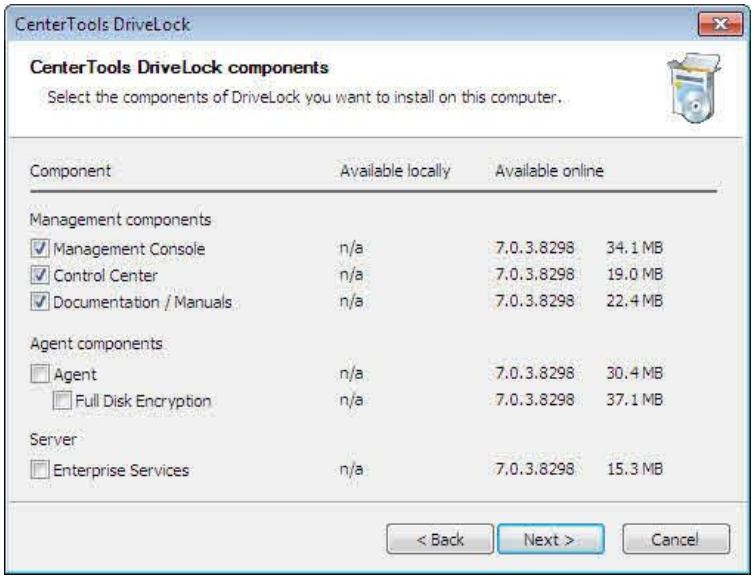
To start the DriveLock Installer, double-click it in Windows Explorer.

 © 2015 CenterTools Software GmbH



If a newer version of the Installer is available, a notification appears and you can select to download the newest version.

Click **Next**, accept the license agreement and then click **Next** again.

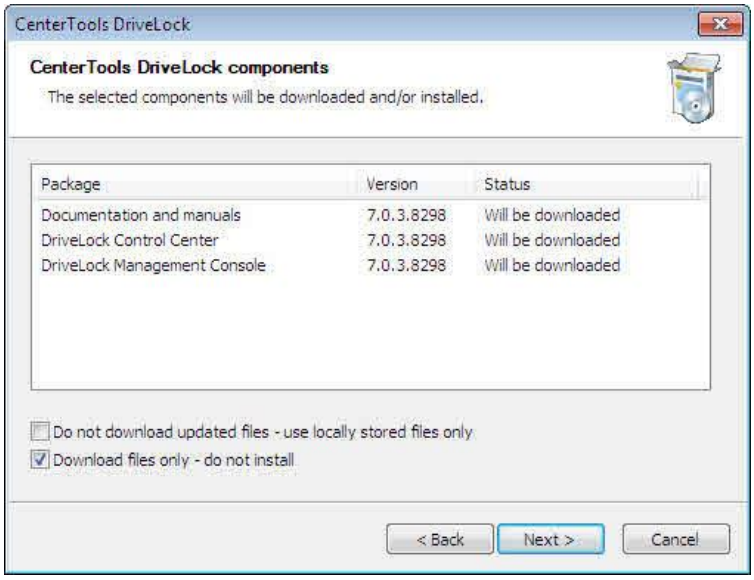


To install the management components and documentation, select the first three checkboxes. The Installer will check whether any of the components are already present and whether newer versions of these components are available.

> When performing an evaluation installation, select all components.

Click **Next**.

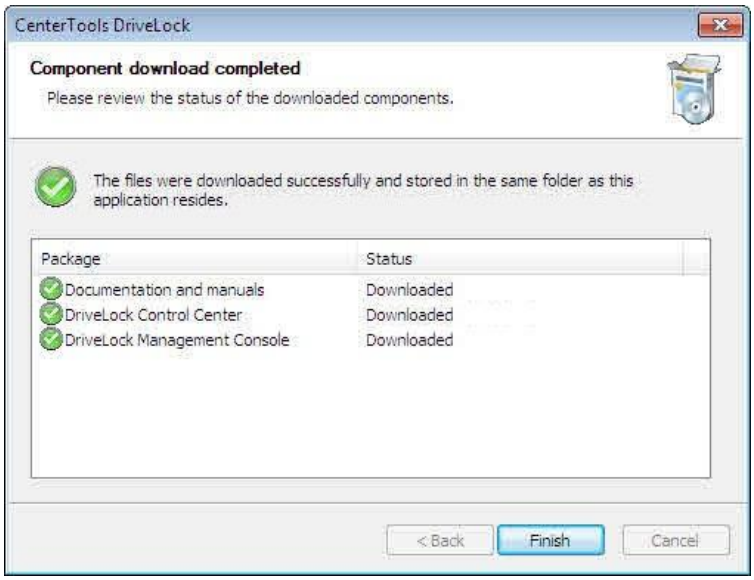
 © 2015 CenterTools Software GmbH



To only download the selected components but not install them select the checkbox *Download files only*.

To use local versions of the selected components without downloading newer versions, select the checkbox *Do not download files*.

Click **Next** to start the download or installation. When the process has complete, a notification is displayed.



Click **Finish** to complete the installation or download.

5.4 Installing the DriveLock Agent

The DriveLock Agent must be installed on each client computer where you want to control access to removable drives and devices.

Standalone Windows Installer packages are provided for installing the DriveLock Agent on client computers that are not administrative workstations. These installation packages (**DriveLockAgent.msi** and **DriveLockAgent_AMD64.msi**) install the DriveLock Agent service without creating any entries in the Start menu and without requiring any user input (silent installation).

 © 2015 CenterTools Software GmbH

> The packages for the DriveLock Agent installation are located on the DriveLock CD (an ISO image for burning a CD is available for downloading) or you can be downloaded by the DriveLock Installer from the Internet.

Before you install the Agent on client computers, you must have created a policy that contains at least the basic configuration settings and whitelist entries that need to be applied on client computers when the Agent is installed. This policy must be available to clients at the time of the installation via Group Policy, centrally stored policy or configuration file. As soon as the Agent installation has completed, the Agent is started and applies either an available policy or the default settings.

If you install the Agent without providing configuration settings, the default settings, which block access to most removable drives, are applied. As a result, devices or drives that are required for proper operation of client computers may be locked.

When using a configuration file you need to customize the Agent installation package before deployment to ensure that the Agent can find the configuration file. When using Group Policy, no customization is required. When using or a centrally stored policy, customization is only required if Quick Configuration is not available. Quick Configuration is not available if you disabled the automatic discovery mechanism or if multicast communications using mDNS/DNS-SD are blocked, which is frequently the case in large corporate networks.

The following sections describe each installation method for the DriveLock Agent.

5.4.1 Installing DriveLock by using Active Directory Group Policy

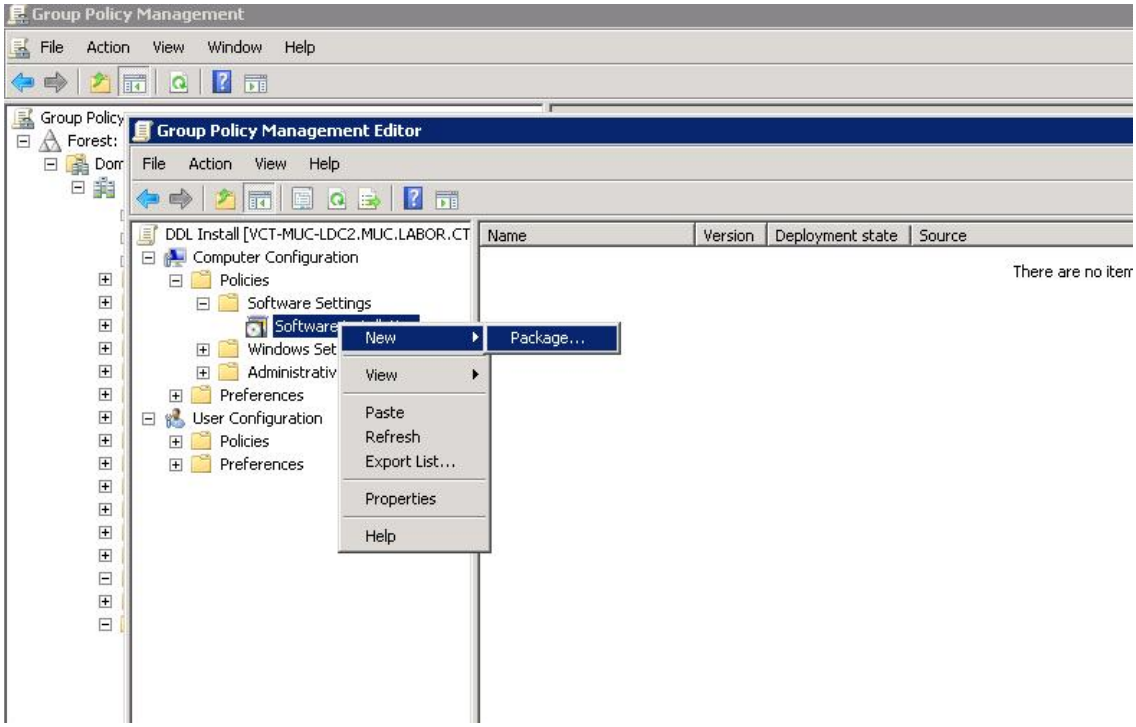
A convenient way to deploy DriveLock Agents to target machines is by using Active Directory Group Policy.

Deploying DriveLock Agents by using Group Policy requires that the **DriveLockAgent.msi** Windows installer package (for 64-bit operating systems use **DriveLockAgent_X64.msi**) is located in a shared folder that the client computer can access.

> Additional information about using Group Policy Objects is available on the Microsoft TechNet Web site.

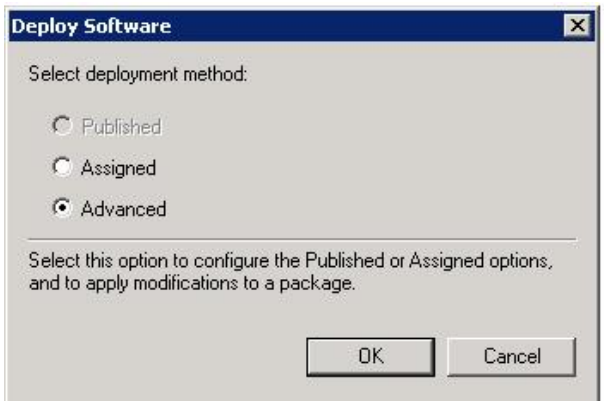
To configure a software deployment policy for 32-bit computers, open an existing Group Policy Object or create a new one. In the Windows Group Policy Object Editor, in the console tree, navigate to **Computer Configuration → Software Settings → Software installation**.

 © 2015 CenterTools Software GmbH



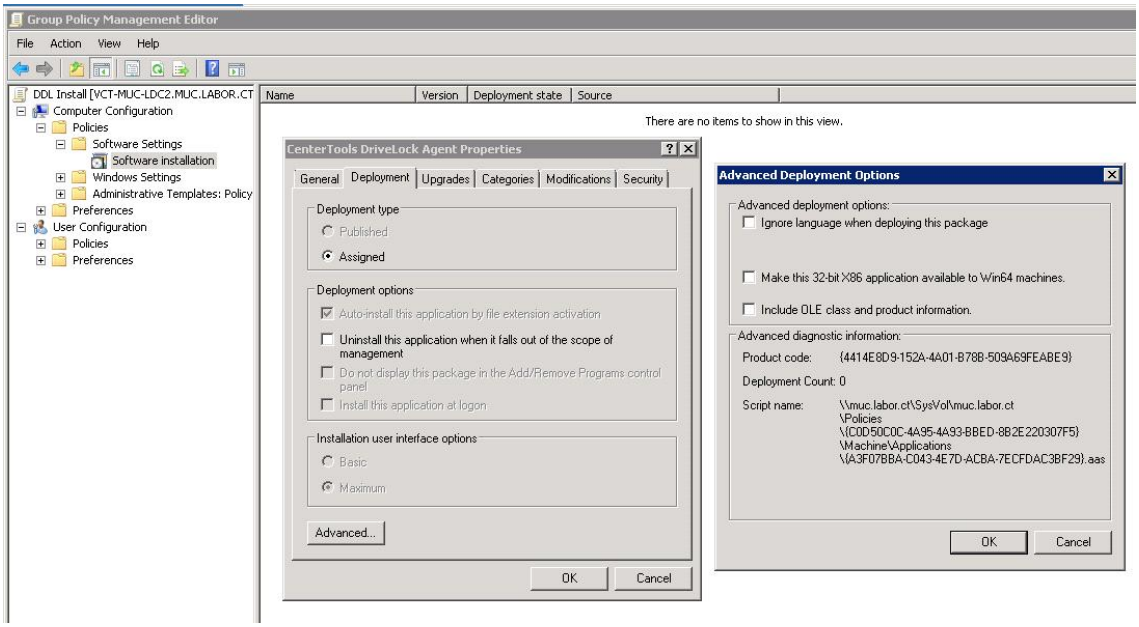
You can also use the DriveLock Management Console to open or create a Group Policy Object.

Right-click **Software installation,** and then click **New → Package**. Navigate to the shared folder that contains the installation package, select the **DriveLockAgent.msi** file and then click **Open**. Ensure that the file name is displayed in Universal Naming Convention (UNC) format (for example, "*\\Server\drivelock$\DriveLockAgent.msi*").



Select *Advanced* as the deployment method and then click **OK**.

 © 2015 CenterTools Software GmbH



Select the **Deployment** tab and click **Advanced**. Uncheck the option "**Make this 32-bit X86 application available to Win64 machines**".

Click **OK** twice.

The Group Policy Object is now configured and the Agent rollout will start after the policy is replicated to domain controllers and applied to the target machines.

Repeat these steps for 64-bit computer, use the DriveLockAgent_X64.msi file instead and don't change the advanced deployment options.

DriveLock should not be assigned to the User Settings in a GPO, as DriveLock is a computer-focused application.

DriveLock configuration settings are not installed automatically with the software package. These settings, including a valid license file, must be provided separately as part of the same or a separate GPO. The use of separate GPOs for installing the Agent and distributing policy settings is recommended.

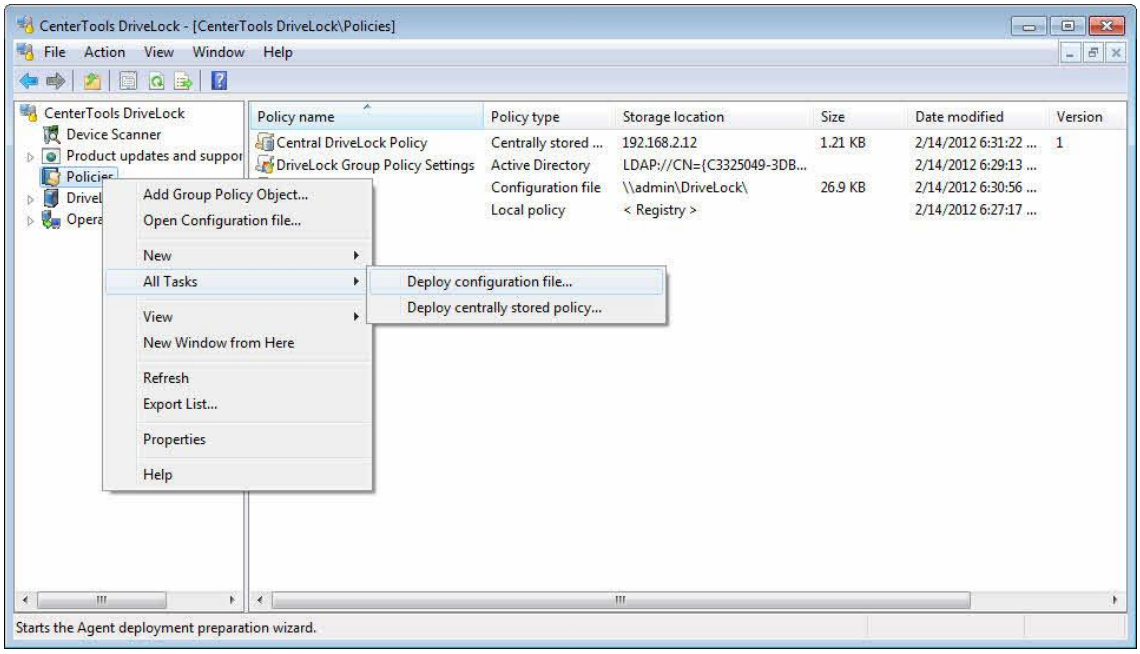
If you install the DriveLock Agent by using Group Policy, it can't be uninstalled from the Add/Remove Programs application in Control Panel. Instead, remove the software package from the GPO.

5.4.2 Installing the Agent by Using Configuration Files

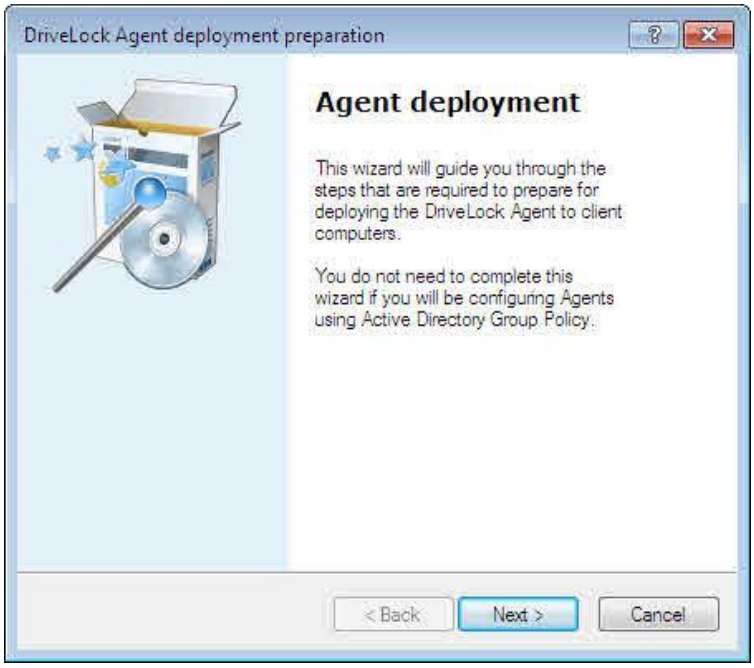
When you use a configuration file to deploy your DriveLock policy to client computers, copy this file to a shared folder, Web server or FTP server and specify the network path or URL during the Agent installation. For information about using a configuration file, refer to the DriveLock Administration Guide.

The DriveLock Deployment Wizard assists you in deploying the DriveLock Agent to computers in your network so that they use the correct configuration file. The wizard helps you create the correct command line for Windows Installer, generates a modified Microsoft Installer (.msi) package, or creates a Microsoft Installer Transform (.mst) file for your installation.

 © 2015 CenterTools Software GmbH

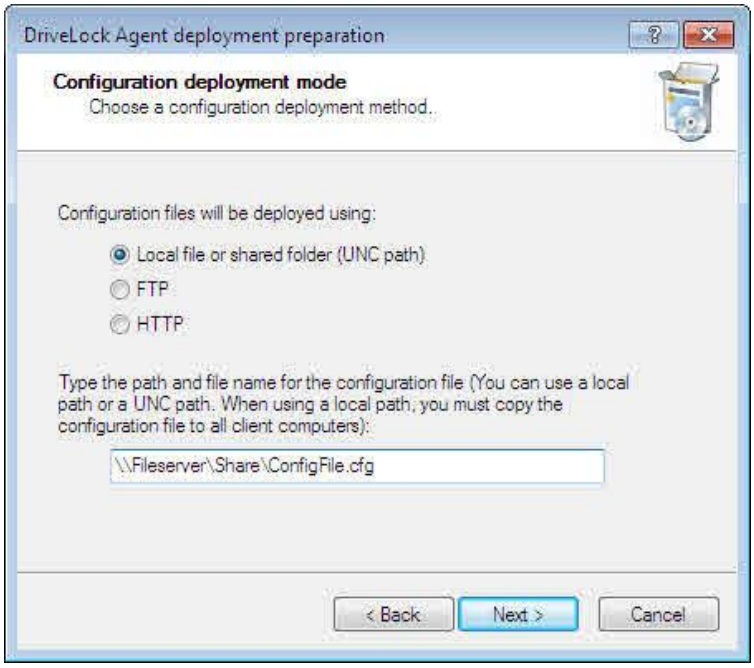


To launch the wizard, right-click **Configuration files**, point to "**All Tasks**" and then click "**Deployment wizard...**".



Click **Next** to continue.

 © 2015 CenterTools Software GmbH



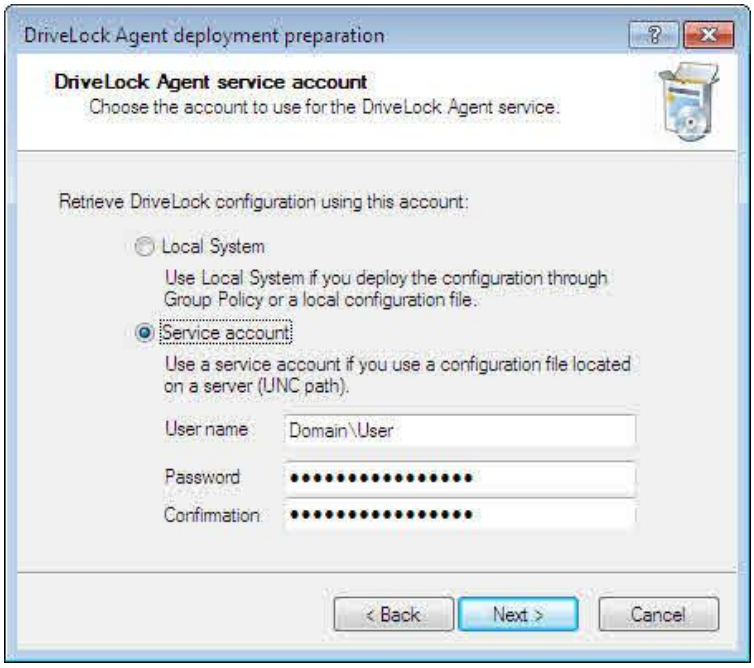
Specify the location from which the DriveLock Agent will retrieve the configuration file. You can specify a UNC path, an FTP location or an HTTP location. You can also specify a local path that can be accessed by the local System account (for example, **C:\Windows\DLConfig**).

After entering the location of the configuration file, click **Next**.

Specify the user credentials that are used to access the configuration file:

- *Local System*: DriveLock will connect to the configuration file by using the local System account on the client computer. This is the recommended setting if the configuration file is stored locally on client computers.
- *Service Account*: DriveLock will use the account you specify. This account must have permissions to access the file on the remote server. The account password will be stored in an encrypted format.
- *Anonymous*: If you have selected either an FTP or HTTP path, type **Anonymous** as the name of the service account and leave the password blank. The FTP or HTTP server must allow anonymous access to the configuration file.

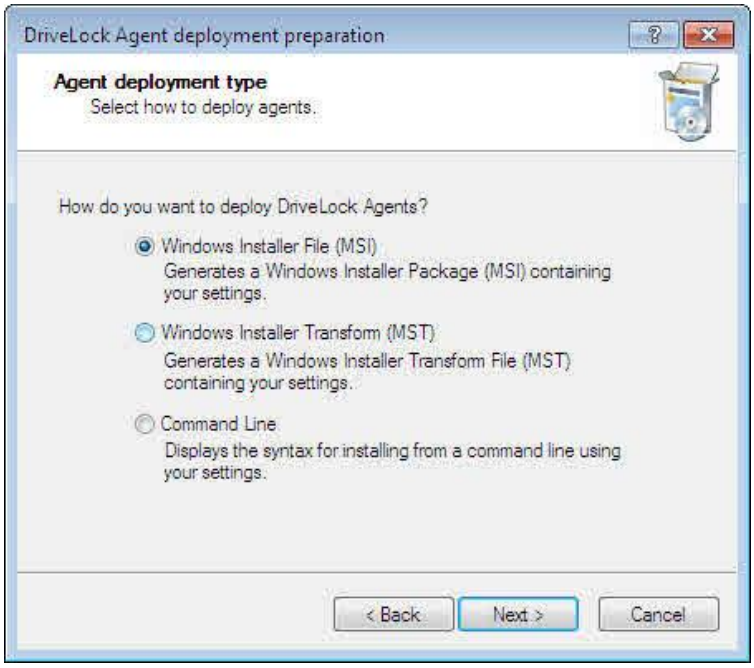
 © 2015 CenterTools Software GmbH



Click **Next**

On the next page select the type of installation package that will be created by the wizard:

- *Microsoft Installer File (MSI)*: Creates a new Microsoft Installer package that contains your settings.
- *Microsoft Installer Transform file (MST)*: Creates a Microsoft Installer Transform (.mst) file that contains your settings. An MST file must be used in conjunction with the original MSI package that is included in the DriveLock installation.
- *Command line*: Shows the Microsoft Installer command line options for implementing the settings you have selected.

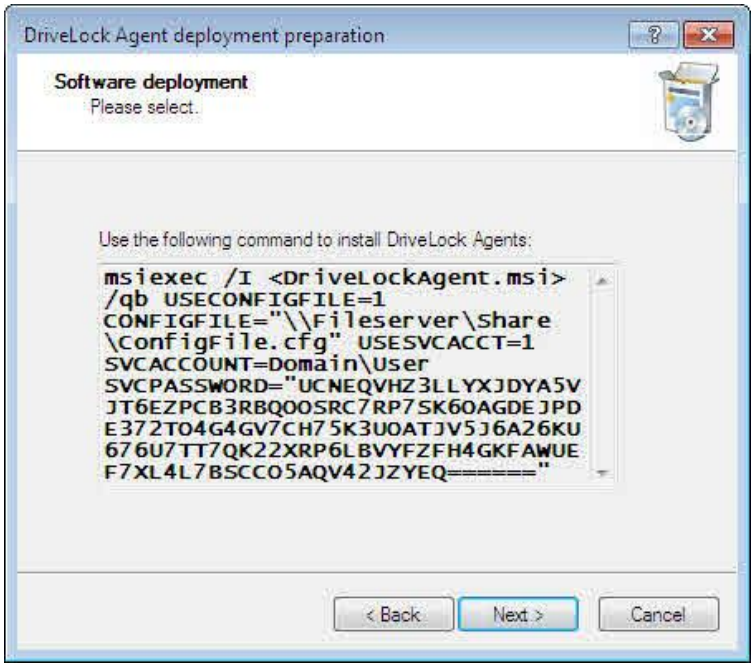


Click **Next**.

If you selected *Command Line*, the next page displays the command you must use to install the DriveLock Agent. When using this command line, you must change "**<DriveLockAgent.msi>**" to the full path of

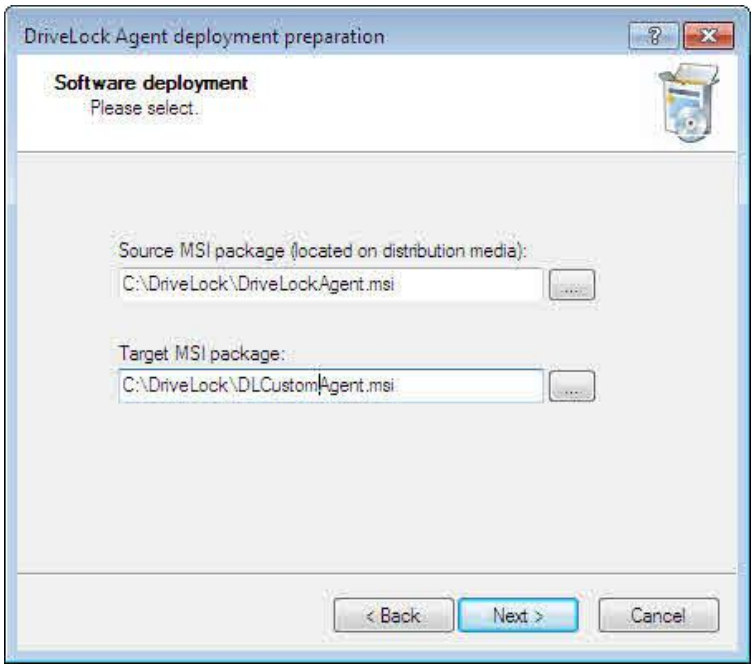
 © 2015 CenterTools Software GmbH

DriveLockAgent.msi file.



> The command can be used for a manual Agent installation. For more information about this, refer to the section Installation from a Command Prompt (Silent Installation).

If you selected the option to generate a new MSI file, you must provide the location and name of the original **DriveLockAgent.msi** file and the customized MSI file to be created.

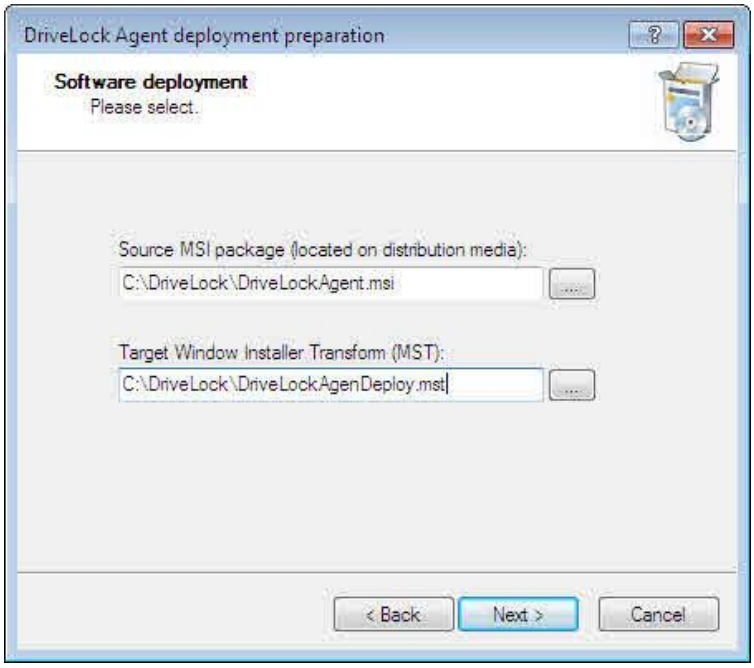


Type the name and location for both files, and then click **Next** to generate the new MSI file.

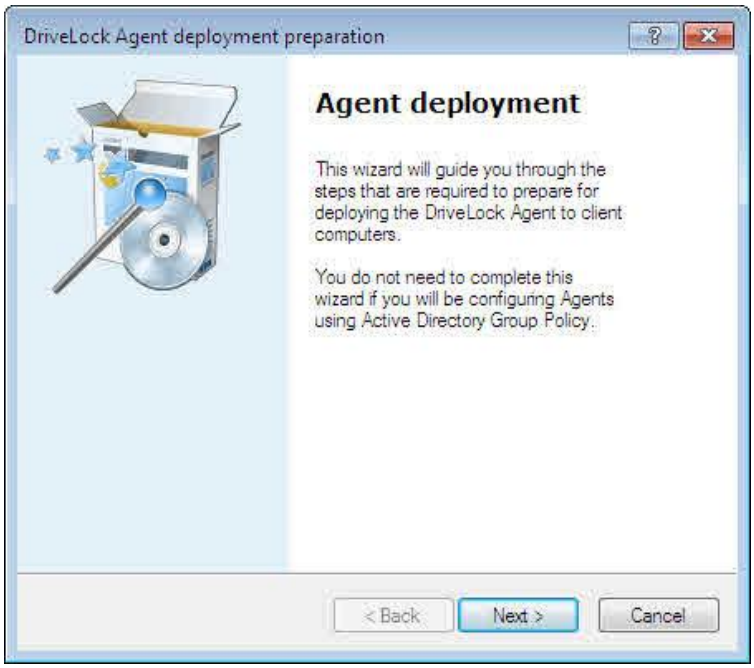
> You can use the modified installer package you created to install the Agent manually or to deploy it using third-party deployment software.

 © 2015 CenterTools Software GmbH

To generate a Microsoft Installer Transform (.mst) file you must provide the location and name original **DriveLockAgent.msi** file and the MST file.



Type the name and location for both files, and then click **Next** to generate the new MST file.

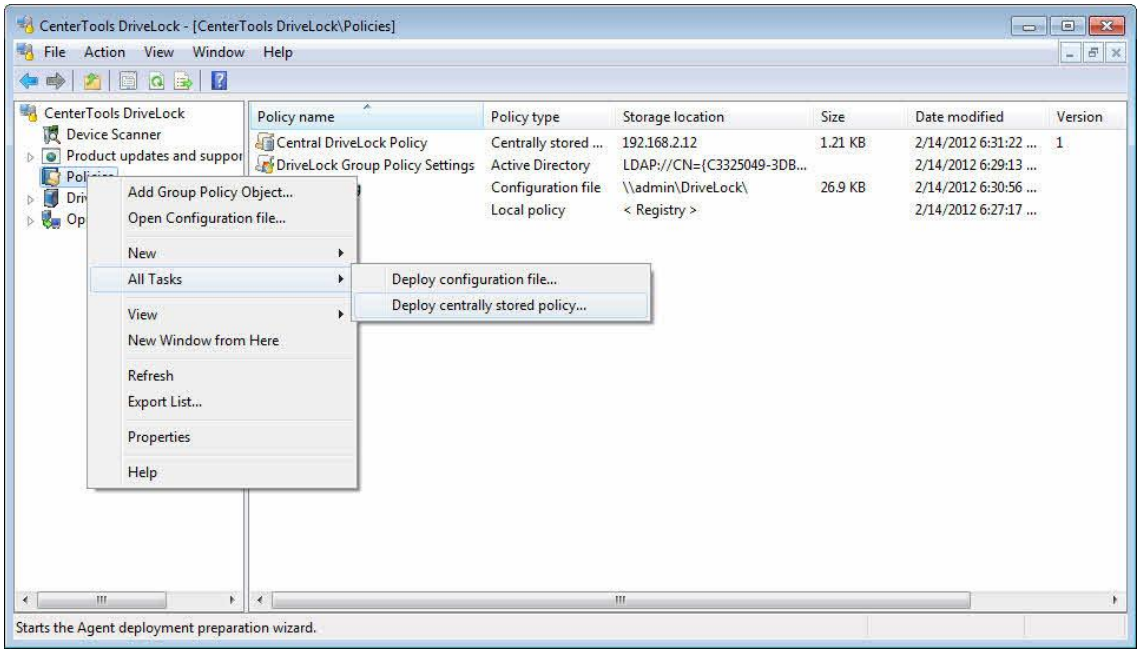


After you have completed the Agent Deployment Wizard you continue the deployment by using the Microsoft Installer package or the command line.

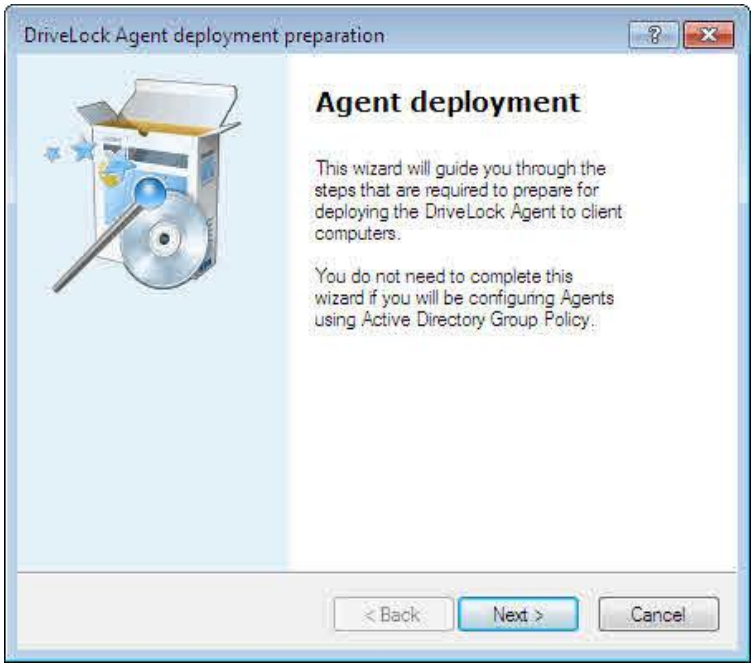
5.4.3 Installing the Agent with a Centrally Stored Policy without Quick Configuration

The DriveLock Deployment Wizard also assists you in deploying the DriveLock Agent to computers in your network by using a Centrally Stored Configuration. The wizard helps you create the correct command line for Windows Installer, generates a modified Microsoft Installer (.msi) package, or creates a Microsoft Installer Transform (.mst) file for your installation.

 © 2015 CenterTools Software GmbH

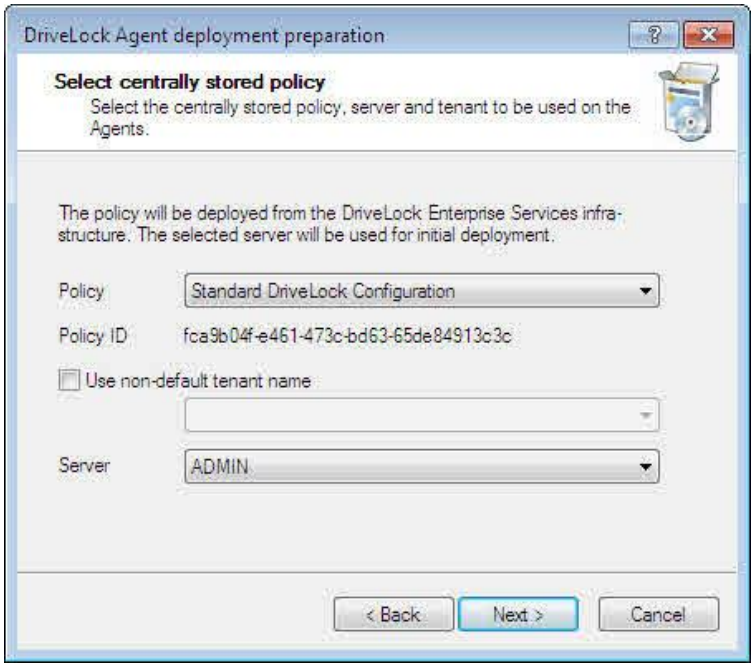


To launch the wizard, right-click **Policies**, point to "**All Tasks**" and then click "**Deploy centrally stored policy...**".



Click **Next** to continue.

 © 2015 CenterTools Software GmbH



Specify the centrally stored policy that the DriveLock Agent will use and the server where the central DriveLock Enterprise Service is running.

If you are using multiple DriveLock configuration environments (tenants), select the tenant from the drop-down list.

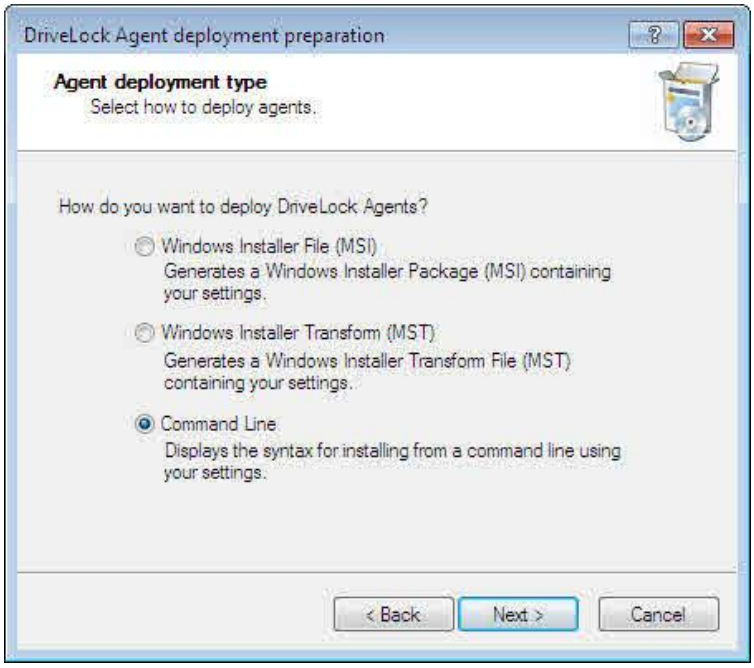
After entering the location of the configuration file, click **Next**.

Click **Next**

On the next page select the type of installation package that will be created by the wizard:

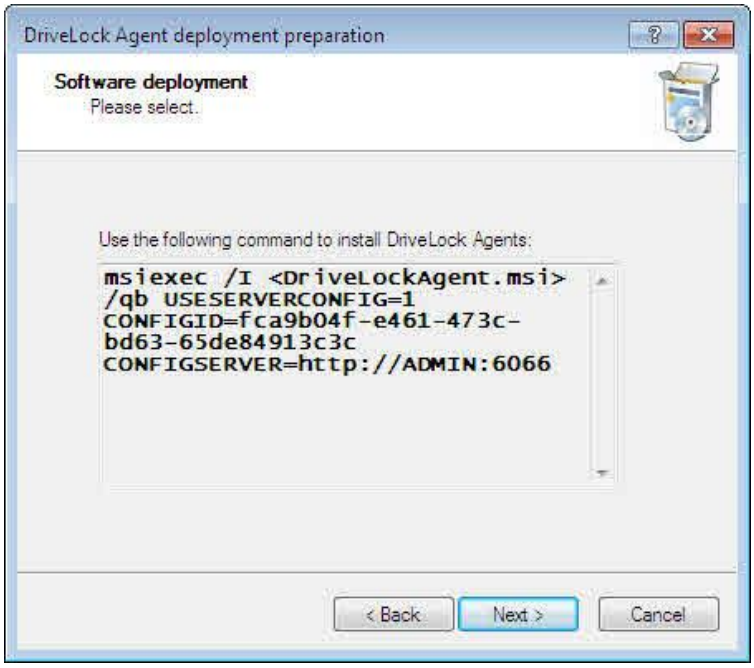
- *Microsoft Installer File (MSI)*: Creates a new Microsoft Installer package that contains your settings.
- *Microsoft Installer Transform file (MST)*: Creates a Microsoft Installer Transform (.mst) file that contains your settings. An MST file must be used in conjunction with the original MSI package that is included in the DriveLock installation.
- *Command line*: Shows the Microsoft Installer command line options for implementing the settings you have selected.

 © 2015 CenterTools Software GmbH



Click **Next**.

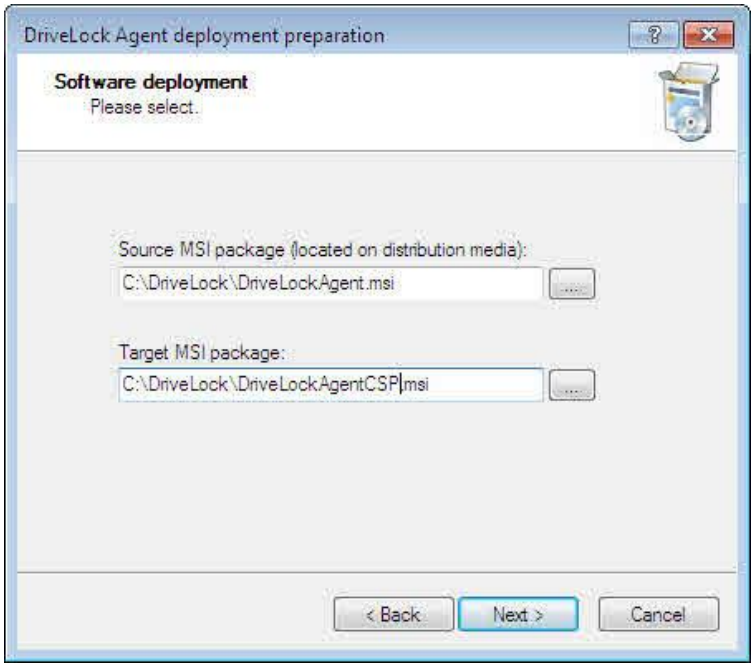
If you selected *Command Line*, the next page displays the command you must use to install the DriveLock Agent. When using this command line, you must change "**<DriveLockAgent.msi>**" to the full path of DriveLockAgent.msi file.



> The command can be used for a manual Agent installation. For more information about this, refer to the section Installation from a Command Prompt (Silent Installation).

If you selected the option to generate a new MSI file, you must provide the location and name of the original **DriveLockAgent.msi** file and the customized MSI file to be created.

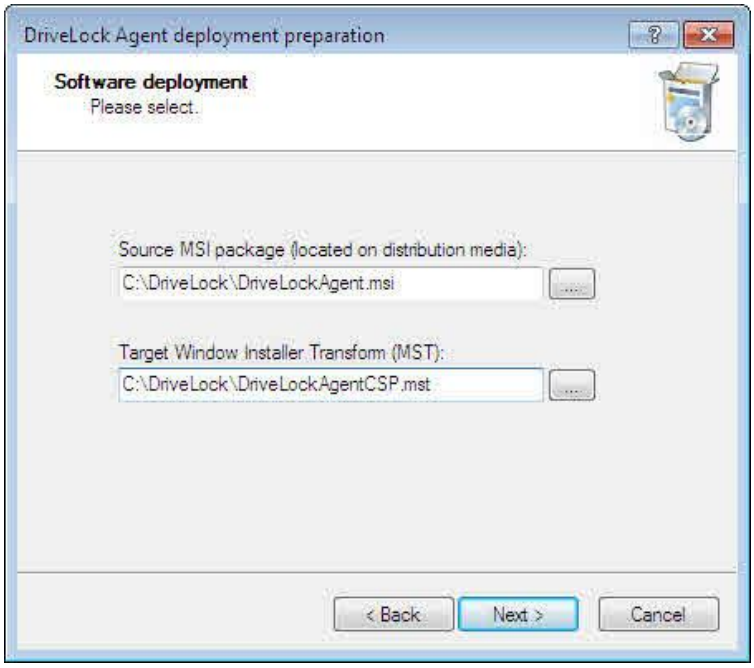
 © 2015 CenterTools Software GmbH



Type the name and location for both files, and then click **Next** to generate the new MSI file.

> You can use the modified installer package you created to install the Agent manually or to deploy it using third-party deployment software.

To generate a Microsoft Installer Transform (.mst) file you must provide the location and name original **DriveLockAgent.msi** file and the MST file.



Type the name and location for both files, and then click **Next** to generate the new MST file.

After you have completed the Agent Deployment Wizard you continue the deployment by using the Microsoft Installer package or the command line.

 © 2015 CenterTools Software GmbH

5.4.4 Installation from a Command Prompt (Silent Installation)

If you install the Agent from a command prompt or a script, you can specify additional options. The options allow you to specify from where the Agent will get its configuration settings and where the Agent retrieves the configuration.

To silently install the Agent without displaying the InstallShield Wizard and with the default configuration settings, use the following command:

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

If you must specify a configuration file location for the Agent, either use an installation package that has been modified by the wizard (.msi file), or use a wizard-generated command such as the following:

```
msiexec /i DriveLockAgent.msi /qn USECONFIGFILE=1 CONFIGFILE="\\fileserver\share\drivelock
```

When installing the Agent to use a centrally stored policy, the available options are:

USESERVERCONFIG=1	Indicates that a centrally stored policy is used.
CONFIGID="<GUID>"	<GUID> is the GUID of the centrally stored policy in the format XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
CONFIGSERVER=<name>	<name> is the name of the server where the DriveLock Enterprise Service is running and from where the configuration will be downloaded.
TENANTNAME=<tenant>	In a multi-tenant DES environment, <tenant> is the name of the tenant the policy has been configured for. If you are not using multiple tenants, specify *root* as the tenant name.

When installing the Agent to use a configuration file, the available options are:

USECONFIGFILE=1	Needed if you specify the location from where the Agent gets its configuration.
CONFIGFILE="<path>"	<path> can be any valid UNC, FTP of HTTP path to the configuration file. Examples: UNC: \\myserver\share$\drivelock\dlconfig.cfg FTP: myserver/pub/drivelock/dlconfig.cfg HTTP: http://myserver/drivelock/dlconfig.cfg
CONFIGPROTOCOL=[0|1|2]	0: <path> is a file location 1: <path> is an FTP location 2: <path> is an HTTP location
USESVCACCT=1	This parameter is needed if a user account is used to access the configuration file.
SVCACCOUNT=<account>	Specifies the account that is used to access the configuration file.

 © 2015 CenterTools Software GmbH

	Example: SVCACCOUNT=mydomain\myuser)
SVCPASSWORD="<encpwd>"	<encpwd> is the account's encrypted password that was created by the wizard.

To create the encrypted password, use the DriveLock Deployment Wizard.

You can also install DriveLock agents by using the original **DriveLockAgent.msi** in conjunction with a wizard-generated .mst file

```
msiexec /i DriveLockagent.msi /qn TRANSFORMS=Your_MST_file.mst
```

5.4.5 Installing the DriveLock FDE Component

The DriveLock Full Disk Encryption Component (FDE) is installed by the DriveLock Agent, as soon as an valid FDE license is available.

To apply the necessary settings, open the MMC policy - Centertools / Encryption / Disk Protection.

Encryption certificats

Create and administer the certificates required for the FDE

Deployment Settings

General - define, where the DriveLock agent will find the FDE installation package.

The FDE installation package is named DLFde.pkg resp. DLFdeX64.pkg and part of the DriveLock installation CD.

To deploy the FDE installation package with the DriveLock Enterprise Service (DES), upload and publish the package by using DriveLock Management Console. For more information about publishing installation packages, refer to the DriveLock Administration manual.

User interface - configure, whether and how a user will be informed during FDE installation and whether he has to confirm the messages.

Options - select how the pre-boot authentication will behave and look like.

> The configured background image must be PNG, the resolution and aspect ratio should be 1024x768, 4:3. It will only be installed during a new installation or when updating the FDE component to a new version. The other options will be activated after a each reboot of the computer.

If you disable the 32-bit PBA, a 16-bit version of the PBA with restricted functionality will be used, which boots faster, especially on older or low performance computers.

For more information about configuring the DriveLock FDE, refer to the DriveLock Administration manual.

 © 2015 CenterTools Software GmbH

Part VI

Updating DriveLock

DON'T GAMBLE WITH YOUR DATA

6 Updating DriveLock

Before updating DriveLock to a newer version, always review the current Release Notes.

Upgrading DriveLock components is generally a very easy process and can be performed using an in-place upgrade.

Starting with DriveLock 7 an automatic update feature is available that can automatically upgrade the DriveLock Agent and management components to the most recent version from the DriveLock Enterprise Service. For more information about this process, refer to the DriveLock Administration Guide.

The recommended order for upgrading DriveLock components is:

1. DriveLock Enterprise Service
2. DriveLock Management Console
3. DriveLock Control Center
4. DriveLock Agents

Because the installed version of the DriveLock Enterprise Service and the DriveLock Control Center must match, you need to upgrade both components at the same time to ensure a smooth transition.

When upgrading any DriveLock components, no Group Policy Objects or configuration files are modified. However, as a precaution, it is recommended to first export all local or Group Policy-based DriveLock policies to a file. For more information about exporting policies, refer to the **DriveLock Administration Guide**.

The following sections describe the manual upgrade process. For information about automatic updating, refer to the *DriveLock Administration Guide*.

6.1 Updating the DriveLock Enterprise Service

To update the DriveLock Enterprise Service to a newer version, perform the steps described in the section Installing the DriveLock Enterprise Service. The installation process will automatically detect an older version that is already installed and update the service and the database it uses.

Before updating the DriveLock Enterprise Service, always perform a database backup because the update process may modify the database to work with the new version.

Before updating a database from DriveLock 7.0 or older, it is recommended to manually perform database grooming to minimize the amount of data that needs to be migrated. To start the grooming process, run the following SQL commands on the database server:

Microsoft SQL Server:

```
EXEC ctsp_groomevents <max. Age of Events in Days>
z.B.: EXEC ctsp_groomevents 30
```

Oracle:

```
DECLARE
```

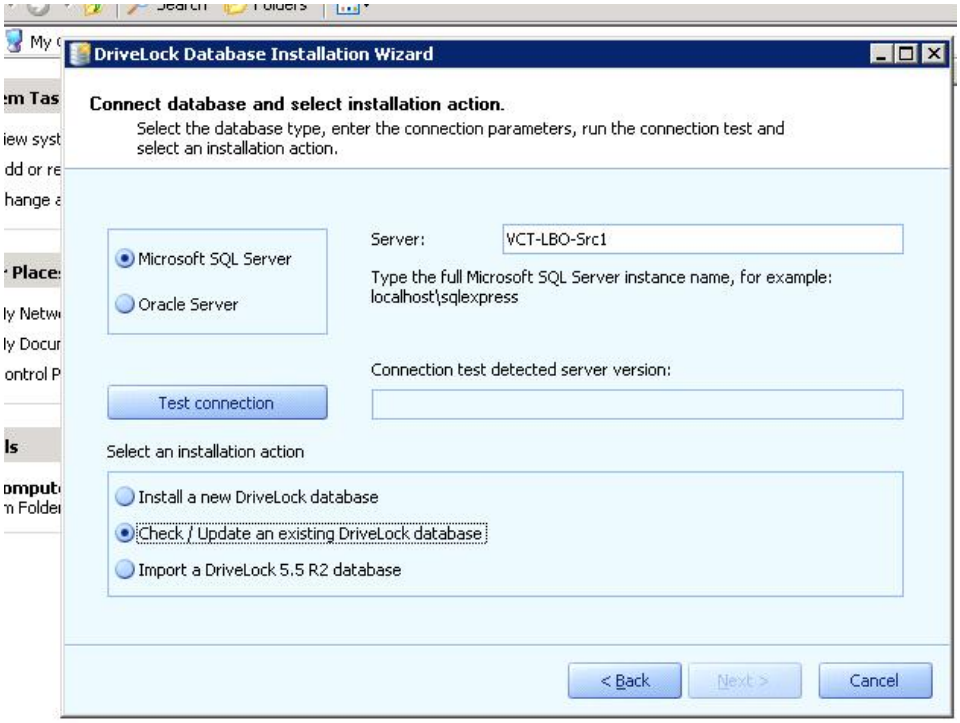
 © 2015 CenterTools Software GmbH

```
  DAYS NUMBER;
BEGIN
  DAYS := <max. Age of Events in Days>;
 "DRIVELOCK".CTSP_GROOMEVENTS(DAYS => DAYS);
END;
```

Upgrading from DES 60 and newer is easy and possible without losing any data.

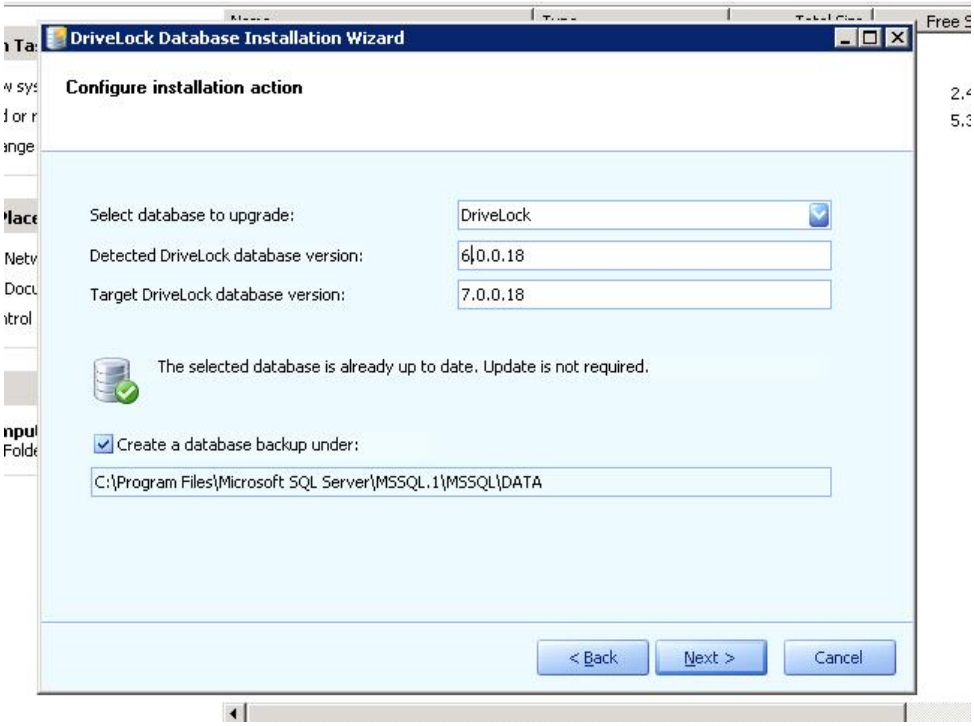
If you are using DES 6.0, first uninstall old DriveLock Enterprise Service and then install the new one. If you are using DES 6.1 you can perform an in-place upgrade over the old one. When performing an upgrade, ensure that you use the same service account.

Whether you are performing a new installation or are doing an in-place upgrade, the database installation wizard starts automatically after the DES installation has completed. Select the option to upgrade an existing database and then click **Next**.



The wizard automatically searches for existing databases. Select the existing DES 6.x database and then click **Next**.

 © 2015 CenterTools Software GmbH



Starting with DriveLock 7.1 the DriveLock Enterprise Service uses two databases. The second database holds all event data and linked entities. For example, it may store the user who connected a flash drive, information about the flash drive and other data. If your policy settings require anonymous storage of event data, certain fields are automatically encrypted. During an update existing data is automatically migrated. The migration process can take a long time, depending on the size of the existing data. Migration speed depends on your hardware, but a general guideline is to assume the processing of one million events per hour.

Also, starting with DriveLock 7.1, communications between the Management Console and the DriveLock Enterprise Service are always secured. Only encrypted communications using SSL are used and the DriveLock Enterprise Service always checks and enforces access permissions.

During an update of the DriveLock Enterprise Service the Database Installation Wizard prompts for a user of group that will initially be assigned permissions to configure the DriveLock Enterprise Service. This user or members of a group you specify can then assign [permissions to additional users and groups. If required user rights are missing, the wizard prompts you to select a user to assign the administrative role to.

After upgrading the DriveLock Enterprise Service you also need to change the DriveLock Management Console connection settings to connect to DES using port 6067 instead of port 6066. This change is automatically performed when you upgrade the DriveLock Management Console to version 7.1.

After upgrading the database, click **Finish** to close the wizard.

While the Database Installation Wizard displays a second, smaller progress bar under the main progress bar, the wizard is still migrating the data. Do not cancel the process until it has completely finished.

After the database migration has completed, the DriveLock Enterprise Service is restarted.

 © 2015 CenterTools Software GmbH

It is recommended to shrink the database after an update to free space that was used by the migration process. The method for shrinking depends on the database server you use:

Microsoft SQL:

- Microsoft SQL Server Management Studio: http://msdn.microsoft.com/en-us/library/ms189035.aspx
- TSQL: http://msdn.microsoft.com/de-de/library/ms190488.aspx

Oracle:

- http://lmgtfy.com/?q=oracle+shrink+datafile

After shrinking the database you should also update the database indexes by using one of the following database commands:

Microsoft SQL:

```
EXEC ctsp_maintenance
```

Oracle:

```
EXEC DRIVELOCK.CTSP_MAINTENANCE;
```

If you configured event grooming jobs to run on the database server, you will need to also create grooming jobs to run for the second database. The name of the second database is <database>-DATA) (where <database> is the name of the main database).

6.2 Updating the DriveLock Control Center

You can perform an in-place upgrade over the old version. You can find additional information about this process in the section "Installing DriveLock Management Components" of this manual.

6.3 Updating DriveLock Management Components

To update the DriveLock Management Console or the DriveLock Control Center, follow the instructions in the section Installing DriveLock Management Components. The installation process detects if an older version of these components is installed and will update them automatically.

For DriveLock 7.1 and 7.0: If you update the DriveLock Management Console make sure the DriveLock Agent on the same computer is already updated to the newest version.

6.4 Updating the Agent

In most cases you can perform an in-place upgrade of the DriveLock Agent and don't need to de-install the older version first. For more information about the Agent installation, refer to the section "Installing the DriveLock Agent" of this manual.

Before installing an updated Agent by using Group Policy, select the existing GPO that you used for the initial deployment and add the new installation file (*.MSI). After adding the installation file, on the Properties page of the software deployment policy, under "**Updates**" select the option "**Update existing packages**". Then click **Add** and select the installation file for the previous version. Ensure that the default option "**Uninstall the existing package, then install the new package**" is selected.

 © 2015 CenterTools Software GmbH

If you install the new Agent by using a configuration file, follow the instructions in the section "Installing the Agent by using Using Configuration Files" that matches the configuration method used. The installation process will detect if an older version of the Agent is installed and will update it automatically.

If you configured an uninstall password when you installed the previous version, you must provide this password for the update. Use the DriveLock Deployment Wizard to generate the encrypted version of this password. As an alternative, you can remove the uninstall password from your DriveLock configuration before updating the Agent.

You can upgrade the DriveLock Agent even if an older version of the Full Disk Encryption (FDE) is installed on a computer. Upgrading the Agent will not change the version of DriveLock FDE. Upgrading DriveLock FDE is not required when upgrading the Agent.

If you have used the DriveLock 6 or DriveLock 6.1 Agent installation package including DriveLock Full Disk Encryption („*DriveLockAgent_FDE.msi*" or „*DriveLockAgent_AMD64_FDE.msi*"), it is necessary to uninstall this software package before you proceed with the DriveLock 7 installation due to technical reasons.

6.4.1 Updating the DriveLock FDE Component

After the DriveLock Agent has been updated, an existing DriveLock FDE installation will be updated automatically and without re-encryption to the most current version. After updating the FDE components, a reboot may be required.

 © 2015 CenterTools Software GmbH

Part VII

Uninstalling the DriveLock Agent

7 Uninstalling the DriveLock Agent

Unless you assigned the DriveLock Agent by using Group Policy, you can remove a DriveLock Agent from a computer by using the Add/Remove Programs application in Control Panel.

DriveLock Agents can also be uninstalled using the following command line, specifying the original installation package (.msi):

```
msiexec /x DriveLockagent.msi
```

If you have configured DriveLock to require a password for uninstalling, you must use one the following commands:

```
msiexec /x DriveLockagent.msi UNINSTPWD=password
msiexec /x DriveLockagent.msi UNINSTPWDENC=encrypted-password
```

To create the encrypted password, use the DriveLock Deployment Wizard.

If you installed the DriveLock Agent by using Group Policy, you can't use the *Add/Remove Programs* application to uninstall DriveLock. Instead, remove DriveLock from the GPO to un-assign DriveLock from the computer. Alternatively, you can use the command line to uninstall DriveLock, but you have to ensure that there is no remaining GPO that assigns DriveLock to the computer.

 © 2015 CenterTools Software GmbH

Part VIII

Migrating a Legacy Database

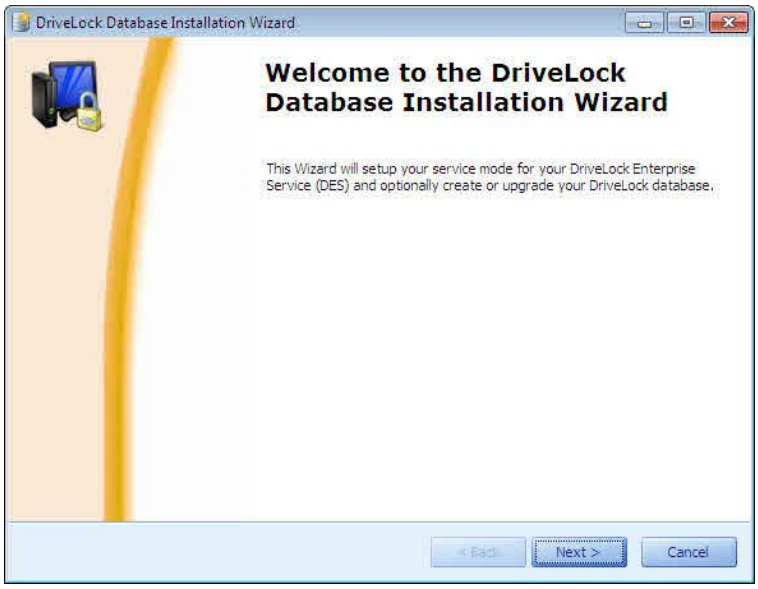
DON'T GAMBLE WITH YOUR DATA

8 Migrating a Legacy Database

Starting with DriveLock 6, the Security Reporting Center components have been replaced by the DriveLock Enterprise Server and the DriveLock Control Center. It is not possible to update an existing database and the Security Reporting Center. Instead, you need to migrate the contents of the existing DriveLock 5.5 R2 database into the new DriveLock 6 database. You need to perform this process using the Database Migration Wizard after you have installed the DriveLock Enterprise Service and the new database. (For details about the DES installation, refer to the chapter "Installing the DriveLock Enterprise Service".)

If the existing version of the SRC server is older than DriveLock 5.5 R2, you must upgrade your existing SRC Server to version 5.5 R2 before you can migrate data by using the Database Migration Wizard.

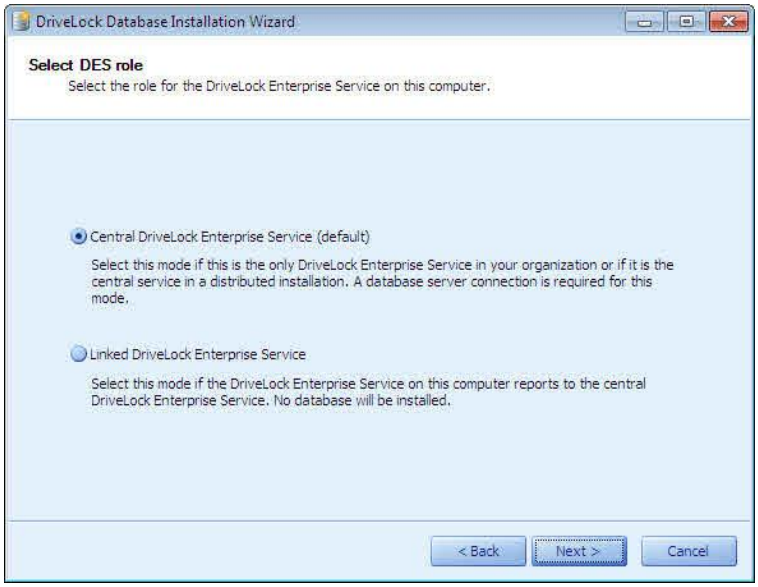
The Database Migration Wizard is installed together with the DriveLock Enterprise Service. To start the program, click "**Start → Programs → CenterTools DriveLock → DriveLock DES Database Installation**".



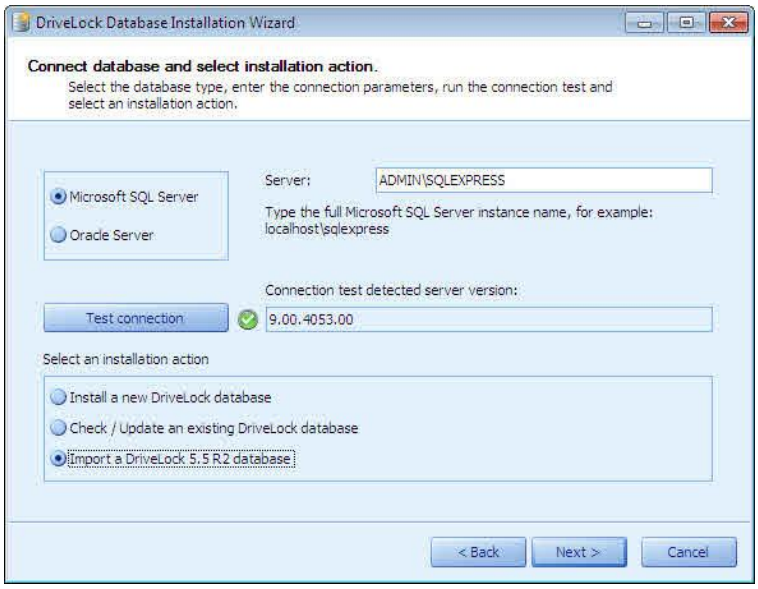
Ensure that you have created a backup of both databases before you continue.

Click **Next**.

 © 2015 CenterTools Software GmbH



Select the server role *Central DriveLock Enterprise Service* because the migration requires a direct connection to the database server.



Select the database server type, Microsoft SQL Server or Oracle. Type the name of the database server and, if required, the name of the database instance. To confirm that DES can connect to the server, click **Test Connection**. Select "Import a *DriveLock 5.5 R2 database*" as the installation action and then click **Next**.

The target database is automatically selected from the current DES settings. Type the server name and the database name of the source database and then click **Check connection**. Both connections must be successfully validated before you can proceed.

Click **Next**.

Select the data types to be imported into the new database:

- *Accounts and permissions*: Existing accounts and general permissions
- *Device Scanner data*: Information about computers, drives and devices that was created by the Device Scanner

 © 2015 CenterTools Software GmbH

- Events: All event information
- *SRC File Cache path*: The folder used for the Security Reporting Center file cache. By default this is "*C:\Program Files\CenterTools\DriveLock Security Reporting Center\SRCFileCache*".
- *Container recovery data*: Data that is required to reset passwords of encrypted removable media or encrypted containers
- *Full Disk Encryption recovery data*: Data that is required to recover encrypted disks or to assist users who forgot a pre-boot authentication password

Access permissions on reports will not be imported from the DriveLock 5.5 R2 database. You need to configure these permissions manually after the import has completed.

Click **Next** twice to view a summary of the installation steps to be performed.

Review the summary of the migration settings and the click **OK** to start the migration.

If the import was successful, a green icon is displayed. In case of an error, review the file *C:\Documents and Settings\All Users\Application Data\CenterTools DriveLock\Log\DatabaseInstallWizard.log* or *C:\ProgramData\CenterTools DriveLock\Log\DatabaseInstallWizard.log* to identify the reasons for the failure.

Click **Finish** to close the Database Import Wizard.

 © 2015 CenterTools Software GmbH

DriveLock Installation Guide

Die in diesen Unterlagen enthaltenen Angaben und Daten, einschließlich URLs und anderen Verweisen auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, Organisationen, Produkte, Personen und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Personen oder Ereignissen ist rein zufällig. Die Verantwortung für die Beachtung aller geltenden Urheberrechte liegt allein beim Benutzer.
Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der CenterTools Software GmbH kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht.
Es ist möglich, dass CenterTools Software GmbH Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von CenterTools Software GmbH eingeräumt.
Weitere in diesem Dokument aufgeführte tatsächliche Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

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.
CenterTools and DriveLock and others are either registered trademarks or trademarks of CenterTools GmbH 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.

© 2015 CenterTools Software GmbH