DriveLock Installationshandbuch 2020.2

14.01.2021

Inhaltsverzeichnis

Teil I

Konventionen

1 Konventionen

In diesem Dokument werden durchgängig folgende Konventionen und Symbole verwendet, um wichtige Aspekte hervorzuheben oder Objekte zu visualisieren.

Achtung: Roter Text weist auf Risiken hin, die beispielsweise zu Datenverlust führen können

Hinweise und Tipps enthalten nützliche Zusatzinformationen.

Menüeinträge oder die Namen von **Schaltflächen** sind fett dargestellt. *Kursive Schrift* repräsentiert Felder, Menüpunkte und Querverweise.

`Systemschrift` stellt Nachrichten oder Befehle auf Basis der Kommandozeile dar.

Ein Pluszeichen zwischen zwei Tasten bedeutet, dass diese gleichzeitig gedrückt werden müssen; „ALT + R“ beispielsweise signalisiert das Halten der ALT-Taste, während R gedrückt wird. Ein Komma zwischen mehreren Tasten fordert ein Nacheinander drücken der jeweiligen Tasten. „ALT, R, U” bedeutet, dass zunächst die ALT-Taste, dann die R- und zuletzt die U-Taste betätigt werden muss.

Teil II

Datensicherheit mit DriveLock

2 Datensicherheit mit DriveLock

DriveLock ist eine Softwarelösung zur Absicherung von Clientrechnern. Es besitzt eine multilinguale Benutzeroberfläche, deren Sprache während der Installation oder Ausführung ausgewählt werden kann und bietet dynamisch konfigurierbaren Zugriff für Laufwerke (Disketten, CD-ROMs, USB-Sticks etc.) und kontrolliert die meisten anderen Gerätetypen wie z.B. Bluetooth, Palm, Windows Mobile, BlackBerry, Smartphones. Durch Konfiguration von Whitelist-Regeln (basierend auf Gerätetyp und Hardware ID) kann exakt spezifiziert werden, wer welches Gerät zu welcher Zeit nutzen kann. Mobile Laufwerke können anhand der Hersteller-, Produkt- & Seriennummer kontrolliert werden, was exakte Definierung und Durchsetzung von Zugriffsrichtlinien erlaubt. Weitere Merkmale ermöglichen das Entsperren bestimmter autorisierter Medien sowie das Setzen von Zeitlimits und Computern für Whitelist-Regeln. Auch die temporäre Deaktivierung der Kontrolle durch DriveLock ist möglich, selbst wenn der Rechner offline und nicht mit einem Netzwerk verbunden ist.

Die Installation der Clientsoftware (DriveLock Agent) und die Verteilung der Regeln kann einfach durch Nutzung vorhandener Softwareverteilungsmechanismen geschehen oder unter Zuhilfenahme der Gruppenrichtlinien des Active Directory. Alternativ können Richtlinien auch durch Konfigurationsdateien für Einzelrechner oder Umgebungen ohne Active Directory verteilt werden.

Die Überwachungsmöglichkeiten von DriveLock in Zusammenspiel mit der Schattenkopie-Funktionalität liefern den erforderlichen Grad an Kontrolle und Informationen, um die Einhaltung bestehender Richtlinien durchzusetzen. Durch Einsatz des DriveLock Device Scanners kann jedes Laufwerk oder Gerät im Netzwerk aufgespürt werden, auch wenn dies nicht mehr mit dem entsprechenden Rechner verbunden ist. Die Nutzung des DriveLock Device Scanner ist nicht an das Vorhandensein des DriveLock Agenten gebunden.

Verschlüsselung ist ein weiteres Hauptmerkmal von DriveLock. Dabei kann die Verschlüsselung erzwungen werden, wenn z.B. Daten auf mobile Laufwerke kopiert werden oder durch Verschlüsselung des kompletten Laufwerkes, um sensible Daten zu schützen. Des Weiteren kann DriveLock auch kritische Daten auf sichere Weise löschen, durch mehrmaliges Überschreiben von Daten unter Nutzung anerkannter Industriestandards.

Der DriveLock Applikationskontrolle ermöglicht eine einfache Kontrolle über alle Anwendungen, die von einem Benutzer gestartet werden könnten. Sie können das Starten von Applikationen anhand von verschiedenen Kriterien, wie z.B. Benutzer oder Gruppen, aktuelle Netzwerkumgebungen oder dem aktuellem Computer, erlauben oder verweigern.

Der DriveLock Enterprise Service (DES) ist die zentrale Datenbank und Berichtskonsole von DriveLock. Der DES sammelt alle DriveLock-Ereignisse und Resultate des Device Scanners in einer Datenbank. Administratoren können diese Daten für die dynamische Generierung von Überwachungs- und Managementberichten nutzen.

Alle DriveLock Module können mit nur einer Konsole verwaltet und konfiguriert werden, was besonders komfortabel für den Administrator ist.

2.1 Die Komponenten von DriveLock

Dieses Kapitel beschreibt die verschiedenen DriveLock-Komponenten.

2.1.1 Der Agent

Der DriveLock Agent ist die wichtigste Komponente der DriveLock-Infrastruktur. Er schützt den Rechner und muss auf jedem Client installiert werden, auf welchem Wechseldatenträger, Geräte oder andere Einstellungen kontrolliert werden sollen. Der Agent ist ein Windows Dienst, der im Hintergrund läuft, die Schnittstellen kontrolliert und die Sicherheitsrichtlinien umsetzt. Um nicht autorisierten Zugriff und die Umgehung der Sicherheitseinstellungen zu verhindern, kann der Dienst nicht durch einen normalen Benutzer gestoppt werden; nur entsprechend berechtigte Benutzer können auf die Eigenschaften dieses Dienstes zugreifen.

2.1.2 Die DriveLock Management Konsole

Die DriveLock Management Konsole dient zur Konfiguration der Sicherheitseinstellungen für alle Rechner und für das Management aller DriveLock-Komponenten. Sie ist als Microsoft Management Konsole (MMC) Snap-in implementiert und so auf einfache Weise in eventuell bereits bestehende MMC Konsolen integrierbar.

Ferner ermöglicht die DriveLock Management Konsole die lokale Konfiguration des Rechners, auf dem sie ausgeführt wird; weiterhin können Gruppenrichtlinien-Einstellungen des Active Directory bearbeitet werden oder Einstellungen in eine Konfigurationsdatei gespeichert werden zum späteren Import auf anderen Rechnern. Weitere Merkmale umfassen die Überwachung des Client-Status sowie der direkte Zugriff auf den DriveLock-Agenten. Mit Hilfe der Management Konsole kann über das Netzwerk die Sperrung von Geräten aufgehoben werden; falls der Rechner gerade nicht mit dem Netzwerk verbunden ist, kann durch Generierung eines Offline-Zugangscodes (den der Benutzer dann auf dem Client eingeben muss) ebenfalls eine vorhandene Sperrung deaktiviert werden. Der DriveLock Device Scanner und der DriveLock Enterprise Server (falls installiert) sind auch in der DriveLock Management Konsole integriert.

2.1.3 Das DriveLock Control Center

Das DriveLock Control Center (DCC) und der DriveLock Enterprise Service (DES) ermöglichen die Sammlung von DriveLock Ereignissen auf einem zentralen Server und die Generierung dynamischer Berichte und forensischer Analysen auf Basis der gesammelten Daten. Dies erlaubt eine Überwachung von Wechseldatenträgern, Geräten und Datentransfers in unterschiedlicher Detailtiefe. Eine zusätzliche Option erweitert diese Funktionalität durch individuelle Berechtigungen für Datenabfragen und Berichtsgenerierung.

Berichte beinhalten typischerweise die Nutzung von Wechseldatenträgern und Verbindungsversuche von Geräten (sowohl erlaubte als auch gesperrte). Zusätzlich können Abfragen darüber erstellt werden, welche Dateien auf Wechseldatenträgern geschrieben oder gelesen wurden – gemäß den Einstellungen der DriveLock Richtlinie, welche Details aufgezeichnet werden sollen. All diese Funktionen und die Möglichkeit zur Generierung grafischer Statistiken machen das DCC zu einem mächtigen Werkzeug für die Überwachung, Berichte und die Ausführung forensischer Analysen mithilfe der Drill down Funktionalitäten des DCC's.

Sie können Ihre Agenten auch innerhalb des DriveLock Control Center's überwachen. Sie bekommen sehr schnell einen Systemüberblick über den aktuellen Status (z.B. ob DriveLock auf lizenzierten Systemen installiert ist) und der Verbindung (z.B. wann sich der Agent zuletzt mit dem zentralen DES verbunden hat), mithilfe leicht zu benutzender Filter- und Gruppierungsfunktionen.

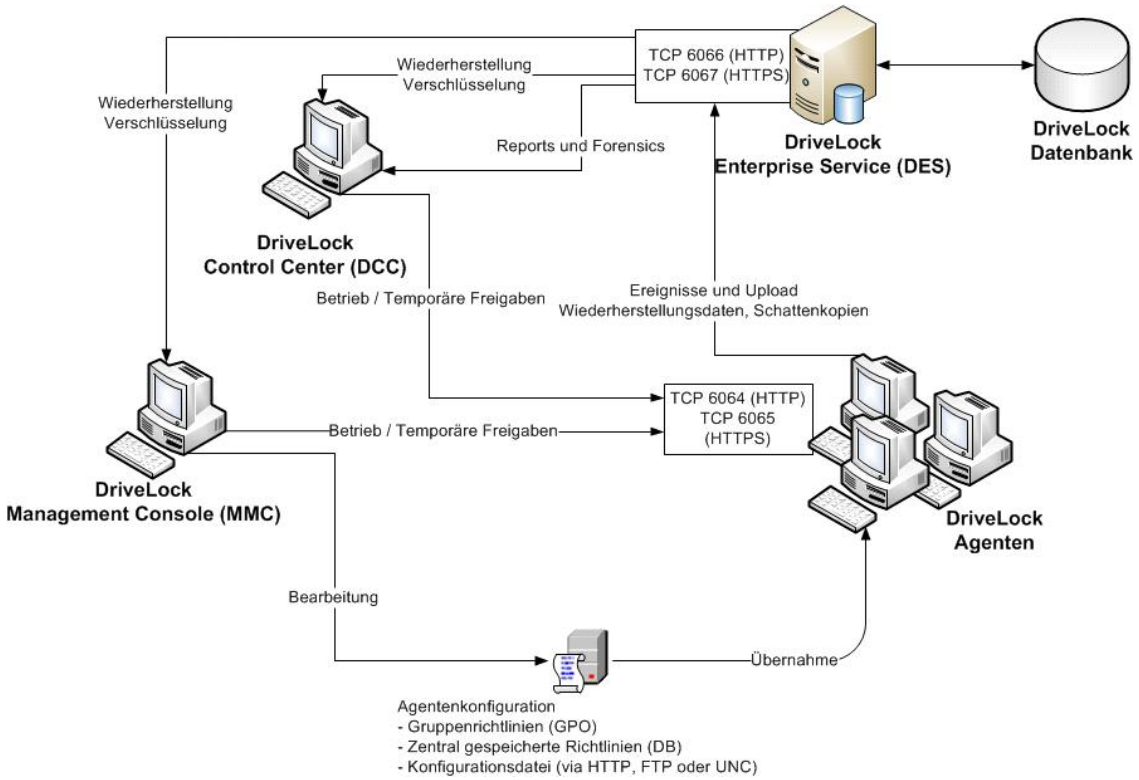
2.1.4 DriveLock Enterprise Service

Der DriveLock Enterprise Service (DES) ist für die zentrale Speicherung der Ereignisse aller DriveLock-Agenten zuständig. Dieser Dienst ermöglicht eine perfekt abgestimmte und komfortable Überwachung des Systemstatus und dient ab Version 7 als zentrale Schaltstelle für die Verteilung der DriveLock Komponenten und zentral gespeicherter Richtlinien. Über das DriveLock Control Center (DCC), der Reporting-Konsole, erfolgt der Zugriff auf die im DES gespeicherten Ereignisse.

Sofern eine oder beide Verschlüsselungsmodule (Encryption-2Go oder Full Disk Encryption) verwendet werden, können Wiederherstellungsdaten ebenfalls zum DES hochgeladen werden, damit die Wiederherstellung noch einfacher und sicherer wird.

2.2 Gesamtstruktur

Die folgende Abbildung zeigt die Kommunikationswege und die Rolle des DriveLock Enterprise Service in der DriveLock Gesamtstruktur:



Standardports für die Kommunikation (Diese Ports können bei Bedarf angepasst werden).

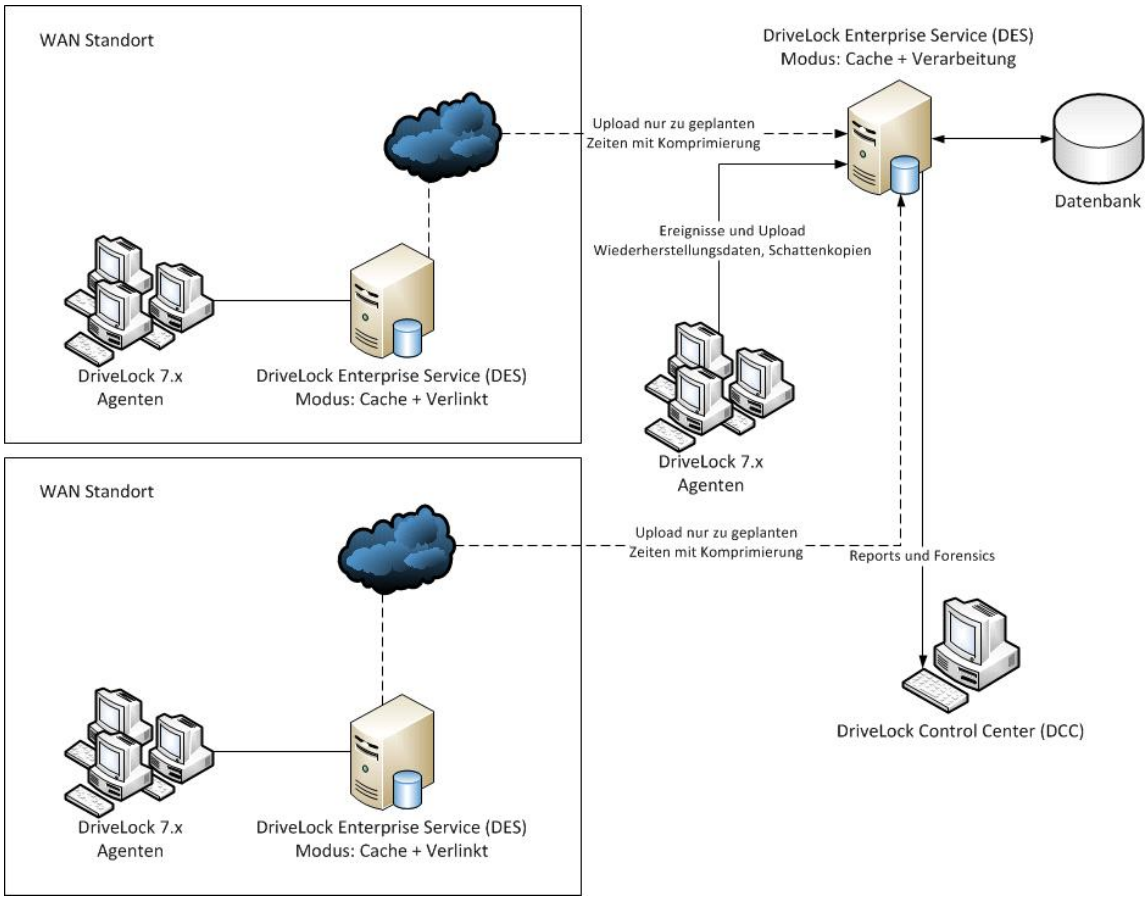
Port	Richtung	Protokoll	Verwendung
6064 TCP	Eingehend	HTTP	DriveLock Agent
6065 TCP	Eingehend	HTTPS	DriveLock Agent
6066 TCP	Eingehend	HTTP	DES
6067 TCP	Eingehend	HTTPS	DES
135 TCP	Ausgehend	RPC	(optional) MMC (Bearbeiten einer GPO)
80 TCP	Eingehend	HTTP	(optional) Server mit Konfigurationsdatei über HTTP
21 TCP	Eingehend	FTP	(optional) Server mit Konfigurationsdatei über FTP
445 TCP; 139 TCP, 137 UDP, 138 UDP	Eingehend	SMB; NetBios	(optional) Server mit Konfigurationsdatei über UNC

DriveLock Cloud Services

Zusätzlich benötigen DES und MMC Zugriff auf die DriveLock Cloud Services auf https://cloudapp.drivelock.com um Lizenzen zu aktivieren, Software-Pakete und AV-Pattern nachzufragen und Clout-Accounts und -Ereignisse zu verwalten.
Zum Laden der Software-Pakete und AV-Pattern verbindet sich der DES zu https://drivelock.blob.core.windows.net .

2.2.1 Verlinkte DriveLock Enterprise Service

Damit Ressourcen und WAN-Bandbreiten geschont werden, kann man in einer größeren Umgebung mehrere DriveLock Enterprise Services verlinken, d.h. ein DriveLock Enterprise Service der im Modus „Cache + Verlinkt“ arbeitet (Außenstelle, verlinkter DES), sammelt Ereignisse genauso wie ein standardmäßiger DriveLock Enterprise Service im Modus „Cache + Verarbeitung“ (Zentrale, zentrales DES), der direkt mit der Datenbank verbunden ist. Der außenstehende DriveLock Enterprise Service überträgt die gesammelten Ereignisse laut einem Zeitplan komprimiert an die Zentrale:



Der Modus eines DriveLock Enterprise Service kann mit dem „Datenbank Installationsassistenten“, welcher standardmäßig beim DriveLock Enterprise Service mit installiert wird, geändert werden. Alle DriveLock Komponenten stehen als separate MSI-Installationspakete sowohl in einer 32-Bit als auch in einer 64-Bit Version zur Verfügung. Zusätzlich gibt es noch ein eigenes Installationspaket für die DriveLock Dokumentation.

Teil III

Vorbereitung der Installation

3 Vorbereitung der Installation

Zur Verteilung der DriveLock Agenten auf den Arbeitsplätzen – nachdem zentrale Einstellungen konfiguriert wurden – kann das Agenten MSI-Installationspaket verwendet werden (siehe auch Abschnitt „*Installation des DriveLock Agenten*“).

Um die Installation komfortabler zu gestalten, steht Ihnen ein DriveLock Installer (*DLSetup.exe*) zur Verfügung. Dieser ist in der Lage zu prüfen, ob neue Versionen der Installationspakete zur Verfügung stehen und diese auf Wunsch vor der Installation aus dem Internet zu laden. Der DriveLock Installer läuft sowohl in 32-Bit als auch in 64-Bit Umgebungen.

Unter www.drivelock.de können Sie auch ein ISO-Image herunterladen und auf eine CD/DVD brennen. Dieses Image beinhaltet den DriveLock Installer, alle Installationspakete für alle Betriebssysteme, die komplette DriveLock Dokumentation als PDF-Dokumente und zusätzliches Informationsmaterial.

Es gibt verschiedene Arten, Konfigurationseinstellungen an Clients zu verteilen. Die folgende Konfigurationsmatrix hilft Ihnen einen Überblick zu bekommen, welche Konfigurationsart für Sie am ehesten in Frage kommt:

	Zentrale Konfiguration	Benötigt zwingend einen DES	Nutzt vorhandene Infrastruktur	Historie / Versionierung	Skalierbarkeit	Schnell-konfiguration
Lokale Konfiguration	Nein	Nein	Nein	Nein	-	Nein
Gruppenrichtlinie	Ja	Nein	Ja (AD)	Nein	Sehr gut	Nein
Zentral gespeicherte Richtlinie	Ja	Ja	Nein	Ja	Gut	Ja
Konfigurations-Datei	Ja	Nein	Ja (UNC, HTTP, FTP)	Nein	Befriedigend	Nein

Es wird empfohlen, sich zunächst mit einer lokalen Konfiguration vertraut zu machen, bevor Einstellungen an mehrere Clients im Netzwerk verteilt werden.

- Lokale Konfiguration: Bei der Lokalen Konfiguration wird nur der lokale Agent (d.h. der Agent, der auf dem gleichen Computer wie die gerade verwendete DriveLock Management Console installiert wurde) konfiguriert. Diese Konfigurationsart eigenet sich ausschließlich für Test- bzw. Evaluationsumgebungen und bietet den Vorteil, dass Konfigurationsänderungen sofort auf dem Einzelplatzsystem wirksam sind.
- Konfiguration über Gruppenrichtlinien: Hier wird die DriveLock Konfiguration innerhalb einer Active Directory Gruppenrichtlinie gespeichert und über das im Active Directory enthaltene Gruppenrichtlinienmanagement an die Client Computer verteilt.
- Zentral gespeicherte Richtlinie: Die DriveLock Konfiguration wird mit Hilfe des DriveLock Enterprise Service in der zentralen Datenbank abgelegt. Die DriveLock Agenten greifen über den DriveLock Enterprise Service auf diese zu. Zentral gespeicherte Richtlinien bieten den Vorteil einer Versionsverwaltung mit History- und Rollback-Funktion über die DriveLock Management Console und die Möglichkeit der Schnellkonfiguration.
- Verwendung von Konfigurationsdateien: Hier wird die DriveLock Konfiguration innerhalb einer Datei gespeichert, welche an zentraler Stelle in Ihrer Systemumgebung abgelegt wird. Der Zugriff der DriveLock Agenten auf diese Datei erfolgt entweder über ein freigegebenes Verzeichnis (Share), über FTP oder über HTTP

(wenn die Datei auf einem Webserver abgelegt wurde). Mit Hilfe eines Webservers kann so eine DriveLock Konfiguration durchaus auch über das Internet (ohne direkte Verbindung ins Unternehmensnetzwerk) verteilt werden.

Eine typische DriveLock Installation erfolgt in vier Schritten:

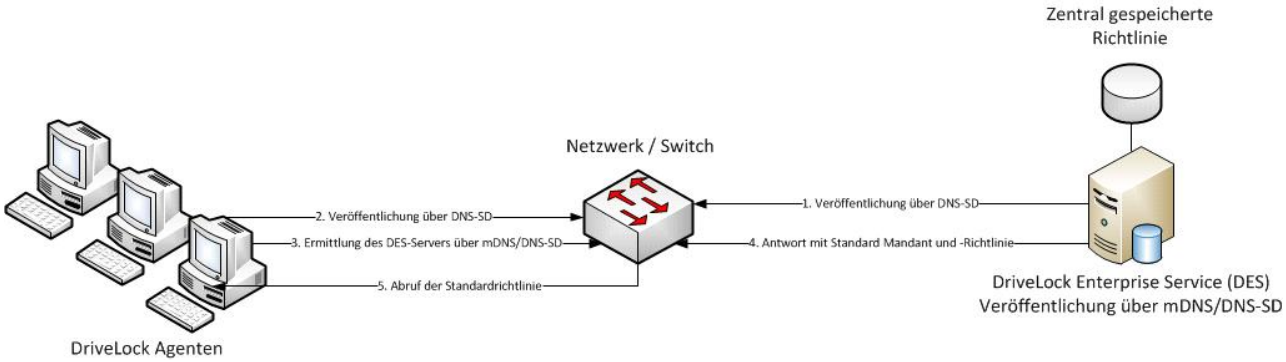
1. Installation des DriveLock Enterprise Service auf einem zentralen Server (benötigt eine Datenbank)
2. Installation der Management Komponenten auf einem oder mehreren Administrationsarbeitsplätzen
3. Erstellen einer ersten DriveLock Konfiguration (z.B. ohne Sperrung von Laufwerken, Geräten und Applikationen)
4. Installation der DriveLock Agenten auf den Arbeitsplätzen abhängig von der gewählten Konfigurationsart

In diesem Dokument sind diese vier Schritte ausführlich dokumentiert. Zusätzliche Abschnitte behandeln die manuelle Aktualisierung von DriveLock, die Deinstallation und die Migration von einer älteren DriveLock Version (V5.5 R2 oder älter).

3.1 Schnellkonfiguration mit mDNS/DNS-SD

Eine besonders einfache und schnelle Variante DriveLock zu konfigurieren, ist über die automatische Dienstveröffentlichung über mDNS und DNS-SD. Dabei werden Client- und Serverdienste über Multicast im Netzwerk registriert. Sobald ein DriveLock Agent startet, kann dieser nun dynamisch seinen DriveLock Enterprise Service ermitteln und eine vom Administrator bereitgestellte Konfiguration abrufen. Der Konfigurationsaufwand ist minimal. Die Installation eines DriveLock Enterprise Services wird vorausgesetzt und ist zwingend notwendig.

Die Ermittlung des DES-Servers und einer Konfiguration erfolgt wie auf folgendem Schema abgebildet:



1. DES – Veröffentlichung über DNS-SD
2. Agent – Veröffentlichung über DNS-SD
3. Agent – Ermittlung des DES-Servers über mDNS/DNS-SD
4. DES – Antwort mit Standard-Mandant und –Richtlinie
5. Agent – Abruf der Standardrichtlinie

In gerouteten Netzwerken kann es vorkommen, dass Multicast-Verkehr nicht geroutet wird. Damit ist die Verwendung über mDNS/DNS-SD leider nicht möglich. Alternativ kann natürlich ein fester Server und eine feste Konfiguration vorgegeben werden.

Weitere Informationen zur Erstellung von zentral gespeicherten Richtlinien und das Zuweisen zur Standardrichtlinie erhalten Sie im Administrationshandbuch.

3.1.1 Deaktivieren von mDNS/DNS-SD

Um mDNS/DNS-SD zu deaktivieren und allen Multicast-Verkehr zu unterbinden, gibt es zwei Optionen in der DriveLock Management Konsole. Damit wird die Schnellkonfiguration deaktiviert, der Netzwerkverkehr nicht zusätzlich belastet, gerade in größeren Netzwerken kann dies wünschenswert sein:

- In der Konfiguration der Agenten, z.B. GPO: *Erweiterte Konfiguration – Globale Einstellungen – Einstellungen – Agentenfernkontroll-Einstellung und –Berechtigungen* – Haken bei *Automatische Agenten-Ermittlung (über DNS-SD) erlauben* entfernen.
- *DriveLock Enterprise Services – Server - <pro DES-Server> - Optionen* – Haken bei *Automatische Server-Ermittlung (mit DNS-SD) abschalten* setzen.

Teil IV

Systemanforderungen

4 Systemanforderungen

DriveLock arbeitet im Hintergrund und erfordert daher nur minimale Hardwareressourcen. Der DriveLock Agent selbst läuft unter normalen Windows Betriebssystemen und erfordert keinerlei zusätzliche Infrastruktur. Für den DriveLock Enterprise Service wird eine Datenbank (Microsoft SQL Server) benötigt.

DriveLock empfiehlt die Installation des jeweils aktuellsten Service Packs und aller Hotfixes, die gerade für das jeweils genutzte Betriebssystem erhältlich sind.

Detaillierte Information zu den unterstützen Plattformen und Hardwareanforderungen finden Sie in den DriveLock Releasenotes.

Ausnahmen für Antivirus Software

Standardmäßig sollten Sie diese Ausnahmen innerhalb jedes eingesetzten Antiviren-Programms definieren, welches auf Systemen installiert ist, auf denen der DriveLock Agent oder der DES läuft.

Beachten Sie bitte auch, die notwendigen Einstellungen des DES Datenbank-Systems vorzunehmen. Die Einstelllungen für MS-SQL-Server können Sie hier finden: How to choose antivirus software to run on computers that are running SQL Server

Dateien & Verzeichnisse:

"C:\SECURDSK"	(EFS)
"C:\Program Files\CenterTools\DriveLock"	(Application Directory)
"C:\ProgramData\CenterTools DriveLock"	(Cache/Working Directory)

Prozesse/Dienste:

Service Name:	**DriveLock**
Service Display Name:	DriveLock
Ausführbarer Pfad:	"C:\Program Files\CenterTools\DriveLock\DriveLock.exe"

Service Name:	**dlhm**
Service Display Name:	DriveLock Health Monitor
Ausführbarer Pfad:	"C:\Program Files\CenterTools\DriveLock\DLHM.exe"

Service Name:	**StorageEncryptionService**
Service Display Name:	DriveLock Full Disk Encryption Encryptor
Ausführbarer Pfad:	"C:\Program Files\CenterTools\DriveLock\DlFdeEncSvc.exe"

Service Name:	**ClientDataManager**
Service Display Name:	DriveLock Full Disk Encryption Manager
Ausführbarer Pfad:	"C:\Program Files\CenterTools\DriveLock\DlFdeMgr.exe"

Service Name:	**dlupdate**
Service Display Name:	DriveLock Update and Installation

Ausführbarer Pfad: "C:\Windows\DLUpdSvc.exe"

Service Name: **dessvc**
Service Display Name: DriveLock Enterprise Service
Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DES.exe"

Program Name: **DESTray**
Function of the program: Displayed in the DES Symbol in the Windows Tray
Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DESTray.exe"

Program Name: **DesRestarter**
Function of the program: Restart the DES service
Ausführbarer Pfad: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DesRestarter.exe"

Disk Encryption

Unterstützte Speicher Hardware

DriveLock Disk Encryption (FDE) kann alle eingebauten (nicht externe) System Partitionen/Festplatten mit einem zugewiesenen Laufwerksbuchstaben (es werden keine versteckten Partition unterstützt) ver-/entschlüsseln, inklusive aller IDE/EIDE, SATA, SCSI Laufwerken. Software-RAID-Arrays werden nicht unterstützt.

Windows muss auf der Boot-Platte (enthält MBR) installiert sein.

DriveLock FDE behindert in keinem Fall die normalen Operationen des Speicher Sub-Systems, mit folgenden Ausnahmen:

- Es ist nicht möglich, irgendeine Partition auf der Systemfestplatte zu formatieren.
- DriveLock FDE unterstützt keine nachträglichen Änderungen, wie das Hinzufügen, Entfernen oder Austauschen von Festplatten.
- Während der Installation prüft DriveLock FDE alle vorhandenen Partitionen im System. Änderungen nach der Installation wie Größenänderungen, Umwandlungen, Aktiv/Passiv setzen oder neu Partitionierungen werden nicht unterstützt. Das betrifft auch Manipulationen am Master Boot Record (MBR).

DriveLock FDE unterstützt die Verwendung von FAT16, FAT32 und NTFS Dateisystemen.

DriveLock FDE unterstützt keine Geräte, die eMMC Flash Memory als Boot-Platte verwenden, wie z.B Microsoft Surface Go.

DriveLock FDE unterstützt keine Multi-Boot Systeme.

MS-DOS kann für die DriveLock FDE Notfall-Wiederherstellung verwendet werden. Defekte DriveLock FDE Systeme können von einer Diskette oder CD nach MS-DOS gestartet werden. Laufwerke die spezielle DOS Treiber voraussetzen (z.B. SCSI) oder TSRs sind für die DriveLock FDE Wiederherstellungs-Tools nur verwendbar, wenn vorher die entsprechenden Treiber geladen wurden.

Unterstützte Netzwerke

DriveLock FDE ist Active-Directory fähig und unterstützt in vollem Umfang Windows Domänen. Es beeinflusst nicht die normalen Aufgaben irgendwelcher Windows Netzwerkdienste, inklusive Remotedesktop-Verbindungen. Windows Domänen-Benutzer, sowie lokale Windows-Benutzer sind in der Lage sich erfolgreich an einem System zu authentifizieren, das von DriveLock FDE geschützt ist. Alle Festplattenpartitionen, die mit DriveLock FDE verschlüsselt sind, können auch als freigegebene Datenträger konfiguriert werden, je nach Ermessen des Systemadministrators.

Software Kompatibilität

DriveLock FDE beeinflusst nicht die normalen Funktionen der meisten Microsoft Windows-konformen Software, Applikationen, Diensten und Werkzeugen. Dennoch sollte man mit Bedacht folgende Programme benutzen:

- *DOS Treiber und TSRs*: Wenn von einer DOS-Diskette (oder CD) gestartet wird, sieht DriveLock FDE Festplatten nur, wenn die entsprechenden DOS Treiber und TSRs geladen wurden.
- *Windows und Dritt-Hersteller Boot Manager*: Beim Systemstart passt DriveLock FDE den Master Boot Record (MBR) an, während die Integrität dessen überprüft wird. Jede Software, die den MBR für seine eigenen Zwecke anpasst, ist inkompatibel zu DriveLock FDE. Das betrifft auch den Standard Windows-Bootmanager.
- *Windows Datenträgerverwaltung*: Alle Partitionierungen, Größenänderungen und Spiegelungskonfigurations-Änderungen, die nach der Installation von DriveLock FDE durchgeführt werden, werden von DriveLock FDE geblockt. Wenn eine der oberen Aktionen notwendig ist, entschlüsseln Sie vorher alle Festplatten und deinstallieren DriveLock FDE, bevor Sie fortfahren.
- *Windows Ordnerkomprimierung*: Die Windows Ordnerkomprimierung wird vollständig unterstützt, mit einer Ausnahme: Das Systemverzeichnis (C:\Securdsk) darf nicht komprimiert werden.

DriveLock FDE darf nicht auf einem komprimierten Systemlaufwerk installiert werden. Das Ergebnis der Komprimierung des Verzeichnisses C:\Securdsk hat Auswirkungen auf den normalen Betrieb.

> Das Verzeichnis *C:\Securdsk* ist ein verstecktes Systemverzeichnis und somit für den normalen Benutzer nicht sichtbar.

- *Windows Systemwiederherstellung*: Windows Systemwiederherstellungspunkte, die vor der Installation vor DriveLock FDE erstellt wurden, sind nicht verwendbar. Das System kann nur von einem Wiederherstellungspunkt hergestellt werden, der nach der Installation von DriveLock FDE erstellt wurde.
- *Schnelle Benutzerumschaltung von Windows*: DriveLock FDE deaktiviert die Standard Windows-Anmeldung, zusammen mit seiner Funktion für die schnelle Benutzerumschaltung.

Teil V

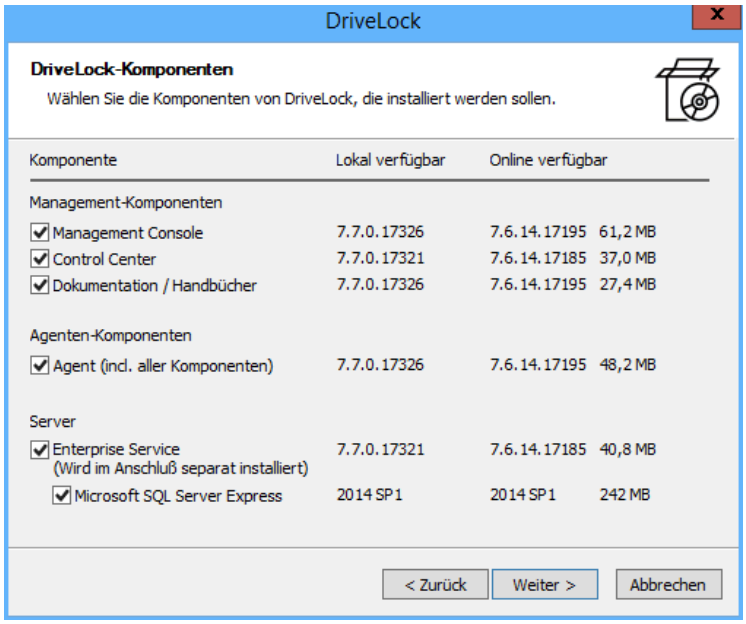
DriveLock installieren

5 DriveLock installieren

5.1 Testinstallation (Evaluierung)

Bei einer Testinstallation werden alle DriveLock Komponenten auf einem lokalen Rechner installiert (ab Windows 7). Zum Test von DriveLock ist dies die empfohlene Installationsart. Als Datenbank empfiehlt sich die Installation von Microsoft SQL Express, die vor der DriveLock Installation erfolgen muss.

Die Installation erfolgt ebenfalls über den DriveLock Installer (**DLSetup.exe**) welcher zunächst die aktuellsten verfügbaren Komponenten (MSI-Pakete) über das Internet lädt und anschließende alle DriveLock Komponenten auf dem Zielsystem installiert. Für eine Evaluierung auf einen Testrechner wählen Sie dort einfach alle Komponenten gleichzeitig aus:



Die Verwendung des DriveLock-Installers wird in Abschnitt *„Installation der DriveLock Management-Komponenten“* beschrieben. Informationen zur Installation des DriveLock Enterprise Service finden Sie im Abschnitt *„Installation des DriveLock Enterprise Service“*.

5.2 Installation des DriveLock Enterprise Service

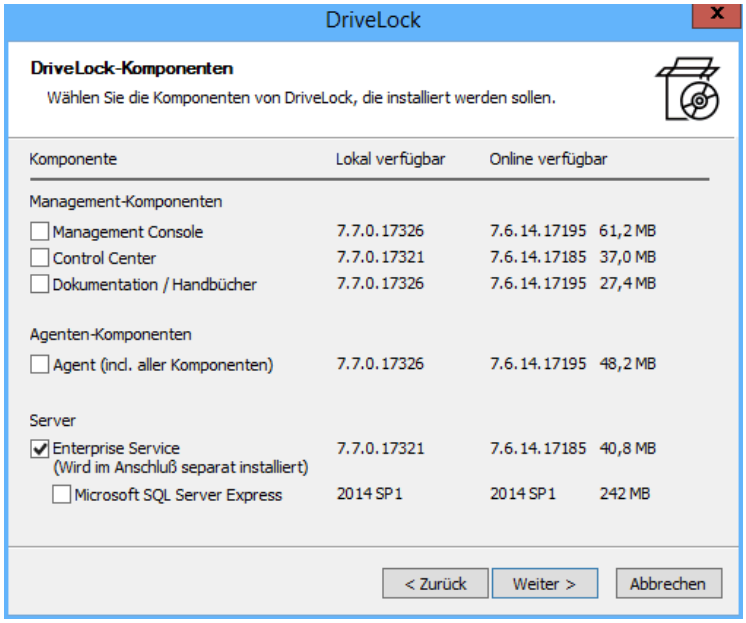
Der DriveLock Enterprise Service (DES) ist die Komponente der DriveLock Produktfamilie, die auf einem zentralen Server installiert wird und einen Datenbankserver für die Erstellung der beiden DriveLock-Datenbanken benötigt.

Wenn Sie eine Microsoft SQL Server Datenbank verwenden, legen Sie vor der Installation des DES den Service Account an, mit dem der DES auf die Datenbank zugreifen soll. Wenn der DES Server nicht auch der Datenbank Server

Auch der DriveLock Enterprise Service kann über den DriveLock Installer installiert werden. Der DriveLock Installer überprüft dabei, ob eine aktuellere DriveLock Enterprise Service Version veröffentlicht wurde und lädt ggf. das Paket über das Internet nach.

Starten Sie den DriveLock Installer (**DLSetup.exe**).

Klicken Sie **Weiter**, akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf **Weiter**.



Markieren Sie Enterprise Service und klicken auf **Weiter** um den DriveLock Enterprise Service zu installieren.

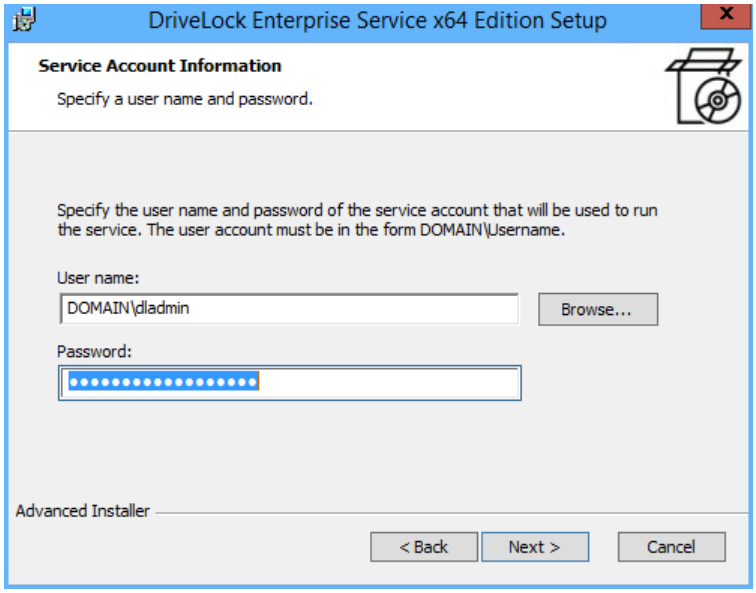
Möchten Sie die zuvor ausgewählte Komponente nicht sofort installieren sondern nur über das Internet laden, aktivieren sie die Option „**Dateien nur herunterladen – nicht installieren**“.

Die Option „**Keine aktualisierten Versionen herunterladen – vorhandene Dateien benutzen**“ ermöglicht Ihnen die Installation der im aktuellen Verzeichnis gespeicherten DriveLock Enterprise Service Version.

Klicken Sie nun auf **Weiter**, um mit dem Download bzw. der Installation zu beginnen. Klicken Sie auf **Fertig stellen**, um den DriveLock Enterprise Service Setup Wizard zu starten.

DriveLock Enterprise Service Setup

Klicken Sie **Next**.



Geben Sie das Benutzerkonto und das dazugehorige Passwort ein, unter welchem der DriveLock Enterprise Service gestartet werden soll. Klicken Sie auf **Browse**, um ein bestehendes Konto auszuwählen.

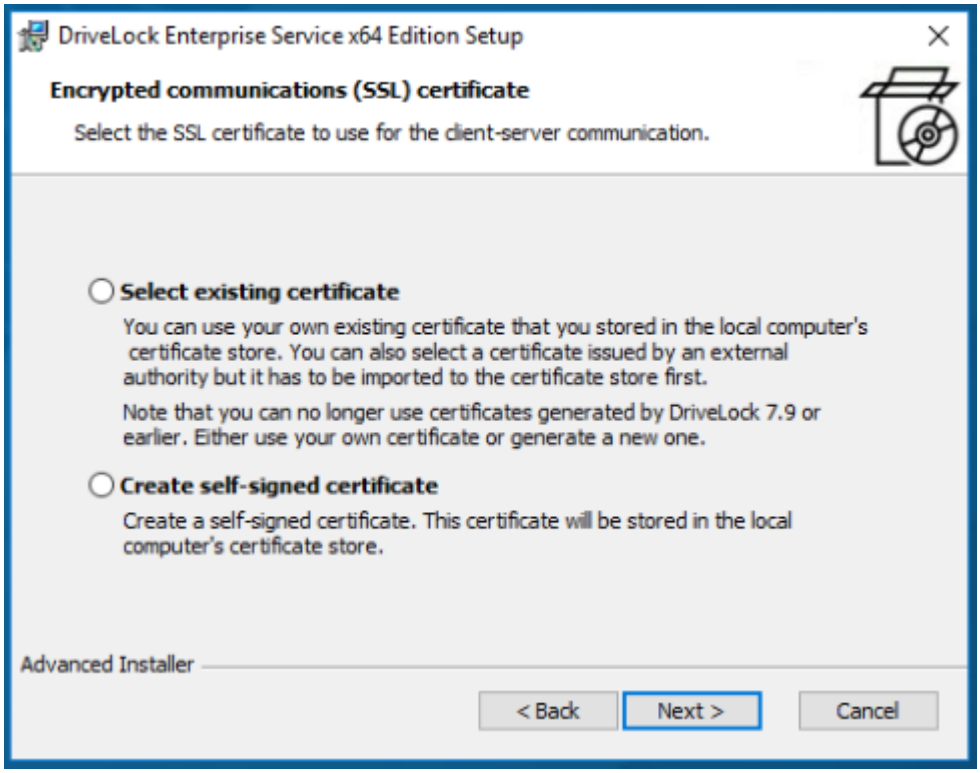
Klicken Sie **Next**, um fortzufahren.

Die Kommunikation zwischen dem DES und der DriveLock Management Konsole bzw. zwischen einem vertrauenswürdigem DES und den DriveLock Agenten wird durch die Verwendung von *Zertifikaten* abgesichert.

> Ab Version 2019.1. bieten die von DriveLock erstellten Serverzertifikate eine zusätzliche Absicherung der Kommunikation durch Verwendung eines *Schlüssels mit 4096-bit Länge* und des Hash-Algorithmus *sha512*.

Beachten Sie bitte, dass Zertifikate, die mit DriveLock 7.9. oder früher generiert worden sind, ab Version 2019.1 nicht mehr verwendet werden können! Sie müssen daher ein neues Zertifikat erstellen oder ein eigenes verwenden.

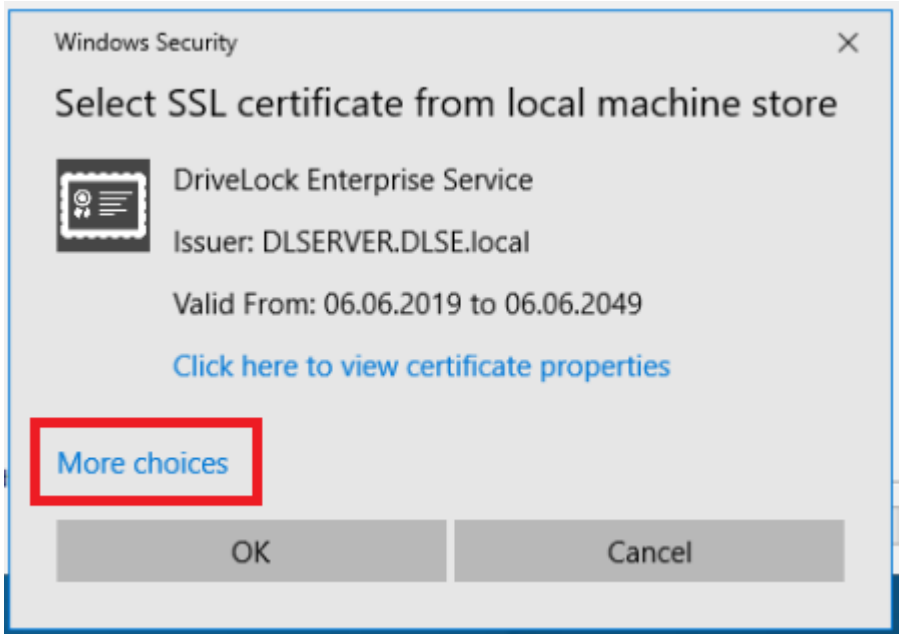
Nachdem Sie das Benutzerkonto und Kennwort für den neuen DES eingegeben haben, wird Ihnen folgender Dialog angezeigt:



Option 1:

Wählen Sie **Select existing certificate**, wenn Sie über eigene Zertifikate im Zertifikatsspeicher des Computers verfügen und diese verwenden wollen.

Klicken Sie auf **Next** und wählen Sie dann das Zertifikat aus der Liste unter **More choices** aus.

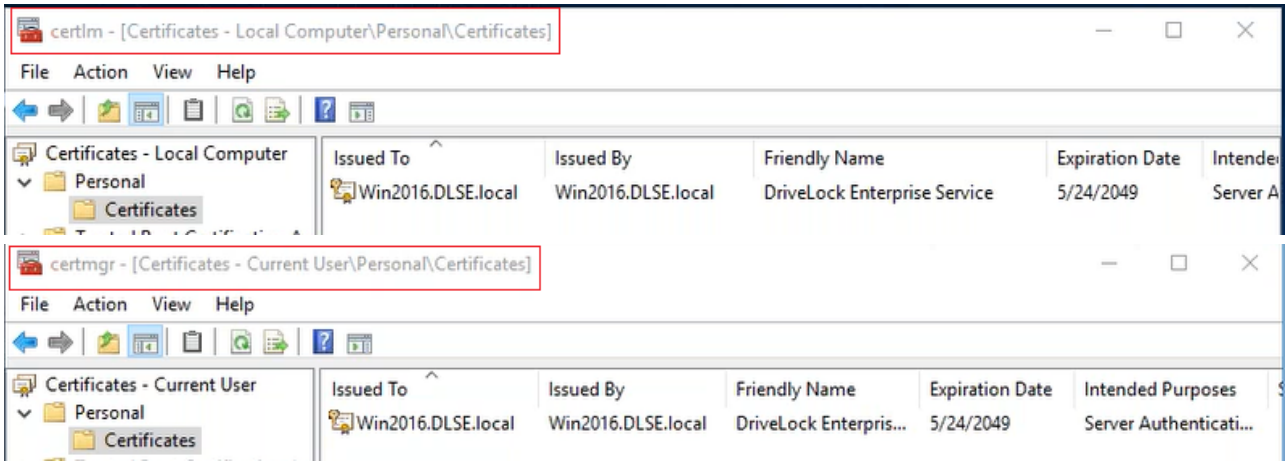


Klicken Sie **OK**, um die Auswahl zu bestätigen.

Option 2:

Wählen Sie **Create self-signed certificate**, wenn DriveLock ein SSL-Zertifikat für Sie erstellen soll und klicken Sie **Next**. Ein gültiges selbstsigniertes Zertifikat wird direkt erstellt.

Hinweis für beide Optionen: Das Zertifikat wird sowohl im lokalen Zertifikatsspeicher des Computers als auch im Zertifikatsspeicher des zuvor eingegebenen DES Benutzers gespeichert (siehe Abbildungen).

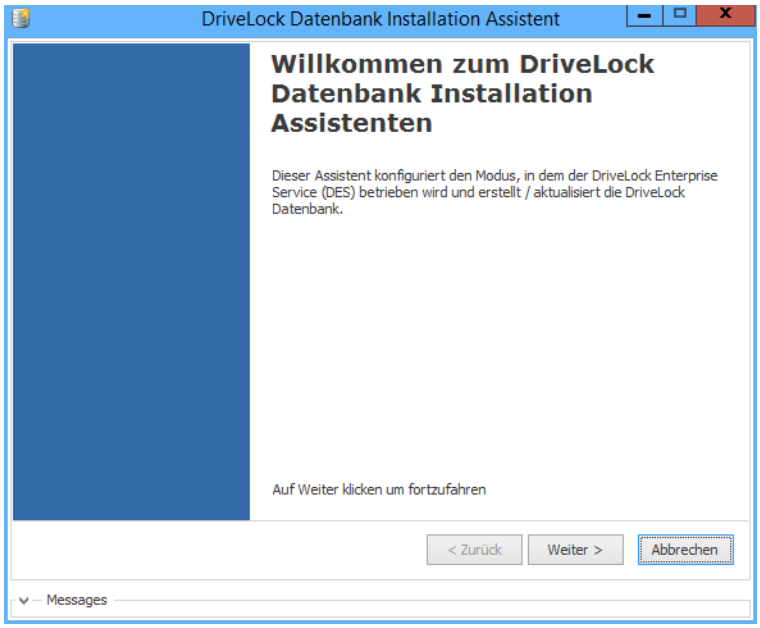


Sie können nun das erstellte Zertifikat in Richtlinien als vertrauenswürdiges Zertifikat für die Kommunikation zwischen DriveLock Agent und DES verwenden. Mehr Informationen hierzu finden Sie im Kapitel **Vertrauenswürdige Zertifikate** im Administrationshandbuch und im Benutzerhandbuch auf https://drivelock.help/

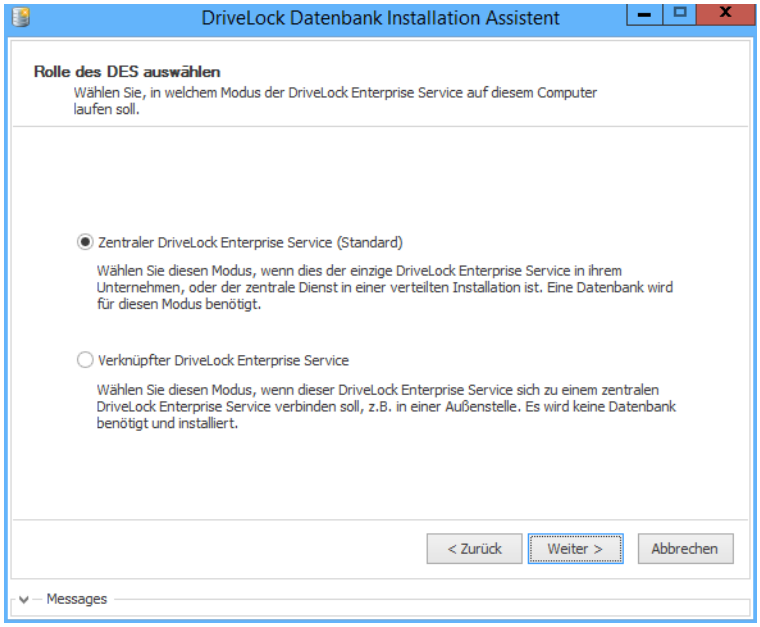
Klicken Sie im nächsten Dialog **Ready to Install** auf die Schaltfläche **Install**, um die Installation des DES fortzusetzen. Wenn Sie nicht möchten, dass das Installationsprogramm automatisch die für den reibungslosen Betrieb des DES benötigten Ports in der Firewall freischaltet, entfernen Sie bei der angezeigten Option den Haken.

Nach Beendigung der Installation klicken Sie **Finish**, um den Installationsassistenten zu beenden. Anschließend startet automatisch der Assistent für die Datenbank-Installation. Dieser Assistent wird Ihnen bei der Installation, Einrichtung und Aktualisierung der DES-Datenbank helfen.

Datenbank Installations-Assistent



Klicken Sie auf **Weiter**.

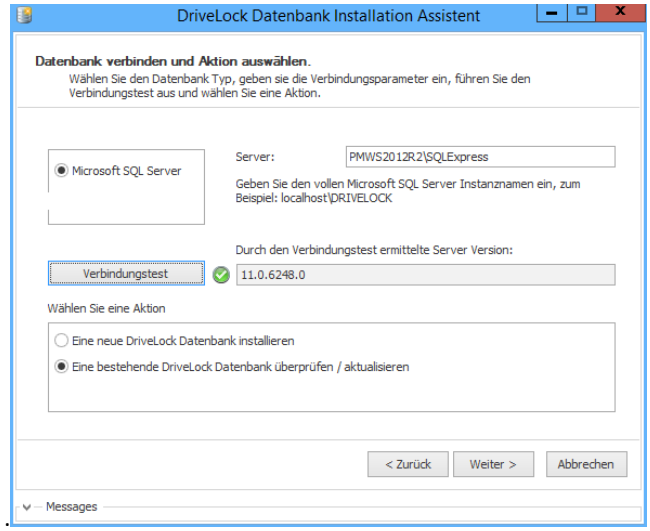


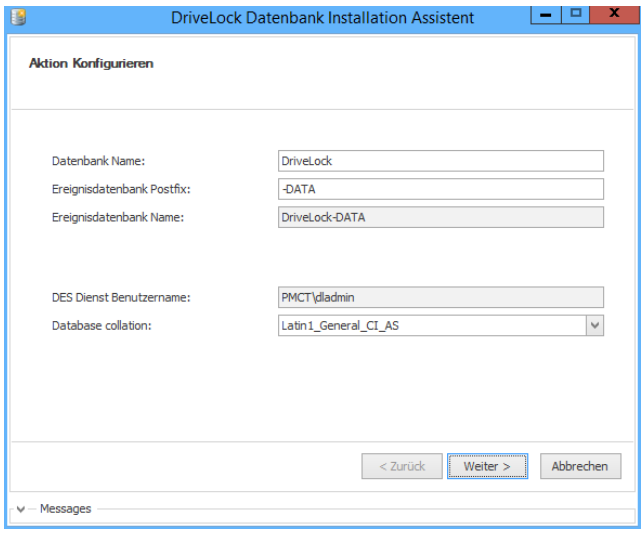
Wählen Sie die Serverrolle aus und klicken auf **Weiter**.

> Wenn dies der erste DriveLock Enterprise Service ist, wählen Sie den Modus Zentraler DriveLock Enterprise Service. Weitere Informationen zum Servermodus finden Sie im Abschnitt „*Gesamtstruktur*“.

Wählen Sie nun Microsoft SQL Server aus.

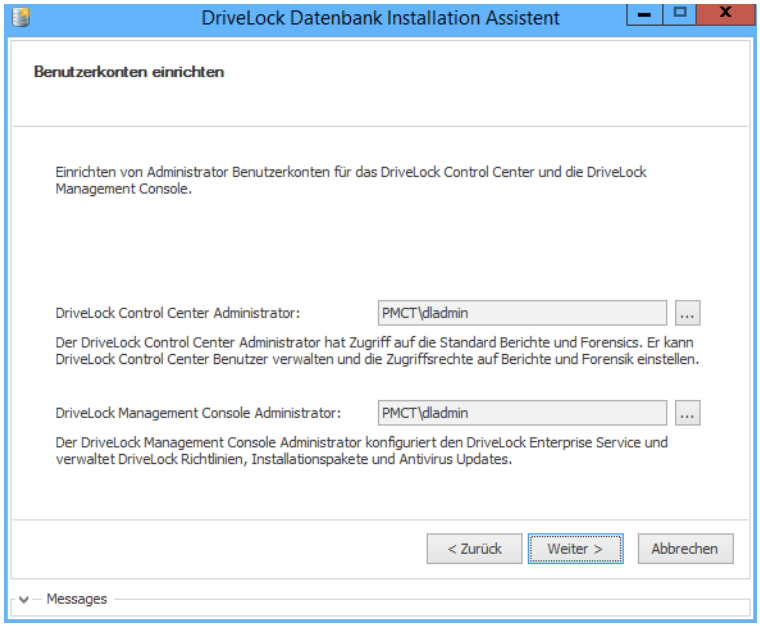
Microsoft SQL Server





Wenn Sie eine SQL-Server Datenbank verwenden, geben Sie einen gültigen Datenbankserver und Instanz-Namen an. Klicken Sie auf **Verbindungstest** und wählen dann aus ob Sie die Datenbank neu installieren oder aktualisieren wollen bevor Sie auf **Weiter** klicken. Im Falle einer Neuinstallationen müssen Sie noch die Datenbank Kollation (Sortierung) festlegen und ihre Eingaben mit **Weiter** bestätigen bestätigen.

Benutzerkonto für Administration und Reporting



Im Falle einer Neuinstallation legen Sie noch folgenden Berechtigungen fest:

- *DriveLock Control Center Administrator*: dieser Benutzer oder diese Gruppe darf später auf das DriveLock Control Center zugreifen (Vollzugriff). Weitere Berechtigungen können später im DriveLock Control Center angepasst werden.
- *DriveLock Management Konsole Administrator*: dieser Benutzer oder diese Gruppe darf später innerhalb der DriveLock Management Konsole DriveLock Enterprise Service Einstellungen konfigurieren. Weitere Berechtigungen können später in der DriveLock Management Konsole vergeben werden

Geben Sie die entsprechenden Administratoren(-Gruppen) an und klicken Sie **Weiter**.

Abschluss der Installation

Die Installationsparameter werden zusammengefasst. Mit einem Klick auf **Weiter** wird die Installation/Aktualisierung gestartet.

Je nach Datenbankserver kann dieser Vorgang mehrere Minuten dauern. Der Installationsassistent erstellt nun zwei Datenbanken anhand der vorgegebenen Parameter (z.B. „DriveLock“ und „DriveLock-Data“ bei SQL-Server) bzw. aktualisiert diese.

Nach erfolgter Installation klicken Sie auf **Weiter** und anschließend auf **Fertigstellen**.

5.3 Installation der DriveLock Management-Komponenten

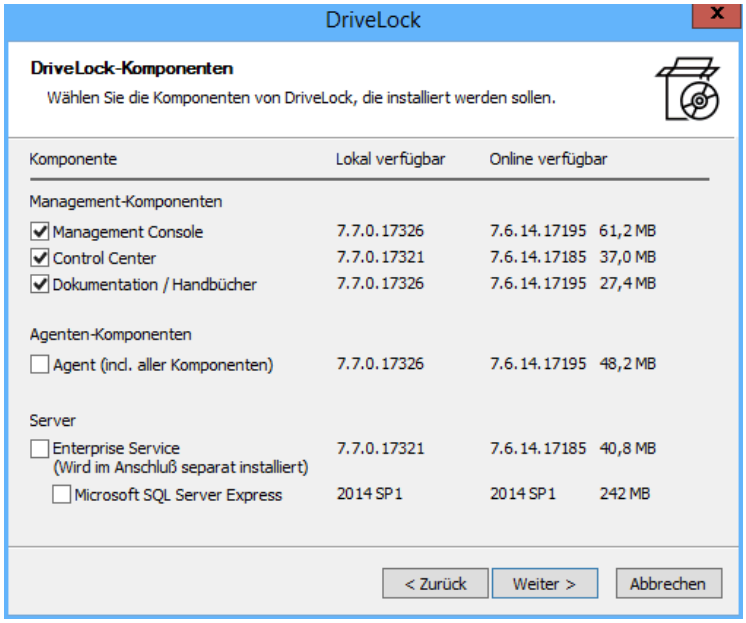
Alle DriveLock Management-Komponenten können über den DriveLock Installer installiert werden. Der DriveLock Installer überprüft dabei, ob eine aktuellere DriveLock Version veröffentlich wurde und lädt ggf. die entsprechenden Pakete über das Internet nach.

Kopieren Sie den DriveLock Installer (**DLSetup.exe**) in ein eigenes Verzeichnis. Alle aus dem Internet geladenen Pakete werden ebenfalls in diesem Verzeichnis abgelegt und können für weitere Installationen verwendet werden.

Starten Sie den DriveLock Installer (**DLSetup.exe**) durch einen Doppel-Klick auf die Datei im Explorer-Fenster.

Sofern eine neuere Version des DriveLock-Installers verfügbar ist, erscheint eine kurze Meldung und Sie können diese aktuellere Version aus dem Internet herunterladen.

Klicken Sie **Weiter**, akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf **Weiter**.



Nun können Sie die zu installierenden bzw. zu ladenden Komponenten auswählen. Markieren Sie die ersten drei Komponenten, um die DriveLock Management Konsole, das DriveLock Control Center und die zugehörige Dokumentation zu installieren. Der DriveLock Installer überprüft dabei, welche Versionen lokal (d.h. im gleichen Verzeichnis wie DLSetup.exe) bzw. online vorhanden sind.

> Bei einer Evaluierung von DriveLock wählen Sie alle Komponenten aus, um diese auf dem aktuellen Rechner zu installieren.

Klicken Sie nun auf **Weiter**.

Möchten Sie die zuvor ausgewählten Komponenten nicht sofort installieren sondern nur über das Internet laden, aktivieren sie die Option „**Dateien nur herunterladen – nicht installieren**“.

Die Option „**Keine aktualisierten Versionen herunterladen – vorhandene Dateien benutzen**“ ermöglicht Ihnen die Installation der im aktuellen Verzeichnis gespeicherten Komponenten.

Über die Option „**32-Bit-Version herunterladen**“ (bzw. „**64-Bit-Version herunterladen**“) können Sie auch die Installationsdateien aus dem Internet laden, die nicht für die gerade verwendete Plattform von Windows geeignet sind.

Klicken Sie nun auf **Weiter**, um mit dem Download bzw. der Installation zu beginnen. Sobald dieser Vorgang abgeschlossen ist, erhalten Sie eine Rückmeldung über den Status des Downloads bzw. der Installation.

Klicken Sie **Fertig stellen**, um die Installation zu beenden.

5.4 Installation des DriveLock Agenten

Um den Zugriff auf Wechseldatenträger zu kontrollieren, muss der DriveLock Agent auf jedem Rechner installiert werden.

Es gibt ein spezielles MSI-Paket, das zur Installation des DriveLock Agenten auf nicht-administrativen Rechnern verwendet werden kann. Dieses Installations-Paket (*DriveLockAgent.msi* bzw. *DriveLockAgent X64.msi*) installiert den DriveLock Agentendienst ohne Erstellung von Startmenüeinträgen und ohne Benutzereingaben während der Installation (Silent Installation).

> Das MSI-Paket für den DriveLock Agenten befindet sich auf der DriveLock ISO-Datei (welches auf eine CD gebrannt werden kann) oder wird durch den DriveLock Installer aus dem Internet heruntergeladen.

> Falls Sie auf einem System, auf dem der DriveLock Agent deinstalliert wurde, eine Neuinstallation durchführen wollen, stellen Sie sicher, dass die Schlüssel HKEY_CURRENT_USER\Software\CenterTools und HKEY_LOCAL_MACHINE\Software\CenterTools in der Registry leer sind. Die Deinstallation des Agenten könnte hier Eintragungen nicht entfernt haben, die erst nach der initialen Installation erzeugt wurden, was zu unerwarteten Resultaten führen kann.

Vor der Installation von Agenten auf den Rechnern des Netzwerks muss mindestens eine Gruppen-Richtlinie, eine zentral zugängliche Konfigurationsdatei oder eine zentral gespeicherte Richtlinie erstellt worden sein, die zumindest Basiseinstellungen und Whitelist-Regeln für erforderliche Geräte enthält und die zum Installationszeitpunkt auf den Client Computern aktiv ist. Nach erfolgreicher Installation wird der DriveLock Agent sofort gestartet und wendet entweder die verfügbare DriveLock Richtlinie oder die bei Laufwerken restriktiven Standardeinstellungen an.

> **Wenn der Agent ohne Konfigurationseinstellungen installiert wird, werden durch Standardeinstellungen eventuell Geräte oder Laufwerke gesperrt, die für die korrekte Funktion der Clients unbedingt erforderlich sind.**

Bei der Verwendung von Konfigurationsdateien muss der DriveLock Agent schon bei der Installation entsprechend konfiguriert werden, da er selbst aktiv auf Aktualisierungen der DriveLock Konfiguration prüfen und diese ggf. vom zuvor konfigurierten Ort herunterladen muss. Verwenden Sie Gruppenrichtlinien zur Verteilung der DriveLock Konfiguration müssen Sie keine Anpassungen des DriveLock Agenten Installationspaketes vornehmen, da der Agent die Konfiguration automatisch bekommt. Wenn Sie eine zentral gespeicherte Richtlinie verwenden, ist die Vorkonfiguration nur notwendig, sofern Sie die automatische Erkennung von DriveLock Enterprise Service und DriveLock Agenten (über mDNS/DNS-SD) deaktiviert oder - wie in größeren Umgebungen häufig der Fall - unterbunden wurde und somit die Schnellkonfigurationsoption abgeschaltet ist.

Die folgenden Abschnitte beschreiben die Installation des DriveLock Agenten für die jeweilige Konfigurationsart genauer.

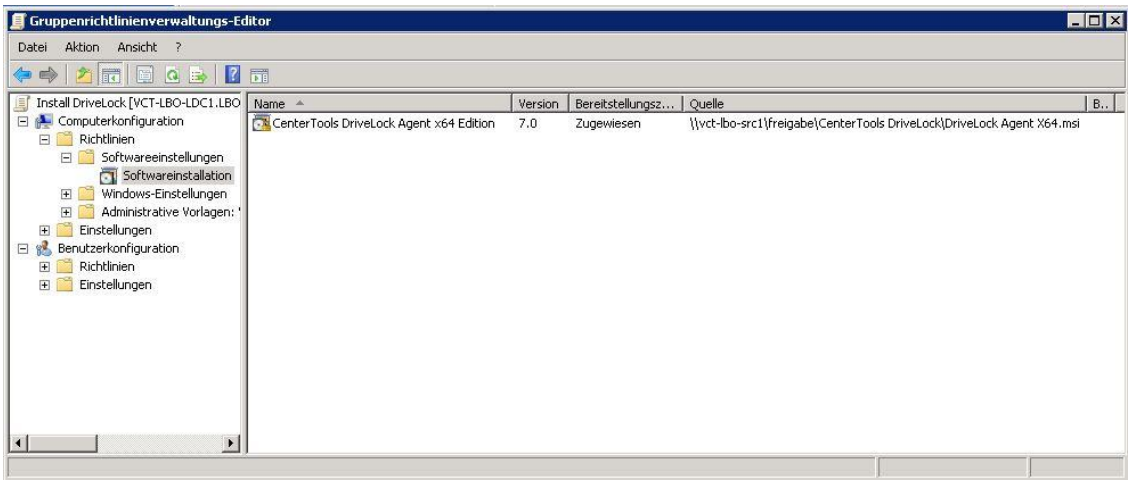
5.4.1 DriveLock Installation mit Active Directory Gruppenrichtlinien

Ein häufig genutzter Weg für die Agentenverteilung von DriveLock ist die Nutzung von Active Directory Gruppenrichtlinien.

Dabei ist es erforderlich, dass sich das **DriveLockAgent.msi** Installationspaket (**DriveLockAgent_X64.msi** für 64-Bit Systeme) auf einem freigegebenen Verzeichnis befindet, auf das die Clients zugreifen können.

> Weitere Informationen zur Benutzung von Gruppenrichtlinienobjekten erhalten Sie auf der Microsoft Website.

Zur Konfiguration einer Softwareverteilungsrichtlinie für 32-Bit Systeme kann ein bestehendes Gruppenrichtlinienobjekt gewählt oder ein neues Gruppenrichtlinienobjekt erstellt werden. Öffnen Sie dazu im Gruppenrichtlinieneditor „**Computerkonfiguration → Softwareeinstellungen → Softwareinstallation“**.



> Zum Öffnen oder Erstellen eines Gruppenrichtlinienobjekts kann auch die DriveLock Management Konsole verwendet werden.

Durch Rechts-Klick auf **Software Installation** und Wahl von „**Neu → Paket**“ öffnet sich ein Dateiauswahldialog. Navigieren Sie zu dem freigegebenen Verzeichnis, welches das Installationspaket enthält und wählen Sie die Datei **DriveLockAgent.msi**. Überzeugen Sie sich dabei davon, dass der Dateiname gemäß der Universal Naming Convention (UNC) angezeigt wird (z.B. „*\\Server\drivelock$\DriveLockAgent.msi*“).

Wählen Sie “**Erweitert**” als Verteilungsmethode und klicken Sie **OK**.

Wählen Sie den Reiter **Verteilung** und klicken Sie auf die Schaltfläche **Erweitert**. Entfernen Sie nun den Haken bei der Option „**Diese 32-Bit X86 Anwendung auf Windows 64 Computern verfügbar machen**“.

Bestätigen Sie alle Einstellungen mit **OK**.

Das Gruppenrichtlinienobjekt ist jetzt konfiguriert und die Verteilung des Agenten wird nach der Replikation der Domain Controller auf die Zielrechner starten.

Für die Verteilung des 64-Bit Paketes wiederholen Sie die gerade genannten Schritte, verwenden Sie bitte jedoch die Datei *DriveLockAgent_X64.msi* und ändern Sie die erweiterten Verteilungseinstellungen nicht.

> DriveLock sollte nicht mittels Benutzer-Richtlinie einer Gruppenrichtlinie verteilt werden, da DriveLock eine computerbezogene Anwendung ist.

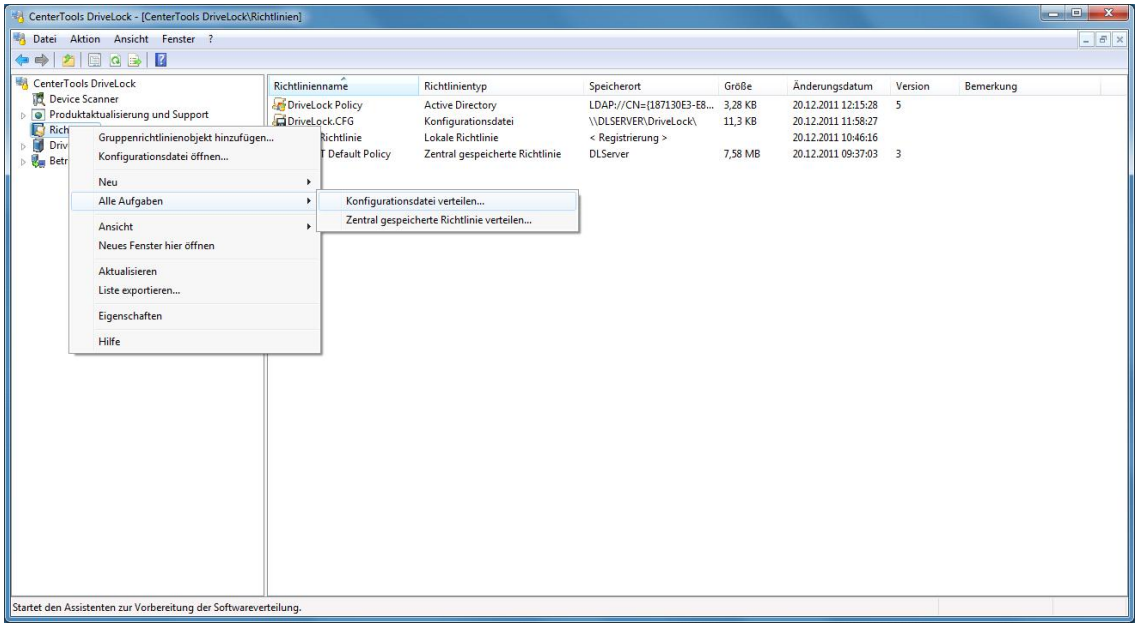
Die Konfigurationseinstellungen von DriveLock werden nicht automatisch mit dem Softwarepaket installiert. Diese müssen zusammen mit einer gültigen Lizenz in derselben oder besser einer separaten Gruppenrichtlinie definiert sein.

Wenn Sie den DriveLock Agenten mittels Gruppenrichtlinien installieren, kann dieser nicht in der Systemsteuerung mittels *„Software / Programme ändern oder entfernen“* deinstalliert werden. Stattdessen muss das Softwarepaket von der Gruppenrichtlinie entfernt werden.

5.4.2 Installation des Agenten bei Verwendung von Konfigurationsdateien

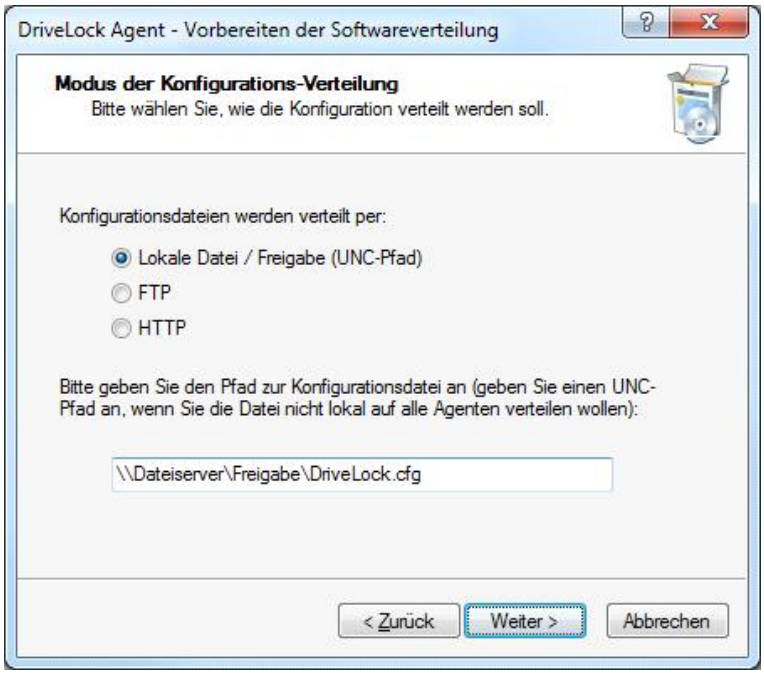
Bei Nutzung einer Konfigurationsdatei zur Verteilung der DriveLock Richtlinie auf Clients muss diese Konfigurationsdatei zunächst in ein freigegebenes Verzeichnis bzw. auf einen FTP-Server oder einen Web-Server kopiert und der Netzwerkpfad bzw. die URL während der Installation des Agenten angegeben werden. Für weitere Informationen zur DriveLock Konfiguration mittels einer Konfigurationsdatei konsultieren Sie bitte das DriveLock Administrationshandbuch.

Der DriveLock Assistent Softwareverteilung hilft Ihnen bei der Verteilung des DriveLock Agenten auf Rechner des Netzwerks bei Nutzung von Konfigurationsdateien. Der Assistent unterstützt Sie bei der Erstellung der richtigen Kommandozeilensyntax für den Windows Installer, generiert ein modifiziertes Microsoft Installer Paket oder ein Microsoft Installer Transform (MST) Datei für die Installation.



Der Assistent kann mittels rechten Mausklicks auf **Richtlinien** gestartet werden Dann wählen Sie bitte „**Alle Aufgaben → Konfigurationsdatei verteilen...**“.

Klicken Sie **Weiter**.



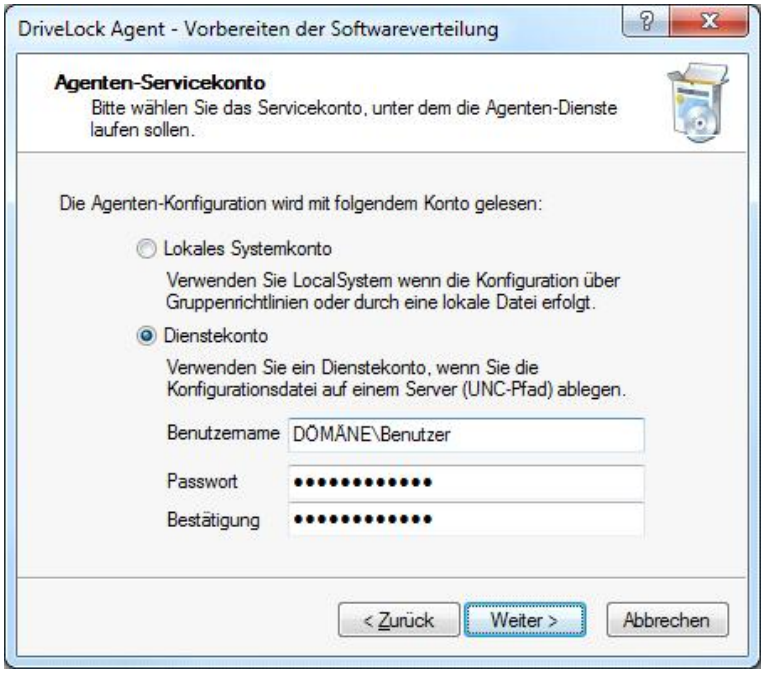
Geben sie die Stelle an, von der der DriveLock Agent die Konfigurationsdatei beziehen kann. Dabei kann ein UNC-Pfad, eine FTP- oder eine HTTP-Lokation definiert werden. Außerdem kann auch ein lokaler Pfad verwendet werden (z.B. **C:\Windows\DLConfig**), der für das lokale Systemkonto zugänglich ist.

Klicken Sie **Weiter** nach Angabe des Pfads der Konfigurationsdatei.

Danach müssen die Anmeldedaten des Benutzers eingegeben werden, dessen Konto für den Zugriff auf die Konfigurationsdatei verwendet wird:

- Lokales System: DriveLock verwendet das lokale Systemkonto zum Zugriff auf die Konfigurationsdatei; das ist die empfohlene Einstellung, wenn die Datei lokal auf dem Client vorgehalten wird.

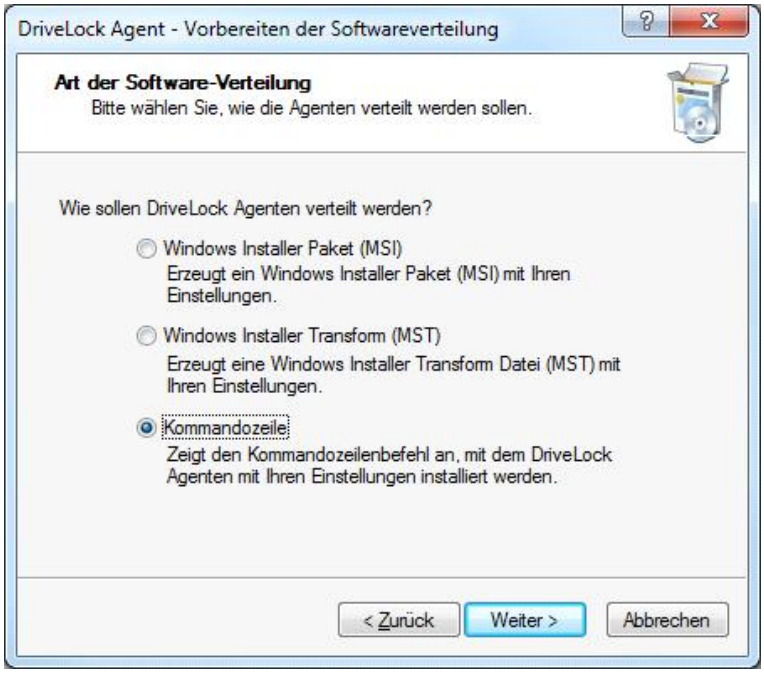
- Dienstkonto: DriveLock benutzt das angegebene Konto. Dieses muss das Recht „Anmelden als Dienst“ besitzen und ausreichende Berechtigungen zum Zugriff auf den Netzwerkpfad aufweisen. Das Passwort des Kontos wird verschlüsselt gespeichert.
- Anonym: Wenn FTP oder HTTP gewählt wurde, muss als Benutzername Anonymous und ein leeres Passwort verwendet werden. Der FTP oder HTTP Server muss anonymen Zugriff zu der Konfigurationsdatei zulassen.



Klicken Sie **Weiter.**

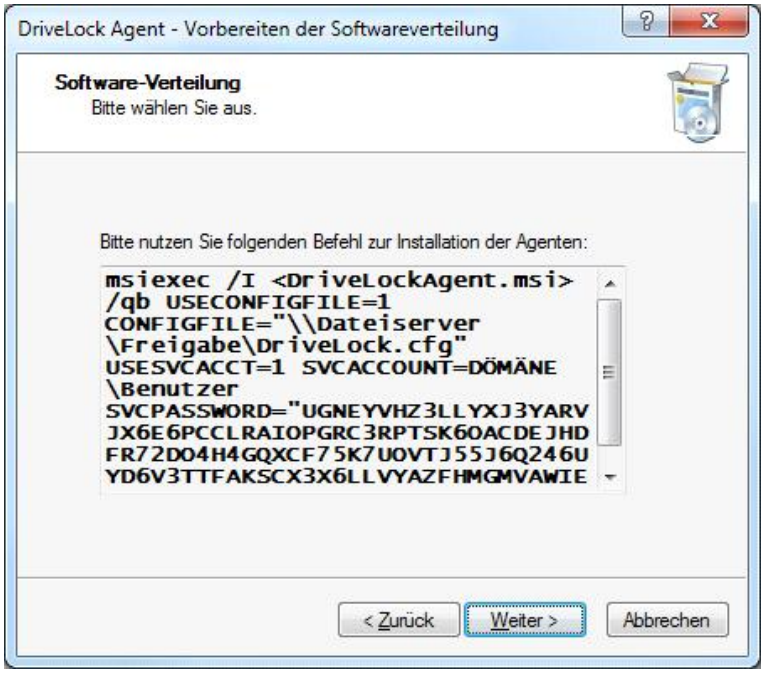
Wählen Sie im nächsten Dialog die Art des Installationspakets, das vom Wizard erstellt werden soll:

- Microsoft Installer Datei (MSI): Erstellt ein neues Microsoft Installer Paket, das die zuvor spezifizierten Einstellungen enthält.
- Microsoft Installer Transform Datei (MST): Erstellt eine Microsoft Installer Transform (MST) Datei mit den gewählten Einstellungen. Eine MST-Datei kann zusammen mit dem Original-MSI-Paket verwendet werden, das in der DriveLock Installation enthalten ist.
- Kommandozeile: Zeigt die Kommandozeilen-Syntax mit den gewählten Einstellungen für den Microsoft Installer an.



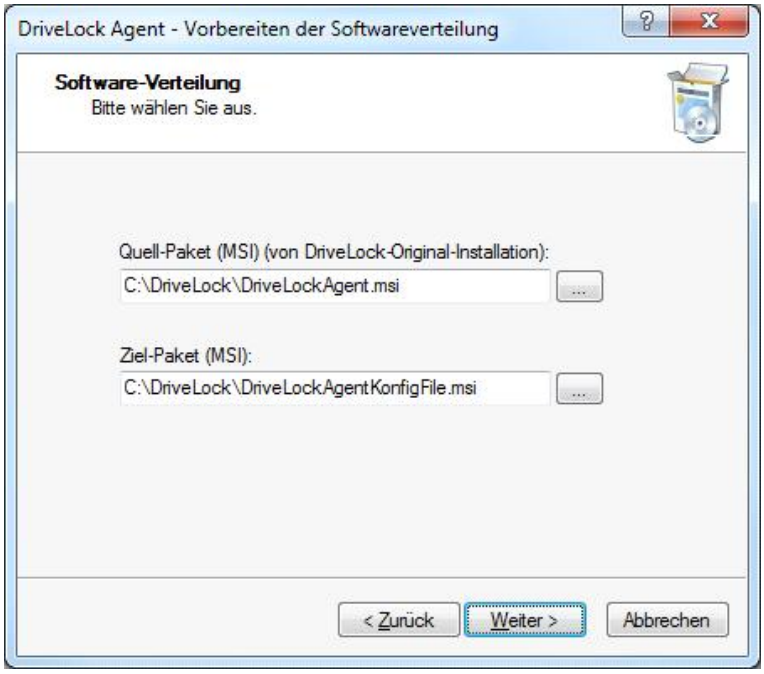
Klicken Sie **Weiter**.

Falls Sie *Kommandozeile* gewählt haben, zeigt der nächste Dialog die Syntax an, die für die Installation des DriveLock Agenten zu verwenden ist. Dabei muss "<DriveLockAgent.msi>" auf den kompletten Pfad der „**DriveLockAgent.msi**"-Datei geändert werden.



Dieser Kommandozeilenbefehl kann für die manuelle Installation des Agenten (siehe auch Abschnitt „Installation mit Kommandozeilenparametern (unbeaufsichtigte Installation)") verwendet werden.

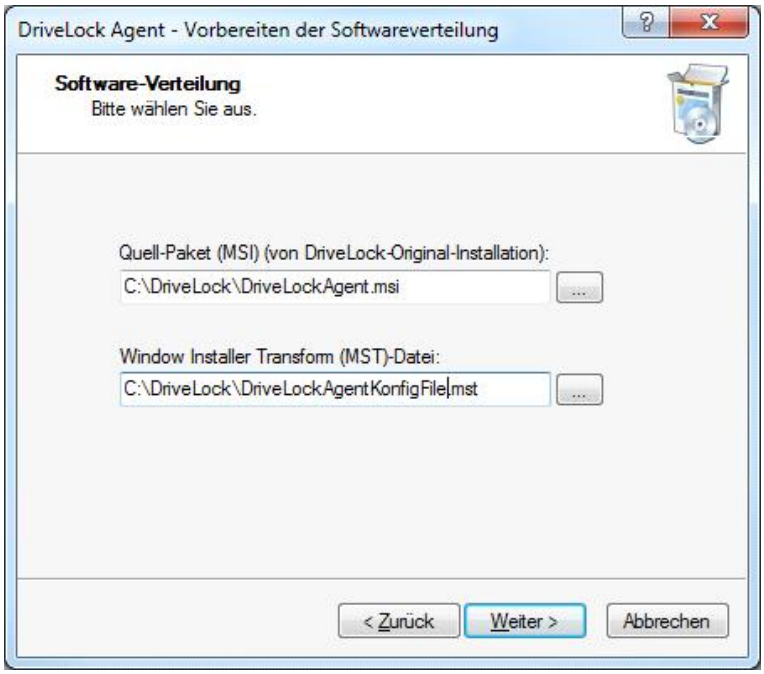
Wenn die Option zur Erzeugung einer neuen MSI-Datei gewählt wurde, müssen Sie Pfad und Name der Original-„*DriveLockAgent.msi*"-Datei und die neue MSI-Datei angeben.



Geben Sie Pfad und Name für beide Dateien an und klicken Sie **Weiter** zur Generierung der neuen MSI-Datei.

> Das modifizierte Installer Paket kann für die manuelle Installation des Agenten oder zur Verteilung mit einem Dritthersteller-Produkt verwendet werden.

Für die Generierung einer Microsoft Installer Transform (MST) Datei muss Pfad und Name der Original *„DriveLockAgent.msi“*-Datei sowie die MST-Datei angegeben werden.

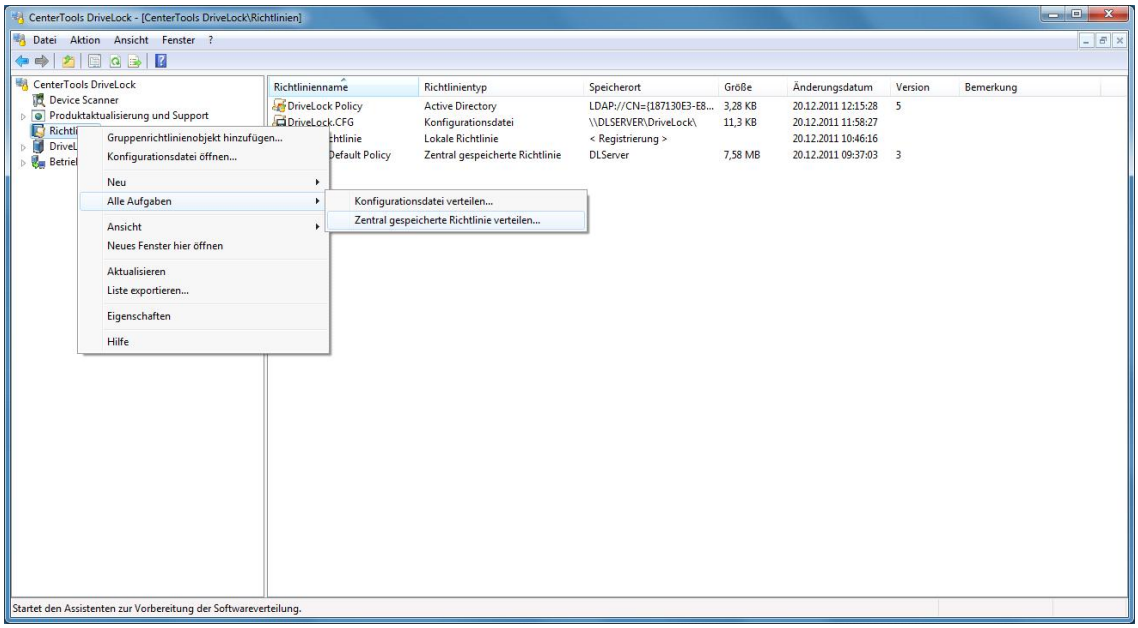


Geben Sie Pfad und Name für beide Dateien an und klicken Sie **Weiter** zur Generierung der neuen MST-Datei.

Nach Abschluss des Assistenten können Sie nun mit der Verteilung des DriveLock Agenten beginnen und entweder das Microsoft Installer Paket oder den Kommandozeilenbefehl verwenden.

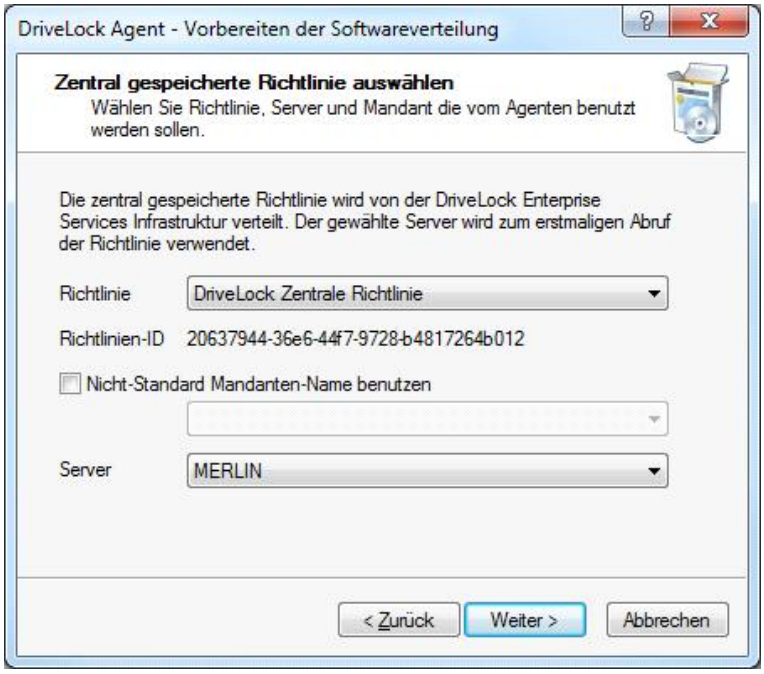
5.4.3 Installation bei Verwendung einer zentral gespeicherten Richtlinie

Der DriveLock Assistent Softwareverteilung hilft Ihnen auch bei der Verteilung des DriveLock Agenten auf Rechner des Netzwerks bei Nutzung von zentral gespeicherten Richtlinien. Der Assistent unterstützt Sie bei der Erstellung der richtigen Kommandozeilensyntax für den Windows Installer, generiert ein modifiziertes Microsoft Installer Paket oder ein Microsoft Installer Transform (MST) Datei für die Installation.



Der Assistent kann mittels rechten Mausklicks auf **Richtlinien** gestartet werden Dann wählen Sie bitte „**Alle Aufgaben → Zentral gespeicherte Richtlinie verteilen...**“.

Klicken Sie **Weiter.**



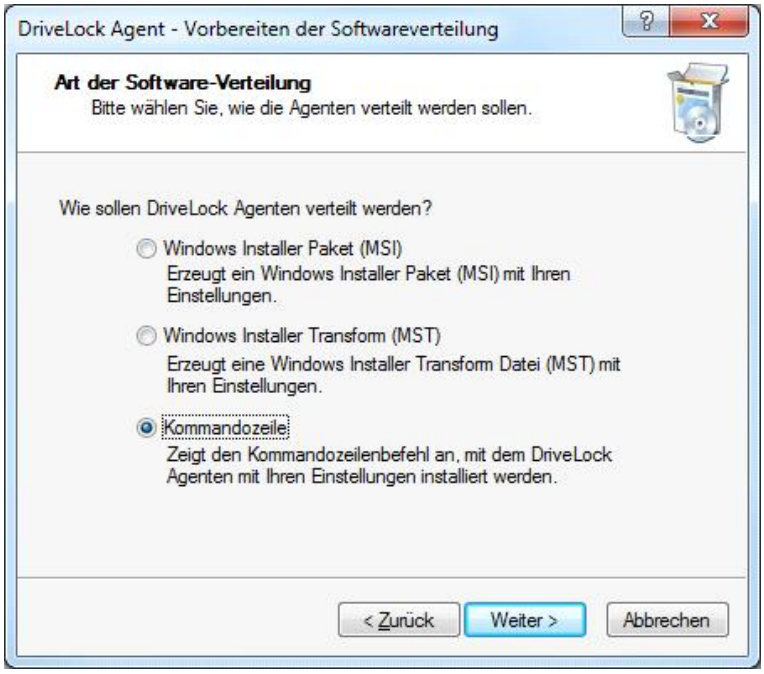
Wählen Sie die zentral gespeicherte Richtlinie, welche von den DriveLock Agenten verwendet werden soll und den Server, auf dem der zentrale DriveLock Enterprise Service installiert ist.

Sofern Sie mehr als eine DriveLock Konfigurationsumgebung haben (Mandantenfähigkeit), aktivieren Sie die Option „**Nicht-Standard Mandanten-Namen benutzen**“ und wählen Sie den für die Agenten zu verwendenden Mandatennamen aus.

Klicken Sie nun auf **Weiter**.

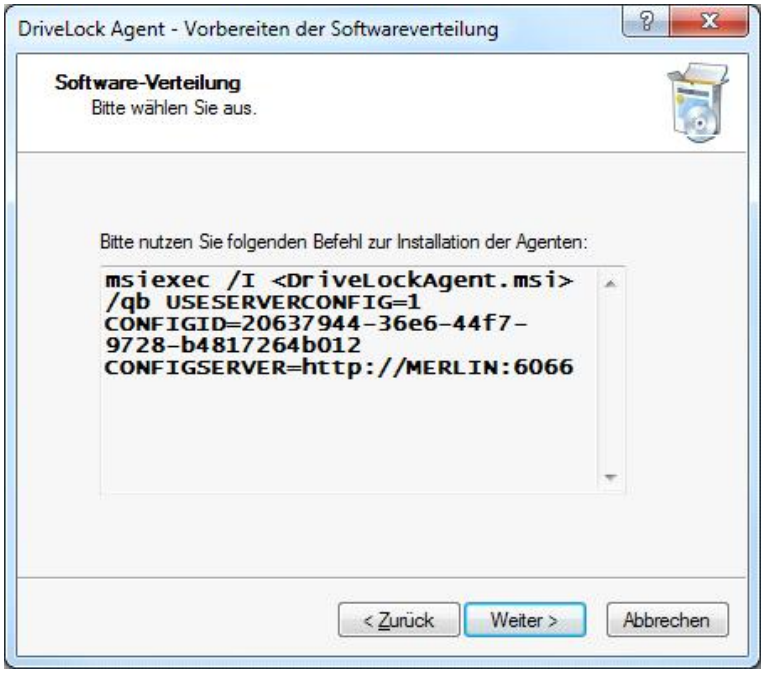
Wählen Sie im nächsten Dialog die Art des Installationspakets, das vom Wizard erstellt werden soll:

- Microsoft Installer Datei (MSI): Erstellt ein neues Microsoft Installer Paket, das die zuvor spezifizierten Einstellungen enthält.
- Microsoft Installer Transform Datei (MST): Erstellt eine Microsoft Installer Transform (MST) Datei mit den gewählten Einstellungen. Eine MST-Datei kann zusammen mit dem Original-MSI-Paket verwendet werden, das in der DriveLock Installation enthalten ist.
- Kommandozeile: Zeigt die Kommandozeilen-Syntax mit den gewählten Einstellungen für den Microsoft Installer an.



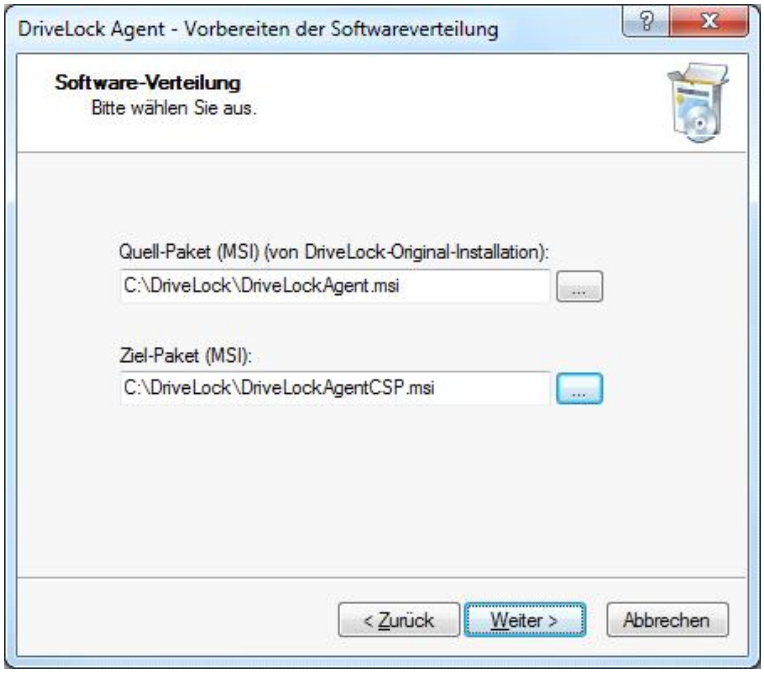
Klicken Sie **Weiter**.

Falls Sie *Kommandozeile* gewählt haben, zeigt der nächste Dialog die Syntax an, die für die Installation des DriveLock Agenten zu verwenden ist. Dabei muss "<DriveLockAgent.msi>" auf den kompletten Pfad der „**DriveLockAgent.msi**"-Datei geändert werden.



> Dieser Kommandozeilenbefehl kann für die manuelle Installation des Agenten (siehe auch Abschnitt „Installation mit Kommandozeilenparametern (unbeaufsichtigte Installation)") verwendet werden.

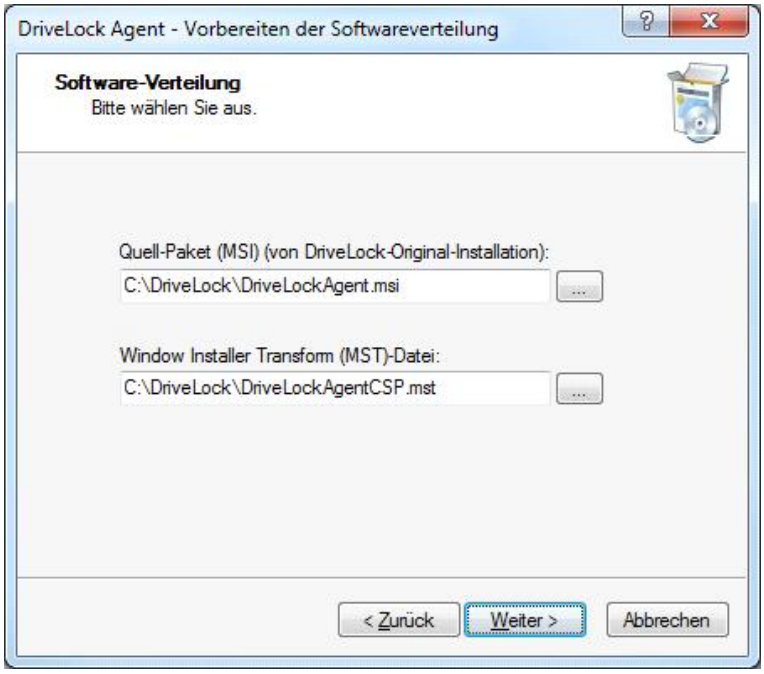
Wenn die Option zur Erzeugung einer neuen MSI-Datei gewählt wurde, müssen Sie Pfad und Name der Original-„*DriveLockAgent.msi*"-Datei und die neue MSI-Datei angeben.



Geben Sie Pfad und Name für beide Dateien an und klicken Sie **Weiter** zur Generierung der neuen MSI-Datei.

> Das modifizierte Installer Paket kann für die manuelle Installation des Agenten oder zur Verteilung mit einem Drittherstellter-Produkt verwendet werden.

Für die Generierung einer Microsoft Installer Transform (MST) Datei muss Pfad und Name der Original *„DriveLockAgent.msi“*-Datei sowie die MST-Datei angegeben werden.



Geben Sie Pfad und Name für beide Dateien an und klicken Sie **Weiter** zur Generierung der neuen MST-Datei.

5.4.4 Installation mit Richtlinien-Signaturzertifikat (Experimentell)

Ein DriveLock Agent kann mithilfe eines Zertifikates installiert werden, um

- bereits bei der Installation Verbindungsparameter zu DES festzulegen,

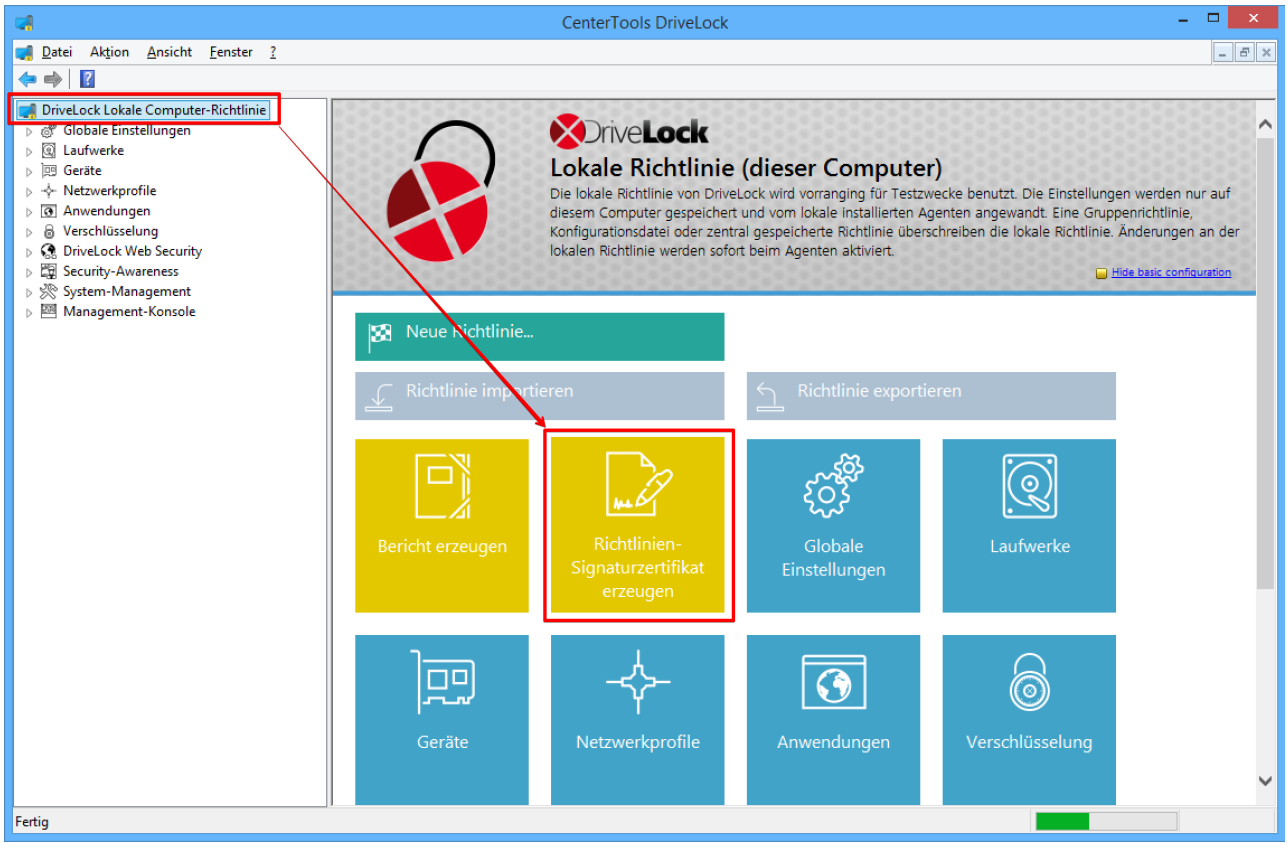
- einen vordefinierten Mandanten zu verwenden,
- eine Standardrichtlinie für den Fall, dass der Agent sich nicht mit einem DES verbinden kann und keine Gruppenrichtlinie vorhanden ist, mitgeben,
- einen zusätzlichen Schutz von Richtlinien gegen manipulative Änderungen zu aktivieren.

Die folgenden Schritte sind notwendig, um einen Agenten mit einem Richtlinien-Signaturzertifikat zu installieren:

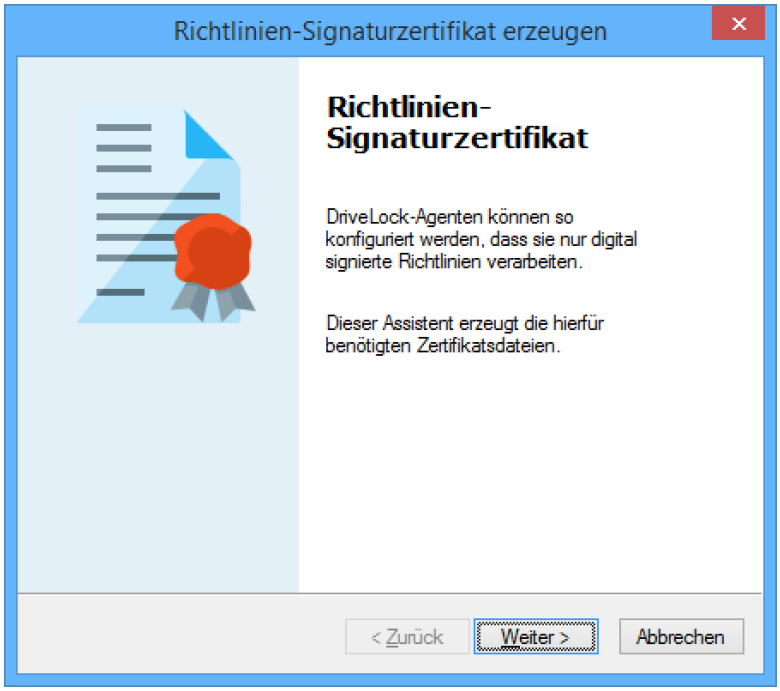
1. Erzeugung mindestens eines Zertifikates zur Signatur von DriveLock Richtlinien
2. Veröffentlichung einer signierten DriveLock Richtlinie
3. Installation eines Agenten mit einem Richtlinien-Signaturzertifikat

Erzeugen eines Zertifikates zum Signieren einer DriveLock Richtlinie

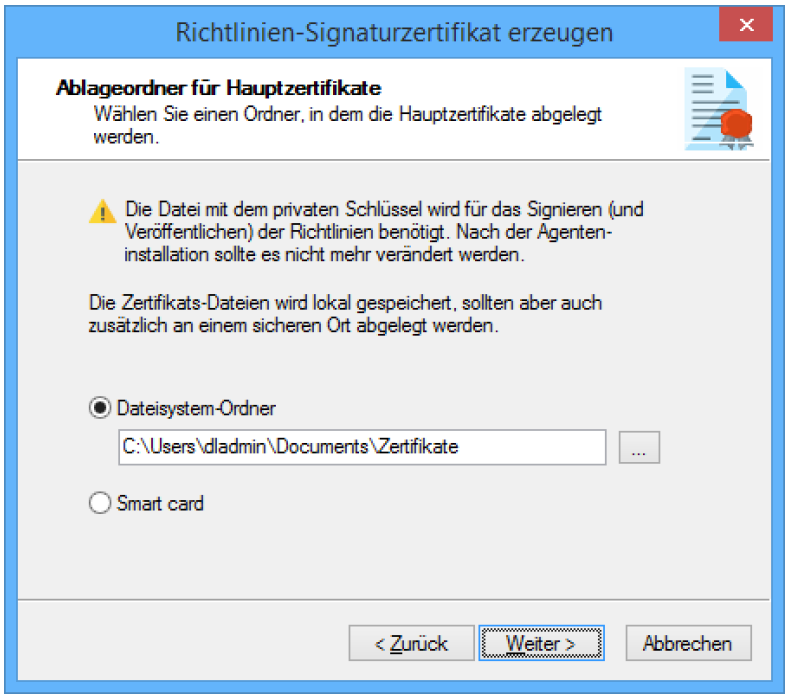
Ein Zertifikat wird innerhalb des DriveLock Richtlinien-Editors erzeugt. Klicken Sie dazu auf den obersten Navigationsknoten und dann auf **Richtlinien-Signaturzertifikat erzeugen**.



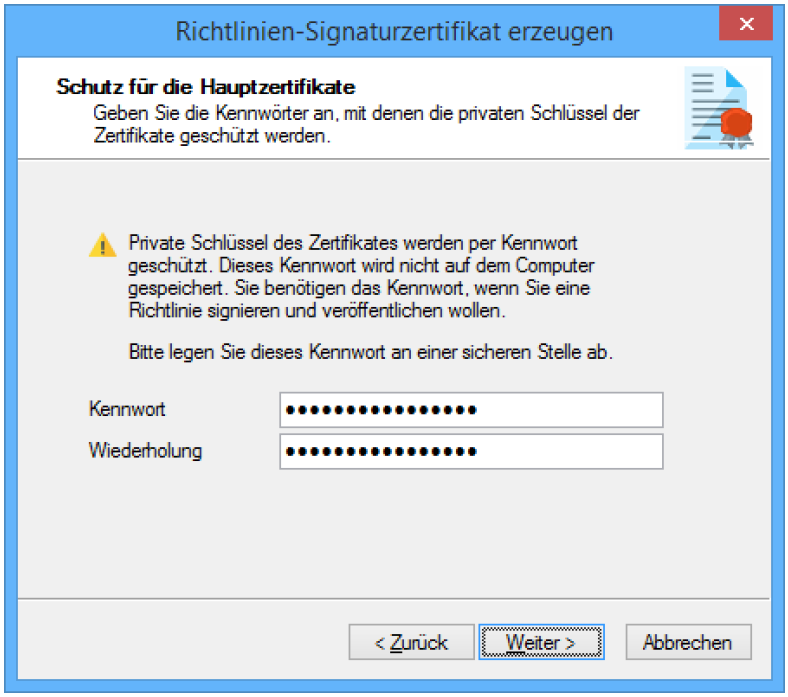
Es startet ein Assistent, der Sie bei der Erzeugung durch die einzelnen Schritte führt.



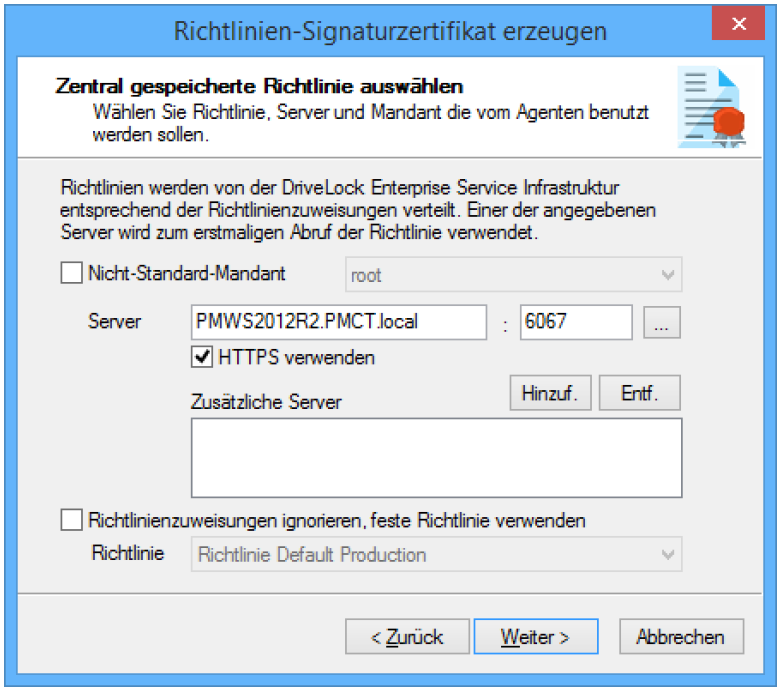
Klicken Sie **Weiter**.



Wählen Sie den Speicherort für das generierte Zertifikat aus. Sie können optional das Zertifikat auch auf einer Smartcard abspeichern.

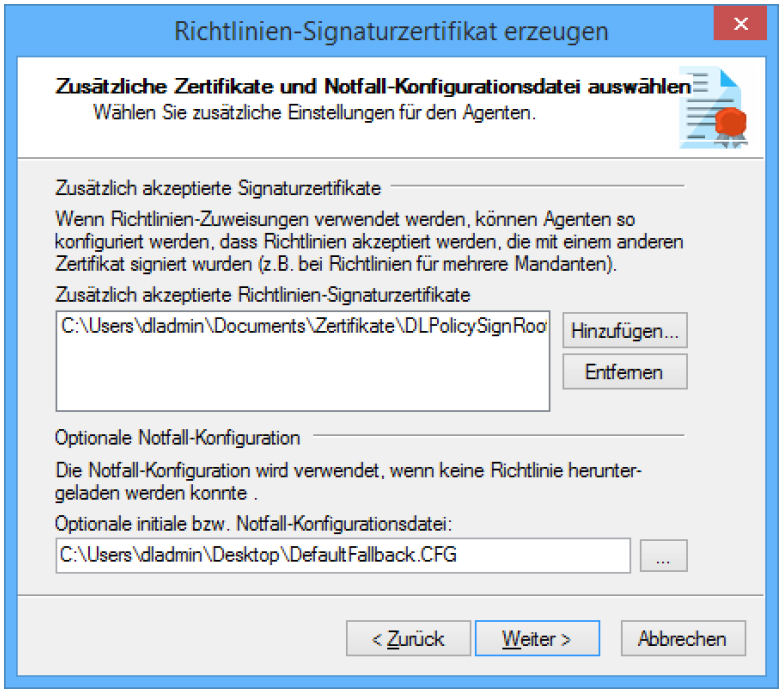


Für den Zugriff auf das Zertifikat bzw. den privaten Schlüssel benötigen Sie später ein Passwort, welches Sie hier eingeben.

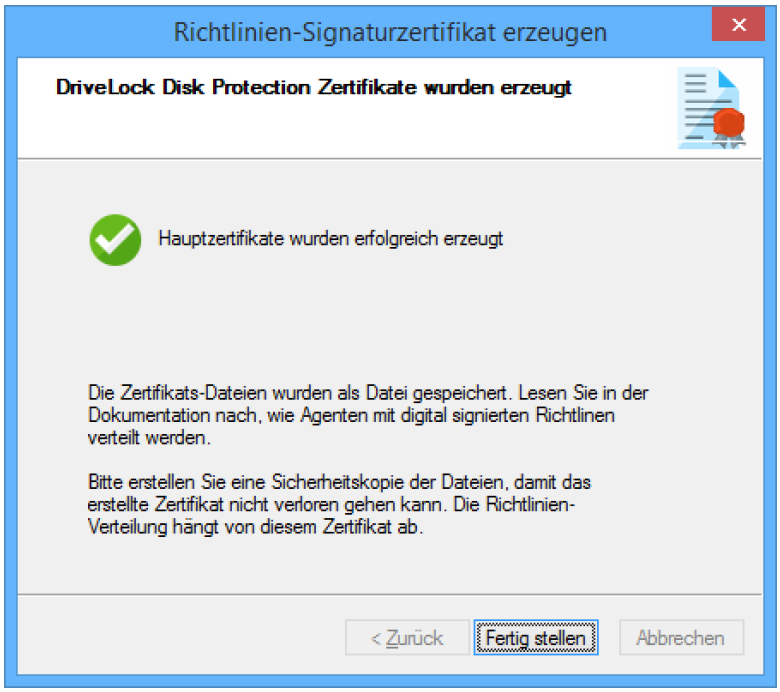


In diesem Schritt können Sie eine oder mehrere Serververbindungen und einen Mandanten konfigurieren, sofern Sie mit mehreren Mandanten arbeiten.

Ebenso können Sie festlegen, dass ein DriveLock Agent, der mit diesem Zertifikat installiert wird, immer eine ganz bestimmte Richtlinie verwendet, unabhängig davon welche Zuweisung Sie in der DriveLock Management Console für die Richtlinien vorgenommen haben.



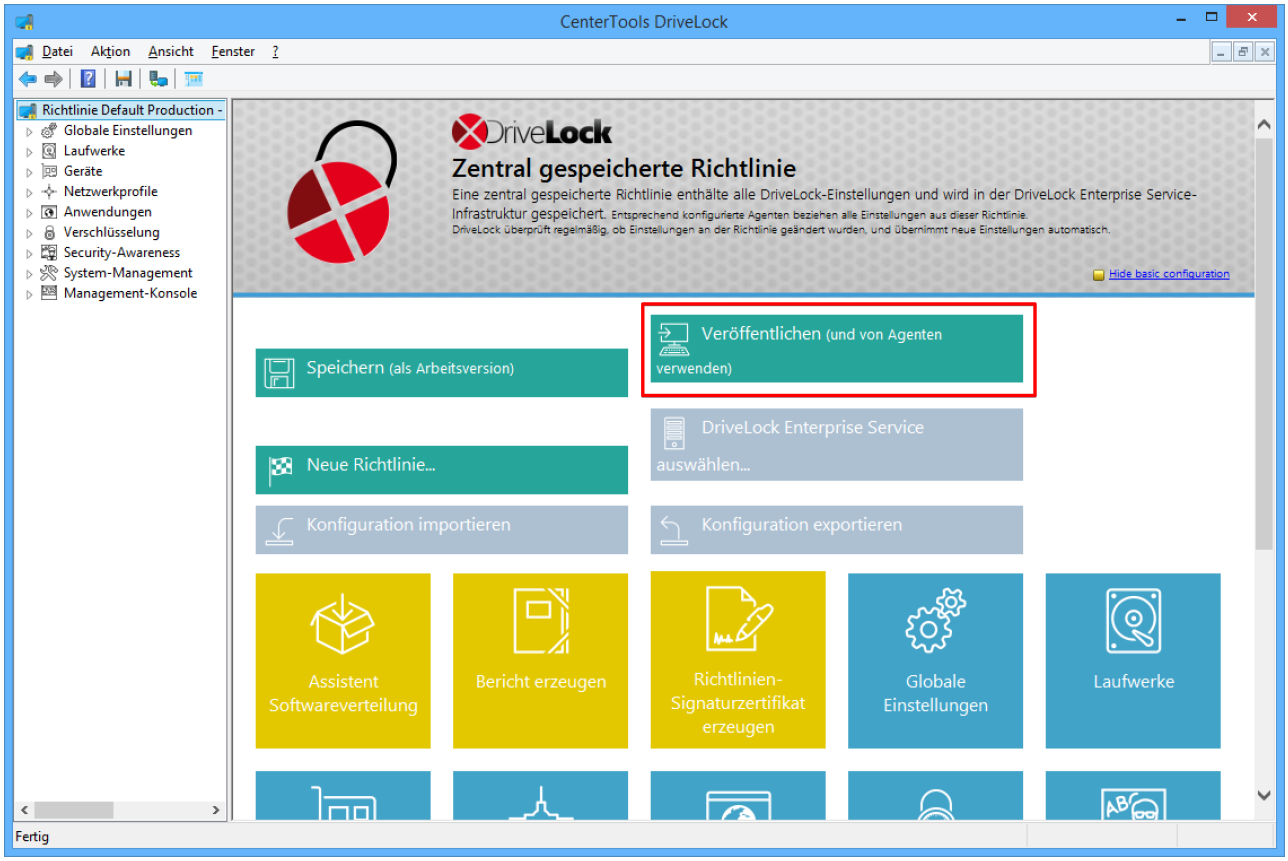
Im letzten Schritt legen Sie fest, ob der mit diesem Zertifikat installierte Agent noch weitere Richtlinien akzeptiert, die mit den hier anzugebenden anderen Zertifikaten signiert wurden.
Außerdem können Sie eine Konfiguration aus einer Konfigurationsdatei hinzufügen, die ein Agent verwendet, solange er keine Richtlinie über einen DES oder eine Gruppenrichtlinie erhält.



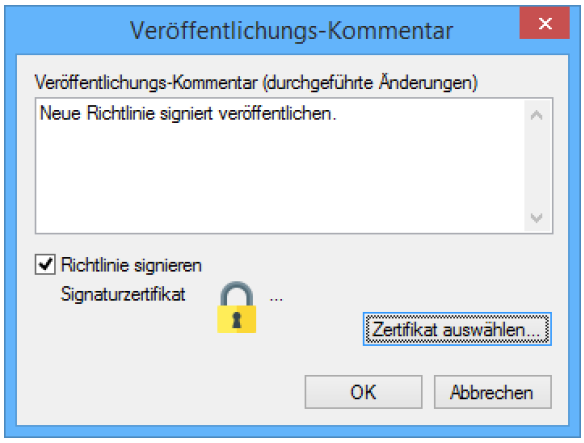
Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

Signieren einer DriveLock Richtlinie

Um eine Richtlinie zu signieren, öffnen Sie diese über die DriveLock Management Console.

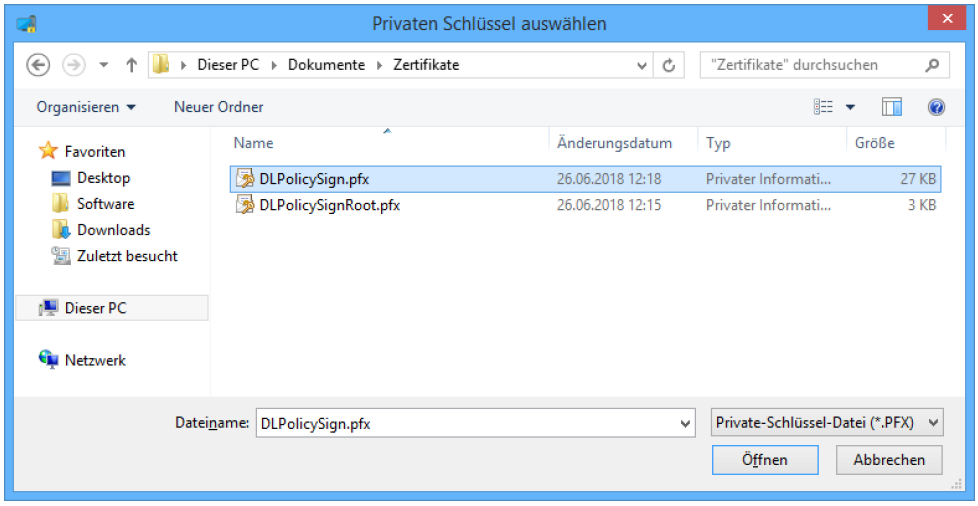


Klicken Sie nun auf **Veröffentlichen (und von Agenten verwenden)**.

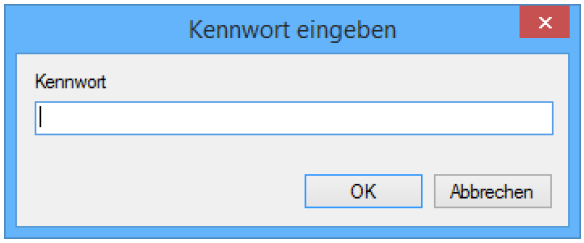


Aktivieren Sie **Richtlinie signieren** und klicken Sie **Zertifikat auswählen**.

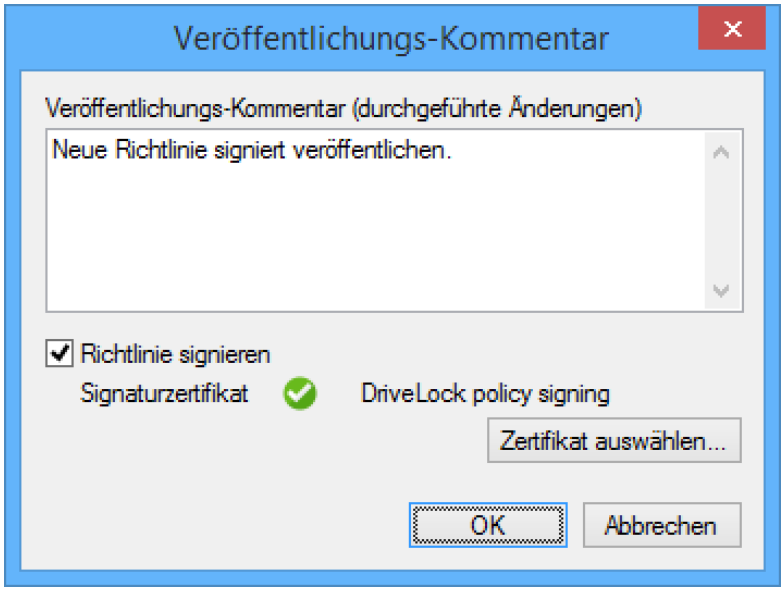
Achten Sie bitte darauf, dass eine Richtlinie jedes Mal signiert werden muss, wenn Sie diese veröffentlichen möchten.



Wählen Sie das zuvor generierte Zertifikat bzw. dessen private Schlüsseldatei aus und klicken Sie **Öffnen**.



Geben Sie nun das bei der Erstellung verwendete Passwort ein und klicken Sie **OK**.



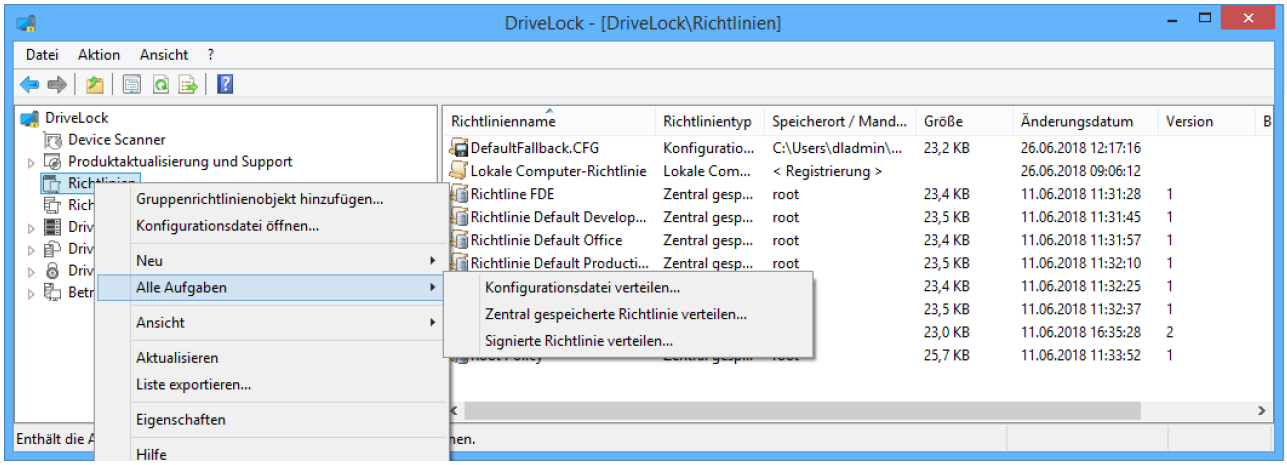
Ein Symbol zeigt Ihnen die erfolgreiche Signatur an.

Klicken Sie auf **OK**, um die jetzt signierte Richtlinie zu veröffentlichen.

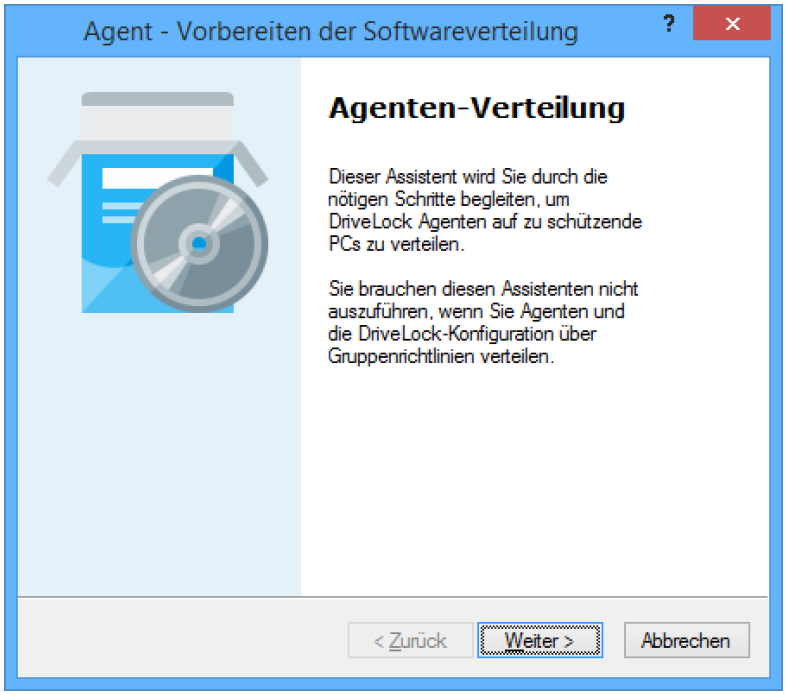
Ein Agent, der so konfiguriert wurde, dass er nur noch signierte Richtlinien akzeptiert, wird nicht signierte Richtlinien nicht beachten und deren Einstellungen nicht anwenden. Alle anderen Agenten verarbeiten sowohl nicht-signierte als auch signierte Richtlinien.

Installation eines DriveLock Agenten mit einem Policy-Zertifikat

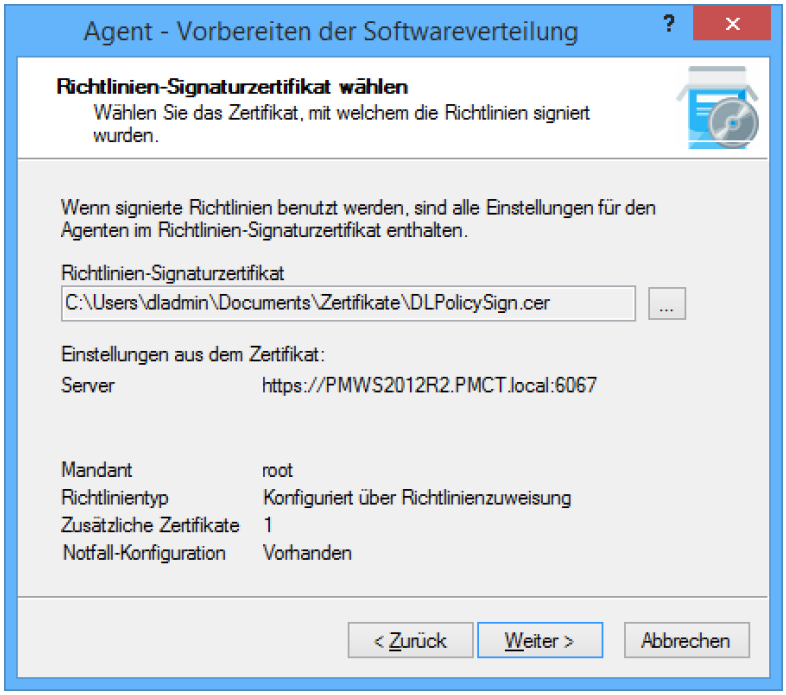
Öffnen Sie die DriveLock Management Console, rechts-klicken Sie **Richtlinien** und wählen Sie **Alle Aufgaben -> Signierte Richtlinie verteilen**, um den Agenten der Softwareverteilung zu starten:



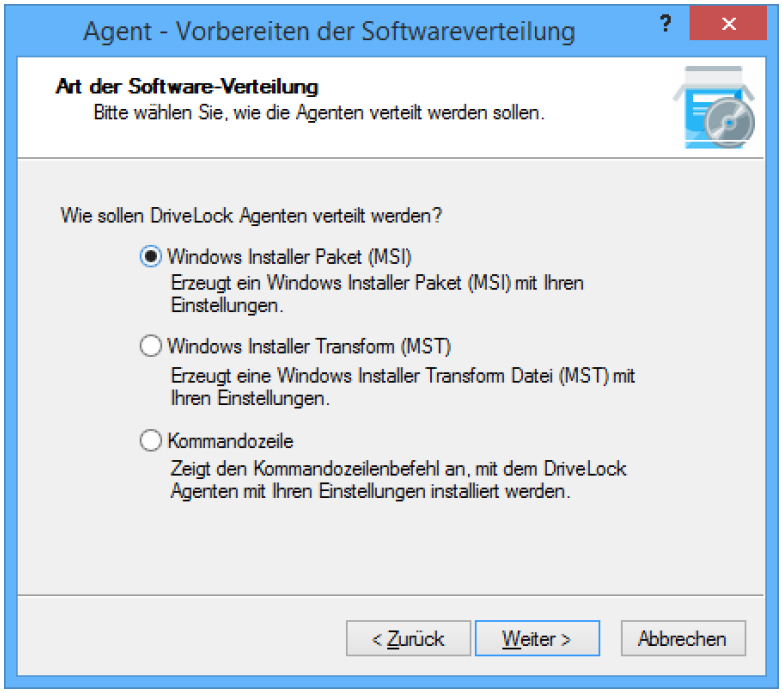
Mit Hilfe dieses Assistenten erzeugen Sie ein präpariertes Installationspaket, welches Sie anschließend für die Installation der DriveLock Agenten in Ihrem Netzwerk verwenden können.



Klicken Sie **Weiter**.



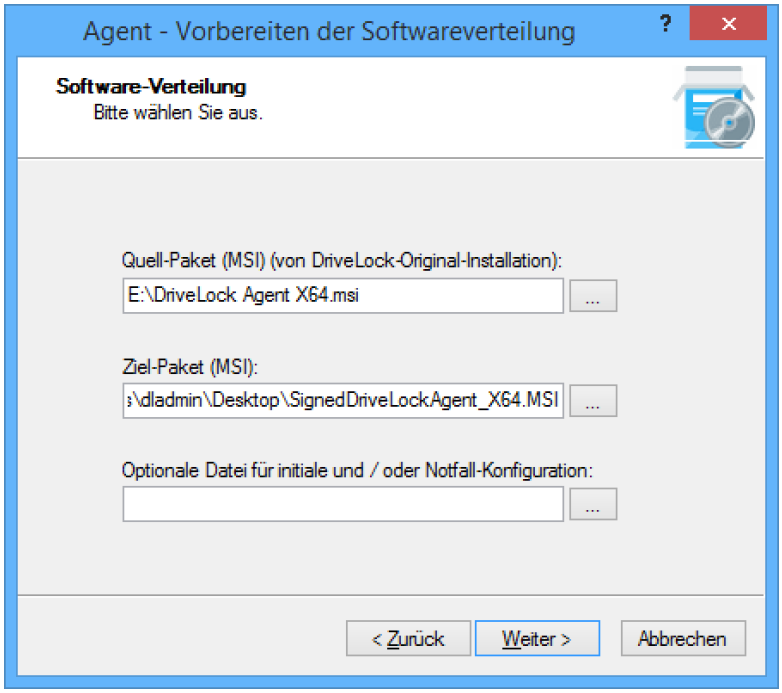
Klicken Sie "**...**" und wählen Sie das Richtlinien-Signaturzertifikat aus, mit dem die DriveLock Richtlinie signiert wurde. Nach der Auswahl werden Ihnen die im Zertifikat gespeicherten Informationen angezeigt. Klicken Sie anschließend auf **Weiter**.



Wählen Sie nun die Art des Installationspakets, das vom Wizard erstellt werden soll:

- *Windows Installer Paket (MSI)*: Erstellt ein neues Microsoft Installer Paket, das die zuvor spezifizierten Einstellungen enthält.
- *Windows Installer Transform (MST)*: Erstellt eine Microsoft Installer Transform (MST) Datei mit den gewählten Einstellungen. Eine MST-Datei kann zusammen mit dem Original-MSI-Paket verwendet werden, das in der DriveLock Installation enthalten ist.

- *Kommandozeile*: Zeigt die Kommandozeilen-Syntax mit den gewählten Einstellungen für den Microsoft Installer an.



Optional können Sie auch an dieser Stelle noch eine Notfall-Konfiguration hinzufügen, sofern Sie diees nicht bereits innerhalb des Zertifikates hinzugefügt hatten.

Klicken Sie auf **Weiter**.

Klicken Sie **Fertig stellen**, um den Assistenten zu schließen. Sie können nun das generierte Installationspaket z.B. über die Softwareverteilung Ihres Unternehmens verteilen.

Alternativ können Sie einen DriveLock Agenten (mit einem unveränderten MSI-Paket) auch über die Kommandozeile installieren und dort die notwendigen Parameter für die Verwendung des Richtlinien-Signaturzertifikates angeben:

```
msiexec /I <DriveLockAgent.msi> /qb USESIGNCERT=1
POLSIGNCERT="<PATHTOCERTIFICATE>\<PolicySigningCertificate>.cer"
```

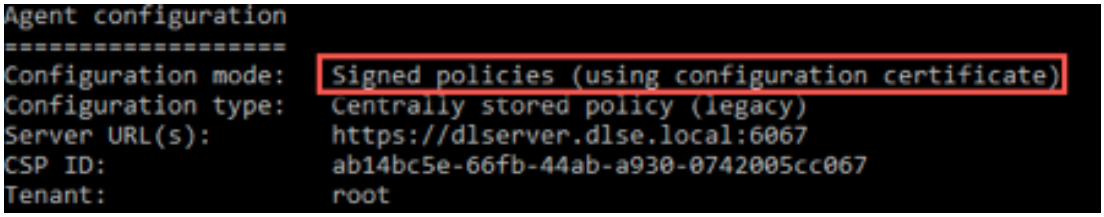

Wenn Sie einen bereits installieren Agenten umkonfigurieren möchten, dass er nur noch mit einem bestimmten Zertifikat signierte Richtlinien akzeptiert, können Sie das mit folgenden Kommandozeilenbefehl bewerkstelligen:

```
drivelock -setconfigcert "<PATHTOCERTIFICATE>\<PolicySigningCertificate>.cer"
```

Bitte beachten Sie, das ein Agent keine nicht-signierten Richtlinien mehr akzeptiert, sobald er einmal zusammen mit einem Signaturzertifikat installiert oder per Kommandozeilenbefehl auf signierte Richtlinien umgestellt wurde! Aus Sicherheitsgründen ist eine Deaktivierung dieser Prüfung nicht mehr möglich!

Sie können mit Hilfe des folgenden Kommandozeilenbefehls den Status der aktuellen Agenten-Konfiguration überprüfen:

```
drivelock -showstatus
```



5.4.5 Installation mit Kommandozeilenparametern (unbeaufsichtigte Installation)

Bei der Installation des Agenten über eine Kommandozeile bzw. ein Skript können zusätzliche Optionen angegeben werden. Dies ermöglicht ebenfalls die Angabe, von wo der Agent seine Konfigurationseinstellungen erhält und wie auf diese zugegriffen wird.

Das **DriveLockAgent.msi** Paket für den DriveLock Agenten befindet sich innerhalb der ISO-Datei (welches auf eine CD gebrannt werden kann) oder kann durch den DriveLock Installer heruntergeladen werden.

Für die unbeaufsichtigte Installation ohne Anzeige des Installationsassistenten und mit Standardeinstellungen kann folgende Syntax verwendet werden:

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

Nachfolgendes Beispiel zeigt eine Installation mit eigenen Parametern:

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

Verfügbare Optionen bei Konfiguration des DriveLock Agenten über eine zentral gespeicherte Richtlinie:

USESERVERCONFIG=1	Angabe, dass eine zentral gespeicherte Richtlinie zum Einsatz kommt.
CONFIGID=<GUID>	<GUID> ist die GUID der zentral gespeicherten Richtlinie in der Form: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
CONFIGSERVER=<name>	<name> ist der Servername, auf dem der DriveLock Enterprise Service installiert wurde und von dem die Richtlinie geladen werden soll.

TENANTNAME=<tenant>	<tenant> ist der Mandanten-Name, für den die Richtlinie gelten soll. Haben Sie keine Mandanten konfiguriert, verwenden Sie bitte „**root**“ als Mandanten-Name.

Verfügbare Optionen bei Konfiguration des DriveLock Agenten über eine Konfigurationsdatei:

USECONFIGFILE=1	Angabe, dass eine Konfigurationsdatei zum Einsatz kommt.
CONFIGFILE=”<path>”	<path> kann ein gültiger UNC, FTP oder HTTP Pfad zur Konfigurationsdatei sein. Beispiele: UNC: \\myserver\share$\drivelock\dlconfig.cfg FTP: myserver/pub/drivelock/dlconfig.cfg HTTP: http://myserver/drivelock/dlconfig.cfg
CONFIGPROTOCOL=[0|1|2]	0: <path> ist Dateipfad 1: <path> ist FTP Pfad 2: <path> ist HTTP Pfad
USESVCACCT=1	Angabe, dass Benutzerkonto verwendet wird zum Zugriff auf die Konfigurationsdatei.
SVCACCOUNT=<account>	Gibt das Konto zum Zugriff auf die Konfigurationsdatei an. Beispiel: SVCACCOUNT=mydomain\myuser)
SVCPASSWORD=”<encpwd>”	<encpwd> ist das verschlüsselte Passwort, das vom Assistenten generiert wurde.

Benutzen Sie den Assistent Softwareverteilung von zur Erzeugung des verschlüsselten Passworts.

DriveLock Agenten können auch mit der Original *DriveLockAgent.msi* und einer vom Assistenten generierten MST-Datei installiert werden:

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


Teil VI

DriveLock aktualisieren

6 DriveLock aktualisieren

Bitte beachten Sie ggf. zusätzliche Informationen zum Updateprozess von DriveLock in den aktuellen Release-Notes.

Grundsätzlich ist die Aktualisierung der DriveLock Komponenten so einfach wie möglich gehalten und kann in der Regel wie eine Neuinstallation erfolgen.

Seit DriveLock Version 7 gibt es auch eine Auto-Update Funktion, bei der mit Hilfe des DriveLock Enterprise Service alle Agenten und die DriveLock Management-Komponenten in Ihrer Umgebung automatisch auf den neuesten Stand gebracht werden können. Mehr dazu können Sie im entsprechenden Abschnitt des Administrationshandbuches nachschlagen.

DriveLock empfiehlt Ihnen, die folgende Update-Reihenfolge einzuhalten:

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

Die Version des DriveLock Agenten darf kleiner, **aber nie größer sein** als die Version des DriveLock Enterprise Services.

Das DriveLock Control Center und die DriveLock Management Console funktioniert nur mit dem DriveLock Enterprise Service der gleichen Version zuverlässig.

DriveLock führt während der Aktualisierung oder Installation keine Änderungen an irgendwelchen Gruppenrichtlinienobjekten oder Konfigurationsdateien durch. Zur Sicherheit empfehlen wir Ihnen dennoch, vor einem Update alle lokalen oder Gruppenrichtlinien-basierten DriveLock Richtlinien in eine Datei zu exportieren. Weitere Informationen über das Exportieren von Richtlinien erhalten Sie im **DriveLock Administrationshandbuch**.

In den folgenden Abschnitten wird das manuelle Update durch einen Administrator beschrieben. Informationen zum automatischen Update finden Sie im entsprechenden Kapitel des Administrationshandbuches.

6.1 DriveLock Enterprise Service aktualisieren

Um den DriveLock Enterprise Service zu aktualisieren, folgen Sie den Schritten, die im Kapitel *„Installation des DriveLock Enterprise Service“* beschrieben werden. Eine ältere Version des DriveLock Enterprise Service wird automatisch erkannt und aktualisiert. Ebenfalls erfolgt eine Aktualisierung der DriveLock Datenbank.

Stellen Sie bitte sicher, dass Sie ein funktionierendes Backup Ihrer DriveLock Datenbank erstellt haben, bevor Sie das Update durchführen.

Das DES TrayIcon zeigt einmalig einen Hinweis an, sobald eine neue DriveLock DES Version verfügbar ist.

6.1.1 Update mit Kommandozeilenparametern (unbeaufsichtigte Installation)

Der DES lässt sich seit Version 7.8 auch ohne Benutzerinteraktion aktualisieren.

Aktualisierung des Dienstes

Sie benötigen Administrator-Berechtigungen, um den DES per Kommandozeilenbefehl zu aktualisieren.

Wenn Sie eine Microsoft SQL Server Datenbank verwenden, legen Sie vor der Installation des DES den Service Account an, mit dem der DES auf die Datenbank zugreifen soll. Wenn der DES Server nicht auch der Datenbank Server ist, muss das ein Domain Account mit einem Passwort das nicht abläuft sein. Spezielle Berechtigungen sind nicht notwendig. Diesen Benutzer verwenden Sie dann innerhalb des Kommandozeilenbefehls.

Verwenden Sie dazu den folgenden Kommandozeilenbefehl und ersetzen Sie die jeweiligen Werte für den Benutzer und dessen Passwort:

```
run msiexec /qn /quiet /l*v DLInstall.log /i "DES X64.msi"
LOGON_USERNAME="<domain>\<username>" LOGON_PASSWORD="<password>"
CONFIGUREFIREWALL=1 LAUNCHDBWIZARD=0
```

Folgende Kommandozeilenparameter sind zwingend erforderlich:

- LOGON_USERNAME: Der Benutzername des DES Service Accounts
- LOGON_PASSWORD: Das Passwort für den DES Service Account

Diese Kommandozeilenparameter können zusätzlich angegeben werden:

- CONFIGUREFIREWALL:
  - 0 = Der Installer nimmt keine Änderungen an den aktuellen Firewalleinstellungen vor (Standardwert)
  - 1 = Die Firewalleinstellungen werden automatisch um Regeln ergänzt, die die Ports für die Kommunikation mit den Agenten und den Management Komponenten von DriveLock freischalten.
- LAUNCHDBWIZARD:
  - 0 = Nach der Installation wird der DB Installationsassistent nicht automatisch gestartet
  - 1 = Nach der Installation wird der DB Installationsassistent automatisch mit Benutzerinterface gestartet (Standardwert)

Setzen Sie den Wert LAUNCHDBWIZARD auf 0, um auch den DB Installationsassistenten ohne Benutzerinteraktionen wie nachfolgend beschrieben über die Kommandozeile zu starten.

Überprüfen Sie die Log-Datei "DLInstall.log", ob das Update erfolgreich durchgeführt wurde oder ob Fehler aufgetreten sind.

Update der Datenbank

Nach erfolgreichem Update des DES starten Sie den DB Installationsassistenten mit folgendem Befehl:

```
"C:\Program Files\CenterTools\DriveLock Enterprise Service\Database Install
Wizard.exe" "C:\Program Files\CenterTools\DriveLock Enterprise
Service\actions.xml"
```

Die Datei "actions.xml" wird zuvor vom Installationsprogramm des DES automatisch erzeugt.

Überprüfen Sie die Log-Datei "C:\ProgramData\CenterTools DriveLock\Log\DBinstall.log", ob das Update erfolgreich durchgeführt wurde oder ob Fehler aufgetreten sind.

> Wenn Sie nun das Programm "DES Service Status" (Tray Icon) starten, können Sie ebenfalls überprüfen, ob das Update erfolgreich durchgeführt wurde.

6.2 DriveLock Control Center aktualisieren

Das DriveLock Control Center kann aktualisiert werden, in dem die gleichen Schritte wie bei einer Neuinstallation durchgeführt werden. Siehe Abschnitt „Installation der DriveLock Management-Komponenten“.

6.3 DriveLock Management Konsole aktualisieren

Die DriveLock Management Konsole kann direkt auf die neueste Version aktualisiert werden, in dem die gleichen Schritte wie bei einer Neuinstallation durchgeführt werden. Siehe Abschnitt „Installation der DriveLock Management-Komponenten“.

6.4 DriveLock Agenten aktualisieren

Grundsätzlich ist es nicht notwendig, einen vorhandenen Agenten vor einem Update zu deinstallieren. Das Update wird wie eine Neuinstallation durchgeführt, welche im Abschnitt „**Installation des DriveLock Agenten**“ beschrieben ist.

Die Aktualisierung der DriveLock Agenten können Sie auch bei installierter Disk Protection vornehmen.

Aktualisierung der DriveLock Disk Protection

Nach dem Update des DriveLock Agenten wird eine ggf. vorhanden Disk Protection ohne Neuverschlüsselung automatisch auf die neueste Version aktualisiert. Danach muss ggf. ein Neustart erfolgen.

Teil VII

DriveLock deinstallieren

7 DriveLock deinstallieren

Falls DriveLock nicht durch eine Gruppenrichtlinie installiert wurde, kann DriveLock über die **Systemsteuerung/Software** deinstalliert werden.

DriveLock Agenten können ferner durch die folgende Kommandozeile deinstalliert werden unter Zuhilfenahme des Original-Installationspakets (MSI):

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

Wenn DriveLock mit einem Passwort für die Deinstallation versehen wurde, sind diese Befehle zu verwenden:

```
msiexec /x DriveLockagent.msi UNINSTPWD=Passwort
msiexec /x DriveLockagent.msi UNINSTPWDENC=Verschlüsseltes Passwort
```

> Um ein verschlüsseltes Passwort zu erstellen, benutzen Sie den DriveLock Assistenten für Softwareverteilung. Darüber hinaus ist es auch möglich, das verschlüsselte Deinstallationspasswort über einer MST-Datei mitzugeben.

Falls der DriveLock Agent mittels Gruppenrichtlinien installiert wurde, kann er nicht über Systemsteuerung/Software deinstalliert werden. Konfigurieren Sie stattdessen die Gruppenrichtlinie so, dass DriveLock nicht mehr zugewiesen wird. Alternativ kann auch die Kommandozeile verwendet werden (dann ist aber sicherzustellen, dass DriveLock von keiner Gruppenrichtlinie mehr zugewiesen wird).

DriveLock Installationshandbuch