DriveLock Administration 2021.2

17.11.2021

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

Hinweise zu diesem Handbuch

2 Hinweise zu diesem Handbuch

Aufgrund der Überarbeitung und Umstrukturierung unserer gesamten Dokumentation finden Sie in diesem Handbuch nur noch Kapitel zu folgenden Themenbereichen: Laufwerks- und Gerätekontrolle, modulübergreifende Einstellungen in Regeln (z.B. Whitelist-Regeln), Netzwerkprofile, Disk Protection (ehemals FDE), File Protection, Encryption 2-Go und Informationen zum Einsatz von DriveLock mit Terminal Servern.

Alle anderen Themen, beispielsweise wie Sie mit der DriveLock Management Konsole oder dem Richtlinien-Editor arbeiten, finden Sie in der Dokumentation DriveLock Administration. Diese steht Ihnen wahlweise als Online-Hilfe oder PDF zur Verfügung.

Außerdem bieten wir für verschiedene Themen eigenständige Dokumentationen an: Application Control, BitLocker Management (beinhaltet auch BitLocker To Go und DriveLock PBA), Defender Management, DOC Companion, DriveLock Events, Linux Agenten, Security Awareness, Self-Service Portal und Vulnerability Scanner. Des weiteren gibt es ein Installationshandbuch und eine Endbenutzerdokumentation.

Die gesamte Produktdokumentation finden Sie auf DriveLock Online Help.

Teil III

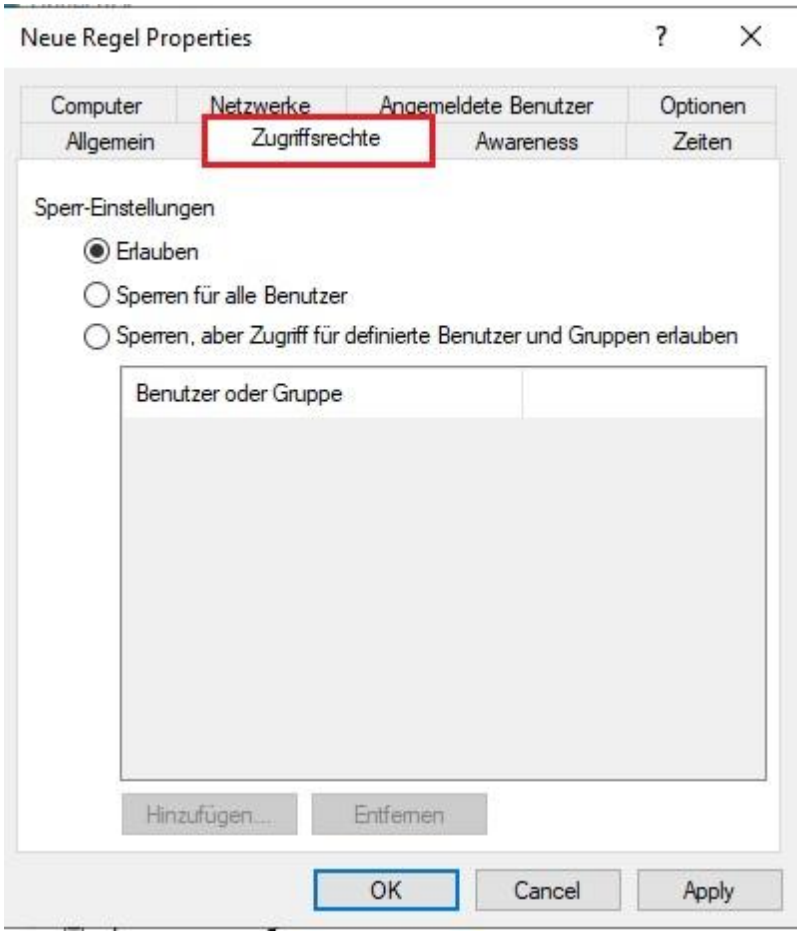
Modulübergreifende Einstellungen in Regeln

3 Modulübergreifende Einstellungen in Regeln

Einige Einstellungen sind modulübergreifend und in den meisten DriveLock-Regeln gleichermaßen verfügbar.

3.1 Zugriffsberechtigungen für Benutzer und Gruppen

Wählen Sie den Reiter „**Zugriffsrechte**“, um festzulegen, welche Benutzer bzw. Gruppen Zugriff auf das Laufwerk erhalten.



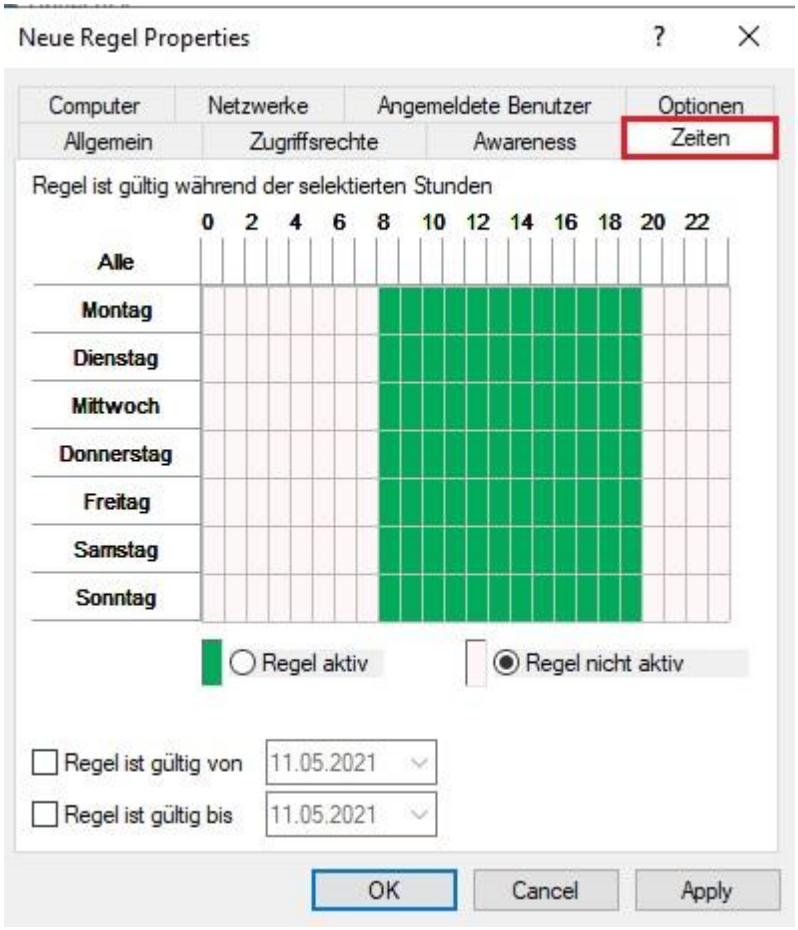
Folgende Möglichkeiten stehen zur Auswahl:

- *Erlauben*: Jeder authentisierte Benutzer kann dieses Laufwerk verwenden
- *Sperren für alle Benutzer*: Der Zugriff auf dieses Laufwerk ist für alle Benutzer gesperrt.
- *Sperren, aber Zugriff für definierte Benutzer und Gruppen erlauben*: Das Laufwerk ist gesperrt, aber Zugriff ist für den oder die angegebenen Benutzer bzw. Gruppen möglich, entweder nur lesend oder auch schreibend.

Klicken Sie auf **Hinzufügen**, um eine weitere Gruppe oder einen Benutzer zur angezeigten Liste hinzuzufügen. Mit **Entfernen** wird der zuvor ausgewählte Eintrag gelöscht. Geben Sie für den Benutzer oder die Gruppe an, ob er/sie Daten auf das Laufwerk kopieren können oder ob nur lesender Zugriff möglich ist.

3.2 Zeitliche Einschränkungen

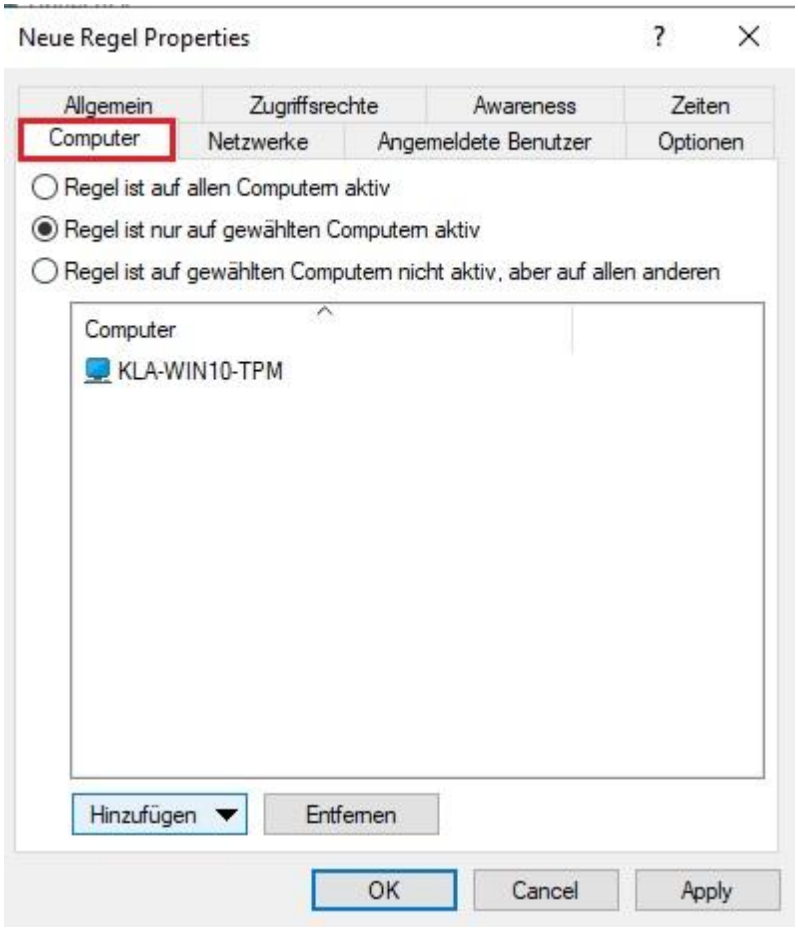
Wenn Sie möchten, dass die Regel nur für einen ganz bestimmten Zeitraum gelten soll, dann können Sie hier einen individuellen Zeitrahmen vorgeben (z.B. nur werktags von 09:00 Uhr bis 17:00 Uhr) Es ist ebenso möglich, ein Datum für den Beginn und das Ende der Gültigkeitsdauer anzugeben.



Markieren Sie den gewünschten Zeitraum, indem Sie entweder ein einzelnes Feld aktivieren, oder jeweils links einen Wochentag oder oben eine Zeit anklicken. Zusätzlich wählen Sie für die Auswahl entweder „**Regel aktiv**“ oder „**Regel nicht aktiv**“.

3.3 Computer Gültigkeitsbereich

Über den Reiter "**Computer**" legen Sie fest, auf welchen Computern die Whitelist-Regel gültig sein soll.



Wählen Sie eine der folgenden Möglichkeiten:

- Die Regel gilt für alle Computer
- Die Regel gilt nur für die aufgelisteten Computer
- Die Regel gilt für alle außer den aufgelisteten Computern

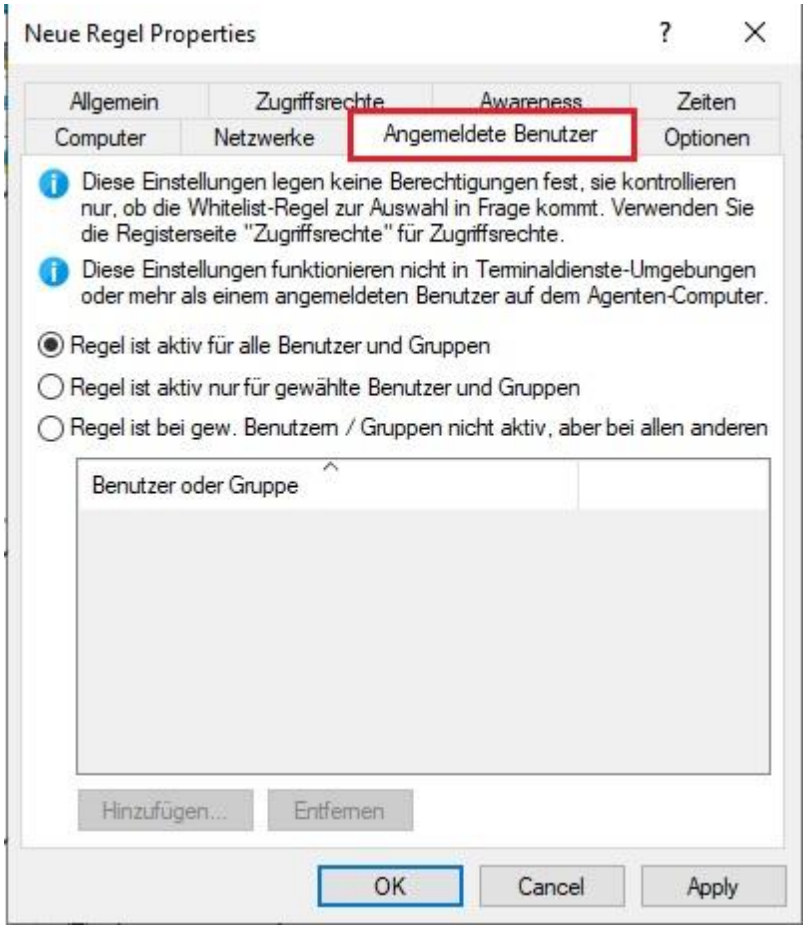
Klicken Sie auf **Hinzufügen**, um weitere Rechner der Liste hinzuzufügen. Dabei können Sie Computer, Gruppen oder Organisationseinheiten aus dem Active Directory verwenden oder den Namen des Computers direkt eingeben.

Durch **Entfernen** werden zuvor ausgewählte Computer aus der Liste gelöscht.

3.4 Angemeldete Benutzer

Über den Reiter "**Angemeldete Benutzer**" können Sie festlegen, für welche Benutzer bzw. Benutzergruppen die Regel angewendet werden soll.

Die Benutzer- und Gruppenprüfung ist nicht zu verwechseln mit den Berechtigungen, welche über den Reiter "*Zugriffsrechte*" konfiguriert werden. Diese Prüfung bestimmt lediglich, ob diese Regel für den gerade angemeldeten Benutzer überhaupt in Betracht gezogen wird. Erst in diesem Fall wird der Zugriff entsprechend der gesetzten Berechtigungen erlaubt bzw. verweigert.



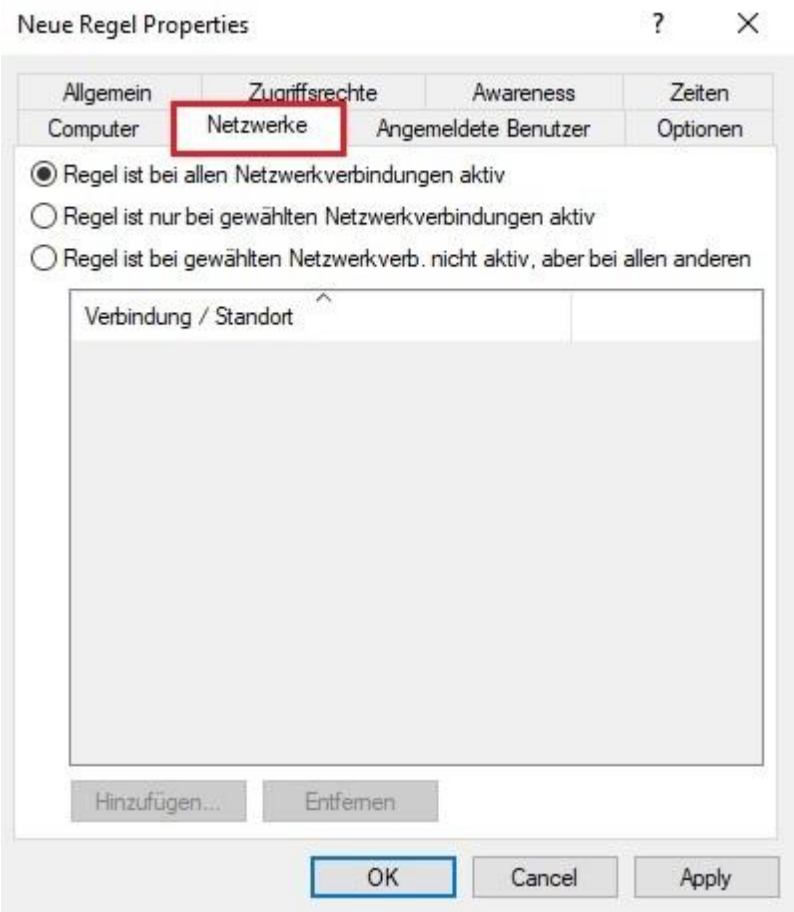
Wählen Sie eine der folgenden Möglichkeiten:

- Die Regel gilt für alle Benutzer
- Die Regel gilt nur für die aufgelisteten Benutzer bzw. Gruppen
- Die Regel gilt für alle außer den aufgelisteten Benutzer bzw. Gruppen

Klicken Sie auf **Hinzufügen**, um weitere Benutzer bzw. Gruppen der Liste hinzuzufügen. Durch **Entfernen** werden zuvor ausgewählte Benutzer bzw. Gruppen aus der Liste gelöscht.

3.5 Netzwerk Profile

Über den Reiter "**Netzwerk**" können Sie festlegen, für welche aktiven Netzwerkverbindungen die Regel angewendet werden soll.



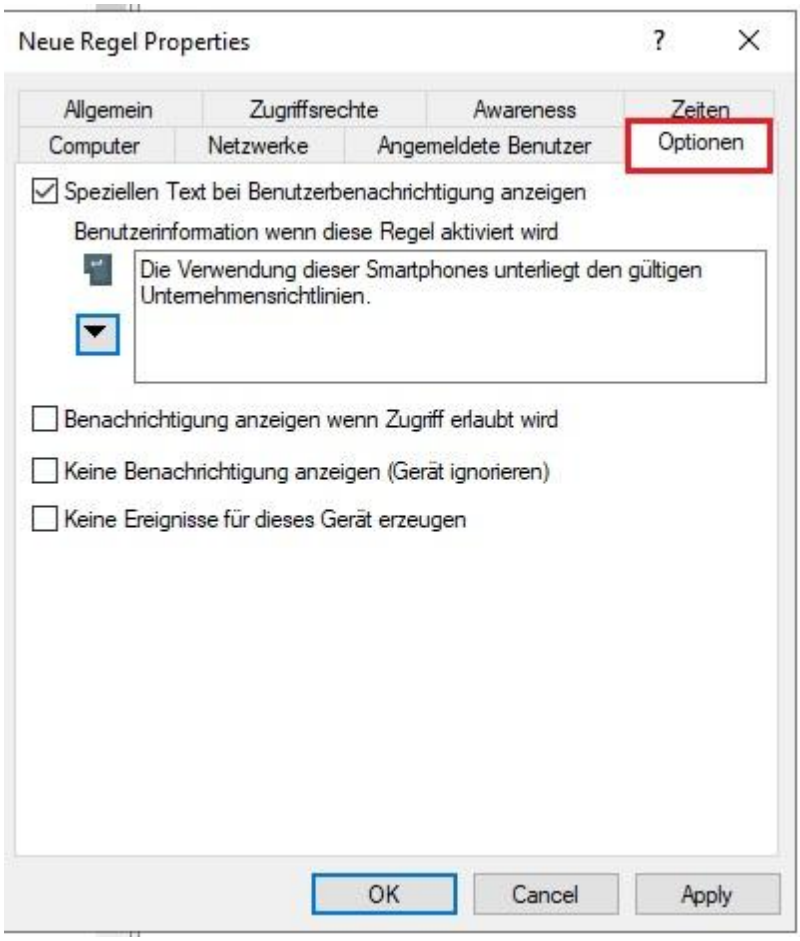
Wählen Sie eine der folgenden Möglichkeiten:

- Die Regel gilt für alle Netzwerkverbindungen
- Die Regel gilt nur für die aufgelisteten Netzwerkverbindungen
- Die Regel gilt für alle außer den aufgelisteten Netzwerkverbindungen

Klicken Sie auf **Hinzufügen**, um weitere Netzwerkverbindungen der Liste hinzuzufügen. Durch **Entfernen** werden zuvor ausgewählte Netzwerkverbindungen aus der Liste gelöscht.

3.6 Weitere Optionen

Sie können für jede Regel eine eigene Benutzermeldung konfigurieren. Sofern nicht anders eingestellt wird diese Meldung den Benutzern gezeigt, wenn der Zugriff auf ein Gerät verweigert wird.



Um eine eigene Meldung für eine Regel zu konfigurieren, aktivieren Sie die Option „**Speziellen Text bei Benutzerbenachrichtigung anzeigen**“. Geben Sie anschließend einen Text ein, welcher unabhängig von der aktuell eingestellten Systemsprache angezeigt wird. Diese sprachunabhängige Meldung wird durch ein Tastensymbol an der linken oberen Ecke des Eingabefeldes dargestellt.

Sofern Sie mehrsprachige Benutzermeldungen definiert haben, können Sie auch eine dieser Nachrichten auswählen. Klicken Sie dazu auf den Pfeil und wählen Sie aus der Liste „**Mehrsprachige Benachrichtigung**“ aus.

Mehrsprachige Meldungen enthalten für eine Nachricht verschiedene Texte für unterschiedliche Sprachen. Bevor Sie mehrsprachige Benutzermeldungen verwenden können, müssen diese im Bereich „**Globale Einstellungen**“ der Richtlinie definiert werden. Wenn Sie eine derartige Meldung verwenden, zeigt DriveLock den Text an, welcher für die aktuelle Systemsprache des angemeldeten Benutzers konfiguriert wurde.

Wählen Sie eine Meldung aus und bestätigen diese mit **OK**.

Diese sprachabhängige Meldung wird durch ein Sprechblasen-Symbol an der linken oberen Ecke des Eingabefeldes dargestellt.

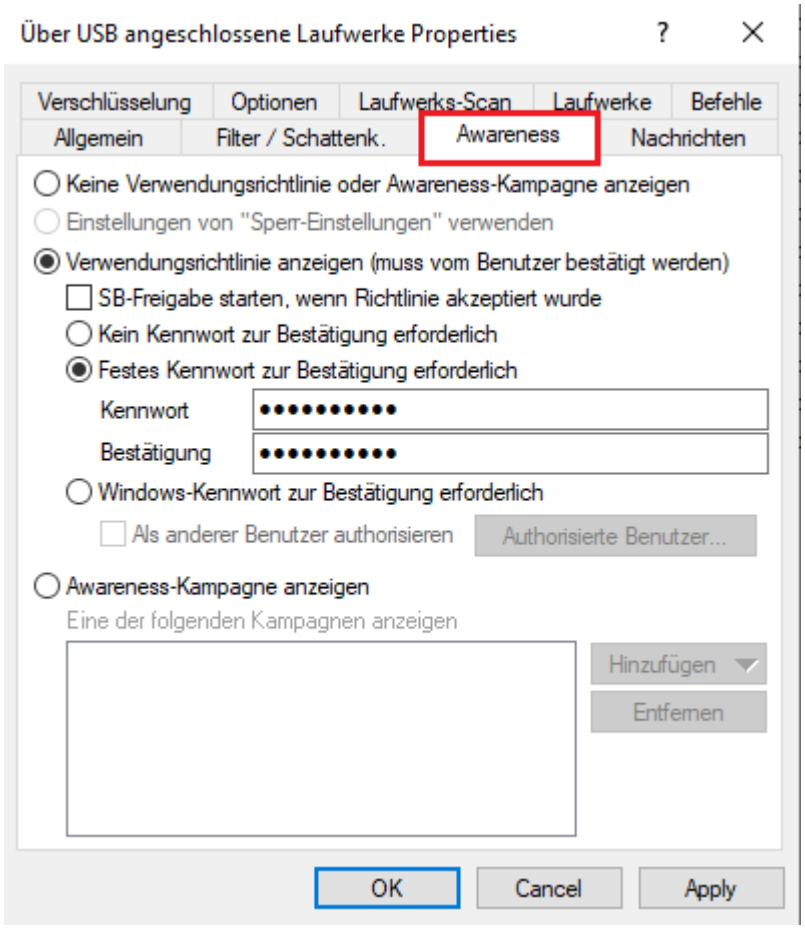
Wenn Sie möchten, dass die Meldung auch dann angezeigt wird, wenn ein Zugriff durch den Benutzer möglich ist, dann aktivieren Sie die entsprechende Option. Sie können auch festlegen, dass dem Benutzer überhaupt keine Meldungen (auch keine Standardnachrichten) angezeigt werden sollen.

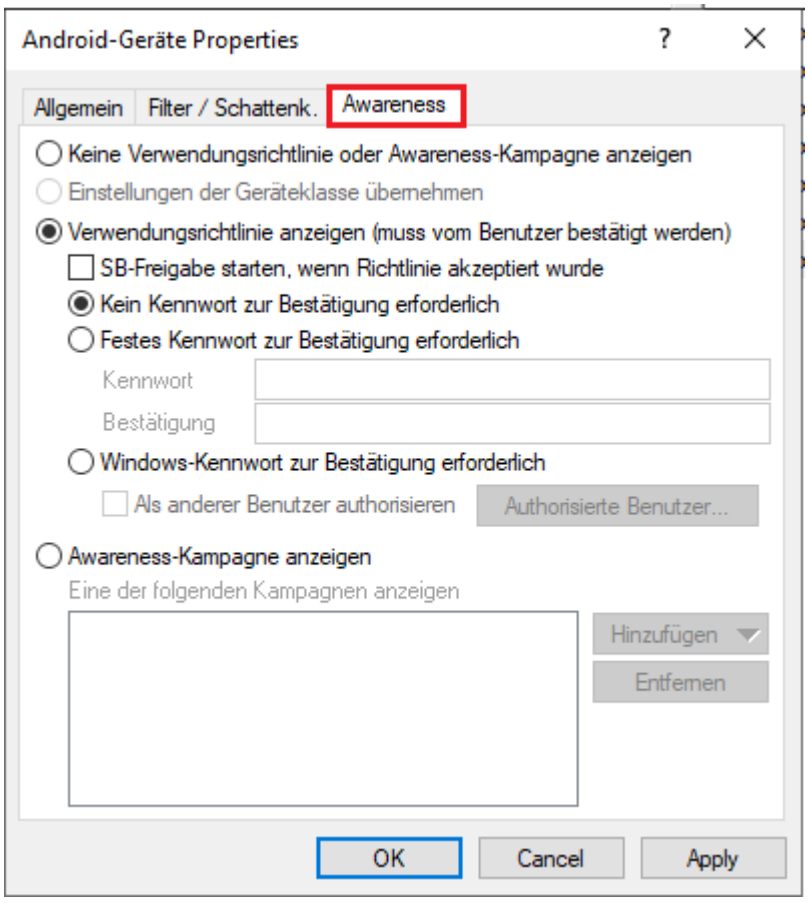
Wenn Sie die Erzeugung von Überwachungsereignissen für diese Whitelist-Regel unterdrücken wollen, markieren Sie bitte „**Keine Ereignisse für dieses Gerät erzeugen**“.

3.7 Awareness

Verwendungsrichtlinie aktivieren

Eine Verwendungsrichtlinie wird an dieser Stelle global für die gesamte Richtlinie erstellt. Aktivieren können Sie diese dann ähnlich wie eine Security Awareness Kampagne innerhalb einer Laufwerks- oder Geräteregel:





Wählen Sie dazu im Tab **Awareness** die Option *Verwendungsrichtlinie anzeigen*.

Folgende Optionen stehen Ihnen noch zur Verfügung:

- SB-Freigabe starten: Nach der Bestätigung der Verwendungsrichtlinie durch den Benutzer wird automatisch der SB-Freigabe Assistent gestartet.
- Festes Kennwort: Geben Sie ein Kennwort vor, welches der Benutzer vor der Freigabe eingeben muss
- Windows-Kennwort: Ist diese Option aktiv, muss der angemeldete Benutzer sein Windows-Kennwort zur Bestätigung eingeben
- Windows-Kennwort und anderer Benutzer: Diese Option erlaubt die Freigabe durch einen anderen als den angemeldeten Benutzer, in dem dieser seinen Benutzernamen und das passende Kennwort eingibt. Optional können Sie dabei die dafür authorisierten Benutzer über die Schaltfläche *Authorisierte Benutzer* festlegen.

Teil IV

Laufwerke und Geräte kontrollieren

4 Laufwerke und Geräte kontrollieren

4.1 Laufwerke kontrollieren

Wie der Produktname schon andeutet, besteht eine wichtige Funktion von DriveLock darin, Laufwerke zu sperren. Dieses Kapitel beschreibt die Möglichkeiten, Schalter und Einstellungen, die es bezogen auf dieses Thema bei DriveLock gibt. Obwohl davon sehr viele zur Verfügung stehen, ist DriveLock trotzdem sehr einfach zu bedienen. Sobald Sie mit den wenigen Grundlagen etwas vertraut sind, stellen auch die anderen nützlichen Funktionen, die für die Anpassung des Produktes an Ihre Anforderungen verwendet werden, kein Problem mehr dar.

Als Beispiel in diesem Handbuch wird eine lokale Richtlinie verwendet, um die nötigen Schritte zum Sperren der USB-Laufwerke, der Freigabe eines USB-Sticks und die Verwendung von Schattenkopien und Dateifiltern zu demonstrieren. Die meisten Schritte gelten analog für alle anderen Laufwerke, Unterschiede werden getrennt davon behandelt.

> Die Konfiguration der Agenten über Gruppenrichtlinien oder andere Wege erfolgt genauso. Außer der unterschiedlichen Verbreitung der Einstellungen gibt es keinen Unterschied.

Es ist wichtig zu verstehen, dass DriveLock das Prinzip von Whitelist-Regeln verwendet. Das bedeutet, dass nach der Aktivierung der grundsätzlichen Sperrung von Laufwerken jedes Laufwerk zunächst gesperrt ist (d.h. die „Firewall“ ist in Betrieb). Jede Ausnahme davon muss getrennt durch eine sog. Whitelist-Regel konfiguriert werden. Das heißt, dass Sie für jedes Laufwerk (bzw. für jede Gruppe von Laufwerken), das verwendet werden soll, eine eigene Regel erstellen müssen. Falls ein Laufwerk nicht über eine entsprechende Regel definiert ist, sperrt DriveLock automatisch den Zugriff darauf und es kann nicht verwendet werden. Damit wird sichergestellt, dass Ihre Sicherheitsrichtlinie intakt bleibt, auch wenn zwischenzeitlich neue und noch mächtigere Geräte entwickelt und durch Ihre Benutzer verwendet werden.

Um eine DriveLock Konfiguration durchzuführen, ist es aufgrund dieses Grundprinzips angeraten, zunächst benötigte Whitelist-Regeln zu erstellen und anschließend das Sperren von Laufwerken zu aktivieren.

Laufwerke wie zum Beispiel USB-Sticks werden ohne eine vorhandene Konfiguration standardmäßig gesperrt. Diese Standardeinstellung wird dann angewendet, wenn Sie einen DriveLock Agenten ohne zuvor konfigurierte und verteile Richtlinie auf einem Arbeitsplatzrechner installieren.

DriveLock bietet die Möglichkeit, Laufwerksregeln für unterschiedliche Geltungsbereiche zu definieren (beginnend mit dem weitreichendsten):

- Laufwerksklassen (z.B. alle Floppy Disk Laufwerke)
- Laufwerksgröße (z.B. alle Laufwerke mit einer Kapazität größer 128 MB)
- Hersteller (z.B. SanDisk)
- Produkt ID (z.B. Ultra II 1 GB Compact Flash)
- Seriennummer

Zusätzlich zum Geltungsbereich kann definiert werden, wann und wo eine Whitelist-Regel angewendet werden soll:

- Auf welchen Computern (alle oder nur bestimme) soll die Regel gelten?
- Für welche aktiven Netzwerkverbindungen soll sie gelten?
- Zu welcher Zeit (z.B. Montag bis Freitag zwischen 09:00 und 18:00 Uhr)?
- Soll eine Regel für alle Benutzer gelten, oder kann eine bestimmte Gruppe ein Laufwerk (oder Gerät) verwenden, während es für alle anderen gesperrt ist?

- Muss der Benutzer einer Unternehmensrichtlinie zustimmen, bevor er Zugriff erhält?
- Ist der angesteckte USB-Stick verschlüsselt?
- Ist der Virenscanner-Dienst aktiv?
- Welcher Benutzer ist gerade angemeldet?
- Enthält der USB-Stick Malware?

Mit der Verwendung dieser Geltungsbereiche (und anderen Mechanismen wie z.B. „Computervorlagen, die später erklärt werden), kann die Anzahl der benötigten Regeln in Ihrer Konfiguration minimiert werden.

Ein Schritt, der durchgeführt werden muss, ist die generelle Aktivierung der Geräte- bzw. Laufwerkssperre. Dieser wird im Abschnitt „Laufwerkssperre aktivieren“ beschrieben.

Wenn Sie DriveLock evaluieren, dürften Sie wahrscheinlich zuerst die generelle Sperrung aktivieren (z.B. mit dem Konfigurationsassistenten), bevor Sie beginnen, einzelne Regeln zu konfigurieren. In einer Produktionsumgebung sollten jedoch zuerst alle notwendigen Regeln erstellt werden, bevor Sie die Sperrung sozusagen „scharf schalten“.

Zwischen DriveLock und einer bestimmten Microsoft Gruppenrichtlinie kann es zu einer Inkompatibilität kommen. Dabei handelt es sich um drei Einstellungen in den sogenannten Sicherheitseinstellungen. Die Inkompatibilität macht sich dadurch bemerkbar, dass über USB angeschlossene Datenträger von DriveLock nicht gesperrt werden können.

Es handelt sich um folgende Einstellungen in einer Gruppenrichtlinie, zu finden unter „Computerkonfiguration/Windows-Einstellung/Sicherheitseinstellung/Lokale Richtlinien/Sicherheitsoptionen“

- Geräte: Formatieren und Auswerfen von Wechseldatenträgern zulassen = Administratoren und Hauptbenutzer / Administratoren und interaktive Benutzer.
- Geräte: Zugriff auf CD-ROM Laufwerke auf lokal angemeldete Benutzer beschränken = Aktiviert
- Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken = Aktiviert

DriveLock erkennt diese Microsoft Gruppenrichtlinien-Einstellungen und meldet diese im Ereignisprotokoll.

Es wird empfohlen, die folgenden Werte bei den folgenden Standard-Einstellungen zu belassen:

- Geräte: Formatieren und Auswerfen von Wechseldatenträgern zulassen = Administratoren
- Geräte: Zugriff auf CD-ROM Laufwerke auf lokal angemeldete Benutzer beschränken = Deaktiviert
- Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken = Deaktiviert

4.1.1 Laufwerke in der Basiskonfiguration sperren

Über die Basiskonfiguration können Sie auf einfache Weise grundsätzliche Sperren aktivieren bzw. deaktivieren und erste Whitelist-Regeln erstellen.

Klicken Sie auf **Laufwerke** im linken Navigationsbaum, um zu den Laufwerkseinstellungen zu wechseln.

Die Ansicht ist in zwei Sektionen unterteilt:

1. Sperr-Einstellungen: Hier können Sie grundlegende Einstellungen für die verschiedenen Geräteklassen festlegen.
2. Whitelist-Regeln: Hier erstellen Sie Whitelist-Regeln, die Ausnahmen von den Geräteklassen-Einstellungen für einzelne Laufwerke (z.B. ein ganz bestimmter USB-Stick) darstellen.

Wenn Sie in den verschiedenen Bereichen auf Erweiterte Konfiguration klicken, können Sie detailliertere und weitreichendere Einstellungen zur Laufwerkskontrolle vornehmen (siehe auch Kapitel „Erweiterte Einstellungen zum Sperren von Laufwerken“).

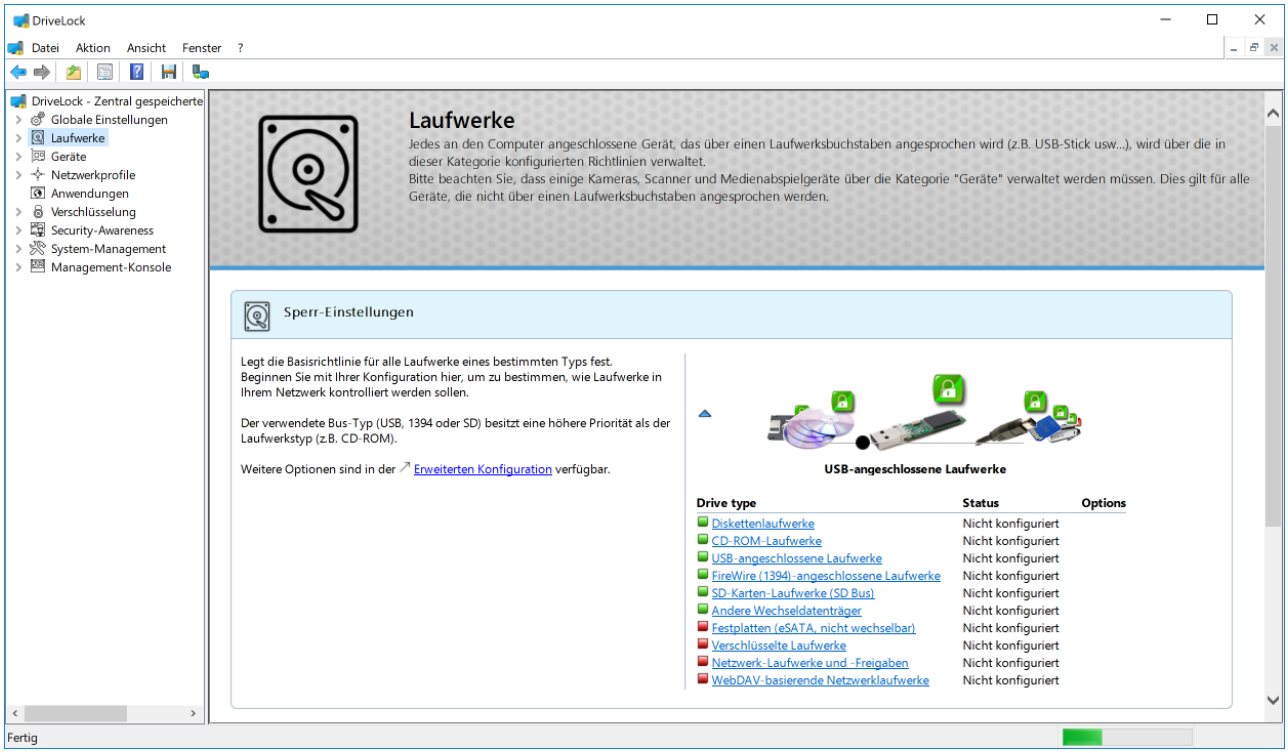
4.1.1.1 Laufwerkssperre aktivieren

DriveLock ist in der Lage, alle Laufwerke zu kontrollieren, die Windows entweder als Wechseldatenträger oder feste Laufwerke erkennen kann. Dies beinhaltet insbesondere die folgenden Klassen:

- Diskettenlaufwerke
- CD-ROM/DVD Laufwerke
- USB-angeschlossene Laufwerke
- Über Firewire (1394) angeschlossene Laufwerke
- SD-Karten-Laufwerke
- Festplatten (z.B. auch eSATA Festplatten)
- WebDAV-basierende Laufwerke
- Netzwerk-Laufwerke und -Freigaben

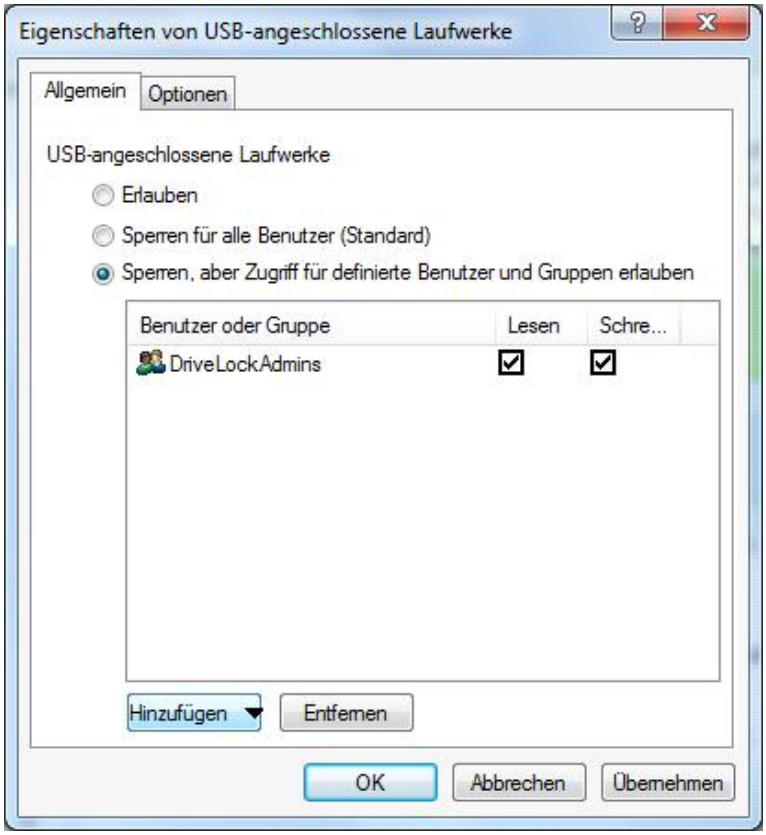
Festplatten, die für Windows die Systemplatte darstellen und Partitionen mit Pagefile werden von DriveLock nicht gesperrt.

Sofern ein Laufwerk über eine andere Schnittstelle verbunden wird, behandelt DriveLock dieses als vom Typ „**Andere Wechseldatenträger**“.



Um die Einstellungen für einen Laufwerkstyp zu ändern (z.B. für USB-angeschlossene Laufwerke), klicken Sie auf den entsprechenden Link. Sie können auf den Ziehregler (schwarzer Punkt) verwenden, das gewünschte Gerät in den Vordergrund holen und anschließen darauf doppelklicken.

Es erscheint ein Dialog, welches die aktuelle Konfiguration anzeigt.

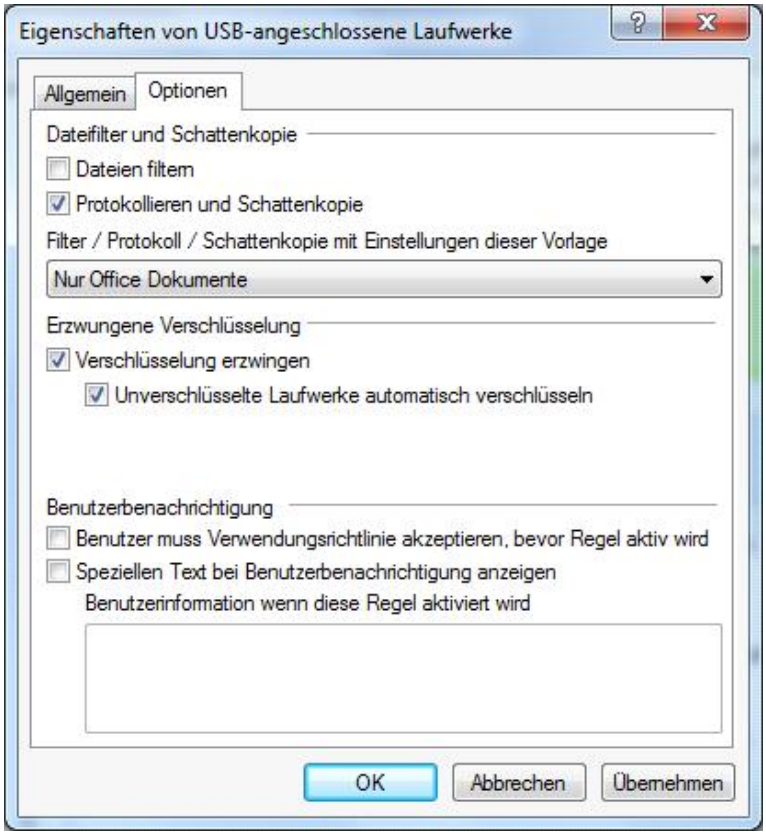


Folgende Möglichkeiten stehen zur Auswahl:

- *Erlauben*: Jeder authentisierte Benutzer kann dieses Laufwerk verwenden
- *Sperren für alle Benutzer*: Der Zugriff auf dieses Laufwerk ist für alle Benutzer gesperrt.
- *Sperren, aber Zugriff für definierte Benutzer und Gruppen erlauben*: Das Laufwerk ist gesperrt, aber Zugriff ist für den oder die angegebenen Benutzer bzw. Gruppen möglich, entweder nur lesend oder auch schreibend.

Klicken Sie auf **Hinzufügen**, um eine weitere Gruppe oder einen Benutzer zur angezeigten Liste hinzuzufügen. Mit **Entfernen** wird der zuvor ausgewählte Eintrag gelöscht. Geben Sie für den Benutzer oder die Gruppe an, ob er/sie Daten auf das Laufwerk kopieren können oder ob nur lesender Zugriff möglich ist.

Wählen Sie nun der Reiter „Optionen“.



Markieren Sie “**Dateien filtern**” bzw. „**Protokollieren und Schattenkopie**“, um die Dateifilterung und die ausgewählten Vorlagen einzuschalten. Wählen Sie aus der Liste einen der mitgelieferten Dateifilter-Vorlagen aus, die Ihnen im Einsteiger Modus zur Verfügung stehen.

Sie können, indem Sie “**Verschlüsselung erzwingen**” aktivieren, spezifizieren, dass jedes der betroffenen Geräte nur dann freigegeben wird, wenn es zuvor verschlüsselt wurde. Zusätzlich lässt sich festlegen, dass unverschlüsselte Laufwerke automatisch verschlüsselt werden.

Um zu erzwingen, dass ein Benutzer zunächst die Verwendungsrichtlinie bestätigen muss, aktivieren Sie die Option „**Benutzer muss Verwendungsrichtlinie akzeptieren, …**“.

Um eine eigene Meldung für eine Regel zu konfigurieren, aktivieren Sie die Option „**Speziellen Text bei Benutzerbenachrichtigung anzeigen**“. Geben Sie anschließend einen Text ein, welcher unabhängig von der aktuell eingestellten Systemsprache angezeigt wird.

Klicken Sie **OK**, um die Einstellungen zu speichern.

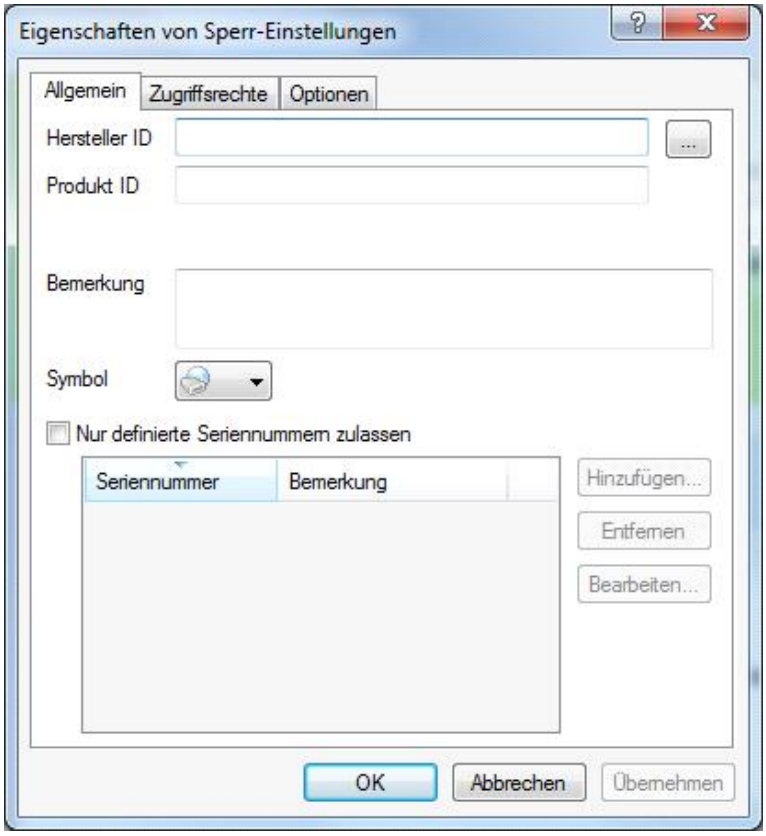
Im Popup-Fenster werden die geänderten Einstellungen nun angezeigt. Klicken Sie auf das Symbol ✖, um das Popup-Fenster zu schließen. Verwenden Sie die kleinen blauen Pfeilsymbole ▾ und ▴, um die Laufwerksdetails ein- bzw. auszuschalten.

Das Symbol des jeweiligen Laufwerkstyps zeigt den jeweiligen Sicherheitslevel der gerade aktuellen Konfiguration an:

- Grünes Symbol: dieser Laufwerkstyps ist für alle Benutzer gesperrt (hoher Sicherheitslevel)
- Gelbes Symbol: dieser Laufwerkstyps ist für einige Benutzer gesperrt und für andere freigegeben (mittlerer Sicherheitslevel)
- Rotes Symbol: dieser Laufwerkstyps ist für alle Benutzer freigegeben (niedriger Sicherheitslevel)

4.1.1.2 Einfache Laufwerksregeln definieren

Klicken Sie auf den Link **Whitelist-Regel erstellen**, um eine neue Whitelist-Regel anzulegen.



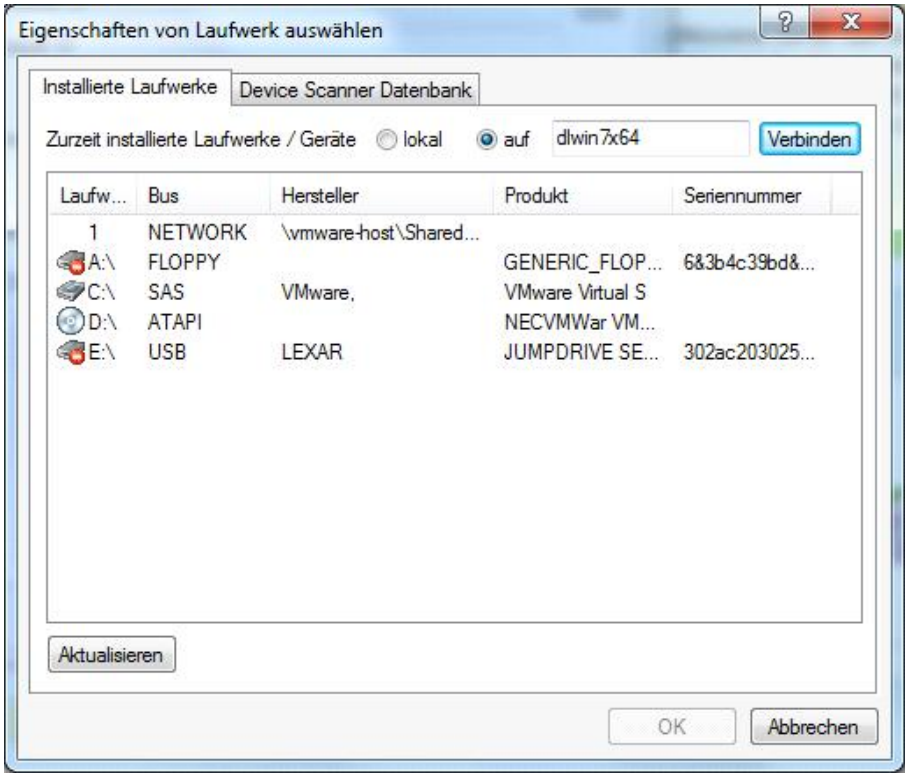
Jedes Laufwerk enthält einige Informationen über die zugrunde liegende Hardware (z.B. Name des Herstellers und des Produktes).

- Hersteller ID: Name oder Abkürzung des Laufwerksherstellers
- Produkt ID: Einzigartige ID des Produktes, vergeben durch den Hersteller

Sie können auch ein gerade verbundenes Gerät auswählen, in dem Sie den Button "**...**" neben dem Herstellerfeld klicken. Eine Seriennummer wird dabei automatisch hinzugefügt, wenn Sie vorher „**Nur definierte Seriennummern zulassen**" aktivieren.

> Sowohl bei der Produkt ID als auch bei der Hersteller ID ist es möglich, folgende Platzhalter zu verwenden: "*" (mehrere Zeichen) und "?" (genau ein Zeichen).

Auch andere Seriennummern können festgelegt werden, in dem Sie auf Hinzufügen klicken und die Seriennummer eingeben. Dabei können wiederum auch Platzhalter („?" oder „*" verwendet werden).



Weitere Laufwerke können ausgewählt werden, in dem Sie sich auf einen anderen Agent per Remote-Verbindung verbinden und ein dort vorhandenes Laufwerk auswählen Wählen Sie dazu „**auf**“ aus und geben Sie den Namen des Computers ein, mit dem Sie sich verbinden möchten. Dazu muss auf dem Zielcomputer der DriveLock Agent installiert sein.

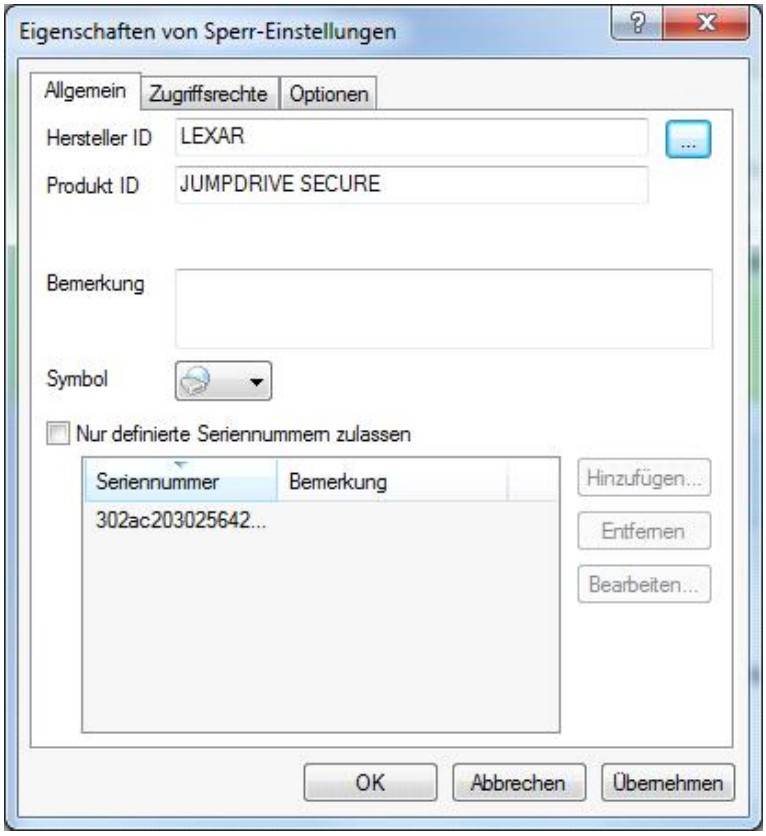
> DriveLock liest die Hardware-Information aus dem Windows Betriebssystem aus. Daher kann DriveLock nur diejenigen Laufwerke anzeigen, die auch im Windows Betriebssystem angezeigt werden.

Um eine Remote-Verbindung zu erstellen, muss (falls vorhanden) die Windows Firewall so konfiguriert sein, dass eingehende Verbindungen über den Ports 6064 bzw. 6065 (voreingestellter Wert) und das Programm „DriveLock“ zugelassen sind.

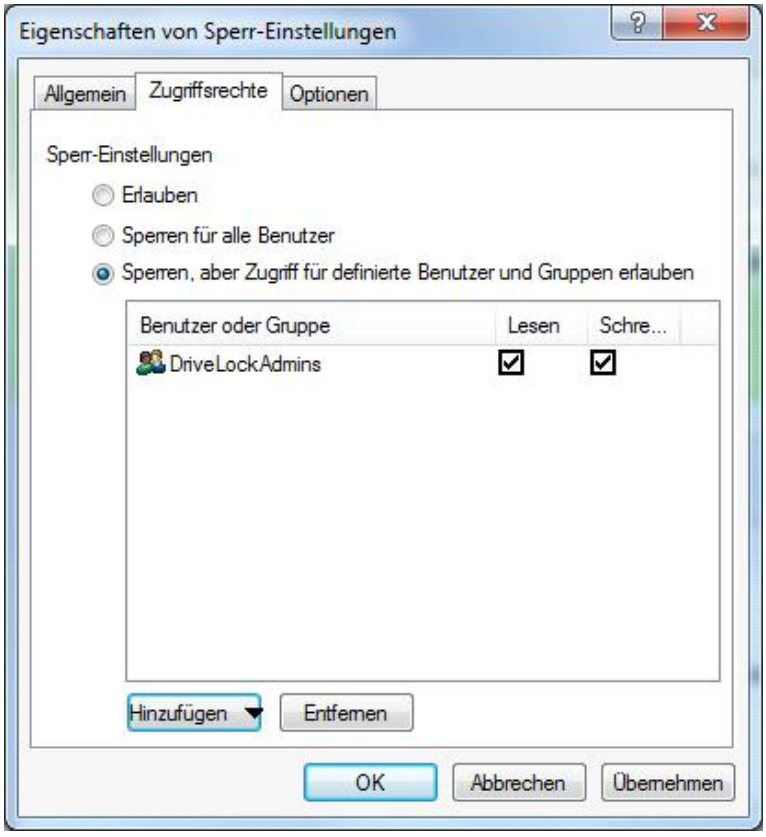
> Wenn Sie sich mit dem lokalen Computer verbinden, werden geblockte Laufwerke nicht angezeigt. Um dies zu umgehen, wählen Sie „auf“ aus und geben den Namen des lokalen Computers ein.

Eine weitere und sehr einfache Möglichkeit, die notwendigen Informationen zu Laufwerken zu erhalten, besteht darin, sich die Ergebnisse in der Device Scanner Datenbank anzusehen. Wählen Sie dazu den „**Device Scanner Datenbank**“ Reiter und anschließend die gewünschten Computer, Hersteller und Produkte aus.

Wählen Sie ein Laufwerk aus und klicken auf **OK**.



Wählen Sie den Reiter „**Zugriffsrechte**“, um festzulegen, welche Benutzer bzw. Gruppen Zugriff auf das Laufwerk erhalten.

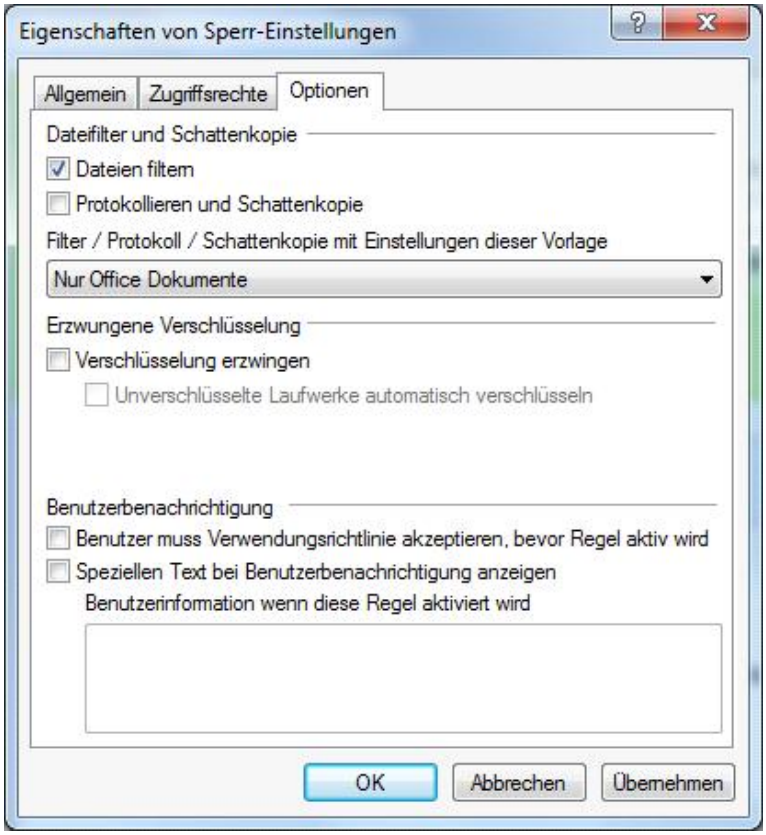


Folgende Möglichkeiten stehen zur Auswahl:

- *Erlauben*: Jeder authentisierte Benutzer kann dieses Laufwerk verwenden
- *Sperren für alle Benutzer*: Der Zugriff auf dieses Laufwerk ist für alle Benutzer gesperrt.
- *Sperren, aber Zugriff für definierte Benutzer und Gruppen erlauben*: Das Laufwerk ist gesperrt, aber Zugriff ist für den oder die angegebenen Benutzer bzw. Gruppen möglich, entweder nur lesend oder auch schreibend.

Klicken Sie auf **Hinzufügen**, um eine weitere Gruppe oder einen Benutzer zur angezeigten Liste hinzuzufügen. Mit **Entfernen** wird der zuvor ausgewählte Eintrag gelöscht. Geben Sie für den Benutzer oder die Gruppe an, ob er/sie Daten auf das Laufwerk kopieren können oder ob nur lesender Zugriff möglich ist.

Wählen Sie nun der Reiter „**Optionen**“.



Markieren Sie “**Dateien filtern**” bzw. „**Protokollieren und Schattenkopie**“, um die Dateifilterung und die ausgewählten Vorlagen einzuschalten. Wählen Sie aus der Liste einen der mitgelieferten Dateifilter-Vorlagen aus, die Ihnen im Einsteiger Modus zur Verfügung stehen.

Sie können, indem Sie “**Verschlüsselung erzwingen**” aktivieren, spezifizieren, dass jedes der betroffenen Geräte nur dann freigegeben wird, wenn es zuvor verschlüsselt wurde. Zusätzlich lässt sich festlegen, dass unverschlüsselte Laufwerke automatisch verschlüsselt werden.

Für CD-Laufwerke ist die Funktion “**Verschlüsselung erzwingen**“ aus technischen Gründen nicht vorhanden.

Um zu erzwingen, dass ein Benutzer zunächst die Verwendungsrichtlinie bestätigen muss, aktivieren Sie die Option „**Benutzer muss Verwendungsrichtlinie akzeptieren, …**“.

Um eine eigene Meldung für eine Regel zu konfigurieren, aktivieren Sie die Option „**Speziellen Text bei Benutzerbenachrichtigung anzeigen**“. Geben Sie anschließend einen Text ein, welcher unabhängig von der aktuell eingestellten Systemsprache angezeigt wird.

Klicken Sie **OK**, um die Einstellungen zu speichern.

In der Taskview-Ansicht können bis zu 50 Whitelist-Regeln angezeigt werden. Klicken Sie auf , um eine bestehende Regel zu ändern. Klicken Sie , um eine Regel zu löschen.

4.1.2 Erweiterte Einstellungen zum Sperren von Laufwerken

Neben den grundlegenden Einstellungen in der Basiskonfiguration stehen noch wesentlich mehr Optionen zur Verfügung, die Sie für Laufwerke über die erweiterten Einstellungen konfigurieren können.

4.1.2.1 Allgemeine Einstellungen zur Laufwerkssperrung

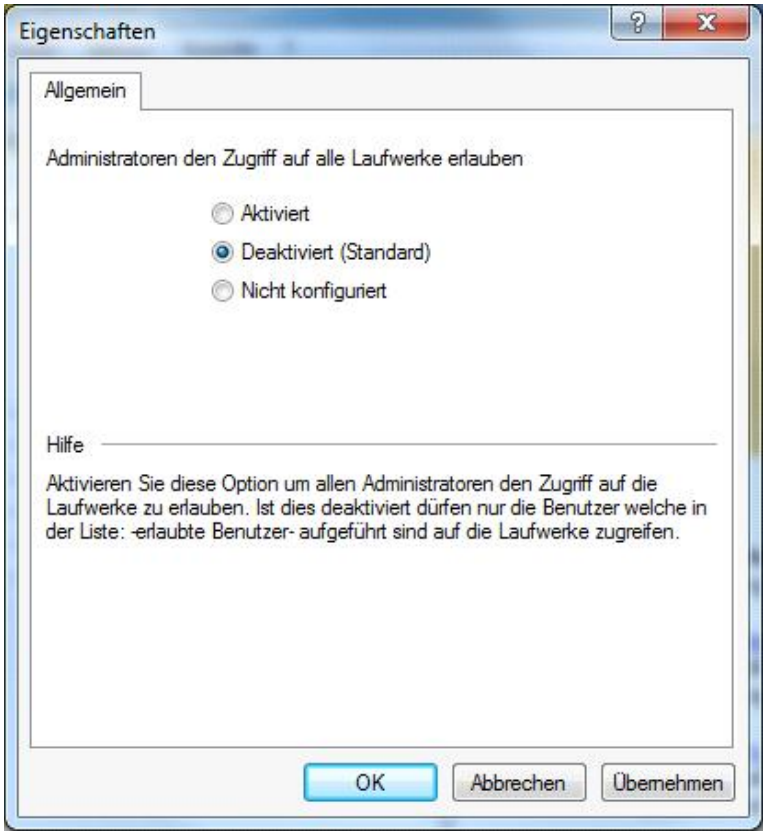
Bei der Konfiguration der Einstellungen für Laufwerkssperren bzw. –freigaben können Sie allgemeine Einstellungen festlegen.

Dazu klicken Sie auf **Einstellungen**, im Navigationsbereich.

4.1.2.1.1 Globale Sicherheits-Einstellungen für die Kontrolle von Laufwerken

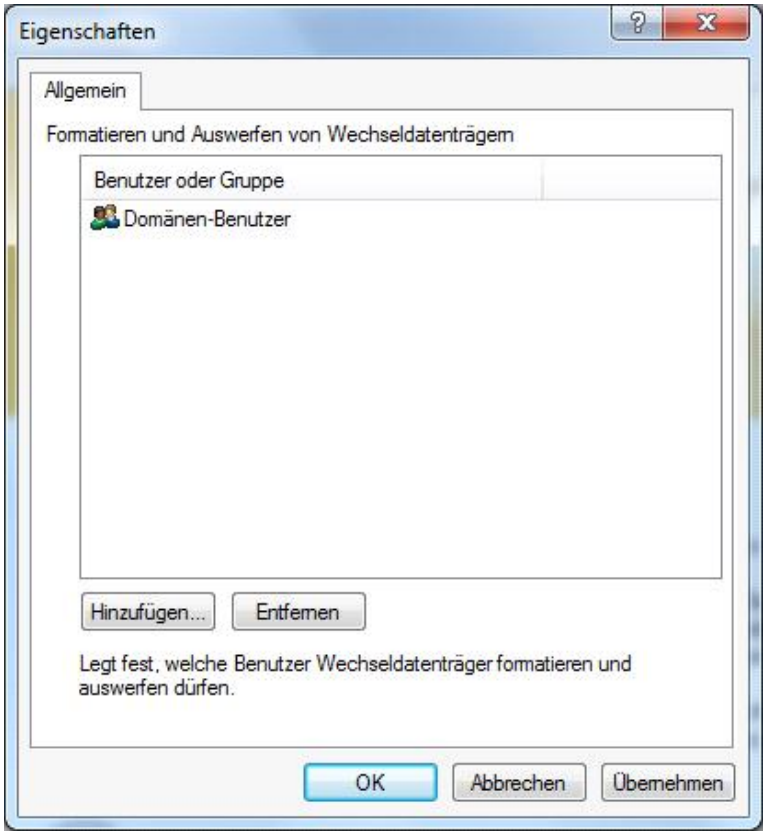
Sie haben die Möglichkeit, für alle Mitglieder der Gruppe der Administratoren den Zugriff auf Laufwerke freizugeben, unabhängig davon, welche Whitelist-Regeln oder Einstellungen aktiviert sind.

Dazu klicken Sie auf **Administratoren den Zugriff auf alle Geräte erlauben**.



Markieren Sie "**Aktiviert**", um diese Einstellung zu aktivieren.

Weiter können Sie vorgeben, welche Benutzer Wechseldatenträger auswerfen bzw. formatieren dürfen. Dazu klicken Sie bitte **Formatieren und Auswerfen von Wechseldatenträgern**.



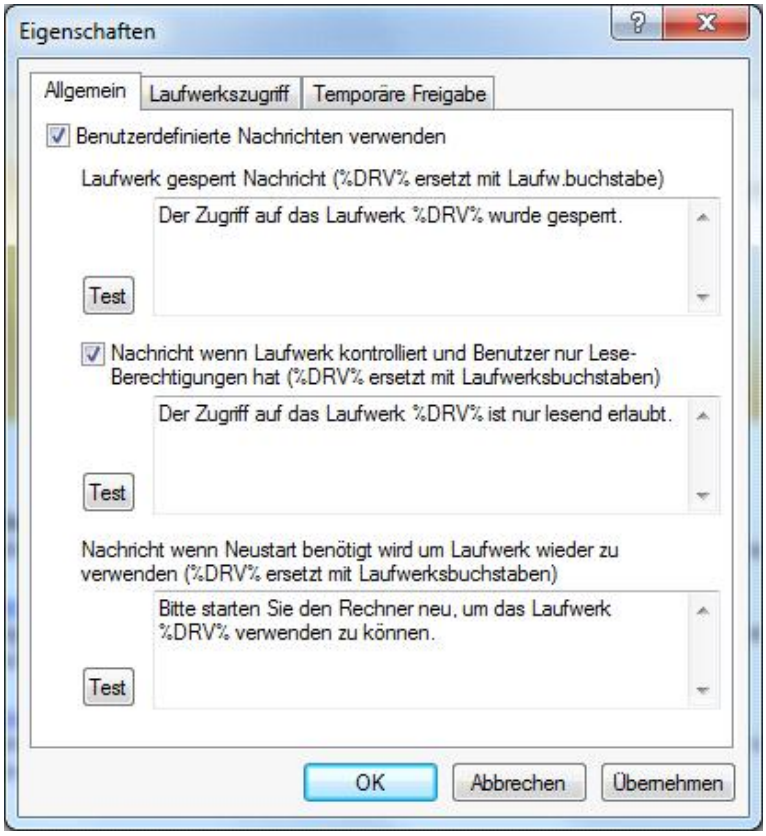
Klicken Sie **Hinzufügen**, um Benutzer oder Gruppen auszuwählen und zur Liste hinzuzufügen. Um Einträge aus der Liste zu löschen, markieren Sie diese und klicken **Entfernen**.

4.1.2.1.2 Konfiguration von Benutzermeldungen

4.1.2.1.2.1 Angepasste Benutzerbenachrichtigungen

Sobald ein Wechseldatenträger durch DriveLock mit Hilfe einer Whitelist-Regel gesperrt wird, kann DriveLock, sofern die entsprechende Option für Dialogfenster aktiviert wurde, dem aktuellen Benutzer eine Meldung anzeigen. Klicken Sie **Angepasste Benutzer-Benachrichtigungen**, um eigene Meldungen zu definieren.

> Wenn Sie mehrsprachige Benutzermeldungen konfiguriert haben, zeigt DriveLock an Stelle dieser Meldungen die Standardmeldungen in der aktuellen Sprache an.



Markieren Sie "**Benutzerdefinierte Nachrichten verwenden**" bzw. „**Nachricht wenn Laufwerk …**", um die hier festgelegten Meldungen zu aktivieren.

Die Variable %DRV% wird durch den Laufwerksbuchstaben ersetzt, wenn die Meldung angezeigt wird.

Klicken Sie **Test**, um zu überprüfen, ob die Meldung korrekt angezeigt wird. DriveLock zeigt die Meldung kurz so an, wie sie auch ein Benutzer sehen wird.

Wählen Sie den Reiter **Laufwerkszugriff**, um die Meldungen für den Zugriff auf Dateien oder das Sperren von CD/DVD-Brennern zu konfigurieren.

Folgende Variablen sind dabei verfügbar und werden entsprechend ersetzt:

- %DRV wird ersetzt durch den Laufwerksbuchstaben.
- %PATH% wird ersetzt durch den Dateipfad.
- %NAME% wird ersetzt durch den Dateinamen.
- %EXT% wird ersetzt durch die Dateiendung.
- %REASON% wird ersetzt durch den Grund, weshalb eine Datei blockiert wurde.

Klicken Sie **Test**, um zu überprüfen, ob die Meldung korrekt angezeigt wird. DriveLock zeigt die Meldung kurz so an, wie sie auch ein Benutzer sehen wird.

Auf der Seite **Temporäre Freigabe** können die Meldungen für die kurzzeitige Freigabe von Laufwerken oder Geräten durch einen Administrator konfiguriert werden.

Die Variable %TIME% wird beim Anzeigen durch die Zeit der Freigabe ersetzt. Sie können unterschiedliche Meldungen konfigurieren, je nachdem die Zeit in Minuten oder ein Zeitraum für die Freigabe verwendet wird.

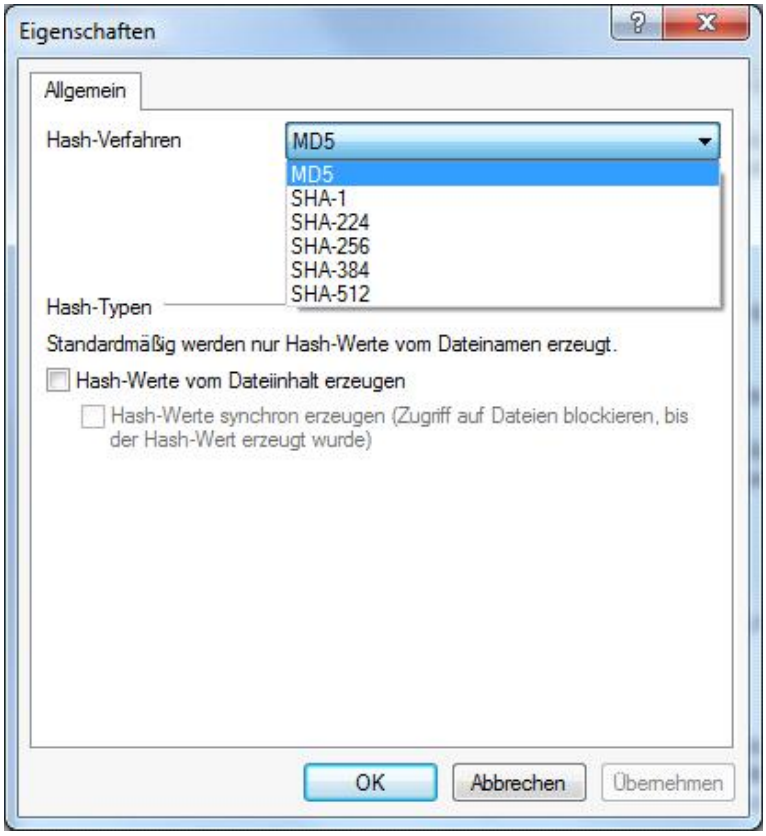
Um diese in einer Vorschau anzeigen zu lassen, klicken Sie **Test**.

> Sie können auf einige der HTML-Tags für die Formatierung Ihrer Nachricht verwenden (z.B. *Text*").

4.1.2.1.3 Einstellungen der Dateihash-Erzeugung

Jedes Mal, wenn eine Datei von einem externen Datenträger gelesen bzw. auf einen solchen geschrieben wird, erzeugt DriveLock einen Hashwert des Dateinamens. Dieser Hashwert kann zur genaueren Untersuchung des Dateitransfers und der Nachverfolgung von Dateien mit Hilfe des DriveLock Control Centers in Ihrem Unternehmen verwendet werden.

Die folgenden Einstellungen legen den verwendeten Hash-Algorithmus und die Generierung eines weiteren Hashwertes (den Inhaltshashwert) fest.



Wählen Sie einen Hash-Algorithmus aus der Liste aus. Der MD5-Algorithmus ist normalerweise schneller als ein SHA-Algorithmus, allerdings kann es aufgrund von Unternehmensrichtlinien erforderlich sein, einen der anderen zu verwenden.

Um die Erzeugung von Inhalts-Hashwerten zu aktivieren, wählen Sie die Option „Hash-Werte vom Dateiinhalt erzeugen“ und stellen Sie ein, ob diese zeitgleich oder zeitversetzt generiert werden sollen. Bei größeren Dateien kann die Erzeugung dieser Hashwerte etwas Zeit in Anspruch nehmen.

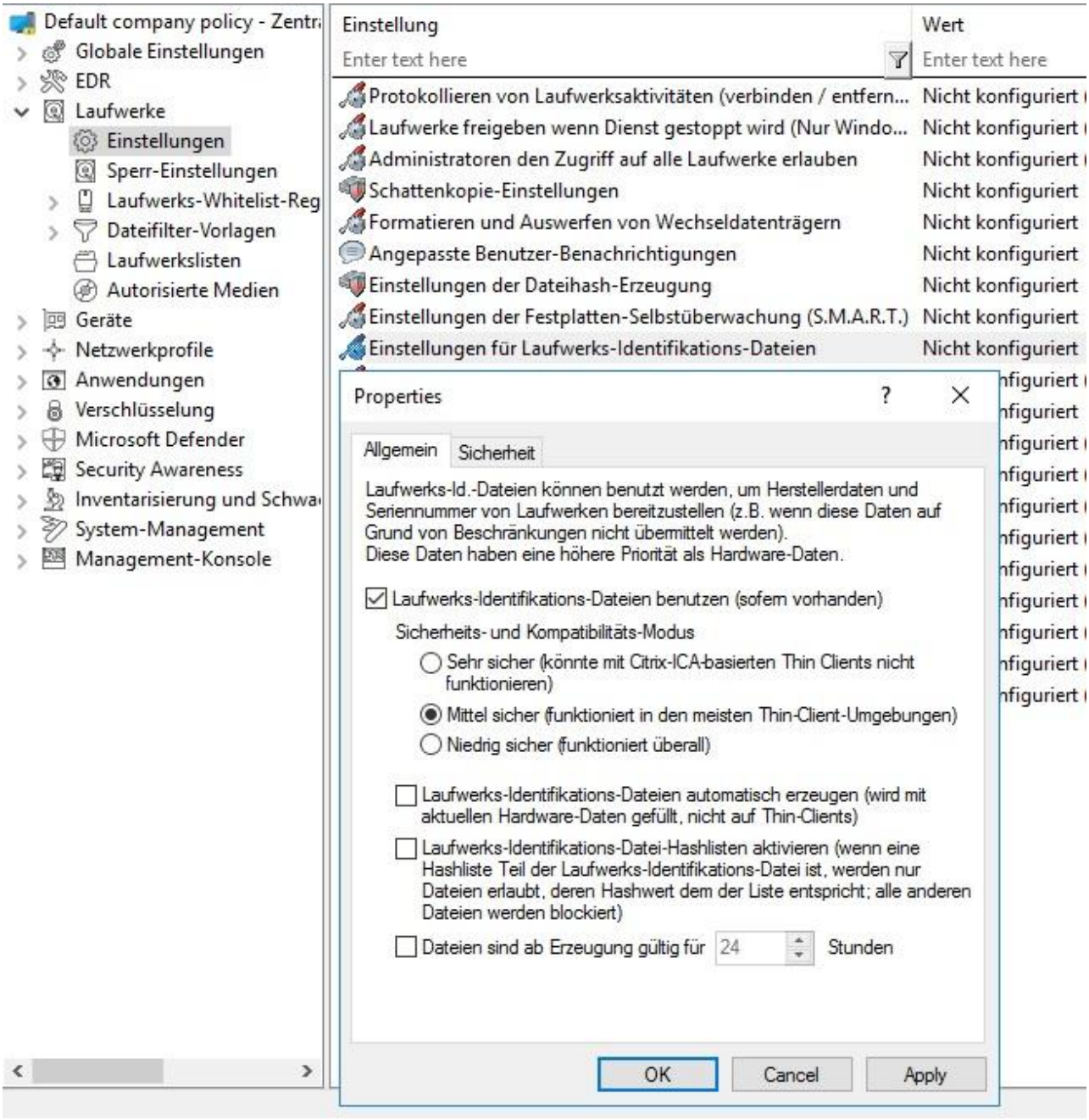
Klicken Sie auf OK, um die Einstellungen zu übernehmen und das Fenster zu schließen.

4.1.2.1.4 Laufwerks-Identifikations-Dateien

In den meisten Fällen sind Speichermedien über eine Hardware-ID (Hersteller-ID, Produkt-ID, Seriennummer) eindeutig identifizierbar. Es gibt auch Speichermedien, wie SD-Cards oder NoName-USB-Sticks ohne Hardware-ID und Fälle, in denen auf die Hardware-ID nicht zugegriffen werden kann. Z.B. wenn die Speichermedien über Thin-Clients (ohne DriveLock Virtual Channel) oder SD-Cards über USB-SD-Card-Reader verbunden werden.

Auf solchen Speichermedien können Laufwerks-Identifikation-Dateien mit einer Laufwerks-ID angelegt werden. Damit werden sie für DriveLock identifizierbar.

Um Laufwerks-Identifikation-Dateien zu nutzen, öffnen Sie in der Richtlinie *Laufwerke / Einstellungen / Einstellungen für Laufwerks-Identifikations-Dateien.*



Markieren Sie *Laufwerks-Identifikations-Dateien benutzen*, dann überschreibt die ID aus der Datei (sofern vorhanden) die die Hardware-ID des Speichermediums.

Sicherheits- und Kompatibilitäts-Modus:

- *Sehr sicher:* die Laufwerks-ID muss zur Volume-Serial-Number der Partition passen. Wenn eine Laufwerks-Identifikations-Datei auf eine andere Partition kopiert wird, ist sie ungültig. Manche ICA basierten Thin-Clients übertragen die Volume-Serial-Number nicht an Windows. DriveLock kann dann die Laufwerks-ID nicht verifizieren.
- *Mittel sicher:* die Laufwerks-ID muss zur Größe der Partition passen. Wenn eine Laufwerks-Identifikations-Datei auf eine Partition mit anderer Größe kopiert wird, ist sie ungültig.

- *Niedrig sicher:* eine Laufwerks-Identifikations-Datei kann auf eine andere Partition kopiert werden. DriveLock akzeptiert eine Laufwerks-ID unabhängig von der Volume-Serial-Number oder der Größe der Partition. Nutzen Sie diese Option nur, wenn Ihr Thin-Client keine Volume-Serial-Number und keine Größe überträgt.

Die Laufwerks-Identifikations-Datei enthält alle drei Sicherheitsmodi. Starten Sie immer mit *Sehr sicher* und reduzieren Sie nur wenn notwendig. Vorhandene Laufwerks-Identifikations-Dateien bleiben weiterhin gültig, auch wenn der Sicherheitsmodus geändert wird.

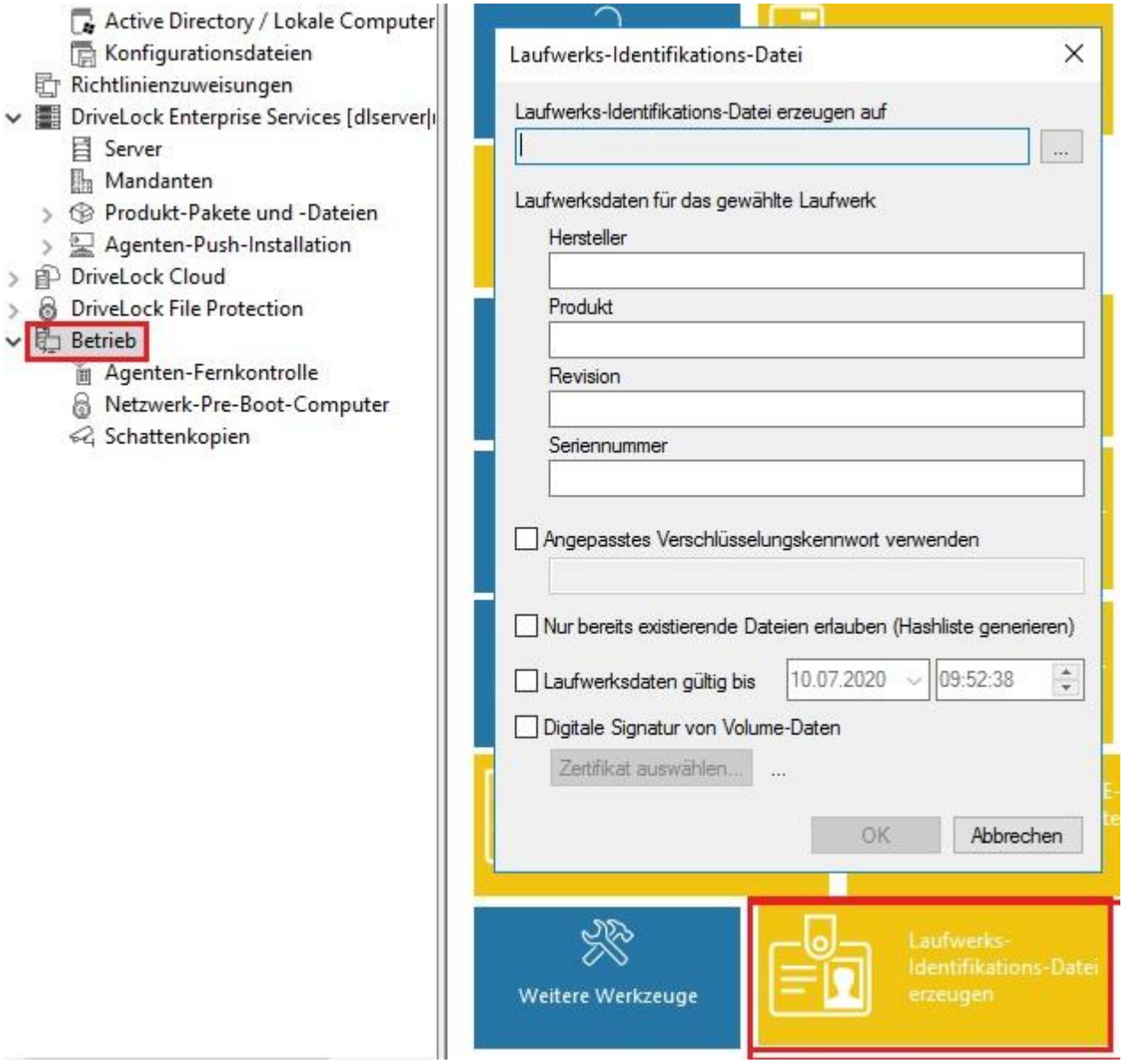
Wenn die Option *Laufwerks-Identifikations-Dateien automatisch erzeugen* eingeschaltet ist, wird eine solche Datei automatisch mit den Hardware-ID-Werten angelegt, sobald ein Speichermedium auf einem FAT-Client (nicht Thin-Client) mit DriveLock verbunden wird.

Laufwerks-Identifikations-Dateien werden entweder mit einem voreingestellten Schlüssel oder, sofern gesetzt, mit dem aus dem kundenspezifischen Passwort erzeugten Schlüssel verschlüsselt. Wenn Sie das Passwort ändern sind alle vorhanden Laufwerks-Identifikations-Dateien ungültig.

> Laufwerks-Identifikations-Dateien sind für normale Anwender nicht sichtbar (Attribute Hidden, System)

Laufwerks-Identifikations-Dateien manuell erstellen

Öffnen Sie das Kontextmenü über **MMC / Betrieb / Agenten-Fernkontrolle / Weitere Werkzeuge / Laufwerks-Identifikations-Datei erzeugen...** und geben die gewünschten Daten ein, um Laufwerks-Identifikations-Dateien, z.B. auf SD-Cards, anzulegen.

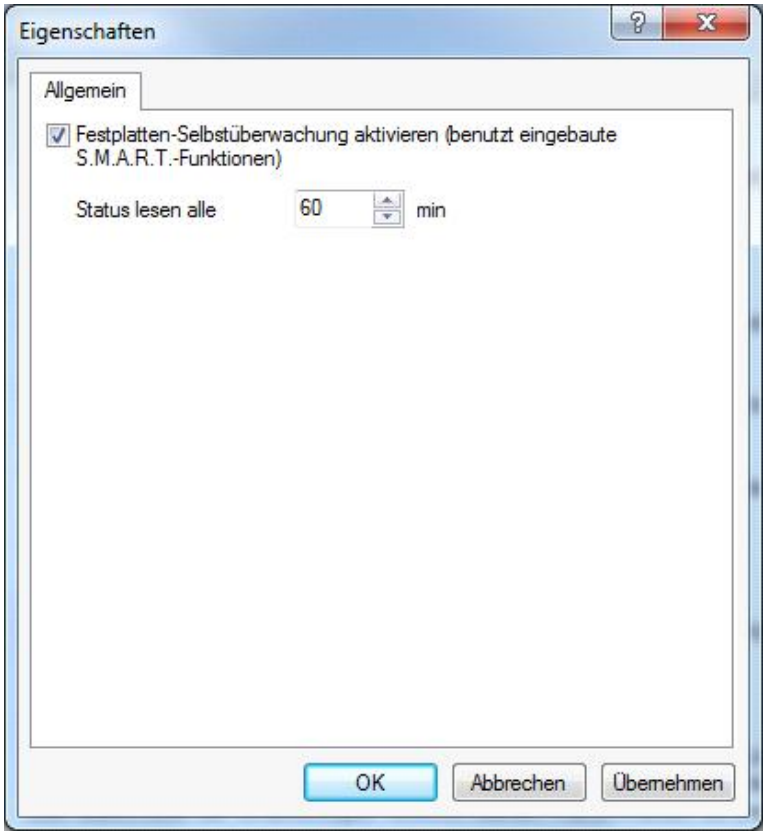


4.1.2.1.5 Schattenkopie-Einstellungen

Bitte sehen Sie im Kapitel „Schattenkopien in Laufwerksregeln konfigurieren“ für Informationen zum Konfigurieren und zur Verwendung von Schattenkopien nach.

4.1.2.1.6 S.M.A.R.T. Festplatten-Selbstüberwachung

Mithilfe der S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) kann der Betriebszustand von internen Festplatten überwacht werden. Das hilft Fehler vorzeitig zu erkennen und lange Ausfallzeiten von Clients aufgrund defekter Festplatten zu vermeiden. Der Status kann dann über das Reporting oder über die Agenten-Fernkontrolle ausgelesen werden. Um die Überwachung zu aktivieren, klicken Sie **Einstellungen der Festplatten-Selbstüberwachung (S.M.A.R.T.)** und setzen den Haken bei *Festplatten-Selbstüberwachung aktivieren…* und geben als Zeitraum z.B. 60 Minuten an:



4.1.2.1.7 Erweiterte Einstellungen zur Kontrolle von Laufwerken

Es existieren noch vier weitere Konfigurationsmöglichkeiten, die über die entsprechenden Links in der Taskview-Ansicht erreicht werden können:

- *Protokollierung von Laufwerksaktivitäten (verbinden/entfernen/sperren)*: Sofern aktiviert, werden zu den drei Ereignissen entsprechende Überwachungsereignisse generiert
- *Laufwerke freigeben, wenn Dienst gestoppt wird*: Aktivieren Sie diese Funktion, um die Sperrung aller Laufwerke aufzuheben, wenn der DriveLock Dienst beendet wird.
- *Dateifilter während temporärer Freigabe abschalten*: Eine Aktivierung dieser Funktion führt dazu, dass der Dateifilter ebenso ausgeschaltet wird, wenn eine temporäre Freigabe erfolgt.

Sofern Sie den Dateifilter während der temporären Freigabe an dieser Stelle global deaktivieren, ist es nicht mehr möglich den Dateifilter gezielt für jede temporäre Freigabe einzeln abzuschalten.

4.1.2.2 Laufwerkssperre aktivieren

DriveLock ist in der Lage, alle Laufwerke zu kontrollieren, die Windows entweder als Wechseldatenträger oder feste Laufwerke erkennen kann. Dies beinhaltet insbesondere die folgenden Klassen:

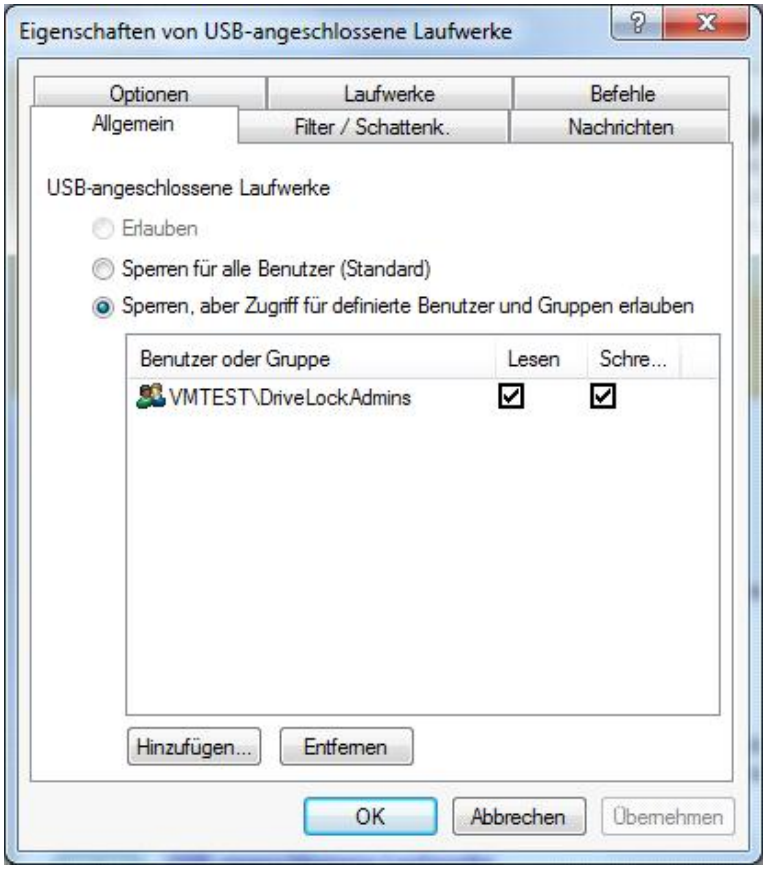
- *Diskettenlaufwerke*: Alle internen Diskettenlaufwerke
- *CD-ROM-Laufwerke*: Interne CD-ROM / DVD / BD Laufwerke (inkl. Brenner)
- *USB-angeschlossene Laufwerke*: Alle Laufwerke die über USB angeschlossen sind, z.B. USB-Sticks, USB-Festplatten, USB-CD-ROM Laufwerke, USB-Kartenlesergeräte.
- *Firewire (1394)-angeschlossene Laufwerke*: Alle Laufwerke die über Firewire angeschlossen sind, z.B. Firewire Festplatten

- *SD-Karten-Laufwerke (SD Bus)*: Speziell bei Notebooks gibt es reine SD-Karten-Leser, die über diese Laufwerksklasse behandelt werden.
- *Andere Wechseldatenträger*: Alle Laufwerke die in keine andere Kategorie fallen, z.B. ZIP-Laufwerke
- *Festplatten (eSATA, nicht wechselbar, kein System enthaltend)*: Alle internen und externen Laufwerke die über IDE, ATAPI, SCSI, RAID, SATA oder eSATA angesteuert werden.
- *Verschlüsselte Container*: Spezielle DriveLock-eigene Laufwerksklasse für von DriveLock verschlüsselte Container. Weitere Informationen finden Sie im Kapitel Encryption 2-Go.
- *Netzwerk-Laufwerke und –Freigaben*: Windows-Netzwerklaufwerke.
- *WebDAV-Netzwerk-Laufwerke*: Laufwerke, die über das WebDAV-Protokoll und http/https angebunden wurden.
- *Windows Terminal Services (RDP) Client-Laufwerkszuordnungen*: Mehr zum Aufbau der verschiedenen Terminalserver-Szenarien erhalten Sie im Kapitel Terminalserver.
- *Citrix XenApp (ICA) Client-Laufwerkszuordnungen*: Mehr zum Aufbau der verschiedenen Terminalserver-Szenarien erhalten Sie im Kapitel Terminalserver.

Festplatten, die für Windows die Systemplatte darstellen und Partitionen mit der Auslagerungsdatei werden von DriveLock nicht gesperrt.

Um die Laufwerkssperre zu aktivieren, öffnen Sie die Verwaltungskonsole und wählen „**Laufwerke -> Sperr-Einstellungen”.**

Klicken Sie auf „**USB-angeschlossene Geräte**“ auf der rechten Seite, um den Konfigurationsdialog zu öffnen (z.B. für eben USB-Geräte).



Hier können Sie Einstellungen vornehmen, die für alle über die USB-Schnittstelle angeschlossenen Laufwerke gleichermaßen gelten sollen.

Diese Einstellungen sind für alle genannten Klassen im Wesentlichen gleich, jedoch sind einige Einstellungsoptionen für einige Klassen nicht verfügbar bzw. unterscheiden sich minimal von den nachfolgend gezeigten.

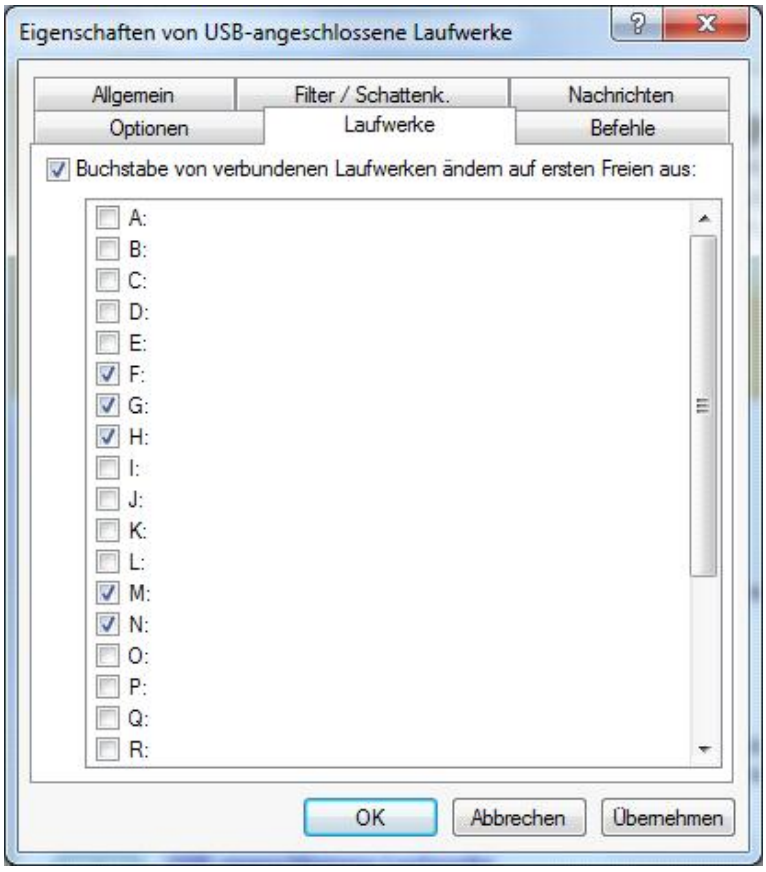
Wählen Sie „**Sperren für alle Benutzer (Standard)**" und klicken **OK**, um die Sperrung aller USB-Laufwerke auf diesem Computer zu aktivieren.

> Um USB-Laufwerke zu sperren ist es nicht notwendig (und auch nicht vorgeschlagen), die Geräteklasse „USB Controller" zu sperren. Damit würden Sie nicht mehr in der Lage sein, die Funktionen für die Freigabe bzw. das Sperren von USB-Laufwerken zu verwenden.

Sofern Sie Benutzern oder Gruppen den Zugriff erlauben, können Sie zusätzlich die erlaubte Zugriffsart (nur lesend oder auch schreibend) konfigurieren. Damit können Sie zum Beispiel für bestimmte Gruppen oder Benutzer festlegen, dass diese nur lesend auf einen USB-Stick zugreifen dürfen.

Ein Hinweis für Diskettenlaufwerke: Wird ein Dateifilter einem Diskettenlaufwerk zugeordnet, so wird dieser erst aktiviert, nachdem eine Diskette eingelegt wurde. Unglückerweise kann Windows nicht automatisch feststellen, wann dies geschieht. Aus diesem Grund muss DriveLock diese Überprüfung selbst durchführen und überprüft das Diskettenlaufwerk in gleichmäßigen Abständen („Polling"). Leider wird dieser Vorgang als „Rattern" akustisch wahrgenommen. Um dies zu vermeiden, verzichten Sie entweder auf Dateifilter zusammen mit Diskettenlaufwerken, oder deaktivieren Sie das „Polling" (Laufwerke: Einstellungen (nur in klassischer MMC Ansicht)). Wenn Sie das „Polling" deaktivieren, kann es sein, dass der Dateifilter bei manchen Diskettenlaufwerken nicht mehr funktioniert.

Möchten Sie spezielle Laufwerksbuchstaben automatisch vergeben, wenn ein Laufwerk von einem Typ an den Computer angeschlossen wird, wählen Sie den Reiter „**Laufwerke**“ und aktivieren die gewünschten Buchstaben in der Liste.



Es ist auch möglich, Laufwerksbuchstaben innerhalb einer Whitelist-Regel zu definieren.

Wie Benutzerberechtigungen vergeben werden, wird im Kapitel “Zugriffsberechtigungen für Benutzer und Gruppen” beschrieben.

4.1.2.3 Laufwerksregeln definieren

Es gibt verschiedene Arten von Whitelist-Regeln, die verwendet werden können:

- *Geräte-Regel*: Das Laufwerk kann detailliert definiert werden (z.B. ein Kingston 1GB Stick mit einer bestimmten Seriennummer)
- *Laufwerkslisten-Regel*: Diese Einstellungen gelten für eine zuvor definierte Liste von Laufwerken
- *Netzwerklaufwerk-Regel*: Konfiguration für ein bestimmtes freigegebenes Netzwerkverzeichnis
- *WebDAV-Netzwerklaufwerk-Regel*: Einstellung für ein über eine URL verbundenes Laufwerk
- *Gerätegröße-Regel*: Das Laufwerk wird aufgrund seiner Größe definiert
- *Basis-Regel*: Diese Regel wird auf eine der fünf Laufwerkstypen angewendet (Sie können diese Regel dazu verwenden, um zeitliche Einschränkungen oder computerbezogene Regeln zu erstellen)
- *Terminaldienste-Regel*: Eine Regel für einen bestimmten Laufwerksbuchstaben innerhalb einer Terminal Server Verbindung
- *Hardware-ID-Regel*: Einstellungen, die für eine bestimmte Hardware-ID gelten sollen

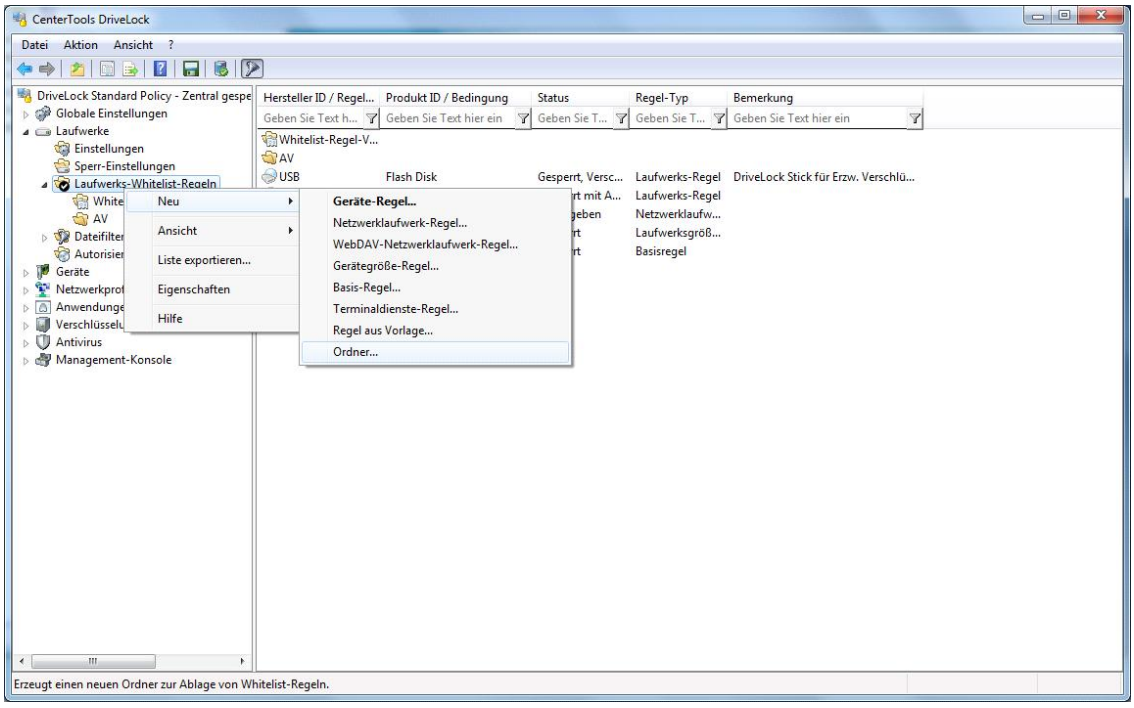
Die Priorisierung der Regeln wird wie folgt durchgeführt:

- Geräte-Regel (eine Regel mit einer Seriennummer hat eine höhere Priorität als eine Regel ohne)
- Gerätegröße-Regel
- Basis-Regel
- Allgemeine Sperreinstellungen

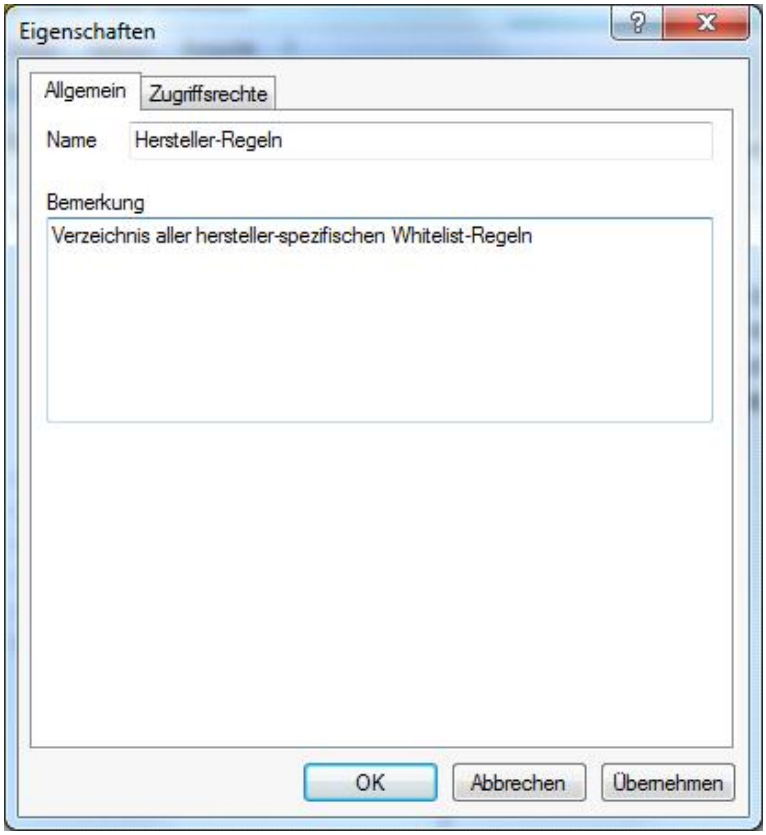
In den nachfolgenden Abschnitten werden die unterschiedlichen Elemente dieser Regeln beschrieben. Das Kapitel „Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren“ enthält die Beschreibung der verschiedenen Konfigurationsmöglichkeiten, die bei mehreren dieser Whitelist-Regeln zur Verfügung stehen.

4.1.2.3.1 Whitelist-Regeln verwalten

Sie können Ihre Whitelist-Regeln in einer Verzeichnisstruktur ablegen (mit Unterverzeichnissen), so wie Sie auch Dateien auf Ihrer Festplatte in verschiedenen Ordnern verwalten.

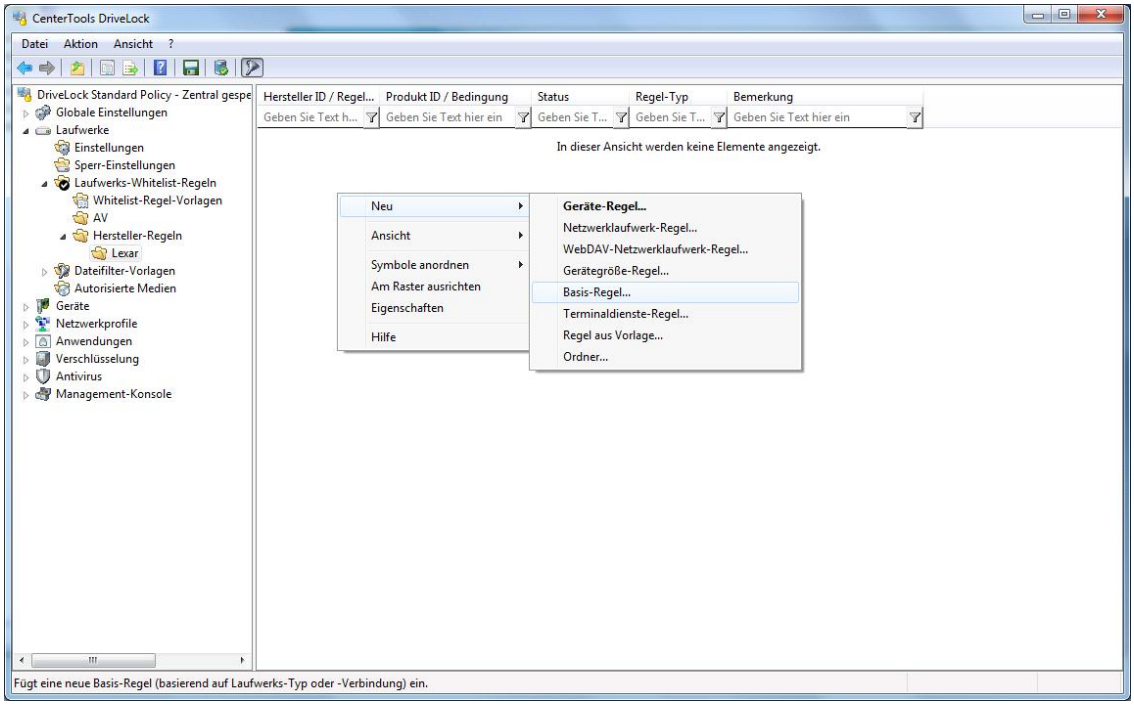


Klicken Sie dazu auf Laufwerks-Whitelist-Regeln und anschließend auf **Neu -> Ordner**. Dadurch wird ein neuer Ordner auf der obersten Ebene angelegt. Um ein Unterverzeichnis anzulegen, rechtsklicken Sie auf den gewünschten Ordner und klicken Sie anschließend ebenfalls auf **Neu -> Ordner**.

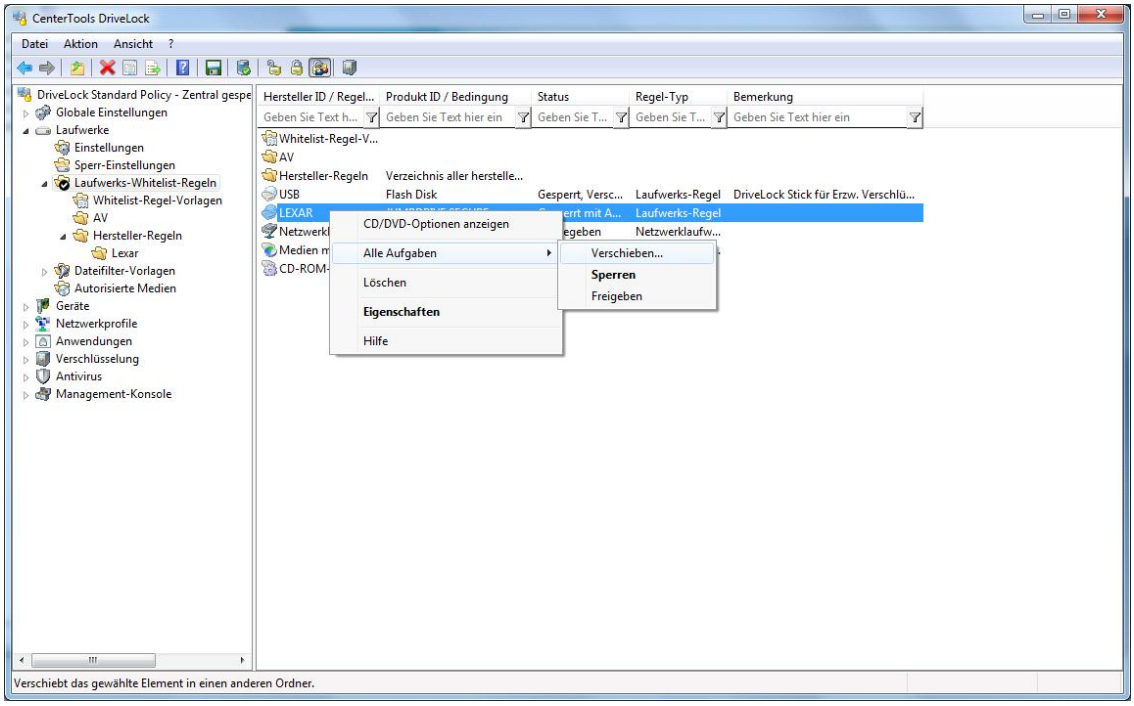


Geben Sie einen neuen Namen ein (und eventuell noch eine Beschreibung in das Feld Bemerkung) und klicken Sie auf **OK**, um den Ordner anzulegen.

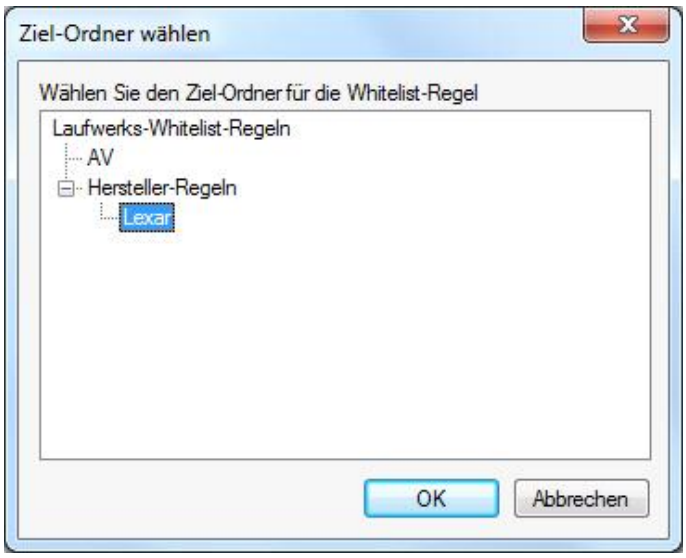
Die neue Ordnerstruktur wird im Navigationsbaum links angezeigt.



Um eine neue Whitelist-Regel gleich in einem bestimmten Ordner anzulegen, rechtsklicken Sie auf den Ordner und wählen Sie anschließend den gewünschten Regeltyp aus, zum Beispiel **Neu -> Basis-Regel**.



Um eine bestehende Regel in ein existierendes Verzeichnis zu verschieben, rechtsklicken Sie auf die Whitelist-Regel und wählen Sie **Alle Aufgaben -> Verschieben**.



Wählen Sie den gewünschten Zielordner und klicken Sie **OK**, um die Regel dorthin zu verschieben.

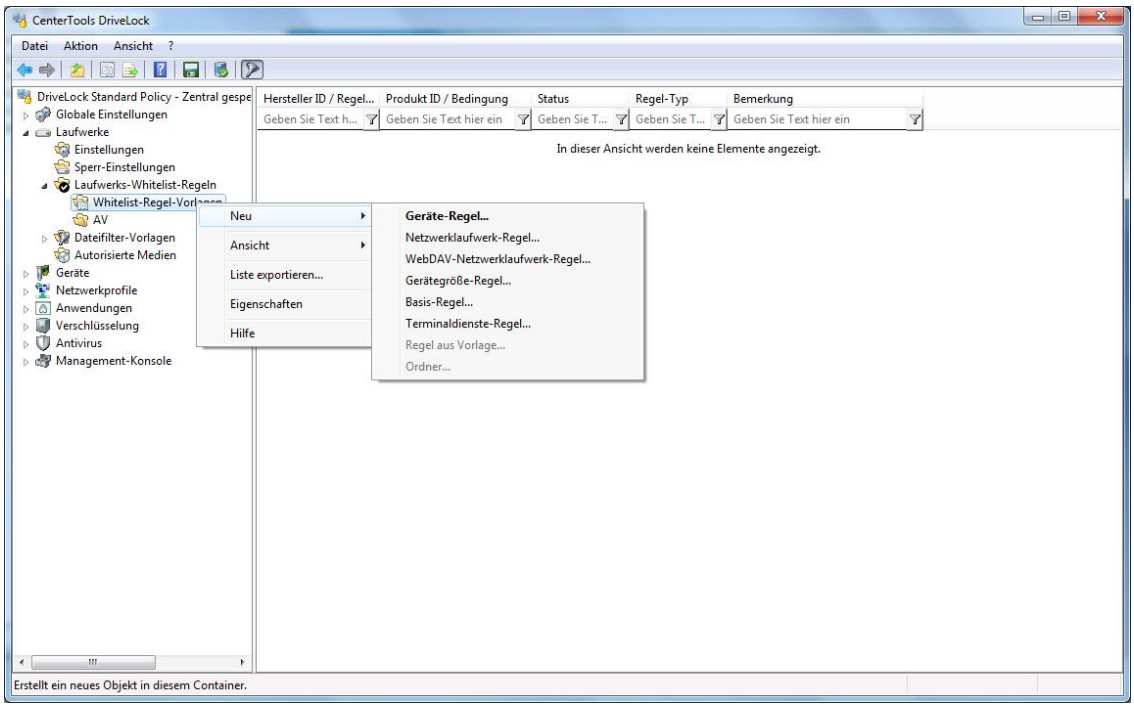
4.1.2.3.2 Whitelist-Vorlagen erstellen

Eine Whitelist-Vorlage ist eine Whitelist-Regel, welche als Vorlage bei der Erstellung anderer Whitelist-Regeln verwendet werden kann. Sie können Whitelist-Vorlagen für die folgenden Regeltypen erstellen:

- *Geräte-Regel*: Das Laufwerk kann detailliert definiert werden (z.B. ein Kingston 1GB Stick mit einer bestimmten Seriennummer)
- Laufwerkslisten-Regel: Diese Einstellungen gelten für eine zuvor definierte Liste von Laufwerken
- *Netzwerklaufwerk-Regel*: Konfiguration für ein bestimmtes freigegebenes Netzwerkverzeichnis
- *WebDAV-Netzwerklaufwerk-Regel*: Einstellung für ein über eine URL verbundenes Laufwerk

- *Gerätegröße-Regel*: Das Laufwerk wird aufgrund seiner Größe definiert
- *Basis Regel*: Diese Regel wird auf eine der fünf Laufwerkstypen angewendet (Sie können diese Regel dazu verwenden, um zeitliche Einschränkungen oder computerbezogene Regeln zu erstellen)
- *Terminaldienste-Regel*: Eine Regel für einen bestimmten Laufwerksbuchstaben innerhalb einer Terminal Server Verbindung
- *Hardware-ID-Regel*: Einstellungen, die für eine bestimmte Hardware-ID gelten sollen

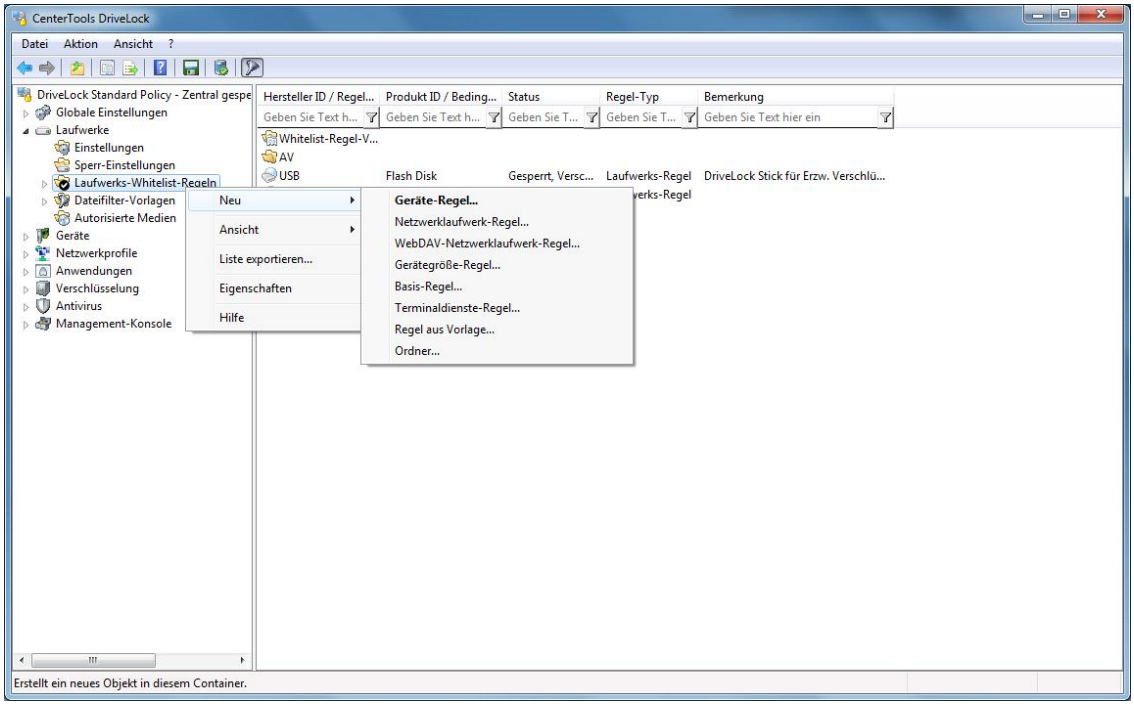
Vorlagen können nicht direkt als Whitelist-Regel verwendet werden, um Laufwerke zu kontrollieren, aber Sie können (wie im Abschnitt „Regeln basierend auf einer Regelvorlage erstellen“ beschrieben) diese dazu verwenden, neue Whitelist-Regeln anzulegen.



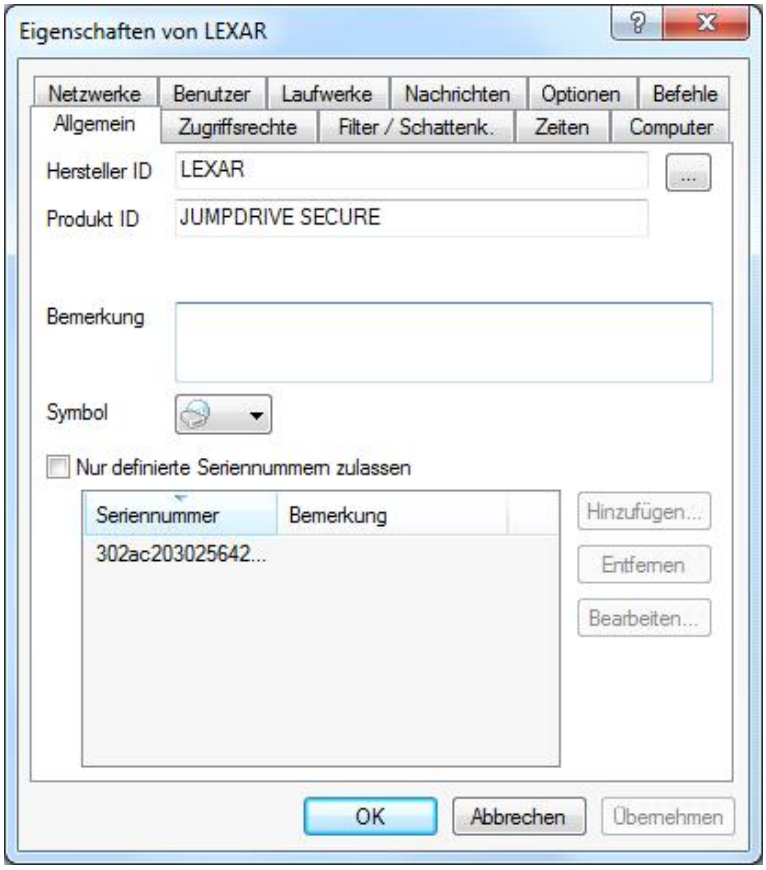
Rechtsklicken Sie auf Whitelist-Vorlage, klicken Sie **Neu** und wählen Sie den gewünschten Regeltyp aus dem Kontextmenü.

Folgen Sie nun den Schritten, welche im Abschnitt „Laufwerksregeln definieren“ beschrieben sind, um weitere Einstellungen vorzunehmen.

4.1.2.3.3 Geräte-Regel



Rechtsklicken Sie auf **Laufwerks-White-List-Regel** und wählen "**Neu -> Geräte-Regel**" aus dem Kontextmenü. Im darauf folgenden Dialogfenster wird das Gerät angegeben, das ge- bzw. entsperrt werden soll. Geben Sie einen Hersteller und eine Produkt-ID ein. Ebenso kann eine zusätzliche Liste an Seriennummern definiert werden, um der Geltungsbereich weiter einzuschränken.

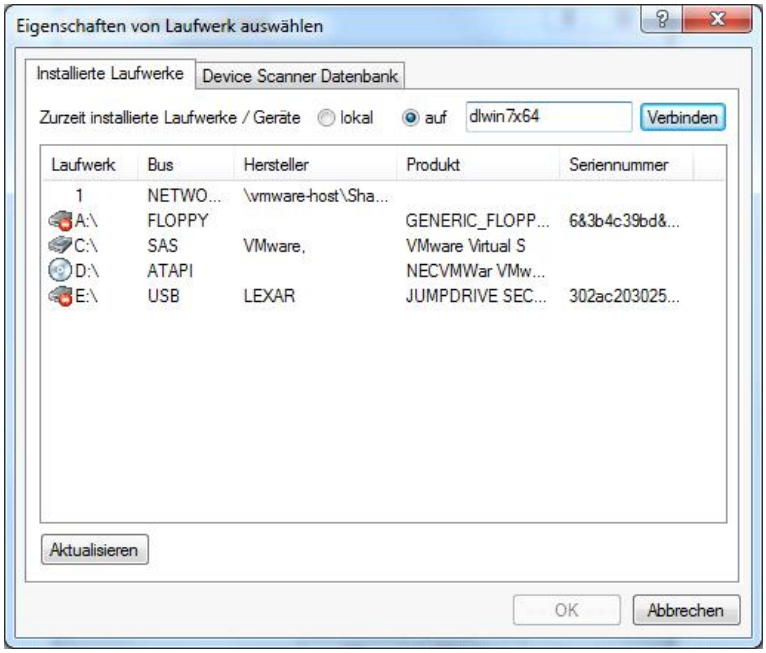


Jedes Laufwerk enthält einige Informationen über die zugrunde liegende Hardware (z.B. Name des Herstellers und des Produktes):
Hersteller ID: Name oder Abkürzung des Laufwerksherstellers
Produkt ID: Einzigartige ID des Produktes, vergeben durch den Hersteller

Sie können auch ein gerade verbundenes Gerät oder ein Gerät aus der Device Scanner Datenbank auswählen, in dem Sie den Button "…" neben dem Herstellerfeld klicken. Eine Seriennummer wird dabei automatisch hinzugefügt, wenn Sie vorher „**Nur definierte Seriennummern zulassen**" aktivieren.

Sowohl bei der Produkt ID als auch bei der Hersteller ID ist es möglich, folgende Platzhalter zu verwenden: "*" (mehrere Zeichen) und "?" (genau ein Zeichen).

Auch andere Seriennummern können festgelegt werden, in dem Sie auf Hinzufügen klicken und die Seriennummer eingeben. Dabei können wiederum auch Platzhalter („?" oder „*" verwendet werden). Ebenso können Sie auch ein gerade verbundenes Gerät oder ein Gerät aus der Device Scanner Datenbank auswählen und dessen Seriennummer übernehmen, in dem Sie den Button "…" neben dem Herstellerfeld klicken.



Wählen Sie ein lokales Laufwerk aus und klicken auf **OK**.

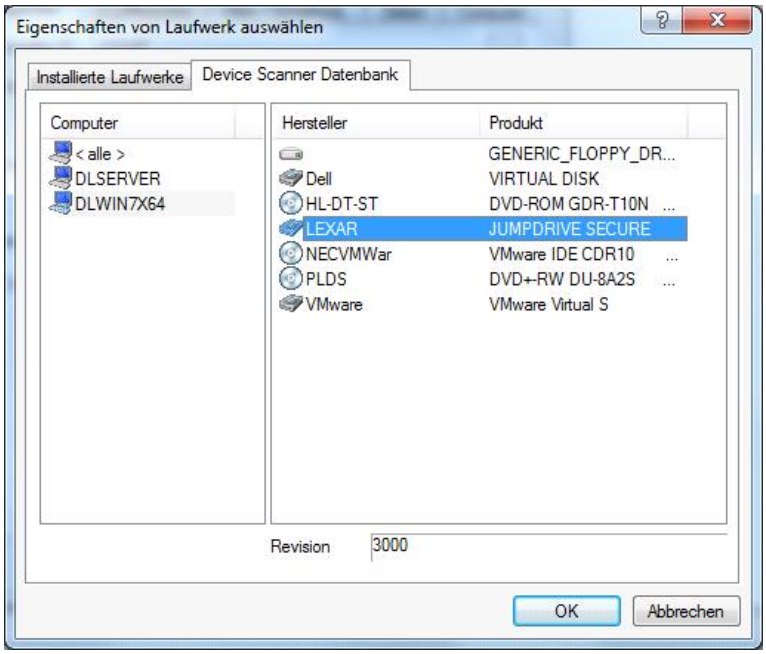
Weitere Laufwerke können ausgewählt werden, in dem Sie sich auf einen anderen Agent per Remote-Verbindung verbinden und ein dort vorhandenes Laufwerk auswählen Wählen Sie dazu „**auf**" aus und geben Sie den Namen des Computers ein, mit dem Sie sich verbinden möchten. Dazu muss auf dem Zielcomputer der DriveLock Agent installiert sein.

DriveLock liest die Hardware-Information aus dem Windows Betriebssystem aus. Daher kann DriveLock nur diejenigen Laufwerke anzeigen, die auch im Windows Betriebssystem angezeigt werden.

Um eine Remote-Verbindung zu erstellen, muss (falls vorhanden) die Windows Firewall so konfiguriert sein, dass eingehende Verbindungen über den Ports 6064 bzw. 6065 (voreingestellter Wert) und das Programm „DriveLock" zugelassen sind.

Wenn Sie sich mit dem lokalen Computer verbinden, werden geblockte Laufwerke nicht angezeigt. Um dies zu umgehen, wählen Sie „auf" aus und geben den Namen des lokalen Computers ein.

Eine weitere und sehr einfache Möglichkeit, die notwendigen Informationen zu Laufwerken zu erhalten, besteht darin, sich die Ergebnisse in der Device Scanner Datenbank anzusehen. Wählen Sie dazu den „**Device Scanner Datenbank**“ Reiter und anschließend die gewünschten Computer, Hersteller und Produkte aus.



Die weiteren Konfigurationsmöglichkeiten werden im Abschnitt „Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren“ beschrieben.

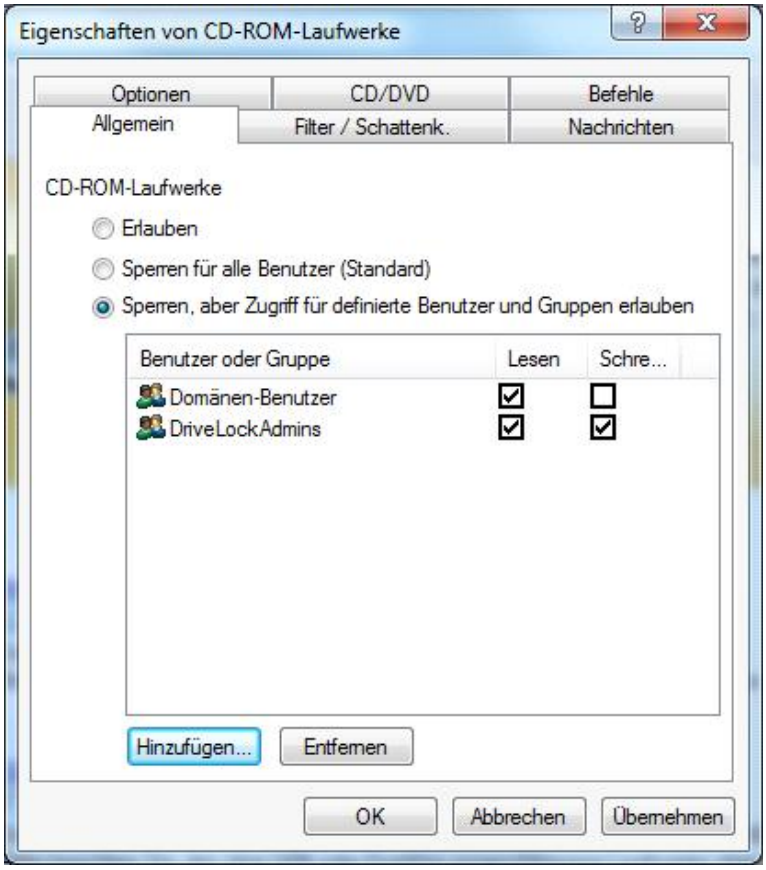
4.1.2.3.4 Sperren und Überwachen von CD/DVD-Brennern

Um CD/DVD-Laufwerke zu sperren, konfigurieren Sie die Einstellungen für die Laufwerksklasse CD/DVD-Laufwerke wie im Abschnitt „Laufwerkssperre aktivieren“ beschrieben.

Immer wieder kommt es aber vor, dass Programme zum Brennen von CDs/DVDs die in Windows integrierten Dateisystem-Treiber umgehen. Daher enthält DriveLock einen zusätzlichen Systemtreiber, welcher als sogenannter „Lowlevel“-Treiber an CD/DVD-Laufwerke angebunden ist und dafür sorgt, das ein Umgehen des Dateisystem-Treibers in den meisten Fällen nicht möglich ist.

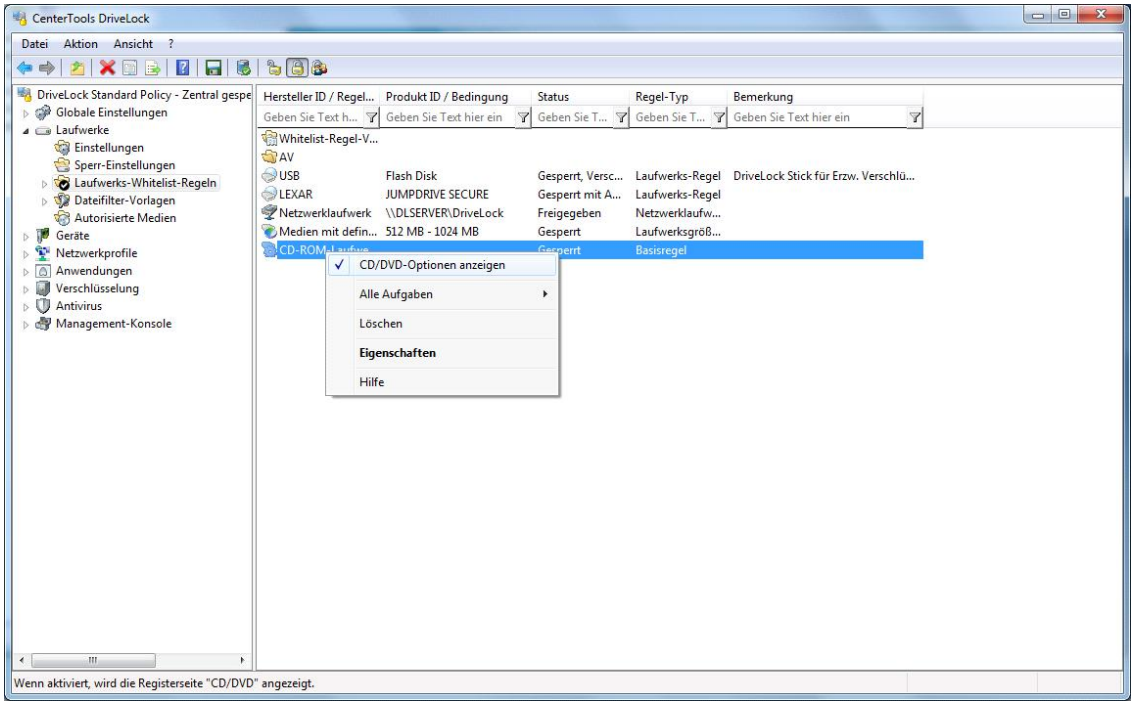
Die folgenden Brenn-Programme wurden mit DriveLock erfolgreich getestet und werden von DriveLock unterstützt: Roxio (WinOnCD), Nero, Windows (IMAPI) und Infra-Recorder.

Um DriveLock nun so zu konfigurieren, dass das Brennen von CDs/DVDs für einige Benutzer gesperrt und für andere wiederum erlaubt ist, müssen Sie die Benutzerberechtigungen bei der Laufwerksklasse für CD/DVD-Laufwerke entsprechend konfigurieren und dabei das Schreibrecht entsprechend den Anforderungen einstellen.

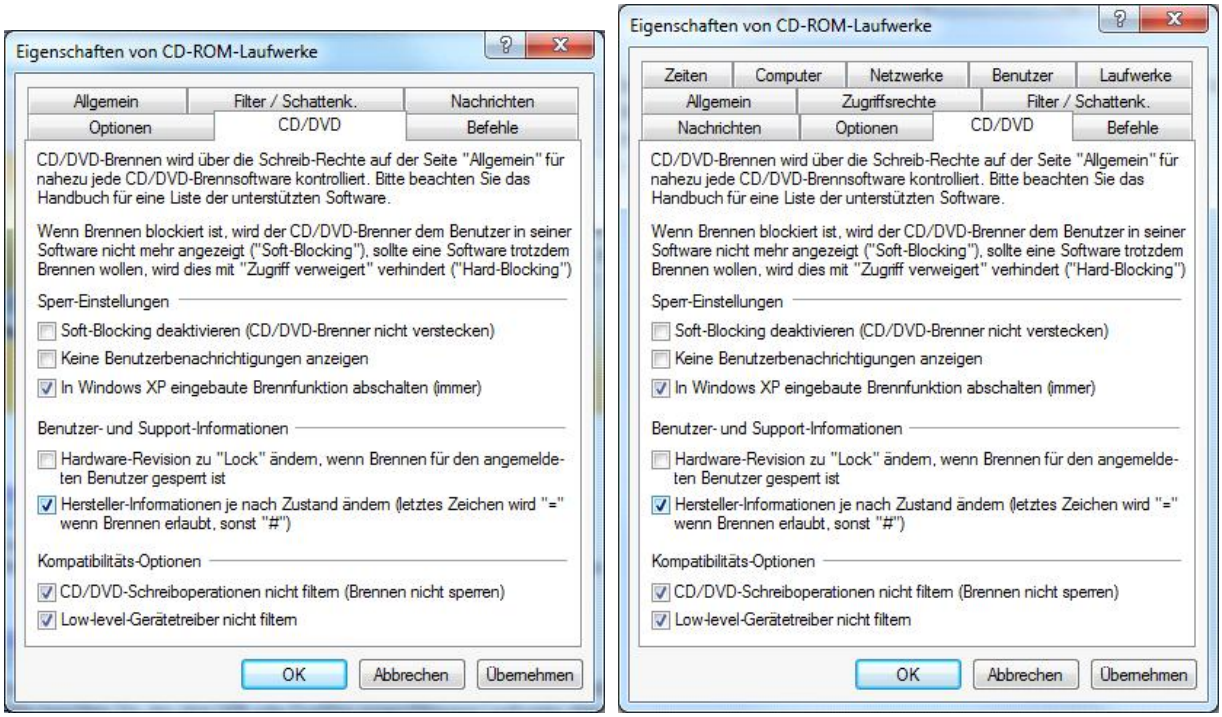


Wenn Sie zusätzlich unter Optionen *Verschlüsselung erzwingen* markieren, erlaubt DriveLock für diese Benutzer das Brennen nur mit dem Assistenten zum *Verschlüsselte Medien brennen*.

Sie können diese Einstellungen auch innerhalb einer Whitelist-Regel vornehmen.



Standardmäßig ist der Reiter „CD/DVD“ innerhalb einer Whitelist-Regel deaktiviert. Um diesen für eine Whitelist-Regel zu aktivieren, rechtsklicken Sie auf die entsprechende Regel und aktivieren Sie die Option „*CD/DVD-Optionen anzeigen*“.



Die Konfigurationsmöglichkeiten sind für die Klasse CD/DVD-Laufwerke und für eine einzelne Whitelist-Regel identisch.

Grundsätzlich wird der CD/DVD-Brenner von DriveLock vor dem Brenn-Programm versteckt (sog. Soft-Blocking) und die Software wird diese Laufwerk als CD/DVD-ROM Laufwerk erkennen, mit dem nicht gebrannt werden kann. Um das Soft-Blocking zu deaktivieren, aktivieren Sie die Option „*Soft-Blocking deaktivieren (…)*“.

> Wenn die Funktion Soft-Blocking deaktiviert wurde (oder wenn das Brenn-Programm wie z.B. Roxio in der Lage sein sollte, dieses Soft-Blocking zu umgehen), erhält der Benutzer die Meldung “*Zugriff verweigert*”, wenn er versucht, ein Medium zu erstellen.

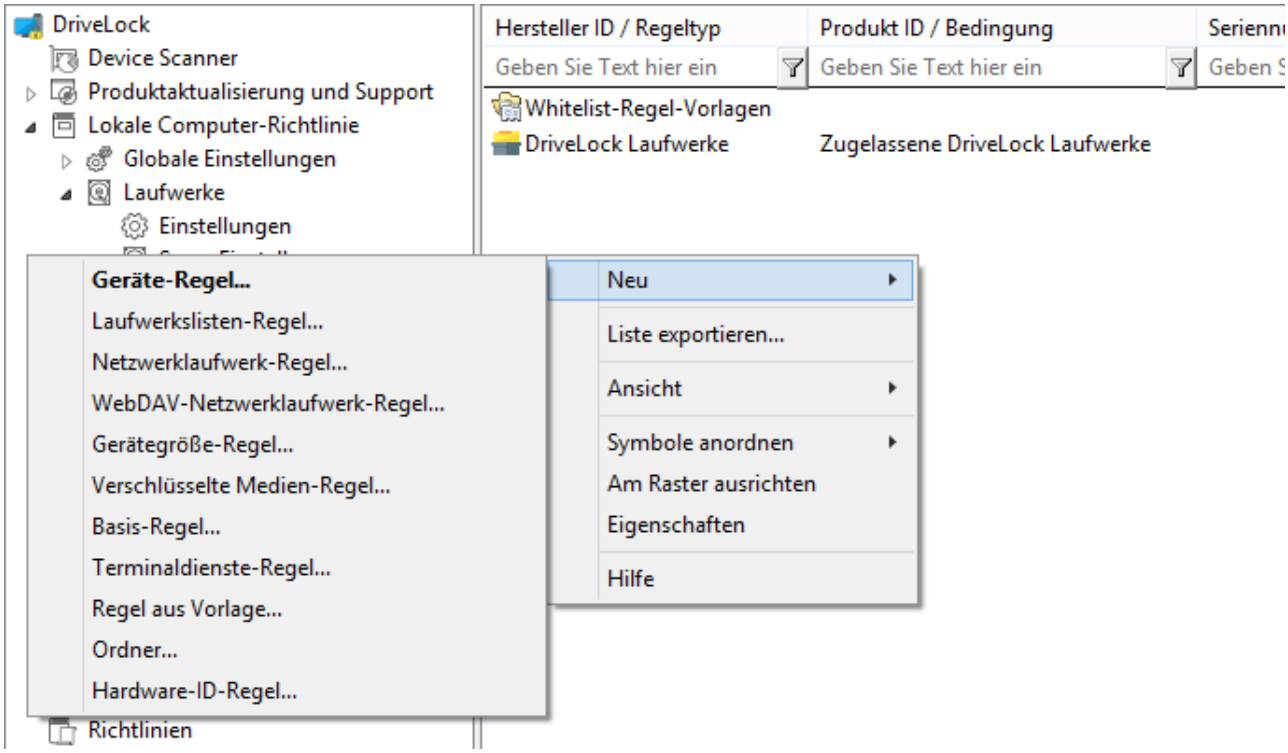
Um Benutzermeldungen zu deaktivieren, wenn das Soft-Blocking aktiv ist, wählen Sie die Option „*Keine Benutzerbenachrichtigungen anzeigen*“.

Um die durch Windows XP selbst zur Verfügung gestellten Möglichkeiten, eine CD/DVD zu erstellen, unabhängig von eingestellten Benutzerberechtigungen vollständig zu deaktivieren, markieren Sie die Option „*In Windows XP eingebaute Brennfunktion abschalten (immer)*“.

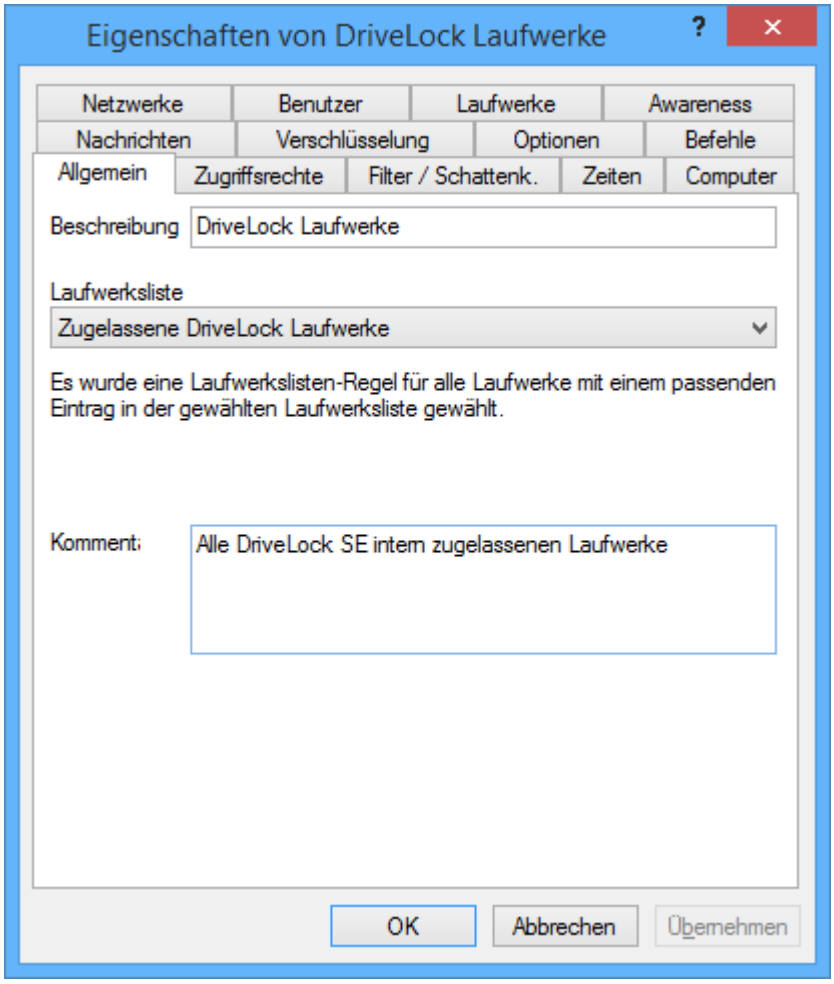
Damit es Administratoren ermöglicht wird zu erkennen, ob das Soft-Blocking aktiv ist, wählen Sie eine (oder beide) der Optionen unter „*Benutzer- und Support-Informationen*“ aus. DriveLock ändert die angezeigten Daten der Hersteller-ID bzw. der -Revisionsnummer.

Um eventuellen Kompatibilitätsproblemen zu begegnen, ist es möglich, mit der entsprechenden Option das Soft-Blocking auch komplett abzuschalten.

4.1.2.3.5 Laufwerkslisten-Regel erstellen



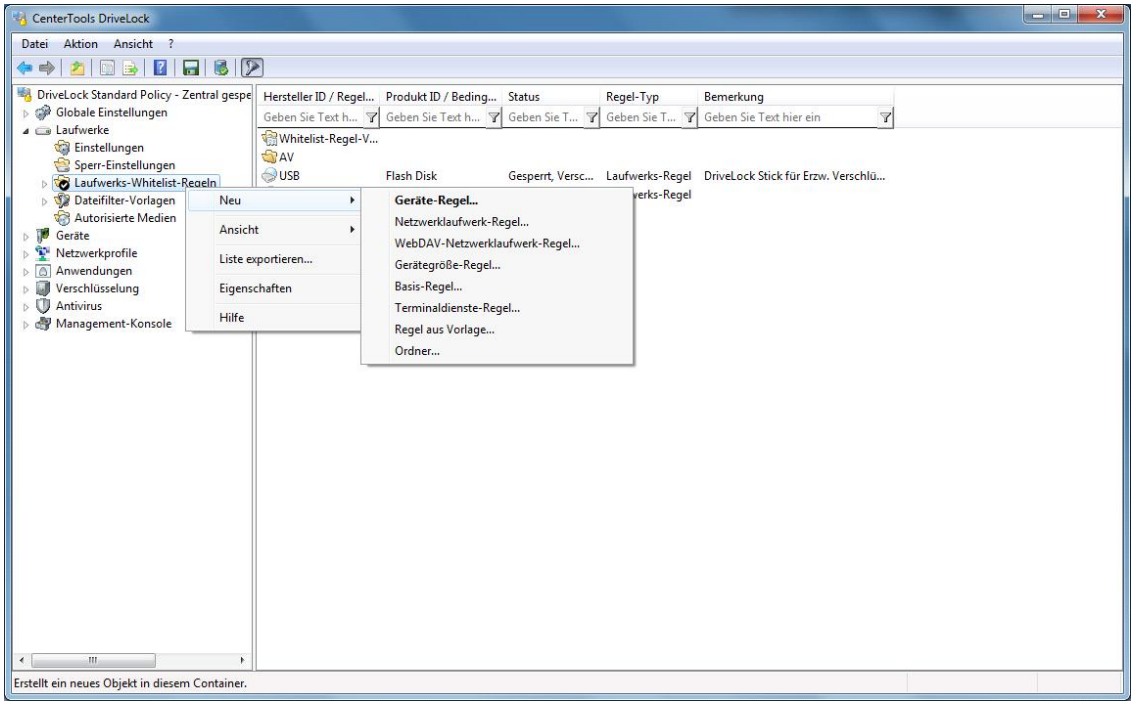
Rechtsklicken Sie auf **Laufwerks-White-List-Regel** und wählen "**Neu -> Laufwerkslisten-Regel**" aus dem Kontextmenü:



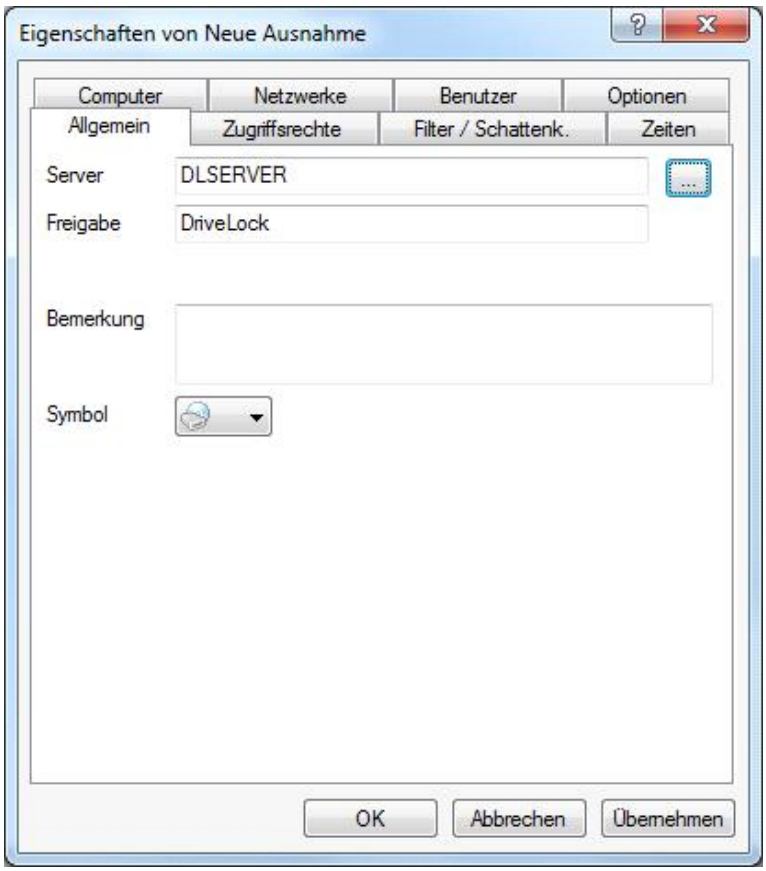
Nachdem Sie eine Beschreibung eingegeben haben, wählen Sie eine zuvor erstellte Laufwerksliste aus. Zusätzlich können Sie einen beschreibenden Kommentar eingeben.

4.1.2.3.6 Netzwerklaufwerk-Regel

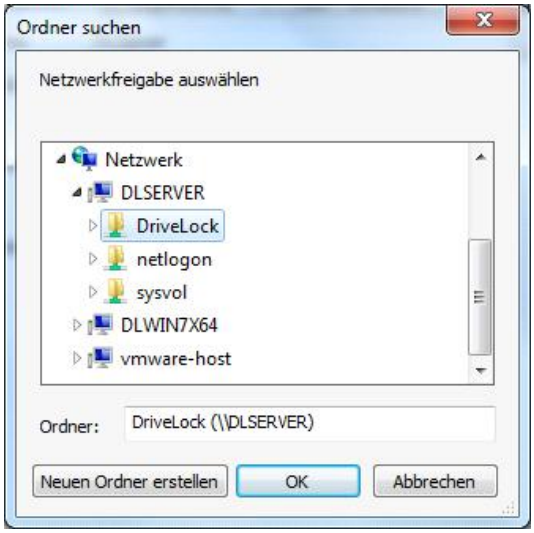
Mit Hilfe einer Netzwerklaufwerk-Regel kann eine Regel erstellt werden, die für im Netzwerk freigegebene Verzeichnisse (Netzwerk-Share) gilt.



Rechtsklicken Sie auf **Laufwerks-White-List-Regel** und wählen "**Neu -> Netzwerklaufwerk-Regel**" aus dem Kontextmenü.



Geben Sie nun den Namen des Servers und des freigegebenen Verzeichnisses an, oder klicken Sie auf die Schaltfläche „**...**", um den Auswahldialog zu öffenen:



Wählen Sie ein Netzwerk-Share aus und klicken Sie auf **OK**.

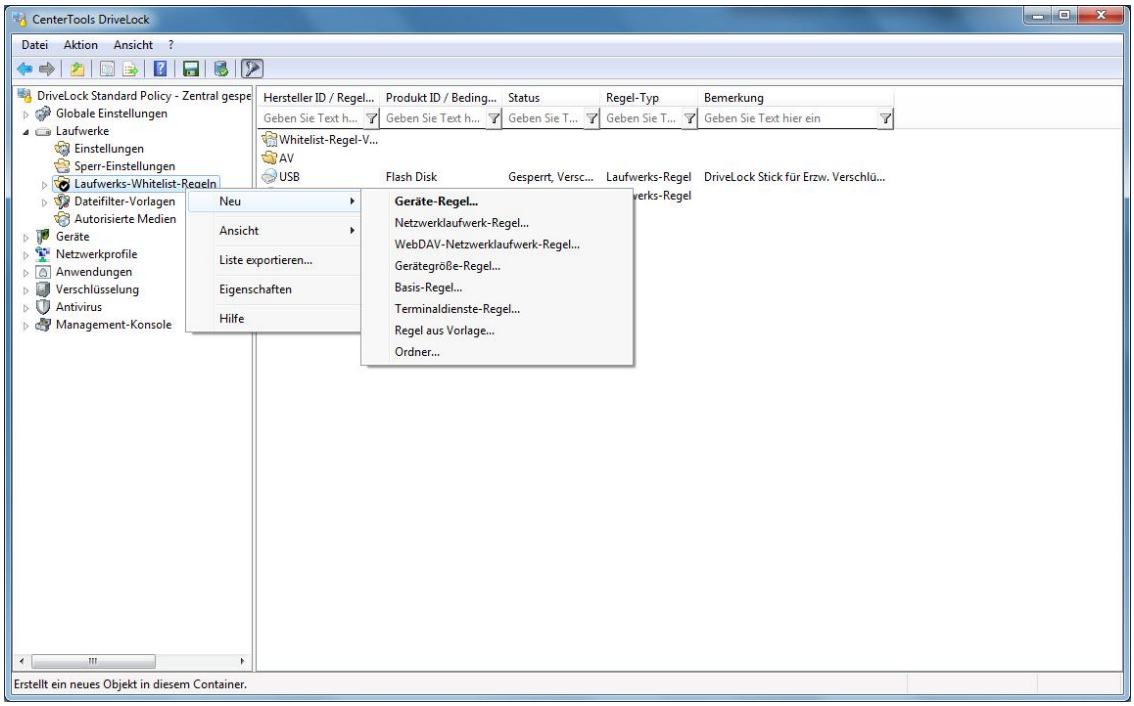
Die Auswahl wird nun entsprechend übernommen und die Werte an der richtigen Stelle eingetragen.

Die weiteren Konfigurationsmöglichkeiten werden im Abschnitt „Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren“ beschrieben.

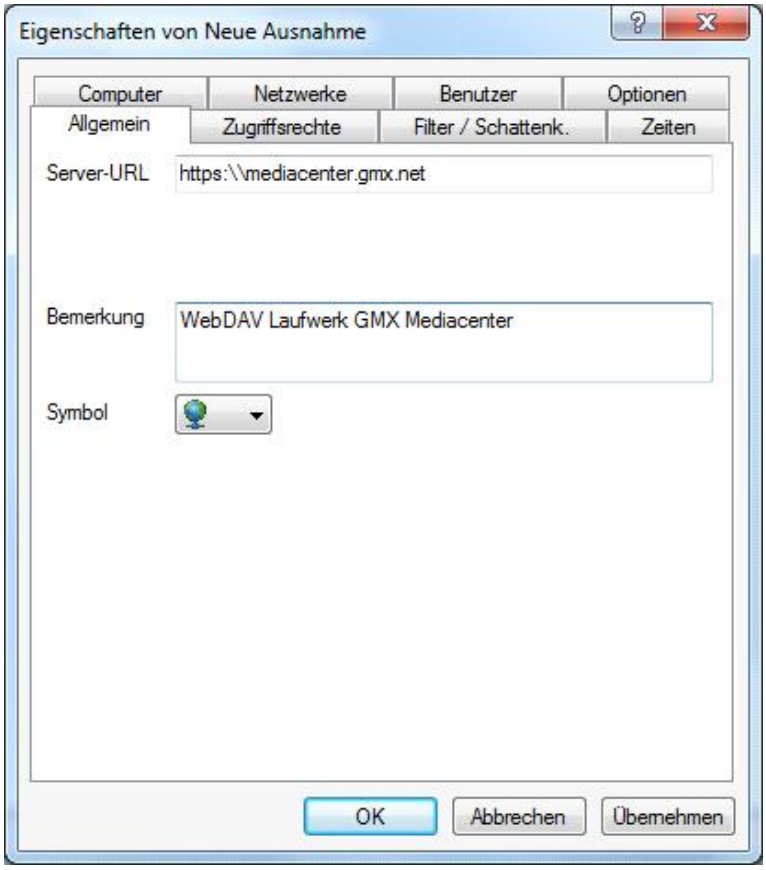
Bei dieser Art von Netzwerk-Laufwerken stehen Ihnen nicht alle verfügbaren Optionen (wie z.B. bei USB-Laufwerken zur Verfügung).

4.1.2.3.7 WebDAV-Netzwerklaufwerk-Regel

Mit Hilfe einer Gerätegröße-Regel kann eine Regel erstellt werden, die für Web-Laufwerke gilt, welche über eine URL und das WebDAV-Protokoll verbunden werden.



Rechtsklicken Sie auf **Laufwerks-White-List-Regel** und wählen “**Neu -> WebDAV-Netzwerklaufwerk-Regel**“ aus dem Kontextmenü.



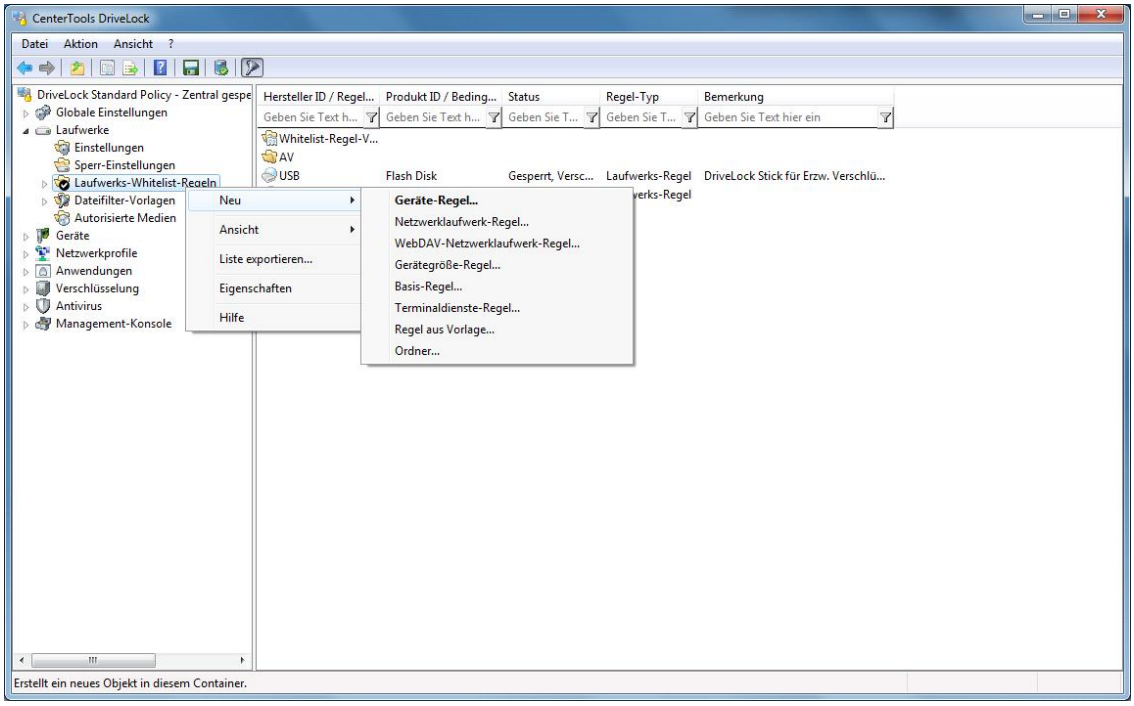
Geben Sie die URL für das WebDAV-Laufwerk beginnend mit „*http://*“ bzw. "*https://*" ein.

Die weiteren Konfigurationsmöglichkeiten werden im Abschnitt „Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren“ beschrieben.

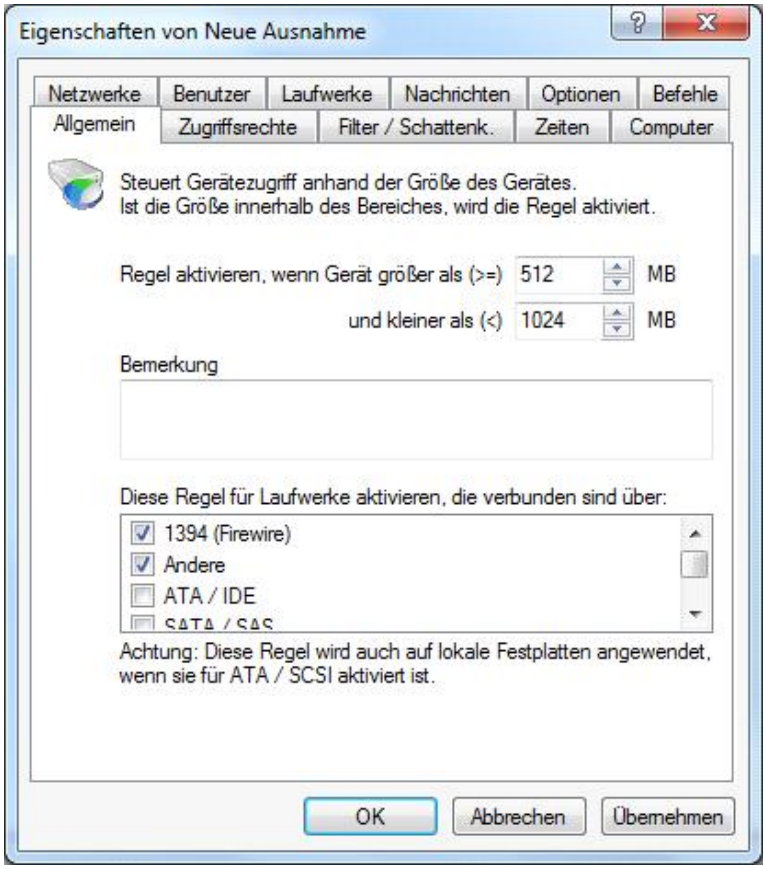
Bei dieser Art von Netzwerk-Laufwerken stehen Ihnen nicht alle verfügbaren Optionen (wie z.B. bei USB-Laufwerken zur Verfügung).

4.1.2.3.8 Gerätegröße-Regel

Mit Hilfe einer Gerätegröße-Regel kann eine Regel erstellt werden, die für Wechseldatenträger mit einer bestimmten Speicherkapazität gilt.



Rechtsklicken Sie auf **Laufwerks-White-List-Regel** und wählen "**Neu -> Gerätegröße-Regel**" aus dem Kontextmenü.



Geben Sie die gewünschte Größe an. Aktivieren Sie einen oder mehrere Bus-Typen, für die diese Regel gelten soll.

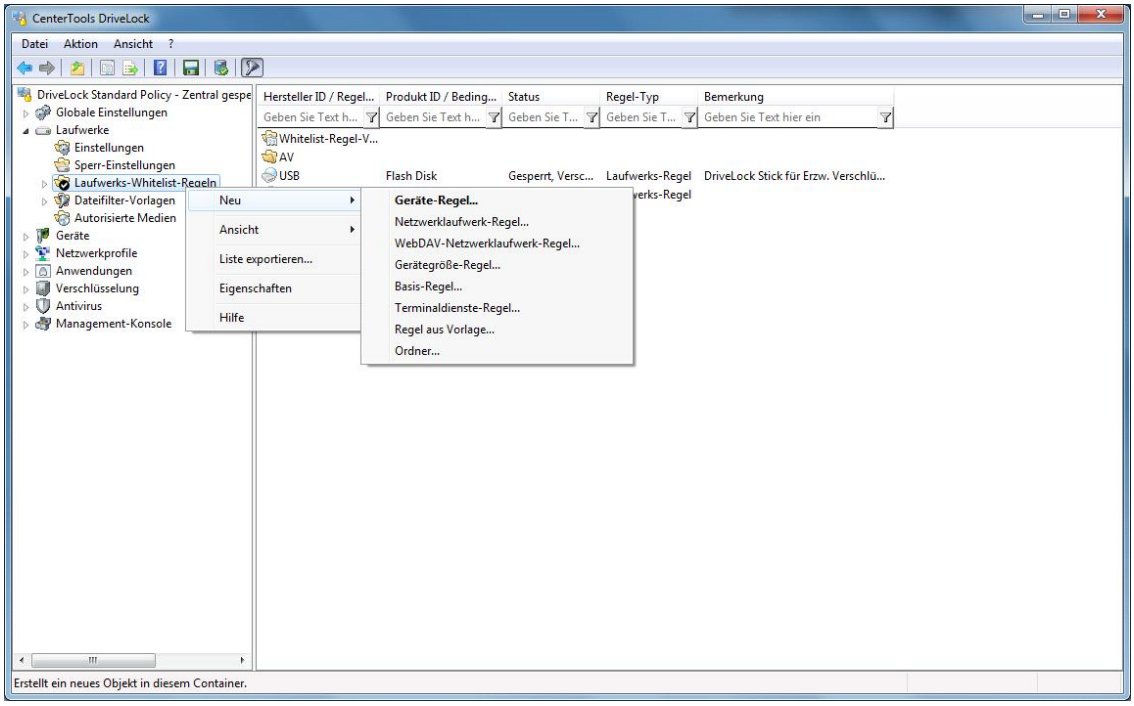
Diese Regel kann ggf. auch für die lokalen Festplatten gelten, wenn als Bus ATA bzw. SCSI aktiviert wurde. Sollten diese Laufwerke fälschlicherweise gesperrt werden, müssen Sie den Computer im „Abgesicherten

Modus“ starten und die Konfiguration entsprechend anpassen. Dies ist aber nur möglich, wenn Sie DriveLock so konfiguriert haben, dass der Agent im „Abgesicherten Modus“ nicht startet.

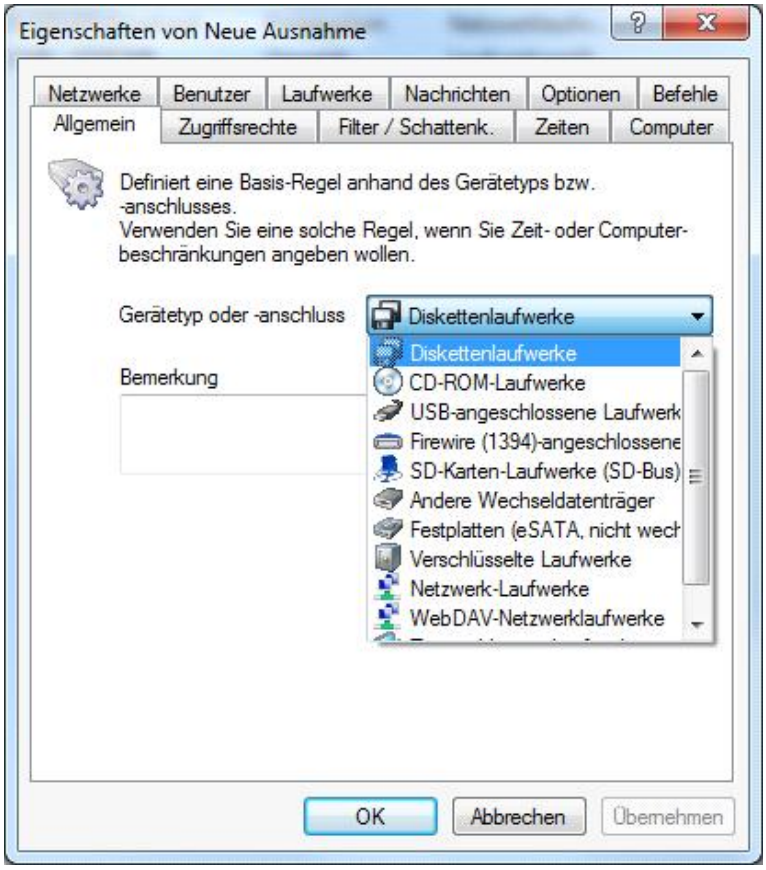
Die weiteren Konfigurationsmöglichkeiten werden im Abschnitt „Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren“ beschrieben.

4.1.2.3.9 Basis-Regel

Um Ausnahmen für eine bestimmte Klasse von Laufwerken zu definierten, kann eine Basis-Regel verwendet werden. Verwenden Sie diese Regel, um Zeitlimits, Computer- oder Netzwerkbeschränkungen für einen Gerätetyp festzulegen. Basis-Regeln sind sinnvoll, wenn die Regeln nicht gerätespezifisch oder abhängig von der Laufwerksgröße sein müssen.



Rechtsklicken Sie auf **Laufwerks-White-List-Regel** und wählen “**Neu -> Basis-Regel**“ aus dem Kontextmenü.



Wählen Sie einen Geräte- bzw. Anschlusstyp aus der Liste, um festzulegen für welchen der Laufwerkstypen die hier getroffenen Einstellungen gelten sollen.

Die weiteren Konfigurationsmöglichkeiten werden im Abschnitt „Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren“ beschrieben.

4.1.2.3.10 Terminaldienste-Regel

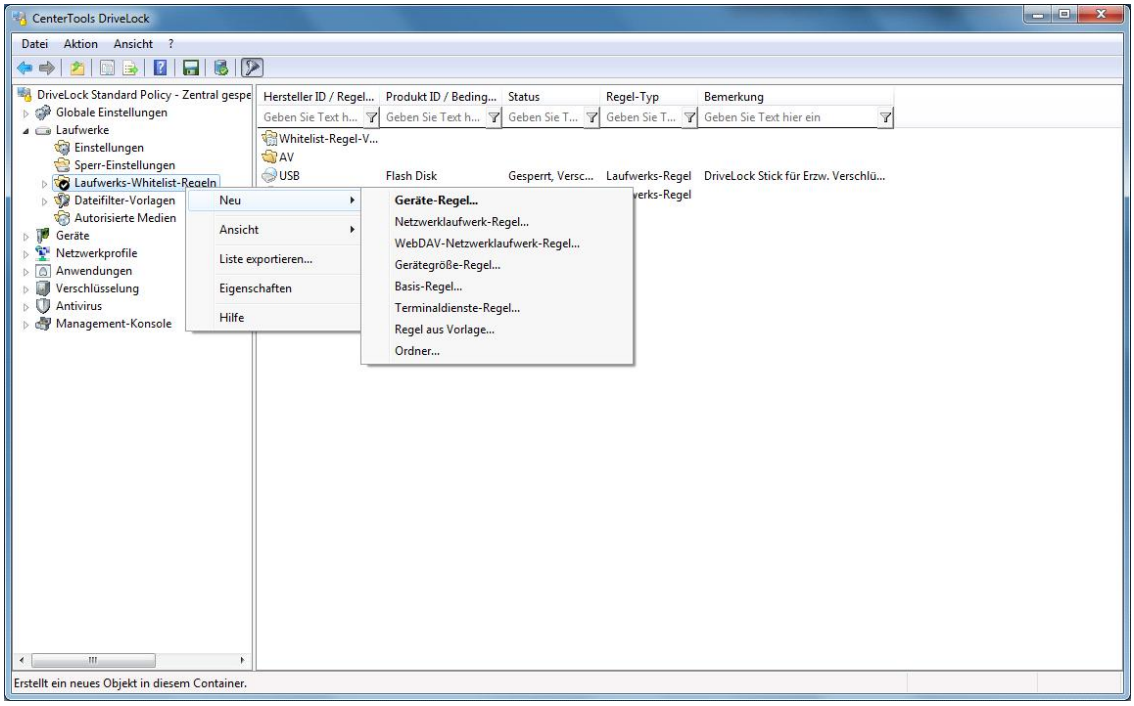
Mehr zum Aufbau der verschiedenen Terminalserver-Szenarien erhalten Sie Im Kapitel Terminalserver.

4.1.2.3.11 Regeln basierend auf einer Regelvorlage erstellen

Wenn es notwendig ist, mehrere Regeln zu erstellen, bei denen gewissen Einstellungen immer gleich bleiben (zum Beispiel für den gleichen Typ von USB-Datenträgern) und sich nur einige Einstellungen ändern, dann kann eine Whitelist-Regel-Vorlage sehr viel Zeit sparen.

Anstatt jede Regel einzeln Schritt für Schritt zu erstellen und immer wieder die gleichen Einstellungen auszuwählen, können Sie eine einzige Whitelist-Regel-Vorlage wie im Abschnitt „“ beschrieben erstellen, die die gleichbleibenden Einstellungen beinhaltet und die Sie bei der Erstellung der verschiedenen Regeln immer wieder als Vorlage verwenden.

Die Erstellung von Whitelist-Regel-Vorlagen ist in Abschnitt „Whitelist-Vorlagen erstellen“ beschrieben.

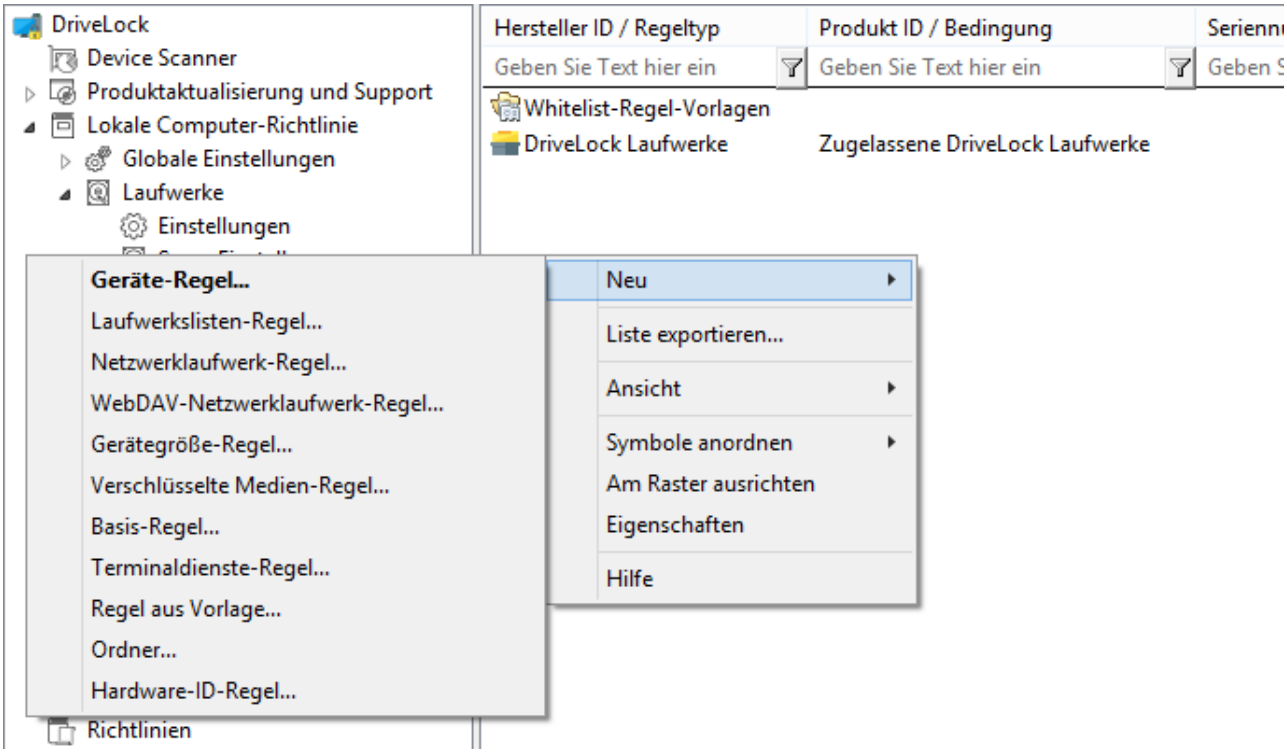


Rechtsklicken Sie auf **Laufwerks-White-List-Regel** und wählen "**Neu -> Regel aus Vorlage**" aus dem Kontextmenü.

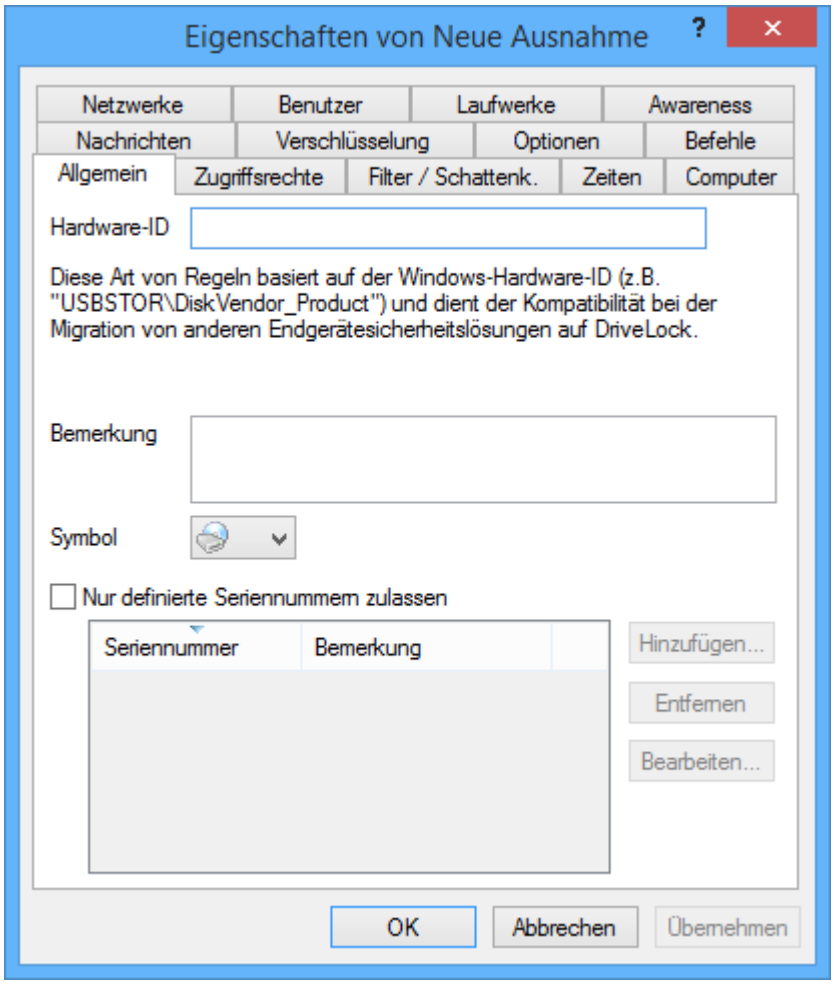
Wählen Sie anschließend eine Whitelist-Regel-Vorlage aus. Nun wird eine neue Whitelist-Regel erzeugt, die bereits die in der Vorlage enthaltenen Einstellungen beinhaltet. Ändern Sie nun die weiteren Konfigurationsmöglichkeiten entsprechend Ihren Anforderungen.

Die weiteren Konfigurationsmöglichkeiten werden im Abschnitt „Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren" beschrieben.

4.1.2.3.12 Hardware-ID-Regel



Rechtsklicken Sie auf **Laufwerks-White-List-Regel** und wählen "**Neu -> Hardware-ID-Regel**" aus dem Kontextmenü:



Geben Sie die gewünschte Hardware-ID ein, für die diese Einstellungen gelten sollen.

> Hardware-ID-Regeln sind in der Regel nur für Kunden interessant, die von einer anderen Endpoint Security Lösung zu DriveLock migrieren und die gewohnte Konfiguration übernehmen bzw. beibehalten wollen. Ansonsten stellen die Geräte-Regel eine praktikablere Konfigurationsmöglichkeit dar, bei der Produkt- und Hersteller-ID als Kriterium dienen.

Ebenso kann wie auch bei der Geräte-Regel eine zusätzliche Liste an Seriennummern definiert werden, um der Geltungsbereich weiter einzuschränken.

4.1.2.3.13 Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren

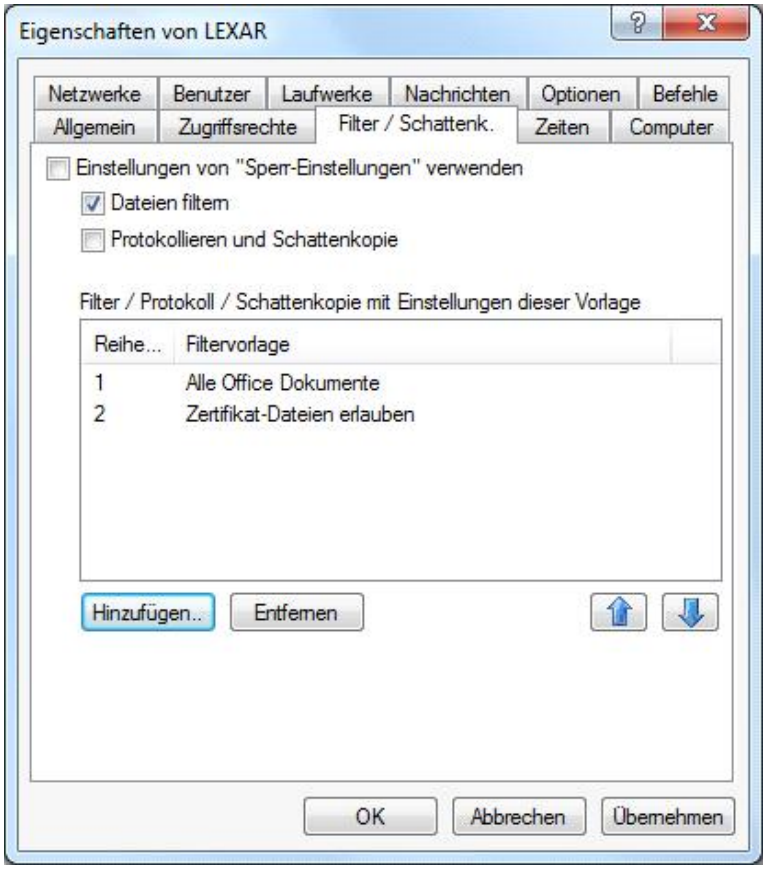
Die Reiter "**Zugriffsrechte**", "**Zeiten**", "**Computer**", "**Netzwerk**", „**Benutzer**", „**Laufwerke**", „**Meldungen**", „**Optionen**" und „**Befehle**" sind für fast alle Regeln gleichermaßen verfügbar und werden daher in diesem Abschnitt zusammenfassend beschrieben.

Der Reiter „**Filter / Schattenk.**" wird in den Abschnitten „Dateifilter-Vorlage verwenden" und "Schattenkopien in Laufwerksregeln " beschrieben.

4.1.2.3.13.1 Dateizugriff einschränken und überwachen

Wählen Sie den Reiter „**Zugriffsrechte**“, um den Zugriff auf bestimmte Dateitypen einzuschränken und die Dateizugriffe zu überwachen.

Es ist vorkonfiguriert, dass der eingestellte Filter des dazugehörigen Laufwerkstyps verwendet wird.



Wenn Sie einen eigenen Filter angeben möchten, deaktivieren Sie „**Einstellungen von „Sperr-Einstelllungen“ verwenden**“, markieren „**Dateien filtern**“ bzw. „**Protokollieren und Schattenkopie”**.

Klicken Sie auf **Hinzufügen**, um eine bestehende Dateifilter-Vorlage zur Liste hinzuzufügen. Mit **Entfernen** können Sie einen Listeneintrag wieder löschen.

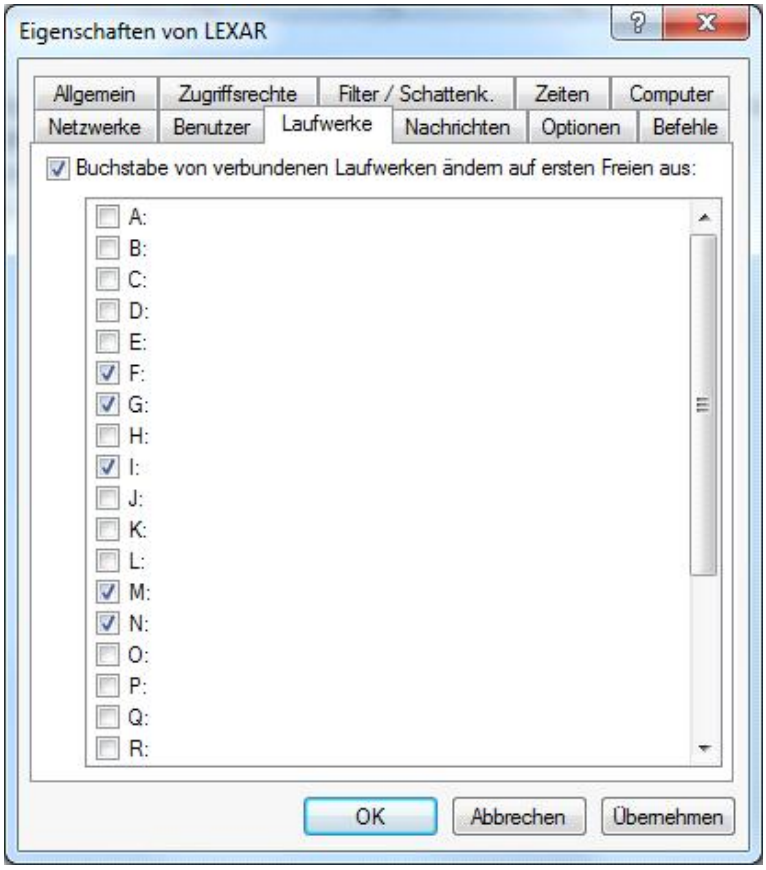
Verwenden Sie die beiden Symbole und , um die Reihenfolge der Dateifilter-Vorlagen zu ändern.

Wenn DriveLock eine Whitelist-Regel aktiviert, werden alle Dateifilter-Vorlagen in der Liste von Oben nach Unten ausgewertet. Die erste Vorlage, bei der die darin konfigurierten Kriterien (z.B. Dateigröße, Ausnahmen, Benutzer und Gruppen, Computer oder Netzwerkverbindungen) vollständig übereinstimmen, wird angewendet. Alle folgenden Vorlagen werden ignoriert.

4.1.2.3.13.2 Laufwerksbuchstaben zuweisen

Mit Hilfe dieser Option (Reiter “**Netzwerke**”) können Sie festlegen, welche Laufwerksbuchstaben verwendet werden, wenn ein bestimmter Wechseldatenträger an den Computer angeschlossen wird.

Wenn Sie mehr als einen Buchstaben aktivieren, wird der DriveLock Agent automatisch den ersten freien Buchstaben dem Laufwerk zuweisen.

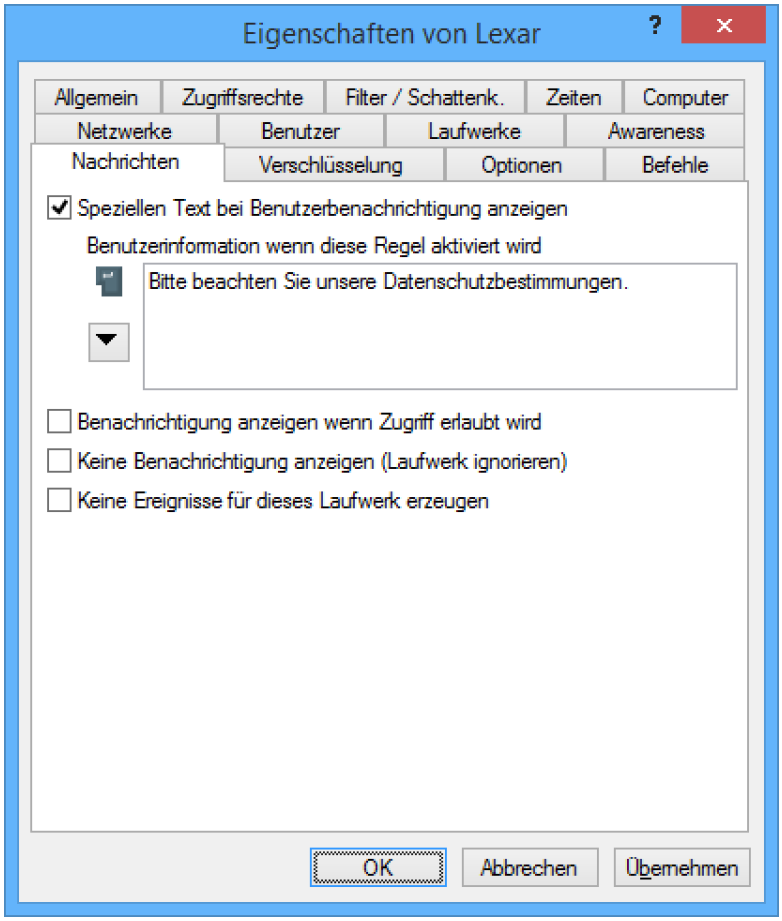


Achten Sie bitte darauf, nicht in Konflikt mit bereits vergebenen Laufwerksbuchstaben (z.B. für Netzwerk-Shares oder Benutzer-Home-Verzeichnisse) zu kommen.

4.1.2.3.13.3 Regelspezifische Benutzermeldungen einrichten

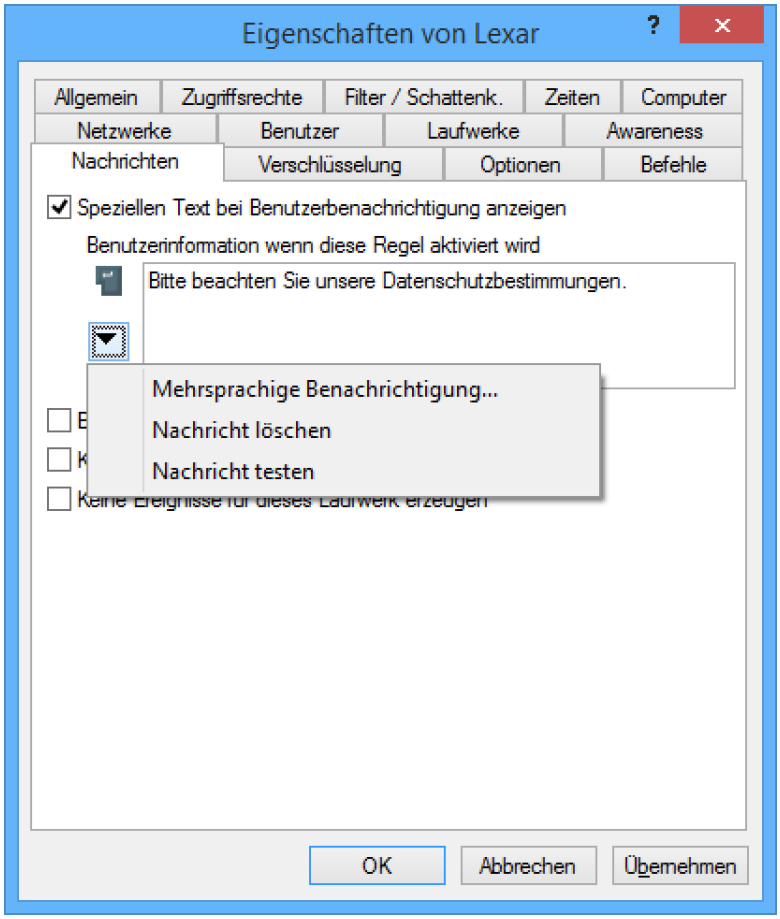
Mit Hilfe dieser Option (Reiter "**Nachrichten**") können Sie Benutzerbenachrichtigungen festlegen.

Sie können für jede Regel eine eigene Benutzermeldung konfigurieren. Sofern nicht anders eingestellt wird diese Meldung den Benutzern gezeigt, wenn der Zugriff auf ein Laufwerk verweigert wird.



Um eine eigene Meldung für eine Regel zu konfigurieren, aktivieren Sie die Option „**Speziellen Text bei Benutzerbenachrichtigung anzeigen**“. Geben Sie anschließend einen Text ein, welcher unabhängig von der aktuell eingestellten Systemsprache angezeigt wird. Diese sprachunabhängige Meldung wird durch ein Tastensymbol an der linken oberen Ecke des Eingabefeldes dargestellt.

Sofern Sie mehrsprachige Benutzermeldungen definiert haben, können Sie auch eine dieser Nachrichten auswählen. Klicken Sie dazu auf den Pfeil und wählen Sie aus der Liste „**Mehrsprachige Benachrichtigung**“ aus.



Mehrsprachige Meldungen enthalten für eine Nachricht verschiedene Texte für unterschiedliche Sprachen. Bevor Sie mehrsprachige Benutzermeldungen verwenden können, müssen diese im Bereich „**Globale Einstellungen**“ der Richtlinie definiert werden. Wenn Sie eine derartige Meldung verwenden, zeigt DriveLock den Text an, welcher für die aktuelle Systemsprache des angemeldeten Benutzers konfiguriert wurde.

Wählen Sie eine Meldung aus und bestätigen diese mit **OK**.

Diese sprachabhängige Meldung wird durch ein Sprechblasen-Symbol an der linken oberen Ecke des Eingabefeldes dargestellt.

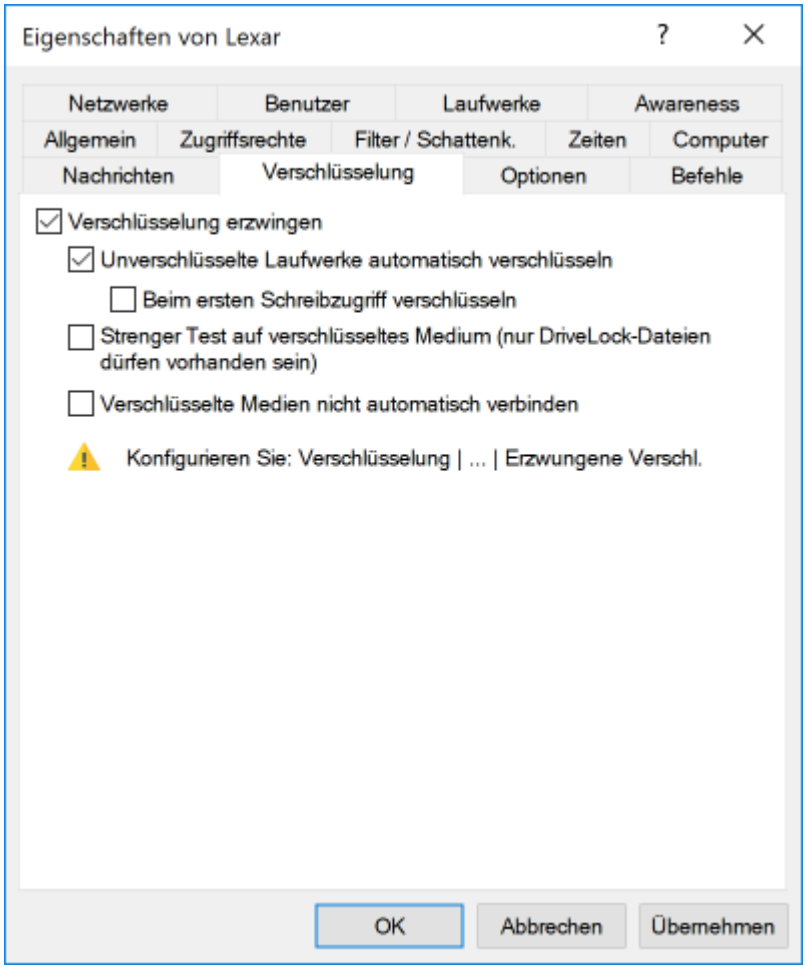
Wenn Sie möchten, dass die Meldung auch dann angezeigt wird, wenn ein Zugriff durch den Benutzer möglich ist, dann aktivieren Sie die entsprechende Option. Um die Anzeige von Meldungen generell zu unterbinden (auch die Anzeige von Standard-Benachrichtigungen), aktivieren Sie „*Keine Benachrichtigung anzeigen*“.

Wenn Sie die Erzeugung von Überwachungsereignissen für diese Whitelist-Regel unterdrücken wollen, markieren Sie bitte „*Keine Ereignisse für dieses Laufwerk erzeugen*“.

4.1.2.3.13.4 Weitere Optionen

Verschlüsselung

Mit Hilfe der Reiters “**Verschlüsselung**” können Sie Einstellungen zur erzwungenen Verschlüsselung festlegen.



Sie können, indem Sie "**Verschlüsselung erzwingen**" aktivieren, spezifizieren, dass jedes der betroffenen Geräte nur dann freigegeben wird, wenn es zuvor verschlüsselt wurde. Zusätzlich lässt sich festlegen, dass unverschlüsselte Laufwerke automatisch verschlüsselt werden.

> Als "Verschlüsselt" werden diejenigen Laufwerke angesehen, die entweder mit File Protection oder BitLocker To Go verschlüsselt wurden oder eine Container-Datei mit der Dateiendung *.DLV enthalten.

Wenn Sie die Option „**Strenger Test auf verschlüsseltes Medium (nur DriveLock Dateien)**" aktivieren, dürfen auf einem Laufwerk mit Container-Verschlüsselung nur zu DriveLock gehörenden Dateien vorhanden sein (für File Protection oder BitLocker To Go hat diese Option keine Auswirkung).

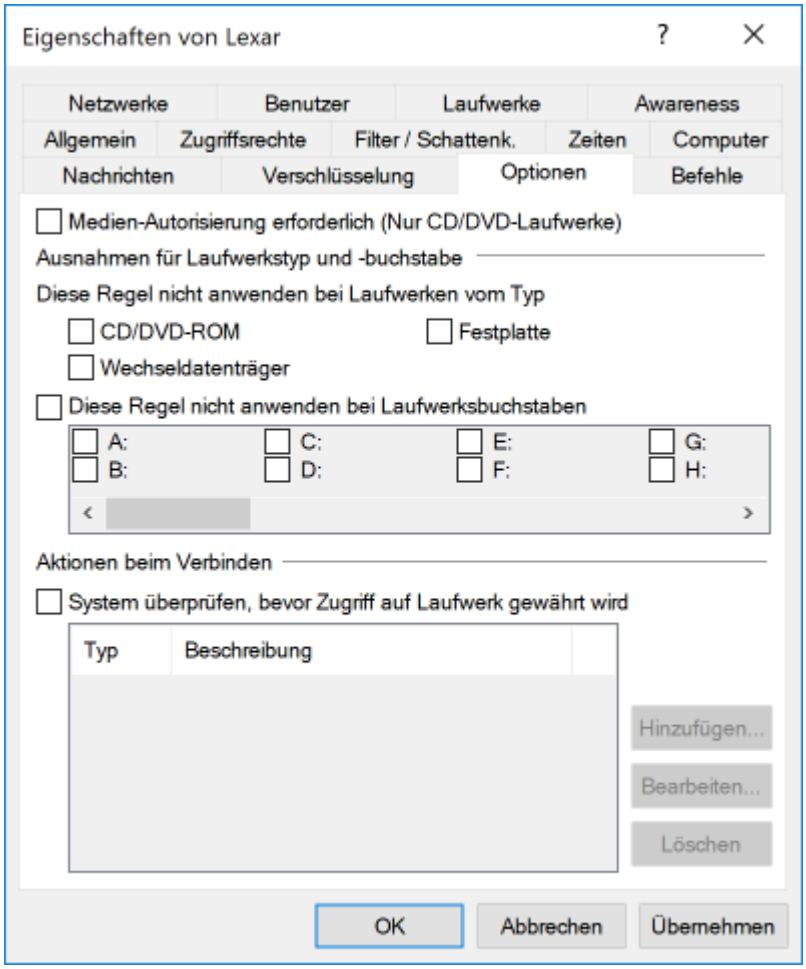
Die Option „**Beim ersten Schreibzugriff verschlüsseln**" bewirkt, dass der Assistent zur automatischen Verschlüsselung erst dann startet, wenn zum ersten Mal nach dem Verbinden ein Schreibzugriff auf das Laufwerk erfolgt.

Sie können zusätzlich festlegen, dass bereits verschlüsselte Medien nicht automatisch verbunden werden sollen. In diesem Fall kann der Benutzer diesen Vorgang manuell starten.

> Für CD-, Netzwerk- oder WebDAV-Laufwerke ist die Funktion "Verschlüsselung erzwingen" aus technischen Gründen nicht vorhanden.

Optionen

Mit Hilfe der Reiters "**Optionen**" können Sie weitere Einstellungen festlegen.



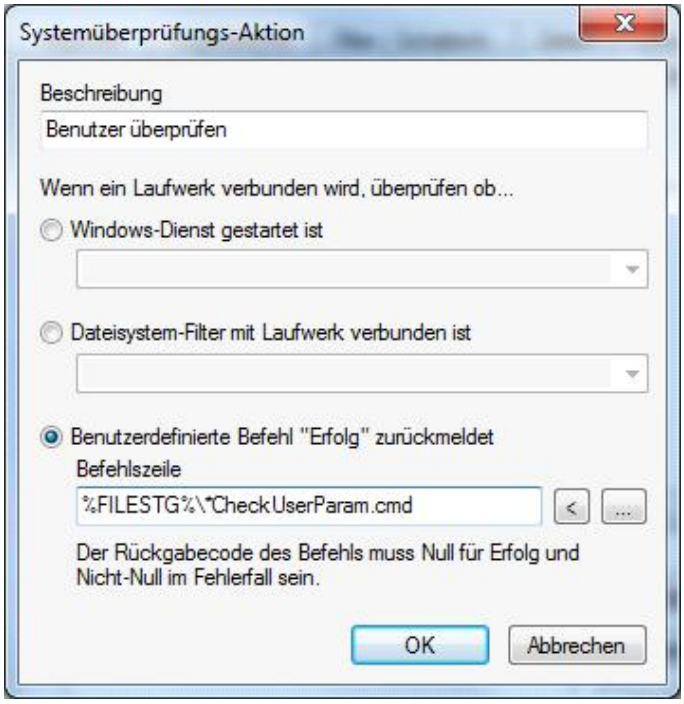
Aktivieren Sie "**Medien-Autorisierung erforderlich**", wenn nur zuvor autorisierte Medien verwendet werden dürfen (siehe Abschnitt "Medien-Autorisierung verwenden").

> Die Option "*Medien-Autorisierung erforderlich*" muss bei CD/DVD-Laufwerken auch dann aktiviert werden, wenn Sie möchten, dass jedes Mal eine Verwendungsrichtlinie angezeigt wird, wenn eine neue CD/DVD eingelegt wurde. Ansonsten würde eine Verwendungsrichtlinie nur dann angezeigt, wenn das (wie z.B. es bei USB-Laufwerken der Fall ist) Laufwerk an sich gewechselt wurde, was bei CD/DVD-Laufwerken relativ selten der Fall sein dürfte.

Um zu verhindern, dass diese Regel bei bestimmten Wechseldatenträgertypen oder Laufwerksbuchstaben nicht aktiviert wird, markieren Sie die entsprechende Option. Diese Einstellungen können zur Unterscheidung von Laufwerken verwendet werden, die unter Windows mit ein und derselben Herstellerkennung, Produktname und Seriennummer erscheinen (z.B. U3-Geräte, die sowohl als Wechseldatenträger als auch als CD-Laufwerk erkannt werden). Um unterschiedliche Zugriffsregeln für diese zu erstellen, konfigurieren Sie separate Whitelist Regeln dafür.

DriveLock bietet Ihnen zusätzlich noch die Möglichkeit, ganz bestimmte Systembedingungen zu überprüfen, bevor der Zugriff auf ein Laufwerk ermöglicht wird (Option „**System überprüfen, bevor Zugriff auf Laufwerk gewährt wird**").

Dazu aktivieren Sie diese Option und Klicken auf **Hinzufügen**, um ein oder mehrere Systemprüfungen hinzuzufügen. Mit **Entfernen** können Sie eine Systemprüfung wieder löschen.



Die folgenden drei Prüfungsarten stehen dabei zur Verfügung:

- Prüfen, ob ein ganz bestimmter Dienst unter Windows gestartet ist
- Prüfen, ob der DriveLock Dateisystemfilter mit diesem Laufwerk verbunden ist
- Ausführung eines eigenen Kommandozeilenbefehls oder eines Skripts, welches eine beliebige Prüfung durchführt und über den Rückgabecode 0 eine erfolgreiche Prüfung meldet.

Ein Programm oder Skript kann dabei entweder als Datei auf dem Arbeitsplatzrechner vorhanden sein, oder über den Richtlinienspeicher innerhalb der Konfiguration von DriveLock mit verteilt werden. Klicken Sie „…“, um einen Dateinamen auszuwählen.

> Der Richtliniendateispeicher ist ein Datei-Container, der als Teil einer lokalen Richtlinie, einer Gruppenrichtlinie oder einer Konfigurationsdatei gespeichert wird. Er kann beliebige Dateien (wie z.B. Skripte oder Anwendungen) enthalten, die automatisch mit einer DriveLock Konfiguration verteilt werden.

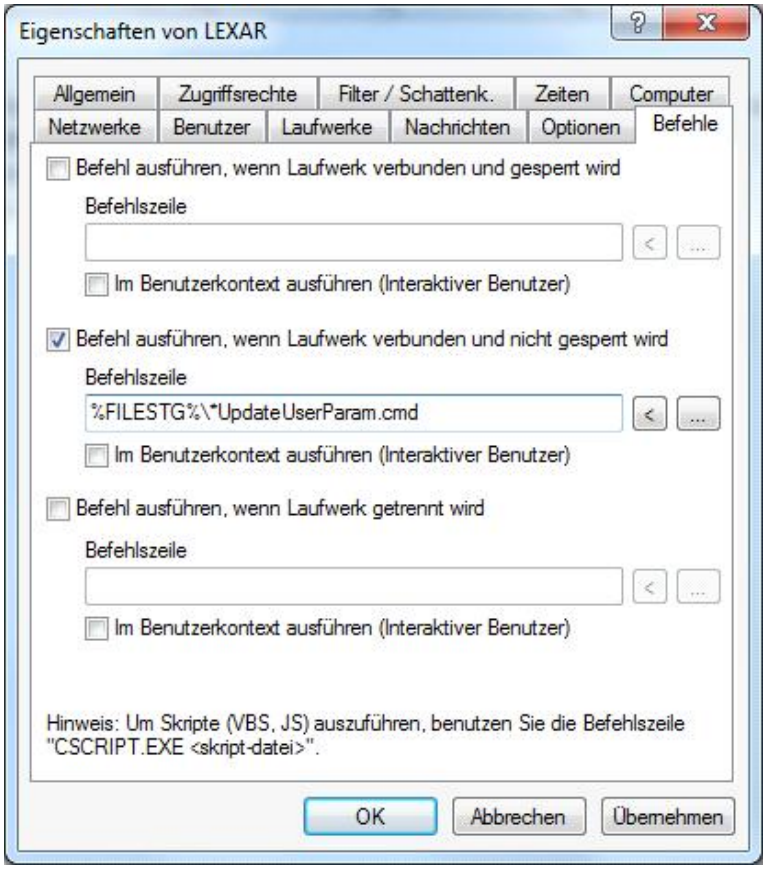
Dateien aus dem Richtlinienspeicher sind mit einem „*“ markiert.

Klicken Sie OK, um die Systemprüfung hinzuzufügen.

4.1.2.3.13.5 Ausführung von eigenen Kommandos

Eine sehr nützliche Funktion von DriveLock ermöglicht es Ihnen, bei den folgend genannten Aktionen einen Kommandozeilenbefehl ausführen zu lassen:

- Ein Wechseldatenträger wurde angeschlossen und von DriveLock gesperrt
- Ein Wechseldatenträger wurde angeschlossen und von DriveLock freigegeben
- Ein Wechseldatenträger wurde entfernt



Die Befehlszeile kann einen beliebigen über die Kommandozeile ausführbaren Befehl enthalten. Somit können Sie zum Beispiel ein Programm (*.exe), ein Visual Basic Skript (*.vbs) oder Skripts für die neue Windows PowerShell ausführen lassen.

Auf diese Weise ist es möglich, auf diese Ereignisse in vielen erdenklichen Variationen zu reagieren. Zum Beispiel können Sie einen Backup-Prozess starten, wenn eine bestimmte externe Festplatte angesteckt wird. Oder Sie verwenden z.B. ein PowerShell-Skript, um Bilder von einer Kamera ganz automatisch auf einen vordefinierten Netzwerkshare zu kopieren.

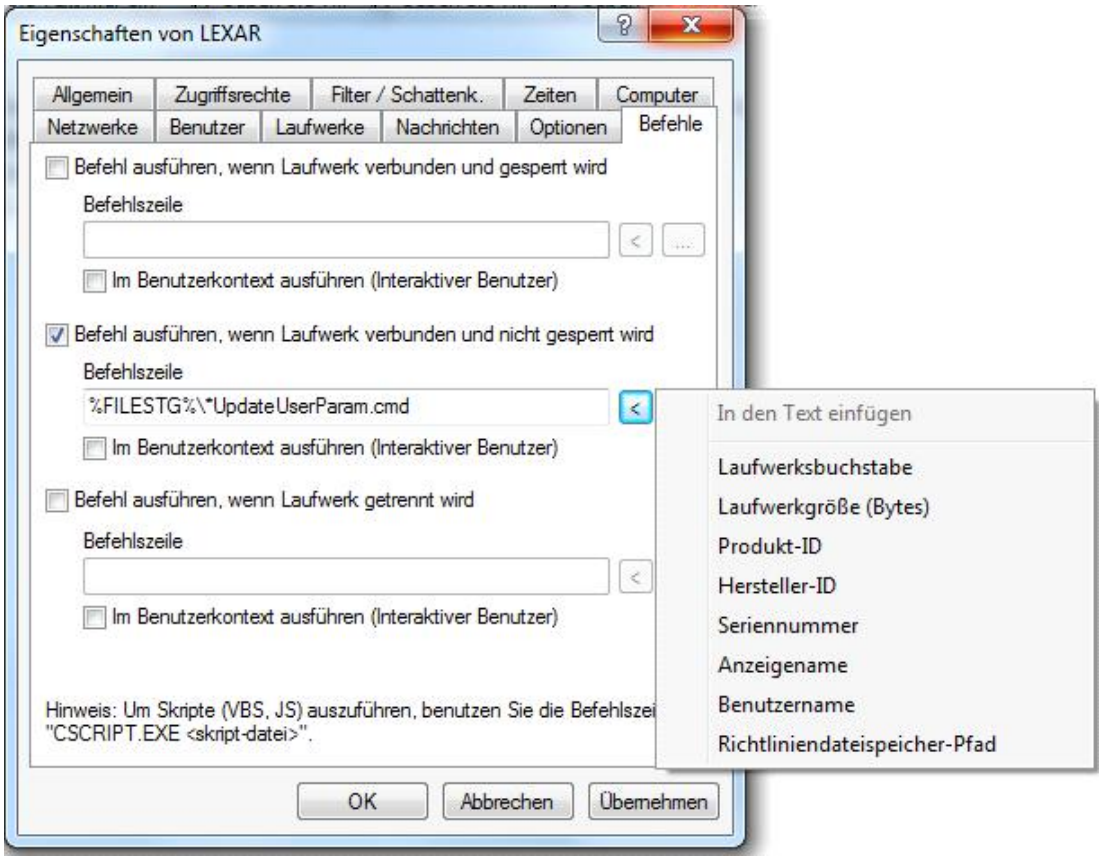
> Sie können an dieser Stelle den Kommandozeilen-Befehl auch verwenden, um das angeschlossene Laufwerk mit Hilfe des installierten Anti-Virus Programms zu scannen.

> Um ein VB-Skript auszuführen, müssen Sie den vollständigen Pfad zur Skript-Datei angeben (z.B. "*cscript c:\programing\scripts\meinscript.vbs*").

Es gibt einige Variablen, die innerhalb der Befehlszeile verwendet werden können und die durch den Agenten vor der Ausführung durch die aktuellen Werte ersetzt werden:

%LTR%	Zugewiesener Laufwerksbuchstabe
%NAME%	Name des Laufwerkes
%SIZE%	Größe des Laufwerkes
%USER%	Name des aktuell angemeldeten Benutzers
%SERNO%	Seriennummer des Laufwerkes

%HWID%	Hardware ID des Gerätes
%PRODUCT%	Produkt-ID des Laufwerkes
%VENDOR%	Hersteller des Laufwerkes
%FILESTG%	Pfad zu einer Datei innerhalb des Richtliniendateispeichers



Klicken Sie dazu "<" und wählen einer dieser Variablen aus, damit diese an der aktuellen Cursor-Position eingefügt wird.

Klicken Sie auf die Schaltfläche „…", um einen Dateinamen an der aktuellen Cursor-Position einzufügen. Dabei können Sie zwischen zwei Möglichkeiten wählen:

- *Dateisystem*: Die Datei ist auf der lokalen Festplatte des Computers vorhanden
- *Richtliniendateispeicher*: Die Datei aus dem Richtliniendateispeicher von DriveLock wird verwendet.

> Der Richtliniendateispeicher ist ein Datei-Container, der als Teil einer lokalen Richtlinie, einer Gruppenrichtlinie oder einer Konfigurationsdatei gespeichert wird. Er kann beliebige Dateien (wie z.B. Skripte oder Anwendungen) enthalten, die automatisch mit einer DriveLock Konfiguration verteilt werden.

Eine Datei, die aus dem Richtliniendateispeicher geladen wird, ist durch ein „*" gekennzeichnet. Wenn Sie eine Datei aus dem Richtliniendateispeicher verwenden, müssen Sie ebenfalls die Variable %FILESTG% als relativen Pfad verwenden.

Darüber hinaus können Sie festlegen, ob der neue Prozess mit der gleichen Berechtigung laufen soll, die auch der Agent besitzt oder ob er im Benutzerkontext (d.h. unter der Kennung des aktuell angemeldeten Benutzers) laufen soll.

4.1.2.4 Dateifilter konfigurieren

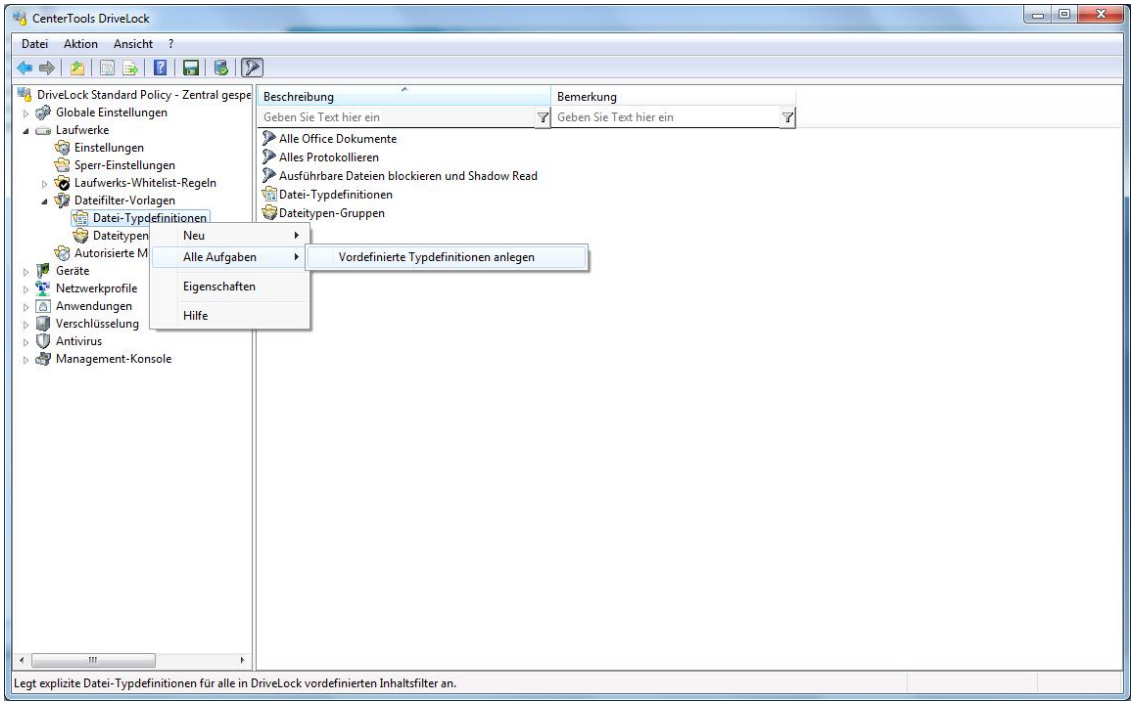
Mit Hilfe von Dateifiltern können Sie eigene Schreib- und/oder Leseberechtigungen für konfigurierte Wechseldatenträger und/oder individuelle Whitelist-Regeln definieren. Diese Filter können unterscheiden zwischen Lese- oder Schreibzugriff und überprüfen auch den Dateitypen. Zum Beispiel ist es möglich, einen Dateifilter zu erstellen, der Lese-Berechtigung für Grafik-Dateien (*.jpg) und Schreibberechtigung für Word-Dokumente (*.doc) enthält. Mit Filtervorlagen können entsprechend Ihrer Anforderungen mehrere dieser Regelungen erstellt werden.

DriveLock beinhaltet darüber hinaus einen sog. Datei-Header-Check, d.h. DriveLock überprüft, ob eine Datei mit einer bestimmten Endung (z.B. *.doc) auch wirklich ein Word-Dokument und keine umbenannte MP3-Datei ist. Dabei ist zu beachten, dass einige Dateiformate den gleichen Header besitzen (z.B. Microsoft Office-Dokumente), während andere keinen spezifischen oder gar einen zufälligen Datei-Header besitzen.

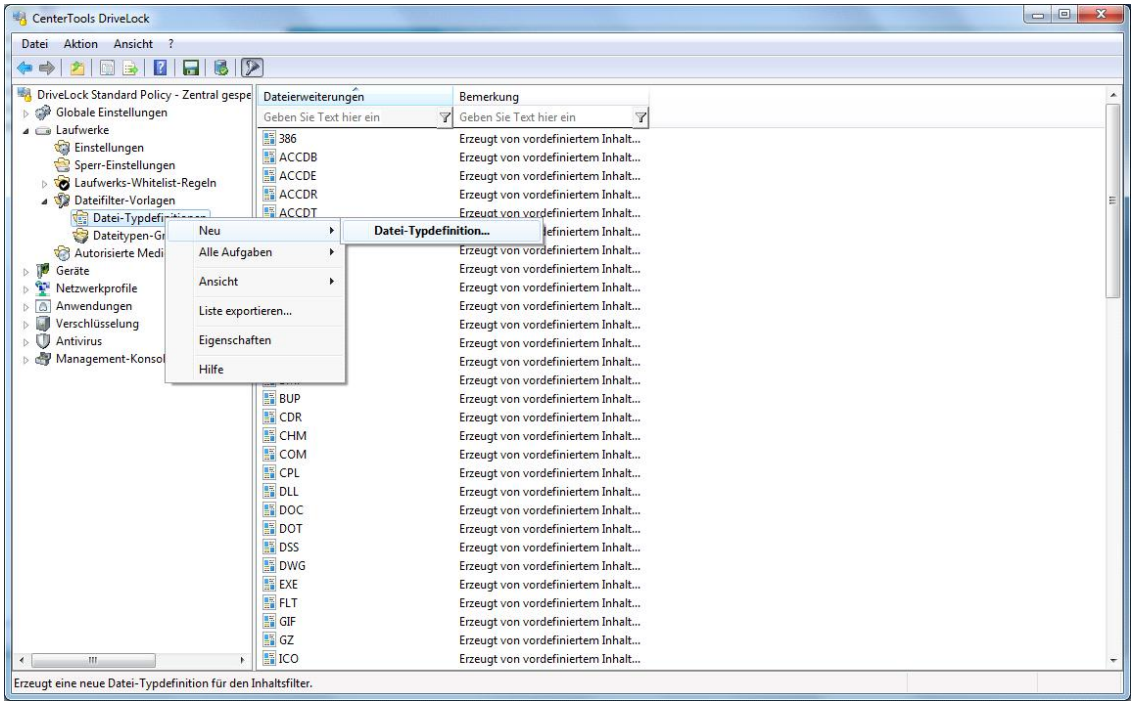
Nachdem Sie eine Dateifilter-Vorlage erstellt haben, kann diese im Rahmen einer Konfiguration eines Laufwerkstypen oder innerhalb einer Whitelist-Regel für Laufwerke verwendet werden.

4.1.2.4.1 Datei-Typdefinitionen erstellen

Sie können mit Hilfe von DriveLock auch eigene Dateitypen mit bestimmten Datei-Endungen und Inhalt definieren. Damit die Erstellung für Sie vereinfacht wird, können die bereits eingebauten Definitionen verwendet werden.

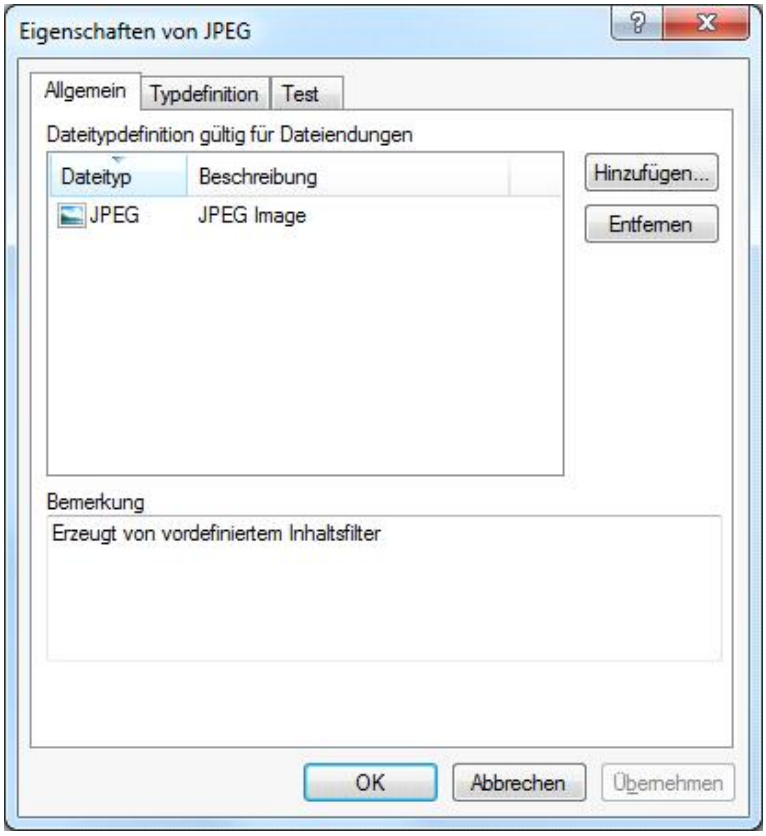


Bevor die eingebauten Typen verwendet werden können, müssen diese erst durch einen Rechtsklick auf **Datei-Typdefinitionen** und Auswahl von **Alle Aufgaben -> Vordefinierte Typdefinitionen anlegen** erzeugt werden.



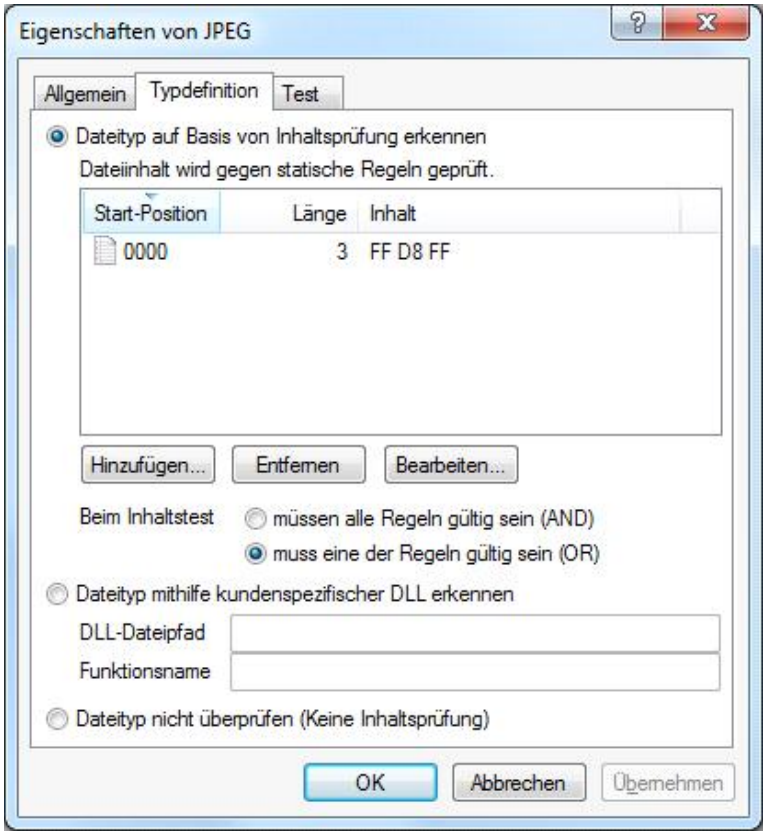
Um einen neuen Dateitypen zu erstellen, rechtsklicken Sie auf **Datei-Typdefinitionen** und wählen **Neu _> Datei-Typdefinition**.

Wenn Sie eine bestehende Definition bearbeiten möchten, doppelklicken Sie auf diese.



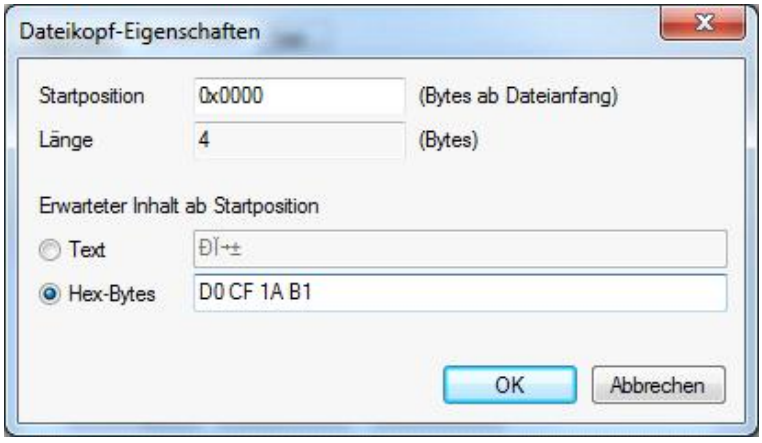
Verwenden Sie die Schaltfläche **Hinzufügen**, um weitere Datei-Endungen, die verwendet werden sollen, zur Liste hinzuzufügen.

Anschließen aktivieren Sie den Reiter **Typdefinition**.



Eine Datei kann entweder durch eine Überprüfung des Inhaltes oder den Aufruf einer kundenspezifischen DLL – die Sie selbst erstellen können – verifiziert werden.

Verwenden Sie **Hinzufügen**, **Entfernen** oder **Bearbeiten**, um die Inhaltsüberprüfungen zu verändern.



Eine Inhaltsprüfung verwendet einen sog. Offset (einen Wert in hexadezimaler Schreibweise) und eine Bytefolge, entweder in Textform oder ebenfalls als hexadezimal dargestellte Bytefolge. Die Länge wird automatisch eingetragen. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.

Geben Sie an, ob alle oder nur einer der angegebenen Überprüfungen für eine Verifikation erfolgreich sein muss.

Wenn Sie eine eigene DLL (Dynamic Link Library) verwenden, geben Sie den vollen Pfad und den Namen der enthaltenen Funktion an.

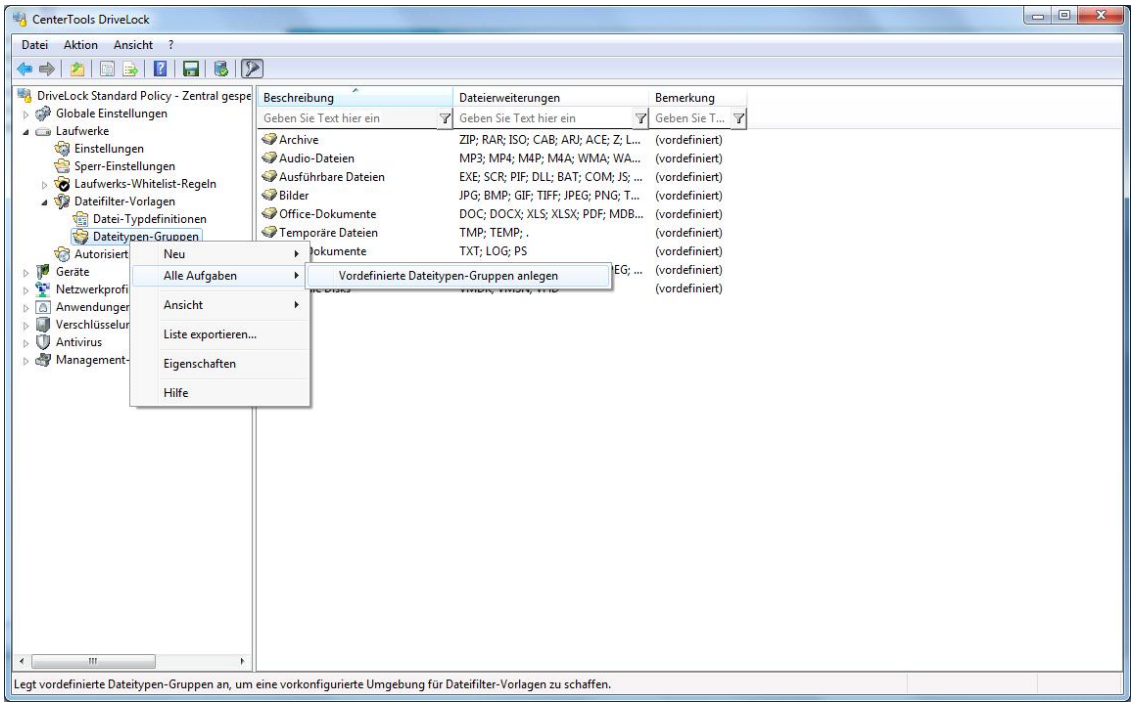
Die angegebene DLL muss lokal auf der Festplatte des Arbeitsplatzrechners vorhanden sein. Es ist nicht möglich, einen UNC-Pfad anzugeben oder den Richtlinienspeicher zu verwenden.

Wenn DriveLock nur die Dateiendung, nicht aber den Dateiinhalt prüfen soll, aktivieren Sie die Option „*Dateityp nicht überprüfen (Keine Inhaltsprüfung)*".

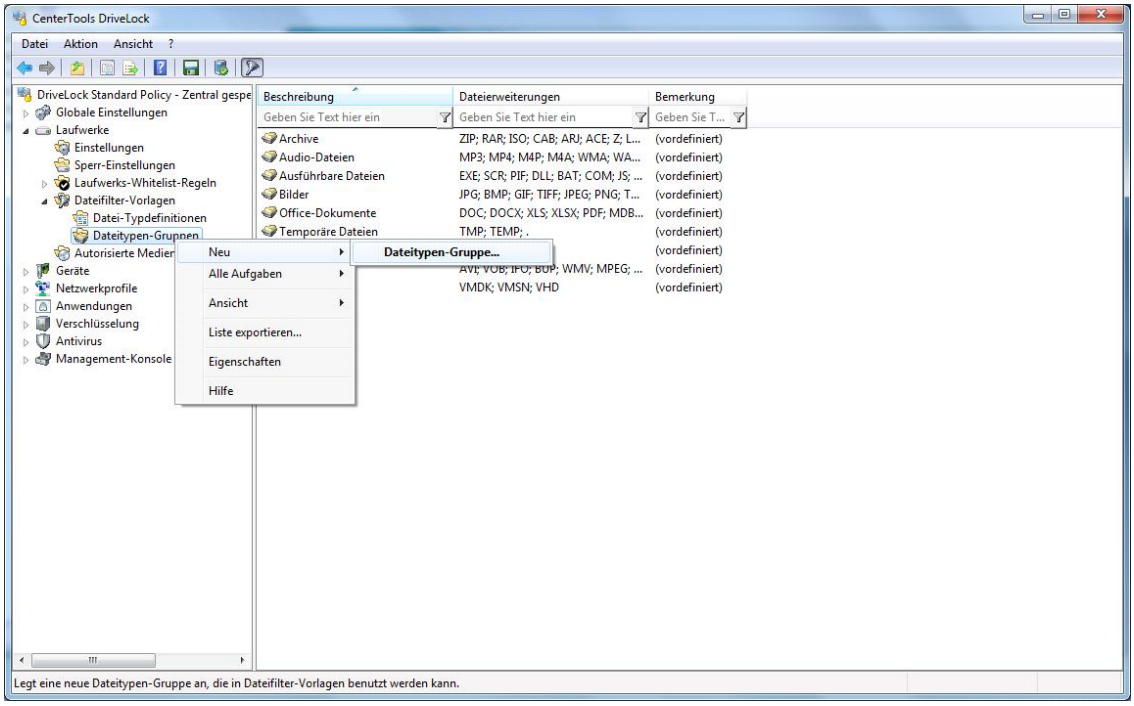
Klicken Sie auf **OK**, um die Anpassungen zu übernehmen.

4.1.2.4.2 Dateitypen-Gruppen erstellen

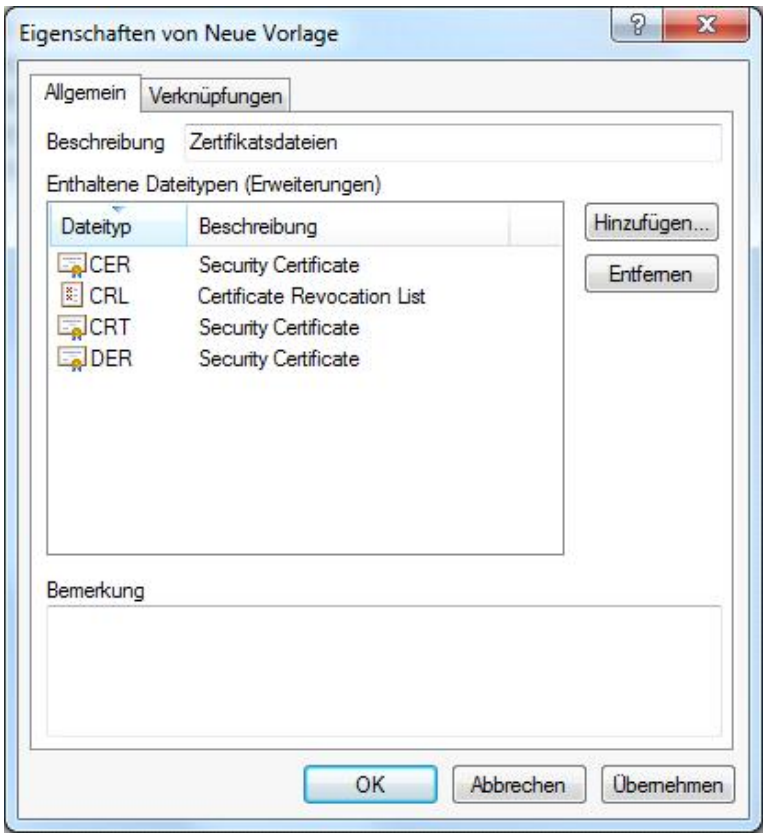
Um zwei oder mehrere Dateityp-Definitionen in einem einzigen Schritt innerhalb einer Dateifilter-Vorlage zu verwenden, können Sie Dateityp-Definitionen zu sogenannten Dateitypen-Gruppen zusammenfassen. Sie können eigene Gruppen erstellen, zusätzlich zu den bereits mit DriveLock mitgelieferten gebräuchlichsten Dateitypen-Gruppen, wie z.B. die Gruppe aller Audio- und Videodateien.



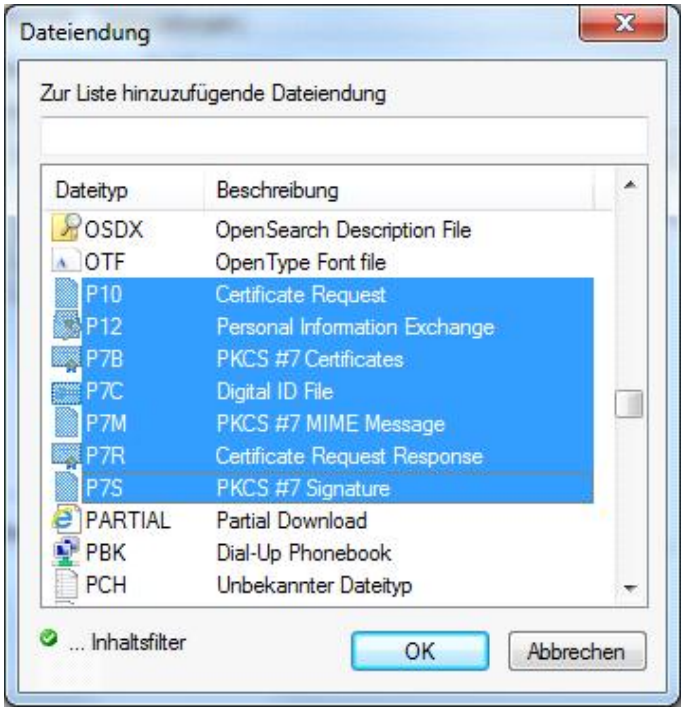
Bevor die eingebauten Gruppen verwendet werden können, müssen diese sofern noch nicht vorhanden erst durch einen Rechtsklick auf **Dateitypen-Gruppen** und Auswahl von **Alle Aufgaben -> Vordefinierte Dateitypen-Gruppen anlegen** erzeugt werden. Um eine bestehende Dateitypen-Gruppe zu ändern, doppelklicken Sie die gewünschte Gruppe.



Um eine neue Dateitypen-Gruppe zu erstellen, rechtsklicken Sie auf **Dateitypen-Gruppen** und wählen **Neu -> Dateitypen-Gruppe**.



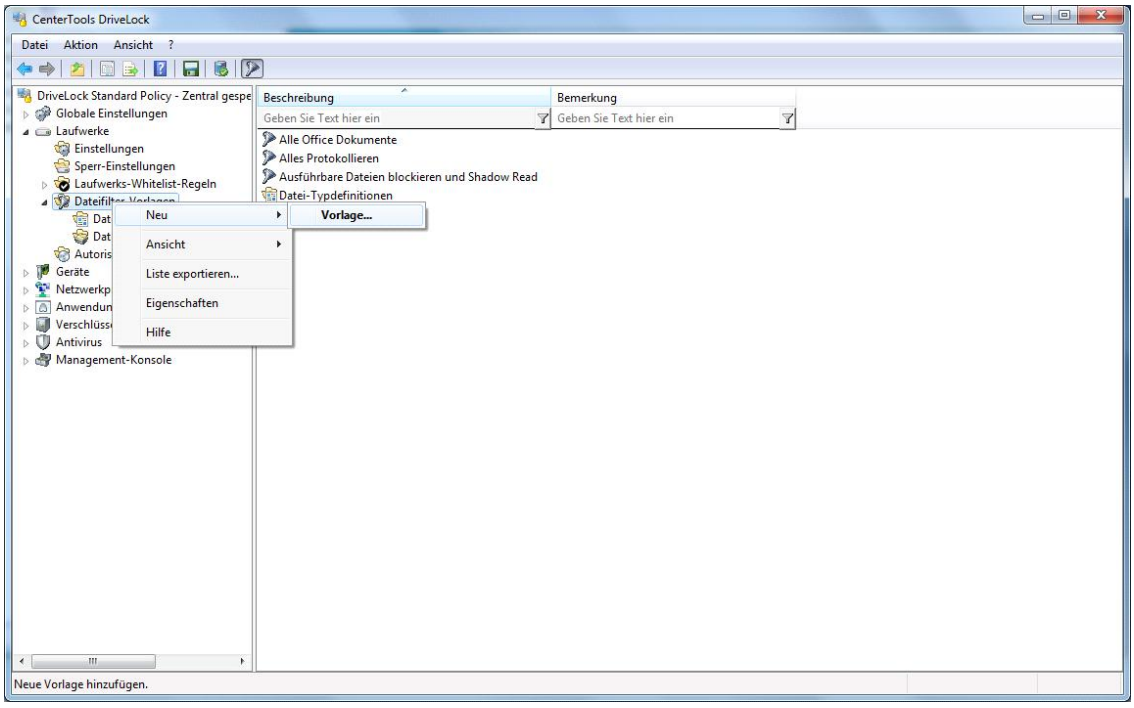
Geben Sie einen Namen in das Feld Beschreibung ein. Um Dateitypen hinzuzufügen, klicken Sie auf **Hinzufügen**. Wählen Sie einen Dateitypen aus Ihrer Liste aus und klicken Sie **Entfernen**, um einen Eintrag aus der Liste zu löschen.



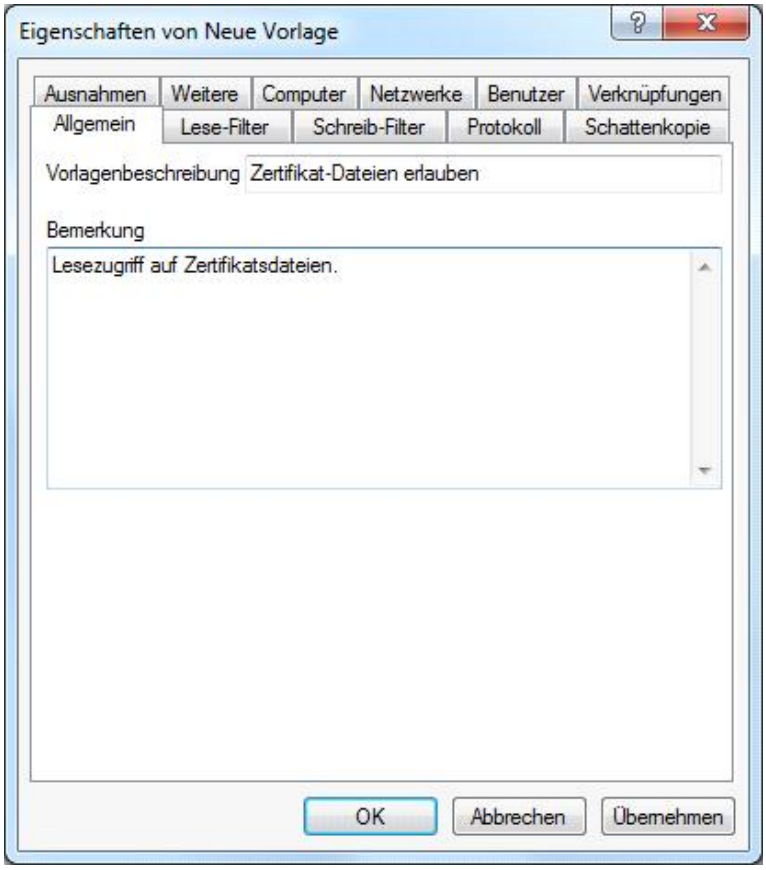
Sie können auch mehrere Dateitypen gleichzeitig hinzufügen, in dem Sie die STRG-Taste gedrückt halten und die gewünschten Dateitypen anklicken. Klicken Sie dann auf **OK**, um die ausgewählten Typen der Gruppe hinzuzufügen.

Klicken Sie nun auf **OK**, um die Änderungen abzuspeichern.

4.1.2.4.3 Neue Dateifilter-Vorlage erstellen

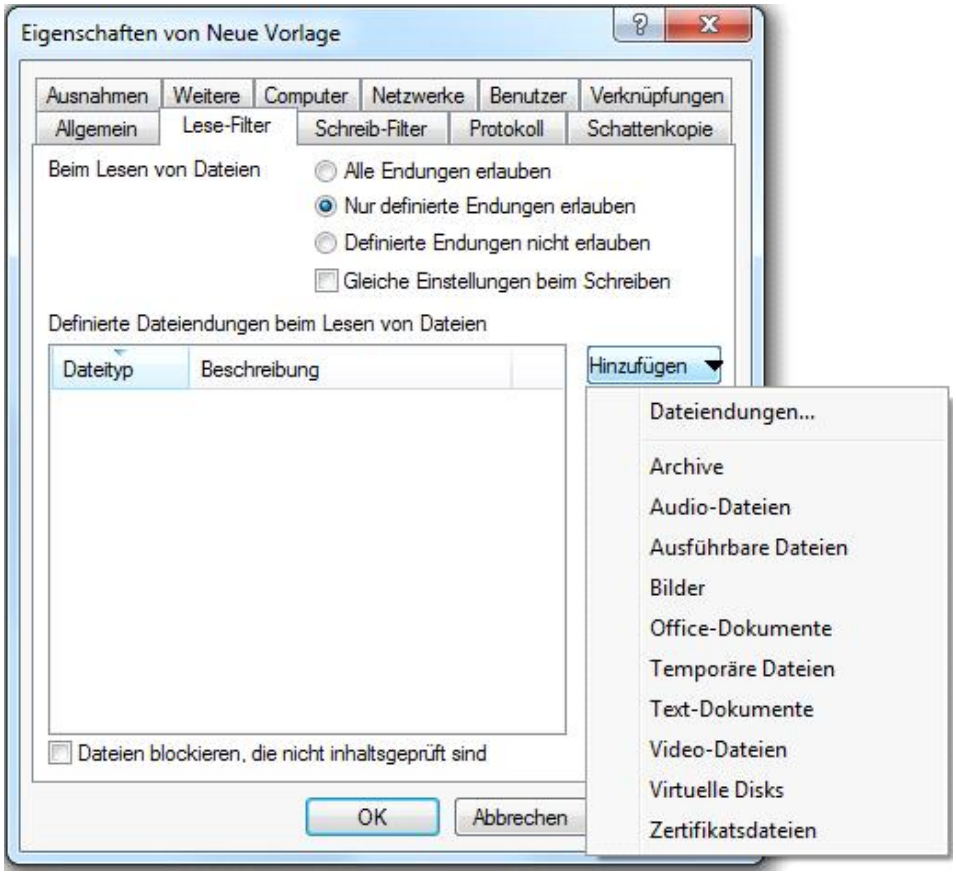


Rechtsklicken Sie bitte auf **Dateifilter-Vorlagen** und wählen anschließen **Neu -> Vorlage**



Geben Sie einen Namen in das Feld "**Vorlagenbeschreibung**" und optional eine Bemerkung als Beschreibung ein.

Als nächstes aktivieren Sie den Reiter **Lese-Filter**.



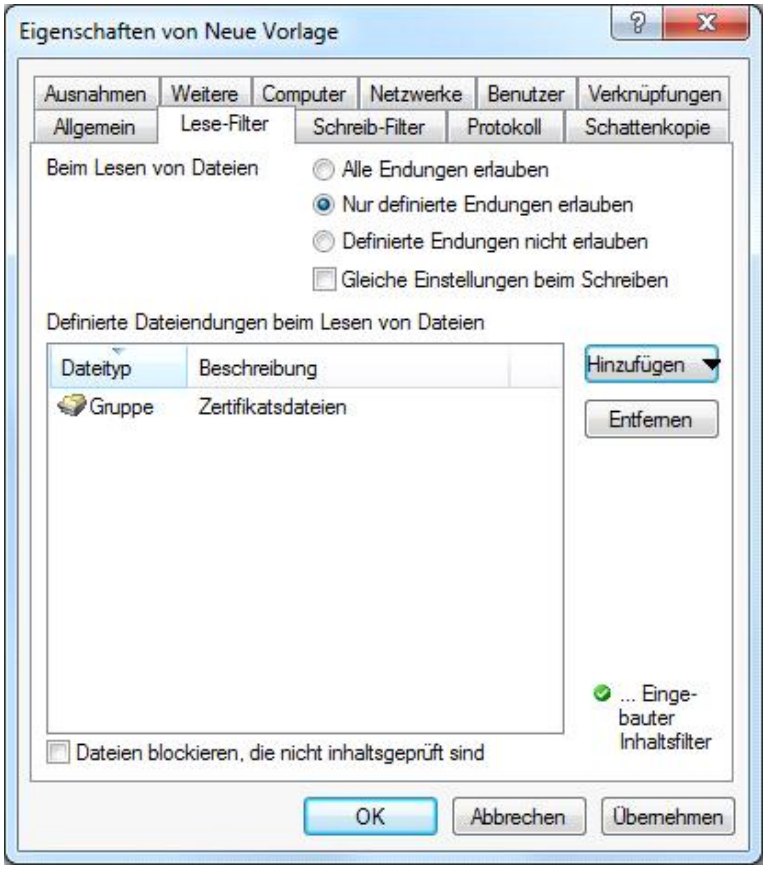
Alle hier angegebenen Datei-Endungen werden überprüft, jedes Mal wenn eine Datei von einem bestimmten Laufwerk (z.B. einer Wechselfestplatte) gelesen bzw. kopiert wird.

Sie können eine Endung entweder zulassen oder verbieten. Aktivieren Sie „**Alle Endungen erlauben**“, wenn Sie keinen Lesefilter einrichten wollen. Wenn nur bestimmte Dateien erlaubt werden sollen, aktivieren sie „**Nur definierte Endungen erlauben**“. Wenn bestimmte Dateien verboten werden sollen, markieren Sie „**Definierte Endungen nicht erlauben**“.

> Sofern bei einem bestimmten Dateityp die Inhaltsprüfung nicht explizit deaktiviert wurde, prüft DriveLock auch, ob der Inhalt und die Dateiendung zusammenpassen. Ist dies nicht der Fall, wird der Zugriff auf diese Datei gesperrt.

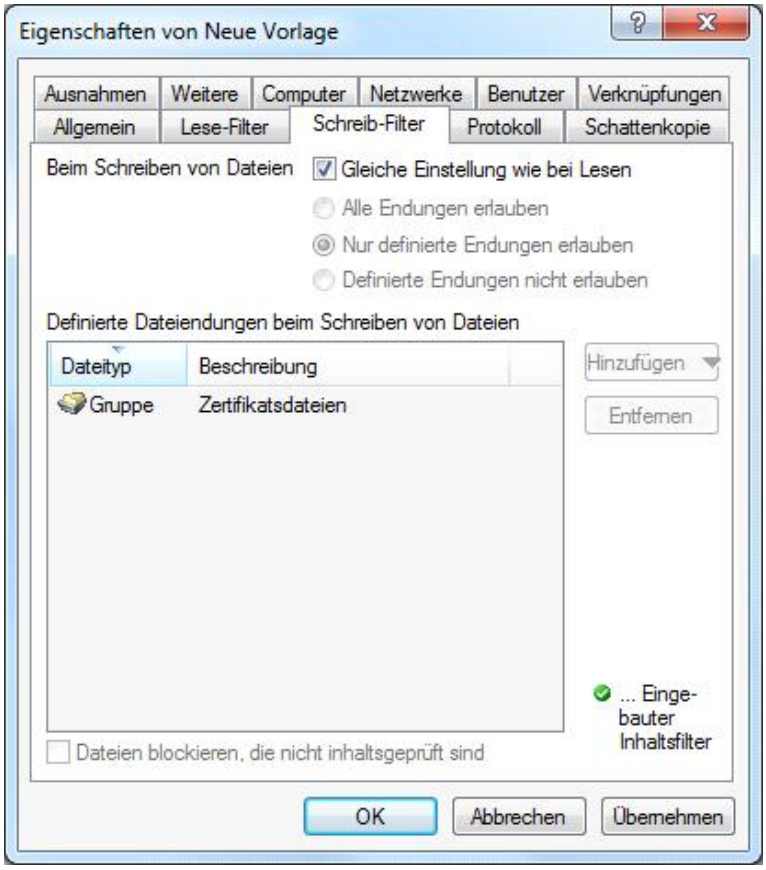
Klicken Sie auf **Hinzufügen**, um weitere Datei-Endungen zur Liste hinzuzufügen. Dabei können Sie auch aus den vorhandenen Dateitypen-Gruppen auswählen.

Wählen Sie die gewünschten Endungen (oder geben die benötigte Endung ein) und klicken **OK**, um die Auswahl zur Liste hinzuzufügen.



Geben Sie als Dateiendung hier nur einen Punkt "." ein, können Sie Dateien ohne eine Endung zulassen (bzw. blockieren). Dies ist zum Beispiel bei der Nutzung von Excel bis 2003 wichtig, da Excel immer zuerst temporär in 8-stelligen Dateien ohne Endung sichert, bevor die eigentliche xls-Datei geschrieben wird.

Als nächstes aktivieren Sie den Reiter **Schreib-Filter**.



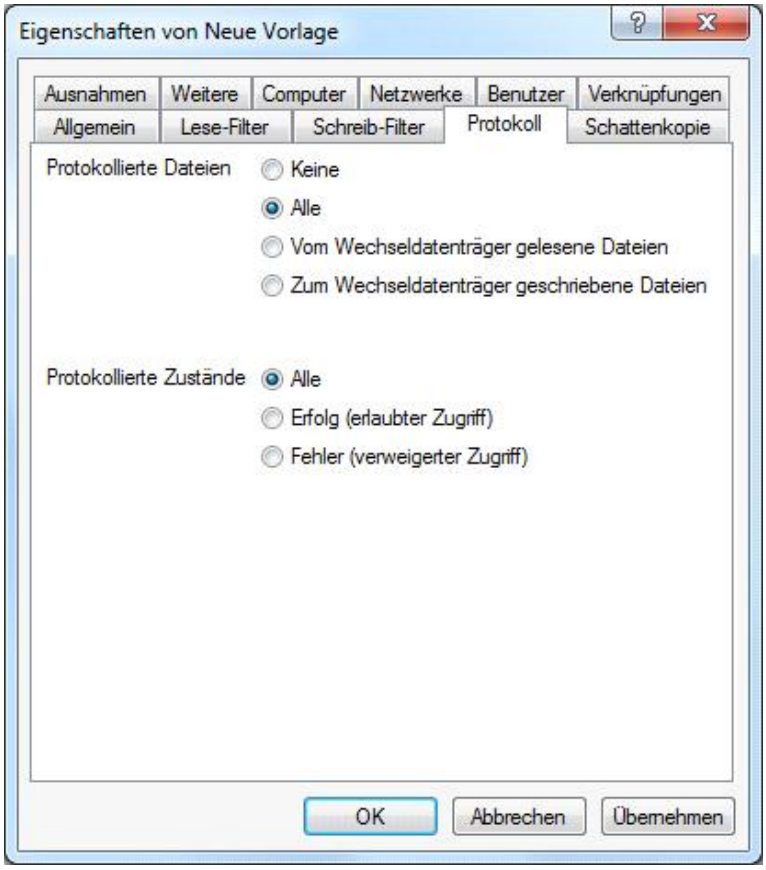
Alle hier konfigurierten Datei-Endungen werden jedes Mal überprüft, wenn eine Datei auf ein bestimmtes Laufwerk (z.B. eine Wechselfestplatte) kopiert wird (bzw. wenn ein Schreibzugriff erfolgt).

Sie können eine Endung entweder zulassen oder verbieten. Aktivieren Sie „**Alle Endungen erlauben**“, wenn Sie keinen Schreibfilter einrichten wollen. Wenn nur bestimmte Dateien erlaubt werden sollen, aktivieren sie „**Nur definierte Endungen erlauben**“. Wenn bestimmte Dateien verboten werden sollen, markieren Sie „**Definierte Endungen nicht erlauben**“.

Klicken Sie wiederum auf **Hinzufügen**, um weitere Datei-Endungen zur Liste hinzuzufügen.

Wenn Sie die Einstellungen des Lesefilters übernehmen wollen, aktivieren Sie „**Gleiche Einstellungen wie beim Lesen**“.

Im nächsten Schritt aktivieren Sie den Reiter **Protokoll**.



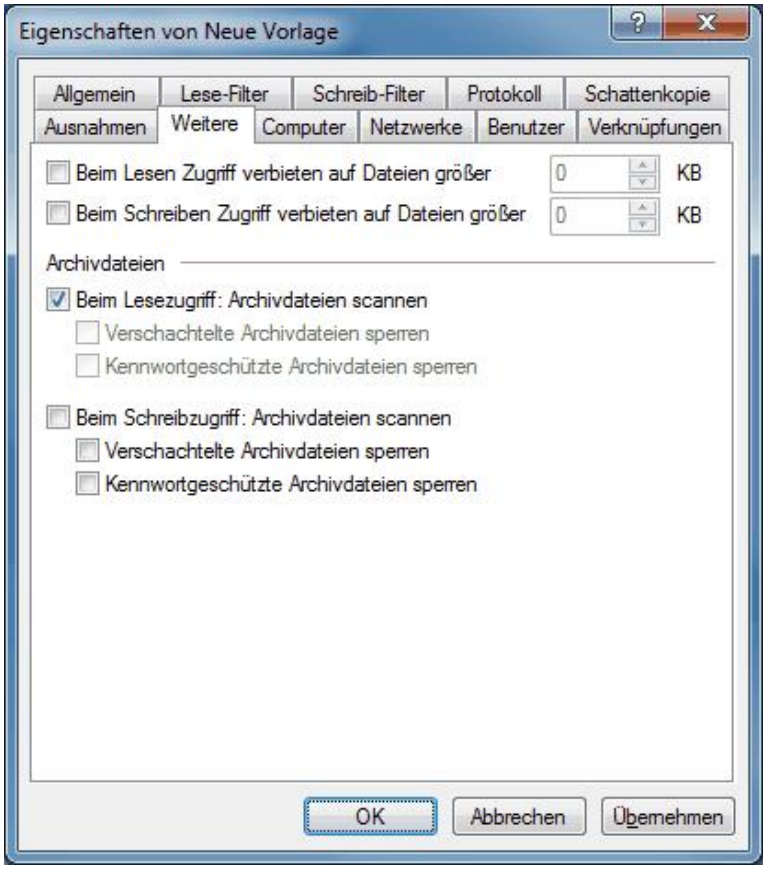
Diese Überwachungseinstellungen legen fest, welche Überwachungsereignisse generiert werden. Passen Sie diese gemäß Ihrer Unternehmensrichtlinie bzw. Ihrer Anforderungen an.

Überwachungsereignisse werden entweder zur Windows Ereignisanzeige übermittelt, oder – falls vorhanden und konfiguriert – zum DriveLock Enterprise Service.

> Bitte beachten Sie, dass die Überwachung von Dateioperationen die Performance Ihrer Systeme beeinträchtigen kann. Weiterhin erzeugt eine Benutzeraktivität unter Umständen mehr als einen Event (z.B. das Öffnen eines Word Dokumentes führt zu drei verschiedenen Einträgen, weil Word die Datei zunächst öffnet, dann Informationen schreibt – Letzter Zugriff – und anschließend erneut öffnet.

Die beiden Reiter **Schattenkopie** und **Ausnahmen** werden im Abschnitt „Schattenkopien in Laufwerksregeln konfigurieren“ beschrieben.

Wählen Sie den Reiter „**Weitere**“.



Wählen Sie eine der beiden Optionen "*... verbieten auf Dateien größer*" aus, um den Lese- bzw. Schreib-Zugriff auf zu große Dateien zu verhindern.

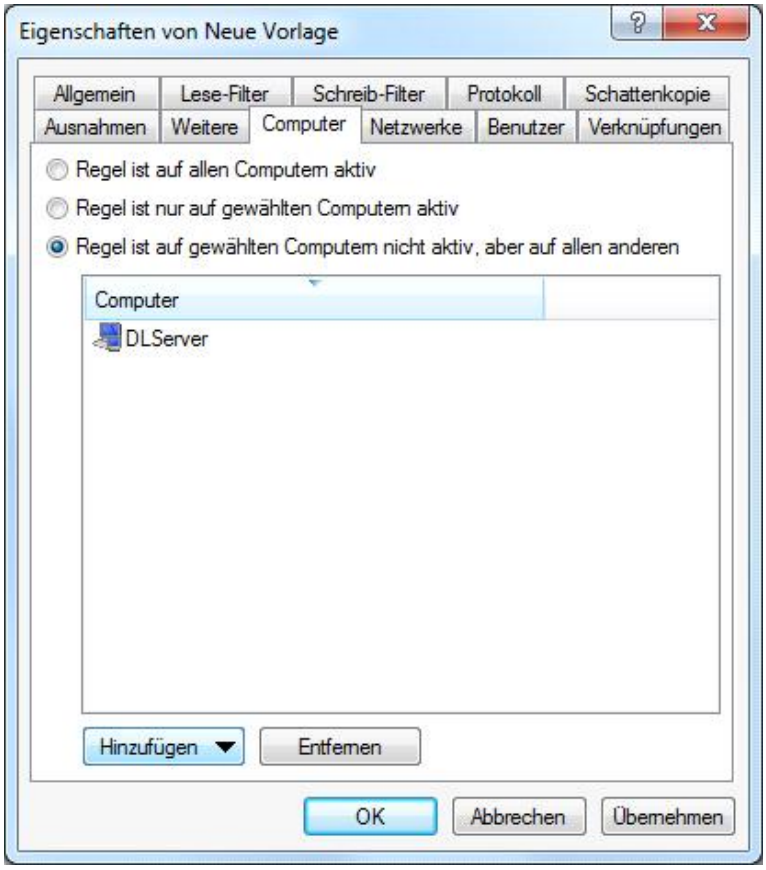
Damit DriveLock diesen Dateifilter auch innerhalb von Archiv-Dateien (ZIP und RAR) anwendet, stehen zwei weitere Optionen (jeweils für Lese- und Schreibzugriffe getrennt) zur Verfügung. Wenn DriveLock innerhalb dieser Archive nach den in dieser Vorlage definierten Dateien suchen soll, aktivieren Sie eine oder beide der Optionen "*... Archivdateien scannen*".

Um dabei Archive grundsätzlich zu sperren, die wiederum selbst Archivdateien enthalten, aktivieren Sie die Option "*Verschachtelte Archivdateien sperren*".

Um Archive grundsätzlich zu sperren, die mit einem Kennwort versehen sind und somit nicht untersucht werden können, aktivieren Sie die Option "*Kennwortgeschützte Archivdateien* sperren".

Bitte beachten Sie, dass aus technischen Gründen eine Überprüfung von Archiven bei Netzwerk- und WebDAV-Laufwerken derzeit noch nicht möglich ist.

Wählen Sie den Reiter „**Computer**“.

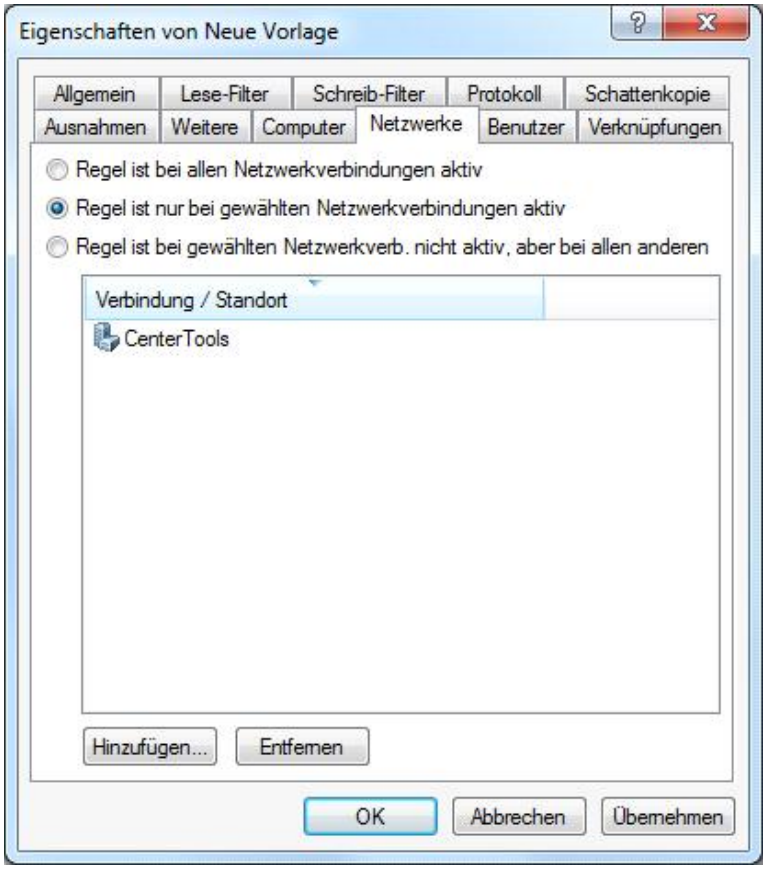


Wählen Sie eine der folgenden Möglichkeiten:

- Der Dateifilter gilt für alle Computer
- Der Dateifilter gilt nur für die aufgelisteten Computer
- Der Dateifilter gilt für alle außer den aufgelisteten Computern

Klicken Sie auf **Hinzufügen**, um weitere Rechner der Liste hinzuzufügen. Durch **Entfernen** werden zuvor ausgewählte Computer aus der Liste gelöscht.

Wählen Sie den Reiter „**Netzwerke**“.

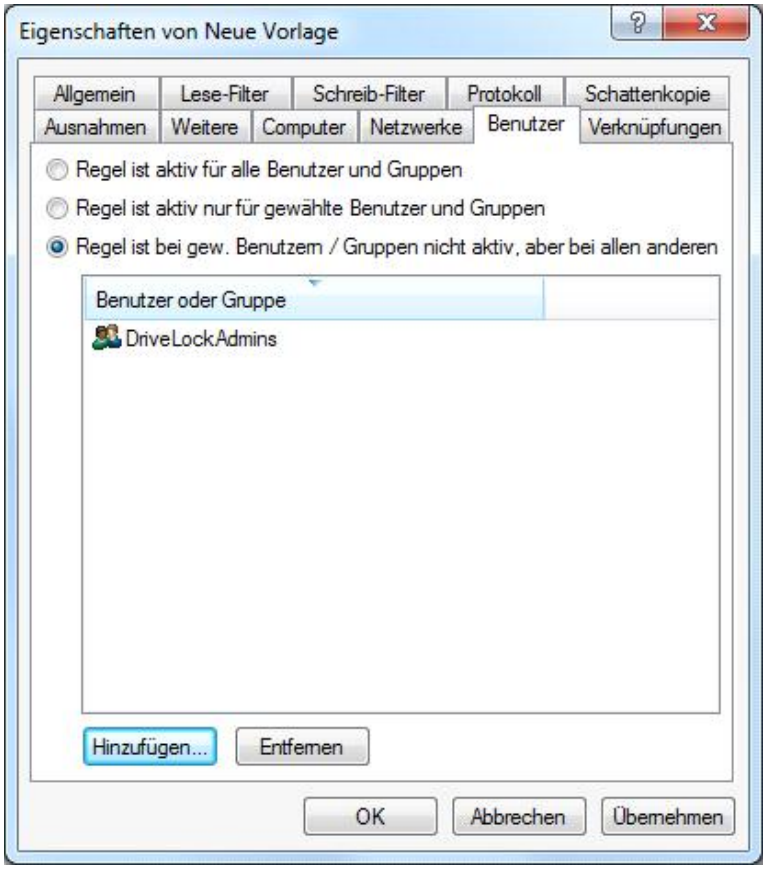


Wählen Sie eine der folgenden Möglichkeiten:

- Der Dateifilter gilt für alle Netzwerkverbindungen
- Der Dateifilter gilt nur für die aufgelisteten Netzwerkverbindungen
- Der Dateifilter gilt für alle außer den aufgelisteten Netzwerkverbindungen

Klicken Sie auf **Hinzufügen**, um weitere Netzwerkverbindungen der Liste hinzuzufügen. Durch **Entfernen** werden zuvor ausgewählte Netzwerkverbindungen aus der Liste gelöscht.

Wählen Sie den Reiter „**Benutzer**“.



Wählen Sie eine der folgenden Möglichkeiten:

- Der Dateifilter gilt für alle Benutzer
- Der Dateifilter gilt nur für die aufgelisteten Benutzer bzw. Gruppen
- Der Dateifilter für alle außer den aufgelisteten Benutzer bzw. Gruppen

Klicken Sie auf **Hinzufügen**, um weitere Benutzer bzw. Gruppen der Liste hinzuzufügen. Durch **Entfernen** werden zuvor ausgewählte Benutzer bzw. Gruppen aus der Liste gelöscht.

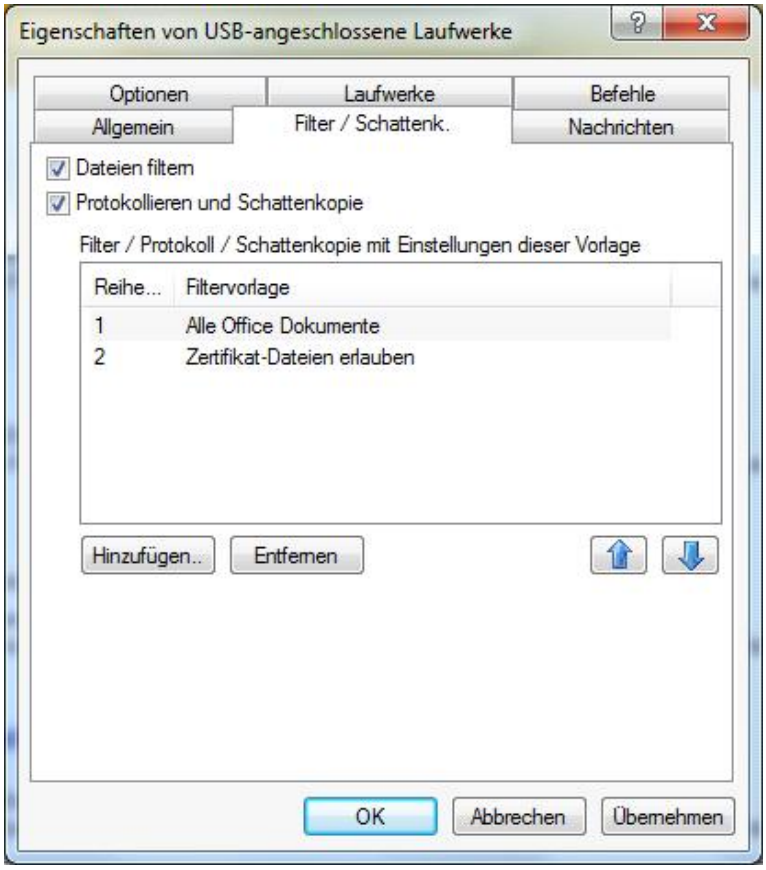
Um sich anzeigen zu lassen, in welchen Regeln dieses Template verwendet wird, wählen Sie den Reiter **Verknüpfungen**.

Klicken Sie **OK**, um die Dateifilter-Vorlage zu speichern.

4.1.2.4.4 Dateifilter-Vorlage verwenden

Eine Dateifilter-Vorlage kann nun entweder für die Konfiguration innerhalb eines Laufwerkstyps verwendet oder in einer einzelnen Laufwerksregel zugewiesen werden.

Öffnen Sie die Konfiguration für einen Laufwerkstypen (zum Beispiel USB-angeschlossene Laufwerke). Dann aktivieren Sie den Reiter **Filter/Schattenk.**



Markieren Sie "**Dateien filtern**" bzw. „**Protokollieren und Schattenkopie**", um die Dateifilterung und die ausgewählten Vorlagen einzuschalten.

Um einen Dateifilter für ein ganz bestimmtes Laufwerk zu verwenden, öffnen Sie die dazu gehörige Laufwerksregel und wählen ebenfalls den Reiter **Filter/Schattenk.**

Es ist vorkonfiguriert, dass der eingestellte Filter des dazugehörigen Laufwerkstyps verwendet wird. Wenn Sie einen eigenen Filter angeben möchten, deaktivieren Sie „**Einstellungen von „Sperr-Einstelllungen" verwenden**", markieren „**Dateien filtern**" bzw. „**Protokollieren und Schattenkopie"**.

Klicken Sie auf **Hinzufügen**, um eine bestehende Dateifilter-Vorlage zur Liste hinzuzufügen. Mit **Entfernen** können Sie einen Listeneintrag wieder löschen.

Verwenden Sie die beiden Symbole und , um die Reihenfolge der Dateifilter-Vorlagen zu ändern.

Wenn DriveLock eine Whitelist-Regel aktiviert, werden alle Dateifilter-Vorlagen in der Liste von Oben nach Unten ausgewertet. Die erste Vorlage, bei der die darin konfigurierten Kriterien (z.B. Dateigröße, Ausnahmen, Benutzer und Gruppen, Computer oder Netzwerkverbindungen) vollständig übereinstimmen, wird angewendet. Alle folgenden Vorlagen werden ignoriert.

Folgendes Beispiel soll die Vorgehensweise noch einmal verdeutlichen. Sie haben zwei Vorlagen erstellt: die erste Vorlage gilt nur für Administratoren und filtert keine Dateien, die zweite Vorlage gilt für alle Benutzer und blockiert den Zugriff auf ausführbare Dateien. Wenn nun ein Administrator auf die Anwendungsdatei zugreifen möchte, wird die erste Vorlage angewendet und der Zugriff erlaubt. Versucht nun ein normaler Benutzer das gleiche, wird die erste Vorlage ignoriert und die zweite angewendet, um den Zugriff zu sperren.

4.1.2.4.5 Dateifilter-Vorlage für verschlüsselte Laufwerke (Encryption 2-Go)

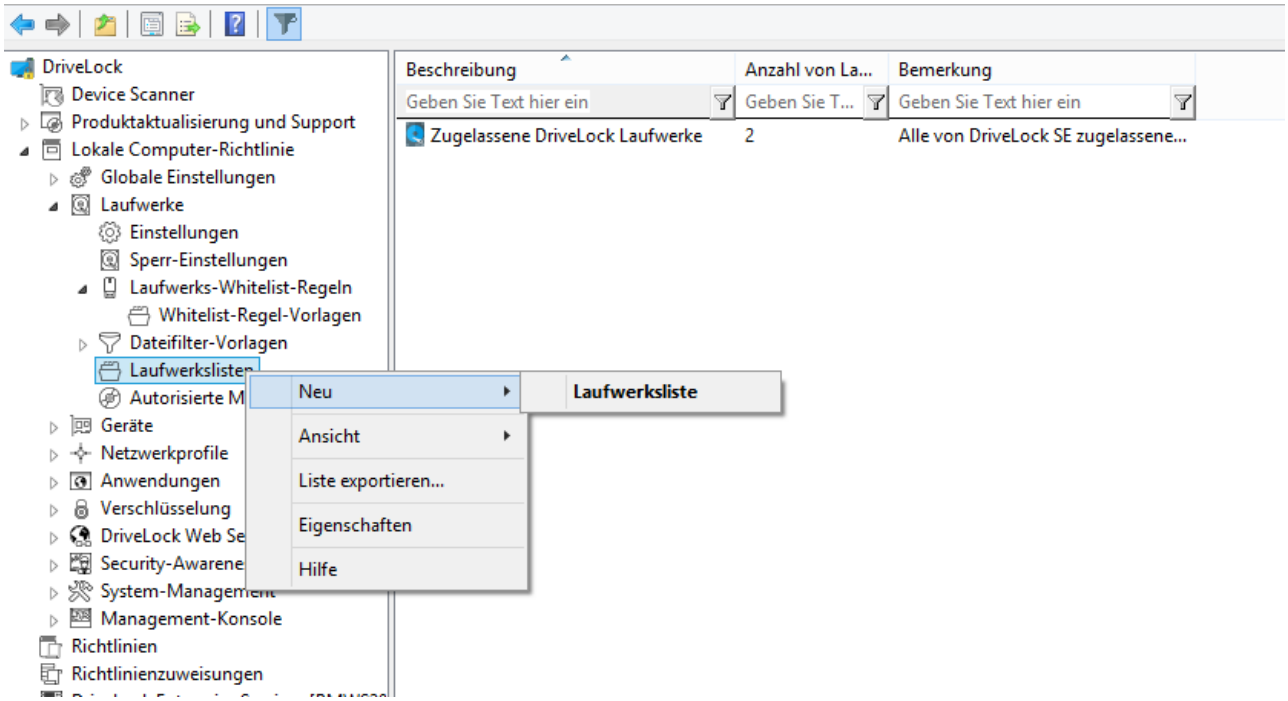
Um eine Dateifilter-Vorlage auch für verschlüsselte Laufwerke zu übernehmen, muss man einen zusätzlichen Schritt ausführen. In diesem Fall reicht es nämlich nicht, wenn ein Dateifilter auf USB-angeschlossene Laufwerke aktiv ist, da es sich hierbei um die unverschlüsselte Partition handelt, die im Idealfall ohnehin für den Benutzer gesperrt ist.

Der verschlüsselte Container (der durchaus auf dem USB-angeschlossenem Laufwerk gespeichert ist) wird als extra Laufwerk geladen und ist aus Sicht von DriveLock eine eigene Laufwerksklasse – *Verschlüsselte Container*.

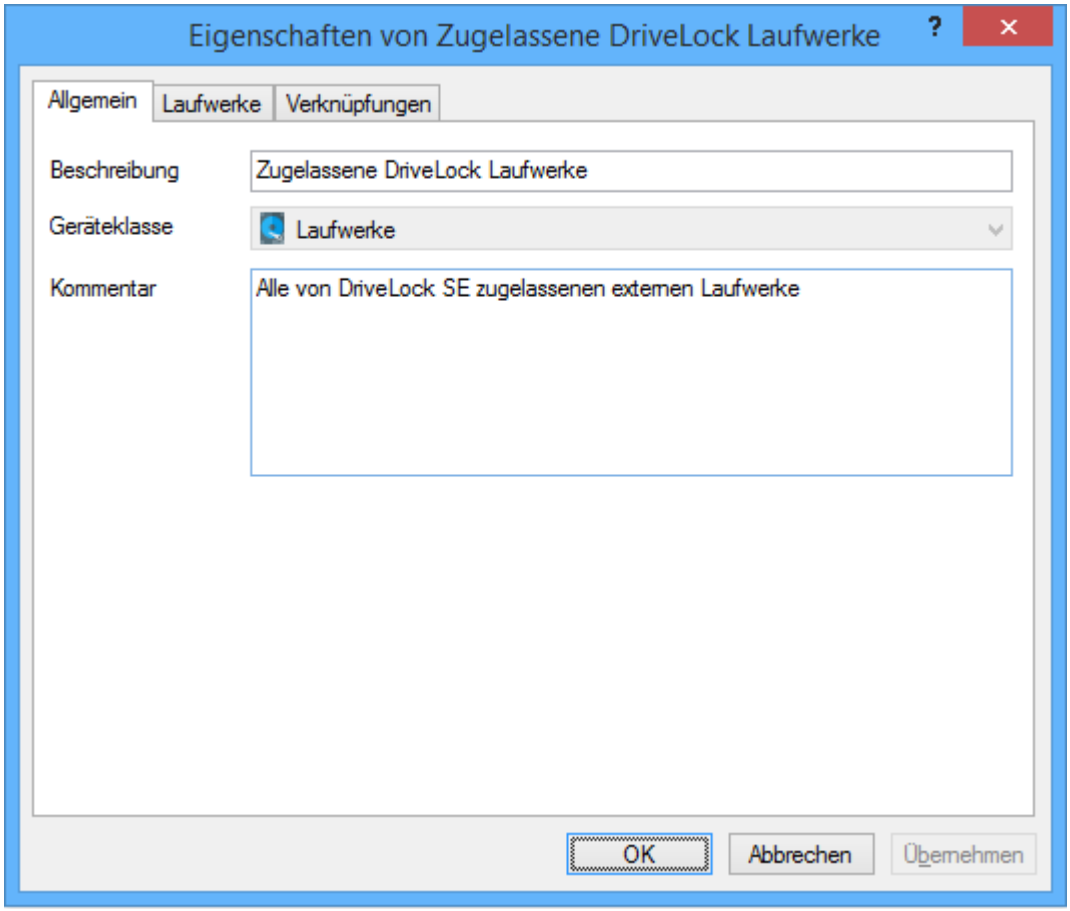
Damit ein Dateifilter also in einem verschlüsselten Container aktiv ist, muss man unter *Laufwerke – Sperr-Einstellungen – Verschlüsselte Container* eine Whitelist-Regel erstellen und dort beim Reiter *Filter / Schattenk.* den Haken bei *Dateien filtern und/oder Protokollieren und Schattenkopie* setzen und eine Vorlagen auswählen.

4.1.2.5 Laufwerkslisten erstellen

Laufwerkslisten stellen eine Möglichkeit dar, die Konfiguration von Einstellungen und Regeln zu vereinfachen und die Anzahl der benötigten Whitelist-Regeln zu verringern, indem alle Laufwerke, für die ein und dieselben Einstellungen gelten sollen, zuerst in einer Laufwerksliste zusammengefasst werden und anschließend dann eine Laufwerkslisten-Regel für diese Liste mit allen Einstellungen erstellt wird.

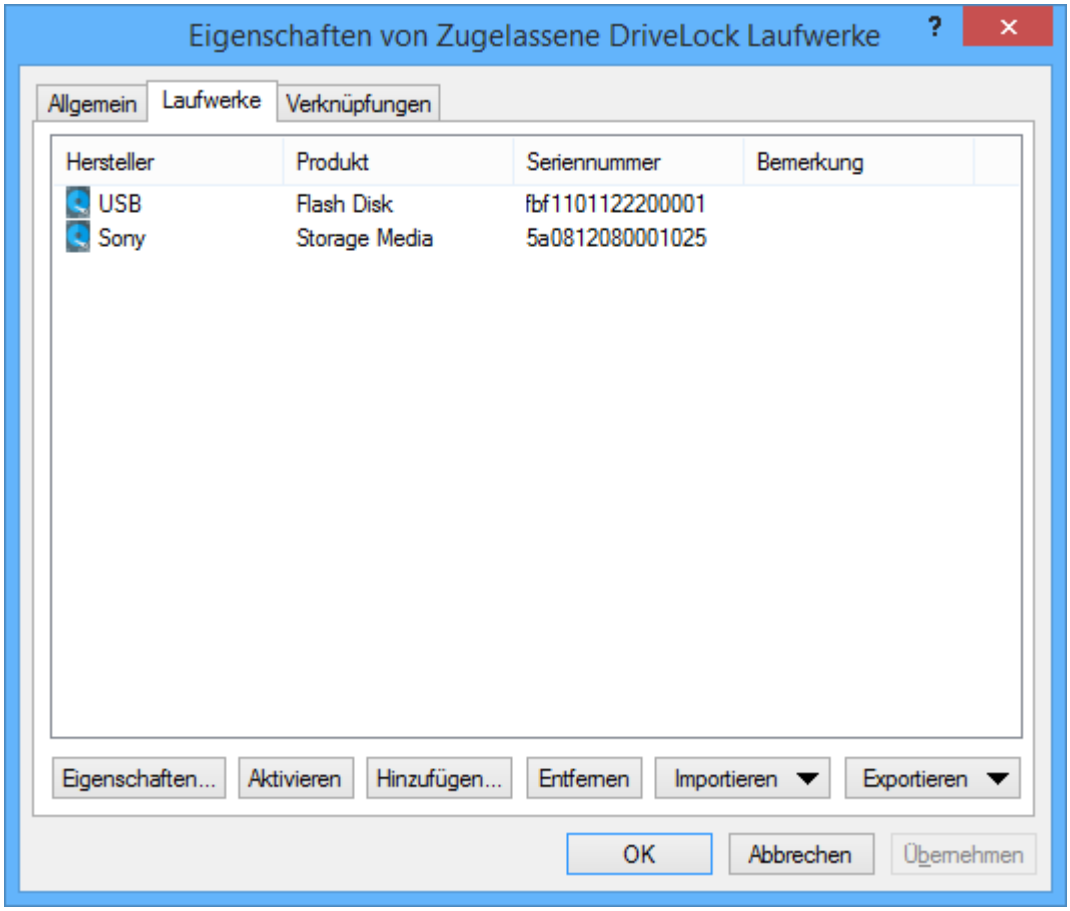


Um eine neue Laufwerksliste zu erstellen, rechtsklicken Sie auf **Laufwerkslisten-Regel** und wählen "**Neu -> Laufwerksliste**" aus dem Kontextmenü:



Geben Sie nun eine Beschreibung und optional einen erklärenden Kommentar ein. Die "Geräteklasse" ist automatisch auf "Laufwerke" eingestellt und kann hier nicht verändert werden.

Wählen Sie nun den Reiter **Laufwerke**.



Hier können Sie bestehende Einträge anzeigen, deaktivieren, bearbeiten und löschen. Ebenso lassen sich neue Einträge hinzufügen.

Wenn Sie neue Einträge hinzufügen möchten, klicken Sie auf **Hinzufügen** und wählen aus, ob sie ein Laufwerk aufgrund seiner Produkt- bzw. Hersteller-ID oder mithilfe der Hardware-ID hinzufügen möchten. Geben Sie im anschließenden Dialog die entsprechenden Informationen ein bzw. wählen Sie diese in gewohnter Weise über die Schaltfläche "..." aus den aktuell angeschlossenen Geräten oder der Device Scanner Datenbank aus.

> Möchten Sie vorhandene Laufwerke nicht komplett löschen, sondern nur für eine bestimmte Zeit aus der Liste entfernen, wählen Sie das gewünschte Laufwerk aus und klicken anschließend auf **Deaktivieren**. Ein kleines zusätzliches Symbol zeigt nun an, das der Eintrag in der Liste derzeit nicht aktiviert ist und für Freigaben berücksichtigt wird. Deaktivierte Listenelement können ebenso wieder aktiviert werden.

Über die Schaltfläche **Import** können Sie mehrere Laufwerke importieren, die entweder in Form einer CSV- oder einen INI-Datei vorliegen. Eine CSV-Datei könnte beispielsweise so aussehen:

HardwareID	Comment	Vendor	Product	SerialNumber
		USB	Flash Disk	fbf1101122200001
		Sony	Storage Media	5a0812080001025
USBSTOR\GenSFloppy	USB FloppyDisk Drive			

Klicken Sie auf **Export**, um die aktuelle Liste in Form einer CSV- oder INI-Datei speichern.

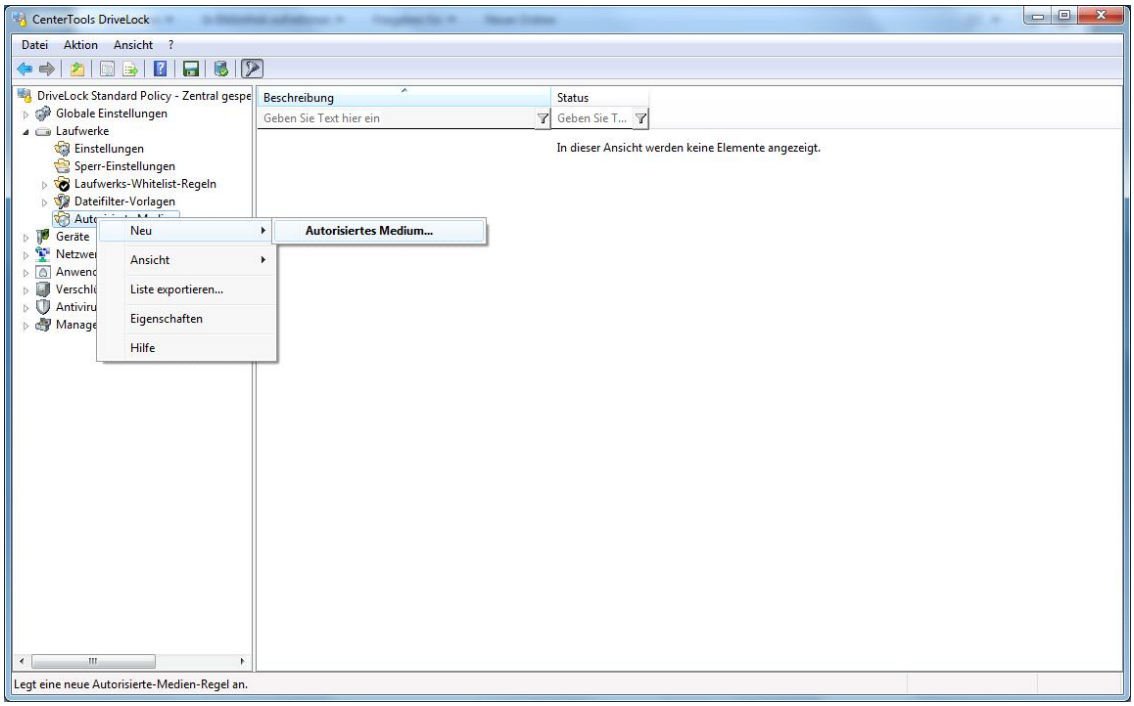
Tipp: Wenn Sie zuvor einige Einträge einzeln erstellt und diese dann als Datei exportiert haben, können Sie diese Datei als Grundlage für einen Import verwenden, da diese bereits den richtigen Aufbau bzw. die notwendigen Spalten besitzt.

Der Reiter **Verknüpfungen** zeigt Ihnen, in welchen Laufwerklisten-Regeln diese Liste bereits verwendet wird.

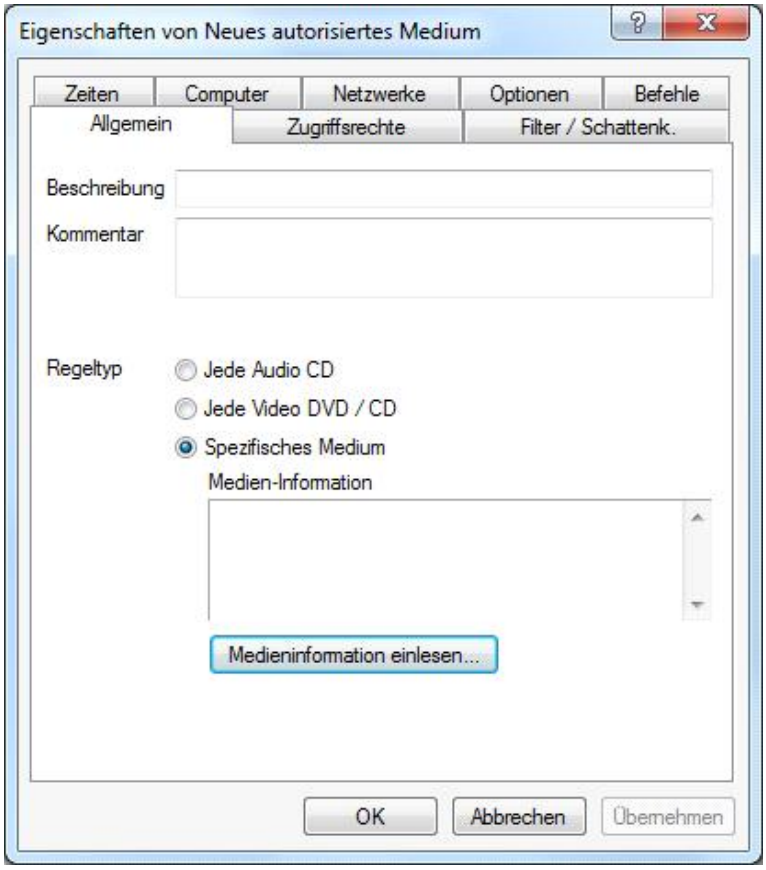
4.1.2.6 Medien-Autorisierung verwenden

Die Medien-Autorisierung ermöglicht es Ihnen, bestimmte vordefinierten Medien (wie zum Beispiel Update-CDs oder spezielle Programm-CDs) freizugeben, auch wenn prinzipiell das CD/DVD-Laufwerk gesperrt ist. Somit sind Sie in der Lage, die Sperrung von CD-Laufwerken selektiver zu konfigurieren.

Wenn Sie eine neue Medien-Regel erstellen, erzeugt DriveLock einen sogenannten Hash-Wert (quasi ein Fingerabdruck) der CD. Dieser wird für die Freigabe verwendet. Daher ist es nicht ratsam, eine derartige Regel bei beschreibbaren Wechseldatenträgern anzuwenden, da in diesem Fall der Wert bei der Überprüfung nicht mehr mit dem gespeicherten Wert übereinstimmen würde, wenn zwischenzeitlich Dateien verändert worden sind. Daher empfehlen wir Ihnen, eine Medien-Regel nur bei Medien zu verwenden, die nicht verändert werden können (wie zum Beispiel CDs oder DVDs).

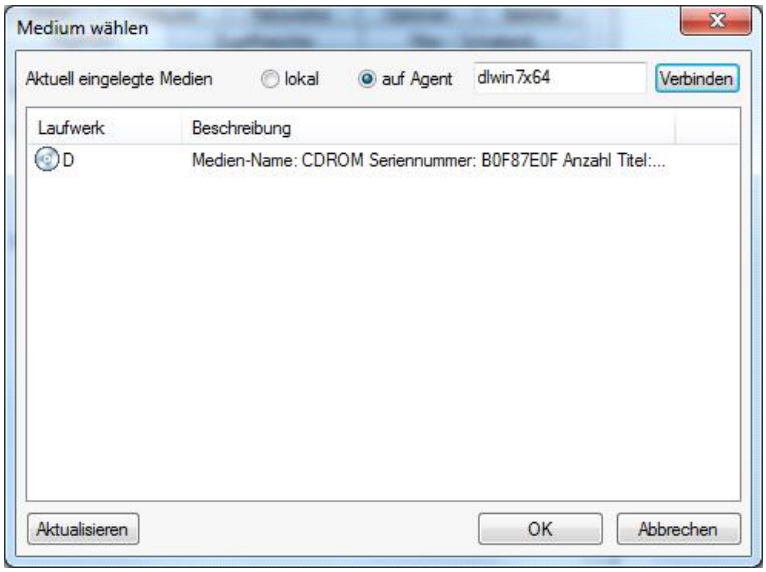


Um eine neue Regel zu erstellen, klicken Sie **Autorisierte Medien** und wählen **Neu -> Autorisiertes Medium.**

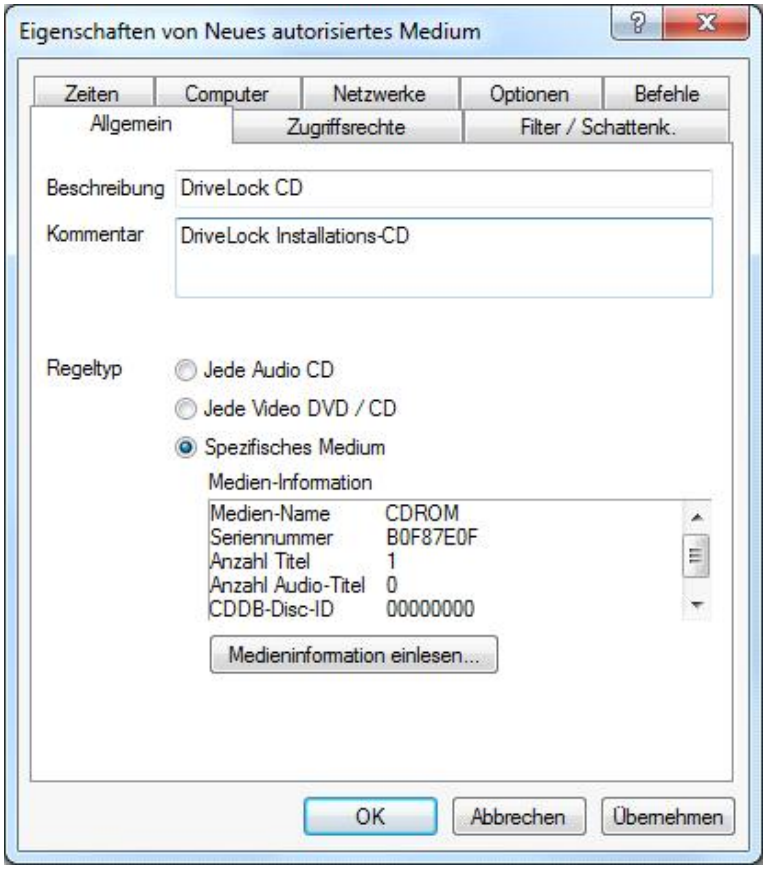


Geben Sie einem Namen in das Beschreibungsfeld und – falls gewünscht – einen Kommentar zur detaillierteren Beschreibung ein.

Es gibt zwei verschieden Typen von Medien: Audio-CDs und Video-CDs/DVDs. Selbstverständlich können Sie auch eigene Medien erstellen, indem Sie "**Spezifisches Medium**" auswählen und auf **Medieninformation einlesen** klicken.



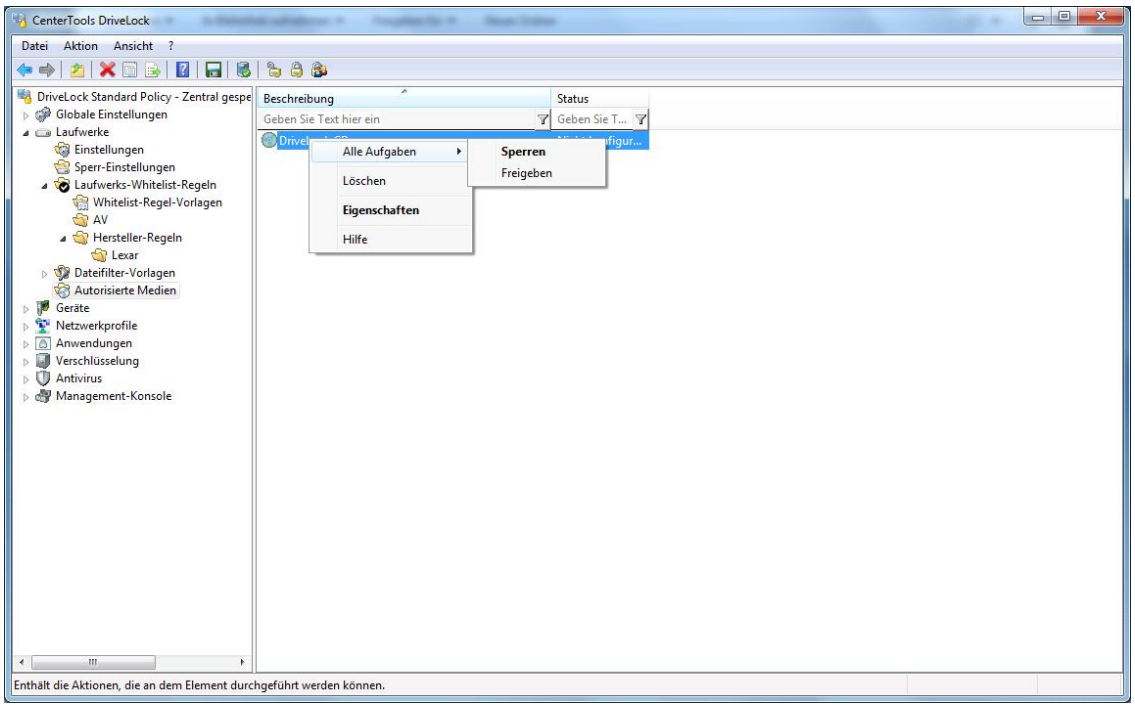
Überprüfen Sie das Laufwerk, in dem die CD/DVD eingelegt ist und klicken **OK**.



Die Informationen zum Medium werden nun ausgelesen und automatisch eingetragen.

Die weiteren Konfigurationsmöglichkeiten, die auf den verschiedenen Reitern konfiguriert werden können, entsprechen den Konfigurationsmöglichkeiten bei Laufwerken und werden im Abschnitt „Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren“ beschrieben.

Klicken Sie **OK** um die Regel zu speichern.



Klicken Sie mit der rechten Maustaste auf eine bestehende Regel und wählen Sie **Alle Aufgaben -> Freigeben (bzw. Sperren),** um schnell den Zugriff für alle Benutzer (bzw. keinen) zu konfigurieren.

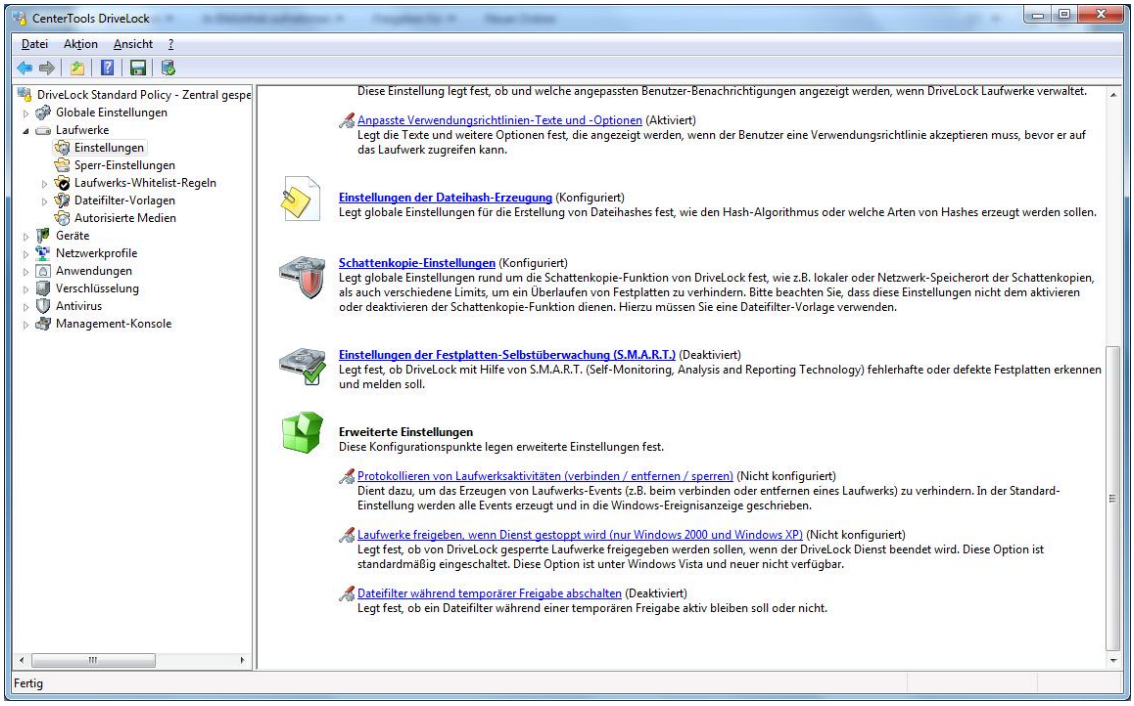
4.1.2.7 Datenübertragung mit Hilfe von Schattenkopien überwachen

Schattenkopien ermöglichen es, eine Kopie von Dateien (oder Teilen davon) zu erzeugen, die zu oder von einem Wechseldatenträger kopiert werden. Diese Schattenkopien können sowohl auf Clients als auch auf einem Server abgelegt werden. Es ist ferner möglich, zu definieren, von welchen Dateien Schattenkopien erzeugt werden sollen.

> Wenn das Erzeugen von Schattenkopien für CD/DVD-Brenner aktiviert wurde, erstellt DriveLock von jeder darüber gebrannten CD/DVD ein ISO-Image und speichert diese Datei an der von Ihnen konfigurierten Stelle.

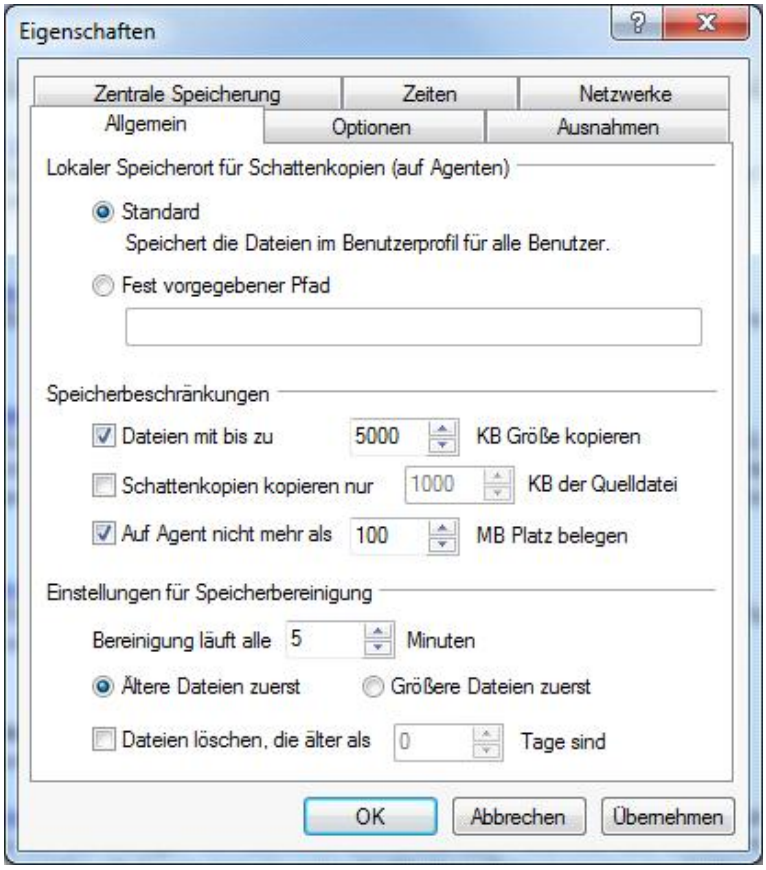
4.1.2.7.1 Allgemeine Schattenkopie-Einstellungen festlegen

Globale Einstellungen für Schattenkopien werden unter den Einstellungen für Laufwerke vorgenommen.



Klicken Sie auf **Schattenkopie-Einstellungen,** um die Einstellungen für Schattenkopien festzulegen.

4.1.2.7.1.1 Allgemeine Einstellungen



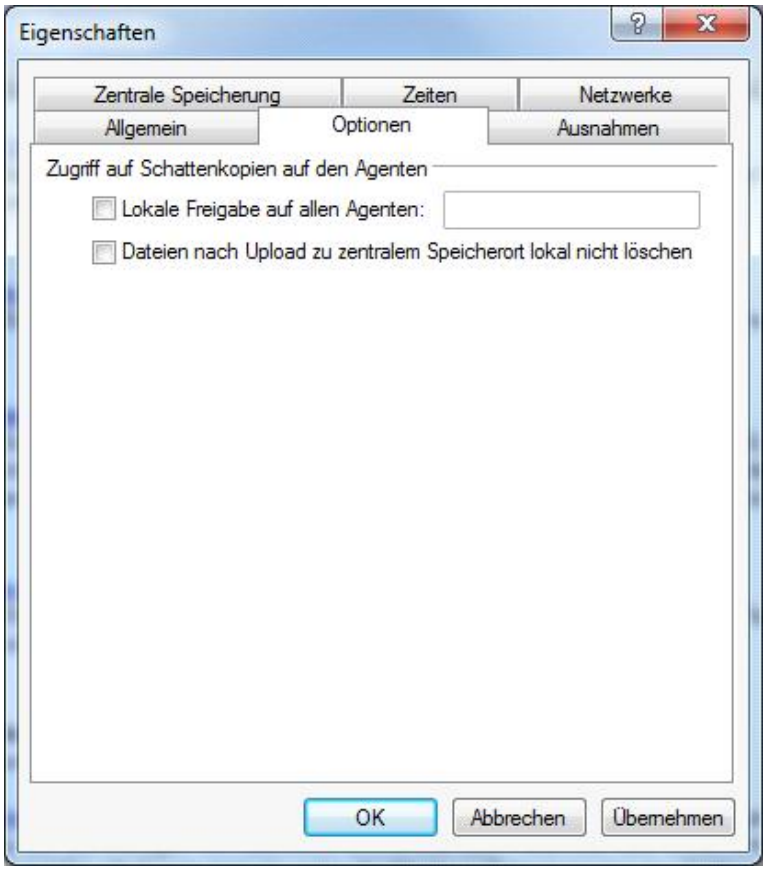
Die Schattenkopien werden standardmäßig im Ordner *C:\ProgramData\CenterTools DriveLock\ShadowFiles* abgelegt. Es ist aber auch möglich, einen anderen Ablageort anzugeben. Wählen Sie dazu „Fest vorgegebener Pfad“ und geben Sie den Ablageort an. Standardmäßig können auf diesen Pfad nur der Administrator und Domänen-Administratoren voll zugreifen.

Die Option “**Speicherbeschränkungen**” erlaubt es, eine maximale Dateigröße oder den maximal von Schattenkopien belegten Speicherplatz anzugeben. Standardmäßig werden nur Dateien mit einer Größe von bis zu 5 MB kopiert und es wird nicht mehr als 100 MB Speicherplatz auf der Festplatte belegt. Optional können Sie definieren, wie viele Daten (KB) jeder Quelldatei kopiert werden sollen. Ist diese Option aktiviert, ist es nicht länger möglich, die kopierten Dateien mit der ursprünglichen Applikation zu öffnen; mit Hilfe eines Hex-Editors können die Inhalte dann betrachtet werden.

Ferner kann konfiguriert werden, welche Dateien zuerst gelöscht werden, wenn die gewählte maximale Speicherkapazität für Schattenkopien erreicht wird und wie oft dieser Vorgang ausgeführt werden soll. Alternativ können die Dateien automatisch auch zu einem festgelegten Zeitpunkt gelöscht werden. Diese Einstellungen betreffen nur die Bereinigung auf Clients. Auf einem zentralen Ablageort (auf einem Server) finden keine Bereinigungen statt. Standardmäßig findet die Speicherbereinigung alle 5 Minuten statt.

4.1.2.7.1.2 Client-Einstellungen für Schattenkopien

Über den Reiter „**Optionen**“ kann der Zugriff auf angelegte Schattenkopien konfiguriert werden.

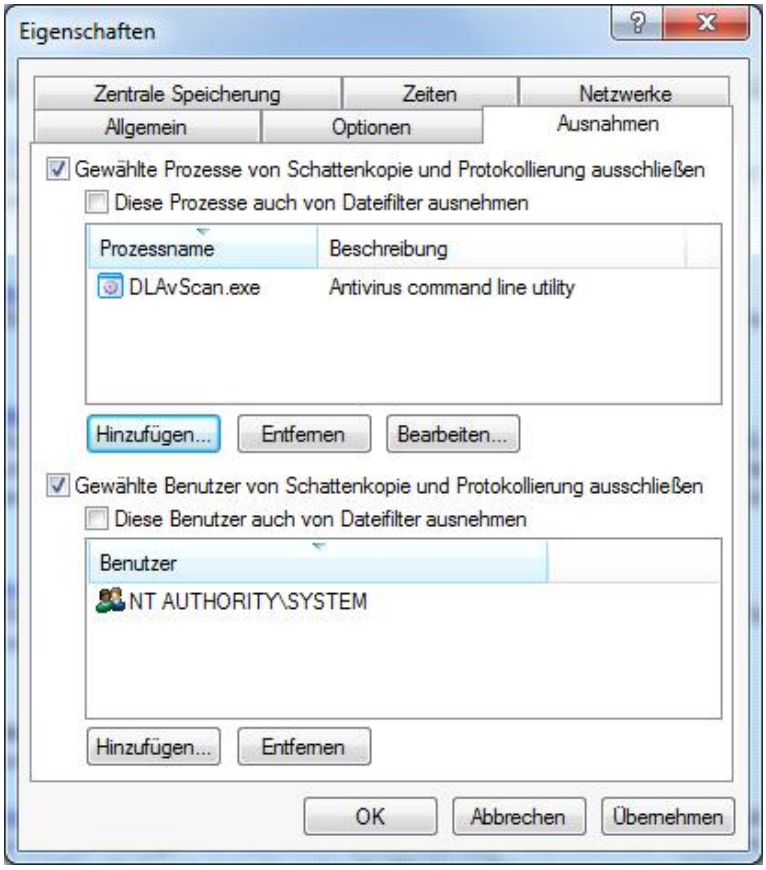


Wenn die Option “**Lokale Freigabe auf allen Agenten**” aktiviert ist, legt DriveLock automatisch eine Netzwerkfreigabe mit dem definierten Namen an. Über diese Netzwerkfreigabe ist dann der Zugriff auf die lokal abgelegten Schattenkopien möglich. Auf diese Freigabe erhalten Lokale Administratoren sowie Domänen-Administratoren Vollzugriff.

Werden Schattenkopien auf einen zentralen Netzwerkserver hochgeladen, so werden sie standardmäßig nach dem Hochladen von den Clients gelöscht. Über die Option „**Dateien nach Upload zu zentralem Speicherort lokal nicht löschen**“ kann dies verhindert werden. Die Schattenkopien unterliegen in diesem Fall aber dennoch den Einstellungen zur Speicherbereinigung.

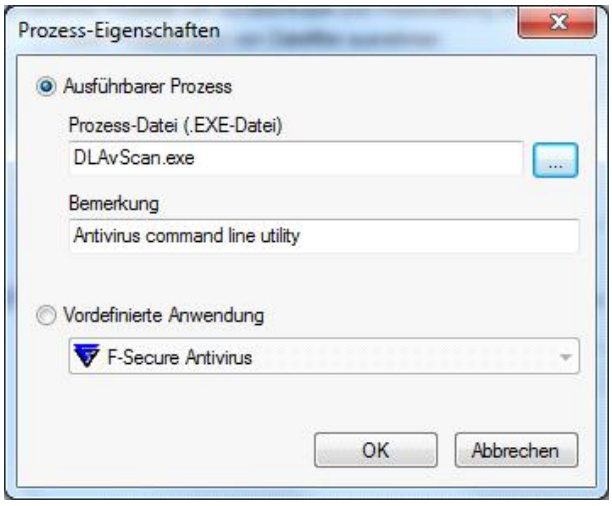
4.1.2.7.1.3 Ausnahmen bei Schattenkopien

Über den Reiter „**Ausnahmen**“ wird gesteuert, welche Prozesse oder Benutzer die Erzeugung von Schattenkopien nicht auslösen.



Es ist möglich, bestimmte Prozesse, Benutzer oder Gruppen von der Erzeugung von Schattenkopien auszunehmen. Wird eine Datei von einem so definierten Prozess, Benutzer oder Gruppe gelesen oder geschrieben, wird in diesem Fall keine Schattenkopie erstellt. Diese Option ist primär dazu gedacht, bestimmte, häufig zugreifende Prozesse – wie Virenscanner – von der Erstellung von Schattenkopien auszunehmen.

Klicken Sie auf **Hinzufügen** oder **Entfernen**, um Prozesse oder Benutzer/Gruppen zu definieren.

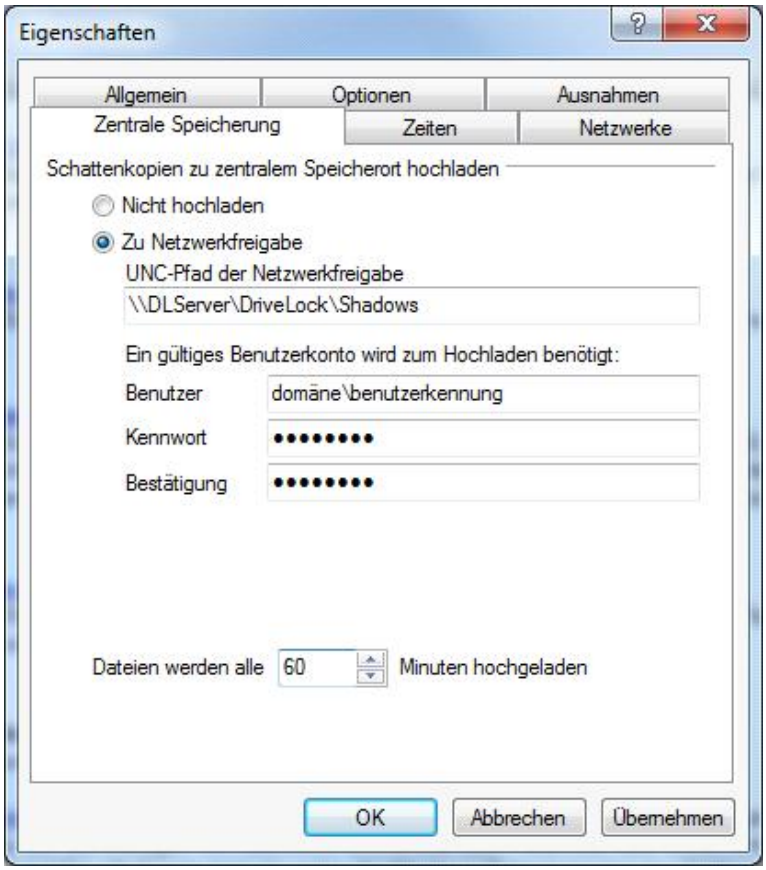


Übernehmen Sie die Einstellungen mit **OK**.

Wenn Sie zusätzlich auch noch diesen Prozess auch noch von der Dateifilterung ausnehmen möchten, aktivieren Sie die gleichnamige Option.

4.1.2.7.1.4 Einstellungen für das Hochladen auf den zentralen Schattenkopie-Server

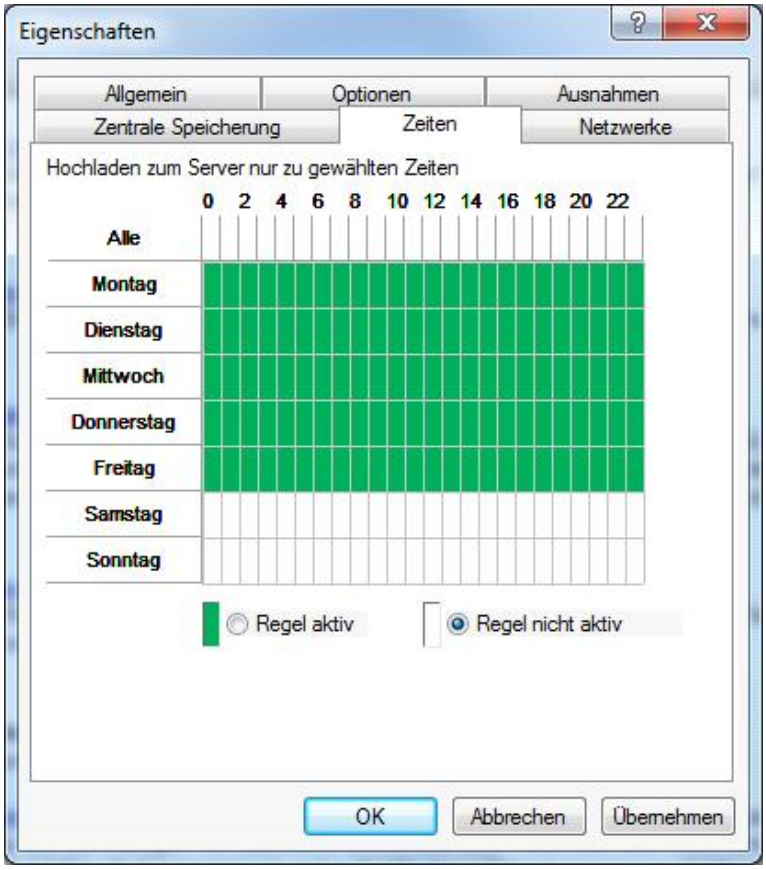
Über den Reiter „**Zentrale Speicherung**“ kann festgelegt werden, ob Schattenkopien auf einen zentralen Server hochgeladen werden sollen oder nicht.



DriveLock bietet die Möglichkeit, Schattenkopien zentral abzulegen. Hierzu kann der Pfad einer Netzwerkfreigabe angegeben werden. DriveLock verwendet das ebenfalls zu definierende Benutzerkonto, um auf die Netzwerkfreigabe zuzugreifen und die Schattenkopien dort abzulegen. Dieser Vorgang erfolgt in einem konfigurierbaren Zeitintervall (Standard 15 min).

4.1.2.7.1.5 Zeitliche Einschränkungen

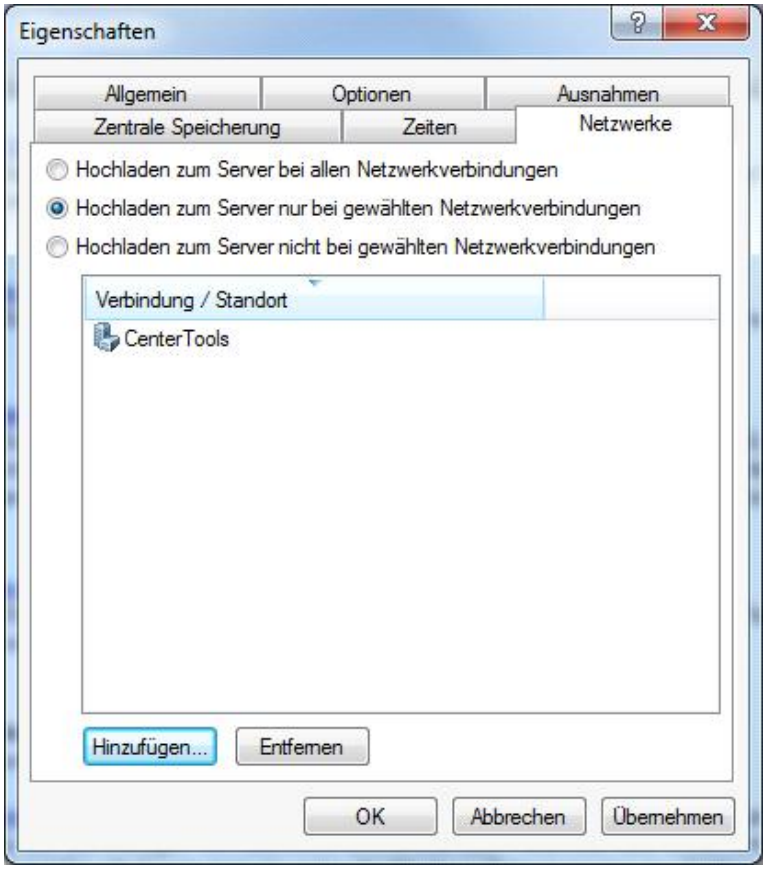
Über den Reiter „**Zeiten**“ kann festgelegt, werden wann Schattenkopien generiert werden. Wenn Sie möchten, dass die Regel nur für einen ganz bestimmten Zeitraum gelten soll, dann können Sie hier einen individuellen Zeitrahmen vorgeben (z.B. nur werktags von 09:00 Uhr bis 17:00 Uhr) Es ist ebenso möglich, ein Datum für den Beginn und das Ende der Gültigkeitsdauer anzugeben.



Markieren Sie den gewünschten Zeitraum, indem Sie entweder ein einzelnes Feld aktivieren, oder jeweils links einen Wochentag oder oben eine Zeit anklicken. Zusätzlich wählen Sie für die Auswahl entweder „**Regel aktiv**“ oder „**Regel nicht aktiv**“.

4.1.2.7.1.6 Netzwerkeinschränkungen

Über den Reiter “**Netzwerk**” können Sie festlegen, für welche aktiven Netzwerkverbindungen die Regel angewendet werden soll.



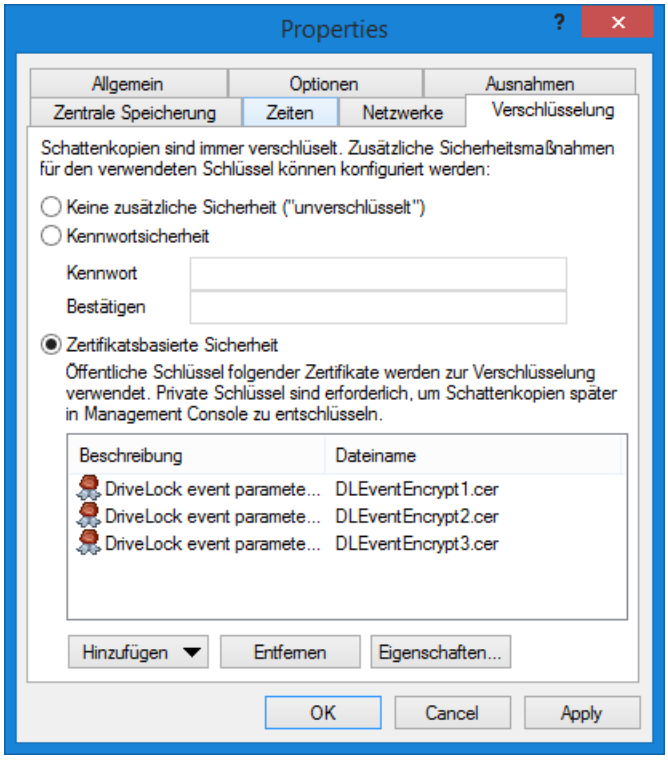
Wählen Sie eine der folgenden Möglichkeiten:

- Die Regel gilt für alle Netzwerkverbindungen
- Die Regel gilt nur für die aufgelisteten Netzwerkverbindungen
- Die Regel gilt für alle außer den aufgelisteten Netzwerkverbindungen

Klicken Sie auf **Hinzufügen**, um weitere Netzwerkverbindungen der Liste hinzuzufügen. Durch **Entfernen** werden zuvor ausgewählte Netzwerkverbindungen aus der Liste gelöscht.

4.1.2.7.1.7 Verschlüsselung

In Analogie zur Datenanonymisierung von Ereignisdaten möchten Sie vielleicht auch die Schattenkopien vor nicht autorisiertem Zugriff schützen. DriveLock verschlüsselt die Schattenkopien vor dem hochladen mit einem internen Schlüssel. Diesen Schlüssel können Sie zusätzlich mit einen Passwort oder mit dem öffentlichen Schlüssel von einem oder mehreren Zertifikaten absichern (Mehr-Augen-Prinzip). In dem Fall benötigen Sie jedes mal, wenn Sie den Schattenkopie-Speicher öffnen, das passende Passwort oder die zugehörigen privaten Schlüssel um Zugang zu den Schattenkopien zu erhalten.

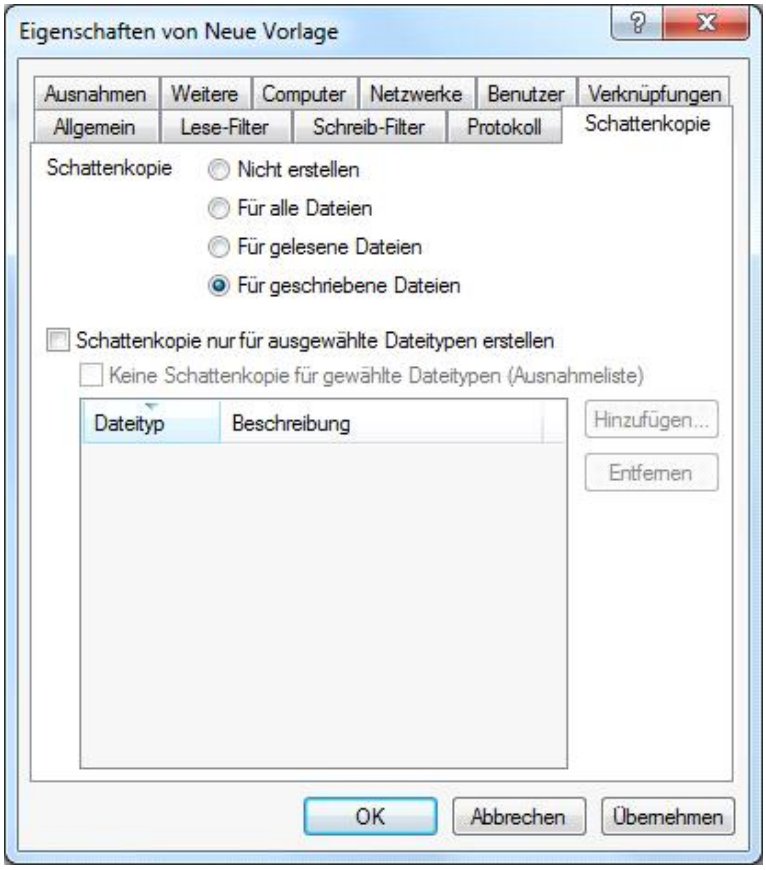


Wenn Sie diese Schlüssel verlieren können Sie den Inhalt der Schattenkopien nicht mehr einsehen.

4.1.2.7.2 Schattenkopien in Laufwerksregeln konfigurieren

Um die Erstellung von Schattenkopien zu aktivieren, muss zunächst eine Dateifilter-Vorlage erstellt werden. Bitte lesen Sie das Kapitel „Neue Dateifilter-Vorlage erstellen“ für mehr Informationen.

Innerhalb der Dateifilter-Vorlage kann angegeben werden, von welchen Dateien Schattenkopien erstellt werden sollen.

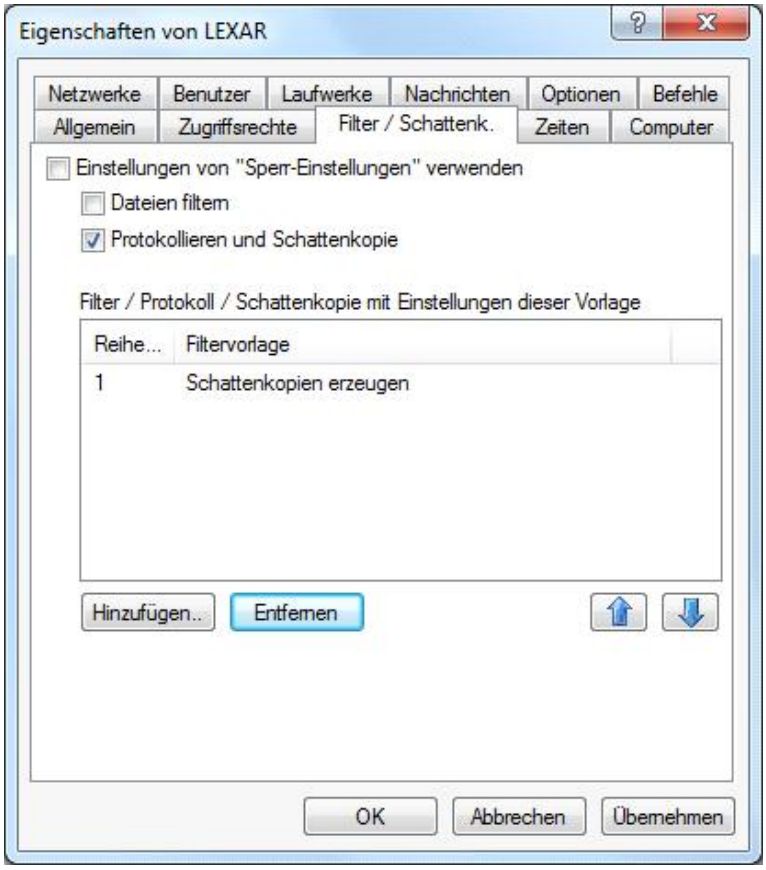


Sie können somit einstellen, ob keine Schattenkopien oder Schattenkopien von allen Dateien erstellt werden, oder nur von Dateien, die gelesen bzw. geschrieben werden. Ferner ist es möglich, eine Liste von Dateiendungen anzugeben, für welche Schattenkopien erstellt werden („**Schattenkopie nur für ausgewählte Dateitypen erstellen**“) oder nicht („**Keine Schattenkopie für gewählte Dateitypen**“).

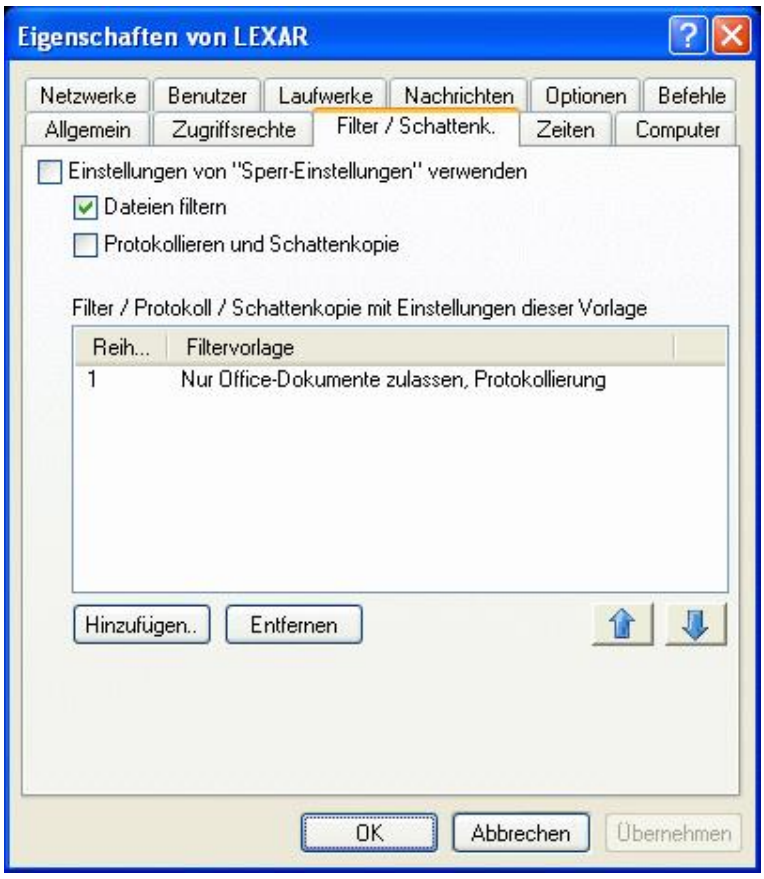
> Es ist möglich, eine Filtervorlage nur für die Erstellung von Schattenkopien anzulegen.

Eine so angelegte Filtervorlage kann für einzelne Whitelist-Regeln ebenso benutzt werden, wie für Laufwerksklassen.

Hierzu wird die Seite „*Filter / Schattenk.*“ auf der betreffenden Laufwerks-Klasse (z.B. USB oder CD-ROM) oder auf Geräte-spezifischen Whitelist-Regeln verwendet.



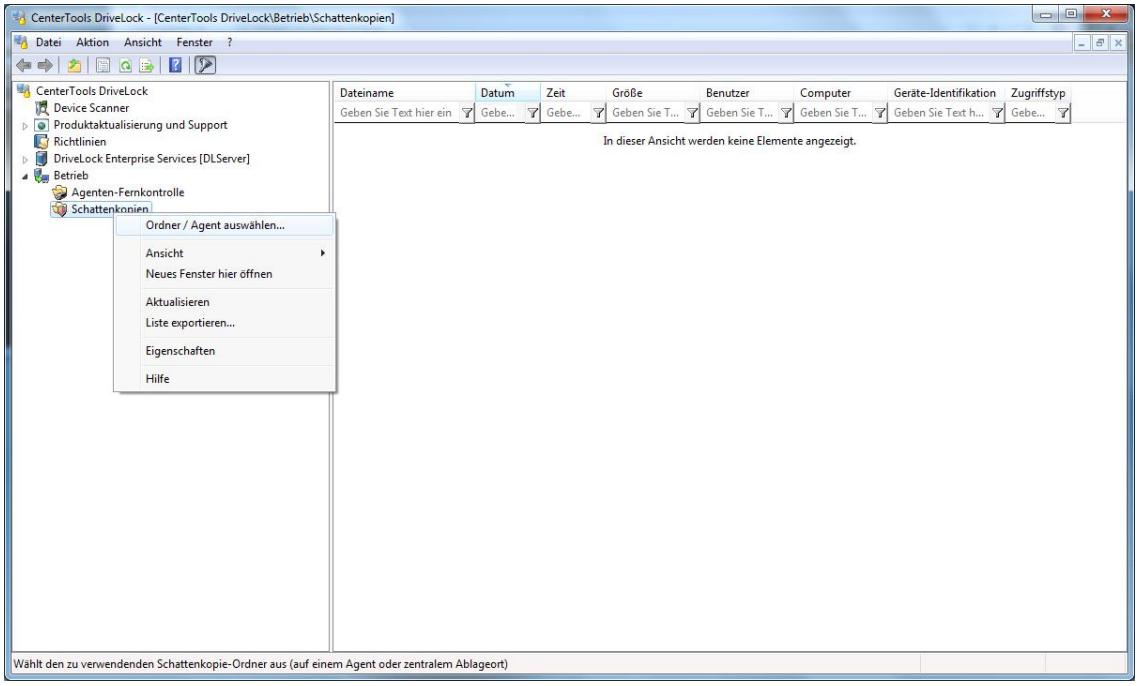
Wählen Sie die Option "*Protokollieren und Schattenkopie*", um die Erstellung von Audit-Ereignissen sowie von Schattenkopien zu aktivieren. Wählen Sie dann eine entsprechend angelegte Filter-Vorlage.



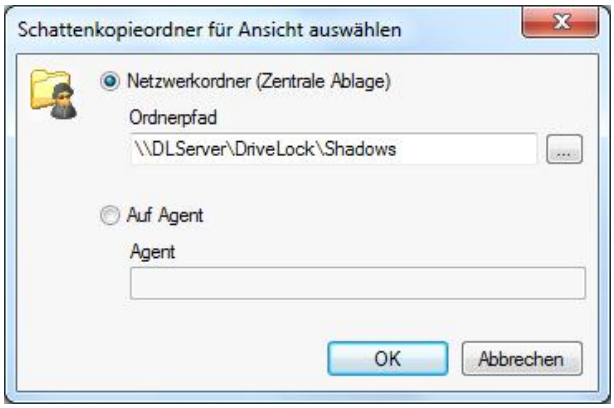
Deaktivieren Sie die Option "*Einstellungen von "Sperr-Einstellungen" verwenden*", um von der Laufwerks-klasse abweichende Einstellungen vornehmen zu können. Aktivieren Sie dann die Option „*Protokollieren und Schattenkopie*", um die Erstellung von Schattenkopien und Audit-Ereignissen zu aktivieren.

4.1.2.7.3 Schattenkopien ansehen

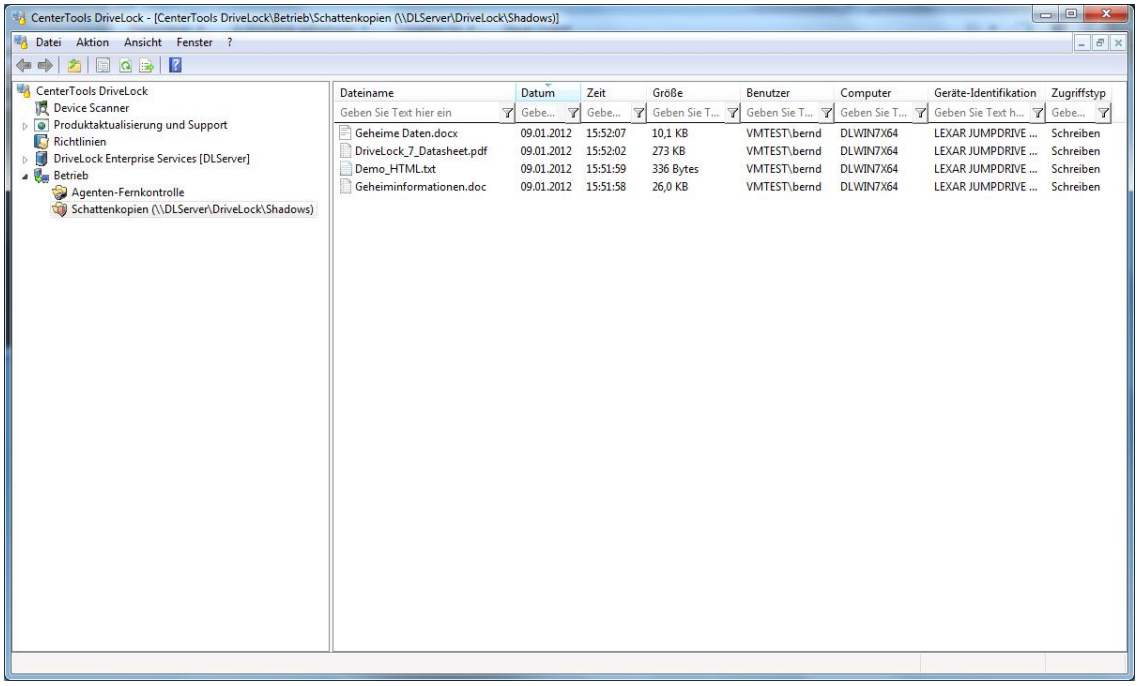
Schattenkopien können mit Hilfe der DriveLock Management Konsole betrachtet werden. Hierzu steht der Punkt *Betrieb* | *Schattenkopien* zur Verfügung.



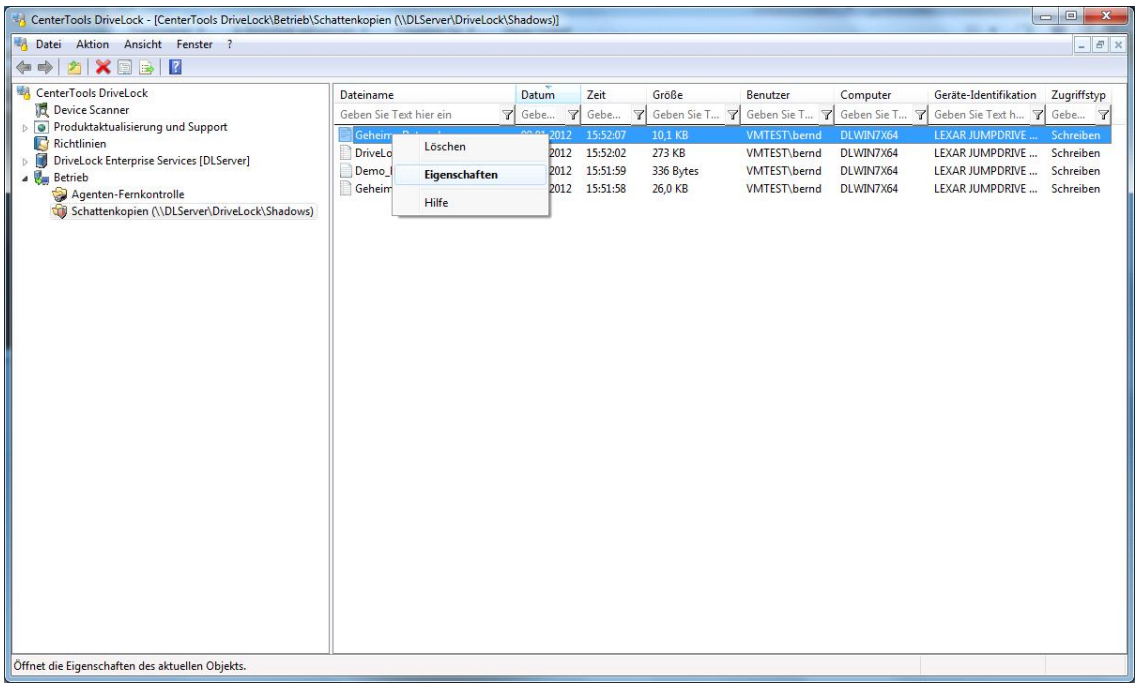
Rechtsklicken Sie auf **Schattenkopie** und wählen Sie **Ordner / Agent auswählen** aus dem Kontextmenü.



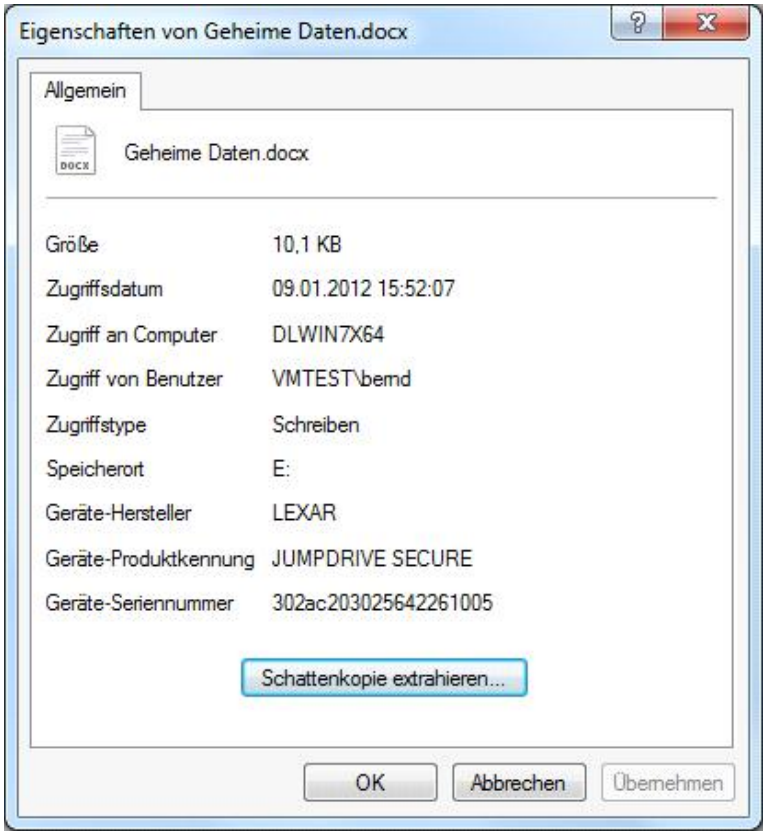
Geben Sie dann den Netzwerkordner ein, auf welchem die Schattenkopien abgelegt wurden (in der Regel ein konfigurierter zentraler Ablageort) oder geben Sie den Namen des Agenten ein, von dem die Schattenkopien betrachtet werden sollen. Klicken Sie auf **OK** um fortzufahren.



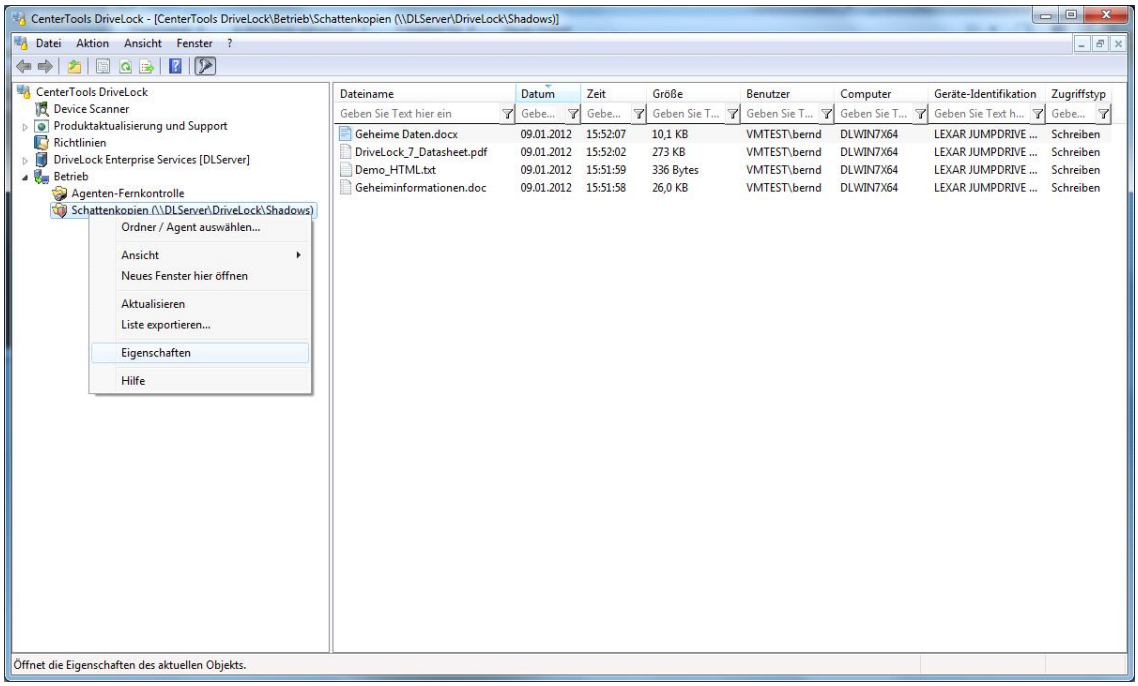
Nach einer erfolgreichen Verbindung werden die Schattenkopien als Liste in der Management Konsole angezeigt.



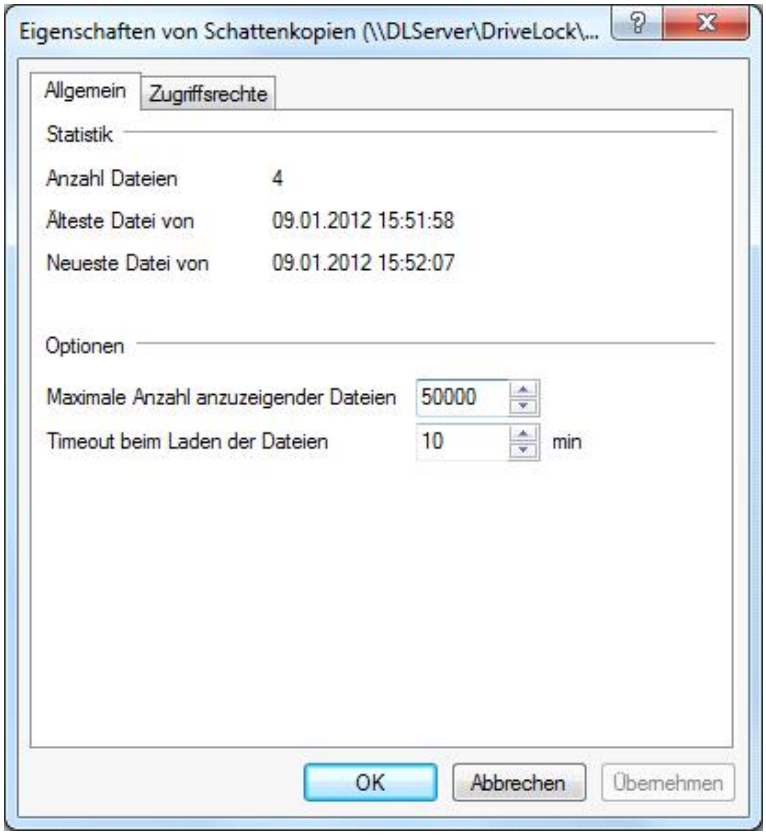
Durch einen Doppelklick lassen sich die Eigenschaften der jeweiligen Datei anzeigen; über den Befehl *„Schattenkopie extrahieren“* wird die Schattenkopie auf einem anderen Ort abgelegt. Wenn Sie ein Passwort oder Zertifikate eingerichtet haben, um die Schattenkopien zu schützen, müssen sich jetzt mit den passenden Schlüsseln authentifizieren.



Klicken Sie **OK**, um das Informationsfenster zu schließen.



Rechtsklicken Sie auf **Schattenkopien** und wählen Sie **Eigenschaften** aus dem Kontextmenü, um sich Details zum ausgewählten Ablageort der Schattenkopien anzeigen zu lassen.



Neben der Information zur Anzahl der enthaltenen Dateien und dem Datum der ältesten und neuesten Datei, können Sie an dieser Stelle auch die maximale Zahl der angezeigten Dateien und einen Timeout-Wert für die Anzeige festlegen. Das ist insbesondere beim Zugriff auf Netzwerkressourcen mit vielen Dateien hilfreich.

Klicken Sie **OK**, um das Fenster zu schließen.

4.2 Geräte kontrollieren

Als Beispiel in diesem Handbuch wird eine zentral gespeicherte Richtlinie verwendet, um die nötigen Schritte zum Sperren von Geräten demonstrieren. Es wird gezeigt, wie Windows-Mobile Geräte gesperrt und ein einzelner Pocket-PC freigegeben werden kann. Die meisten Schritte gelten analog für alle anderen Gerätetypen, Unterschiede werden getrennt davon behandelt.

> Die Konfiguration der Agenten über Gruppenrichtlinien oder Konfigurationsdateien erfolgt auf demselben Weg. Außer der unterschiedlichen Verbreitung der Einstellungen gibt es keinen Unterschied.

Es ist wichtig, zu verstehen, dass DriveLock das Prinzip von Whitelist-Regeln verwendet. Das bedeutet, dass nach der Aktivierung der grundsätzlichen Sperrung von Geräten jedes Gerät zunächst gesperrt ist (d.h. die „Geräte-Firewall" ist in Betrieb). Jede Ausnahme davon muss getrennt durch eine sog. Whitelist-Regel konfiguriert werden. Das bedeutet, dass Sie für jedes Gerät (bzw. für jede Gruppe von Geräten), das verwendet werden soll, eine eigene Regel erstellen müssen. Falls ein Gerät nicht über eine entsprechende Regel definiert ist, sperrt DriveLock automatisch den Zugriff darauf und es kann nicht verwendet werden. Damit wird sichergestellt, dass Ihre Sicherheitsrichtlinie intakt bleibt, auch wenn zwischenzeitlich neue und noch mächtigere Geräte entwickelt und durch Ihre Benutzer verwendet werden.

Um eine DriveLock Konfiguration durchzuführen, ist es aufgrund dieses Grundprinzips angeraten, zunächst benötigte Whitelist-Regeln zu erstellen und anschließend das Sperren von Laufwerken bzw. Geräten zu aktivieren.

Es muss für jedes Gerät, dass auf einem Computer verwendet werden soll bzw. muss, eine eigene Regel erstellt werden muss. Um diese Aufgabe zu vereinfachen, bietet DriveLock die Möglichkeit, Regeln für unterschiedliche Geltungsbereiche auf unterschiedlichen Ebenen zusammenzufassen:

- Geräteklasse (z.B. alle Bluetooth Transmitter)
- Geräte-Bus (z.B. alle PCI Netzwerkkarten)
- Hardware ID (z.B. ein spezielles Smartcard Lesegerät)

Zusätzlich zum Geltungsbereich kann definiert werden, wann und wo eine Whitelist-Regel angewendet werden soll:

- Auf welchen Computern (alle oder nur bestimme) soll die Regel gelten?
- Für welche aktiven Netzwerkverbindungen soll sie gelten?
- Zu welcher Zeit (z.B. Montag bis Freitag zwischen 09:00 und 18:00 Uhr)?
- Soll eine Regel für alle Benutzer gelten, oder kann eine bestimmte Gruppe ein Gerät verwenden, während es für alle anderen gesperrt ist?

Mit der Verwendung dieser Geltungsbereiche (und anderen Mechanismen wie z.B. Computervorlagen, die später erklärt werden), kann die Anzahl der benötigten Regeln in Ihrer Konfiguration minimiert werden.

Ein Schritt, der durchgeführt werden muss, ist die generelle Aktivierung der Gerätesperre. Dieser wird im Abschnitt „Gerätesperrung aktivieren“ beschrieben.

> Wenn Sie DriveLock evaluieren, dürften Sie wahrscheinlich zuerst die generelle Sperrung aktivieren (z.B. mit dem Konfigurationsassistenten), bevor Sie beginnen, einzelne Regeln zu konfigurieren. In einer Produktionsumgebung sollten jedoch zuerst alle notwendigen Regeln erstellt werden, bevor Sie die Sperrung sozusagen „scharf schalten“.

4.2.1 Geräte in der Basiskonfiguration sperren

Geräte können auf die gleiche Art und Weise gesperrt werden, wie Laufwerke. In der Voreinstellung sperrt DriveLock zunächst keine Geräte (bzw. Geräte-Klassen). Wenn Sie eine Geräte-Klasse sperren, werden alle Geräte, die zu dieser Klasse gehören (oder über den gleichen Controller oder dieselbe Schnittstelle verbunden sind) ebenfalls gesperrt. Ausnahmen dazu werden wieder über Whitelist-Regeln definiert.

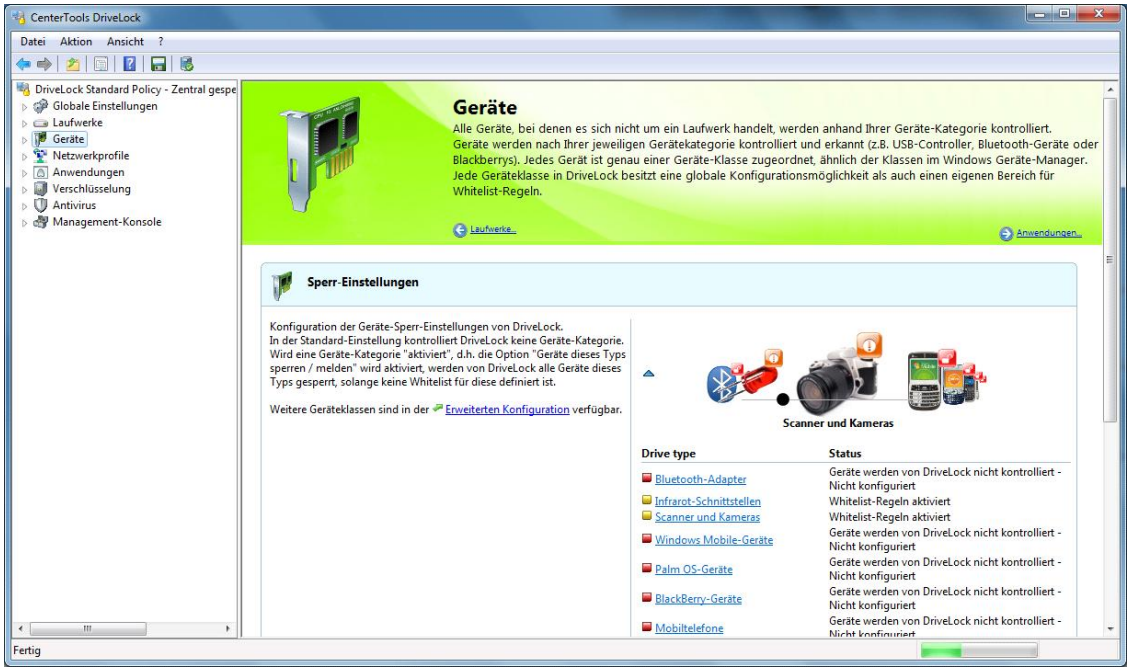
DriveLock unterscheidet zwischen Controller, Schnittstellen und Geräten. Sie können für die folgenden Controller oder Schnittstellen eine Sperrung einrichten:

- Serielle (COM) und Parallele (LPT) Schnittstelle
- Bluetooth Schnittstelle
- Infrarotschnittstelle
- USB Controller
- Firewire (1394) Controller
- PCMCIA Controller

Hier die Liste der Geräte, die DriveLock kontrollieren und sperren kann:

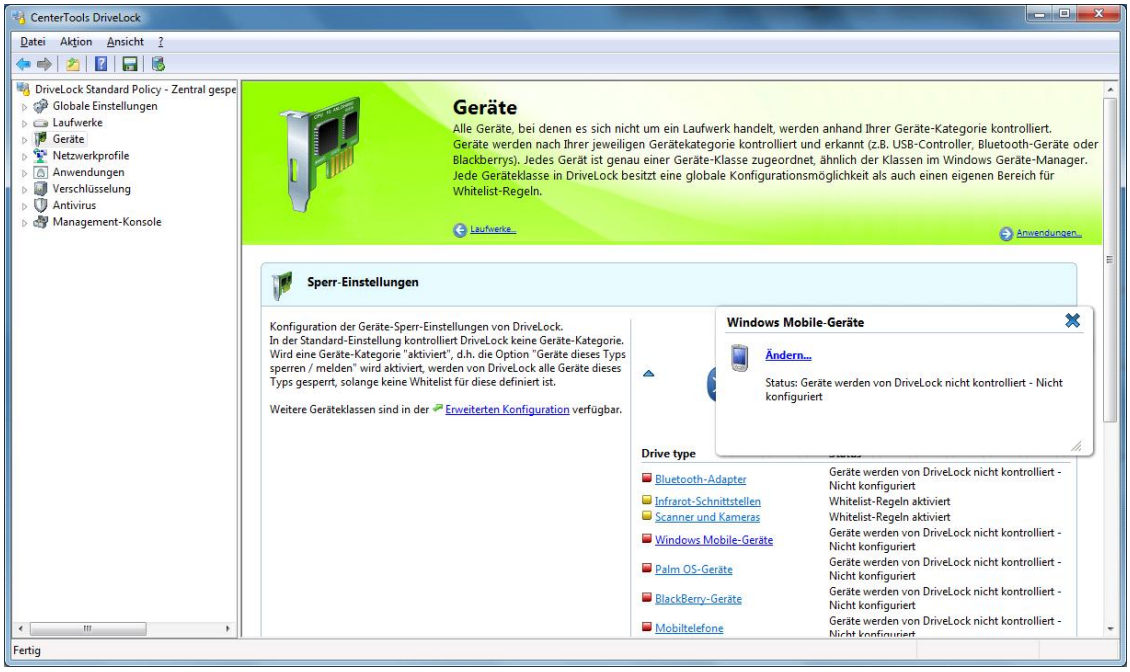
- Windows CE Handhelds und Smartphones
- Palm OS Handhelds und Smartphones
- Scanner und Kameras
- Modems
- Drucker
- Netzwerkadapter

- Smartcard-Leser
- Audio-, Video, und Game Controller
- Blackberry Geräte
- Virtuelle Geräte (VM Ware)
- Mobiltelefone
- Eingabegeräte
- Media Player Geräte
- Biometrische Geräte
- Geräte zum Softwareschutz (Dongles)
- Secure Digital Host Controllers
- Bandlaufwerke
- PCMCIA und Flashspeicher Geräte
- IEC 61883 (AVC) Bus Geräte
- Media Center Extender Geräte
- SideShow Geräte
- Sensor Geräte

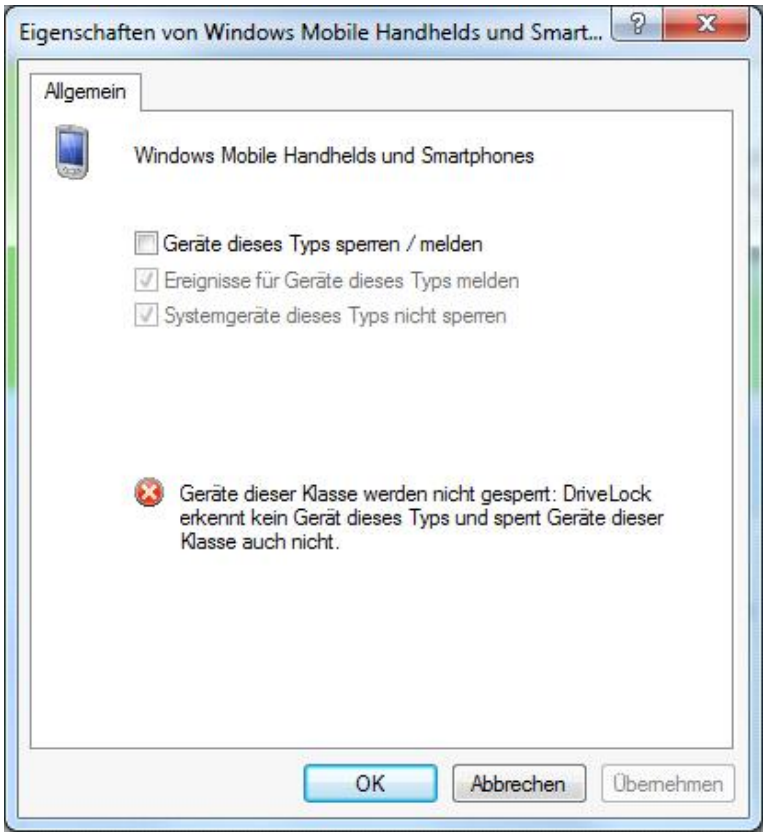


Verwenden Sie die kleinen blauen Pfeilsymbole ▾ und ▴, um die Gerätedetails ein- bzw. auszuschalten.

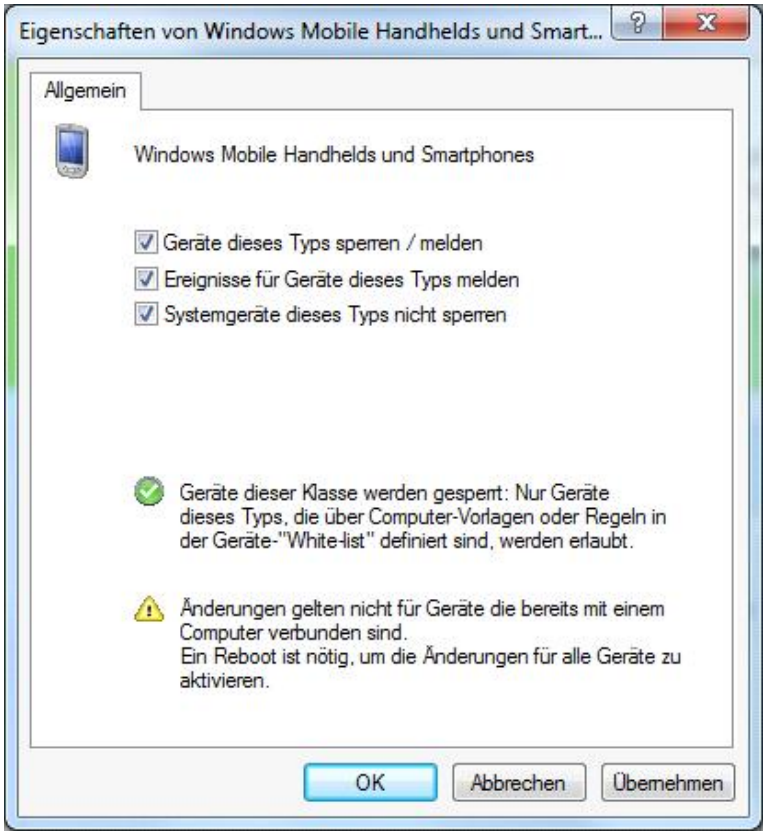
Um die Einstellungen für einen Gerätetyp (z.B. Windows Mobile-Geräte) zu ändern, klicken Sie auf den entsprechenden Link. Sie können auf den Ziehregler (schwarzer Punkt) verwenden, das gewünschte Gerät in den Vordergrund holen und anschließen darauf doppelklicken.



Es erscheint ein kleines Popup-Fenster, welches die aktuell konfigurierten Einstellungen anzeigt. Klicken Sie auf **Ändern**.



Die Konfiguration ist für alle Geräte-Klassen mit Ausnahme der Klassen "*Serielle Schnittstelle*" und "*Parallele Schnittstelle*" identisch. Die Konfiguration dieser Schnittstellen ist im Abschnitt „Konfigurieren der Schnittstellen COM und LPT" beschrieben.



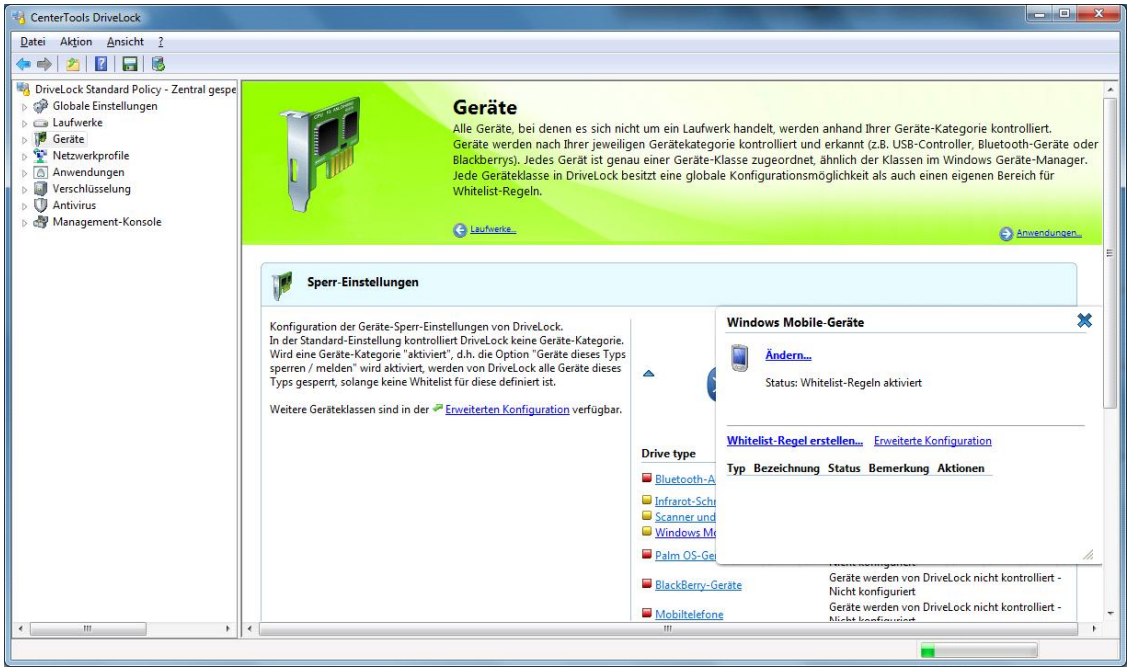
Durch Auswahl von "**Geräte dieses Typs sperren / melden**" wird die Sperrung für die ausgewählte Geräte-Klasse aktiviert.

> Eine Sperrung kann auch anhand eines gelben Ausrufezeichens innerhalb des Windows Geräte-Manager erkannt werden.

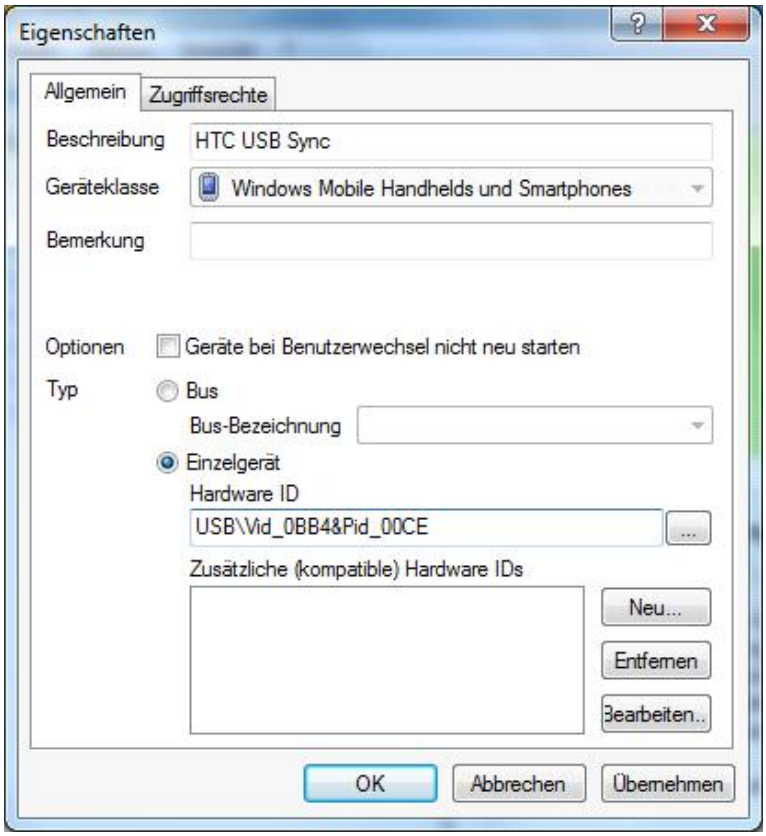
Zusätzlich können Sie angeben, ob die dazugehörenden Überwachungsereignisse generiert werden. Sofern diese Funktion aktiviert ist, werden die Ereignisse an die konfigurierten Stellen (z.B. Windows Ereignisanzeige, DriveLock Enterprise Service) übertragen.

Ein Systemgerät ist zum Beispiel eine Netzwerk-Miniport-Treiber oder ein UBS-Root-Hub. Damit nicht für diese „Software"-Geräte eigene Whitelist-Regeln definiert werden müssen, ist diese Option zunächst grundsätzlich aktiviert. Wenn Sie diese deaktivieren, müssen für alle diese Systemgeräte eigene Regeln erstellt werden.

Klicken Sie **OK**, um die Änderungen zu übernehmen.



Klicken Sie auf **Whitelist-Regel erstellen**, um eine neue Whitelist-Regel für diesen Gerätetyp hinzuzufügen.



Geben Sie einen Namen für die Whitelist-Regel in das Feld „*Beschreibung*“ ein. Sie können zusätzlich noch eine Bemerkung als zusätzliche Beschreibung eingeben.

Schränken Sie den Geltungsbereich durch die Angabe zusätzlicher Informationen weiter ein. Sie können entweder einen Bus auswählen oder eine Hardware ID eingeben. Wenn Sie eine Regel für ein Gerät erstellen möchten, dass über einen bestimmten Bus verbunden wird, dann wählen Sie „**Bus**“ und den passenden Eintrag aus der Dropdown-Liste aus.

Somit wird diese Regel nur angewandt, wenn das Gerät zur gleichen Geräte-Klasse gehört (hier: Windows Mobile Handhelds und Smartphones) und über den konfigurierten Bus angeschlossen wird.

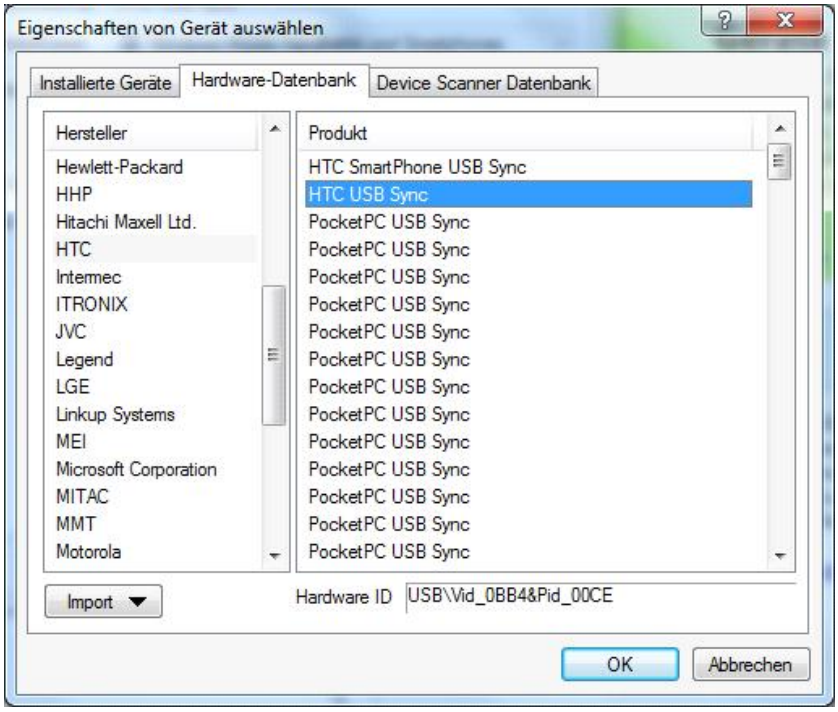
Beispiel: Wenn Sie alle eingebauten PCI-Karten freigeben möchten, erstellen Sie eine neue Whitelist-Regel für alle kontrollierten Geräte-Klassen und wählen als Bus "**PCI**" aus. Dadurch könnten Sie nun andere Netzwerkkarten, die über andere Schnittstellen angebunden werden können (z.B. USB, PCMCIA usw.) sperren.

Um Geräte noch genauer voneinander zu unterscheiden, werden Hardware IDs und deren sogenannte Compatible IDs verwendet. Jedes Gerät besitzt eine einzigartige Hardware ID. Zusätzlich pflegt Windows eine Liste mit dazu kompatiblen Geräten (Compatible ID). Die Hardware ID oder die Compatible ID wird dazu verwendet, um den passenden Treiber zu finden. Zusätzlich können die Hardware IDs auch noch eine Revisionsnummer, die durch den Hersteller vergeben wird, enthalten (die jedoch für die Wahl des Treibers irrelevant ist). In diesem Fall wird von Windows eine der Compatible IDs verwendet, die nicht diese Revisionsnummer enthält.

Geben Sie die korrekte Hardware ID in das entsprechende Feld ein, um das gewünschte Gerät anzugeben. Die Hardware ID kann entweder aus der Ereignisanzeige oder der Registrierungsdatenbank ausgelesen werden.

Stellen Sie sicher, dass keine Leerzeichen vor oder nach der Hardware ID eingegeben wurden.

Ein weitaus bequemerer Weg, um die Hardware ID zu ermitteln, besteht darin, die mitgelieferte Hardware-Datenbank zu verwenden, indem Sie auf den Button „…" neben dem Hardware ID Feld klicken.



Nun können Sie im Augenblick vorhandene Geräte auswählen, oder sich zu einem anderen Agenten auf einem entfernten Rechner verbinden, um die dort verfügbaren Geräte zu ermitteln.

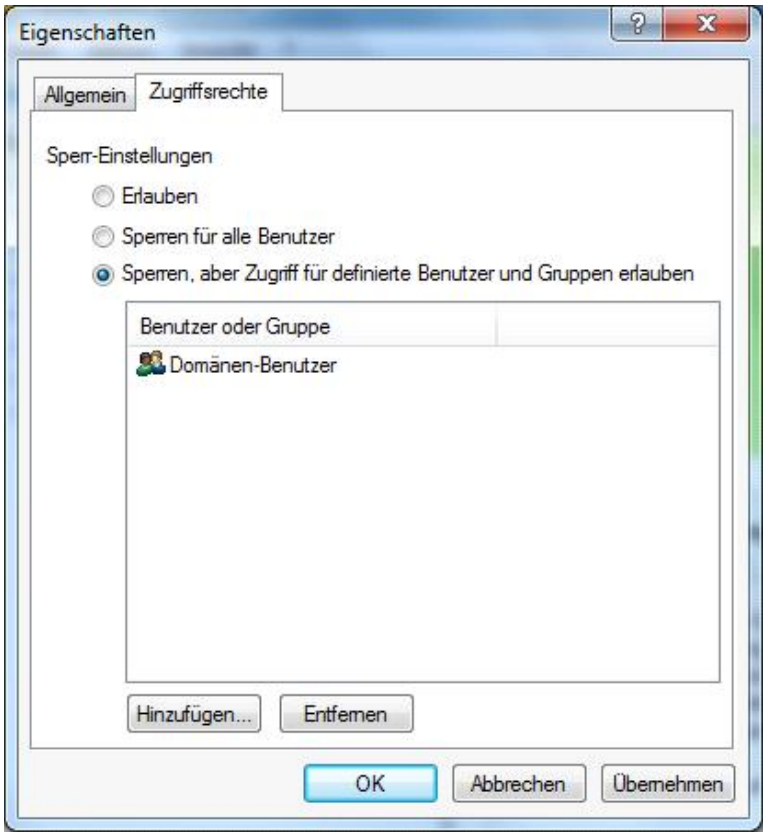
Klicken Sie **Aktualisieren**, um kürzlich neu hinzugekommene Geräte anzeigen zu lassen. Palm oder Windows CE basierte Handhelds sind üblicherweise solange verbunden, so lange ActiveSync oder HotSync läuft.

Die Option „**Systemgeräte nicht anzeigen**" verbirgt alle Windows Systemgeräte, die in der Grundeinstellung über die Funktion „**Systemgeräte dieses Typs nicht sperren**" in den Sperreinstellungen für die Geräte-Klassen freigegeben sind.

Weiterhin können Sie den Tab **Hardware-Datenbank** oder **die Device Scanner Datenbank** verwenden, um ein Gerät aus der dann angezeigten Liste zu wählen.

Wählen Sie einen Eintrag und klicken Sie auf **OK**.

Wählen Sie den Reiter „**Zugriffsrechte**“, um festzulegen, welche Benutzer bzw. Gruppen Zugriff auf das Gerät erhalten.

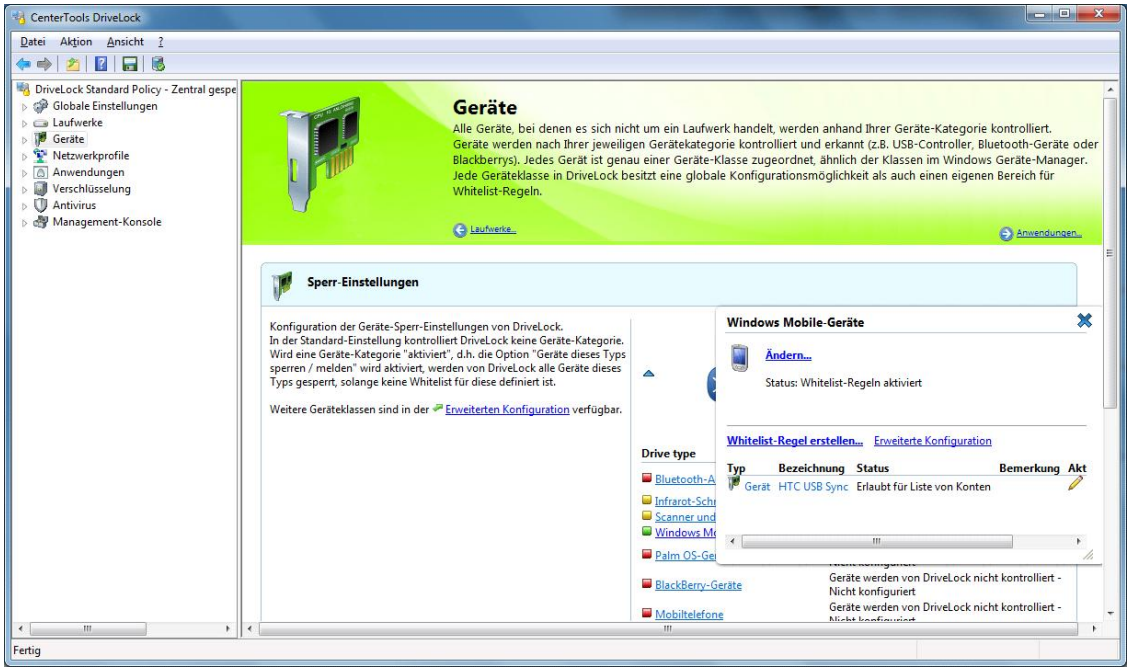


Folgende Möglichkeiten stehen zur Auswahl:

- *Erlauben*: Jeder authentisierte Benutzer kann dieses Gerät verwenden
- *Sperren für alle Benutzer*: Der Zugriff auf dieses Gerät ist für alle Benutzer gesperrt.
- *Sperren, aber Zugriff für definierte Benutzer und Gruppen erlauben*: Das Gerät ist gesperrt, aber Zugriff ist für den oder die angegebenen Benutzer bzw. Gruppen möglich.

Klicken Sie auf **Hinzufügen**, um eine weitere Gruppe oder einen Benutzer zur angezeigten Liste hinzuzufügen. Mit **Entfernen** wird der zuvor ausgewählte Eintrag gelöscht.

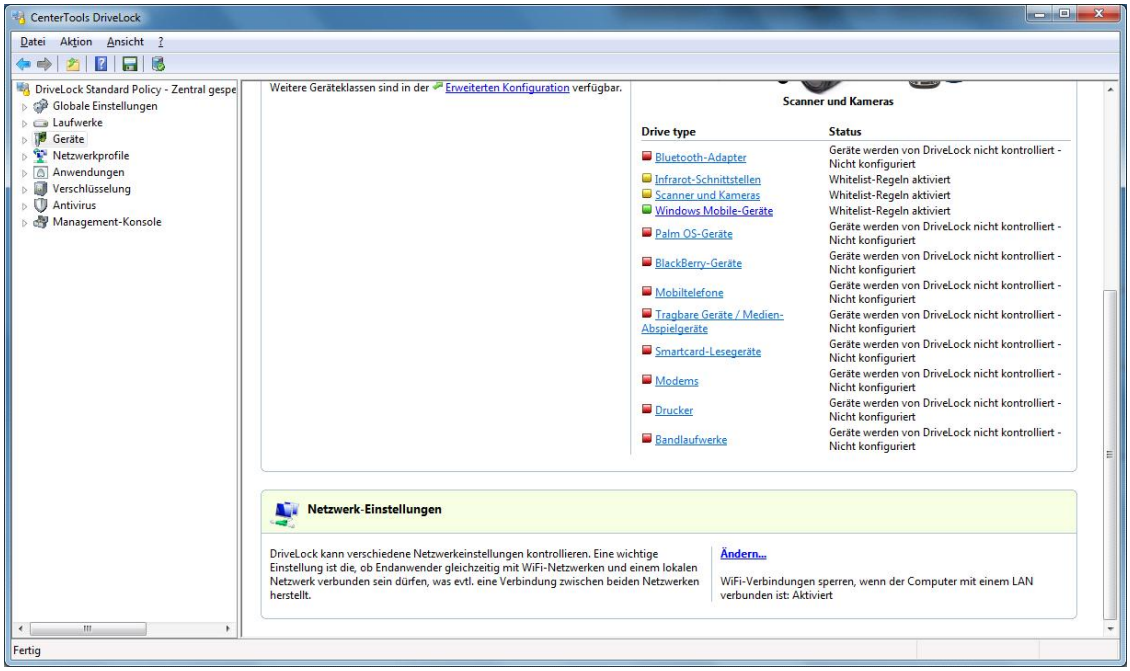
Klicken Sie **OK**, um alle Einstellungen zu übernehmen.



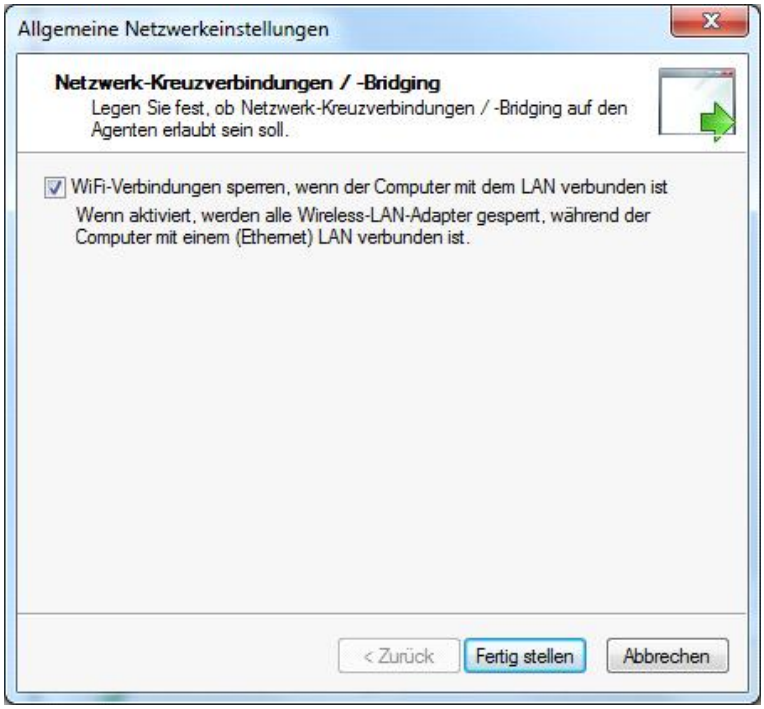
Im Popup-Fenster wird die neu erstellte Regel nun angezeigt. Klicken Sie auf das Symbol ✖, um das Popup-Fenster zu schließen.

Das Symbol des jeweiligen Gerätetyps zeigt den jeweiligen Sicherheitslevel der gerade aktuellen Konfiguration an:

- *Grünes Symbol*: diese Geräteklasse ist für alle Benutzer gesperrt (hoher Sicherheitslevel)
- *Gelbes Symbol*: diese Geräteklasse ist für einige Benutzer gesperrt und für andere freigegeben (mittlerer Sicherheitslevel)
- *Rotes Symbol*: diese Geräteklasse ist für alle Benutzer freigegeben (niedriger Sicherheitslevel)



Scrollen Sie nach unten und klicken Sie auf **Ändern**, um einzustellen, ob DriveLock alle WLAN-Geräte deaktiviert, sobald der Computer über ein Netzwerkkabel mit einem Netz verbunden ist.

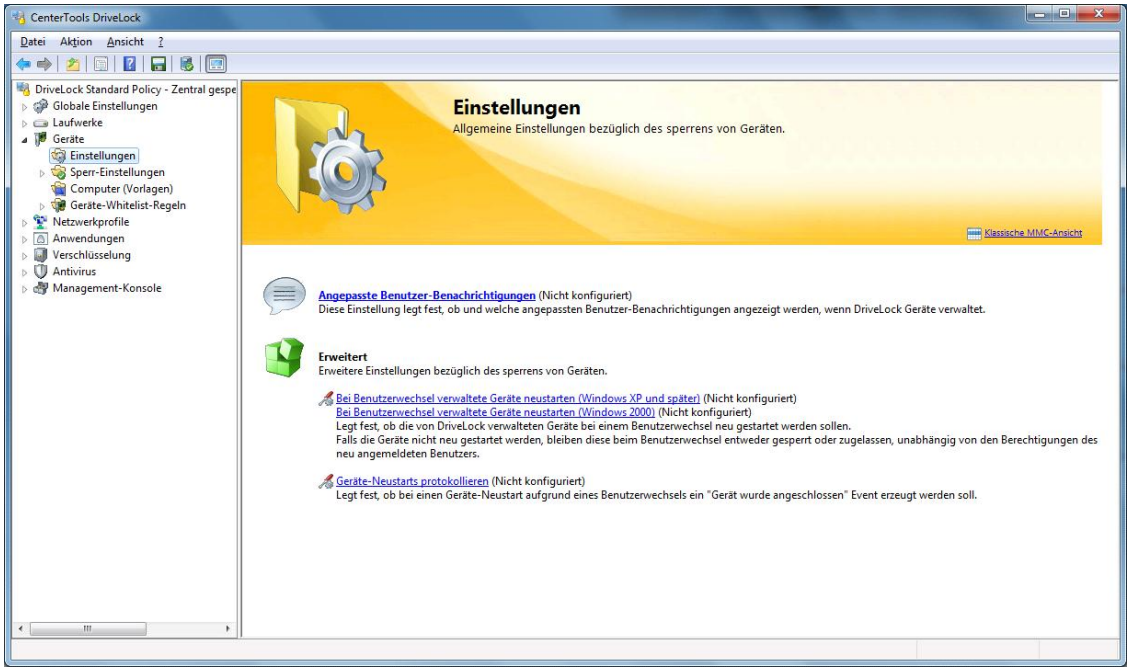


Aktivierten Sie diese Option, um sogenannte Cross-Network-Links zu unterbinden. Klicken Sie **Fertig stellen**, um die Einstellung zu übernehmen.

Die aktuell konfigurierte Einstellung wird in der DriveLock Management Konsole angezeigt.

4.2.2 Erweiterte Einstellungen zum Sperren von Geräten

Bei der Konfiguration der Einstellungen für Gerätesperren bzw. –freigaben können Sie noch weitere allgemeinere Einstellungen festlegen.



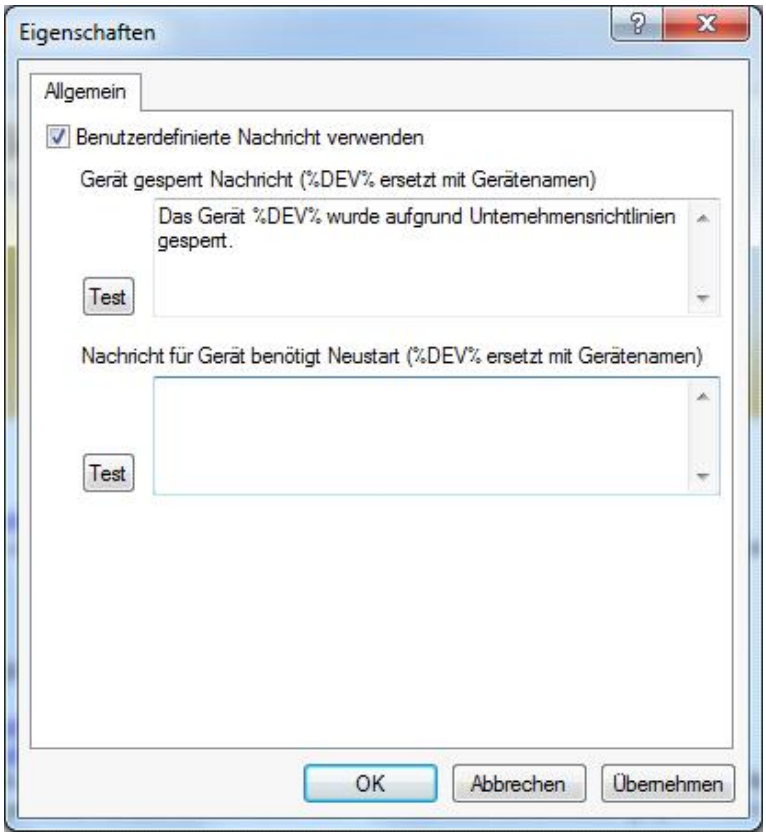
Um diese Einstellungen zu konfigurieren, klicken Sie auf **Geräte** und anschließend auf **Einstellungen**.

4.2.2.1 Allgemeine Einstellungen zur Gerätesperrung

4.2.2.1.1 Konfiguration von Benutzermeldungen

Sobald ein Gerät durch DriveLock mit Hilfe einer Whitelist-Regel gesperrt wird, kann DriveLock, sofern die entsprechende Option für Dialogfenster aktiviert wurde, dem aktuellen Benutzer eine Meldung anzeigen. Klicken Sie **Angepasste Benutzer-Benachrichtigungen**, um eigene Meldungen zu definieren.

> Wenn Sie mehrsprachige Benutzermeldungen konfiguriert haben, zeigt DriveLock an Stelle dieser Meldungen die Standardmeldungen in der aktuellen Sprache an.



Markieren Sie "**Benutzerdefinierte Meldungen verwenden**", um die hier festgelegten Meldungen zu aktivieren. Die Variable "%DEV%" wird zur Laufzeit mit dem aktuellen Namen des gesperrten Gerätes ersetzt.

Klicken Sie auf **Test**, um sich die eingegebene Meldung als Vorschau anzeigen zu lassen.

> Sie können auf einige der HTML-Tags für die Formatierung Ihrer Nachricht verwenden (z.B. Text").

4.2.2.1.2 Erweiterte Einstellungen zur Kontrolle von Geräten

Es existieren noch weitere Konfigurationsmöglichkeiten, die über die entsprechenden Links in der Taskview-Ansicht erreicht werden können:

- *Bei Benutzerwechsel verwaltete Geräte neu starten*: Falls diese Funktion aktiviert ist, werden all Geräte automatisch neu gestartet, wenn ein Benutzerwechsel stattfindet.
- *Geräte-Neustarts protokollieren*: DriveLock generiert Überwachungsereignisse bei einem Geräte-Neustart, wenn diese Funktion aktiviert ist.

Wählen Sie jeweils entweder „**Aktiviert**“, „**Deaktiviert**“ oder „**Nicht konfiguriert**“ aus.

4.2.2.2 Gerätesperrung aktivieren

Geräte können auf die gleiche Art und Weise gesperrt werden, wie Laufwerke. In der Voreinstellung sperrt DriveLock zunächst keine Geräte (bzw. Geräte-Klassen). Wenn Sie eine Geräte-Klasse sperren, werden alle Geräte, die zu dieser Klasse gehören (oder über den gleichen Controller oder dieselbe Schnittstelle verbunden sind) ebenfalls gesperrt. Ausnahmen dazu werden wieder über Whitelist-Regeln definiert.

DriveLock unterscheidet zwischen Controller, Schnittstellen, Smartphones und Geräten. Sie können für die folgenden Controller oder Schnittstellen eine Sperrung einrichten:

- Serielle (COM) und Parallele (LPT) Schnittstelle
- Bluetooth Schnittstelle
- Infrarotschnittstelle
- USB Controller
- Firewire (1394) Controller
- PCMCIA Controller

Die folgenden unterschiedlichen Smartphones können getrennt gesperrt werden:

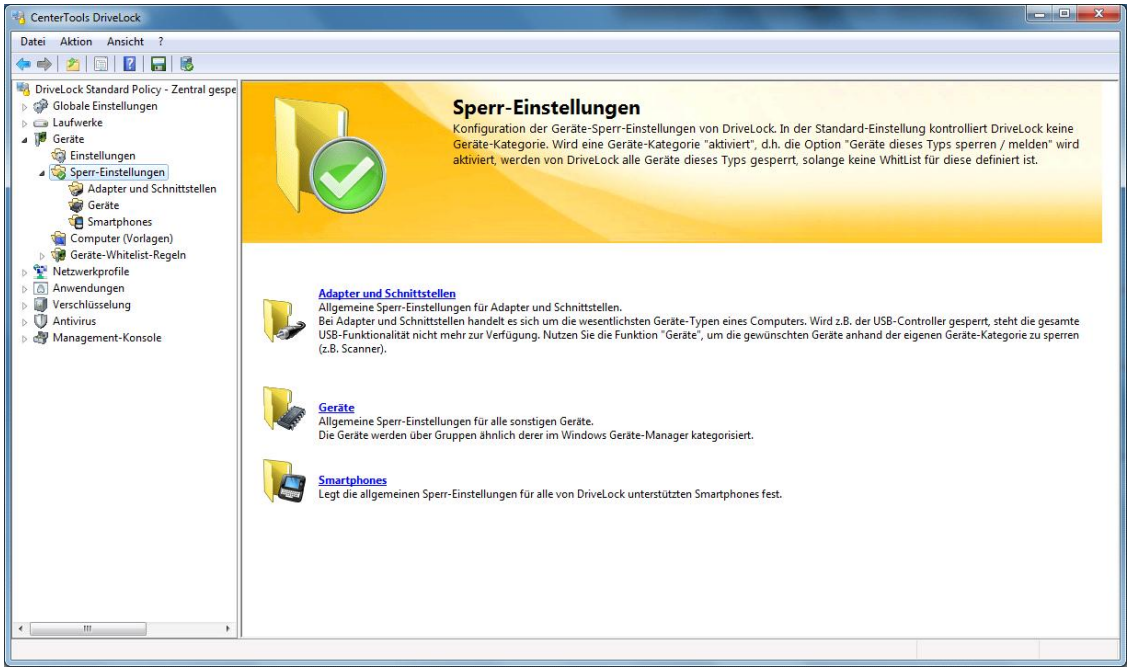
- Windows CE Handhelds und Smartphones
- Palm OS Handhelds und Smartphones

- Apple iTunes-synchronisierte Geräte
    - iTunes-Softwarebeschränkungen
- BlackBerry-Geräte
- Mobiltelefone (Nokia)

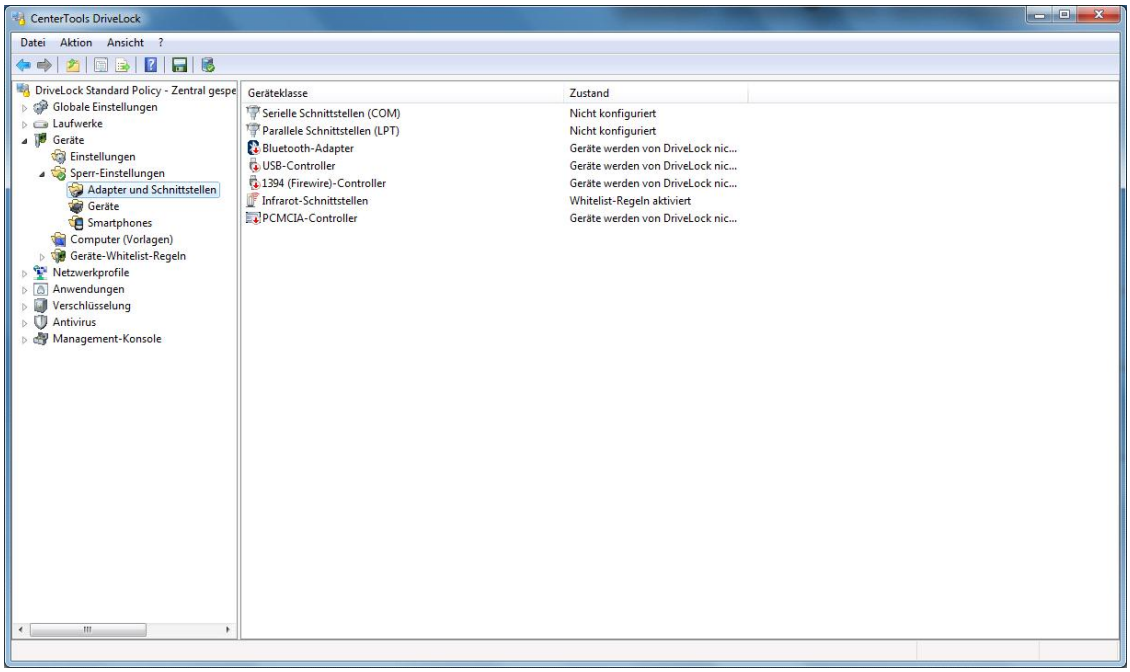
Hier die Liste der Geräte, die DriveLock kontrollieren und sperren kann:

- Scanner und Kameras
- Modems
- Drucker
- Netzwerkadapter
- Smartcard-Leser
- Audio-, Video, und Game Controller
- Virtuelle Geräte (VM Ware)
- Eingabegeräte
- Media Player Geräte
- Biometrische Geräte
- Geräte zum Softwareschutz (Dongles)
- Secure Digital Host Controllers
- Bandlaufwerke
- PCMCIA und Flashspeicher Geräte
- IEC 61883 (AVC) Bus Geräte
- Media Center Extender Geräte
- SideShow Geräte
- Sensor Geräte

Um die Sperrung von Geräten zu aktivieren, öffnen Sie die DriveLock Management Console und wählen "**Lokale Richtlinie -> Geräte -> Sperr-Einstellungen**" auf der linken Seite.

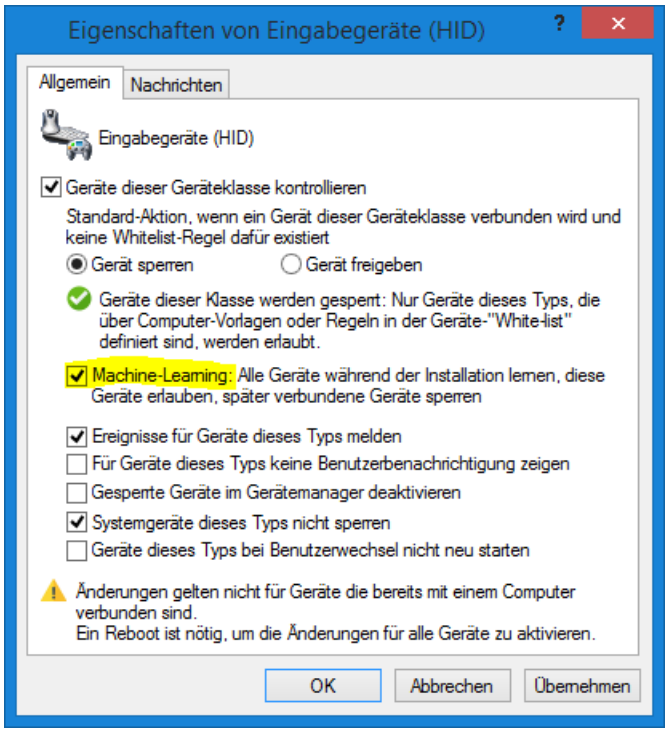


Klicken Sie auf **Adapter und Schnittstellen, Geräte** oder **Smartphones**, um alle dazugehörenden Geräte-Klassen aufzulisten.



Oder:

Klicken Sie **Eingabegeräte (HID)** (oder eine andere Klasse), um das Konfigurationsfenster zu öffnen.



Machine Learning

Für viele Gerätetypen können Sie **Machine-Learning** einschalten. Wenn diese Regel zum ersten Mal angewendet wird, werden zum Installationszeitpunkt verbundene Geräte in einer lokalen Whitelist gelernt und sind in Zukunft während der Bootphase freigegeben. Geräte dieses Typs, die später verbunden werden, bleiben geblockt. Im Beispiel oben, würde ein BAD-USB Stick, der eine Tastatur simuliert, geblockt werden. Um die lokale Whitelist neu zu lernen, führen Sie `drivelock -recreatebootdevs` in der Kommandozeile aus.

Die Konfiguration ist für alle Geräte-Klassen mit Ausnahme der Klassen “Serielle Schnittstelle” und “Parallele Schnittstelle” identisch. Die Konfiguration dieser Schnittstellen ist im Abschnitt „Konfigurieren der Schnittstellen COM und LPT“ beschrieben.

> Eine Sperrung kann auch anhand eines gelben Ausrufezeichens innerhalb des Windows Geräte-Manager erkannt werden.

Zusätzlich können Sie angeben, ob die dazugehörenden Überwachungsereignisse generiert werden. Sofern diese Funktion aktiviert ist, werden die Ereignisse an die konfigurierten Stellen (z.B. Windows Ereignisanzeige, DriveLock Enterprise Service) übertragen.

Ein Systemgerät ist zum Beispiel ein Netzwerk-Miniport-Treiber oder ein UBS-Root-Hub. Damit nicht für diese „Software"-Geräte eigene Whitelist-Regeln definiert werden müssen, ist diese Option zunächst grundsätzlich aktiviert. Wenn Sie diese deaktivieren, müssen für alle diese Systemgeräte eigene Regeln erstellt werden.

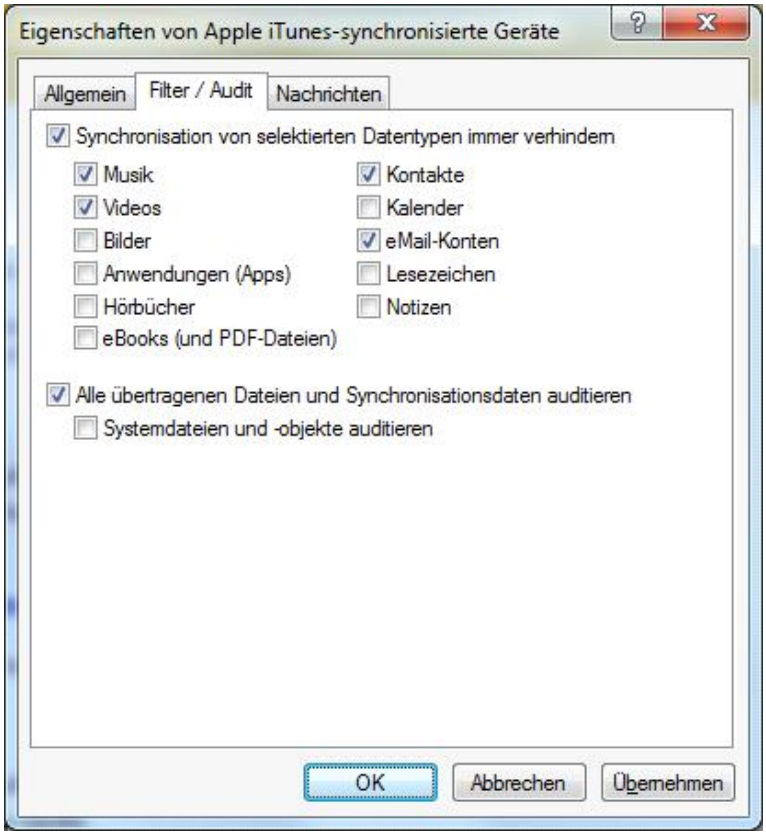
4.2.2.3 Detaillierte Kontrolle von iTunes und iTunes-synchronisierten Geräte

Normalerweise können Geräte nur freigeben oder gesperrt werden. Eine detaillierte Unterscheidung nach Zugriffsrechten gibt es dort nicht. Eine Ausnahme stellt die neue iTunes Geräteklasse dar. Damit können alle iPods und iPhones sehr genau kontrolliert und der Datentransfer nachvollzogen werden. Unabhängig von den Geräten lässt sich auch der Funktionsumfang, also die freigeschalteten Funktionen von iTunes selbst einschränken. So kann man z.B. in iTunes TV deaktivieren.

Um generell den Zugriff von Apple-Geräten zu steuern, gibt es unter Geräte – Sperr-Einstellungen – Smartphones – eine Geräteklasse Apple iTunes-synchronisierte Geräte.

Neben den reinen Zugriffsberechtigungen auf dem Reiter Allgemein, können auf dem Reiter Filter / Audit einzelne zu synchronisierende Elemente blockiert werden:

- Musik
- Videos
- Bilder
- Anwendungen (Apps)
- Hörbücher
- eBooks (und PDF-Dateien)
- Kontakte
- Kalender
- eMail-Konten
- Lesezeichen
- Notizen
- Alle übertragenen Dateien und Synchronisationsdaten auditieren : Dies kommt der Dateiprotokollierung im Dateifilter gleich, d.h. jeglicher Datenaustausch wird protokolliert.

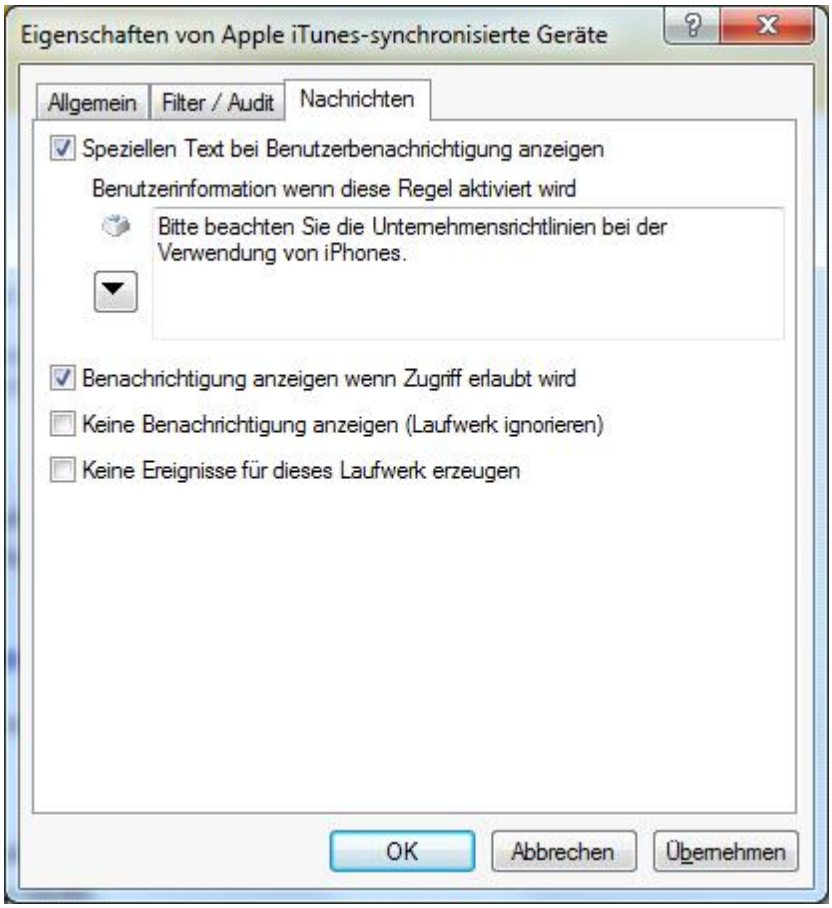


Die iTunes Software Einschränkungen kann man unter *Erweiterte Konfiguration – Geräte – Sperr-Einstellungen – Smartphones – iTunes-Softwareeinschränkungen* festlegen:

- Geräte-Synchronisierung
    - Verschlüsselte Gerätesicherung erzwingen
    - Neue Geräte nicht registrieren
    - Geräte nicht automatisch synchronisieren
- Softwareaktualisierung
    - Nicht nach iTunes-Aktualisierungen suchen
    - Nicht nach App-Aktualisierungen suchen
    - Nicht nach Geräte-Firmware suchen
- Media-Funktionen
    - Podcasts deaktivieren
    - iTunes-Store deaktivieren
    - Nicht-Jugendfreien Inhalt deaktivieren
    - Internet-Radio deaktivieren
    - iTunes-Ministore deaktivieren
    - Album-Bilder nicht herunterladen
    - Plugins deaktivieren
    - Öffnen von Streams deaktivieren

- Apple TV deaktivieren
- Diagnosefunktionen deaktivieren
- Freigaben deaktivieren
- Privatfreigabe deaktivieren
- iTunes Ping! deaktivieren
- Zugriff auf iTunesU erlauben

Wählen Sie den Reiter „**Nachrichten**“, um benutzerspezifische Anzeigen zu konfigurieren:



Um eine eigene Meldung für eine Regel zu konfigurieren, aktivieren Sie die Option „**Speziellen Text bei Benutzerbenachrichtigung anzeigen**“. Geben Sie anschließend einen Text ein, welcher unabhängig von der aktuell eingestellten Systemsprache angezeigt wird. Diese sprachunabhängige Meldung wird durch ein Tastensymbol an der linken oberen Ecke des Eingabefeldes dargestellt.

Sofern Sie mehrsprachige Benutzermeldungen definiert haben, können Sie auch eine dieser Nachrichten auswählen. Klicken Sie dazu auf den Pfeil und wählen Sie aus der Liste „**Mehrsprachige Benachrichtigung**“ aus.

Mehrsprachige Meldungen enthalten für eine Nachricht verschiedene Texte für unterschiedliche Sprachen. Bevor Sie mehrsprachige Benutzermeldungen verwenden können, müssen diese im Bereich „**Globale Einstellungen**“ der Richtlinie definiert werden. Wenn Sie eine derartige Meldung verwenden, zeigt DriveLock den Text an, welcher für die aktuelle Systemsprache des angemeldeten Benutzers konfiguriert wurde.

Wählen Sie eine Meldung aus und bestätigen diese mit **OK**.

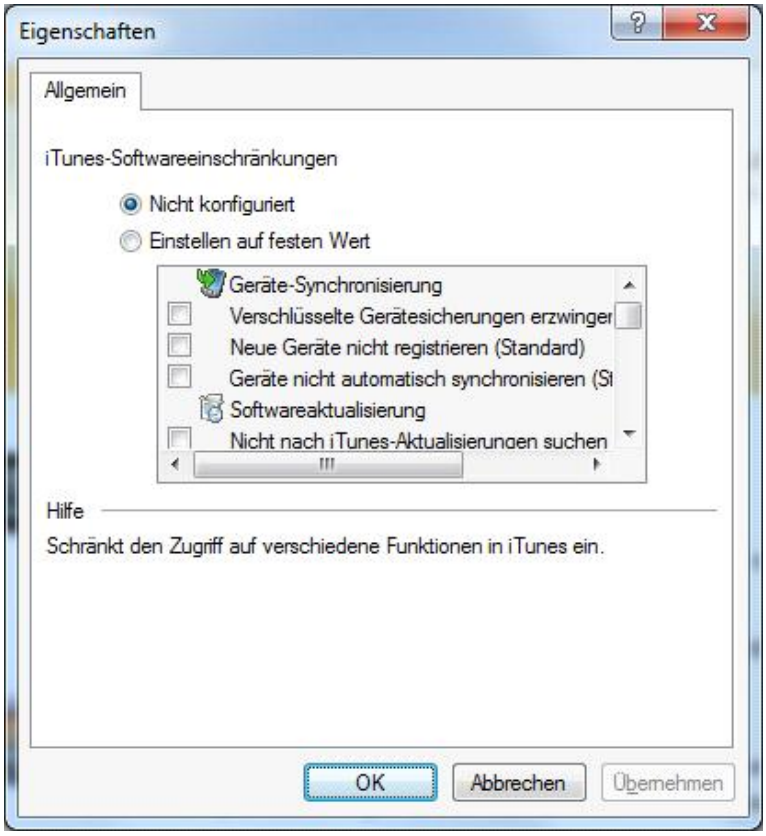
Diese sprachabhängige Meldung wird durch ein Sprechblasen-Symbol an der linken oberen Ecke des Eingabefeldes dargestellt.

Wenn Sie möchten, dass die Meldung auch dann angezeigt wird, wenn ein Zugriff durch den Benutzer möglich ist, dann aktivieren Sie die entsprechende Option. Um die Anzeige von Meldungen generell zu unterbinden (auch die Anzeige von Standard-Benachrichtigungen), aktivieren Sie „**Keine Benachrichtigung anzeigen**“.

Wenn Sie die Erzeugung von Überwachungsereignissen für diese Whitelist-Regel unterdrücken wollen, markieren Sie bitte „**Keine Ereignisse für dieses Laufwerk erzeugen**“.

Klicken Sie **OK**, um die Einstellungen zu übernehmen.

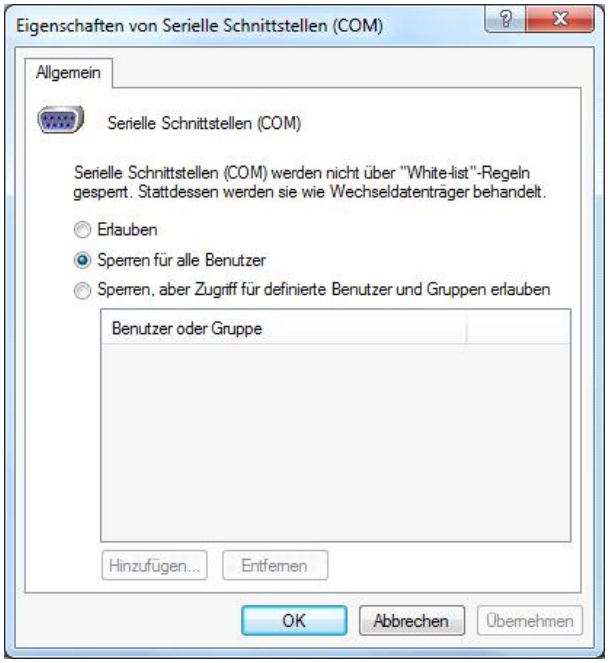
Klicken Sie **iTunes-Softwarebeschränkungen**, um festzulegen, welche Funktionen von iTunes der Benutzer verwenden kann bzw. wie iTunes auf dem Rechner konfiguriert werden soll.

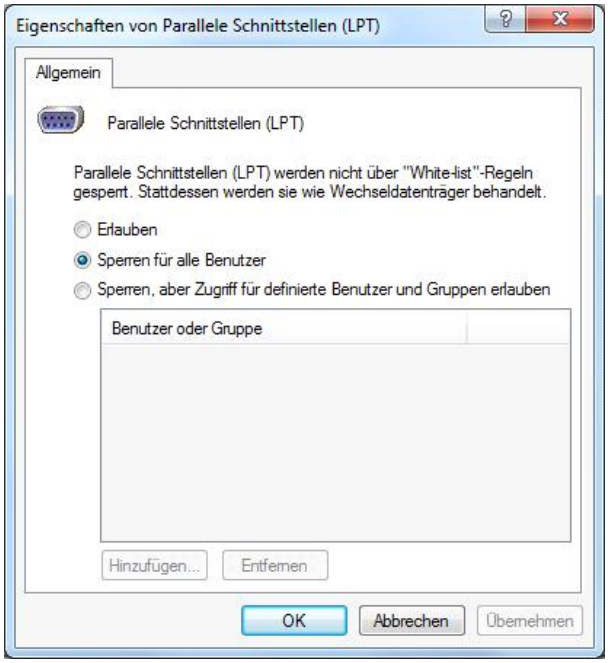


Aktivieren Sie **Einstellen auf festen Wert** und wählen Sie aus der Liste die gleichnamigen iTunes Funktionen, um das Verhalten festzulegen.Klicken Sie auf **OK**, um die Einstellungen zu übernehmen.

4.2.2.4 Konfigurieren der Schnittstellen COM und LPT

Die Konfiguration der beiden Schnittstellen COM und LPT beschränkt sich auf das Sperren bzw. Freigeben für bestimmte oder alle Benutzer. Diese werden nicht wie andere Geräte oder Schnittstellen kontrolliert, sondern stattdessen wie Wechseldatenträger behandelt.





Folgende Möglichkeiten stehen zur Auswahl:

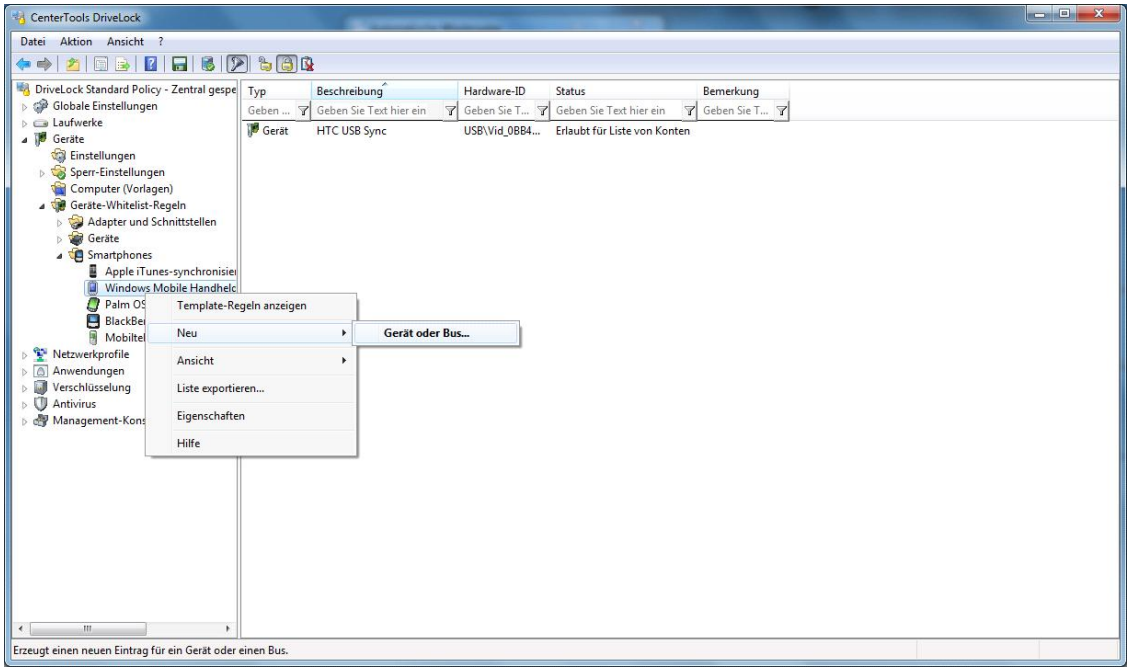
- *Erlauben*: Jeder authentisierte Benutzer kann diese Schnittstelle verwenden
- *Sperren für alle Benutzer*: Der Zugriff auf diese Schnittstelle ist für alle Benutzer gesperrt.
- *Sperren, aber Zugriff für definierte Benutzer und Gruppen erlauben*: Diese Schnittstelle ist gesperrt, aber Zugriff ist für den oder die angegebenen Benutzer bzw. Gruppen möglich.

Klicken Sie auf **Hinzufügen**, um eine weitere Gruppe oder einen Benutzer zur angezeigten Liste hinzuzufügen. Mit **Entfernen** wird der zuvor ausgewählte Eintrag gelöscht.

PalmOS Geräte oder auch Windows CE Geräte, welche über die serielle Schnittstelle mit dem Computer verbunden sind, können nur über die Option *„Serielle Schnittstellen (COM)“* gesperrt werden. Es ist nicht möglich diese Geräte über die Geräteklassen *„Windows CE Handhelds und Smartphones“* oder *„Palm OS Handhelds und Smartphones“* zu kontrollieren, da Windows an den seriellen Schnittstellen (COM) keine Hardwareerkennung ermöglicht.

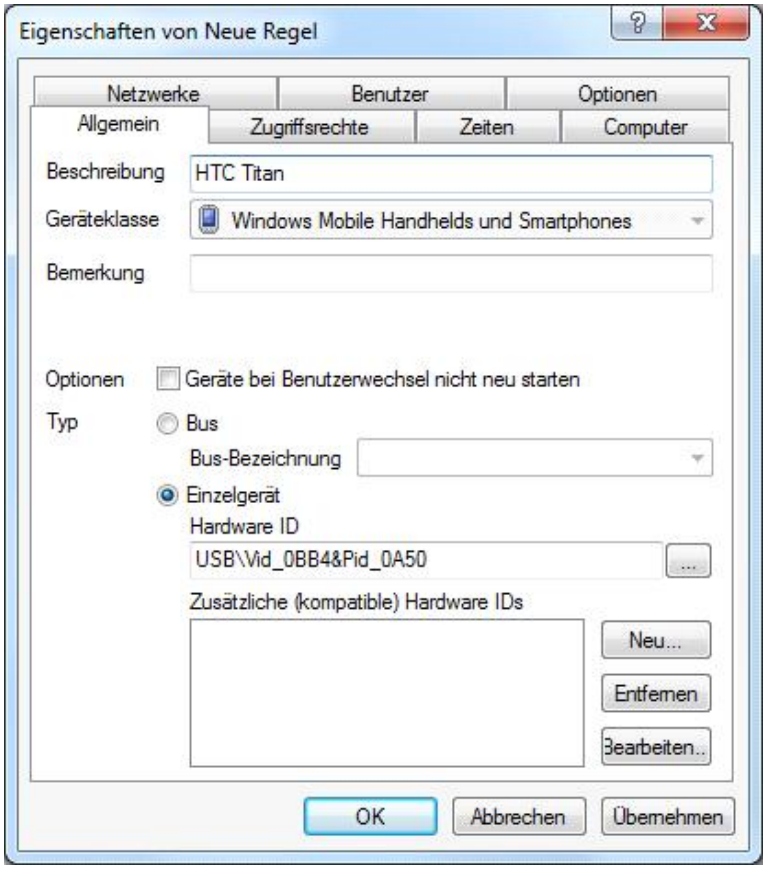
4.2.2.5 Geräteregeln definieren

Whitelist-Regeln für Geräte werden analog zu den Laufwerksregeln erstellt. Das folgende Beispiel zeigt die Erstellung einer Regel für ein Smartphone.



Dazu navigieren Sie in der DriveLock Management Konsole zu den Geräteeinstellungen (siehe Abbildung) und klicken mit der rechten Maustaste auf **Windows Mobile Handhelds und Smartphones.** Wählen Sie anschließend "**Neu -> Gerät oder Bus**" aus dem Kontextmenü.

Konfigurieren Sie Ihre Einstellungen im folgenden Eigenschaften-Fenster.



Geben Sie einen Namen für die Whitelist-Regel in das Feld „**Bezeichnung**" ein. Sie können zusätzlich noch eine Bemerkung als zusätzliche Beschreibung eingeben.

Schränken Sie den Geltungsbereich durch die Angabe zusätzlicher Informationen weiter ein. Sie können entweder einen Bus auswählen oder eine Hardware ID eingeben. Wenn Sie eine Regel für ein Gerät erstellen möchten, dass über einen bestimmten Bus verbunden wird, dann wählen Sie „**Bus**“ und den passenden Eintrag aus der Dropdown-Liste aus.

Somit wird diese Regel nur angewandt, wenn das Gerät zur gleichen Geräte-Klasse gehört (hier: **Windows Mobile Handhelds und Smartphones**) und über den konfigurierten Bus angeschlossen wird.

> Beispiel: Wenn Sie alle eingebauten PCI-Karten freigeben möchten, erstellen Sie eine neue Whitelist-Regel für alle kontrollierten Geräte-Klassen und wählen als Bus “PCI” aus. Dadurch könnten Sie nun andere Netzwerkkarten, die über andere Schnittstellen angebunden werden können (z.B. USB, PCMCIA usw.) sperren.

Wenn in der Liste der von Ihnen benötigte Bus nicht vorhanden ist, können Sie durch Eingabe des passenden Namens in das Feld diesen nachträglich spezifizieren.

Sollte es sich gegenseitig beeinflussende Whitelist-Regeln geben, wird DriveLock sie wie folgt verwenden:

- Bus gesperrt und Gerät freigegeben -> Gerät freigegeben
- Bus gesperrt und Gerät gesperrt -> Gerät gesperrt
- Bus freigegeben und Gerät gesperrt -> Gerät gesperrt
- Bus freigegeben und Gerät freigegeben -> Gerät freigegeben

Eingerichtete Computervorlagen haben bezüglich der manuell erzeugten Whitelist-Regeln keine spezielle Priorisierung.

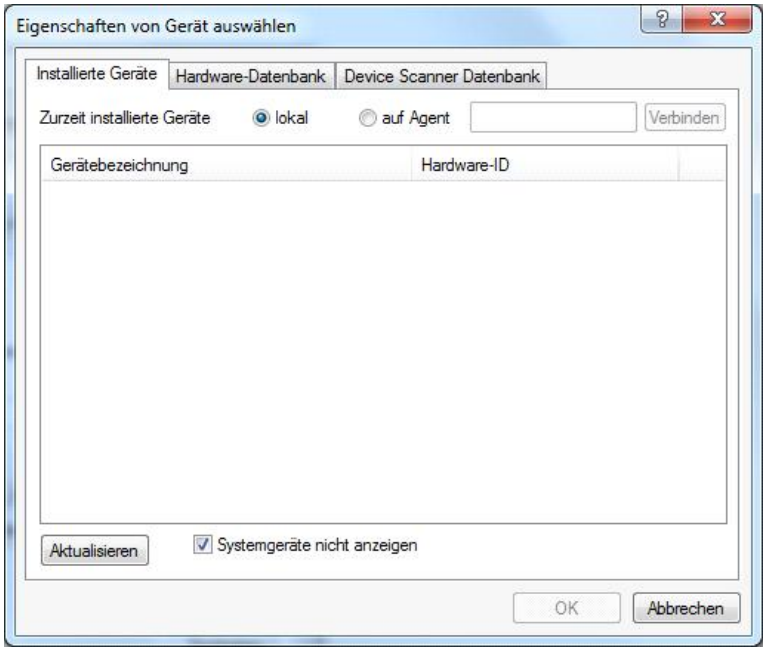
Wenn ein Gerät oder Bus in einer Regel zugelassen, in einer anderen jedoch gesperrt ist, wird das Gerät bzw. der Bus freigegeben.

Um Geräte noch genauer voneinander zu unterscheiden, werden Hardware IDs und deren sogenannte Compatible IDs verwendet. Jedes Gerät besitzt eine einzigartige Hardware ID. Zusätzlich pflegt Windows eine Liste mit dazu kompatiblen Geräten (Compatible ID). Die Hardware ID oder die Compatible ID wird dazu verwendet, um den passenden Treiber zu finden. Zusätzlich können die Hardware IDs auch noch eine Revisionsnummer, die durch den Hersteller vergeben wird, enthalten (die jedoch für die Wahl des Treibers irrelevant ist). In diesem Fall wird von Windows eine der Compatible IDs verwendet, die nicht diese Revisionsnummer enthält.

Geben Sie die korrekte Hardware ID in das entsprechende Feld ein, um das gewünschte Gerät anzugeben. Die Hardware ID kann entweder aus der Ereignisanzeige oder der Registrierungsdatenbank ausgelesen werden.

Stellen Sie sicher, dass keine Leerzeichen vor oder nach der Hardware ID eingegeben wurden.

Ein weitaus bequemerer Weg, um die Hardware ID zu ermitteln, besteht darin, die mitgelieferte Hardware-Datenbank zu verwenden, indem Sie auf den Button „...“ neben dem Hardware ID Feld klicken.



Nun können Sie im Augenblick vorhandene Geräte auswählen, oder sich zu einem anderen Agenten auf einem entfernten Rechner verbinden, um die dort verfügbaren Geräte zu ermitteln.

Klicken Sie **Aktualisieren**, um kürzlich neu hinzugekommene Geräte anzeigen zu lassen. Palm oder Windows CE basierte Handhelds sind üblicherweise solange verbunden, so lange ActiveSync oder HotSync läuft.

Die Option „**Systemgeräte nicht anzeigen**“ verbirgt alle Windows Systemgeräte, die in der Grundeinstellung über die Funktion „**Systemgeräte dieses Typs nicht sperren**“ in den Sperreinstellungen für die Geräte-Klassen freigegeben sind.

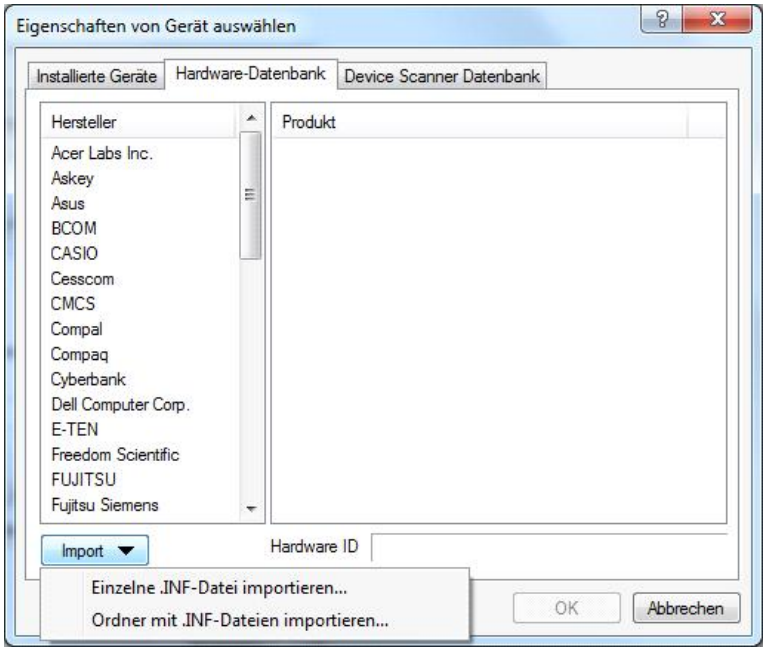
Weitere Geräte können ausgewählt werden, in dem Sie sich auf einen anderen Agent per Remote-Verbindung verbinden und ein dort vorhandenes Gerät auswählen. Wählen Sie dazu „**auf**“ aus und geben Sie den Namen des Computers ein, mit dem Sie sich verbinden möchten. Dazu muss auf dem Zielcomputer der DriveLock Agent installiert sein.

> Beachten Sie dabei, dass auf diesem Wege auch die Hardware-ID ausgelesen und mit in die Whitelist-Regel übernommen wird. Das kann bei der Verwendung aus einer virtuellen Umgebungen heraus (z.B. VMWare) dazu führen, dass diese Regel nicht beachtet wird, da in diesen virtuellen Umgebungen Geräte emuliert werden und die Hardware-ID nicht vorhanden oder unterschiedlich ist.

Weiterhin können Sie den Tab **Hardware-Datenbank** oder die **Device Scanner Datenbank** verwenden, um ein Gerät aus der dann angezeigten Liste zu wählen.

Die Hardwaredatenbank enthält viele Daten über die Geräte, für die im Betriebssystem Windows XP durch Microsoft bereits Treiber mitgeliefert werden. DriveLock verwendet diese Informationen, um Ihnen die Arbeit mit Geräten und die Erstellung von Whitelist-Regeln zu vereinfachen. Da DriveLock jedoch nicht beeinflussen kann, welche Hardware durch Microsoft unterstützt wird, erhebt die Datenbank keinen Anspruch auf Vollständigkeit, kann jedoch durch Sie leicht erweitert werden.

Um neue Geräte au seiner vorhandenen INF-Datei zu importieren, klicken Sie auf **Import**.



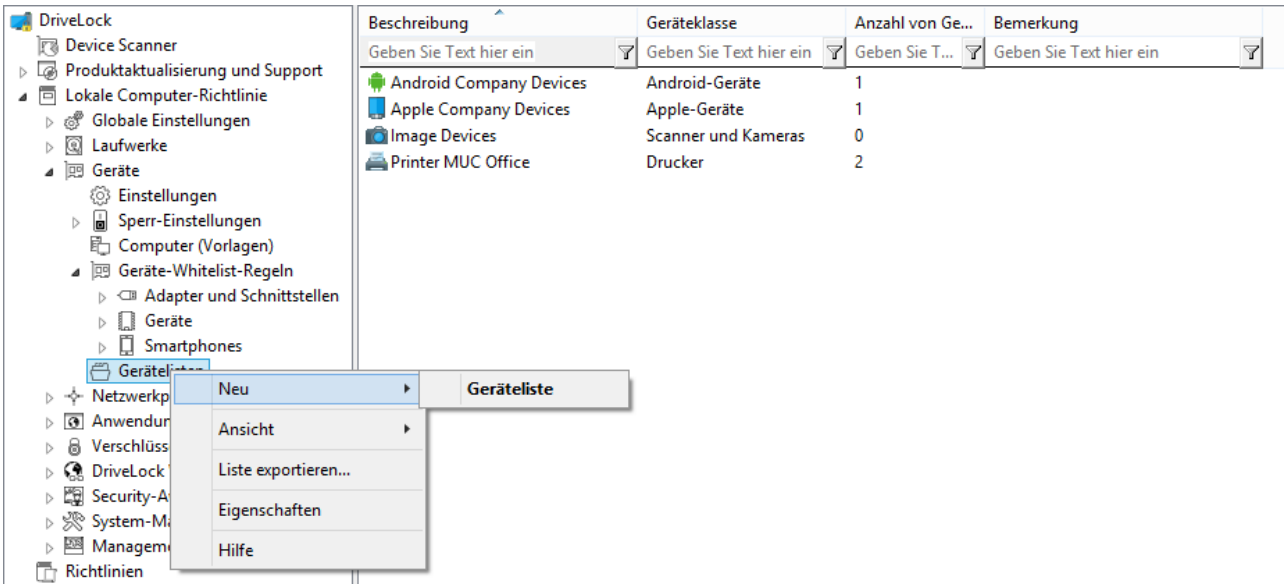
Wählen Sie aus, ob Daten aus einer einzelnen Datei oder mehreren INF-Dateien eines bestimmten Verzeichnisses eingelesen werden sollen. Wählen Sie anschließend entweder die Datei oder das Verzeichnis aus.

4.2.2.6 Gerätelisten verwenden

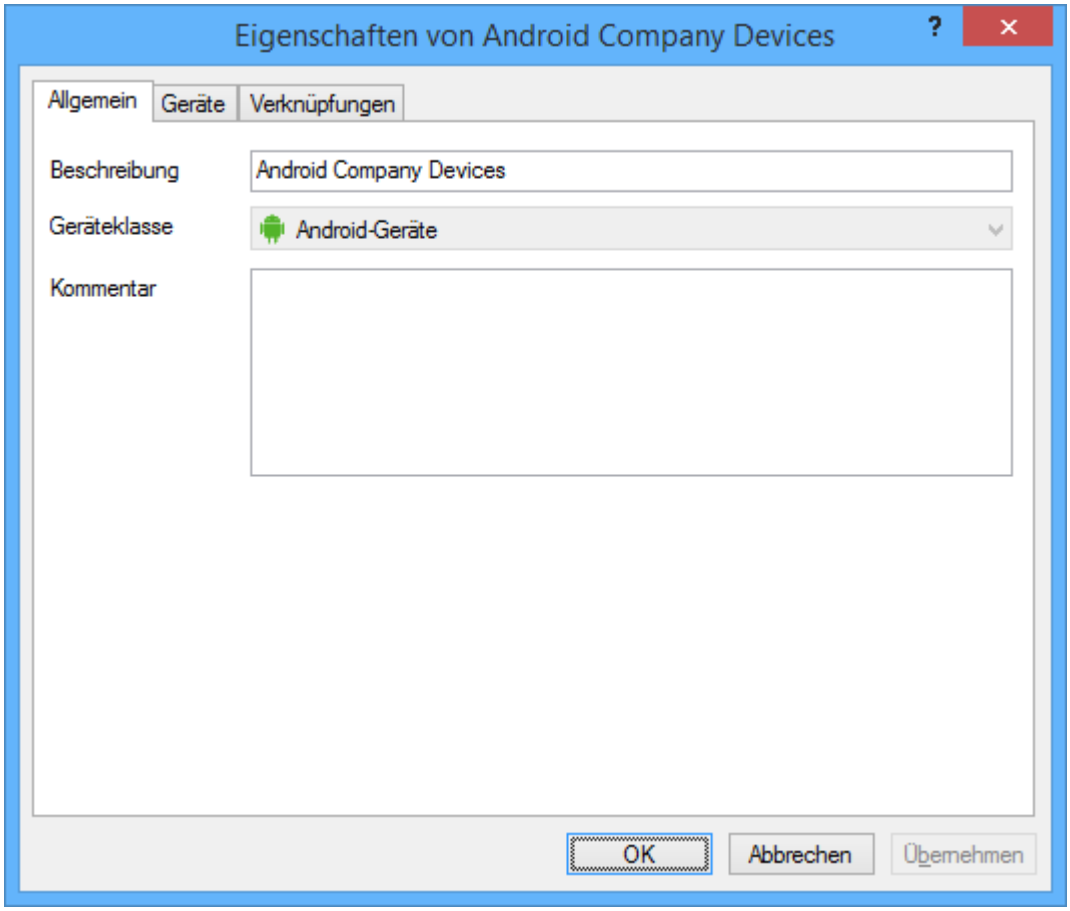
Gerätelisten vereinfachen die Verwaltung von Geräten des gleichen Typs, wenn dafür gleiche Einstellungen gelten sollen und reduzieren dabei die Anzahl der benötigten Whitelistregeln. Gerätelisten können mehrere gleichartige Geräte enthalten und für die Konfiguration von Whitelistregeln verwendet werden - analog zur Verwendung von einzelnen Geräten anhand deren Hardware ID.

Gleichzeitig wird dabei die Verwaltung der Listen selbst von der Konfiguration der Sicherheits- und Sperreinstellungen für Geräte getrennt.

Erstellen einer Geräteliste



Um eine neue Liste zu erstellen, klicken Sie mit der rechten Maustaste auf Gerätelisten. Wählen Sie anschließend "**Neu -> Geräteliste**" aus dem Kontextmenü.

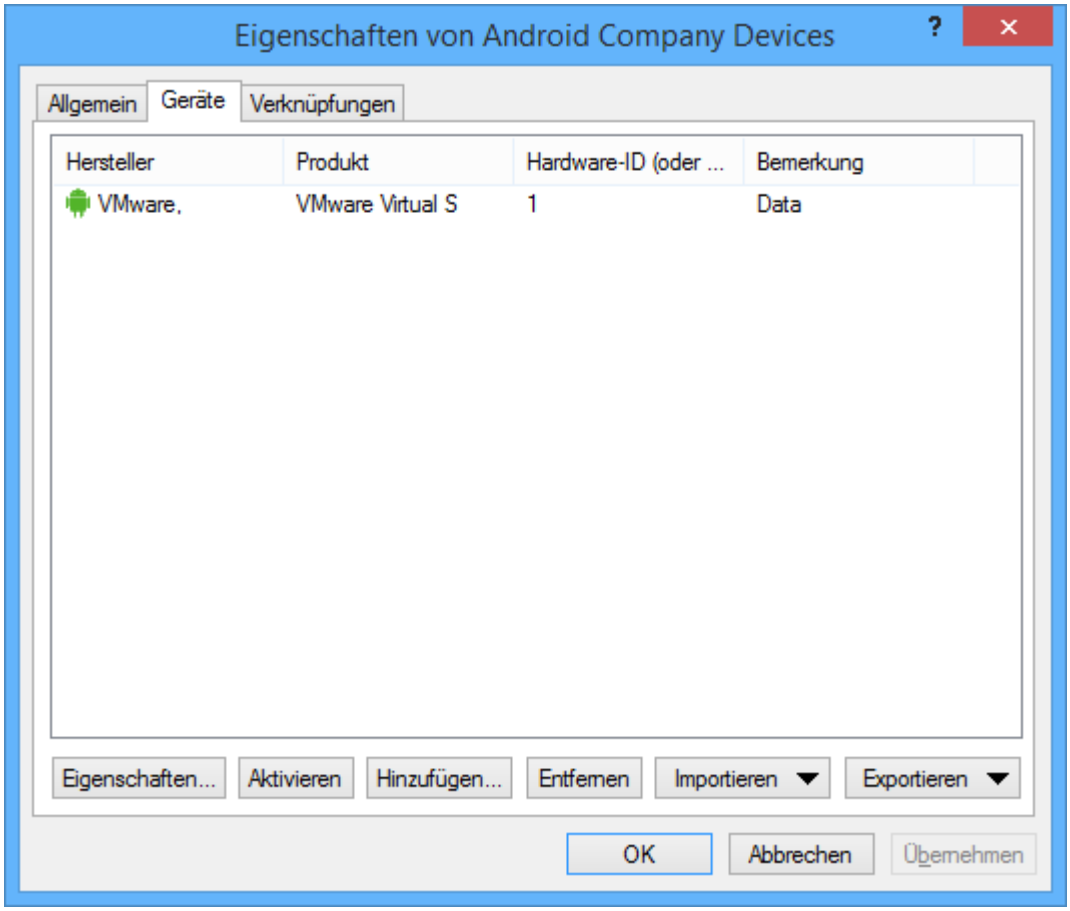


Sie können der Liste eine aussagekräftige Beschreibung geben und zusätzlich einen Kommentar hinterlegen.

Bei der Erstellung einer neuen Liste wählen Sie außerdem die Geräteklasse aus der Liste der verfügbaren Klassen aus. Diese Geräteklasse bestimmt, welche Typen von Geräten Sie in die Liste aufnehmen können und kann nach dem ersten Speichern nicht mehr geändert werden.

> Die Auswahl der Geräteklasse bestimmt später, bei welcher Klasse diese Liste zur Konfiguration verwendet werden kann und welche technischen Optionen Ihnen damit zur Kontrolle dieser Geräte zur Verfügung stehen.

Klicken Sie den Reiter **Geräte** an, um die in dieser Liste enthaltenen Geräte zu verwalten.



Hier können Sie bestehende Einträge anzeigen, deaktivieren, bearbeiten und löschen. Ebenso lassen sich neue Einträge hinzufügen.

Wenn Sie neue Einträge hinzufügen möchten, klicken Sie auf **Hinzufügen** und wählen ggf. aus, ob sie ein Gerät aufgrund seiner Produkt- bzw. Hersteller-ID oder mithilfe der Hardware-ID hinzufügen möchten (nur bei Geräten, die über diese Informationen verfügen - ansonsten wird nur die Hardware ID abgefragt). Geben Sie im anschließenden Dialog die entsprechenden Informationen ein bzw. wählen Sie diese in gewohnter Weise über die Schaltfläche "..." aus den aktuell angeschlossenen Geräten oder der Device Scanner Datenbank aus.

> Möchten Sie vorhandene Geräte nicht komplett löschen, sondern nur für eine bestimmte Zeit aus der Liste entfernen, wählen Sie das gewünschte Gerät aus und klicken anschließend auf **Deaktivieren**. Ein kleinen zusätzliches Symbol zeigt nun an, das der Eintrag in der Liste derzeit nicht aktiviert ist und für Freigaben berücksichtigt wird. Deaktivierte Listenelement können ebenso wieder aktiviert werden.

Über die Schaltfläche **Import** können Sie mehrere Geräte importieren, die entweder in Form einer CSV- oder einen INI-Datei vorliegen. Eine CSV-Datei könnte beispielsweise so aussehen:

HardwareID	Comment	Vendor	Product	SerialNumber	Enabled	ClassId
MF\BRMFC860LPT_PRT0,Brother_MFC-860	Brother MFC-8600				1	{4D36E979-E325-11CE-BFC1-08002BE10318}
Xerox4520CCAD,Xerox_4520_PS	Xerox 4520 PSS				1	{4D36E979-E325-11CE-BFC1-08002BE10318}

Klicken Sie auf **Export**, um die aktuelle Liste in Form einer CSV- oder INI-Datei speichern.

> Tipp: Wenn Sie zuvor einige Einträge einzeln erstellt und diese dann als Datei exportiert haben, können Sie diese Datei als Grundlage für einen Import verwenden, da diese bereits den richtigen Aufbau bzw. die notwendigen Spalten besitzt.

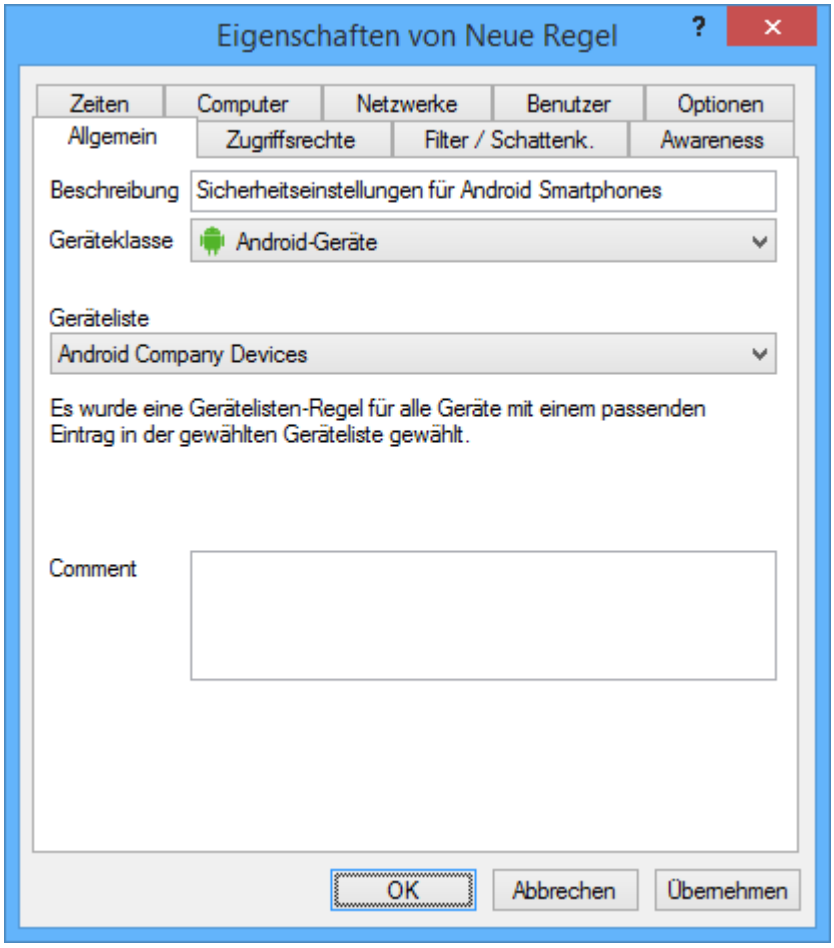
Der Reiter **Verknüpfungen** zeigt Ihnen, in welchen Gerätelisten-Regeln diese Liste bereits verwendet wird.

Solange eine Geräteliste in einer Regel verwendet wird, kann die Liste nicht gelöscht werden.

Klicken Sie **OK**, um die Liste bzw. Ihre Änderungen zu speichern und zur Listenansicht zurückzukehren.

Eine Geräteliste zur Konfiguration verwenden

Die Geräteliste einer bestimmten Geräteklasse kann nun zur Konfiguration von Einstellungen für diese Klasse verwendet werden. Dazu navigieren Sie in der DriveLock Management Konsole zu den Geräteeinstellungen (zum Beispiel **Geräte-Whitelist-Regeln -> Smartphones -> Android-Geräte**) und klicken mit der rechten Maustaste auf **Android-Geräte.** Wählen Sie anschließend "**Neu -> Gerätelisten-Regel**" aus dem Kontextmenü.



Nun können Sie eine Beschreibung und einen Kommentar hinzufügen. Wählen Sie aus der Geräteliste die gewünschte zuvor erstellte Liste aus.

Es werden nur die Listen angezeigt, die die gleiche Geräteklasse besitzen.

Über die weiteren Reiter können Sie nun analog zur Geräte-Regel die Sicherheitseinstellungen für die DriveLock Richtlinie vornehmen.

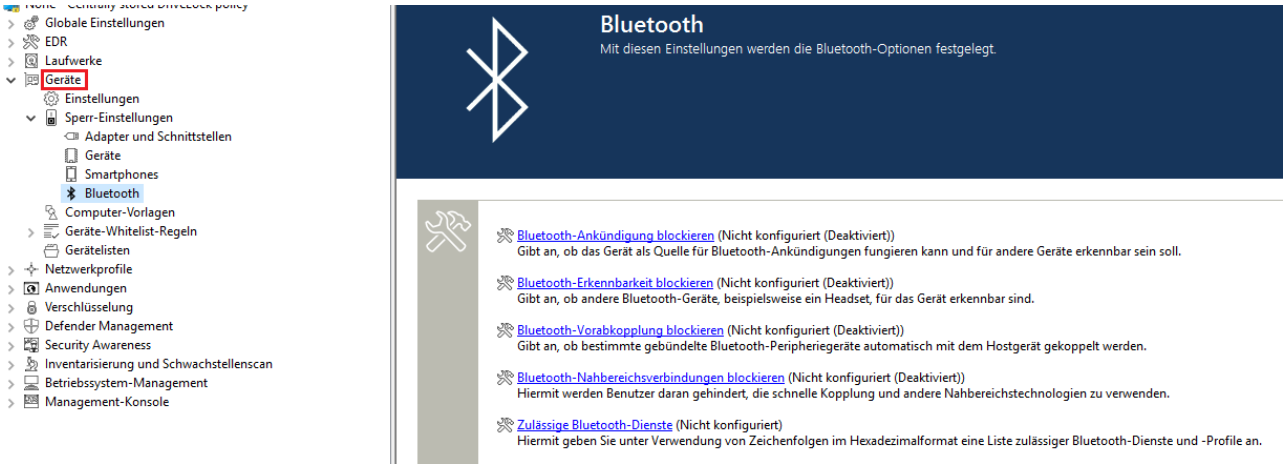
Wenn Sie die Einstellungen speichern möchten, klicken Sie **Übernehmen**. Wenn Sie **OK** klicken, werden die Änderungen ebenfalls gespeichert, zusätzlich wird das Eigenschaftenfenster geschlossen.

4.2.3 Bluetooth-Geräte

Mit den Einstellungen für die Verbindung von Geräten über Bluetooth können Sie ab DriveLock Version 2021.1 beispielsweise Kopplungen mit neuen Geräten unterbinden oder Einschränkungen auf gewünschte Bluetooth-Dienste konfigurieren.

Konkreter Anwendungsfall: Sie wollen die Verwendung von einigen Bluetooth-Geräten (z. B. Maus, Tastatur oder Microsoft Surface Pen) steuern. Die Verwendung dieser Geräte soll erlaubt, aber alle anderen Bluetooth-Geräte (inklusive deren Funktionen wie z. B. Dateitransfer) sollen gesperrt werden.

Öffnen Sie in der DriveLock Management Konsole den Knoten **Geräte** und wählen Sie in den **Sperr-Einstellungen** den Unterknoten **Bluetooth** aus.



Folgende Einstellungen stehen Ihnen hier zur Verfügung. Standardmäßig sind sie deaktiviert.

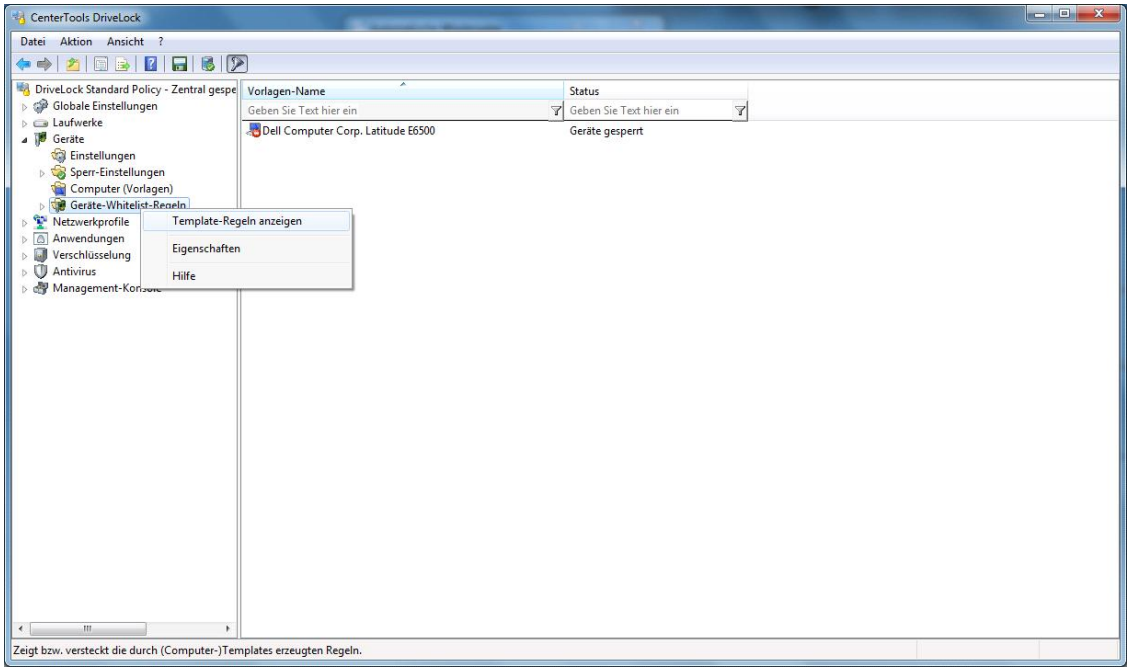
- **Bluetooth-Ankündigung blockieren**
  Wählen Sie diese Option, wenn das Gerät als Quelle für Bluetooth-Ankündigungen dienen und für andere Geräte erkennbar sein soll.
- **Bluetooth-Erkennbarkeit blockieren**
  Legen Sie mit dieser Einstellung fest, ob das Gerät für andere Bluetooth-Geräte, z.B. ein Headset, erkennbar sein soll.
- **Bluetooth-Vorabkopplung blockieren**
  Wählen Sie diese Option, wenn bestimmte gebündelte Bluetooth-Peripheriegeräte automatisch mit dem Hostgerät gekoppelt werden sollen.
- **Bluetooth-Nahbereichsverbindungen blockieren**
  Mit dieser Option werden Benutzer daran gehindert, die schnelle Kopplung und andere Nahbereichstechnologien zu verwenden.
- **Zulässige Bluetooth-Dienste**
  Mit dieser Einstellung können Sie zulässige Bluetooth-Dienste und -Profile auf eine Liste setzen (unter Verwendung von Zeichenfolgen im Hexadezimalformat).

4.2.4 Computervorlagen verwenden

Computervorlagen dienen dazu, Geräte-Freigaben (bzw. Sperrungen) für bestimmte Computer-Typen mit gleicher eingebauter Hardware zu erstellen. Diese Geräte, die dann innerhalb der Vorlage definiert wurden, werden von DriveLock automatisch freigegeben, die Erstellung von zusätzlichen Geräte-Regeln ist dann nicht mehr notwendig.

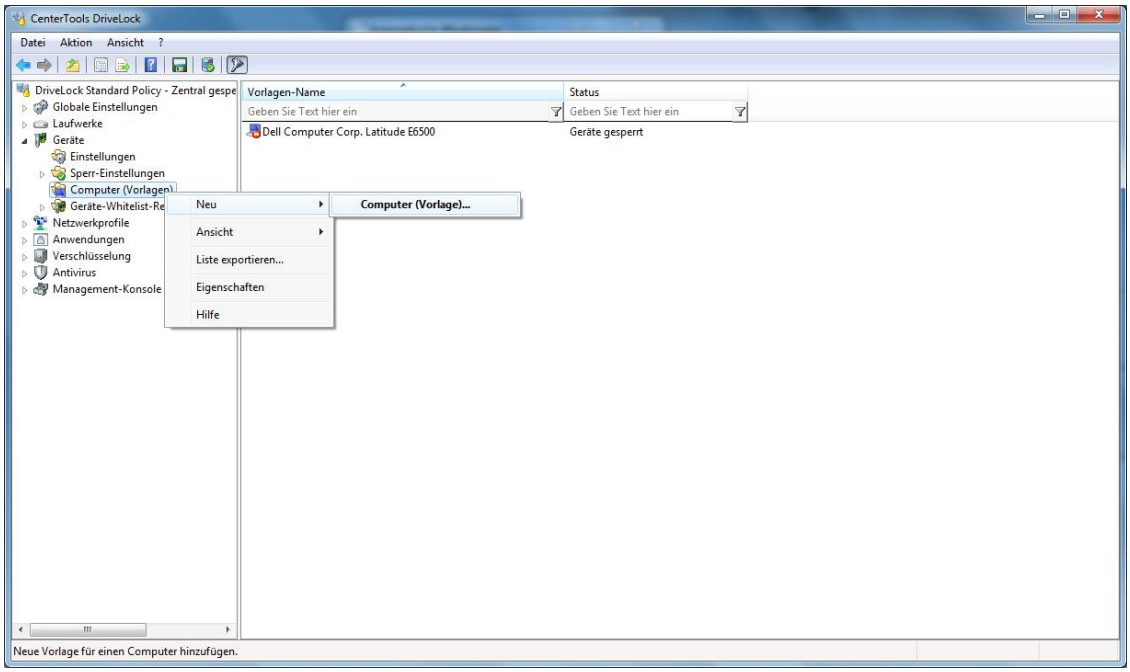
Während Sie eine Computervorlage erstellen, haben Sie Zugriff auf die Hardwaredatenbank, welche bereits für einige gebräuchliche Rechnerkonfigurationen Daten zu Geräten enthält.

Alternativ können Vorlagen auch anhand von Geräte-Klassen erstellt werden. Dabei ist es möglich, z.B. einen Scanner-Pool anzulegen und dort den Zugriff zu erlauben bzw. diese zu sperren

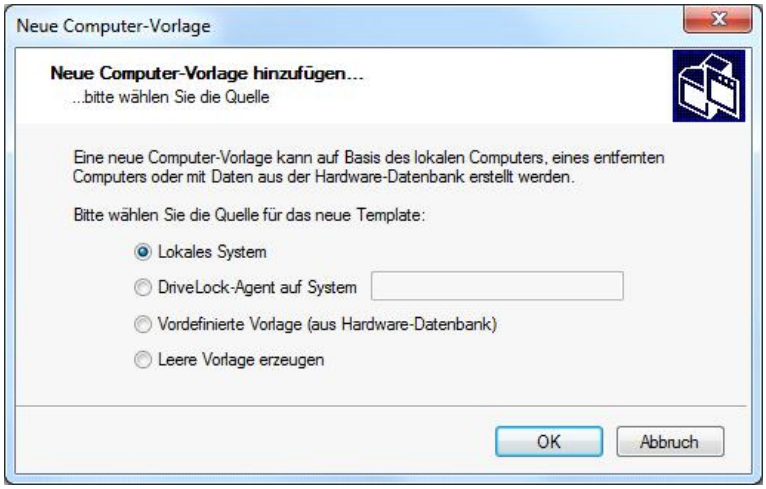


Rechtklicken Sie **Geräte Whitelist-Regeln** und aktivieren Sie die Option **Template-Regeln anzeigen**, um all die Geräte anzuzeigen, die innerhalb einer Vorlage anstatt über eine Whitelist-Regel definiert worden sind. Sie können anhand des Icons zwischen den beiden Typen unterscheiden.

4.2.4.1 Computervorlage erstellen

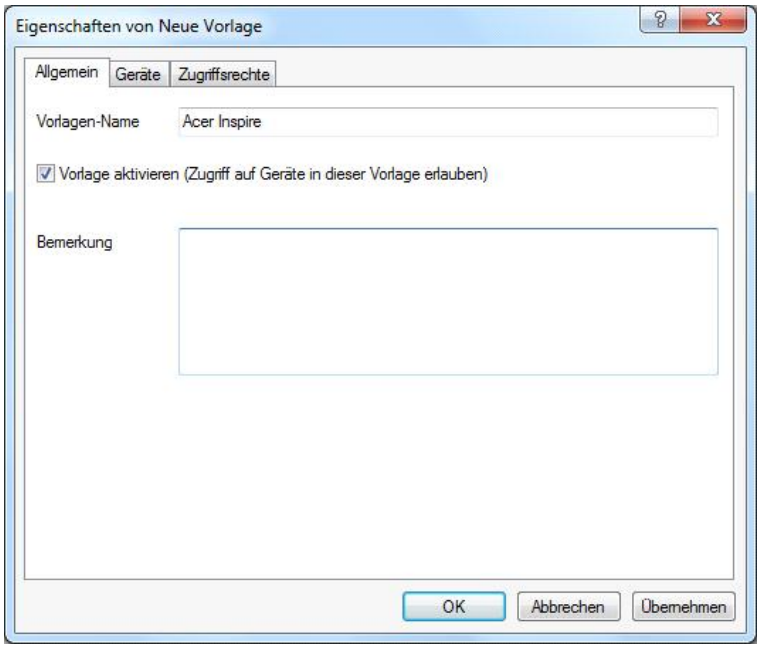


Um eine neue Computervorlage zu erstellen, rechtsklicken Sie auf **Computer (Vorlagen)** und wählen **Neu -> Computer (Vorlage)**.



4.2.4.1.1 Erstellen einer Computervorlage anhand des aktuellen Systems

Wählen Sie die Option **Lokales System** als Quelle und klicken Sie **OK**.



Geben Sie einen Namen für die Vorlage ein (z.B. den Produktnamen).

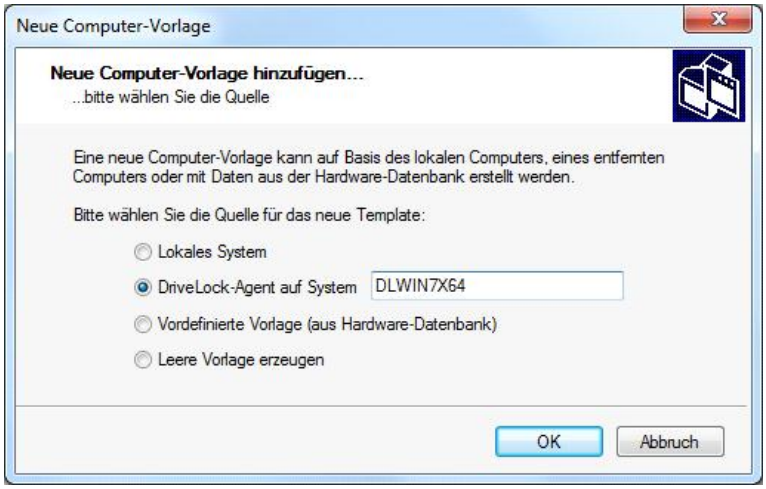
Aktivieren Sie den Reiter „**Geräte**". Anschließend beginnt DriveLock den aktuellen Computer nach Hardware zu durchsuchen und trägt anschließend alle gefundenen Geräte in die Liste ein.

Springen Sie nun zum Kapitel „Computervorlagen verwenden", wenn Sie weitere Geräte hinzufügen und die Berechtigungen konfigurieren möchten.

4.2.4.1.2 Erstellen einer Computervorlage von einem anderen Rechner

Das Erstellen einer Vorlage, die auf der Konfiguration eines entfernten Rechners basiert, funktioniert auf die gleiche Weise, als wenn Sie eine Vorlage des aktuellen Systems erstellen würden.

Wählen Sie die Option "**DriveLock Agent auf System**" und geben den Namen des gewünschten Computers ein. Klicken Sie anschließend auf **OK**.



Der DriveLock Agent muss dazu auf diesem Computer installiert und gestartet worden sein.

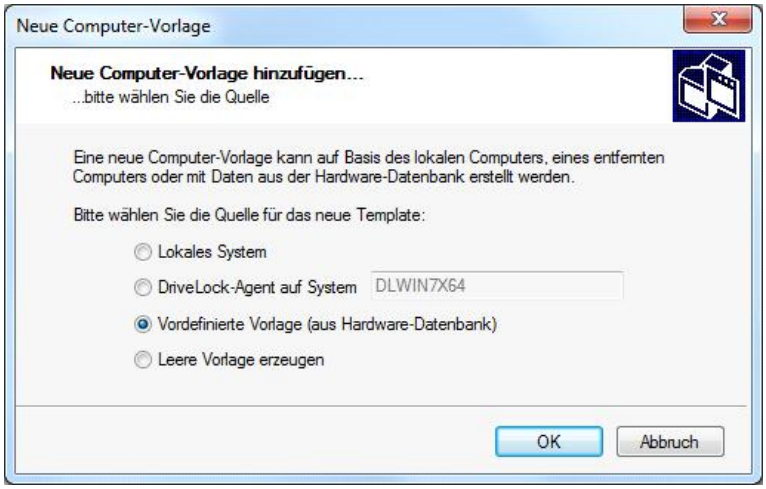
Um eine Verbindung zwischen zum entfernten Rechner unter Windows XP SP2 herzustellen, muss dort in den Einstellungen der Firewall (falls vorhanden) die TCP Ports 6064 und 6065 (Voreinstellung) und das Programm "DriveLock" für eingehende Verbindungen zugelassen werden.

Aktivieren Sie den Reiter „**Geräte**". Anschließend beginnt DriveLock den aktuellen Computer nach Hardware zu durchsuchen und trägt anschließend alle gefundenen Geräte in die Liste ein.

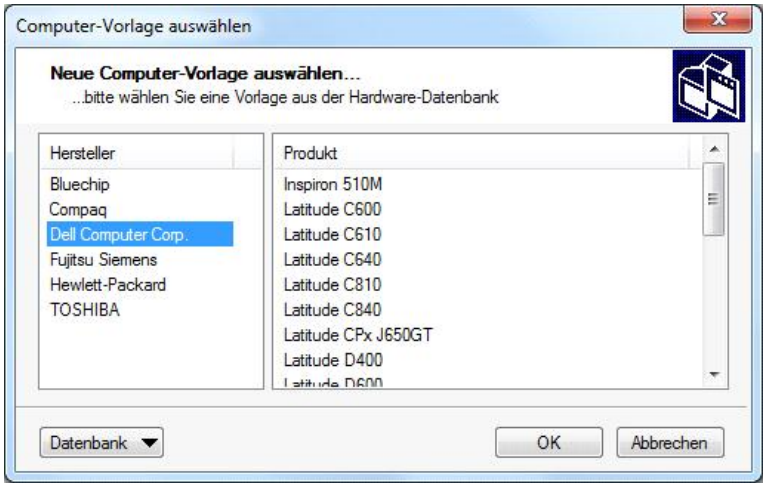
Springen Sie nun zum Kapitel „Computervorlagen verwenden", wenn Sie weitere Geräte hinzufügen und die Berechtigungen konfigurieren möchten.

4.2.4.1.3 Verwenden einer vordefinierten Vorlage aus der Hardware-Datenbank

Hierbei besteht die Möglichkeit, auf die Hardware-Datenbank zuzugreifen und aus dieser Geräte für den Import in die neue Vorlage auszuwählen.



Aktivieren Sie "**Vordefinierte Vorlage (aus Hardware-Datenbank)**" und klicken **OK**, um die Datenbank zu öffnen.



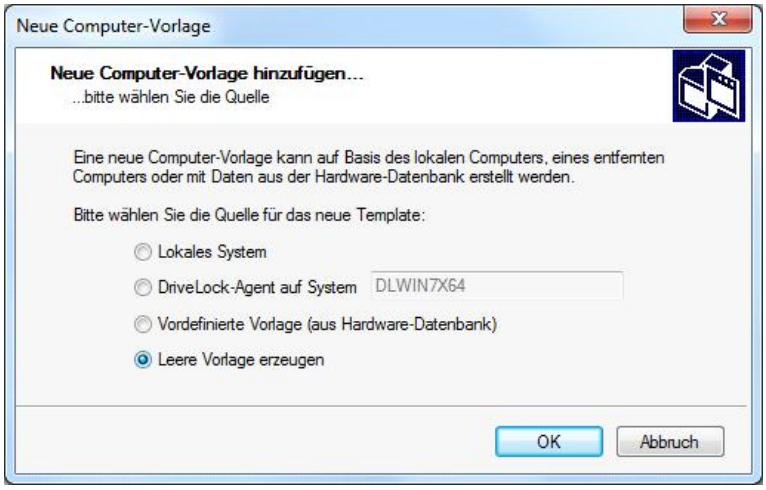
Wählen Sie die gewünschte Vorlage aus und klicken Sie **OK**.

Anschließend werden die Daten über die in der Vorlage enthaltenen Geräte aus der Datenbank gelesen und automatisch zur Liste hinzugefügt.

Springen Sie nun zum Kapitel „Computervorlagen verwenden“, wenn Sie weitere Geräte hinzufügen und die Berechtigungen konfigurieren möchten.

4.2.4.1.4 Erzeugen einer leeren Vorlage

Aktivieren Sie “**Leere Vorlage erzeugen**” und klicken Sie **OK**, um eine Vorlage ohne Geräteinformationen zu erstellen.

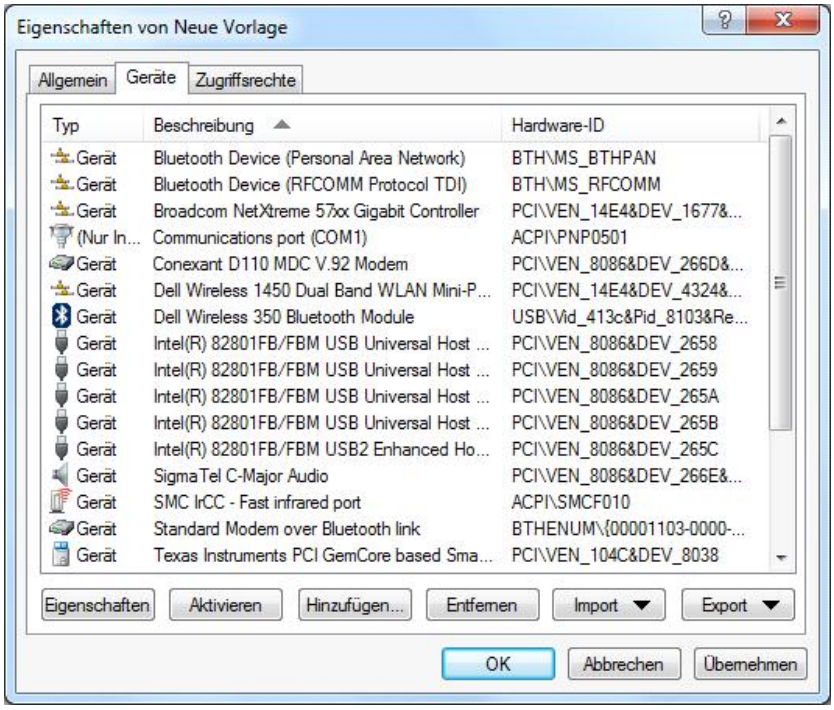


Wenn Sie den Reiter “**Geräte**” auswählen, wird kein Gerät aufgelistet.

4.2.4.2 Computervorlagen verwenden

Sofern Sie keine leere Vorlage erzeugt haben, hat DriveLock bereits automatisch eine Liste mit Geräten für Ihre Vorlage erzeugt, entweder aufgrund der Daten aus dem lokalen System, von einem weiteren Rechner oder aus der Hardware-Datenbank.

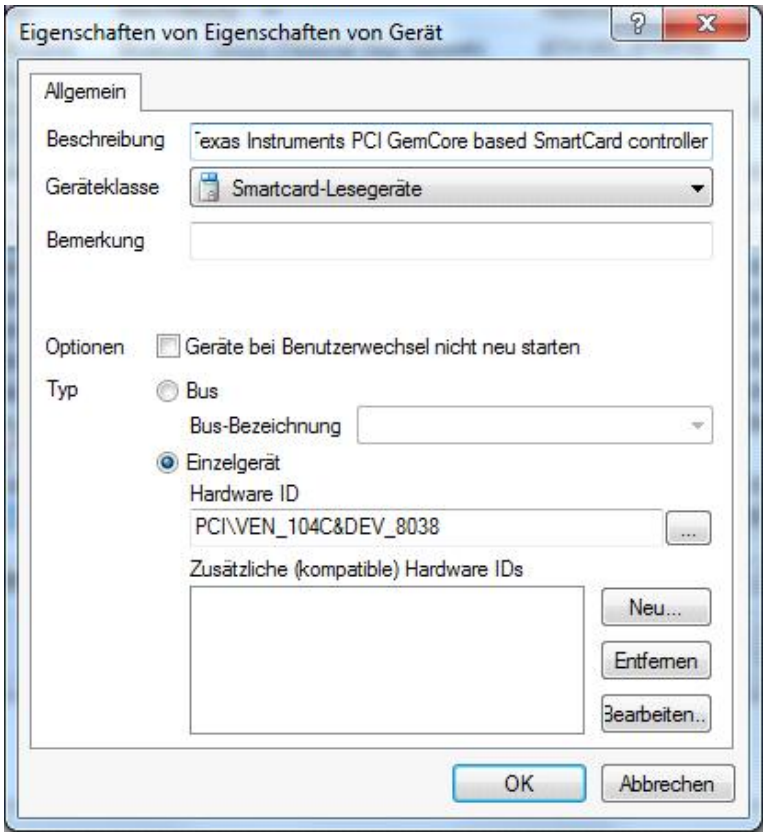
Sie können nun diese Liste verwenden, um weitere hinzuzufügen, oder bestehende Geräte zu bearbeiten oder zu löschen.



Falls als Typ "*Nur Info*" angezeigt wird, bedeutet diese, dass DriveLock dieses Gerät zwar erkennt, aber in der aktuellen Version nicht sperren kann.

4.2.4.2.1 Bearbeiten der Geräteliste in der Computervorlage

Wählen Sie ein Gerät aus der Liste und klicken **Eigenschaften**, um dessen Bezeichnung, Geräte-Klasse oder –Typ (Bus oder Einzelgerät) zu ändern.



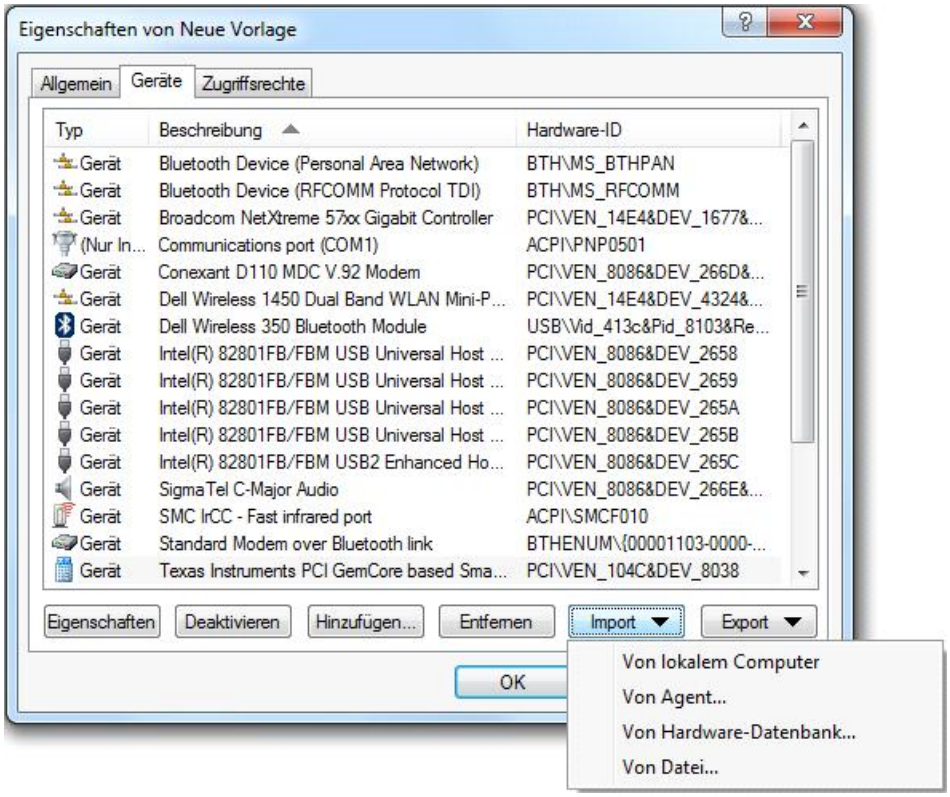
Der Abschnitt „Geräteregeln definieren" enthält Informationen darüber, wie Geräte ohne Vorlagen konfiguriert werden können.

Klicken Sie auf **Deaktivieren**, um ein vorher markiertes Element aus der Liste zu deaktivieren, ohne es aus der Liste zu löschen. Somit wird es dennoch gesperrt, wenn Sie die Vorlage für die Freigabe verwenden.

Klicken Sie auf **Hinzufügen** oder **Entfernen**, um die Liste zu erweitern oder zu verkürzen. Ein Gerät zur Liste hinzuzufügen funktioniert auf die gleiche Weise, wie ein Gerät zur Whitelist-Regel hinzugefügt wird (siehe Abschnitt „Geräteregeln definieren").

4.2.4.2.2 Neue Geräte in die Computervorlage importieren

Klicken Sie auf **Import** und wählen Sie zwischen den unterschiedlichen Quellen aus, um Geräteinformationen in die bestehende Computervorlage einzufügen.



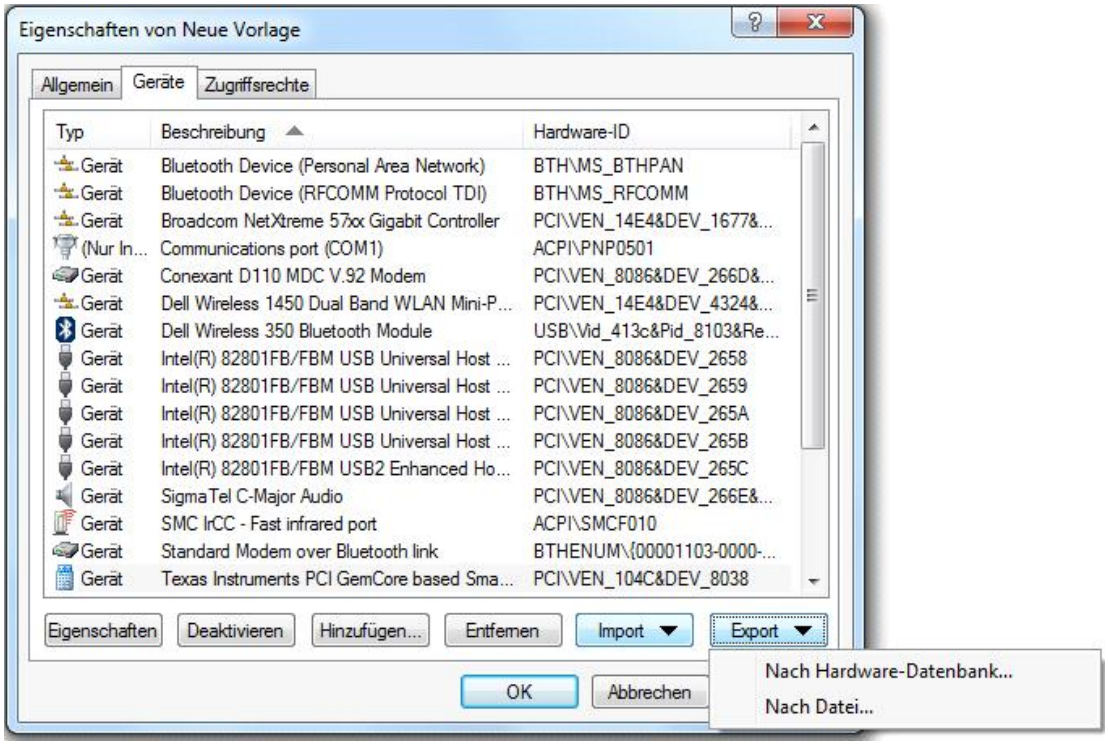
Der Import von einem lokalen Computer, einem anderen Rechner oder aus der Hardware-Datenbank erfolgt auf die gleiche Art und Weise wie während der Erstellung einer neuen Computervorlage.

Klicken Sie **Aus Datei** und wählen eine vorhandene INF-Datei aus, um deren Informationen in die Liste zu importieren.

4.2.4.2.3 Geräte aus einer Computervorlage exportieren

Klicken Sie auf **Export**, um die Geräteliste entweder in eine einzelne INF-Datei oder in die Hardware-Datenbank zu exportieren.

Stellen Sie bitte sicher, dass Sie einen Namen für die aktuelle Vorlage vergeben haben, bevor Sie Daten in die Hardware-Datenbank exportieren.



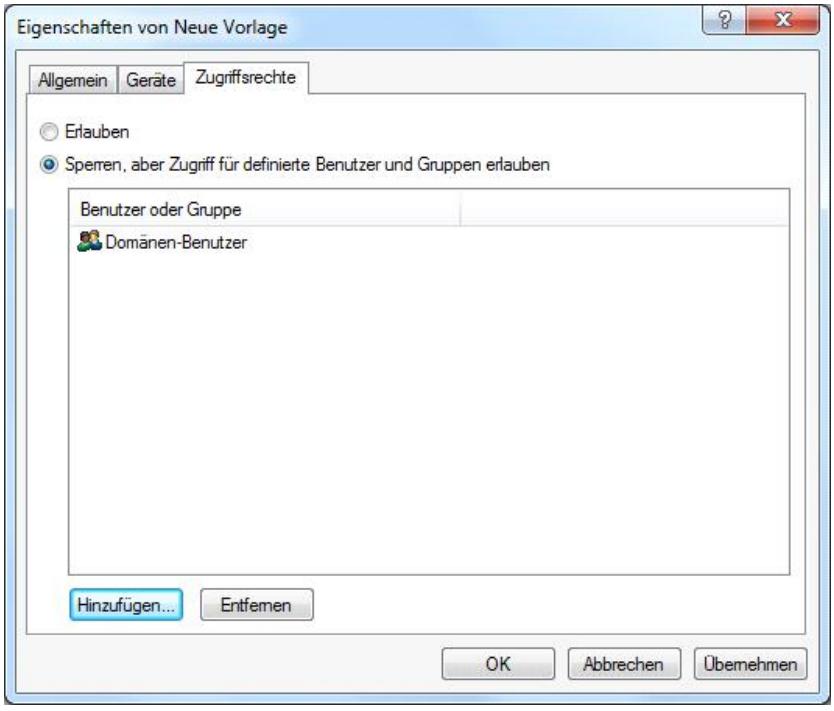
Klicken Sie auf **Nach Hardware-Datenbank** und wählen einen Hersteller aus der Liste, um die Geräteinformationen in die Datenbank zu exportieren. Die Daten werden immer zu einem Hersteller zugeordnet gespeichert.

Um fortzufahren, klicken Sie auf **OK**.

Klicken Sie auf **Nach Datei** und wählen Sie einen Dateinamen aus, um die aktuelle Geräteliste in eine INF-Datei zu exportieren.

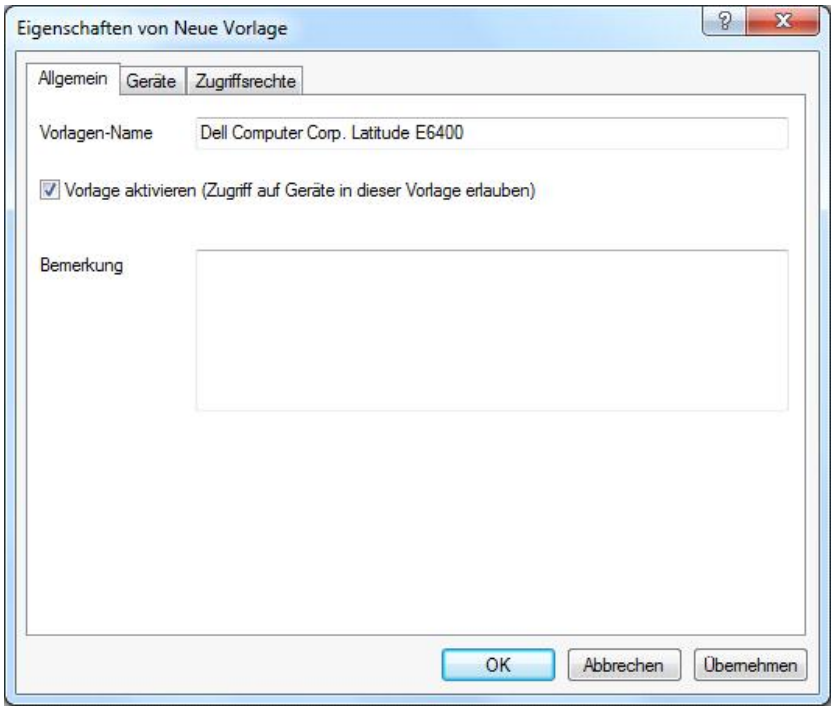
4.2.4.2.4 Zugriffsrechte innerhalb einer Computervorlage definieren

Als Vorgabe ist der Zugriff auf Geräte innerhalb der Vorlage für alle Benutzer erlaubt.



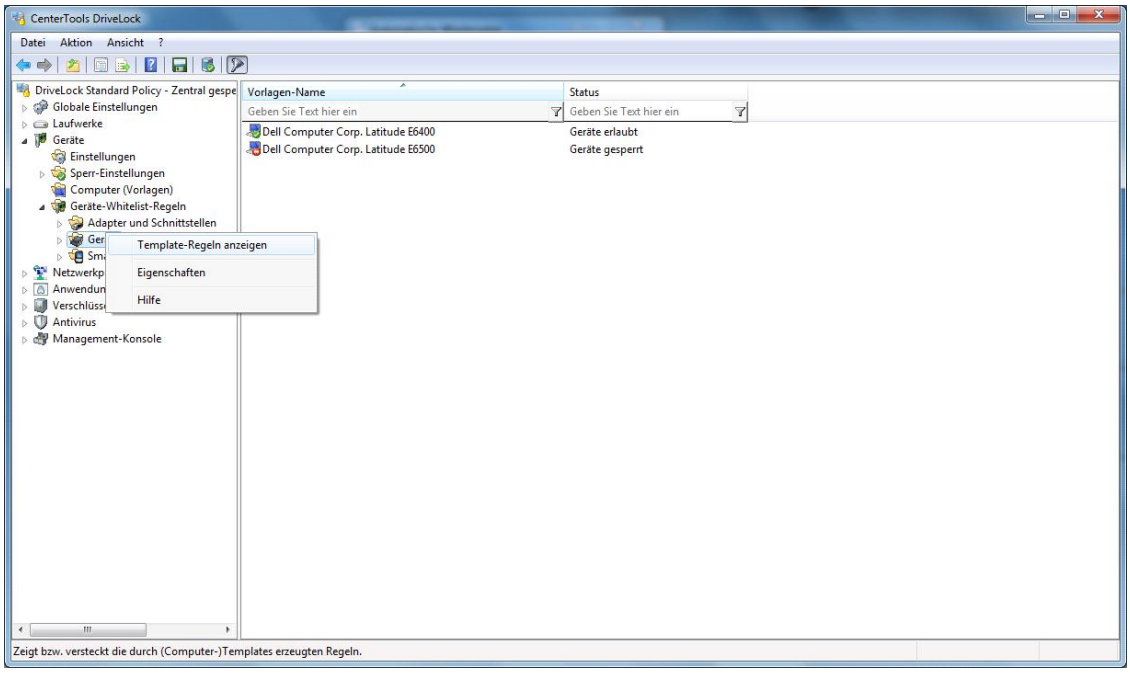
Aktivieren Sie "**Sperren, aber Zugriff für definierte Benutzer und Gruppen erlauben**", um den Zugriff auf die Geräte für einen bestimmten Benutzerkreis einzuschränken. Klicken Sie auf **Hinzufügen**, um eine weitere Gruppe oder einen Benutzer zur angezeigten Liste hinzuzufügen. Mit **Entfernen** wird der zuvor ausgewählte Eintrag gelöscht.

4.2.4.2.5 Aktivieren einer Computervorlage



Markieren Sie "**Vorlage aktivieren (…)**" und klicken Sie auf **OK**, um die Vorlage zu aktivieren. Ab diesem Zeitpunkt wird die Verwendung aller enthaltenen Geräte entsprechend der vergebenen Berechtigungen erlaubt.

4.2.4.2.6 Anzeige der durch eine Computervorlage definierten Geräte



Diese Option zeigt für die jeweilige Geräte-Klasse an, welche Geräte über eine Computer-Vorlage freigegeben sind. Wenn Sie eine Vorlage erstellen, erzeugt DriveLock automatisch dazu passende Whitelist-Regeln, die mit Hilfe dieser Option angezeigt werden können.

Vorlage-Regeln werden mit einem gelben Zahnrad auf dem zugehörigen Symbol gekennzeichnet.

Die so angezeigten Regeln können nicht direkt bearbeitet werden. Dazu müssen Sie die zugehörige Computervorlage bearbeiten.

Teil V

Netzwerkprofile

5 Netzwerkprofile

DriveLock ermöglicht es Ihnen, verschiedene Einstellungen in Abhängigkeit zur augenblicklichen Netzwerkverbindung zu konfigurieren. Während dies möglicherweise bei Desktopsystemen nicht ganz so interessant erscheinen mag, ist diese Funktionalität sehr hilfreich bei mobilen Computern (wie zum Beispiel Laptops), wo Benutzer an unterschiedlichen Orten arbeiten müssen, z.B. im Büro, Home-Office oder bei Kunden.

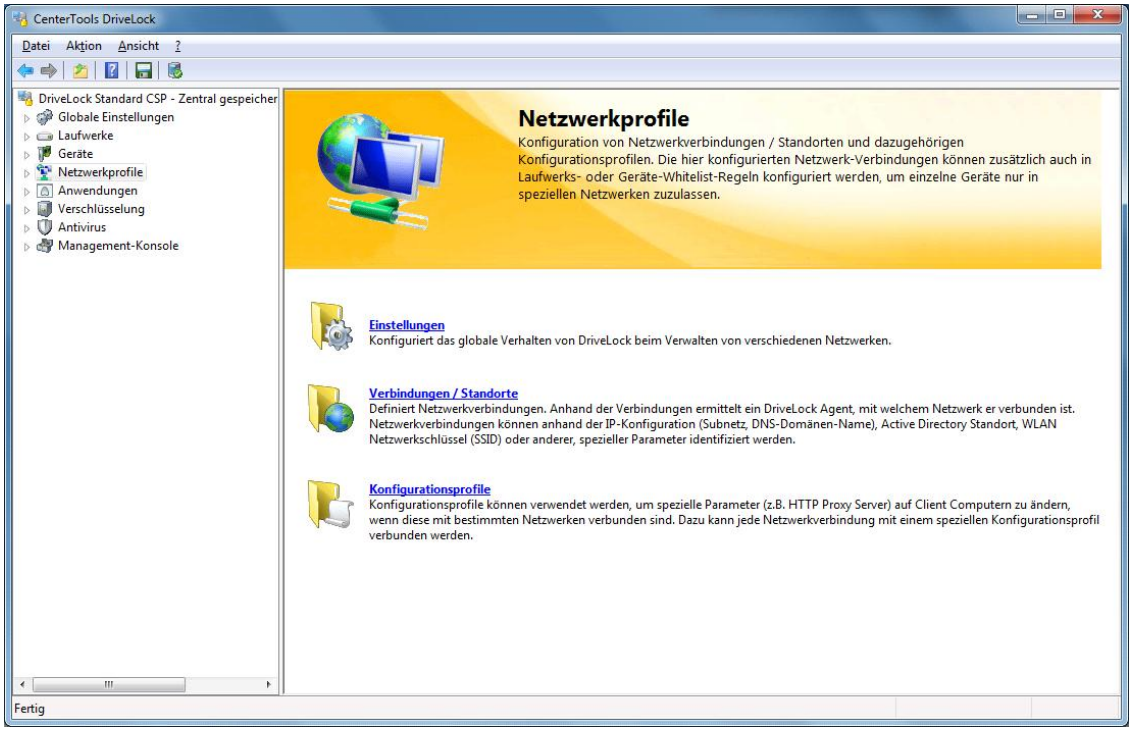
Aus Sicherheitssicht besteht bei Verbindungen zu externen Netzwerken immer das Risiko, unbekannten Situationen ausgesetzt zu sein, da diese Netzwerke außerhalb des kontrollierbaren Bereichs liegen. Währen der Computer mit dem internen Netzwerk verbunden ist, können Sie erzwingen, dass das zentrale Internet-Gateway verwendet wird. Aber was passiert, wenn der Vertriebsmitarbeiter sein Notebook zuhause anschließt. Können Sie sicherstellen, dass auch dort eine aktuelle Firewall oder ein Virenscanner läuft? Die Antwort lautet: Natürlich können Sie das nicht. Im Normalfall müssen Sie hier eine Sicherheitsrichtlinie aufsetzen, die auch dieses Szenario mit berücksichtigt und entsprechende Sicherheit gewährleistet. Dazu fällt diese Richtlinie möglicherweise strenger aus, als sie ohne das unkontrollierbare Netzwerk wäre.

Mit DriveLock können nun Whitelist-Regeln so konfiguriert werden, dass Sie für bestimmte Netzwerke gelten. Zum Beispiel ist es möglich, dass alle Netzwerkgeräte deaktiviert werden, sobald ein Notebook an ein anderes Netzwerk als das eigene angeschlossen wird (das ist zugegeben eine sehr strenge Richtlinie). Aber nicht nur Regeln können dynamisch aktiviert werden, auch bestimmte Einstellungen bzgl. der Netzwerkverbindung können verändert werden. Diese Einstellungen beinhalten die Internet Explorer Proxy Konfiguration oder Einstellung für den Microsoft Messenger oder den aktuellen Standard-Drucker. Des Weiteren kann DriveLock erzwingen, dass die Gruppenrichtlinien aktualisiert werden, sobald eine Veränderung der Netzwerkverbindungen erkannt wird.

Diese Netzwerkprofile können ebenfalls in Verbindung mit der Applikationskontrolle eingesetzt werden. Auf diese Weise können Sie die Ausführung bestimmter Programme in Abhängigkeit der aktuellen Netzwerkverbindung erlauben oder verbieten. Zum Beispiel möchten Sie nicht, dass Benutzer den MS Messenger oder Skype innerhalb Ihres Netzwerkes verwenden. Die Verwendung zu Hause oder unterwegs sollte aber schon möglich sein.

Auch für die Konfiguration der Antivirus-Engine können Netzwerkprofile verwendet werden. So kann zum Beispiel die Scan-Heuristik in unbekannten Netzwerken verschärft werden, um noch genauer nach Malware zu suchen.

Netzwerkprofile und Konfigurationseinstellungen können mit der DriveLock Management Konsole (oder auch entsprechend mit dem GPO-Editor) definiert werden. Im Folgenden werden die Begriffe Netzwerkprofile und Netzwerkverbindungen als Synonym füreinander verwendet.

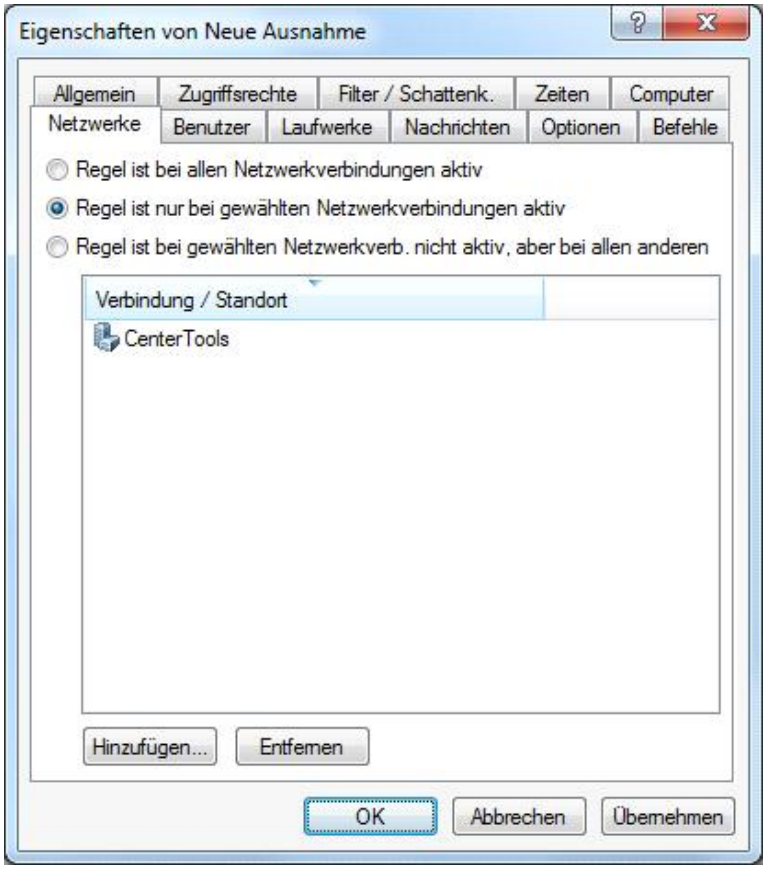


In den folgenden Abschnitten wird beschrieben, aufgrund welcher Informationen DriveLock in der Lage ist, eine Netzwerkverbindung zu erkennen und wie Konfigurationsänderungen für die Erstellung von Konfigurationsrichtlinien verwendet werden können.

Bitte beachten Sie, dass aus technischen Gründen ein Neustart erfolgen muss, wenn die Netzwerkverbindung (Kabel) während des Ruhezustandes / Energiesparmodus getrennt wird und der Computer danach keine neue Netzwerkverbindung eingeht, bevor DriveLock erkennen kann, dass der Computer „offline“ ist.

Nachdem Sie nun die verschiedenen Netzwerkverbindungen eingerichtet haben, können Sie diese in einer Whitelist-Regel verwenden. Netzwerkverbindungen können bei einer Laufwerks-, Geräte- oder Anwendungsregel Verwendung finden.

Wählen Sie dazu innerhalb einer Whitelist-Regel den Reiter Netzwerk und eine der nachfolgenden Optionen aus:

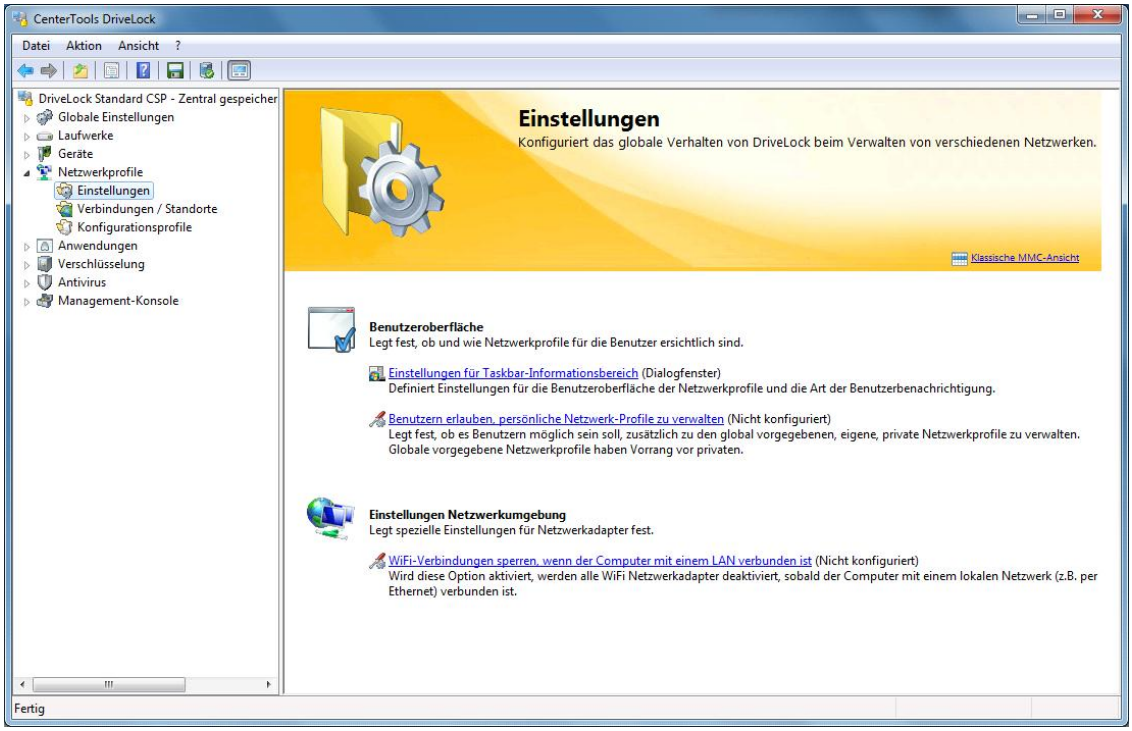


- Die Regel gilt für alle Netzwerkverbindungen
- Die Regel gilt nur für die aufgelisteten Netzwerkverbindungen
- Die Regel gilt für alle außer den aufgelisteten Netzwerkverbindungen

"**Regel ist bei allen Netzwerkverbindungen aktiv**" ist bei neuen Whitelist-Regeln automatisch vorgegeben.

Sofern Sie die vordefinierten Einstellungen ändern, wählen Sie mindestens eine Netzwerkverbindung aus. Klicken Sie auf **Hinzufügen**, um weitere Netzwerkverbindungen der Liste hinzuzufügen. Durch **Entfernen** werden zuvor ausgewählte Netzwerkverbindungen aus der Liste gelöscht.

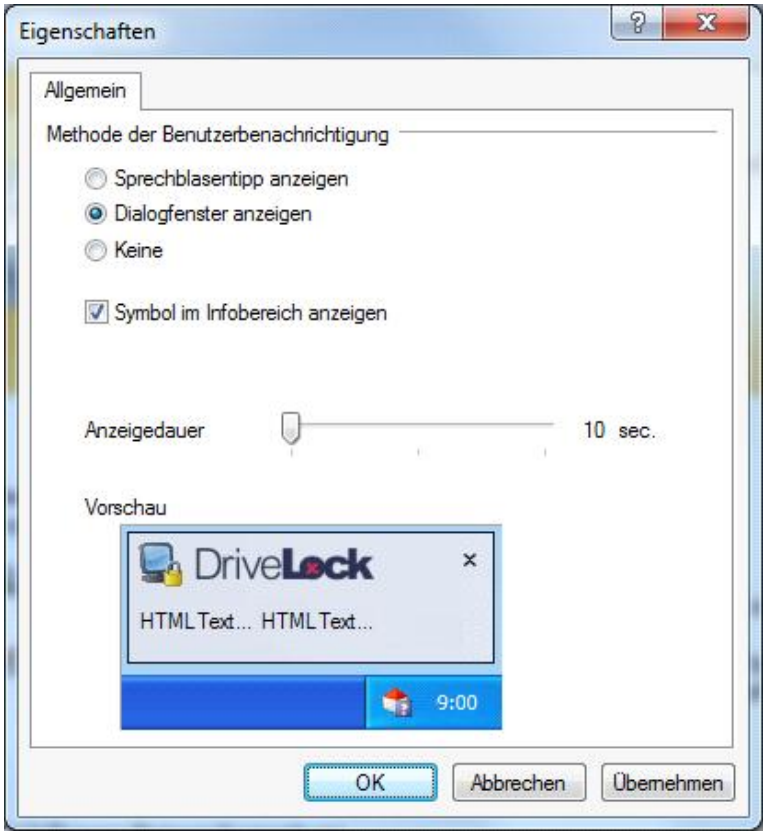
5.1 Allgemeine Netzwerkprofil-Einstellungen



Es gibt drei verschiedene allgemeinere Einstellungen für Netzwerk Profile, die nicht an eine bestimmte Netzwerkverbindung gebunden sind und bei jeder konfigurierten Verbindung angewendet werden. Zwei davon legen die Art und Weise fest, wie die Interaktion mit dem Benutzer erfolgt, die dritte legt das Verhalten der WiFi-Adapter bei einer LAN-Verbindung fest. Wenn Sie wissen möchten, wie Benutzer ihre eigenen privaten Netzwerk Profile erstellen können, sehen Sie im Abschnitt „Benutzerspezifische Netzwerkprofile erstellen" nach.

5.1.1 Benutzerbenachrichtigung einrichten

Klicken Sie **Einstellungen für den Taskbar-Informationsbereich**, um die Sichtbarkeit von Profilen und deren Erscheinungsbild beim Benutzer zu konfigurieren.



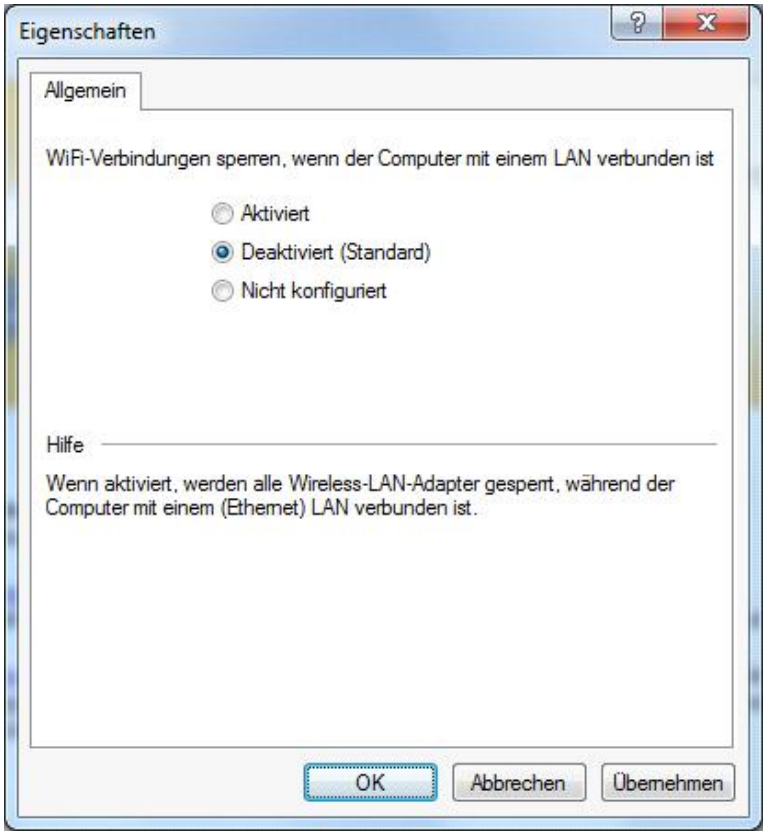
Wenn Sie nicht möchten, dass Netzwerk Profile angezeigt werden, deaktivieren Sie die Funktion "**Symbol im Infobereich anzeigen**". Ist diese aktiviert, wird das bei einer Netzwerkverbindung definierte Icon in der Taskleiste angezeigt. Darüber hinaus können Sie auswählen, ob das Symbol nur währen einer Meldung oder der ganzen Zeit sichtbar ist.

Verwenden Sie den Schieberegler, um die Dauer der Anzeige in Sekunden festzulegen,

5.1.2 WiFi Verbindungen bei LAN-Anbindung verhindern

DriveLock bietet die Möglichkeit, drahtlose Netzwerkadapter (falls vorhanden) abzuschalten, wenn der Computer mit einem LAN verbunden ist. Dadurch können sog. Cross-Network-Links verhindert werden, die üblicherweise ein Sicherheitsrisiko für Ihre Infrastruktur darstellen können.

Um WiFi-Verbindungen in dieser Zeit zu verhindern, klicken Sie **WiFi-Verbindungen sperren, wenn der Computer mit einem LAN verbunden ist** und aktivieren Sie die Funktion.



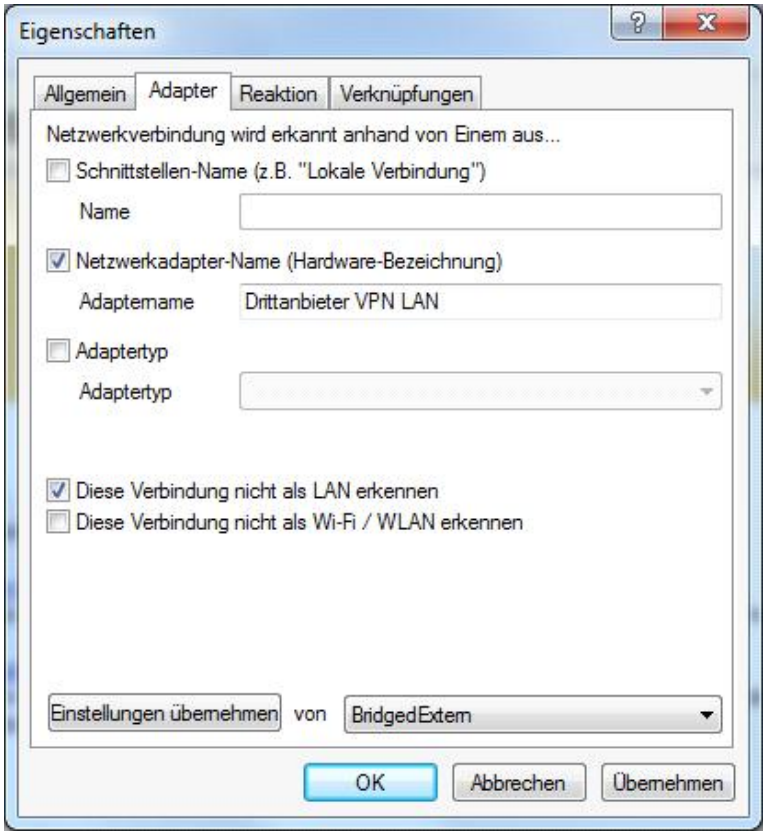
5.1.2.1 VPN-Clients von Drittanbietern einsetzen

Wenn die Option *„WiFi-Verbindungen sperren, wenn der Computer mit einem LAN verbunden ist*“ gesetzt ist, muss bei dem Einsatz von VPN-Clients von Drittanbietern ein weiterer Punkt berücksichtigt werden.

Beispiel: WiFi-Verbindungen sollen nicht zugelassen werden, wenn eine Netzwerkverbindung besteht. Auf Notebooks kommt der VPN-Client eines Drittanbieters (also keine Windows integrierte VPN-Verbindung) zum Einsatz, um mobile Benutzer mit dem Firmennetzwerk zu verbinden. Der VPN-Client des Drittanbieters installiert eine virtuelle Netzwerkkarte. Angenommen der Client ist über WLAN verbunden und baut eine Verbindung über VPN auf. Wenn die Option WiFi-Verbindungen sperren, wenn der Computer mit einem LAN verbunden ist aktiviert ist, wird die WLAN Verbindung getrennt, da DriveLock denkt es ist mit einem physikalischem Netzwerk verbunden.

Damit die im Beispiel beschriebene VPN-Verbindung über WLAN zulässig ist, muss in DriveLock die virtuelle Netzwerkkarte des VPN-Clients ausgenommen werden:

Klicken Sie auf **Netzwerkprofile -> Verbindungen / Standorte** – Rechtsklick auf **Neu -> Netzwerkadapter** – Reiter **Adapter**:



Wählen Sie dort eine Methode aus, um die virtuelle Netzwerkkarte des VPN-Clients eindeutig und zuverlässig zu identifizieren. Wenn der VPN-Client lokal installiert ist, kann man Daten über die Auswahl der Netzwerkkarte und Einstellungen übernehmen gleich als Kriterien übernehmen:

- *Schnittstellen-Name*: Name der Netzwerkverbindung. Dieser Name kann variieren.
- *Netzwerkadapter-Name*: Bezeichnung des Netzwerkadapters. Dieser Name bleibt i.d.R. identisch.
- *Adaptertyp*: Typ des Netzwerkadapters. Der gemeldete Wert kann sich pro Netzwerkadapter unterscheiden.

Damit der Adapter für dieses Szenario ausgenommen wird, muss Diese Verbindung nicht als LAN erkennen gewählt werden:

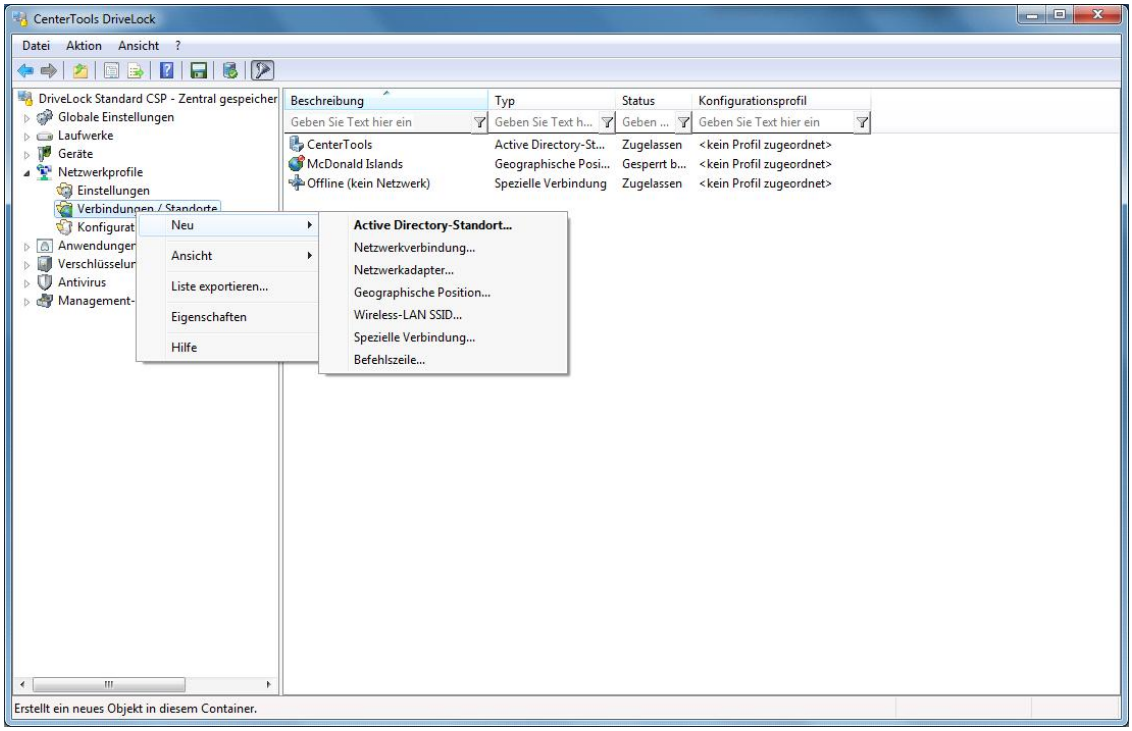
- *Diese Verbindung nicht als LAN erkennen*: Der gewählte Adapter wird nicht als Netzwerkverbindung erkannt. Regeln die sich auf LAN-Netzwerke beziehen, werden nicht für diesen Adapter angewandt.
- *Diese Verbindung nicht als Wi-Fi / WLAN erkennen*: Der gewählte Adapter wird nicht als Wireless LAN erkannt. Regeln die sich auf WLAN-Netzwerke beziehen, werden nicht für diesen Adapter angewandt.

5.2 Netzwerkverbindungen festlegen

Bevor sie Konfigurationen automatisch anpassen oder Whitelist-Regeln von einer Netzwerkverbindung abhängig machen können, müssen Sie festlegen, wie eine bestimmte Netzwerkverbindung erkannt werden kann. Folgende Arten von Standorten stehen dazu zur Verfügung:

- Active Directory Standort
- Netzwerkverbindung (basierend auf IP-Informationen)
- Netzwerkadapter
- Geographische Position

- WLAN SSID
- Spezielle Verbindungen
- Ergebnis einer Befehlszeilenoperation



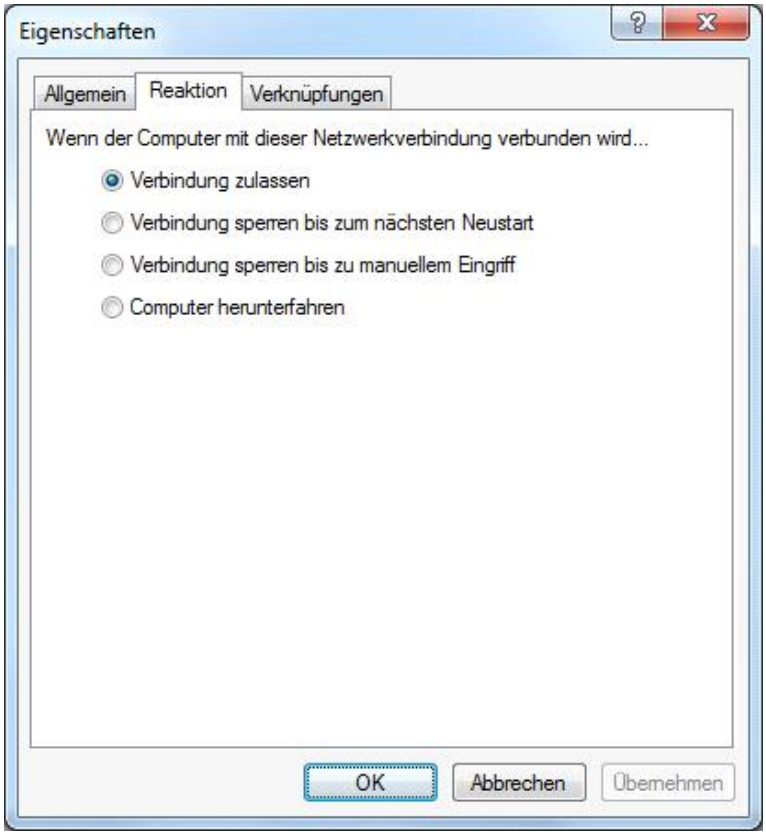
Klicken Sie mit der rechten Maustaste auf **Verbindungen/Standorte** und wählen **Neu** und den gewünschten Typ aus dem Kontextmenü.

Bei jedem Typ müssen Sie später ggf. auch noch das gewünschte Konfigurationsprofil aus einer Liste auswählen.

> Sofern Sie bisher noch keine Konfigurationsprofile definiert haben, verschieben Sie die Auswahl auf einen späteren Zeitpunkt. Sie können dann durch einen Doppelklick auf eine bestehende Verbindung den Konfigurationsdialog erneut öffnen und das gewünschte Profil auswählen.

Zusätzlich können Sie bei jedem Typ ein passendes Symbol aus einer Liste auswählen, dass ggf. später den Benutzern in der Taskleiste im Informationsbereich angezeigt wird.

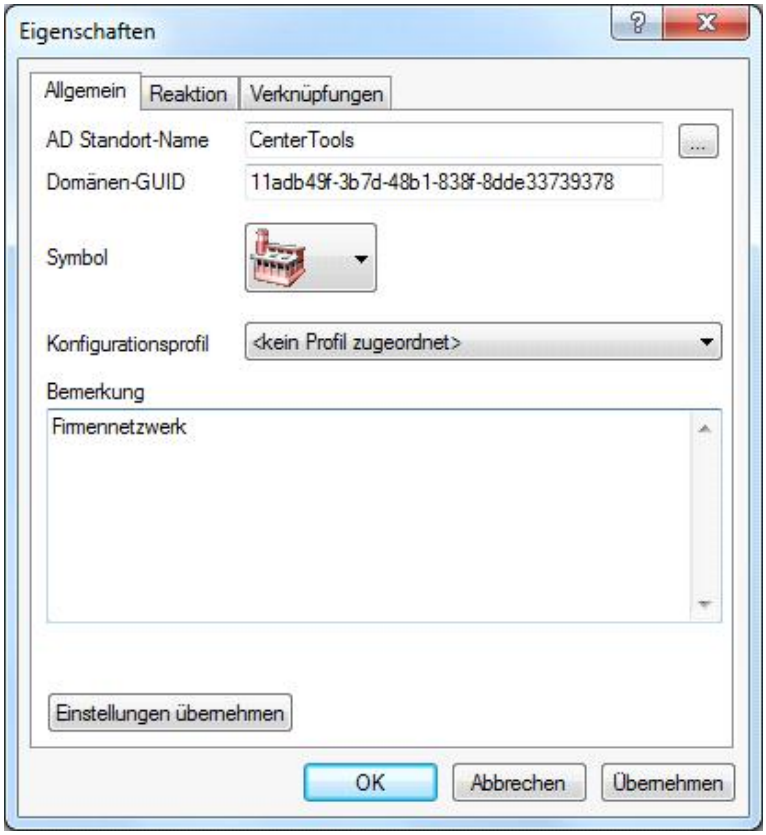
Wenn Sie eine Netzwerkverbindung definieren, müssen Sie auch angeben, was passieren soll, wenn DriveLock diese erkennt. Dazu wählen Sie eine der beim Reiter "**Reaktion**" angegebenen Optionen:



Seien Sie bitte sehr vorsichtig, wenn Sie Agenten anweisen, Netzwerkverbindungen zu deaktivieren. Wenn DriveLock die Netzwerk-verbindungen bis zu einem manuellen Eingriff sperrt, müssen Sie jeden Computer von Hand und einzeln neu konfigurieren, da eine Verbindung über das Netzwerk anschließend nicht mehr möglich ist.

5.2.1 Active Directory Standort

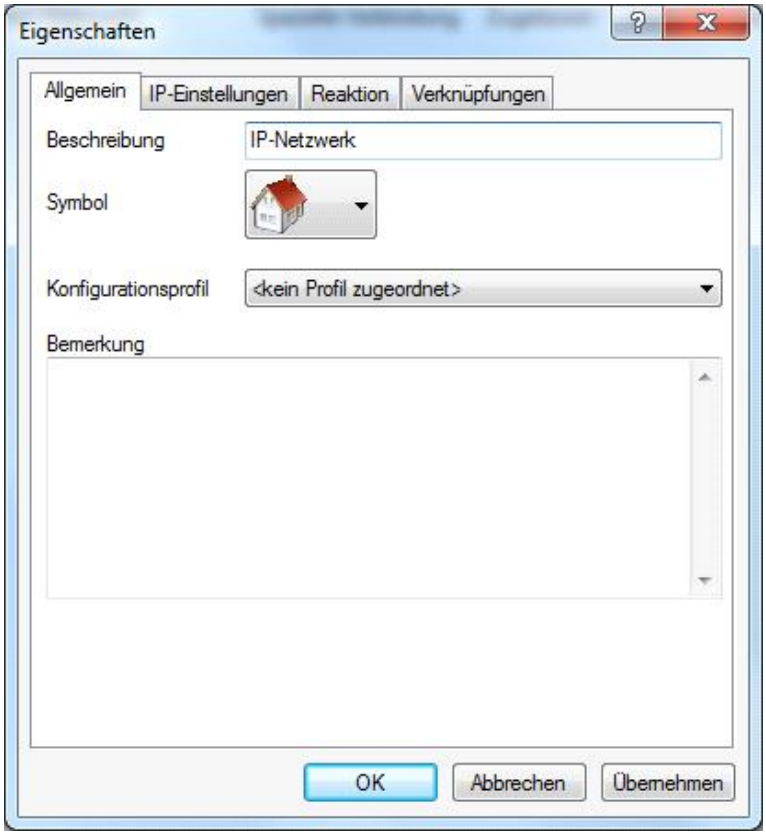
Wenn Sie einen Active Directory Standort wählen, wird die Verbindung aufgrund des aktuellen Namens des Standortes ermittelt.



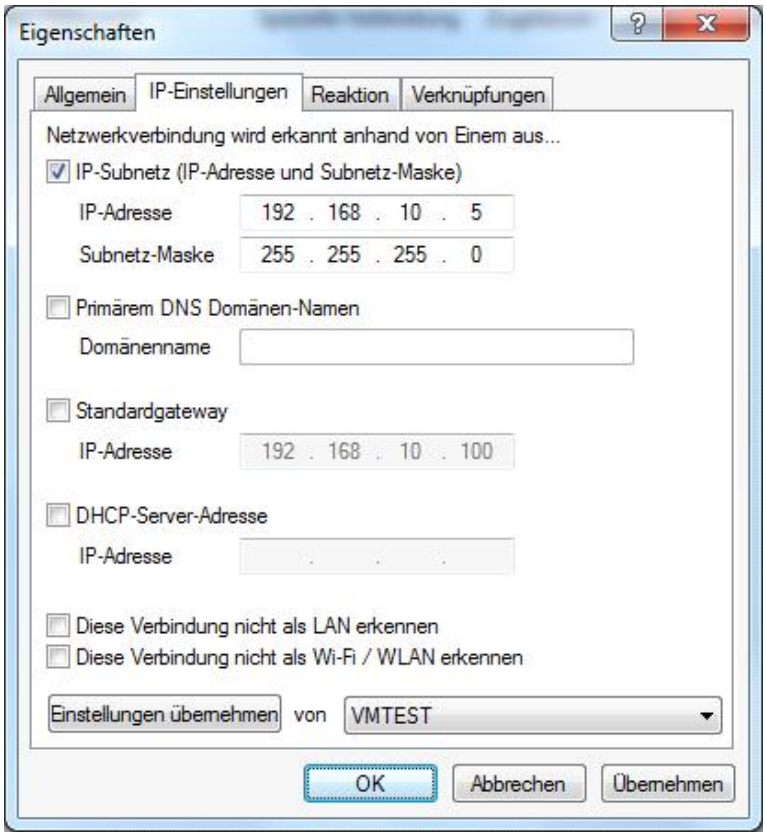
Sie haben die Möglichkeit, die derzeit gültigen Einstellungen mit einem Klick auf die gleichnamige Schaltfläche zu übernehmen. Daraufhin liest DriveLock diese Informationen direkt aus dem Active Directory und füllt die Eingabefelder "**AD Standort-Name**" und "**Domänen-GUID**" automatisch aus. Alternativ können Sie den Namen auch selbst eingeben oder durch klicken auf die Schaltfläche "**...**" einen im Active Directory vorhandenen Standort auswählen.

5.2.2 Netzwerkverbindung anhand IP-Einstellungen festlegen

Sollte es notwendig sein, die Verbindung anhand von IP-Informationen (wie z.B. einem IP-Adressraumes) zu definieren, wählen Sie **Netzwerkverbindung** aus dem Kontextmenü.



Geben Sie wiederum einen Namen ein und wählen ein Symbol für die Anzeige. Anschließend aktivieren Sie den Reiter IP-Einstellungen, um die IP-Informationen zu konfigurieren.



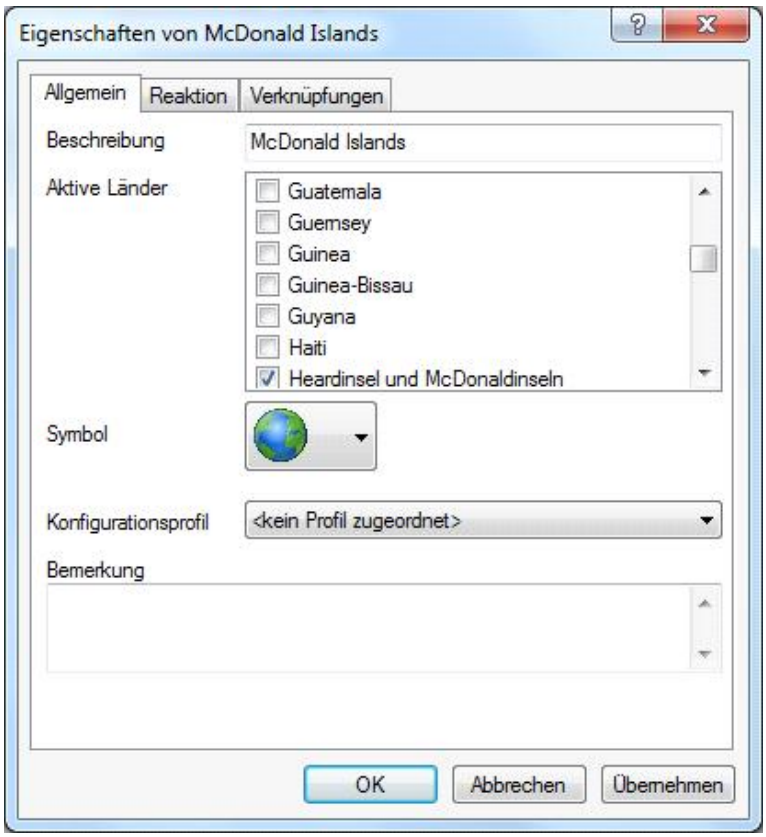
Sie haben die Möglichkeit, die aktuellen Einstellungen aus einer der vorhandenen Netzwerkverbindungen auszulesen oder die Eingaben von Hand vorzunehmen. Dazu aktivieren Sie die jeweiligen Kriterien und geben die notwendigen Informationen (wie z.B. IP-Adressraum, Gateway oder DHCP-Server) ein.

5.2.3 Netzwerkadapter

Die Einstellung für Netzwerkadapter wird in Verbindung mit VPN-Client von Drittanbietern benötigt und wird im Abschnitt „*VPN-Clients von Drittanbietern einsetzen*“ beschrieben.

5.2.4 Geographische Position

Ein Standort kann auch anhand der öffentlichen IP-Adresse zugeordnet werden. DriveLock versucht dazu die öffentliche IP-Adresse des Clients zu ermitteln und vergleicht Sie mit der lokalen GEO-IP Datenbank. Um den Client anhand des aktuellen Landes zu identifizieren, gehen Sie auf **Netzwerkprofile -> Verbindungen / Standorte** – Rechtsklick auf **Neu -> Geographische Position**:



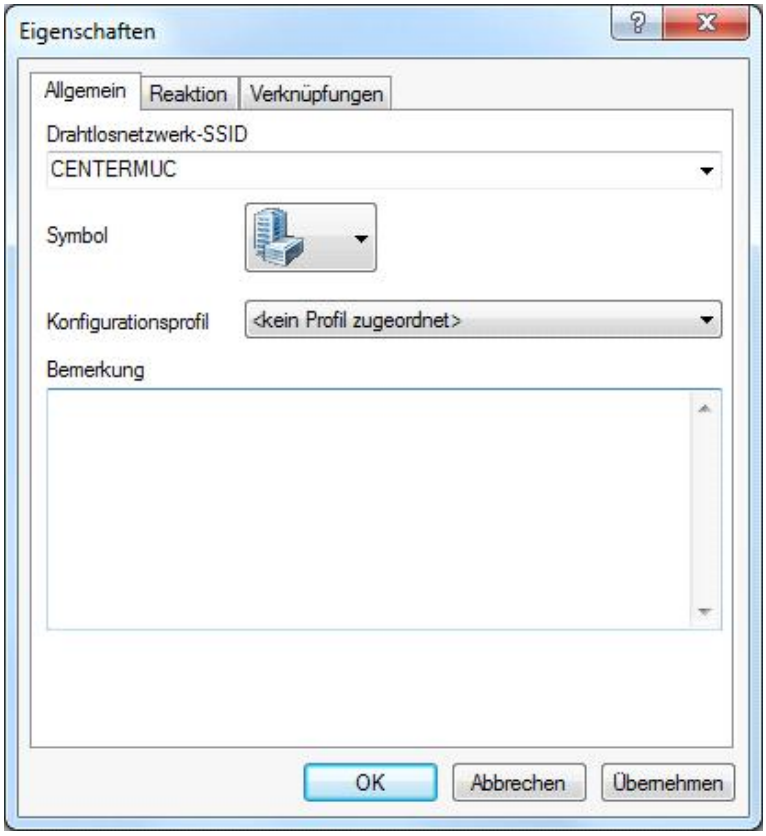
Wählen Sie nun ein oder mehrere Länder aus, die Sie in weiteren DriveLock-Regeln als ein Standort verwenden möchten. Sie können damit für ein bestimmtes Land auch generell die Netzwerkverbindung sperren (über den Reiter Reaktion).

Beispiel: Sie haben mobile Mitarbeiter die ausschließlich in der D-A-CH Region arbeiten und reisen. Sie möchten sicherstellen, dass generell keine Netzwerkverbindung möglich ist, wenn ein Notebook außerhalb der Länder Deutschland, Österreich, Schweiz erkannt wird.

> Um die geographische Position zu erkennen, wird eine aktive Internetverbindung benötigt.

5.2.5 Drahtlosnetzwerk mit SSID

Wenn Ihre Netzwerkverbindung anhand einer WLAN-SSID erkannt werden soll, wählen Sie **Wireless-LAN-SSID** aus dem Kontextmenü aus.



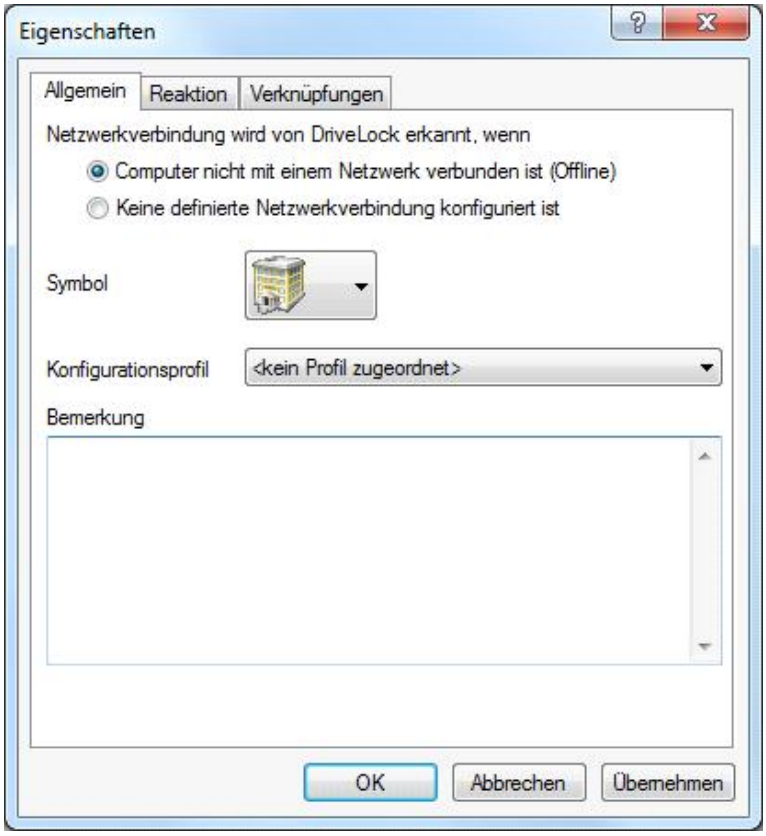
Geben Sie anschließend die SSID in das entsprechende Feld ein.

5.2.6 Besondere Netzwerkverbindung

Eine spezielle Verbindung kann aus zwei Gründen verwendet werden:

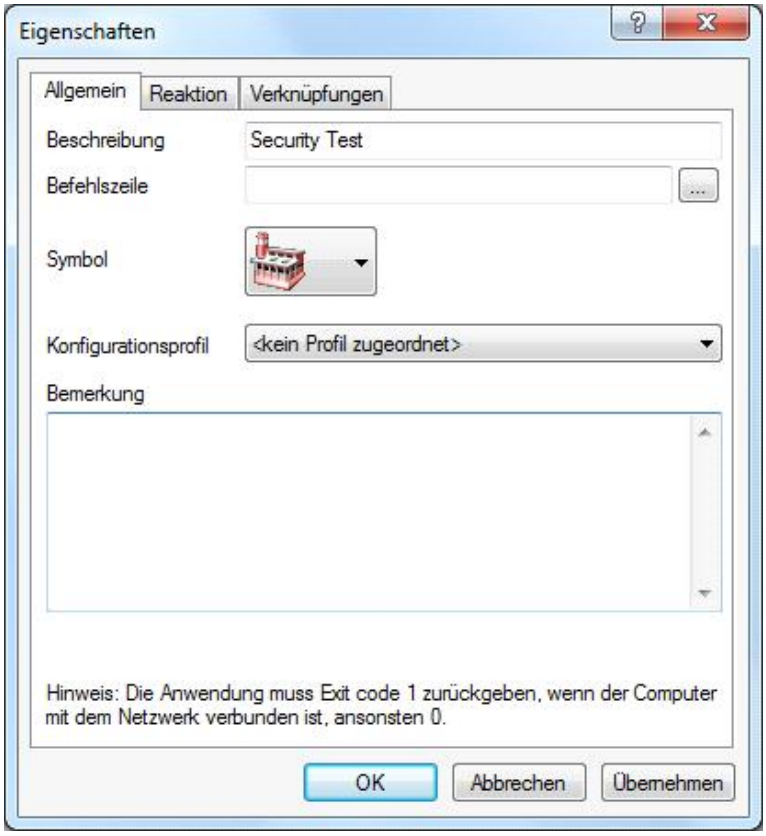
- Sie müssen Einstellungen automatisch anpassen, wenn der Computer mit keinem Netzwerk verbunden ist (Offline)
- Sie möchten Einstellungen konfigurieren (oder eine Aktion festlegen), wenn der Computer mit einem Netzwerk verbunden ist, welches nicht erkannt werden konnte

Auch hier kann wieder ein entsprechendes Icon ausgewählt werden.



5.2.7 Befehlszeile

In einigen Situationen kann es aus Sicherheitsgründen nicht akzeptabel sein, ein Netzwerk nur anhand der Active Directory Domänen-GUID oder der IP-Adresse zu erkennen. Da es aber vielfältige Möglichkeiten gibt, das eigene Netzwerk nach Identitätsmerkmalen abzusuchen, können Sie dazu ein selbstgeschriebenes Programm oder Skript verwenden. Gibt dies den Wert “1” zurück, wird der Test als bestanden akzeptiert. So ist es zum Beispiel möglich, das Vorhandensein bestimmter Rechner mit bestimmten Namen, Diensten oder Einstellungen zu prüfen. Oder Sie stellen sicher, dass ein Rechner vorgegebenen Sicherheitsrichtlinien entspricht, bevor die Verbindung zu einem Netzwerk erlaubt wird.



Eine Befehlszeile ist ein auf der Kommandozeile ausführbarer Befehl. Sie können so z.B. ein Programm (*.exe) oder ein Visual Basic Skript (*.vbs), ja sogar ein Skript der neuen Windows PowerShell ausführen lassen.

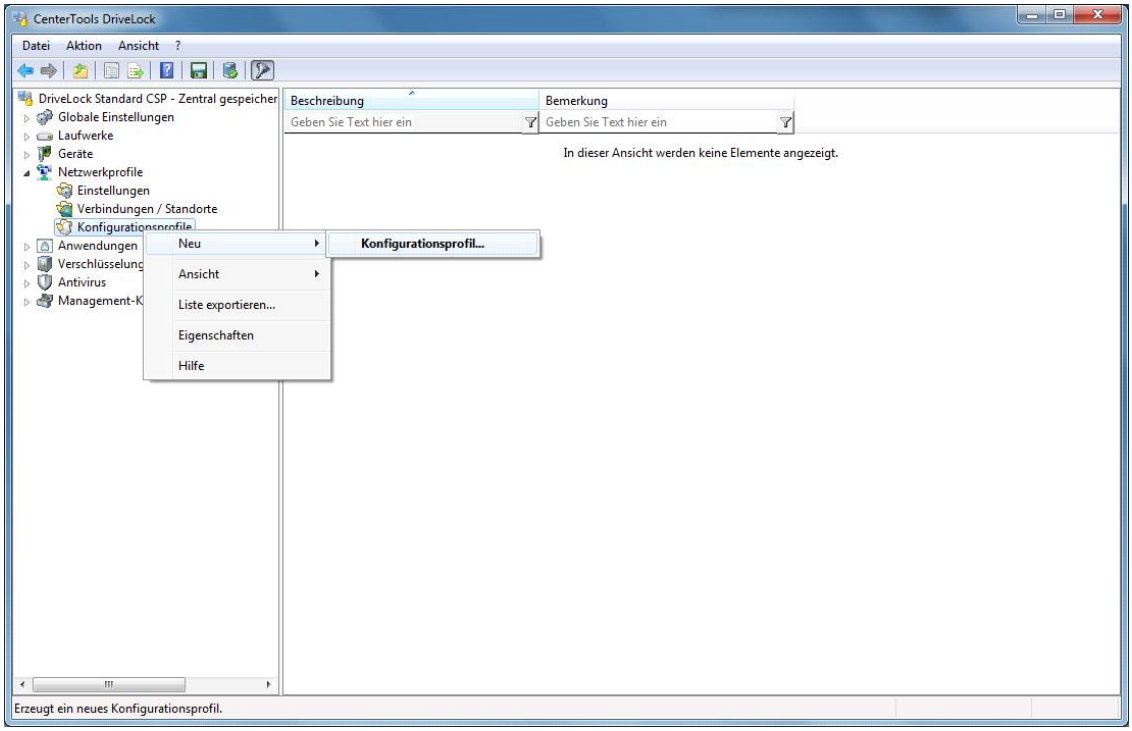
> Um zum Beispiel ein VB-Skript zu starten, müssen Sie den vollständigen Pfad zur Skript-Datei angeben (z.B. "*cscript c:\programing\scripts\meinscript.vbs*").

5.3 Konfigurationsprofile erstellen

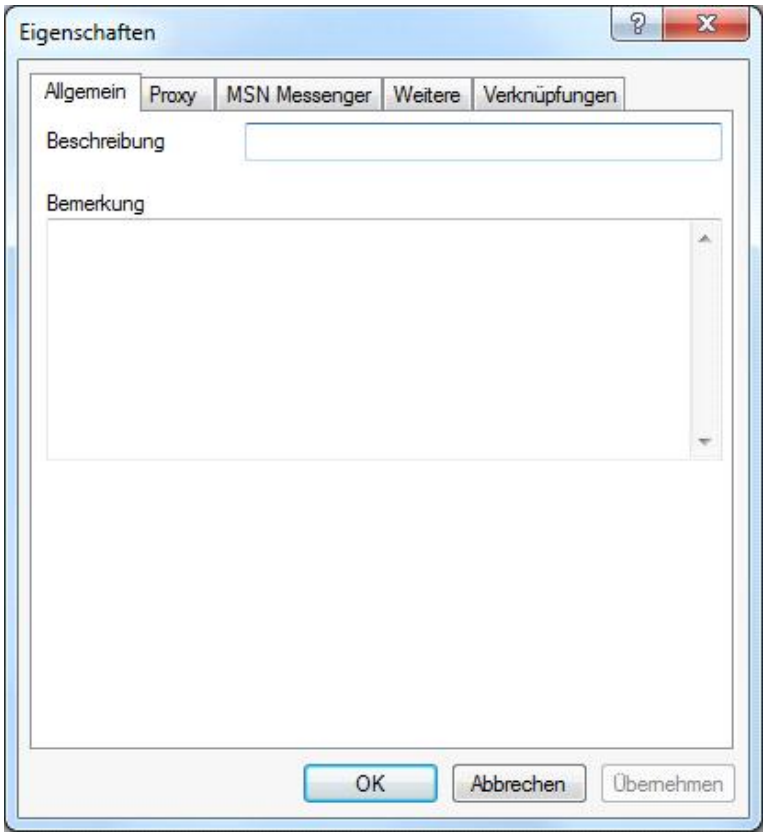
In dem Sie ein Konfigurationsprofil zusammen mit einer Netzwerkverbindung verwenden, ist DriveLock in der Lage, bestimmte Computereinstellungen nach Erkennung der Verbindung automatisch anzupassen. Das Profil definiert dabei, in welchen der folgenden Bereichen Änderungen durchgeführt werden:

- Internet Explorer Proxy Einstellungen
- Microsoft Messenger Einstellungen
- Standarddrucker

Zusätzlich kann der DriveLock Agent die Aktualisierung der Gruppenrichtlinien für den Computer und/oder den Benutzer erzwingen, wenn sich die Netzwerkverbindung ändert, oder ein Skript oder Programm ausführen.



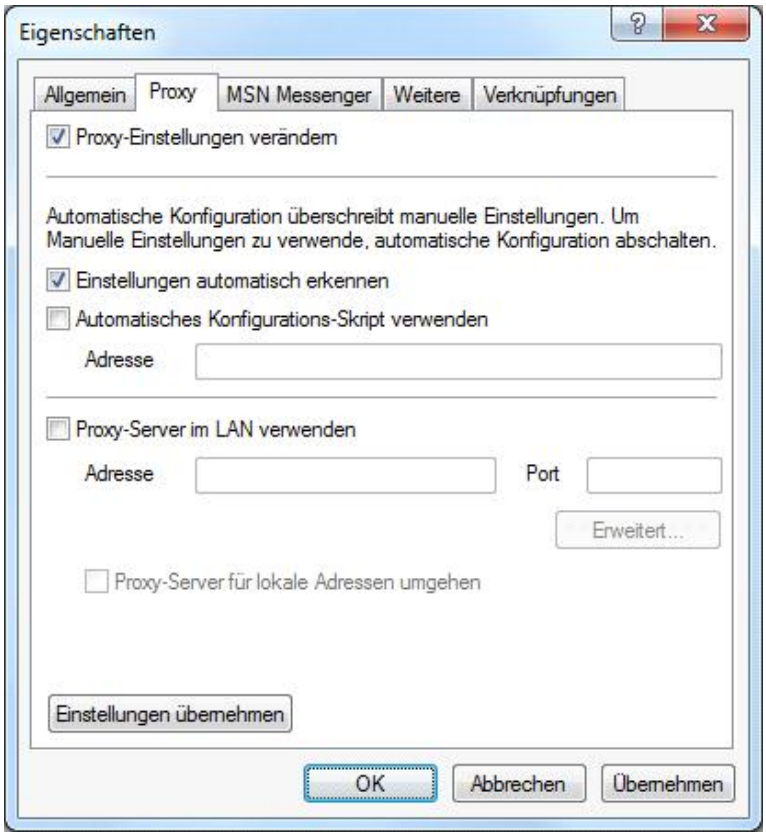
Rechtsklicken Sie auf **Konfigurationsprofile** und wählen **Neu : Konfigurationsprofil** aus dem Kontextmenü.



Geben Sie zunächst einen Namen für dieses Profil in das Feld "**Beschreibung**" ein. Zur Dokumentation können Sie noch einen Kommentar in das Bemerkungsfeld eingeben.

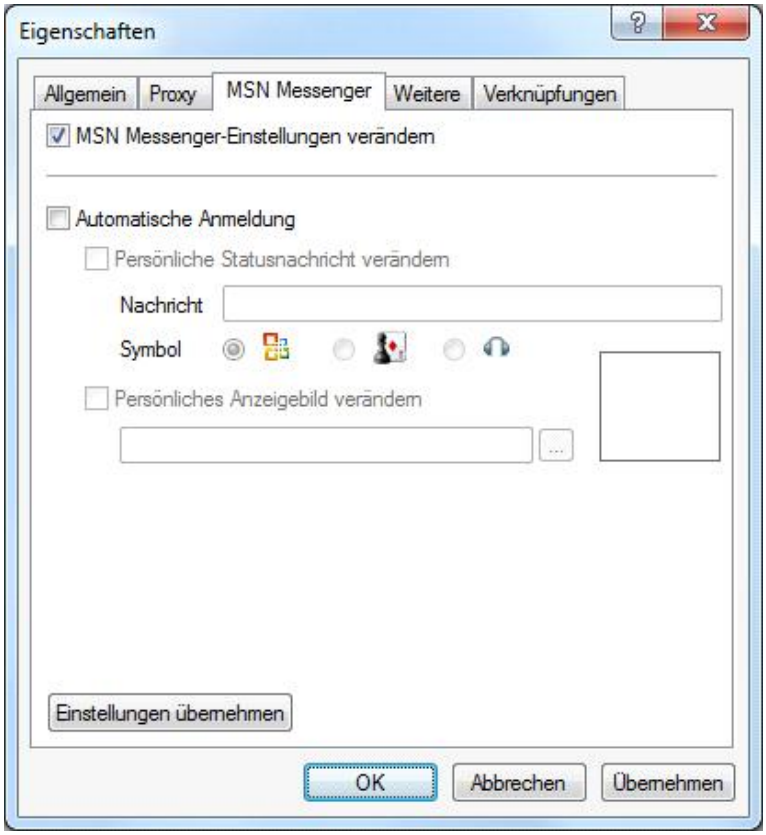
5.3.1 Internet Explorer Proxy Einstellungen

Nachdem Sie ein neues Profil erstellt haben, aktivieren Sie den Reiter **Proxy**.



Um die automatische Anpassung der Internet Explorer Einstellungen zu ermöglichen, aktivieren Sie "**Proxy-Einstellungen verändern**". Anschließend können Sie die derzeit gültigen Einstellungen aus der lokalen Konfiguration des IE auslesen, indem Sie die Schaltfläche **Einstellungen übernehmen** klicken. Mehr zu den Einstellungen und deren Auswirkungen entnehmen Sie bitte der entsprechenden Dokumentation für den Internet Explorer.

5.3.2 MSN Messenger Einstellungen



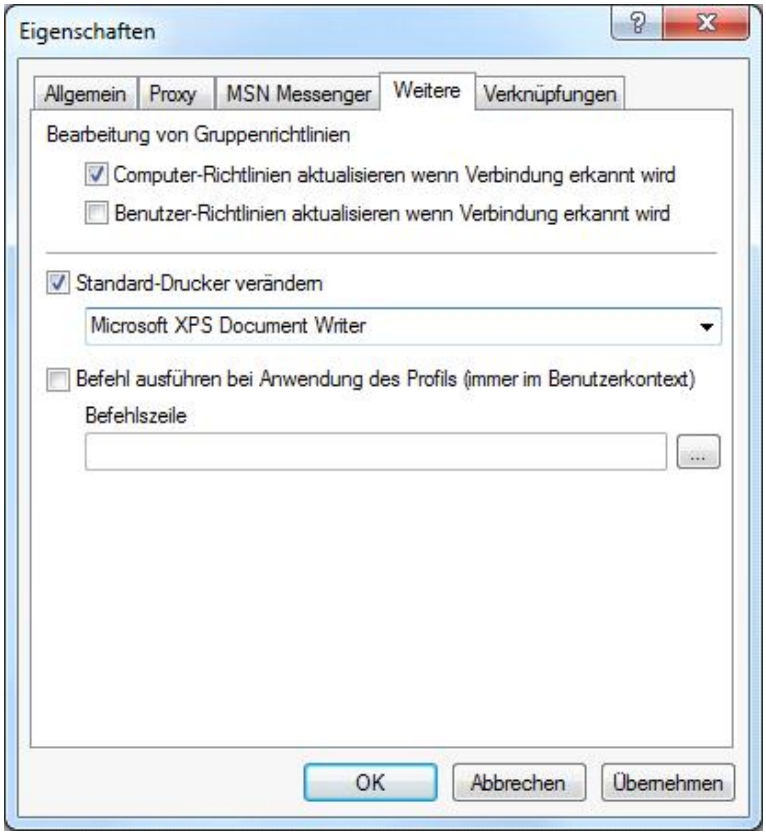
Wählen Sie den Reiter MSN Messenger und aktivieren Sie "**MSN Messenger-Einstellungen verändern**", um die automatische Anpassung zu aktivieren. Konfigurieren Sie die verschiedenen Einstellungen entsprechend Ihrer Vorstellung. Auch hier können Sie wiederum die aktuell gültigen Einstellungen aus Ihrer Messenger Konfiguration übernehmen.

Ändern Sie Ihre Statusmeldung und wählen Sie ein Bild, dass vor Ihrer persönlichen Meldung angezeigt werden soll. Um das persönliche Anzeigebild anzupassen, aktivieren Sie "**Persönliches Anzeigebild verändern**" und wählen mit Hilfe der Schaltfläche "**...**" eine Bilddatei aus.

Für weitere Informationen zu den verschiedenen Einstellmöglichkeiten konsultieren Sie bitte die Dokumentation zum MS Messenger.

5.3.3 Weitere Aktionen bei Erkennung von Netzwerken

Um den aktuellen Standard-Drucker anzupassen, aktivieren Sie den Reiter "**Weitere**" und markieren die Option "**Standard-Drucker verändern**".



Wählen Sie einen Drucker aus der Dropdown-Liste.

Wenn Sie einen oder beide der Gruppenrichtlinien-Optionen aktivieren, wird der DriveLock Agent bei der Veränderung der Netzwerkverbindung dafür sorgen, dass die entsprechenden Gruppenrichtlinien neu geladen werden.

Die Befehlszeile kann einen beliebigen über die Kommandozeile ausführbaren Befehl enthalten. Somit können Sie zum Beispiel ein Programm (*.exe), ein Visual Basic Skript (*.vbs) oder Skripts für die neue Windows PowerShell ausführen lassen.

Auf diese Weise ist es möglich, auf eine erkannte neue Netzwerkverbindung in vielen erdenklichen Variationen zu reagieren.

> Um ein VB-Skript auszuführen, müssen Sie den vollständigen Pfad zur Skript-Datei angeben (z.B. "*cscript c:\programing\scripts\meinscript.vbs*").

Klicken Sie auf die Schaltfläche „**...**", um einen Dateinamen an der aktuellen Cursor-Position einzufügen. Dabei können Sie zwischen zwei Möglichkeiten wählen:

- *Dateisystem*: Die Datei ist auf der lokalen Festplatte des Computers vorhanden
- *Richtliniendateispeicher*: Die Datei aus dem Richtliniendateispeicher von DriveLock wird verwendet.

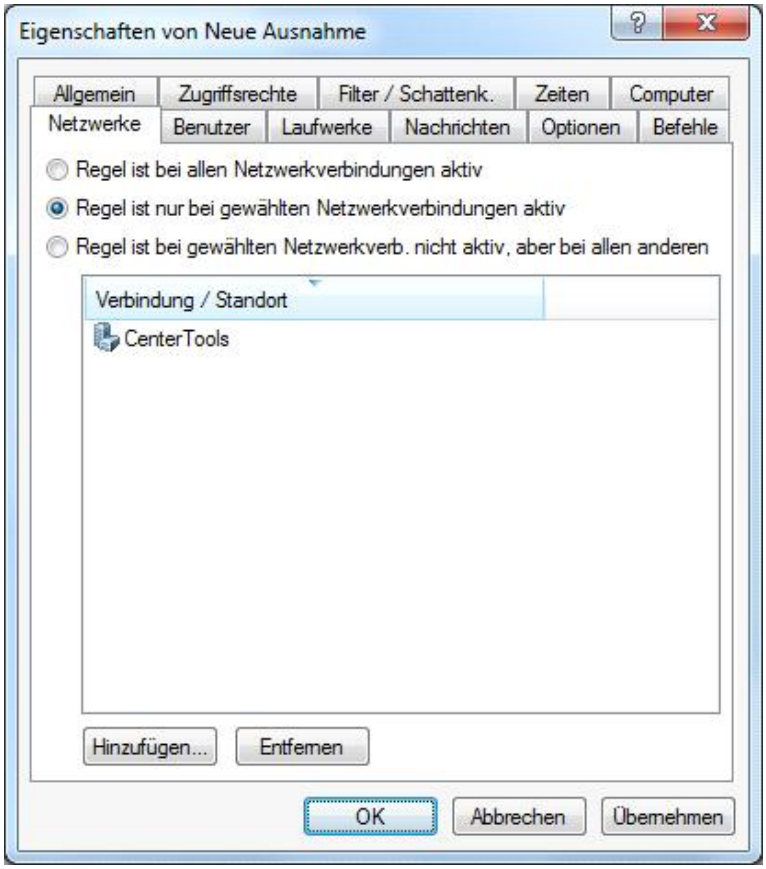
> Der Richtliniendateispeicher ist ein Datei-Container, der als Teil einer lokalen Richtlinie, einer Gruppenrichtlinie oder einer Konfigurationsdatei gespeichert wird. Er kann beliebige Dateien (wie z.B. Skripte oder Anwendungen) enthalten, die automatisch mit einer DriveLock Konfiguration verteilt werden.

Eine Datei, die aus dem Richtliniendateispeicher geladen wird, ist durch ein „*" gekennzeichnet.

5.4 Whitelist-Regel für eine Netzwerkverbindung einrichten

Nachdem Sie nun die verschiedenen Netzwerkverbindungen eingerichtet haben, können Sie diese in einer Whitelist-Regel verwenden. Netzwerkverbindungen können bei einer Laufwerks-, Geräte- oder Anwendungsregel Verwendung finden.

Wählen Sie dazu innerhalb einer Whitelist-Regel den Reiter Netzwerk und eine der nachfolgenden Optionen aus:



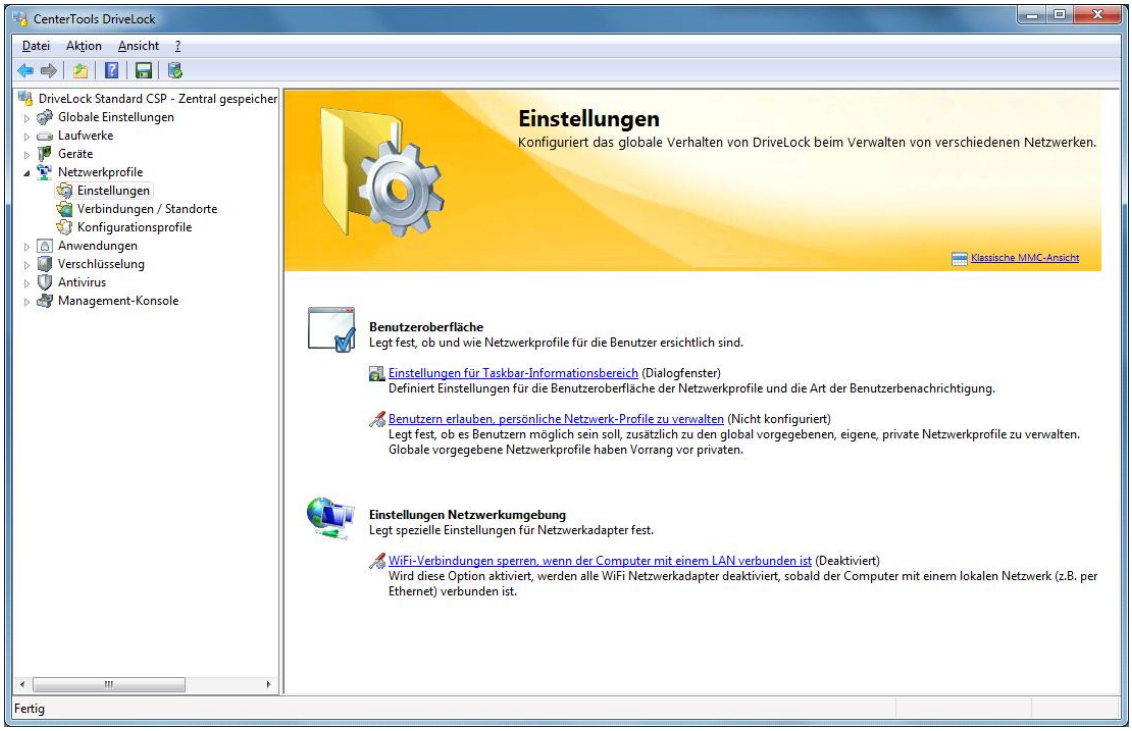
- Die Regel gilt für alle Netzwerkverbindungen
- Die Regel gilt nur für die aufgelisteten Netzwerkverbindungen
- Die Regel gilt für alle außer den aufgelisteten Netzwerkverbindungen

> "*Regel ist bei allen Netzwerkverbindungen aktiv*" ist bei neuen Whitelist-Regeln automatisch vorgegeben.

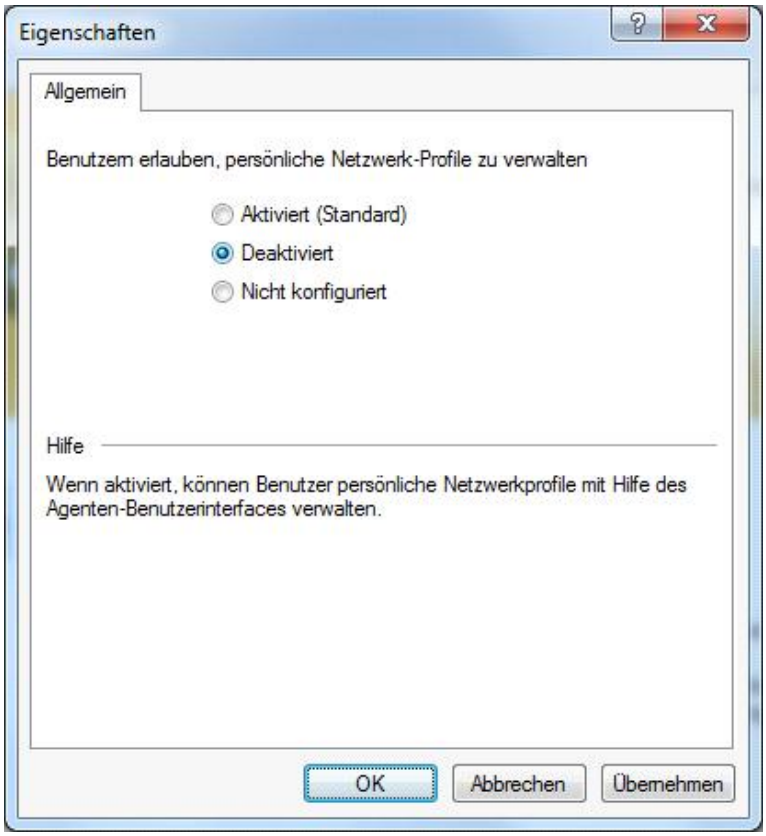
Sofern Sie die vordefinierten Einstellungen ändern, wählen Sie mindestens eine Netzwerkverbindung aus. Klicken Sie auf **Hinzufügen**, um weitere Netzwerkverbindungen der Liste hinzuzufügen. Durch **Entfernen** werden zuvor ausgewählte Netzwerkverbindungen aus der Liste gelöscht.

5.5 Benutzerspezifische Netzwerkprofile erstellen

Netzwerkverbindungen und –standorte dienen dem Administrator dazu, Unternehmensrichtlinien in Bezug auf Sicherheit in einer flexibleren Art und Weise umzusetzen. Aber einige der Einstellungen, die DriveLock verändern kann, sind nicht sicherheitsbezogen, sondern dienen dem Komfort der Benutzer. Und wer kann die Anforderungen eines Benutzers besser einschätzen, als der Benutzer selbst? Aus diesem Grund kann es Benutzern erlaubt werden, eigene Netzwerkprofile mit eigenen Konfigurationen zu erstellen.



Damit Benutzer Zugang zu dieser Funktion bekommen, klicken Sie **Einstellungen** (wie in der Abbildung gezeigt) und klicken auf **Benutzern erlauben, persönliche Netzwerk-Profile zu verwalten**.



Wählen Sie hier aus, ob diese Funktion aktiviert werden soll oder nicht.

Wie ein Benutzer eigene Profile erstellen kann, ist im *DriveLock Benutzerhandbuch* beschrieben.

Teil VI

DriveLock Disk Protection

6 DriveLock Disk Protection

DriveLock Disk Protection ist zentraler Bestandteil des Produktes DriveLock DiskProtect und wurde in früheren Versionen auch als DriveLock Full Disk Encryption (FDE) bezeichnet.

Im heutigen Computerzeitalter sind Festplatten ein Massenspeicher für vertrauliche Informationen geworden. Das weit verbreitete Windows Betriebssystem stellt keinen ausreichenden Datenschutz zur Verfügung, entweder auf einen Einzelplatz PC oder einem Netzwerk Computer (in den meisten Umgebungen). Wie auch immer, die Datensicherheit kann nicht gewährleistet werden, z.B. im Fall von System- (oder Festplatten-) Verlust. Wenn keine Maßnahmen zur Sicherung der betreffenden Daten getroffen wurde, kann jede Festplatte von einem System entfernt und die Daten darauf gelesen werden.

Um diese Sicherheitslücken zu schließen, ist eine Sicherheits- und Datenverschlüsselungs-Lösung für Festplatten in DriveLock integriert. DriveLock Disk Protection ist für folgende BIOS Versionen und Betriebssysteme einsetzbar:

- Legacy BIOS: Windows 7 SP1, Windows 8.1 und Windows 10, jeweils 32-bit/64-bit
- UEFI BIOS: Windows 10, nur 64-bit

DriveLock Disk Protection stellt die nachfolgenden Funktionen zur Verfügung.

Festplattenverschlüsselung

Disk Protection bietet eine sichere Datenverschlüsselung, die für den Benutzer vollkommen transparent ist und unbemerkt bleibt. Disk Protection ver- und entschlüsselt automatisch einzelne oder mehrere Festplatten-Partitionen. Wenn verschlüsselte Daten gelesen werden, entschlüsselt Disk Protection diese „on the fly“, so dass alle Programme und das Betriebssystem davon nichts mitbekommen. Alle Daten, die auf die Festplatte zurück geschrieben werden, werden ebenfalls wieder automatisch verschlüsselt. Somit bleiben die normalen System-Operationen unbeeinträchtigt.

Pre-Boot Benutzer Authentifizierung (PBA)

Die PBA dient der Anmeldung des Benutzers, bevor das Betriebssystem gestartet wird, damit die Betriebssystemdateien und der Rest der verschlüsselten Festplatte(n) entschlüsselt werden kann. Dafür verwaltet Disk Protection seine eigene Pre-Boot Benutzerdatenbank. Nach der Benutzer-Authentifizierung innerhalb der PBA kann die Festplatte entschlüsselt und das Betriebssystem geladen werden.

Diese Pre-Boot Benutzerdatenbank hat die folgenden Eigenschaften:

- Maximale Anzahl von Benutzern/Zertifikaten – 2.000
- Benutzername Länge/Syntax – 1 bis 20 Zeichen
- Passwort Länge/Syntax – bis zu 127 Groß-/Kleinbuchstaben (Kein Minimum, Windows-Passwortlänge)

Disk Protection kann die Pre-Boot Authentifizierung von Benutzern auf Einzelplatz (nur lokales Windows) und Windows Domänen Systemen vornehmen. Zusätzlich zur lokalen Passwort oder Domänen Passwort Anmeldung wird ebenfalls die Anmeldung mit Smart Card/Token und PIN Eingabe unterstützt.

Single Sign-On oder manuelle Windows Authentifizierung

Disk Protection kann so konfiguriert werden, dass Benutzer automatisch an Windows authentifiziert werden, nachdem eine erfolgreiche Pre-Boot Authentifizierung durchgeführt wurde. Diese Methode der automatischen Windows Authentifizierung wird als Single Sign-On bezeichnet. Als eine Alternative zum Single Sign-On Modus erlaubt es Disk Protection, den standardmäßigen Windows-Anmeldebildschirm anzuzeigen, um den Benutzer die manuelle Authentifizierung mit dem entsprechendem Windows (Domänen) Konto zu ermöglichen.

Notfall Wiederherstellung von Pre-Boot Benutzern und Token Anmeldungen

Disk Protection stellt Notfall Anmeldeverfahren zur Verfügung, damit sich Smartcard/Token oder Windows Domänen Benutzer einmalig an der Pre-Boot Anmeldung authentifizieren können, wenn z.B. das Passwort oder die PIN vergessen wurde. Vor einer Disk Protection Installation müssen Wiederherstellungsschlüssel erstellt werden. Diese werden dazu benötigt, um eine Notfall-Wiederherstellung von Daten oder ein Notfall Anmeldeverfahren vorzunehmen. Es gibt dazu verschiedene Schlüssel:

- *Hauptzertifikat (MSC = Master Security Certificate)* – Die DLFDEMaster.cer und DLFDEMaster.pfx Dateien ergeben ein öffentliches/privates Schlüsselpaar. DLFDEMaster.pfx wird dazu benutzt, um die Festplatten zu entschlüsseln. Die DLFDEMaster.pfx sollte geheim sein und als solche muss sie sicher gespeichert werden und nur durch die Personen zugreifbar sein, die eine Notfall-Wiederherstellung durchführen. DLFDEMaster.cer ist der öffentliche Schlüssel des Hauptzertifikates (MSC) und wird für jede Installation verwendet.
- *Wiederherstellungszertifikat (RSC = Recovery Support Certificate)* – Das DLFDERecovery.cer und DLFDERecovery.pfx ergeben ein öffentliches/privates Schlüsselpaar. DLFDERecovery.pfx wird für das Notfall Anmeldeverfahren verwendet. Die DLFDERecovery.pfx Datei sollte geheim sein, muss als solche sicher gespeichert werden und soltle nur durch die Personen verwendet werden, die eine Passwort Wiederherstellung durchführen müssen (z.B. Helpdesk/Support Personal). DLFDERecovery.cer ist die öffentliche Schlüssel Komponente des Wiederherstellungszertifikates (RSC) und wird für jede Installation verwendet.
- *Recovery Envelope* – Die RecoveryEnvelope.env Datei wird für jeden Client PC erstellt und wird für das Notfall Anmelde-Verfahren verwendet. Der Client Name ist Bestandteil des Dateinamens, wenn die Datei von Disk Protection automatisch zentrali n einem Share (anstatt dem zentralen DES) gespeichert wird und lautet wie folgt: <Computername>.Recovery.env.

Für Einzelplatz Installationen beginnt die Vorbereitung für die Notfall-Wiederherstellung mit regelmäßigen System-Sicherungen. Disk Protection erstellt Wiederherstellungs-Schlüssel, die später benutzt werden können, um ein defektes System zu entschlüsseln. Diese Schlüssel werden an den zentralen DES geschickt und sollten nicht auf dem Client System selbst gesichert werden. Die Sicherungsdateien, die erstellt und in Verbindung mit dem Hauptzertifikat (MSC) verwendet werden, dienen der Festplatten-Wiederherstellung. Disk Protection stellt ebenfalls ein Kommandozeilen-Wiederherstellungswerkzeug zur Verfügung, das dazu verwendet werden kann, um Notfall-Wiederherstellungsaufgaben, wie die Daten-Entschlüsselung durchzuführen. Das Wiederherstellungswerkzeug ist in der Disk Protection Installation enthalten und wird generell nur vom System Administrator verwendet.

Notfall Wiederherstellungs- und Administrationstools

Verschiedene administrative Tätigkeiten, die sich nicht auf die Disk Protection beziehen, können einen automatischen Neustart gefolgt von einer automatischen Pre-Boot Authentifizierung notwendig machen. Disk Protection stellt diese Funktion mit Hilfe eines speziellen Benutzerkontos zur Verfügung. Dazu kann ein spezielles Kommandozeilen-Programm verwendet werden notwendig, um eine gewünschte Anzahl von Autologon-Anmeldungen einzustellen.

Disk Protection stellt Tools zur Verfügung, um im Falle einer defekten Festplatte Daten auf dieser Festplatte wieder zu entschlüsseln.

6.1 Vorbereitung der DriveLock Disk Protection

Überprüfen Sie die folgenden Punkte und stellen Sie sicher, dass Sie die notwendigen Schritte vor der Installation von Disk Protection ausgeführt haben.

Bevor Disk Protection verteilt wird, haben sich die folgenden Punkte als hilfreich herausgestellt:

- Defragmentieren Sie alle Laufwerke, die von Disk Protection verschlüsselt werden sollen.

- Stellen Sie sicher, dass das Speichersystem gut geplant ist und keine weiteren Änderungen irgendwelcher Partitionen nötig wird. Falls nötig, nutzen Sie die Windows Datenträgerverwaltung, um Laufwerks-Spiegelungen, Partitionsgrößen etc. einzurichten.
- Verwenden Sie CHKDSK /f und die Festplatten-Hersteller-Diagnosetools, um die Integrität des Dateisystems aller Laufwerke sicherzustellen, die Sie zu verschlüsseln beabsichtigen. Reparieren Sie alle fehlerhafter Sektoren, falls welche existieren, da Disk Protection diese sonst nicht verschlüsseln kann.
- Sichern Sie alle wichtigen Daten vor der Laufwerks-Verschlüsselung.
- Deaktivieren Sie während der Installation der DriveLock Disk Protection den DriveLock Application Launch Filter (Applikationskontrolle, Whitelist-Modus), um die Ausführung von gesperrten Applikationen zu verhindern.

Die Werkzeuge, die von den Festplatten-Herstellern zur Verfügung gestellt werden, sind typischerweise die robustesten Werkzeuge, um Laufwerksfehler zu beheben.

Schrittweise Einführung

Für die Einführung der Disk Protection hat sich folgende Vorgehensweise bewährt:

1. Planung des Konzepts zum Emergency Logon und zur Datenwiederherstellung:

   Machen Sie sich mit der Funktionsweise und den Möglichkeiten der Recovery-Mechanismen der DriveLock Disk Protection vertraut und lernen Sie die beiden verschiedenen Recovery-Dateien und deren Ablagemöglichkeiten kennen. Die Verfügbarkeit und Sicherung dieser Dateien ist eine unabdingbare Voraussetzung dafür, um später erfolgreich bei vergessenen Passwörtern oder beschädigten Festplatten das System erfolgreich wiederherzustellen.

2. Durchführung von Tests auf ausgewählten Systemen in einer Testumgebung:

   Die innerhalb der DriveLock Disk Protection integrierten Komponenten wurden ausführlich auf verschiedensten Computersystemen und Laptops auf korrekte Funktionsfähigkeit getestet. Durch die sehr Hardware-nahe Programmierung sind jedoch Inkompatibiltäten nie ganz auszuschließen.

Um eine reibungslose Einführung vorzubereiten, raten wir dringend dazu, die Verschlüsselung zunächst auf Referenzsystemen zu testen, um zum Beispiel mögliche Inkompatibilitäten mit älterer oder ganz neuer Hardware auszuschließen.

3. Generierung der zentralen Recovery-Zertifikate und Sicherung dieser Zertifikate:

   Zunächst müssen die zentralen Zertifikate generiert werden, die für alle Recovery-Mechanismen benötigt werden. Stellen Sie sicher, dass Sie diese zusätzlich zu den von DriveLock angebotenen Möglichkeiten sichern bzw. aufbewahren, z.B. auf einer Smartcard.

4. Rollout und Installation der Software planen:

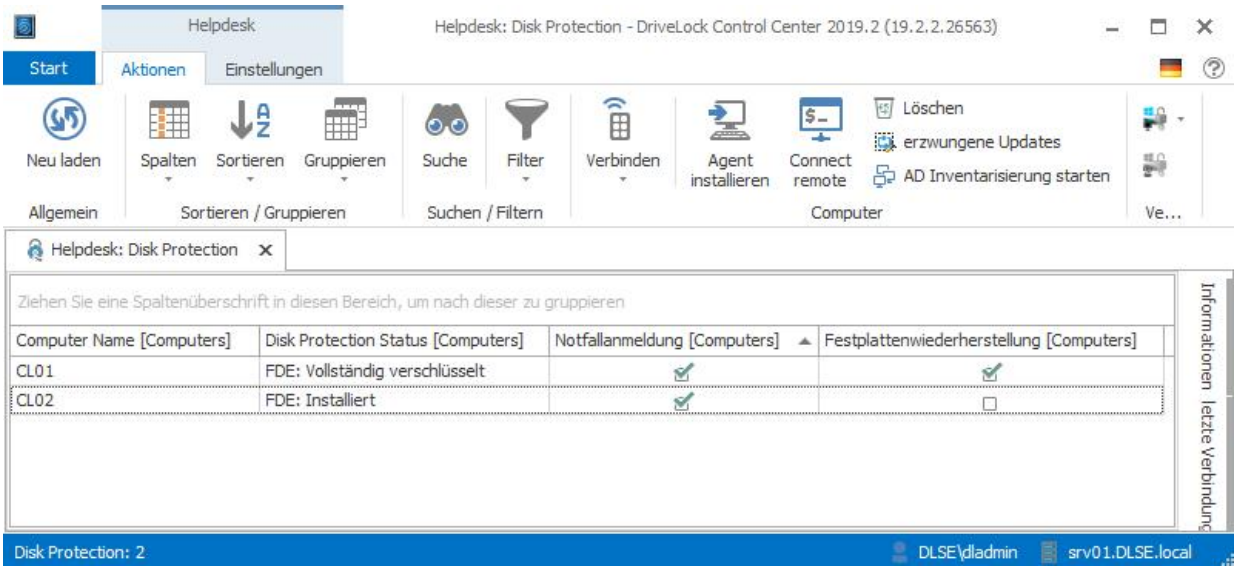
   Planen Sie die Installation der DriveLock Disk Protection im Voraus. Möglicherweise ist eine stufenweise Einführung mit Begleitung der betroffenen Benutzer eine für Sie geeignete Alternative.

5. Disk Protection Installationsparameter (inklusive der Recovery-Parameter der Verschlüsselung) konfigurieren und Disk Protection auf den Client Systemen installieren:

   Zunächst ist es möglich, die Software auf allen Clients zu installieren, ohne dass bereits die Pre-Boot Authentisierung oder sogar die Verschlüsselung aktiviert wird. Nach erfolgreicher Installation generiert jeder Client die individuelle sogenannte Envelope-Datei, die z.B. bei vergessenen Passwörtern für ein Emergency-Logon Recovery benötigt wird. Planen Sie hier ggf. einen Neustart des Rechners mit ein.

6. Kontrolle, ob alle Envelope-Dateien für das Emergency-Logon an den DES gesendet oder an zentraler Stelle gespeichert wurden:

Stellen Sie sicher, dass die individuellen Envelope-Dateien für alle installierten Systeme vorhanden und an zentraler Stelle außerhalb der installierten Clients abgesichert zugänglich sind. Die Verwendung des DriveLock Enterprise Services an dieser Stelle bringt nicht nur den Vorteil einer automatisierten zentralen Speicherung dieser Dateien, über das DriveLock Control Center lässt sich auch sehr einfach die Vollständigkeit und Verfügbarkeit ermitteln.



7. Pre-Boot Authentisierung konfigurieren (ggf. auch Notfall-Konto erstellen) und aktivieren:

Die Pre-Boot Authentisierung ist eigentlich der einzige, jedoch bedeutsamste Punkt, an dem die betroffenen Benutzer mit der Einführung der DriveLock Disk Protection konfrontiert werden, da ab diesem Zeitpunkt bereits kurz nach dem Systemstart eine Anmeldung erfolgt, die sich auch optisch von der Windowsanmeldung unterscheidet. Ein zentrales Notfallkonto, welches kein aktives Benutzerkonto in einer Windows-Domäne sein muss, sollte an dieser Stelle bereits eingerichtet werden, sofern ein derartiges Konto für bestimmte Prozesse (z.B. erstmalige Pre-Boot Authentifizierung, Anmeldungshilfe,...) verwendet werden soll.

8. Einführung der Pre-Boot Authentisierung bei den Benutzern begleiten:

Gerade hier kann eine Unterstützung der Benutzer dabei helfen, den Umgang mit der neuen Situation zu meistern. Gleichzeitig macht sich an dieser Stelle dann auch schon bezahlt, wenn die Verfahren zum Emergency-Logon Recovery beim Benutzer und den Administratoren bekannt und geläufig sind.

9. Konfiguration der Verschlüsselungsparameter und Aktivierung der Verschlüsselung

Die Aktivierung der eigentlichen Datenverschlüsselung ist einer der letzten Punkte, die bei einer stufenweisen Einführung umgesetzt werden. Nach der Aktivierung beginnt der einzelne Client im Hintergrund damit, die Daten auf der bzw. den Festplatten zu verschlüsseln. Bis diese Verschlüsselung vollständig durchgeführt ist, werden etwas mehr Systemressourcen als später im laufenden Betrieb benötigt und der Benutzer kann diese Verzögerung insbesondere bei zugriffsintensiven Anwendungen oder Aktionen bemerken. Nach erfolgreicher Verschlüsselung generiert jeder Client die individuelle sogenannte Daten-Recovery-Datei, die bei einer Wiederherstellung verschlüsselter Daten benötigt wird.

10. Kontrolle, ob alle Daten-Recovery-Dateien (*backup.zip*) zentral an den DES gesendet oder in einer Datei gespeichert wurden:

Stellen Sie wiederum sicher, dass die individuellen Daten-Recovery-Dateien für alle installierten Systeme vorhanden und an zentraler Stelle außerhalb der verschlüsselten Clients abgesichert zugänglich sind. Die

Verwendung des DriveLock Enterprise Servers an dieser Stelle bringt wiederum den Vorteil einer automatisierten zentralen Speicherung dieser Dateien, über das DriveLock Control Center lässt sich auch sehr einfach die Vollständigkeit und Verfügbarkeit ermitteln.

Im neuen DriveLock Operations Center werden noch nicht alle für Disk Protection relevanten Informationen korrekt angezeigt, daher verwenden Sie bitte das DriveLock Control Center für die Disk Protection.

Stellen Sie auch sicher, dass diese Dateien, die für Notfall-Anmeldung und Daten-Wiederherstellung verwendet werden, zusätzlich gesichert werden. Bitte sichern Sie die DES-Datenbank, sofern Sie die Recovery-Dateien im DES speichern (Standard).

6.2 Grundsätzliche Konfiguration der Disk Protection

Zunächst müssen einige grundsätzliche Einstellungen vorgenommen werden:

- Lizenzierung
- Generierung der Wiederherstellungsschlüssel

Klicken Sie innerhalb der Richtlinie auf Verschlüsselung und scrollen zum unteren Ende der Taskpad-Ansicht, bis Sie den Bereich **Disk Protection** vollständig sehen.

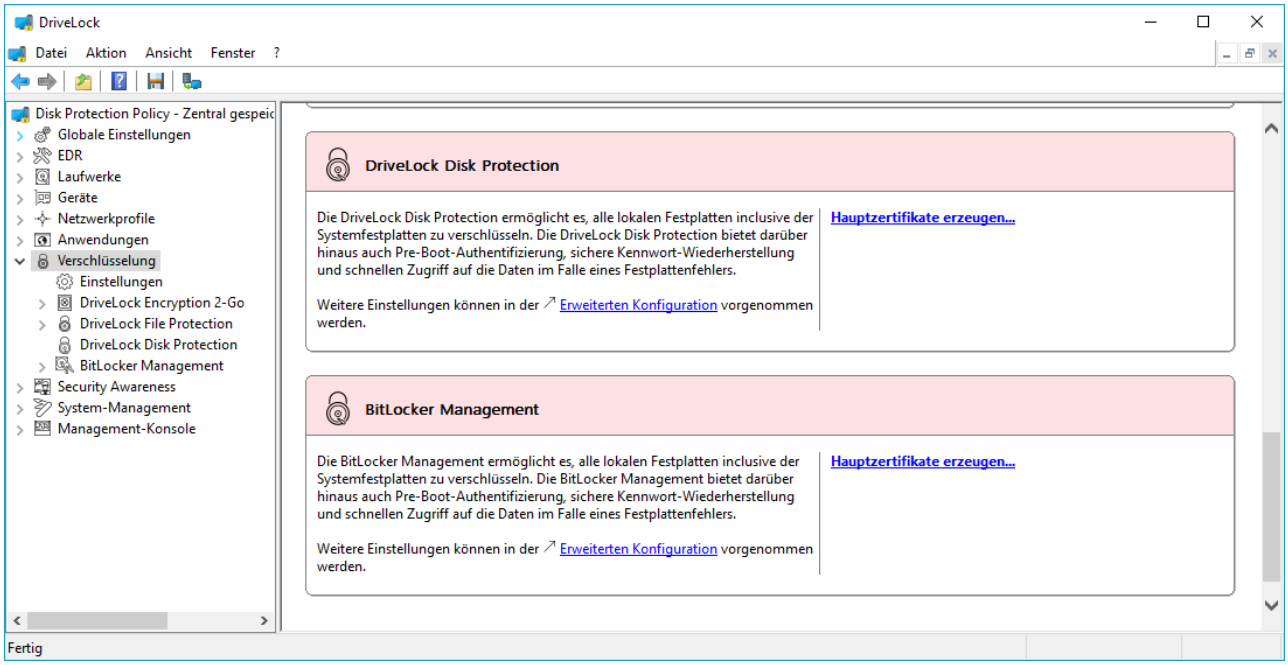
6.2.1 Erstellen der Wiederherstellungs-Schlüssel

Vor einer Disk Protection Installation müssen Zertifikate für die Datenwiederherstellung erstellt werden. Diese Dateien werden dazu benötigt, um ein Notfall-Recovery oder ein Notfall-Anmeldeverfahren vorzunehmen. Folgende Zertifikate müssen erstellt werden:

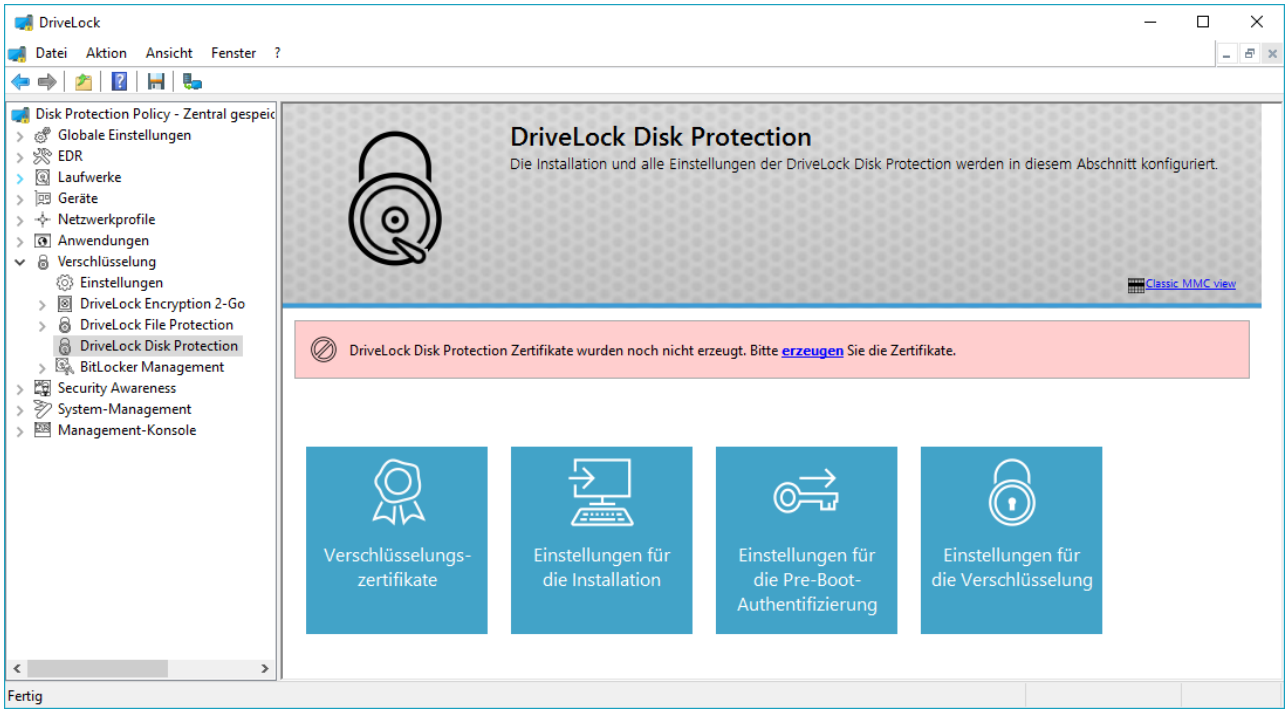
- *Hauptzertifikat (MSC = Master Security Certificate)*: Die DLFDEMaster.cer und DLFDEMaster.pfx Dateien ergeben ein öffentliches/privates Schlüsselpaar. DLFDEMaster.pfx wird dazu benutzt, um die Festplatten zu entschlüsseln. Die DLFDEMaster.pfx sollte geheim sein und als solche muss sie sicher gespeichert werden und nur durch Einzelne zugreifbar sein, die eine Notfall-Wiederherstellung durchführen. DLFDEMaster.cer ist der öffentliche Schlüssel des Hauptzertifikates (MSC) und wird automatisch für jede Installation verwendet.
- *Wiederherstellungszertifikat (RSC = Recovery Support Certificate)*: Das DLFDERecovery.cer und DLFDERecovery.pfx ergeben ein öffentliches/privates Schlüsselpaar. DLFDERecovery.pfx wird für das Notfall-Anmeldeverfahren verwendet. Die DLFDERecovery.pfx Datei sollte geheim sein und als solche muss sie sicher gespeichert werden und nur durch Einzelne zugreifbar sein, die eine Passwort Wiederherstellung durchführen (z.B. Helpdesk/Support Personal). DLFDERecovery.cer ist die öffentliche Schlüssel Komponente des Wiederherstellungszertifikates (RSC) und wird automatisch für jede Installation verwendet.

Ohne die Wiederherstellungs-Schlüssel und der Passwörter werden Sie nicht in der Lage sein, irgendwelche Daten wiederherzustellen oder Benutzern zu helfen, ihr Passwort zurückzusetzen.

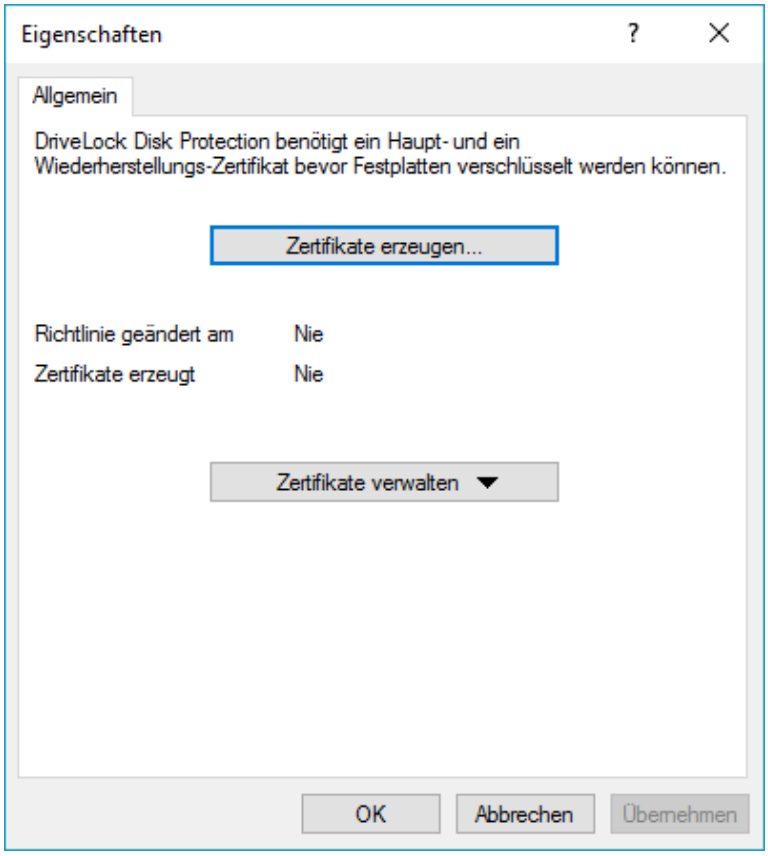
Wenn Sie Disk Protection das erste Mal starten, wurden die Hauptzertifikate und Schlüssel noch nicht erstellt.



Klicken Sie auf **Hauptzertifikate erzeugen**, um neue Verschlüsselungszertifikate zu erzeugen. Es startet direkt der Assistent zum Erstellen der Zertifikate.

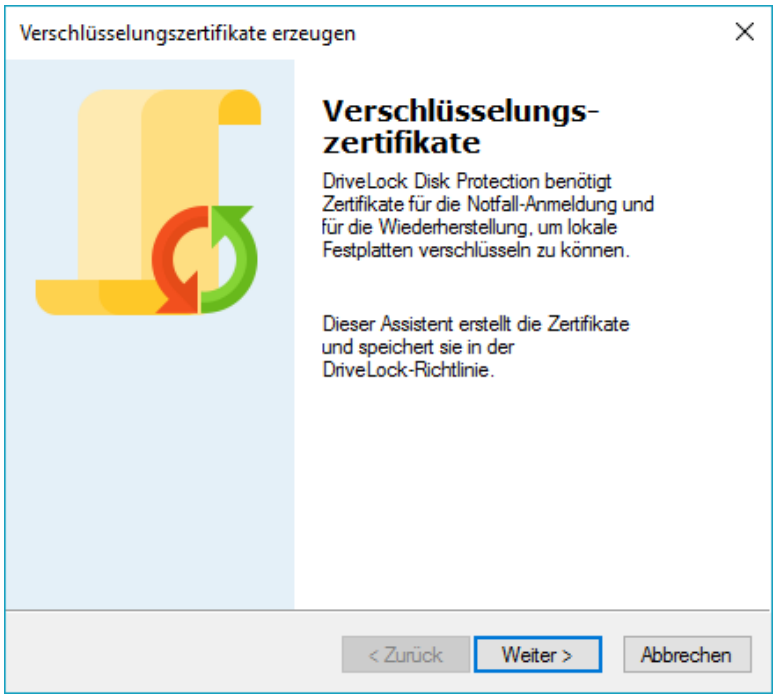


Ebenso können SIe links auf **DriveLock Disk Protection** und dann auf **Verschlüsselungszertifikate** klicken.

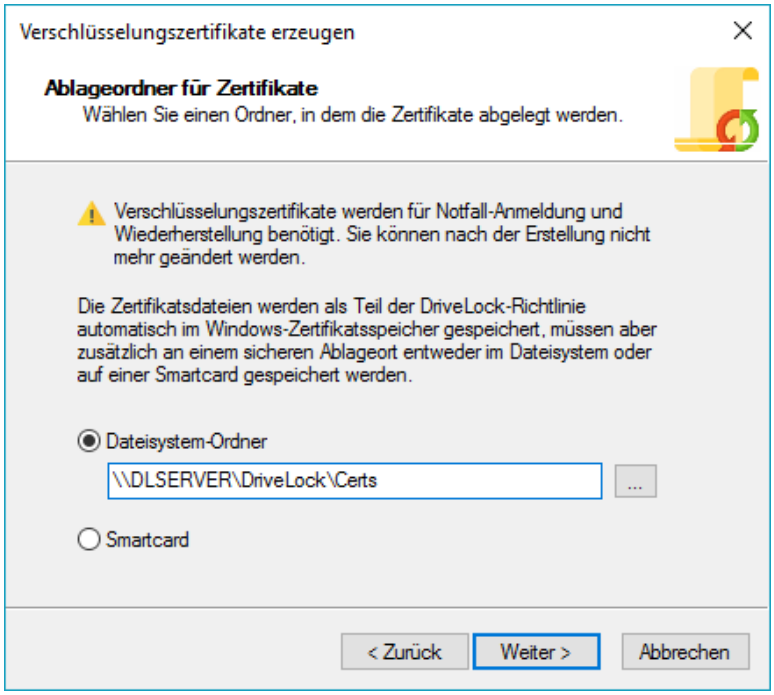


Klicken Sie nun auf **Zertifikate erzeugen**, um den Assistenten zur Erzeugung der Zertifikarte zu starten.

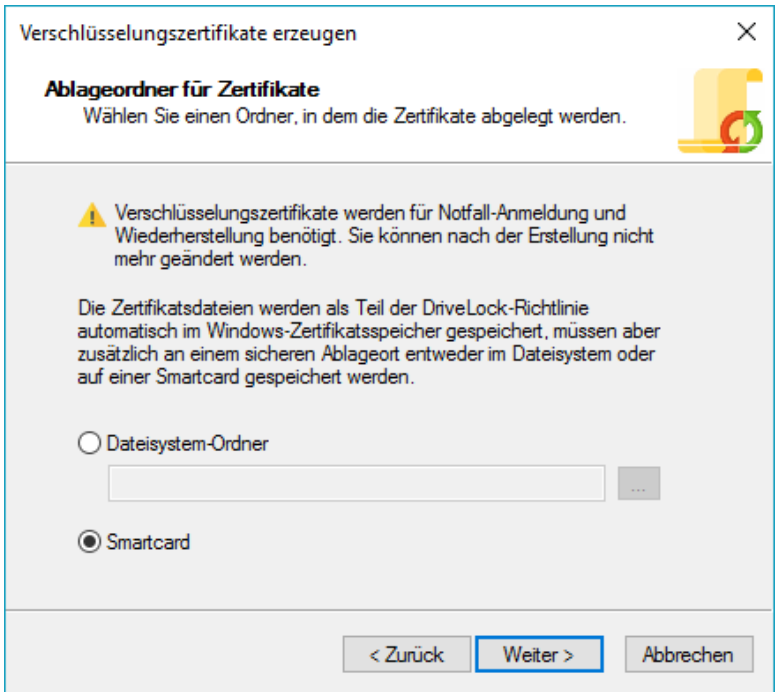
Erzeugen der Verschlüsselungszertifikate



Klick auf **Weiter**.



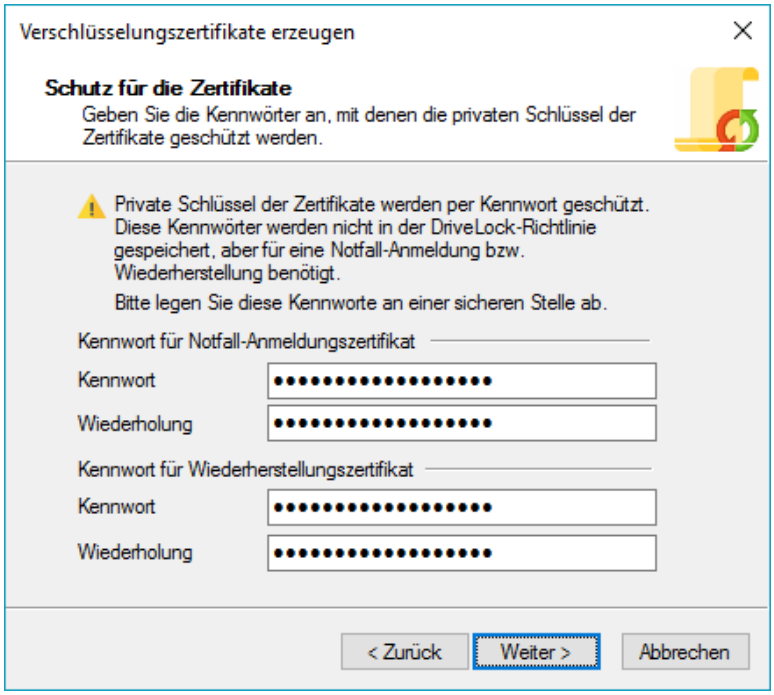
Geben Sie entweder den Ordner an, wo Sie die Zertifikats-Dateien abspeichern möchten oder wählen Sie alternativ eine Smartcard als Speicherort.



Klicken auf **Weiter**.

Sofern Sie eine Smartcard zur Speicherung verwenden, werden Sie abhängig von der verwendeten Karte nun gebeten, die Karte einzulegen und auszuwählen.

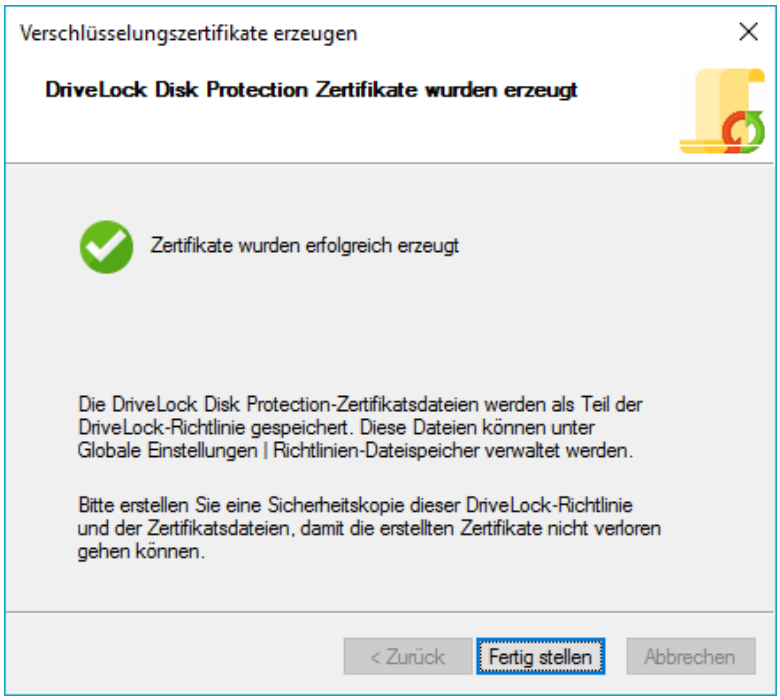
Stellen Sie sicher, dass diese Dateien zusammen mit dem Passwort an einem sicheren Ort abgespeichert werden, da sie für Notfall-Anmeldung und Daten-Wiederherstellung verwendet werden. Eine Wiederherstellung ohne diese Daten ist nicht möglich.



Geben Sie die Passwörter für das Haupt- und Wiederherstellungszertifikat an. Sie müssen jedes Passwort aus Sicherheitsgründen zweifach eingeben. Um Fortzufahren, klicken Sie auf **Weiter**.

Es dauert einige Sekunden, um die Hauptzertifikate zu erzeugen. Anschließend werden Sie benachrichtigt, wenn der Prozess abgeschlossen ist und die Dateien an dem zuvor angegebenen Ort abgespeichert wurden.

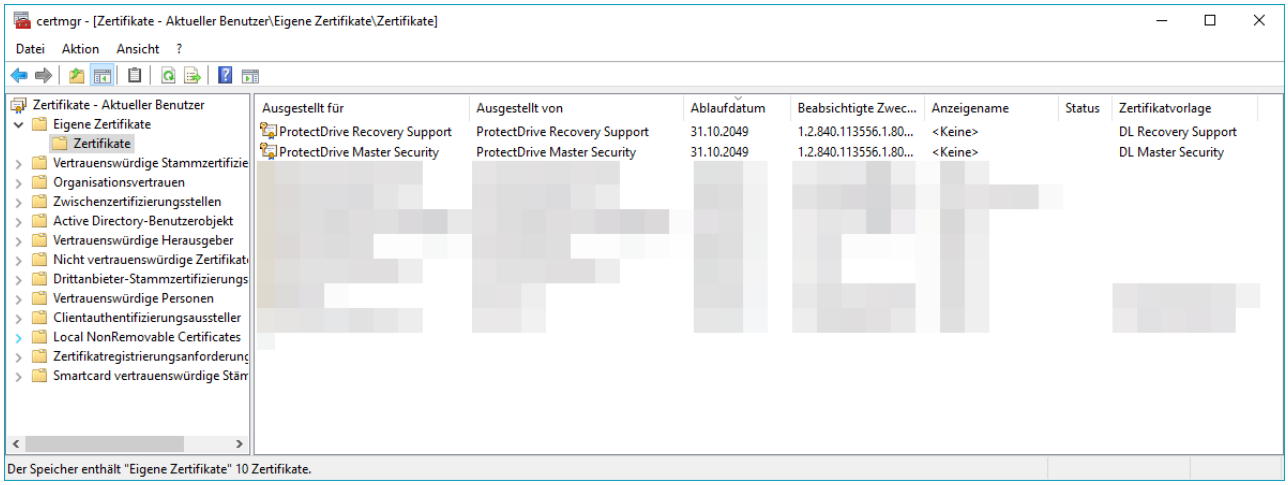
Sofern eine Smartcard zur Speicherung verwendet wird, werden Sie aufgefordert, die PIN für den Zugriff auf die Smartcard einzugeben.



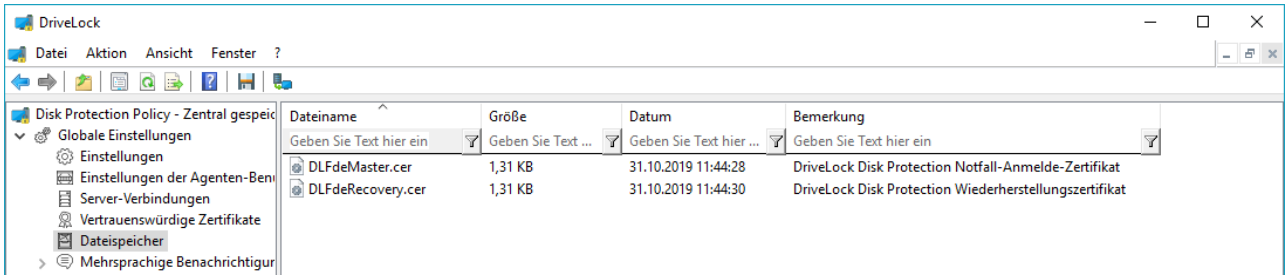
Klicken Sie auf **Fertig stellen**.

Wenn die Verschlüsselungszertifikate erzeugt wurden, zeigt die DriveLock Management Konsole die Erstellungszeit und das Datum an.

Die Zertifikate werden ebenfalls in dem privaten Zertifikatsspeichers des aktuellen Benutzers gespeichert:



Die beiden öffentlichen Schlüssel werden auch innerhalb des DriveLock Richtlinien-Dateispeichers abgelegt:

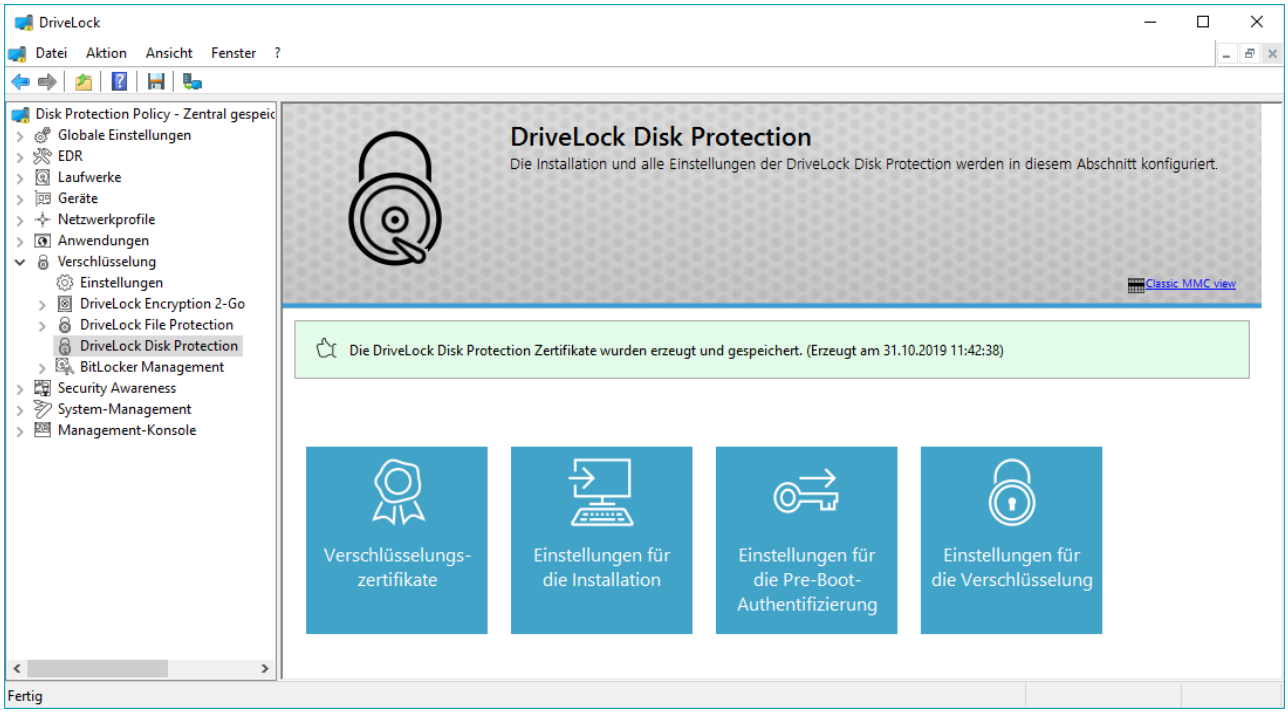


Sobald die Zertifikate erzeugt und die Disk Protection auf den Client Computern installiert wurde, dürfen keine neuen Zertifikate mehr erstellt werden, da die alten damit überschrieben und somit für eine Wiederherstellung nicht mehr verwendet werden können.

Wenn Sie den Erstellungs-Assistenten abgebrochen haben oder es während der Erstellung zu einem Problem gekommen ist, wird DriveLock die entsprechende Meldung anzeigen und Sie müssen die Dateien neu erzeugen.

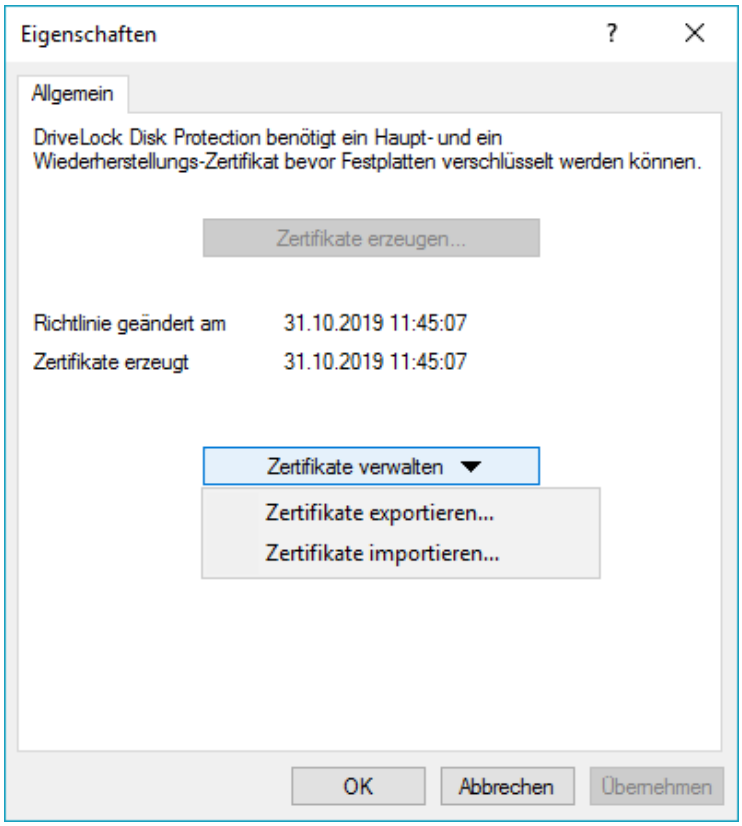
6.2.2 Exportieren und Importieren von Verschlüsselungszertifikaten

Wenn Sie die Hauptzertifikate erstellt haben, können Sie die öffentlichen Schlüssel aus dem DriveLock Richtlinien-Dateispeicher exportieren.



Klicken Sie dazu auf **Verschlüsselungszertifikate** in der DriveLock Management Konsole.

Importieren Sie Hauptzertifikate nur, wenn Sie genau wissen was Sie tun. Ein Szenario ist die Wiederherstellung einer Konfiguration. Dort müssen die gleichen Zertifikate verwendet werden. Ein weiteres Szenario wäre der Aufbau einer komplett identischen Konfiguration. Ein nachträgliches Ändern der Zertifikate, auf bereits installierten und verschlüsselten DiskProtection-Clients wird nicht unterstützt.



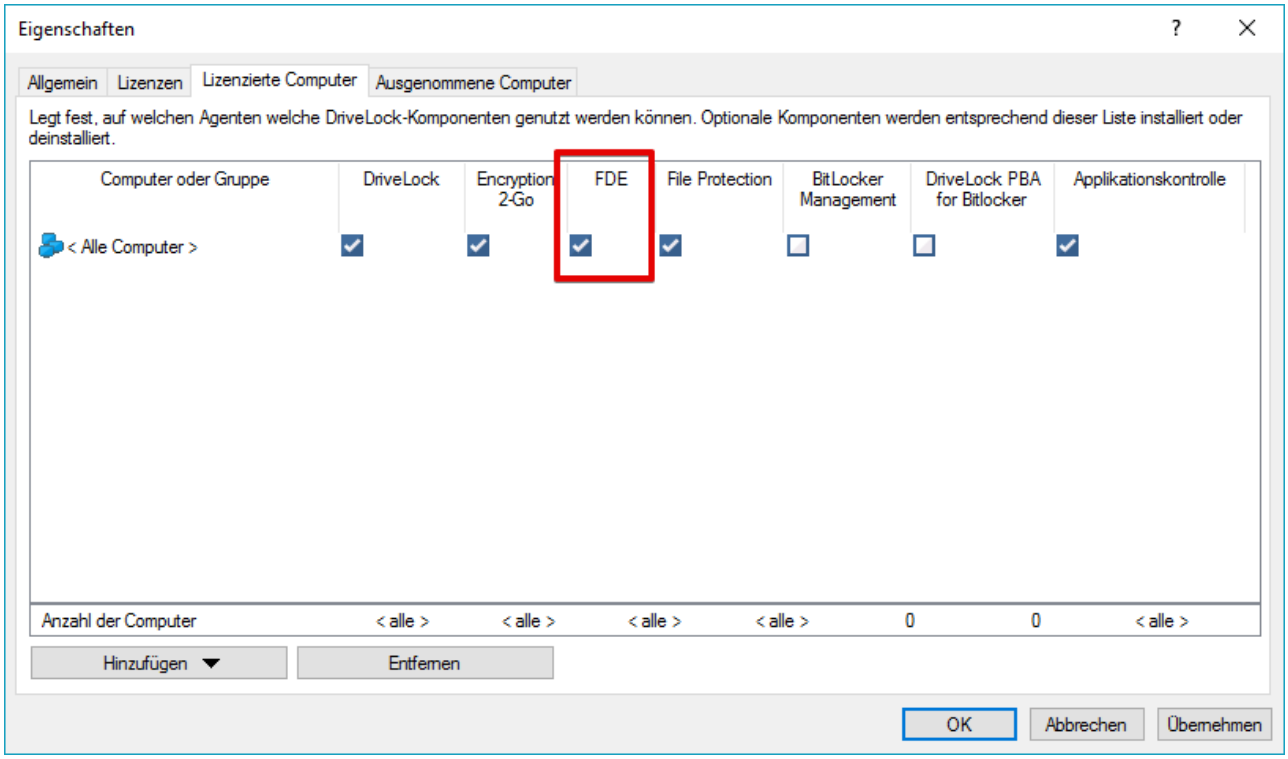
Um die zwei Zertifikate zu exportieren, klickt man auf **Zertifikate verwalten** und wählt aus dem Drop-Down Menü *Hauptzertifikate exportieren* aus. Wählen Sie ein Verzeichnis, um die Dateien zu speichern.

Zertifikate, die zuvor an einem anderen Ort erstellt wurden, können auch in den DriveLock Richtlinien-Dateispeicher importiert werden.

Um die zwei öffentlichen Schlüssel zu importieren, klickt man auf **Zertifikate verwalten** und wählt aus dem Drop-Down Menü *Hauptzertifikate importieren* aus. Wählen Sie das Verzeichnis, das die beiden Zertifikats-Dateien enthält.

6.2.3 Lizenzeinstellungen

Sobald ein Computer, auf dem der DriveLock Agent bereits installiert ist, für Disk Protection lizenziert ist, werden alle benötigten extra Dienste und Schnittstellen installiert. Die Freischaltung erfolgt über die Lizenz (unter *Globale Einstellungen – Lizenz*) durch Setzen des Hakens in der Spalte FDE:



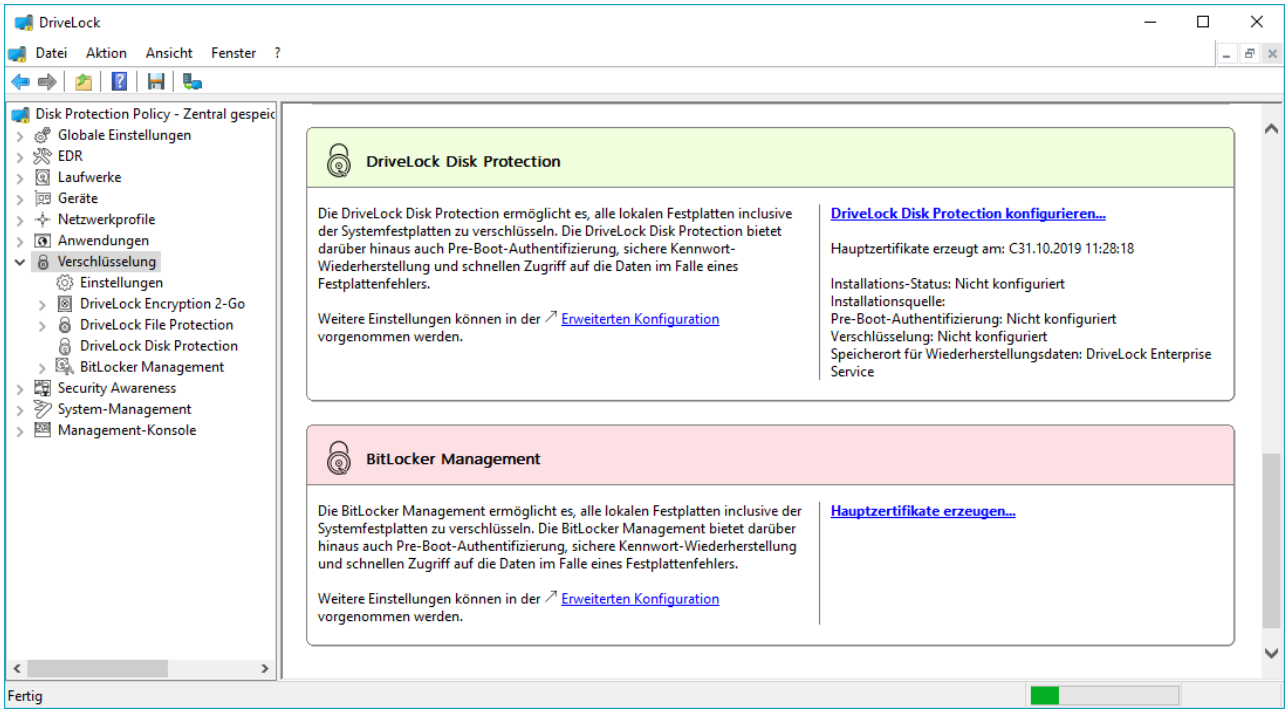
Die Installation wird ausschließlich über die Lizenz gesteuert.

Wenn der Haken bei FDE nicht gesetzt werden kann, enthält Ihre Lizenz vermutlich nicht das Modul für FDE. Bitte setzen Sie sich in diesem Fall mit Ihrem Vertriebspartner in Verbindung.

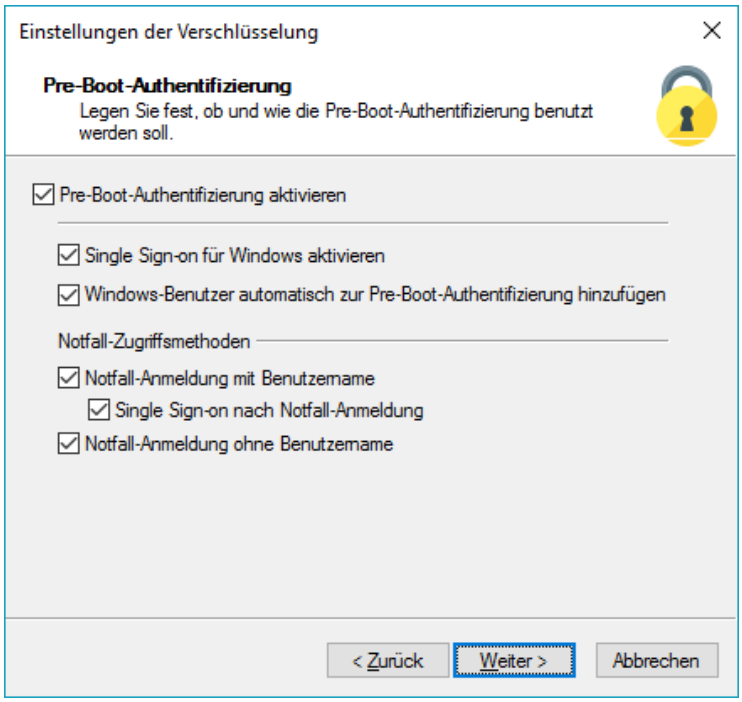
Disk Protection kann auf die gleiche Weise deinstalliert werden. Durch entfernen des Hakens bei FDE ist ein Client nicht mehr lizenziert und dieser beginnt mit der Deinstallation von DriveLock Disk Protection. Diese Deinstallation kann durch eine Einstellung um bis zu 3 Tage verzögert werden.

6.2.4 Disk Protection Einstellungen

In diesem Abschnitt wird gezeigt, wie die wichtigsten Einstellungen in der Basiskonfiguration vorgenommen werden können. Alle zusätzlichen Einstellungsmöglichkeiten werden im darauf folgenden Abschnitt beschrieben.



Öffnen Sie **Verschlüsselung** und klicken Sie auf **DriveLock Disk Protection konfigurieren**, um die grundlegenden Einstellungen für die DriveLock Disk Protection vorzunehmen.



Um die Pre-Boot-Authentifizierung auf Ihren Client-Computern zu aktivieren, wählen Sie *„Pre-Boot-Authentifizierung aktivieren“*.

> Sobald der DriveLock Agent die neue Konfiguration erhält, wird die Pre-Boot-Authentifizierung aktiviert. Stellen Sie sicher, dass alle anderen Parameter innerhalb des Dialoges konfiguriert wurden und Ihre Benutzer über die Änderung informiert sind. Der Benutzer bekommt eine Nachricht angezeigt, wenn die PBA aktiviert wurde.

Um die Disk Protection ohne Deinstallation zu deaktivieren, wählen Sie diese Checkbox ab. Alle Punkte der Disk Protection inklusive der Festplatten Verschlüsselung werden deaktiviert. Wenn diese Checkbox nicht markiert ist,

können Änderungen anderer Einstellungen innerhalb des Dialoges gemacht werden, aber die Änderungen treten nicht in Kraft, bis die Disk Protection wieder über die Checkbox *„Pre-Boot-Authentifizierung aktivieren“* aktiviert wird.

Um Zugriff auf ein System zu bekommen welches durch die Disk Protection geschützt ist, ist eine Authentifizierung sowohl an der Pre-Boot-Authentifizierung als auch der Windows Zugriffsebene notwendig.

Im Single Sign-on Modus muss sich ein Benutzer für beide Ebenen (Pre-Boot und Windows) nur einmal anmelden. Diese Option ist nur verfügbar, wenn die Authentifizierung für beide Pre-Boot und Windows Zugriffsebenen für mindestens eine gleiche Authentifizierungs-Methode aktiviert ist.
Markieren Sie *“Single Sign-on für Windows aktivieren“*, um diesen Modus zu aktivieren.

Standardmäßig fügt die Disk Protection jeden Benutzer zur Pre-Boot Datenbank hinzu, wenn dieser erfolgreich an Windows angemeldet werden konnte. Entfernen Sie den Haken *„Single Sign-on für Windows aktivieren*“, wenn die Benutzer nicht automatisch hinzugefügt werden sollen.

Die Notfall-Anmeldung ist verfügbar, wenn diese auf der Pre-Boot Ebene aktiviert wurde.

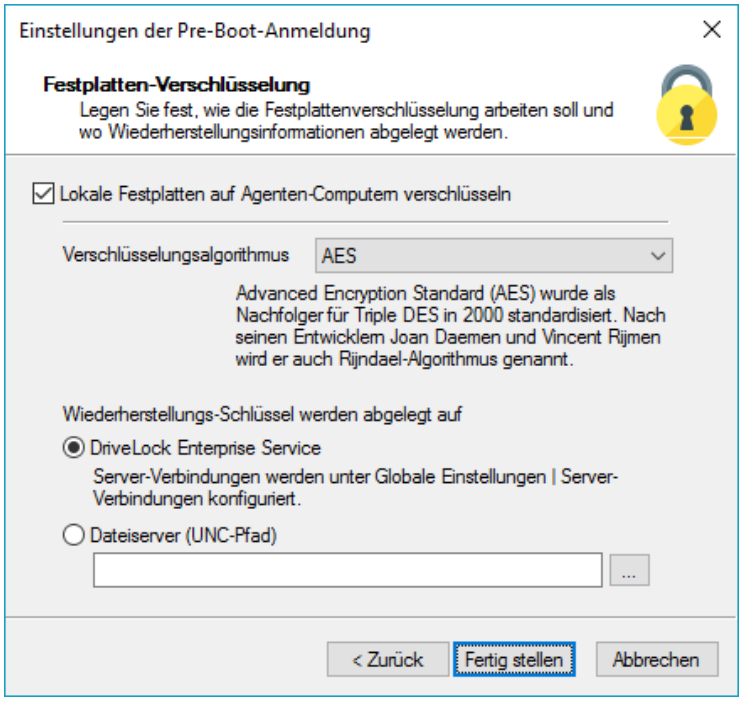
Notfall-Anmeldung mit Benutzername – Falls aktiviert, erlaubt die Option dem Benutzer das Verfahren *Notfall-Anmeldung mit Benutzername* aufzurufen. Es wird in dem Fall verwendet, wenn der Benutzer sein Pre-Boot Authentifizierungs-Passwort (nicht die PIN) vergessen hat. Das betrifft Windows-Domänen oder lokale Windows-Benutzer Passwort-Accounts, die der Disk Protection Benutzerdatenbank hinzugefügt wurden. Es erlaubt einen einmaligen Pre-Boot Zugriff auf das System.

> Dieses Feature setzt voraus, dass sich ein Benutzer zuvor mindestens einmal erfolgreich an der Pre-Boot Authentifizierung angemeldet hat, bevor es von diesem Benutzer aufgerufen werden kann. Wenn ein Benutzer sich noch nie angemeldet hat, muss er das Verfahren Notfall Anmeldung ohne Benutzername aufrufen.

- *Single Sign-on nach Notfall-Anmeldung*: Falls aktiviert, erlaubt die Option es dem Benutzer sich sofort automatisch an Windows zu authentifizieren, eine erfolgreiche Anwendung des Verfahrens Notfall Anmeldung mit Benutzername vorausgesetzt.

Notfall-Anmeldung ohne Benutzername – Falls aktiviert, können neu erstellte Windows-Domänen oder lokale Windows-Benutzer das Verfahren Notfall-Anmeldung ohne Benutzername aufrufen. Das erlaubt einen einmaligen Pre-Boot Zugriff auf das System für alle Benutzer, die noch niemals am System angemeldet waren.

Klicken Sie auf **Weiter** um fortzufahren.



Um generell die Festplatten Verschlüsselung zu aktivierten, wählen Sie die Option *"Lokale Festplatten auf Agenten-Computer verschlüsseln"* aus.

> In Abhängigkeit der Laufwerksgröße kann die Ver- bzw. Entschlüsselung einige Zeit in Anspruch nehmen. Der Rechner kann während dieser Zeit jedoch weiterhin verwendet werden, eine geringfügige Beeinträchtigung der Systemleistung ist denkbar. Ebenfalls kann der Rechner in dieser Phase heruntergefahren oder neu gestartet werden. In diesem Fall wird der Vorgang im Anschluss fortgesetzt. Der aktuelle Stand der Verschlüsselung auf einem Rechner kann über die DriveLock Management Konsole überprüft werden, indem Sie sich mit dem Agenten verbinden und sich dessen Eigenschaften anzeigen lassen.

Sie können zwischen verschiedenen unterschiedlichen Verschlüsselungs-Algorithmen auswählen, allerdings empfehlen wir die Auswahl *AES* (AES 256-bit).

> Die Wiederherstellungsdaten werden sofort, nachdem der Agent die Disk Protection auf dem Client-Computer installiert hat, erstellt und zu dem nachfolgend angegebenen Ort gesendet.

Die Wiederherstellungs-Dateien sollten entweder im DriveLock Enterprise Server (empfohlen) oder einer zentralen Dateifreigabe gespeichert werden.

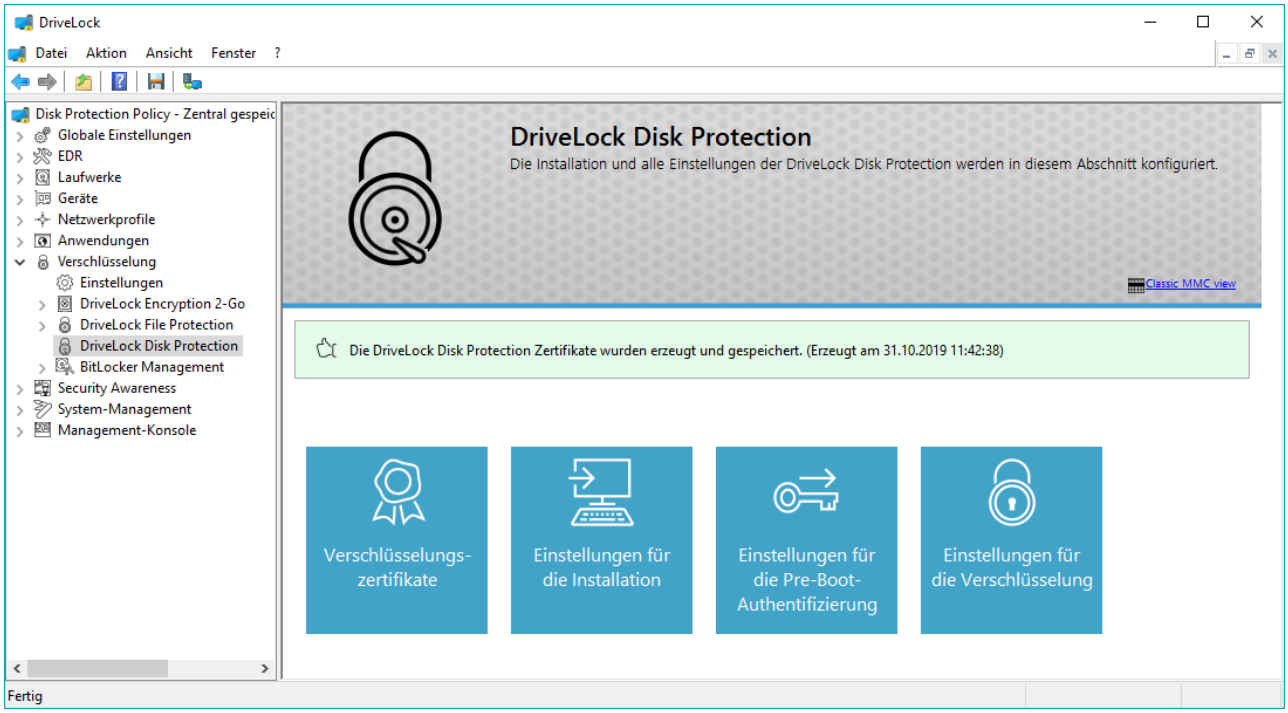
> Wenn die Dateien auf einer zentralen Dateifreigabe gespeichert werden, sind die Dateinamen wie folgt: *<Computer>.envelope.env* und *<Computer>.backup.zip.*

6.3 Weitere Konfigurationseinstellungen

Dieser Abschnitt behandelt alle Einstellungsmöglichkeiten der DriveLock Disk Protection für die

- Installation der Software
- Die Pre-Boot Authentifizierung PBA
- Die Verschlüsselung der Festplatten

Alle Einstellung können in der DriveLock Management Konsole über den Menüpunkt *DriveLock Disk Protection* vorgenommen werden:



6.3.1 Einstellungen für die Installation

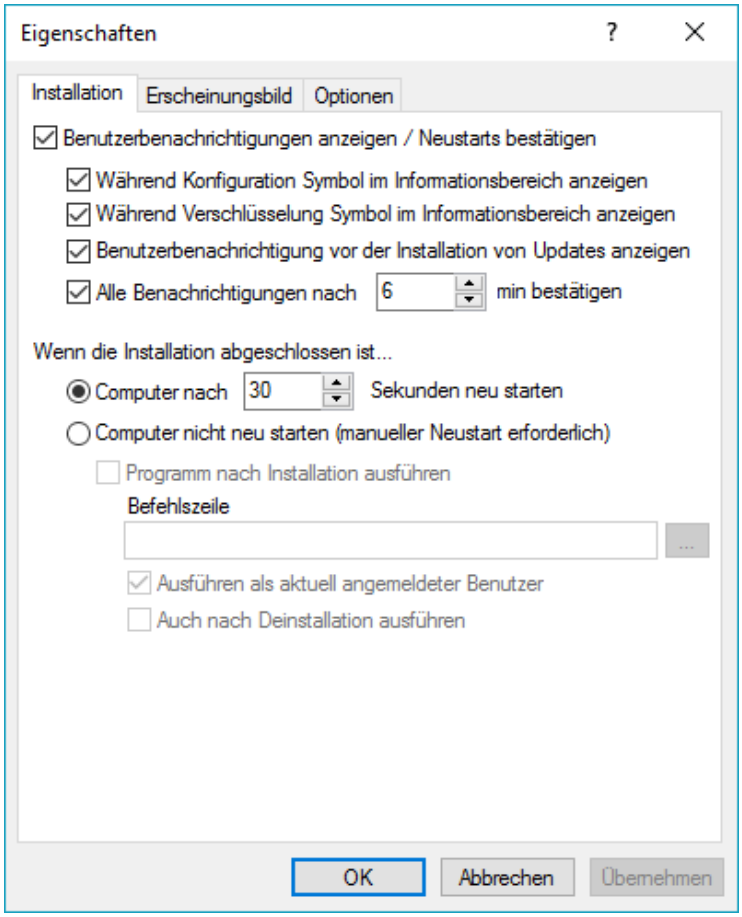
Nachdem die Verschlüsselungszertifikate erstellt wurden, können die Disk Protection Einstellungen für die Installation angepasst werden.

Bevor Sie die Einstellungen für die Installation festlegen, sollten Sie festlegen, wo DriveLock die für die Notfallanmeldung benötigten Wiederherstellungsdaten (Envelope-Datei) speichern sollen, die am Ende der Disk Protection Installation automatisch für jeden Rechner individuell erstellt werden.

Klicken Sie dazu auf **Einstellungen für die Verschlüsselung**. Die weiteren Schritte sind im Abschnitt „Ablage der Wiederherstellungs-Dateien festlegen“ beschrieben.

Konfiguration der Installationsparameter

Klicken Sie **Einstellungen für die Installation**, damit sich das dazugehörige Dialogfenster öffnet. Wählen Sie den Reiter *Installation* (falls dieser nicht aktiv ist).



Wenn Sie generell nicht möchten, dass Nachrichten auf dem Client-Computer angezeigt werden, während Disk Protection installiert wird, wählen Sie *„Benutzerbenachrichtigungen anzeigen / Neustarts bestätigen“* ab.

Ansonsten können Sie die einzelnen Optionen getrennt festlegen:

- Sie können die Anzeige eines Symbols unterbinden/aktivieren, das während der Installation im Informationsbereich angezeigt wird.
- Sie können die Anzeige eines Symbols unterbinden/aktivieren, das während der Verschlüsselung im Informationsbereich angezeigt wird.
- Sie können Benutzerbenachrichtigungen vor der Installation eines Disk Protection Updates anzeigen lassen bzw. unterbinden.
- Zusätzlich können Sie auswählen, ob angezeigte Nachrichten automatisch nach einer gewissen Anzahl von Minuten bestätigt werden oder nicht.

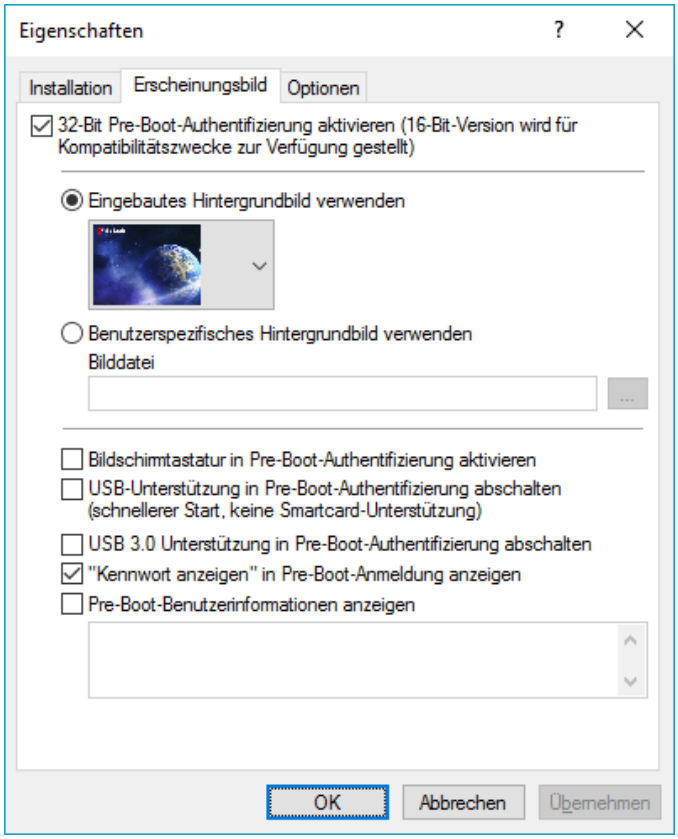
Da die Installation der Disk Protection einen Neustart des Rechners erfordert, können Sie hier noch Einstellungen vornehmen, um den Neustart zu verzögern bzw. selbst zu steuern.

Sofern Sie sich für einen manuellen Neustart entschieden haben, können Sie zusätzlich über einen Kommandozeilenbefehl nach der Installation ein Programm ausführen, z.B. um ein weiteres, eigenes Installationsskript zu starten. Dafür können noch zwei weitere Optionen festgelegt werden:

- *Ausführen als aktuell angemeldeter Benutzer*: Das Skript wird mit den Benutzerrechten ausgeführt, der gerade angemeldet ist. Standardmäßig läuft es sonst unter dem lokalen System.
- *Auch nach Deinstallation ausführen*: Das Skript wird nicht nur bei der Installation, sondern auch bei der Deinstallation ausgeführt.

Konfiguration des Erscheinungsbildes/Verhaltens der PBA für Endbenutzer

Wählen Sie den Reiter *Erscheinungsbild*, um das Aussehen von Disk Protection für Ihre Benutzer festzulegen.



Lassen Sie die Option "*32-Bit Pre-Boot-Authentifizierung aktivieren ...*" ausgewählt. Die alte 16-Bit Version steht nur noch aus Kompatibilitätszwecken für Legacy-BIOS Systeme zur Verfügung.

> Für die neue DriveLock Pre-Boot Authentifizierung unter UEFI-Systemen wird die 16-Bit PBA nicht mehr unterstützt.

An dieser Stelle lässt sich das Hintergrundbild der Pre-Boot Authentifizierung einstellen. Disk Protection liefert bereits vorgefertigte Hintergrundbilder mit, aus denen Sie das gewünschte Bild auswählen können.

Für ein eigenes Hintergrundbild (Format PNG, maximal 32 MB, optimale Auflösung 1024x768) setzen Sie den Haken bei *Benutzerspezifisches Hintergrundbild verwenden* und geben Sie die gewünschte Datei an. Diese sollte sich am besten bereits im Richtliniendateispeicher befinden, damit Sie sich nicht um die Verteilung dieser Datei auf die Clients kümmern müssen. Dann können Sie die Datei aus dem Richtliniendateispeicher oder aus dem Dateisystem auswählen.

Weiterhin können Sie folgende Optionen an- oder abwählen:

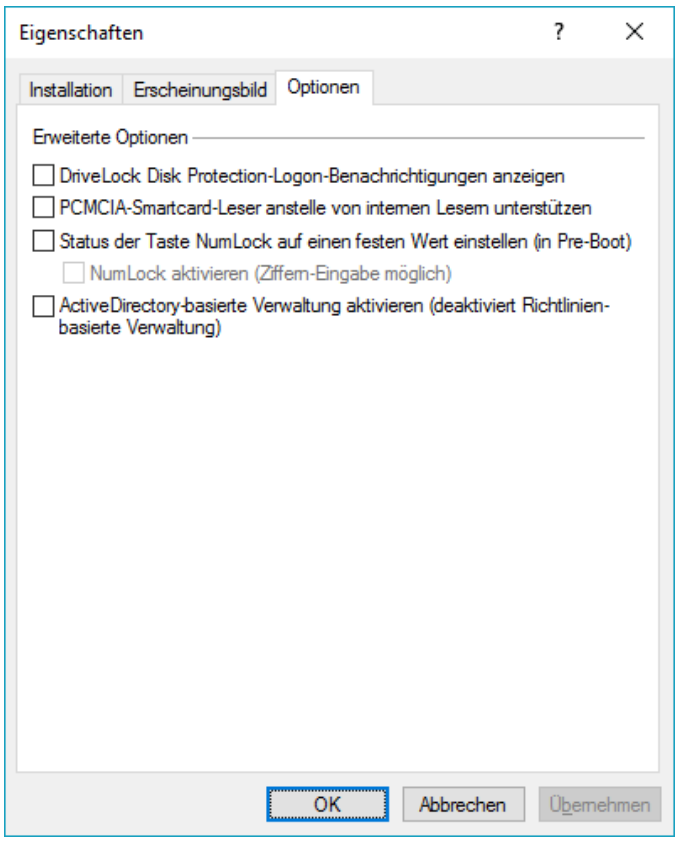
- Bildschirmtastatur (nur UEFI PBA): Mit Hilfe einer virtuellen Tastatur können Benutzereingaben auch ohne vorhandene reale Tastatur erfolgen.
- USB-Unterstützung: Ist diese deaktiviert, kann die PBA schneller geladen werden. Allerdings funktionieren damit keine über die USB-Schnittstelle angeschlossenen Geräte, wie z.B. Maus oder Smartcard Leser
- USB 3.0 Unterstützung: Diese Option deaktiviert den Support von modernen USB 3.0 Geräten innerhalb der PBA
- Kennwort anzeigen: Damit kann verhindert werden, dass ein eingegebenes Passwort im Klartext angezeigt wird

Möchten Sie eigene Benutzerinformationen innerhalb der PBA anzeigen, z.B. für Hinweise zur Verwendung oder Ansprechpartner / Kontakte für die Kennwort-Wiederherstellung, dann aktivieren Sie die Option "*Pre-Boot-Benutzerinformationen anzeigen*" und geben in dem nachfolgenden Textfeld den anzuzeigenden Text ein.

Weitere Optionen

Wählen Sie den Reiter *Optionen*, um zusätzliche Einstellungen für BIOS-Systeme nach Rücksprache mit dem DriveLock Support und bei Bedarf zu konfigurieren.

> Für die neue UEFI-PBA sind die beiden mittleren Optionen unwirksam.



Klicken Sie auf **OK** oder **Übernehmen,** um die Einstellungen zu speichern oder **Abbrechen,** um abzubrechen.

Wenn der Agent seine neue Konfiguration bekommt und Disk Protection installiert wird, zeigt der Agent dem angemeldeten Benutzer folgende Information an:

Die Envelope-Datei wird sofort nachdem der Agent die Disk Protection auf dem Client-Computer installiert hat erstellt und zu dem angegebenen Ort gesendet. Stellen sie daher sicher, dass Sie auch die dazugehörigen Wiederherstellungsoptionen ordnungsgemäß konfiguriert haben (siehe Kapitel „Ablage der Wiederherstellungs-Dateien festlegen“).

Die Installation der DriveLock Festplattenverschlüsselung kann über einen Registry-Schlüssel gesteuert bzw. unterbunden werden, auch wenn die DriveLock Konfiguration entsprechend konfiguriert ist: *HKEY_LOCAL_MACHINE\SOFTWARE\CenterTools\DLStatus*

Ist dort der Registry-Key (DWORD) NoFDEInstallation vorhanden und auf den Wert 1 gesetzt, führt der DriveLock Agent trotz entsprechender Konfiguration keine Installation durch. Per Kommandozeilenbefehl *dlfdecmd enabledelayinst* bzw. *dlfdecmd disabledelayinst* kann dieser Registry-Key ebenfalls gesetzt bzw. gelöscht werden.

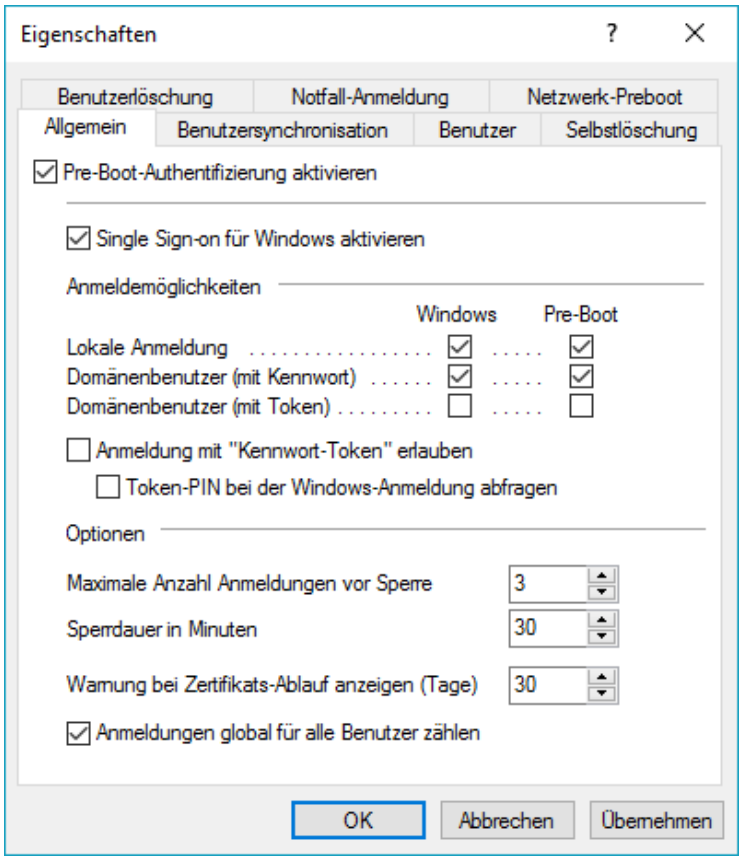
6.3.2 Konfiguration der Pre-Boot Authentifizierung

Sobald Disk Protection auf Ihren Client-Computern verteilt und installiert worden ist, können Sie damit beginnen, Einstellungen für die Pre-Boot Authentifizierung vorzunehmen.

Man kann die Pre-Boot Authentifizierung aktivieren und konfigurieren, bevor man damit beginnt, die Laufwerke der Client-Computer zu verschlüsseln. Das kann bei der Verteilung in größeren Umgebungen helfen, um die Benutzern zu unterstützen sich mit dem neuen Anmeldeverfahren vertraut zu machen.

Klicken Sie auf **Einstellungen für die Pre-Boot-Authentifizierung**, um den Konfigurationsdialog zu öffnen.

6.3.2.1 Authentifizierungs-Methoden und Anmeldeeinstellungen



Um die Pre-Boot-Authentifizierung auf Ihren Client-Computern zu aktivieren, wählen Sie *„Pre-Boot-Authentifizierung aktivieren“*.

> Sobald der DriveLock Agent die neue Konfiguration erhält, wird die Pre-Boot-Authentifizierung aktiviert. Stellen Sie sicher, dass alle anderen Parameter innerhalb des Dialoges konfiguriert wurden und Ihre Benutzer über die Änderung informiert sind.

Der Benutzer wird folgende Nachricht bekommen, wenn die PBA aktiviert wurde:

Um die DriveLock PBA (ohne Entschlüsselung) zu deaktivieren, wählen Sie diese Checkbox ab.

Achtung: auch wenn die Festplatte weiter verschlüsselt bleibt, wird die Sicherheit dadurch herabgesetzt, daß Windows startet, bevor sich ein berechtigter Benutzer am Rechner authentifiziert hat. DriveLock empfiehlt, die PBA nur zu Test und Wartungszwecken zu deaktivieren.

Wenn diese Checkbox nicht markiert ist, können Änderungen anderer Einstellungen innerhalb des Dialoges gemacht werden, aber die Änderungen treten nicht in Kraft, bis die Disk Protection wieder über die Checkbox *„Pre-Boot-Authentifizierung aktivieren“* aktiviert wird.

Um Zugriff auf ein System zu bekommen welches durch die Disk Protection geschützt ist, ist eine Authentifizierung sowohl an der Pre-Boot-Authentifizierung als auch der Windows Zugriffsebene notwendig.

Eine oder eine Kombination aus lokalen Benutzern, Passwort Domäne und Token Domäne Authentifizierungs-Methoden stehen dem Benutzer für die Pre-Boot und Windows-Authentisierung zur Verfügung. Diese Authentifizierungs-Methoden werden weiter unten im Detail beschrieben.

Um eine Authentifizierungsmethode für einen Benutzer verfügbar zu machen, muss entweder die *Windows* oder die *Pre-Boot* Checkbox ausgewählt werden, entsprechend Ihren Anforderungen und der Sicherheitsrichtlinien Ihres Unternehmens. Mindestens eine Checkbox muss für jeweils beide, Windows und Pre-Boot Authentifizierungs-Methoden aktiviert werden. Wird zum Beispiel nur die Pre-Boot Checkbox markiert, muss sich der Benutzer bei der Windows-Anmeldung erneut authentifizieren.

Konfigurieren Sie Disk Protection nicht so, dass nur Windows Anmeldung/Authentifizierung mit Tokens (und Smartcards) möglich ist, wenn Sie keine Tokens (Treiber sind nicht installiert) haben, um sich an Windows anzumelden. Wenn Disk Protection in solch einer Weise konfiguriert und der PC gesperrt wird, gibt es keinen Weg den PC wieder zu entsperren, da Disk Protection dann nur Token Anmeldungen erlaubt. Der Administrator sollte sicherstellen, dass es ein gültiges Token für beide PBA und Windows-Anmeldung (Entsperren) gibt, bevor Disk Protection nur für Token Zugriff konfiguriert wird.

- Lokale Anmeldung – Standardmäßig aktiviert, erlaubt es diese Methode lokalen Windows-Benutzern sich mit ihrem lokalen Windows Benutzernamen, Passwort und lokalen Systemnamen am System zu authentifizieren.
- Domänenbenutzer (mit Kennwort) – Diese Methode erlaubt es Windows Domänen-Benutzern sich mit ihrem Windows Domänen-Benutzernamen, Passwort und Domänennamen am System zu authentifizieren.

- Domänenbenutzer (mit Token) – Diese Methode erlaubt es Windows Domänen-Benutzern eine Smartcard/Token und PIN für die Authentifizierung zu benutzen.

Anmeldung mit Kennwort-Token erlauben – Diese Methode erlaubt die Pre-Boot Authentifizierung für einen Kennwort-Token Benutzer. Wenn diese Option markiert ist, muss mindestens noch eine Windows Authentifizierung ausgewählt werden.

Im sogenannten Single Sign-on Modus muss sich ein Benutzer für beide Ebenen (Pre-Boot und Windows) nur einmal anmelden. Diese Option ist dann automatisch verfügbar, wenn die Authentifizierung für beide, Pre-Boot und Windows Zugriffsebene, für mindestens eine gleiche Authentifizierungs-Methode aktiviert ist.

Nach einer bestimmten Anzahl von fehlerhaften Anmeldungen kann ein Benutzer für eine bestimmte Zeit gesperrt werden, um das System vor einer Brute-Force Attacke mit automatischen Anmelde-Skripten zu schützen. Ändern Sie die Standard-Werte gemäß Ihren Unternehmens-Sicherheitsrichtlinien.

Die Option „*Anmeldungen global für alle Benutzer zählen*“ ist dabei standardmäßig aktiviert. Sie bewirkt, dass Fehlversuche nicht für einen einzelnen Benutzer hochgezählt werden, sondern der Zähler für Fehlversuche unabhängig vom verwendeten Benutzer inkrementiert wird.

Wenn man Zertifikate für die Authentifizierung benutzt, kann man auch die Anzahl der Tage festlegen, wann Disk Protection den Benutzer informiert, bevor sein Zertifikat ausläuft.

6.3.2.2 AD Benutzersynchronisation

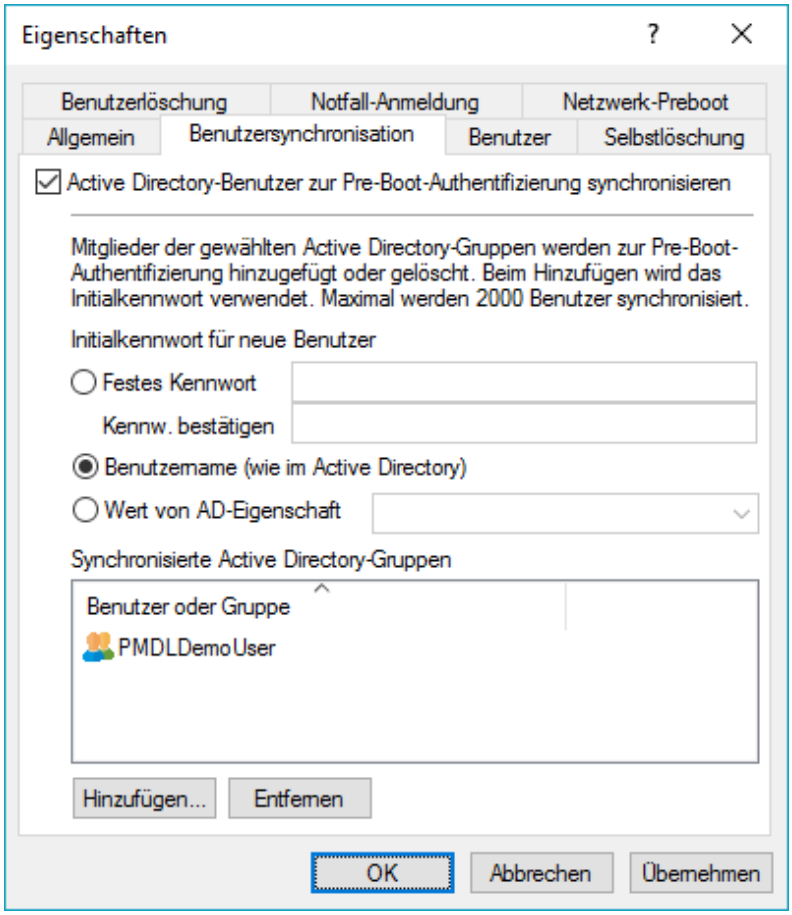
DriveLock unterscheidet 4 Typen von Pre-Boot-Nutzern.

Hinzugefügt von	Beschreibung
DlFdeUser	Benutzer wurde lokal mit *DlFdeUser.exe* erstellt
Policy	Benutzer wurde durch die Richtlinie erstellt - und wird mit Änderungen der Richtlinie synchronisiert/entfernt.
WinLogon	Benutzer wurde durch Windows-Login erstellt - das Passwort wird bei jedem erfolgreichen Windows-Login synchronisiert.
AD sync	Benutzer wurde aus AD-Gruppen synchronisiert - und wird gelöscht, wenn er aus der AD-Gruppe bzw. Benutzersynchronisation gelöscht wird. Das Passwort wird bei jedem erfolgreichen Windows-Login lokal synchronisiert.

Das Kommando *DlFdeUser.exe* kann auch andere Benutzertypen löschen. Diese werden beim nächsten Windows-Login oder Laden der Richtlinie wieder hinzugefügt.

Windows-Benutzer, die sich zum ersten mal an einem PC anmelden, der mit DriveLock Disk Protection und Per-Boot-Authentifizierung (PBA) geschützt ist, sind mit ihren Windows-Anmeldedaten noch nicht in der PBA-Datenbank synchronisiert. Sie müssen sich an der PBA entweder mit einem vorkonfigurierten *DlFde*- oder *Policy*-Benutzer anmelden oder ein anderer berechtigter Benutzer meldet sich an der PBA an, um den Windows-Anmeldedialog anzuzeigen.

Wollen Sie die PBA so vorkonfigurieren, dass Benutzer aus ihrem AD bereits enthalten sind, müssen Sie die AD **Benutzersynchronisation** einschalten.



Dazu aktivieren Sie *Active Directory-Benutzer zur Pre-Boot-Authentifizierung synchronisieren*. Fügen Sie die AD-Gruppen und -Benutzer für die Benutzer hinzu, die in die PBA-Datenbank synchronisiert werden sollen.

> Bitte beachten Sie, dass die Mitglieder der Gruppe "Domänen-Benutzer" nicht synchronisiert werden. Diese Gruppe verwendet einen "berechneten" Mechanismus, der auf der "primären Gruppen-ID" des Benutzers basiert, um die Mitgliedschaft zu bestimmen, und speichert Mitglieder normalerweise nicht als mehrwertige verknüpfte Attribute.

Als initiales Kennwort können Sie ein **festes Kennwort** (identisch für alle Benutzer), den **Benutzernamen** oder jeden verfügbaren **Wert von AD-Eigenschaft** vergeben.

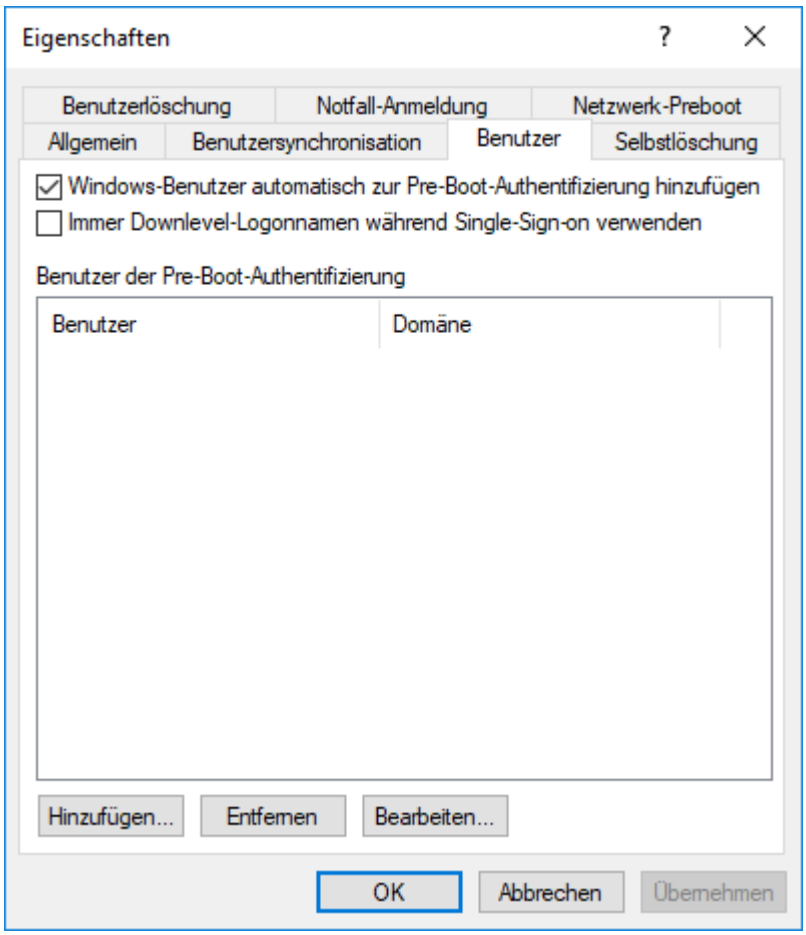
> Das vergebene Passwort wird nur beim Anlegen verwendet, aber nicht für Benutzer synchronisiert/geändert, die bereits in der PBA-Datenbank vorhanden sind. Sobald sich ein AD Sync-Benutzer an Windows anmeldet wird lokal das initiale Passwort durch sein Windows-Passwort ersetzt.

AD Sync-Benutzer werden jedes mal synchronisiert, wenn die Richtlinie geladen wird. Fügen Sie Benutzer zu den den konfigurierten AD-Gruppen hinzu oder entfernen Sie diese, werden bei der nächsten Synchronisation auf allen betroffenen PCs diese Benutzer auch in der PBA-Datenbank hinzugefügt/entfernt.

Auch wenn die PBA-Datenbank bis zu 2.000 Einträge aufnehmen kann, empfehlen wir, nicht mehr als 500 Benutzer für die AD Benutzersynchronisation zu verwenden. Wollen Sie mehr Systeme konfigurieren, erstellen Sie separate Richtlinien, die unterschiedlichen Computergruppen zugeordnet sind.

6.3.2.3 Benutzer

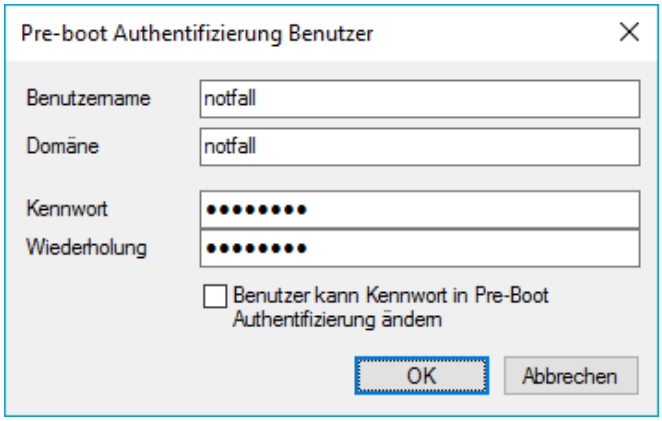
Man kann Benutzer manuell zu der Pre-Boot-Authentifizierungs-Datenbank hinzufügen. Disk Protection kann fast bis zu 2000 Benutzer in der Datenbank speichern. Ein Pre-Boot-Authentifizierungs-Benutzer muss nicht unbedingt ein Windows Benutzerkonto sein, Sie können zusätzliche Anmeldedaten (Benutzername / Passwort) nur für die Pre-Boot-Authentifizierung verwenden (z.B. ein Notfallkonto).



Standardmäßig fügt Disk Protection jeden Benutzer zur Pre-Boot-Authentifzierungs-Datenbank hinzu, der erfolgreich an Windows angemeldet wurde. Deaktivieren Sie *„Windows-Benutzer automatisch zur Pre-Boot-Authentifizierung hinzufügen“,* wenn Sie nicht möchten, dass Windows-Benutzer automatisch hinzugefügt werden.

Wenn Sie die Option "*Immer Downlevel-Logonnamen während Single-Sign-on verwenden*" aktivieren, ist die Benutzeranmeldung nur noch mit den sogenannten Downlevel-Logonnamen möglich. Diese haben die Form "DOMAIN\Benutzername". Eine Anmeldung mit benutzername@domain.org (sog. User-Principal Names) ist damit nicht mehr zugelassen.

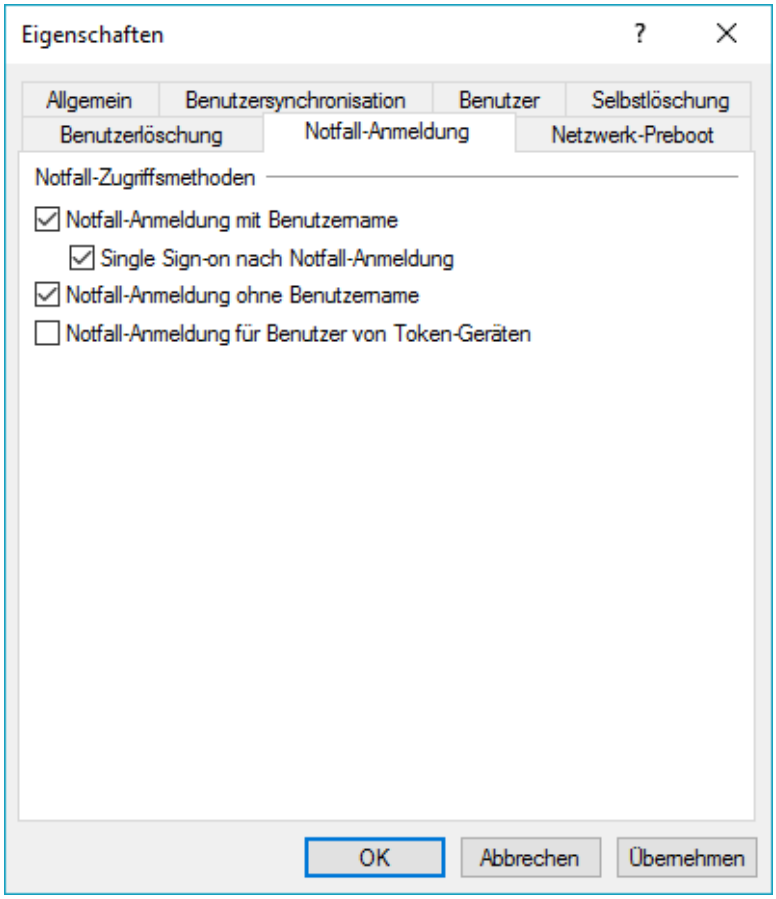
Benutzen Sie die Buttons **Hinzufügen**, **Entfernen** oder **Bearbeiten,** um bestehende Benutzer zu ändern, entfernen oder neue Benutzer zur Datenbank hinzuzufügen.



Wenn Sie die Informationen eingegeben und das Passwort bestätigt haben, klicken Sie auf **OK,** um den Benutzer zu speichern.

6.3.2.4 Notfall-Anmeldung

Diese Einstellungen geben an, welche Anmeldeverfahren zur Verfügung stehen, falls ein Benutzer nicht mehr in der Lage ist, sich anzumelden (z.B. Kennwort vergessen).



Notfall-Anmeldeeinstellungen sind verfügbar, wenn die Authentifizierung auf der Pre-Boot Ebene aktiv ist und wenn *Lokale Anmeldung* und/oder *Domänenbenutzer* Checkbox ausgewählt sind.

Notfall-Anmeldung mit Benutzername: Falls aktiviert, erlaubt die Option dem Benutzer das Verfahren Notfall-Anmeldung mit Benutzername aufzurufen. Es wird in dem Fall verwendet, wenn der Benutzer sein Pre-Boot Authentifizierungs-Passwort (nicht die PIN) vergessen hat. Das betrifft Windows-Domänen oder lokale Windows-Benutzer Passwort-Accounts, die der Disk Protection Benutzerdatenbank hinzugefügt wurden. Es erlaubt einen einmaligen Pre-Boot Zugriff auf das System.

Dieses Feature setzt voraus, dass sich ein Benutzer zuvor mindestens einmal erfolgreich an der Pre-Boot Authentifizierung angemeldet hat, bevor es von diesem Benutzer aufgerufen werden kann. Wenn ein Benutzer sich noch nie angemeldet hat, muss er das Verfahren Notfall Anmeldung ohne Benutzername aufrufen.

Single Sign-on nach Notfall-Anmeldung: Falls aktiviert, erlaubt die Option es dem Benutzer sich sofort automatisch an Windows zu authentifizieren, eine erfolgreiche Anwendung des Verfahrens Notfall Anmeldung mit Benutzername vorausgesetzt.

Dieses Feature ermöglicht es Benutzern, die ihr Passwort vergessen haben, dennoch an Windows anzumelden und damit zu arbeiten - auch wenn ein Administrator das Passwort noch nicht zurückgesetzt hat.

Notfall-Anmeldung ohne Benutzername: Falls aktiviert, können neu erstellte Windows-Domänen oder lokale Windows-Benutzer das Verfahren Notfall-Anmeldung ohne Benutzername aufrufen. Das erlaubt einen einmaligen Pre-Boot Zugriff auf das System für alle Benutzer, die noch niemals am System angemeldet waren.

Notfall-Anmeldung für Benutzer von Token-Geräten: Diese Option ist nur verfügbar, wenn mindestens eine der folgenden Pre-Boot-Authentifizierungs-Methoden aktiviert ist: Domänenbenutzer (mit Token) oder Zugriff mit Shared Key. Wenn diese Option aktiviert ist, sind Smartcard/Token Benutzer (die ihr Token verlegt oder ihre PIN vergessen haben) berechtigt das Verfahren für die Notfall-Anmeldung für Token Benutzer aufzurufen. Diese Verfahren erlaubt einen einmaligen Pre-Boot Zugriff auf das System ohne Nutzung eines Tokens.

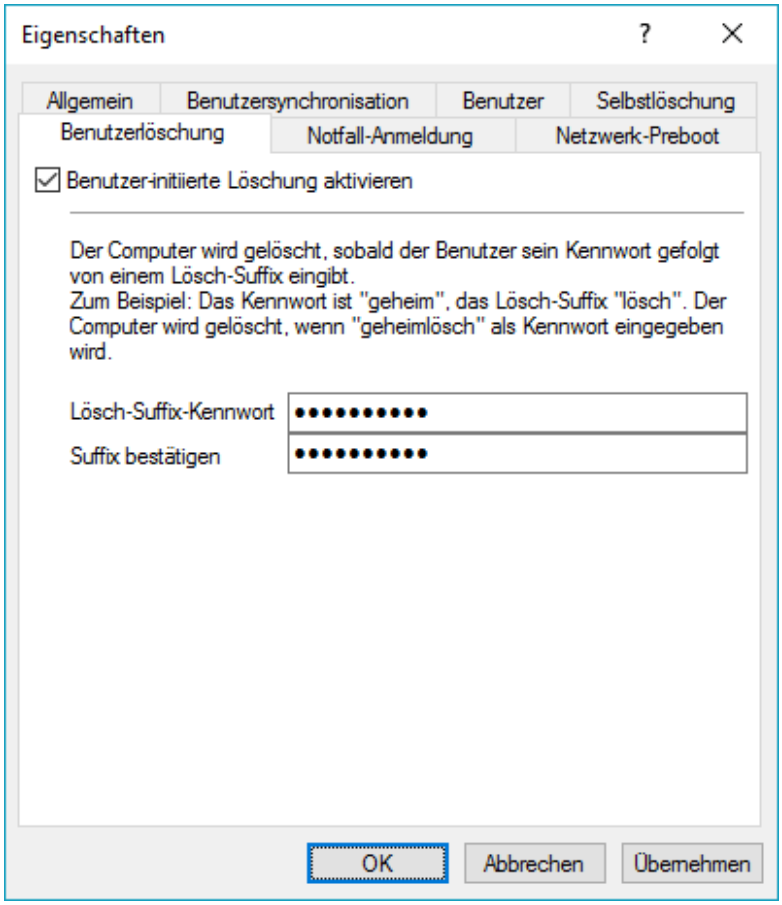
6.3.2.5 Löschen der PBA-Datenbank

DriveLock bietet drei verschiedene Arten an, die PBA-Datenbank zu löschen:

- Löschung durch einen Benutzer (Benutzerlöschung)
- Automatische Löschung bei fehlender Netzwerkverbindung (Selbstlöschung)
- Löschung durch einen Administrator (Fernlöschung)

Benutzerlöschung

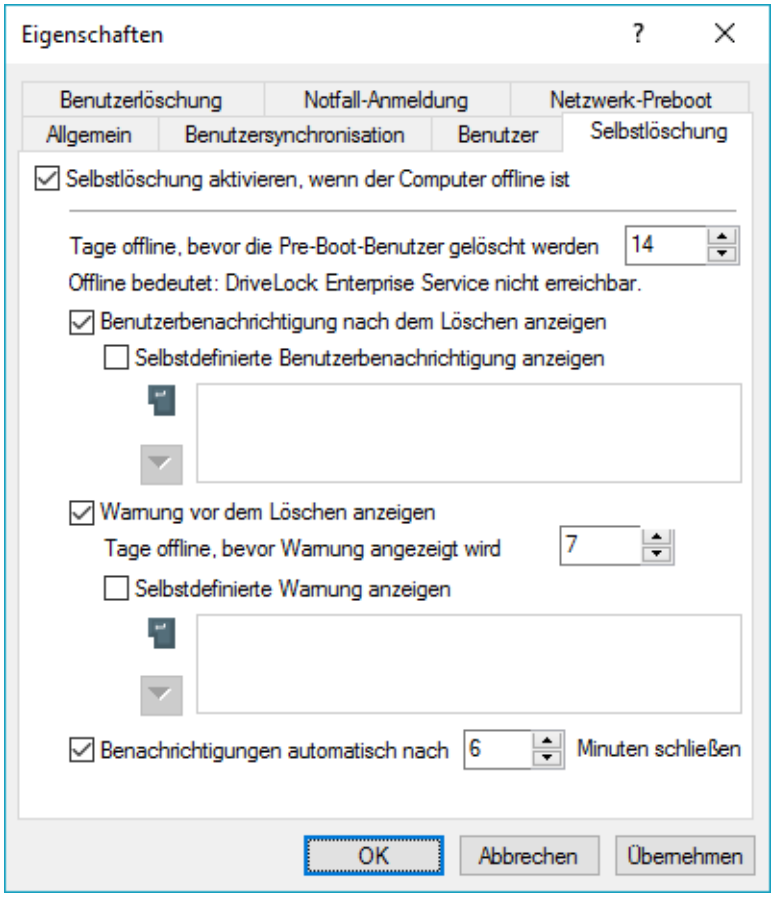
Zum Konfigurieren der Benutzerlöschung wählen Sie den Reiter *Benutzerlöschung*, markieren *Benutzer-initiiere Löschung aktivieren* und geben ein **Lösch-Suffix** ein.



Selbstlöschung

Die Selbstlöschung hat hauptsächlich zwei Anwendungsszenarien. Entweder möchten Sie die Daten auf einem verloren gegangenen PC schützen, der sich nicht mehr mit dem DES verbindet und/oder Sie wollen mobile Benutzer dazu zwingen sich regelmäßig mit dem Firmennetz zu verbinden.

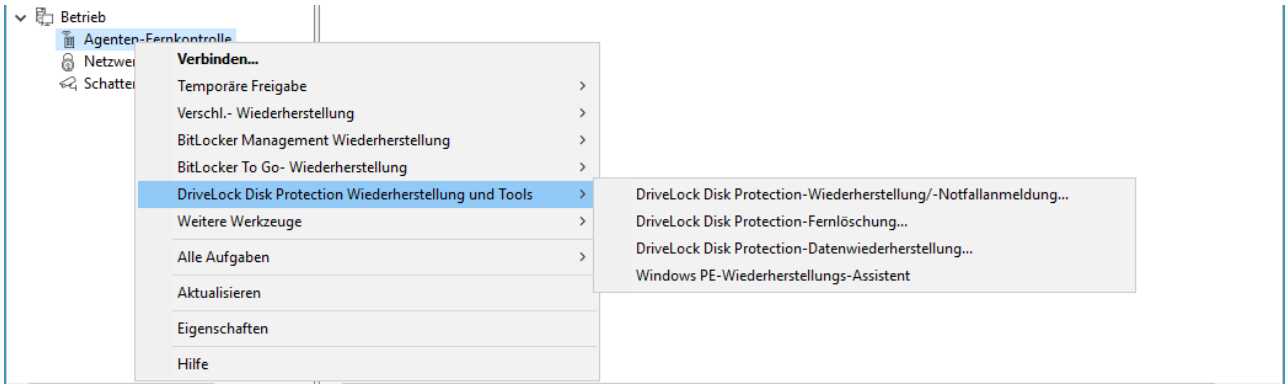
Zum Konfigurieren der Selbstlöschung wählen Sie den Reiter *Selbstlöschung*, markieren *Selbstlöschung aktivieren, wenn der Computer offline ist* und konfigurieren die für Sie geeigneten Einstellengen wie im Dialog beschrieben.



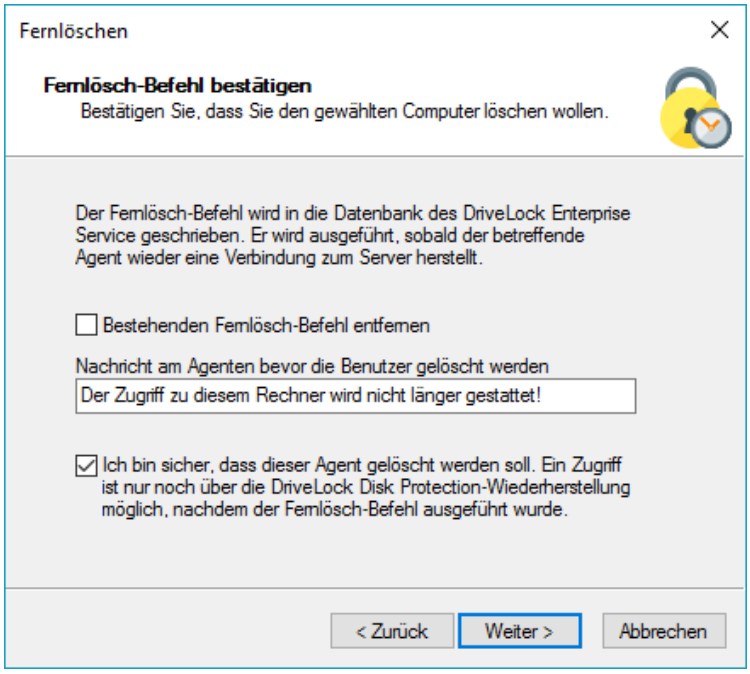
Nach Ablauf der angegebenen Offline-Zeit löscht DriveLock die PBA-Datenbank.

Fernlöschung initiieren

Die Aktivierung der Fernlöschung erfolgt durch einen Rechts-Klick in der DriveLock Management Konsole auf **Betrieb / Agenten Fernkontrolle** im Abschnitt *Disk Protection Wiederherstellung und Tools* **/ DriveLock Disk Protection Fernlöschung**.



Für die Aktivierung der Fernlöschung benötigen Sie den privaten Schlüssel des Wiederherstellungs-Zertifikates. Geben Sie den Pfad zur Datei *DLFDERecovery.pfx* und das korrekte Passwort ein. Anschließend wählen Sie den Computer aus, den Sie löschen möchten. Im nächsten Dialog müssen sie den **Fernlösch-Befehl bestätigen**. Die Einstellungen, die Sie festlegen werden beim nächsten Mal, wenn sich der Computer mit dem DES verbindet, aktiviert. Damit die Fernlöschung auch außerhalb des Firmennetzwerkes funktioniert, muss der DES aus dem Internet erreichbar sein.



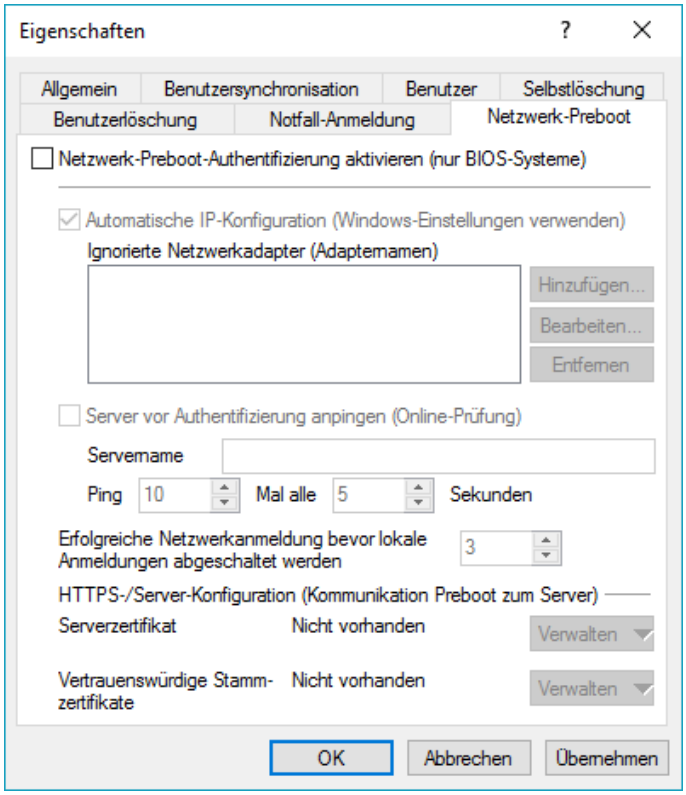
Konfigurieren sie die Einstellungen wie im Dialog angezeigt.

Markieren Sie *Bestehenden Fernlösch-Befehl entfernen* um einen zuvor erteilten Fernlösch-Befehl zu widerrufen (sofern die PBA Datenbank noch nicht gelöscht ist).

6.3.2.6 Netzwerk-Pre-Boot (BIOS)

Für bestimmte Legacy-BIOS Systeme bietet Disk Protection eine netzwerk-fähige Pre-Boot Authentifizierung an, die automatisch erkennen kann, ob sich der Rechner in einem vordefinierten Unternehmensnetzwerk befindet und eine Anmeldung an der PBA deaktiviert (Auto-Boot).

iese Funktionalität steht nur für bestimmte Systeme Verfügung und darf nur bei entsprechender Begleitung durch einen Mitarbeiter des DriveLock Professional Service Teams aktiviert werden. Daher wird an dieser Stelle auch auf eine Beschreibung dieser Funktionen bewusst verzichtet.



6.3.2.7 Netzwerk-Pre-Boot (UEFI)

Die Einstellungen auf dem Reiter Netzwerk-Pre-Boot (UEFI) sind je nach Lizenz sowohl für DriveLock Disk Protection, als auch für DriveLock BitLocker Management verfügbar, da in beiden Fällen die DriveLock Pre-Boot-Authentifizierung verwendet wird. Bitte entnehmen Sie die Informationen zu diesem Thema aus dem Kapitel Netzwerk-Pre-Boot (UEFI) in der BitLocker Management Dokumentation auf https://drivelock.help/.

6.3.2.8 Einstellungen für die PBA

Die drei folgenden Einstellungen beziehen sich auf die Konfiguration der PBA auf den DriveLock Agenten:

1. **Änderungen der lokalen PBA-Konfiguration zulassen**
   Mit dem Kommandozeilenprogramm 'dlsetpb.exe' können Sie auf einem Computer Anpassungen an der PBA-Konfiguration vornehmen. Diese Einstellung bestimmt, ob diese Konfigurationsänderungen bei der nächsten Aktualisierung der Richtlinie beibehalten oder überschrieben werden (mit den Einstellungen aus der Richtlinie, z.B. welcher Tastaturtreiber verwendet werden soll). Standardmäßig werden die Änderungen des Kommandozeilenprogramms beibehalten.
   Beim Update von einer Version vor 2020.2 werden alle Einstellungen so behandelt, als wären sie vom Kommandozeilenprogramm gesetzt worden.
2. **SmartCard-Treiber in PBA laden**
   Hiermit geben Sie an, ob SmartCard-Treiber verwendet werden sollen. Wenn Sie keine SmartCards einsetzen, benötigen Sie diese Einstellung nicht.
3. **PBA-Tastaturtreiber auswählen**
   Mit dieser Einstellung können Sie den Tastaturtreiber für die PBA festlegen.
   Wenn der verwendete Standardtreiber beispielsweise keine unterschiedlichen Tastaturlayouts kennt, können Sie hier einen Treiber von DriveLock auswählen. Der Kombi-Treiber kombiniert sowohl Tastatur- als auch

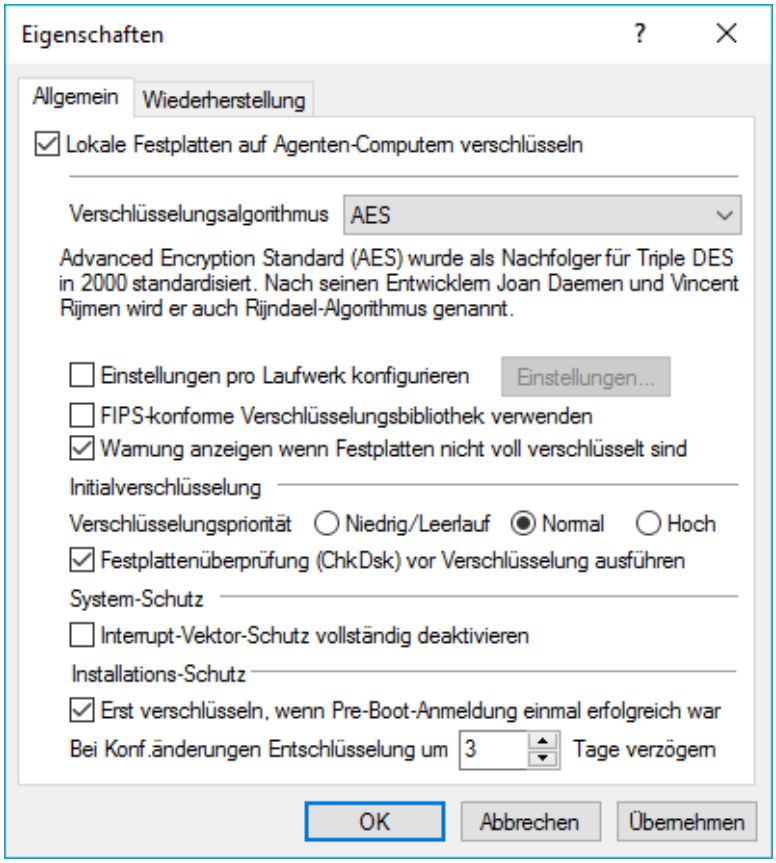
Maustreiber in einem. Wenn dieser nicht zum gewünschten Resultat führt, können Sie auch den (älteren) DriveLock-Tastaturtreiber verwenden.
Beachten Sie, dass Sie möglicherweise auf unterschiedlichen Geräte unterschiedliche Treiber einstellen müssen.

6.3.3 Einstellungen für die Verschlüsselung

Dieses Kapitel enthält Informationen darüber, wie man die DriveLock Disk Protection einrichtet und wie Recovery-Informationen der Agenten bereitgestellt und zentral gespeichert werden.

Klicken Sie auf **Einstellungen für die Verschlüsselung,** um den Eigenschaften-Dialog zu öffnen.

6.3.3.1 Verschlüsselungseinstellungen konfigurieren



Um generell die Festplatten Verschlüsselung zu aktivierten, wählen Sie die Option *"Lokale Festplatten auf Agenten-Computer verschlüsseln"* aus.

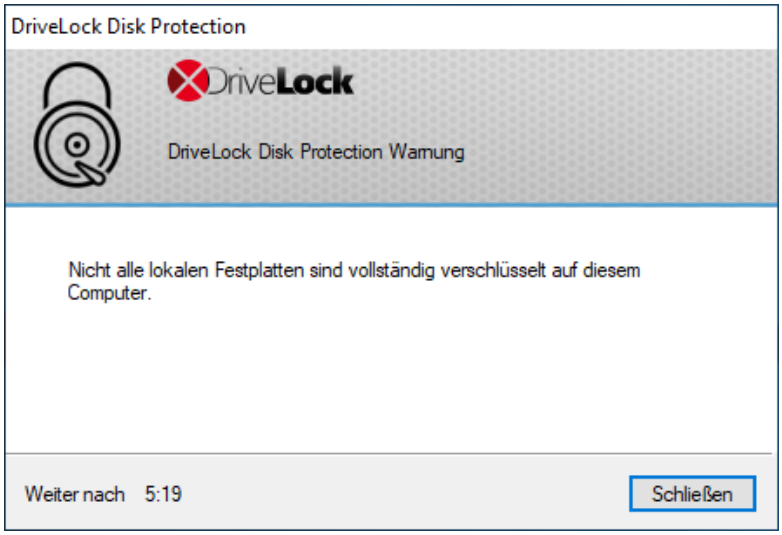
In Abhängigkeit der Laufwerksgröße kann die Ver- bzw. Entschlüsselung einige Zeit in Anspruch nehmen. Der Rechner kann während dieser Zeit jedoch weiterhin verwendet werden, eine geringfügige Beeinträchtigung der Systemleistung ist denkbar. Ebenfalls kann der Rechner in dieser Phase heruntergefahren oder neu gestartet werden. In diesem Fall wird der Vorgang im Anschluss fortgesetzt. Der aktuelle Stand der Verschlüsselung auf einem Rechner kann über die DriveLock Management Konsole überprüft werden, indem Sie sich mit dem Agenten verbinden und sich dessen Eigenschaften anzeigen lassen.

Sie können zwischen verschiedenen unterschiedlichen Verschlüsselungs-Algorithmen auswählen, allerdings empfehlen wir die Auswahl *AES* (AES 256-bit).

Standardmäßig verschlüsselt Disk Protection alle lokalen Festplatten. Wählen Sie *„Einstellungen pro Laufwerk konfigurieren"* und klicken auf **Einstellungen**, um die Verschlüsselung für jedes verfügbare Laufwerk separat zu konfigurieren.

Wählen Sie die Checkbox *"FIPS-konforme Verschlüsselungsbibliothek verwenden",* um die FIPS Bibliothek zu verwenden. Wenn diese Option nicht ausgewählt wird, ist die Performance besser und eine CC EAL-2 zertifizierte Nicht-FIPS-Bibliothek verwendet die, sofern ihre PCs dies unterstützen, automatisch die Hardware-Unterstützung AES NI aktiviert (Intel® Advanced Encryption Standard (AES) Instructions Set).

Um allen Benutzern einen Warnhinweis anzuzeigen, der auf eine unvollständige Laufwerks-Verschlüsselung hinweist, muss die Checkbox *„Warnung anzeigen wenn Festplatten nicht voll verschlüsselt sind"* gesetzt werden. Der Warnhinweis wird sofort nach der Windows Anmeldung angezeigt:



Disk Protection verwaltet einen Speicher für manche BIOS Interrupt-Vektor-Adressen (nur Legacy BIOS). Das erlaubt es Disk Protection, potenzielle Angriffe zu erkennen, die durch das Ändern der Interrupt-Vektor-Adressen gestartet werden. Wenn es einen Unterschied zwischen der BIOS Interrupt-Vektor-Adresse und der zuvor gespeicherten Kopie erkennt, wird eine Fehlermeldung angezeigt.

> Wenn sich die Interrupt-Vektor-Adresse ändert (z.B. durch ein BIOS Update), wird der Fehler weiterhin angezeigt. Die System-Schutz Gruppe stellt einen Mechanismus zur Verfügung um berechtigte Änderungen, durch Aktualisierung der Disk Protection's Kopie der Festplatte, Tastatur und Clock-Tick Interrupt-Vektor-Adressen, zu akzeptieren.

Über die Option "**Interrupt-Vektor-Schutz vollständig deaktivieren**" können Sie die Überprüfung der Interrupt-Vektoren komplett deaktivieren.

Die Option "Erst verschlüsseln, wenn Pre-Boot-Anmeldung einmal erfolgreich war" kann aktiviert werden, um die Verschlüsselung der Festplatten so lange zu verzögern, bis sich ein Benutzer einmalig an der Pre-Boot Authentifizierung erfolgreich angemeldet hat und damit in der Benutzerdatenbank der PBA gespeichert wurde.

Die Entschlüsselung von Festplatten kann aufgrund folgender Gründe starten:

- Sie deaktivieren die Option *"Lokale Festplatten auf Agenten-Computer verschlüsseln"* innerhalb der Richtlinie
- Die Zuweisung der Richtlinie mit den Disk Protection Einstellungen zu Computern wird entfernt bzw. aufgehoben
- Die Lizenzoption "FDE" innerhalb einer zugewiesenen Richtlinie wird entfernt

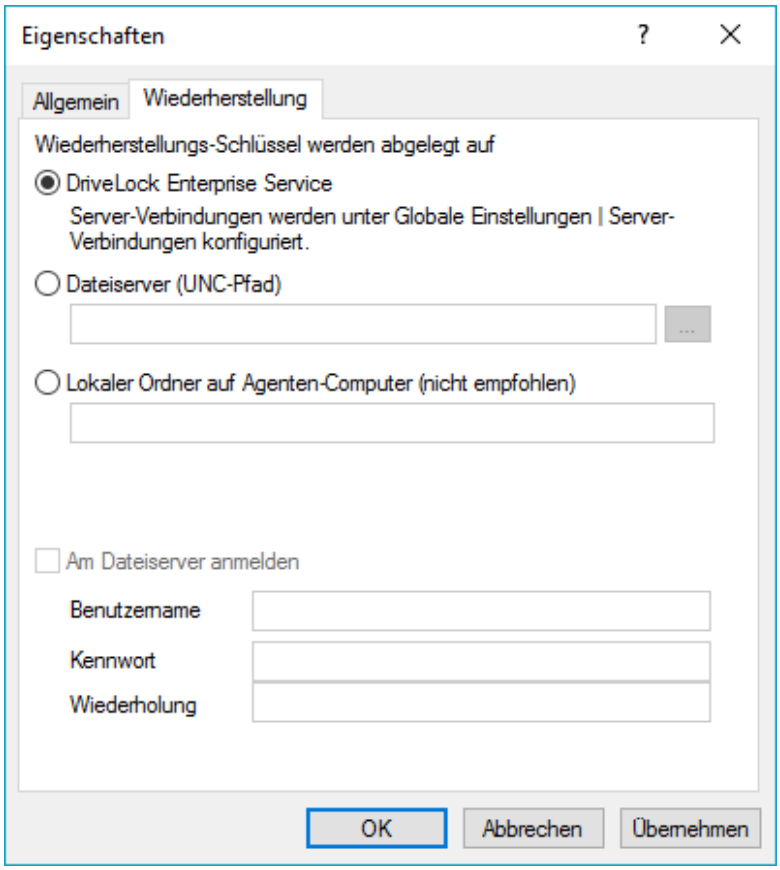
Um eine unbeabsichtigte, sofortige Entschlüsselung von Festplatten zu verhindern, kann diese um einige Tage verzögert werden. Setzen Sie den Wert bei Tagen auf 0, um eine sofortige Entschlüsselung einzustellen.

> Dieser Verzögerungswert ist auch hilfreich in Umgebungen mit einer schlechten Netzwerk-Anbindung. Erhält ein Agent temporär eine fehlerhafte oder unvollständige Richtlinie und wurde die lokal vorhandene gespeicherte

Richtlinie (Cache) entfernt, kann dadurch eine sofortige Entschlüsselung verhindert und der Zeitraum überbrückt werden, bis der Agent wieder eine vollständige RIchtlinie übermittelt bekommt.

6.3.3.2 Ablage der Wiederherstellungs-Dateien festlegen

Um einzustellen, wo der Client seine Wiederherstellungs-Schlüssel speichern soll, wählen Sie den Reiter *Wiederherstellung*.



Die Wiederherstellungs-Schlüssel bestehen aus folgenden Dateien:

- *Recovery.env* – Das ist die Envelope-Datei für die Notfall-Anmeldung
- *DiskKeyBackup.zip* – Diese ZIP Datei enthält die EFS Wiederherstellungsdatei für das Recovery Verfahren zur Datenwiederherstellung.

Die Envelope-Datei wird sofort nachdem der Agent die Disk Protection auf dem Client-Computer installiert hat erstellt und zu dem angegebenen Ort gesendet. Die ZIP-Datei mit den EFS Wiederherstellungs-Dateien wird erst erstellt und kopiert, nachdem alle Laufwerke vollständig verschlüsselt wurden.

Die Wiederherstellungs-Dateien sollten entweder im DriveLock Enterprise Server oder einer zentralen Dateifreigabe gespeichert werden. Zusätzlich können die Dateien lokal auf dem Computer gespeichert werden, obwohl es wegen Sicherheits- und Wiederherstellungsgründen nicht empfohlen ist.

Wenn die Dateien auf einer zentralen Dateifreigabe gespeichert werden, sind die Dateinamen wie folgt: *<Computer>.envelope.env* und *<Computer>.backup.zip*

Um auf eine Dateifreigabe zuzugreifen, ist es möglicherweise auch erforderlich, eine Benutzerkennung anzugeben.

Sie müssen den Benutzer im Format <Domäne>\<Benutzer> angeben, wenn ein Domänen-Benutzer verwendet wird, um sich an zentraler Stelle anzumelden.

Stellen Sie bitte sicher, dass Sie alle Wiederherstellungs-Schlüssel all Ihrer Computer gespeichert haben, da diese für Notfall-Anmeldeverfahren oder die Datenwiederherstellung unbedingt notwendig sind. Sofern Sie den DriveLock Enterprise Service als zentralen Ablageort verwenden, können Sie mit Hilfe des DriveLock Control Center's - Helpdesk auf einfache Weise überprüfen, für welche Computer die Wiederherstellungsinformationen vorliegen. Informationen dazu finden sich im *DriveLock Control Center Handbuch*.

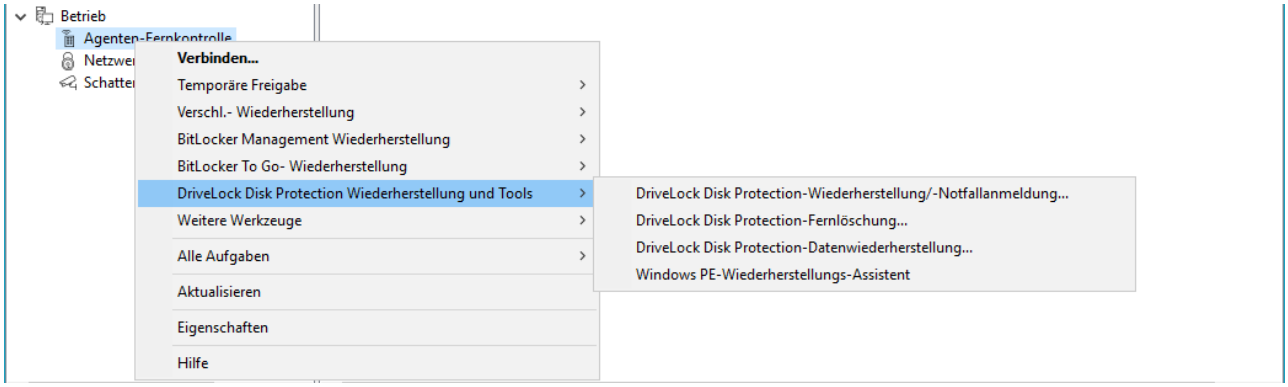
6.4 Wiederherstellungsverfahren

Disk Protection deckt zwei verschiedene Wiederherstellungsverfahren ab:

- Notfall Anmeldeverfahren
- Wiederherstellung verschlüsselter Laufwerke (Daten)

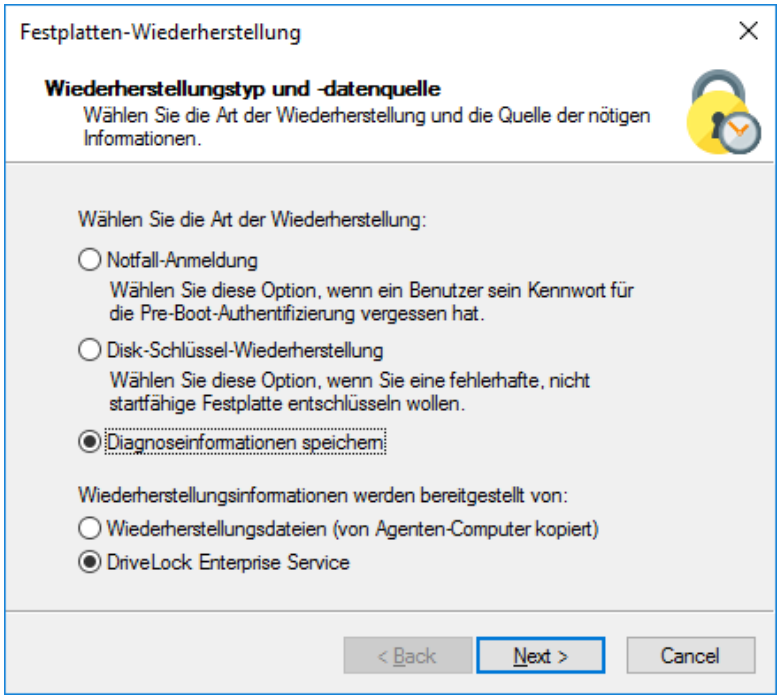
Die Notfall Anmeldeverfahren werden benutzt, wenn ein Benutzer nicht mehr in der Lage ist, sich an der Pre-Boot-Authentifizierung anzumelden (z.B. der Benutzer hat sein Passwort oder PIN vergessen). Wiederherstellung von Laufwerken wird notwendig, wenn auf lokale Laufwerke nicht mehr zugegriffen werden kann (z.B. wenn Datensektoren des Laufwerkes defekt sind und man sich nicht mehr an Windows anmelden kann).

Um den Recovery-Assistenten zu starten, öffnen Sie die DriveLock Management Konsole, wählen *Betrieb / Agenten-Fernkontrolle,* rechtsklicken auf **Agenten-Fernkontrolle** und wählen *Disk Protection Wiederherstellung und Tools* **/** *DriveLock Disk Protection-Wiederherstellung/-Notfallanmeldung* aus.

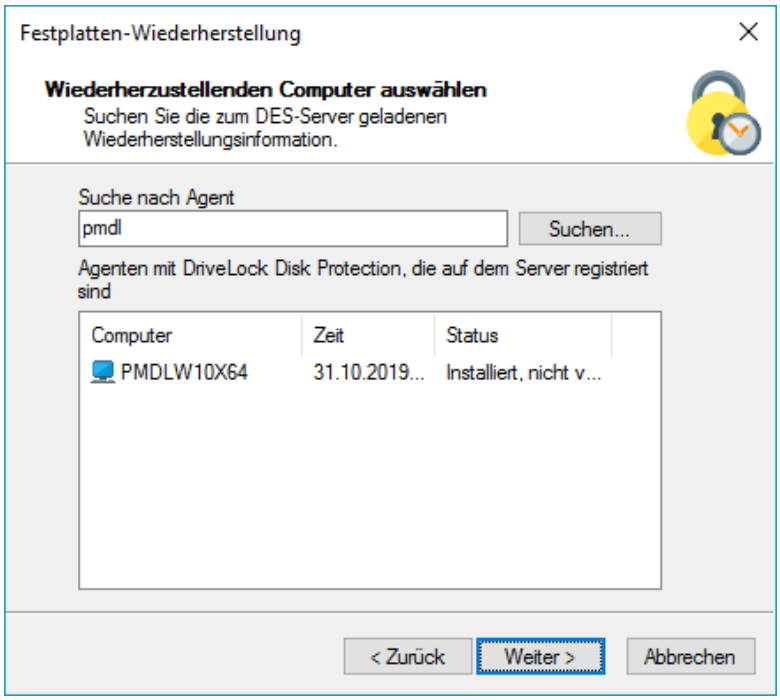


6.4.1 Diagnoseinformationen speichern

Wenn die DriveLock Disk Protection installiert ist, sendet der DriveLock Agent das Installationsprotokoll zu dem DriveLock Enterprise Service. Falls die FDE-Installation fehlgeschlagen ist, kann man diese Datei aus der DriveLock Datenbank holen, um weitere Details zu bekommen.



Wählen Sie "**Diagnoseinformationen speichern**" und "**DriveLock Enterprise Service**" aus und klicken auf **Weiter**.



Wählen Sie die DES-Serververbindung aus der Auswahlliste aus.

Um einen registrierten Agenten in der DriveLock-Datenbank zu finden, geben Sie den Computernamen oder einen Teil des Namens ein und klicken auf **Suchen**. Die Disk Protection zeigt alle registrierten Computer an, die den Suchtext als Teil ihres Computernamens haben. Um alle registrierten Computer zu sehen, geben Sie gar keinen Text an und klicken auf **Suchen**.

Wählen Sie den entsprechenden Computer aus der Liste aus und klicken auf **Weiter** um fortzufahren.

Klicken Sie auf "**...**" und wählen Sie den Pfad aus, unter der die Diagnosedatei abgespeichert werden soll. Klicken Sie auf **Weiter,** um die Datei aus der DriveLock-Datenbank zu empfangen.

Nachdem Sie die Datei erhalten haben, klicken Sie auf **Fertig stellen**.

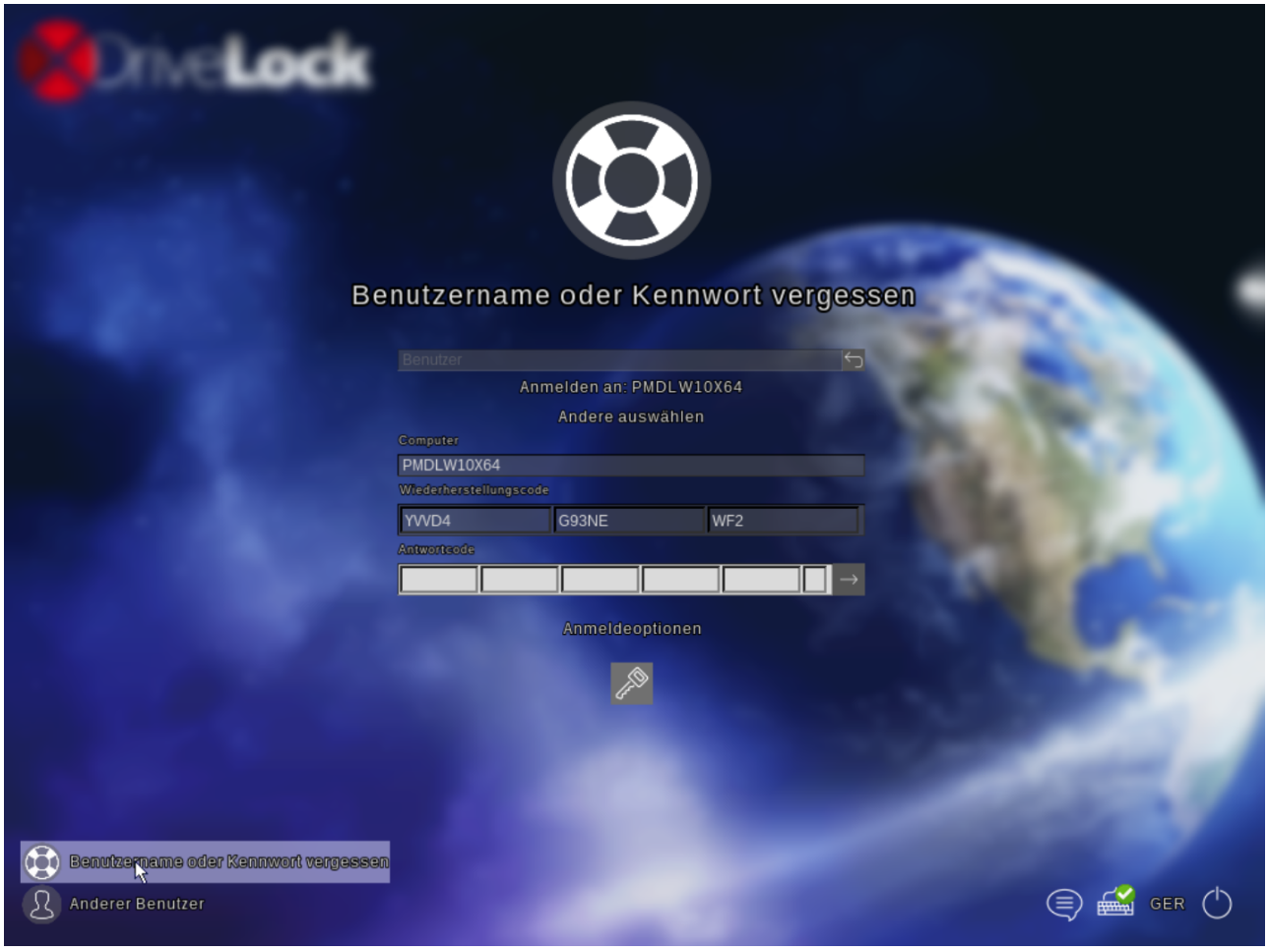
An dem ausgewählten Pfad wurde eine ZIP-Datei abgelegt, die Sie nun entpacken können.

6.4.2 Notfall Anmeldeverfahren

Es gibt drei verschiedene Notfall Anmeldeverfahren an der Pre-Boot-Authentifizierung:

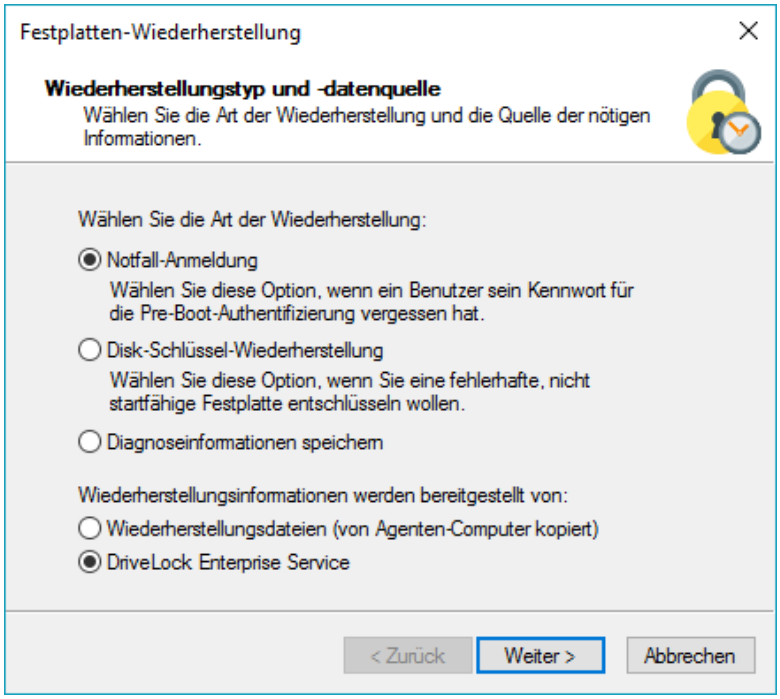
- Notfall Anmeldung mit Benutzernamen
- Notfall Anmeldung ohne Benutzernamen
- Notfall Anmeldung für Token Benutzer

Sie können die verfügbaren Verfahren während der Pre-Boot-Authentifizierung in Disk Protection konfigurieren. Informationen hierzu finden Sie im Kapitel „Konfiguration der Notfall-Anmeldung“.



Der Benutzer klickt auf die Option *Benutzername oder Kennwort vergessen* in der PBA (neue UEFI-PBA für Windows 10).

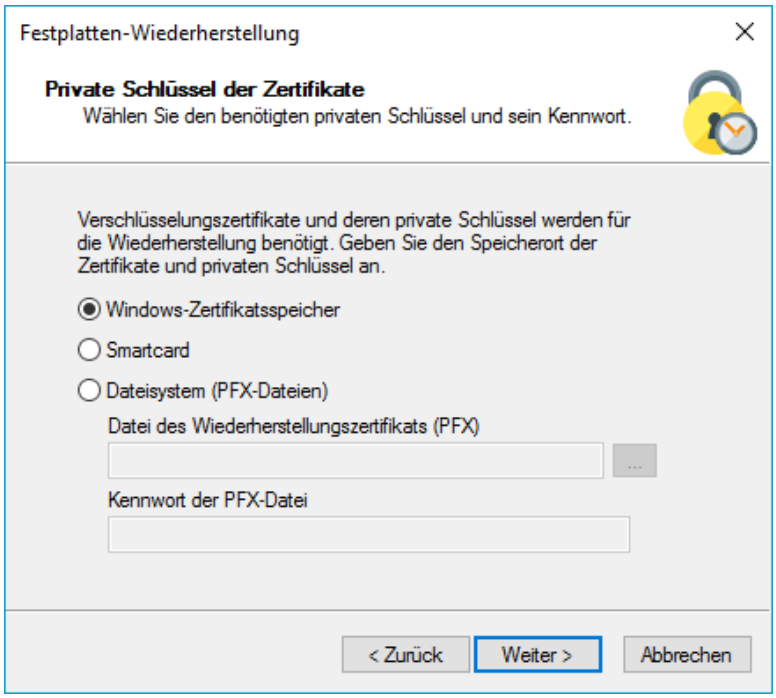
Öffnen Sie die DriveLock Management Konsole, wählen *Betrieb / Agenten-Fernkontrolle,* rechtsklicken auf **Agenten-Fernkontrolle** und wählen *Disk Protection Wiederherstellung und Tools / DriveLock Disk Protection-Wiederherstellung/-Notfallanmeldung* aus.



Wählen Sie die Option *Notfall-Anmeldung* als Wiederherstellungs-Art.

Wenn Sie Disk Protection so konfiguriert haben, dass die Client Wiederherstellungs-Schlüssel zum DriveLock Enterprise Service gesendet werden, wählen Sie die Option *„DriveLock Enterprise Service“* aus. Wenn Sie den Pfad später zu den benötigten Wiederherstellungs-Schlüsseln angeben möchten, wählen Sie *„Wiederherstellungsdateien (von Agenten-Computer kopiert)“* aus.

Klicken Sie auf **Weiter** um fortzufahren.



Für das Notfall-Anmeldeverfahren benötigen Sie den privaten Schlüssel des Wiederherstellungs-Zertifikates.

Geben Sie entweder den Pfad zur Datei *DLFDERecovery.pfx* an und geben das korrekte Passwort ein.

Alternativ können Sie auch eine Smartcard verwenden, auf der zuvor die Zertifikatsinformationen gespeichert wurden. Aktivieren Sie dazu die Option *„Smartcard“*.

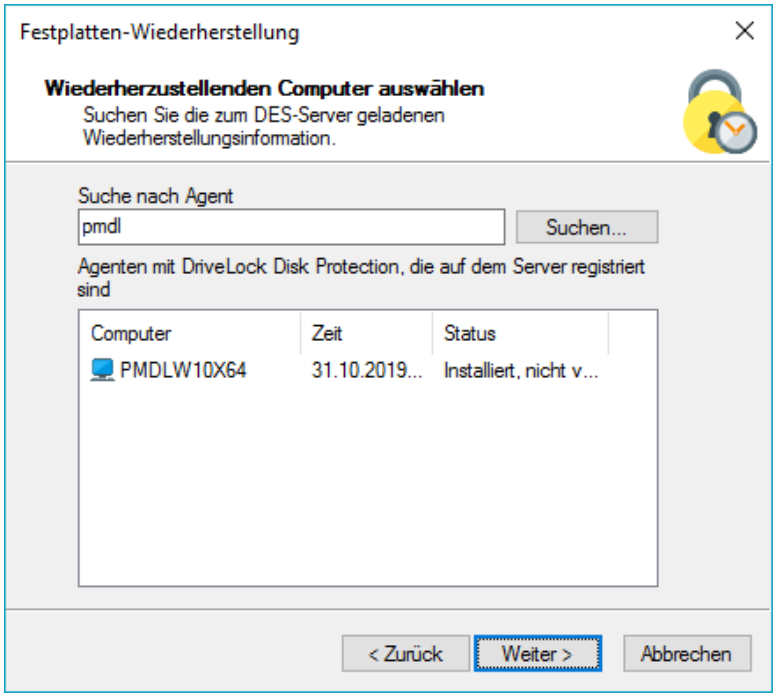
Wurden die Zertifikatsinformationen mit dem privaten Schlüssel in den lokalen Zertifikatsspeicher des aktuell angemeldeten Benutzers importiert, können Sie auch die erste Option „*Windows-Zertifikatsspeicher*“ auswählen.

Wenn Sie den privaten Schlüssel verloren haben, ist eine Wiederherstellung nicht länger möglich.

Klicken Sie **Weiter,** um fortzufahren.

Sofern Sie eine Smartcard verwenden, werden Sie nun abhängig von der verwendeten Karte aufgefordert, diese einzulegen und auszuwählen.

Wenn Sie ausgewählt haben, die Wiederherstellungsinformationen vom DriveLock Enterprise Service zu beziehen, sehen Sie folgenden Dialog (ansonsten springen Sie zum nächsten Schritt):



Wählen Sie den DriveLock Enterprise Service aus dem Drop-Down Menü aus. Klicken Sie auf **Optionen,** wenn Sie Anmeldedaten angeben müssen.

Man kann auf dem ausgewähltem Server nach registrierten Agenten suchen, indem man den Computernamen eingibt und auf den Button **Suchen** klickt. Man kann auch nur einen Teil des Namens eingeben, da Disk Protection nach jedem registriertem Computer sucht, der die Zeichenfolge enthält. Wenn Sie nichts eingeben, werden alle registrierten Computer angezeigt.

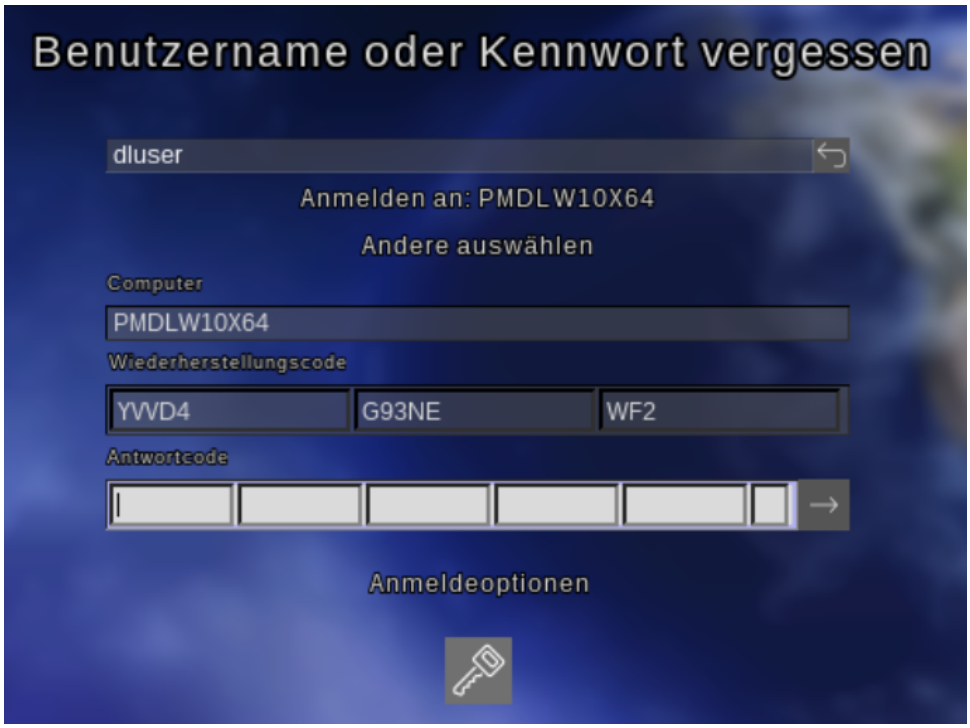
Wählen Sie den gewünschten Computer aus der Liste aus und klicken Sie auf **Weiter**.

Wenn Sie ausgewählt haben, die Wiederherstellungsinformationen aus einer Datei zu laden, müssen Sie die Wiederherstellungs-Datei nun angeben (ansonsten wird dieser Schritt übersprungen). Geben Sie den korrekten Pfad an oder klicken Sie auf den Button “...” um einen Dateiauswahl-Dialog zu öffnen und navigieren Sie manuell zu der Datei.

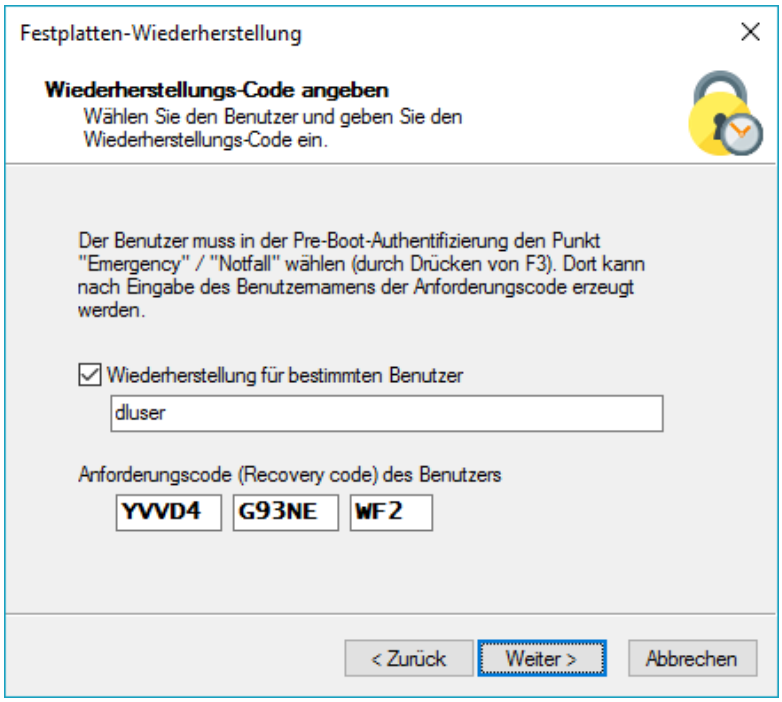
Jeder Client-Computer hat seine eigene entsprechende Envelope-Datei, die für die Notfall-Anmeldung verwendet werden muss. Wenn Sie Disk Protection so konfiguriert haben, dass die Datei automatisch auf eine zentrale Dateifreigabe abgelegt wird, beginnt der Dateiname mit dem Namen des Client-Computers (z.B. *DE2319WX.Envelope.env*).

Klicken Sie **Weiter**.

Wenn der Benutzer sich früher bereits an der Pre-Boot-Authentifizierung angemeldet hat, bitten Sie ihn, seinen Benutzernamen einzugeben (*Notfall Anmeldeverfahren mit Benutzername*) und die Eingabetaste zu drücken (neue UEFI-PBA für Windows 10):



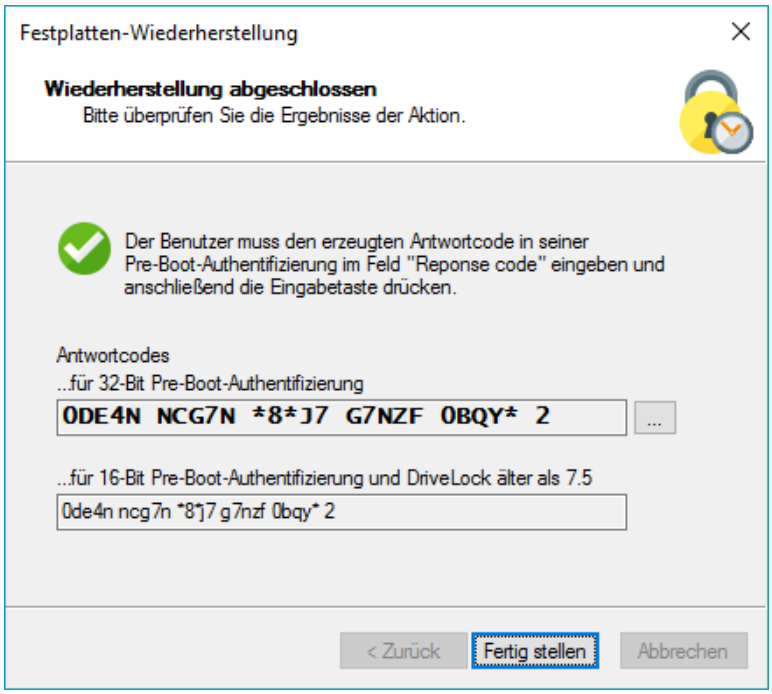
Wenn der Benutzer sich noch nie an der Pre-Boot-Authentifizierung angemeldet hat oder PIN Authentifizierung benutzt wird, braucht kein Name eingegeben zu werden (*Notfall Anmeldeverfahren ohne Benutzername* oder *Notfall Anmeldeverfahren für Token Benutzer*).



Geben Sie den Benutzernamen (bei Wiederherstellung mit einem Benutzernamen) und den Recovery Code, der vom Benutzer bereitgestellt wird, ein.

Der Benutzer muss zunächst korrekte Werte für Benutzername und Domain eingeben bzw. auswählen.

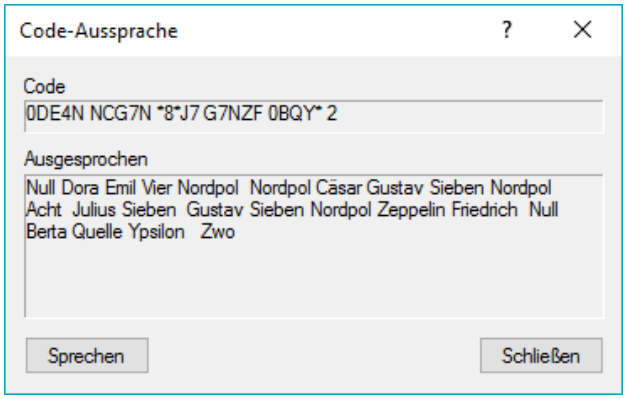
Klicken Sie auf **Weiter,** um den Antwortcode für den Benutzer zu erzeugen.



Sofern Sie eine Smartcard verwenden, werden Sie nun aufgefordert, die PIN für den Zugriff auf die Karte einzugeben.

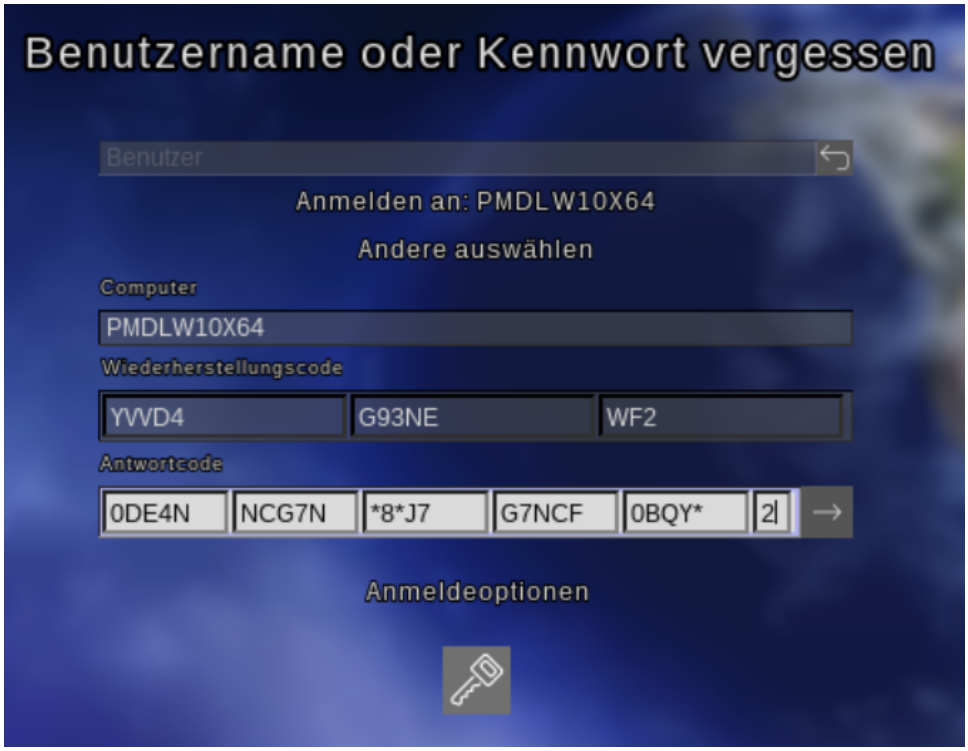
Wenn ein Fehler während der Erstellung auftritt, wird eine entsprechende Nachricht angezeigt.

Klicken Sie auf "..." um eine Hilfe bei der mündlichen Übermittlung des Codes zu erhalten:



Klicken Sie in diesem Fall auf **Fertig stellen** und starten Sie den Wiederherstellungs-Vorgang erneut.

Der Benutzer muss den generierten Antwortcode in das folgende Feld eingeben und das Pfeil-Symbol rechts anzuklicken (alternativ: Eingabetaste nach Eingabe des letzen Zeichens) (neue UEFI-PBA für Windows 10):



An diesem Punkt wird Windows fortfahren, normal zu starten.

6.4.3 Wiederherstellung verschlüsselter Laufwerke

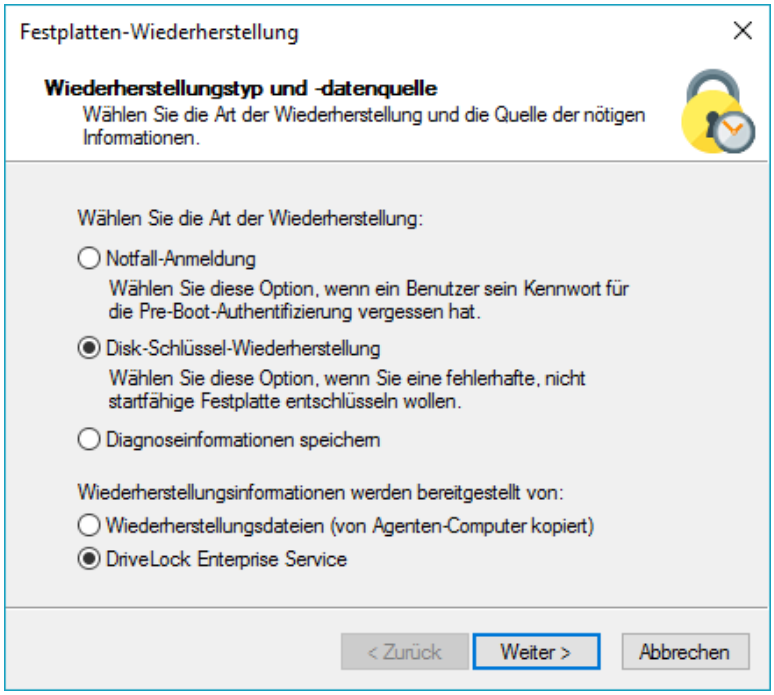
Die Wiederherstellung von Laufwerken ist nötig, wenn auf lokale Laufwerke nicht mehr zugegriffen werden kann (z.B. wenn Datensektoren des Laufwerkes defekt sind).

Um ein verschlüsseltes Laufwerk wiederherzustellen (zu entschlüsseln), muss man die folgenden vier Schritte ausführen:

1. Erstellen Sie die Wiederherstellungsdateien
2. Kopieren Sie alle für die Entschlüsselung notwendigen Dateien auf eine Diskette, USB Wechseldatenträger oder mit auf die Recovery-CD
3. Booten Sie den Rechner mit der Recovery-CD
4. Benutzen Sie die Wiederherstellungsdateien und -tools, um die gewünschte(n) Festplatte(n) auf dem betroffenen Computer zu entschlüsseln.

Diese Schritte und die Erstellung einer Recovery-CD werden als nächstes detailliert beschrieben.

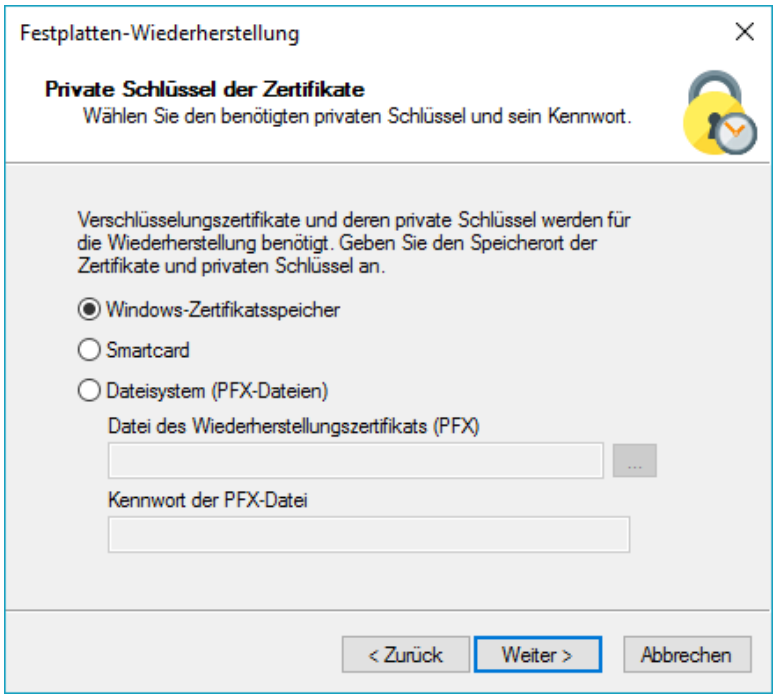
6.4.3.1 Erstellung der notwendigen Dateien für die Entschlüsselung



Wählen Sie die Option *„Disk-Schlüssel-Wiederherstellung“* als Wiederherstellungs-Art.

Wenn Sie Disk Protection so konfiguriert haben, dass die Client Wiederherstellungs-Schlüssel zum DriveLock Enterprise Service gesendet werden, wählen Sie die Option *„DriveLock Enterprise Service“* aus. Wenn Sie den Pfad später zu den benötigten Wiederherstellungs-Schlüsseln angeben möchten, wählen Sie *„Wiederherstellungsdateien (von Agenten-Computer kopiert)“* aus.

Klicken Sie auf **Weiter**.



Für das Notfall-Anmeldeverfahren benötigen Sie den privaten Schlüssel des Wiederherstellungs-Zertifikates.

Geben Sie entweder den Pfad zur Datei *DLFDEMaster.pfx* an und geben das korrekte Passwort ein.

Alternativ können Sie auch eine Smartcard verwenden, auf der zuvor die Zertifikatsinformationen gespeichert wurden. Aktivieren Sie dazu die Option „*Smartcard*“.

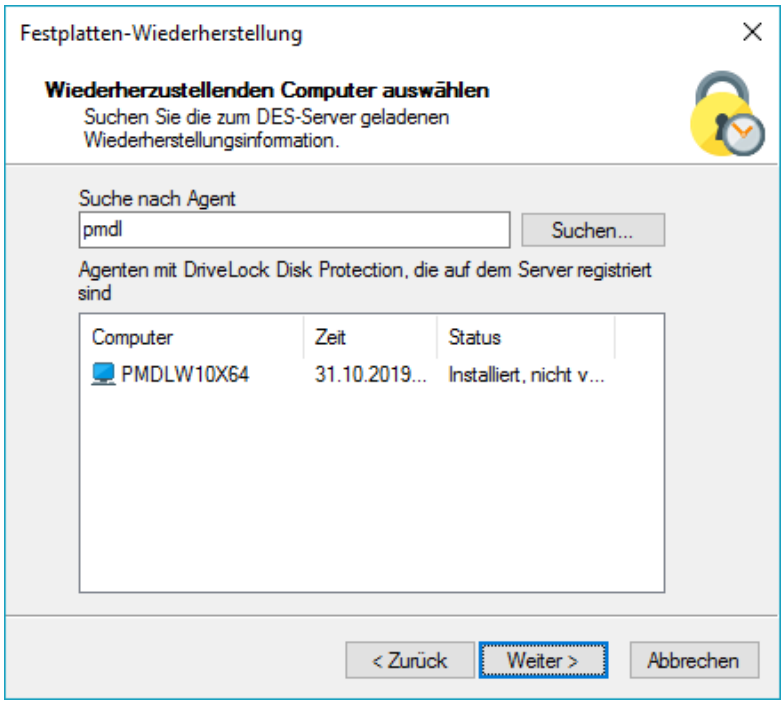
Wurden die Zertifikatsinformationen mit dem privaten Schlüssel in den lokalen Zertifikatsspeicher des aktuell angemeldeten Benutzers importiert, können Sie auch die erste Option „*Windows-Zertifikatsspeicher*“ auswählen.

Wenn Sie den privaten Schlüssel verloren haben, ist eine Wiederherstellung nicht länger möglich.

Klicken Sie **Weiter**, um fortzufahren.

Sofern Sie eine Smartcard verwenden, werden Sie nun abhängig von der verwendeten Karte aufgefordert, diese einzulegen und auszuwählen.

Wenn Sie ausgewählt haben, die Wiederherstellungsinformationen vom DriveLock Enterprise Service zu beziehen, sehen Sie folgenden Dialog (ansonsten springen Sie zum nächsten Schritt):



Man kann auf dem DriveLock Enterprise Service nach registrierten Agenten suchen, indem man den Computernamen eingibt und auf den Button **Suchen** klickt. Man kann auch nur einen Teil des Namens eingeben, da Disk Protection nach jedem registriertem Computer sucht, der die Zeichenfolge enthält.

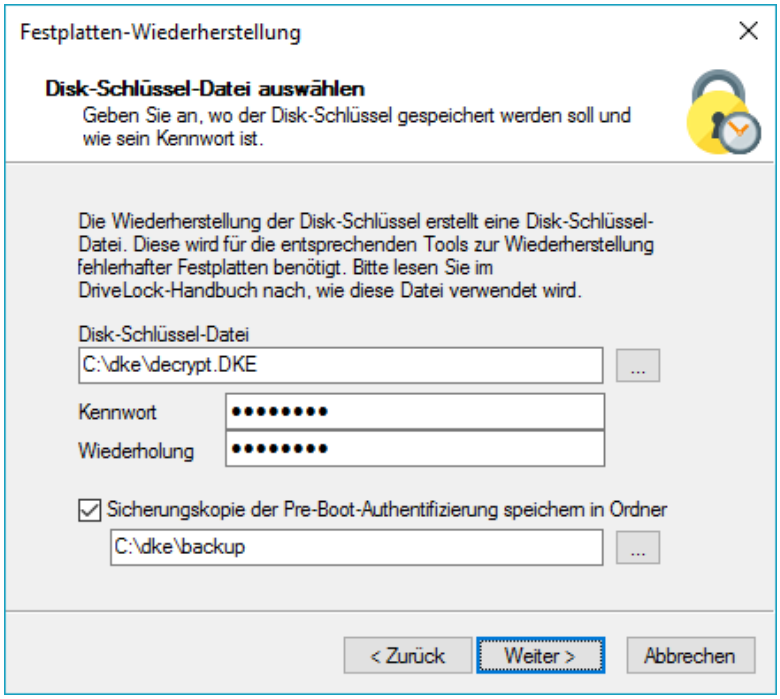
Wählen Sie den gewünschten Computer aus der Liste aus und klicken Sie auf **Weiter**.

Wenn Sie ausgewählt haben, die Wiederherstellungsinformationen aus einer Datei zu laden, geben Sie den korrekten Pfad an oder klicken Sie auf den Button “...”, um einen Dateiauswahl-Dialog zu öffnen und navigieren Sie manuell zu der Datei.

Jeder Client-Computer hat seine eigene entsprechende EFS Wiederherstellungs-Datei, die für die Laufwerks-Wiederherstellung verwendet werden muss. Wenn Sie Disk Protection so konfiguriert haben, dass die Datei automatisch auf eine zentrale Dateifreigabe abgelegt wird, beginnt der Dateiname mit dem Namen des Client-Computers (z.B. *DE2319WX.Backup.zip*).

Die EFS Wiederherstellungs-Dateien werden automatisch vom DriveLock Agenten erzeugt, sobald die Festplattenverschlüsselung beginnt.

Klicken Sie auf **Weiter**.



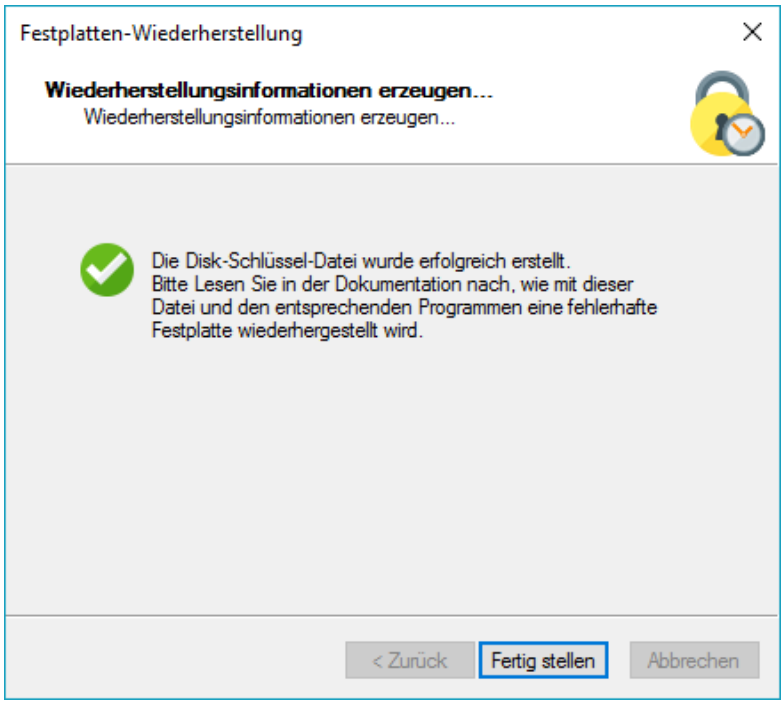
Es ist erforderlich, dass Disk Protection einen speziellen Disk-Schlüssel erstellt. Sie müssen einen Dateinamen und Pfad angeben, indem Sie den Button „…“ wählen. Alternativ können Sie den Pfad und Dateinamen manuell angeben. Stellen Sie sicher, die korrekte Dateiendung (.dke) anzugeben.

Geben Sie ein Passwort an, um den Zugriff auf diese Datei abzusichern. Bestätigen Sie das Passwort durch eine Wiederholung. Das Passwort muss mindestens sechs Zeichen lang sein. Es wird später für die Wiederherstellung benötigt.

Wählen Sie die Option „*Sicherungskopie der Pre-Boot-Authentifizierung speichern in Ordner*“ um alle Wiederherstellungsdaten, die in der DriveLock Datenbank gespeichert sind, in eine Backup.zip zu exportieren.

Klicken Sie auf **Weiter,** um den Disk-Schlüssel zu erstellen.

Sofern Sie eine Smartcard verwenden, werden Sie nun aufgefordert, die PIN für den Zugriff auf die Karte einzugeben.



Nachdem die Datei mit dem Disk-Schlüssel erfolgreich erstellt wurde, wird eine entsprechende Nachricht angezeigt.

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

Jetzt können Sie die erstellte Datei auf eine Diskette, USB Laufwerk oder die Recovery-CD kopieren, um diese in den nächsten Schritten zu verwenden.

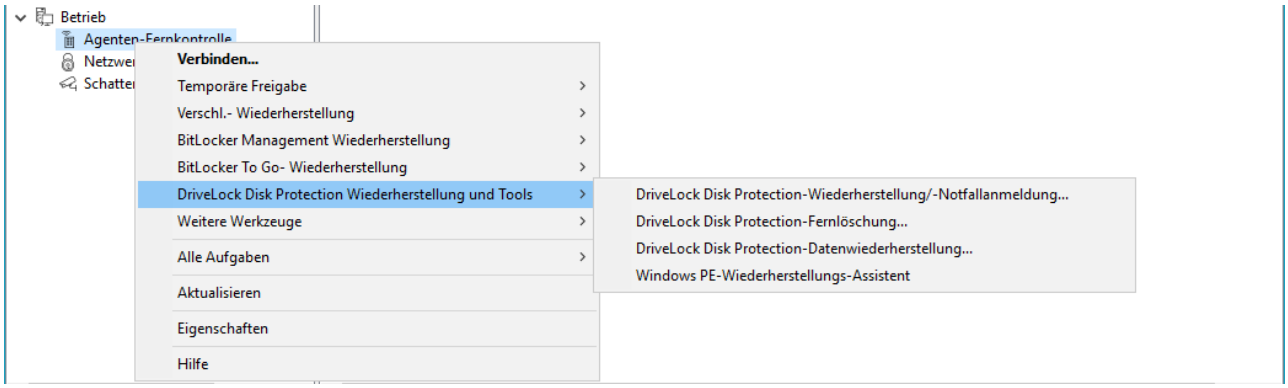
6.4.3.2 Erstellen eines Wiederherstellungs-Mediums

Um ein System wiederherzustellen, das nicht mehr gestartet werden kann, wird eine bootfähiges Wiederherstellungsmedium (oder Recovery CD) für den Systemstart benötigt.

> Sie benötigen nur ein Wiederherstellungsmedium für Ihre Systemumgebung, da die individuelle Wiederherstellungsdatei auf einen weiteren USB-Stick kopiert wird.

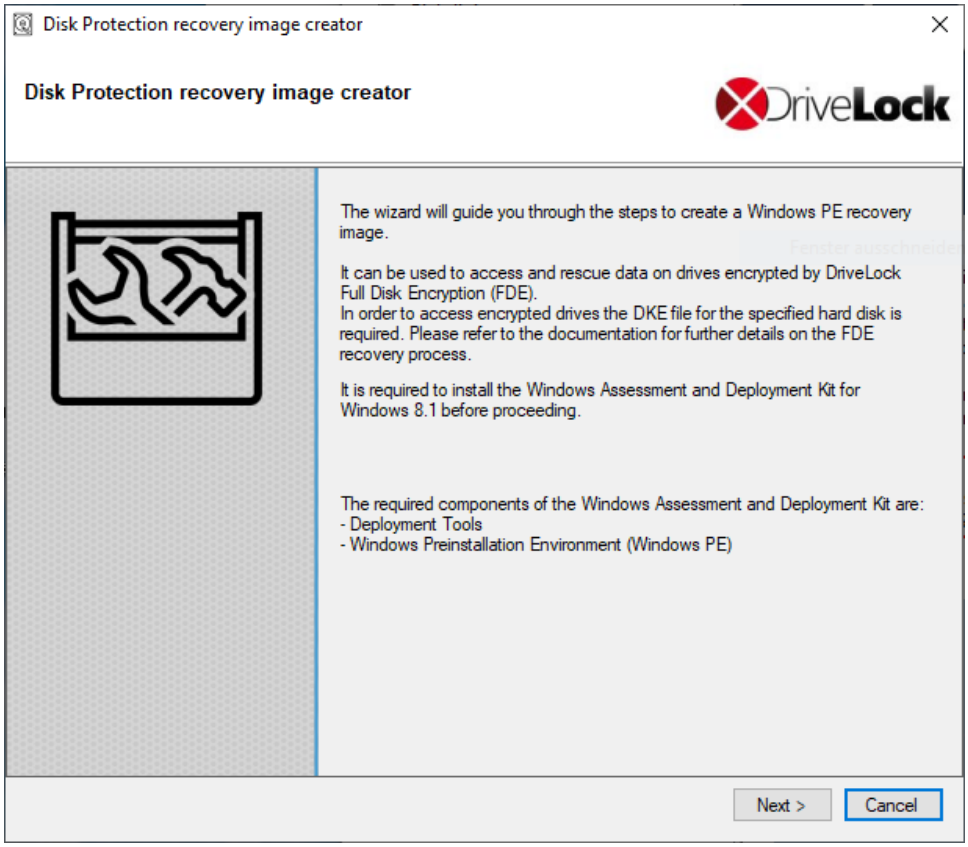
Bevor Sie den Assistenten starten, stellen Sie sicher dass folgende Bedingungen erfüllt sind:

- Sie besitzen auf Ihrem Rechner administrative Rechte, um ggf. das *Windows Assesment and Deployment Kit (ADK)* zu installieren (sofern noch nicht geschehen).
- Auf Ihrem Rechner ist die aktuelle DriveLock Management Konsole installiert.
- Ein USB-Stick (mind. 1GB) oder eine beschreibbare CD für das Windows PE Wiederherstellungsmedium liegt bereit.



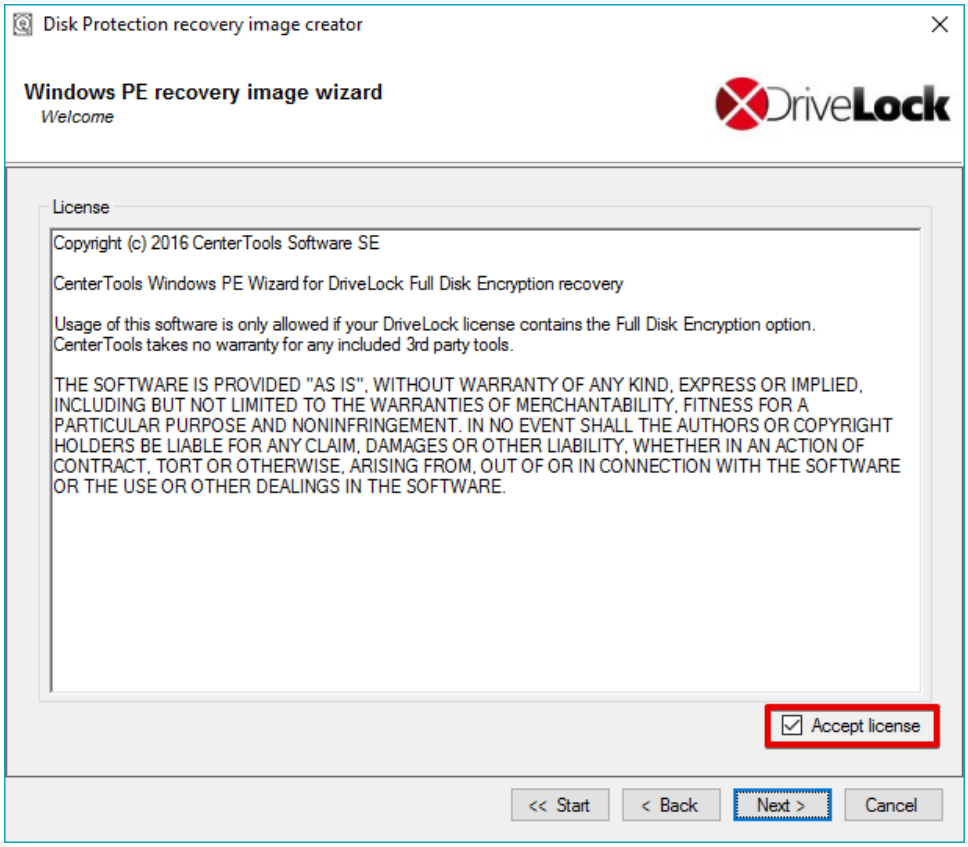
Um den Assistent zur Erstellung einer Windows PE CD zu starten, öffnen Sie die DriveLock Management Konsole, wählen *Betrieb* / *Agenten-Fernkontrolle,* rechtsklicken auf **Agenten-Fernkontrolle** und wählen *Disk Protection Wiederherstellung und Tools* / *Windows PE-Wiederherstellungs-Assistent* aus.

> Der Assistent steht nur in Englischer Sprache zur Verfügung.

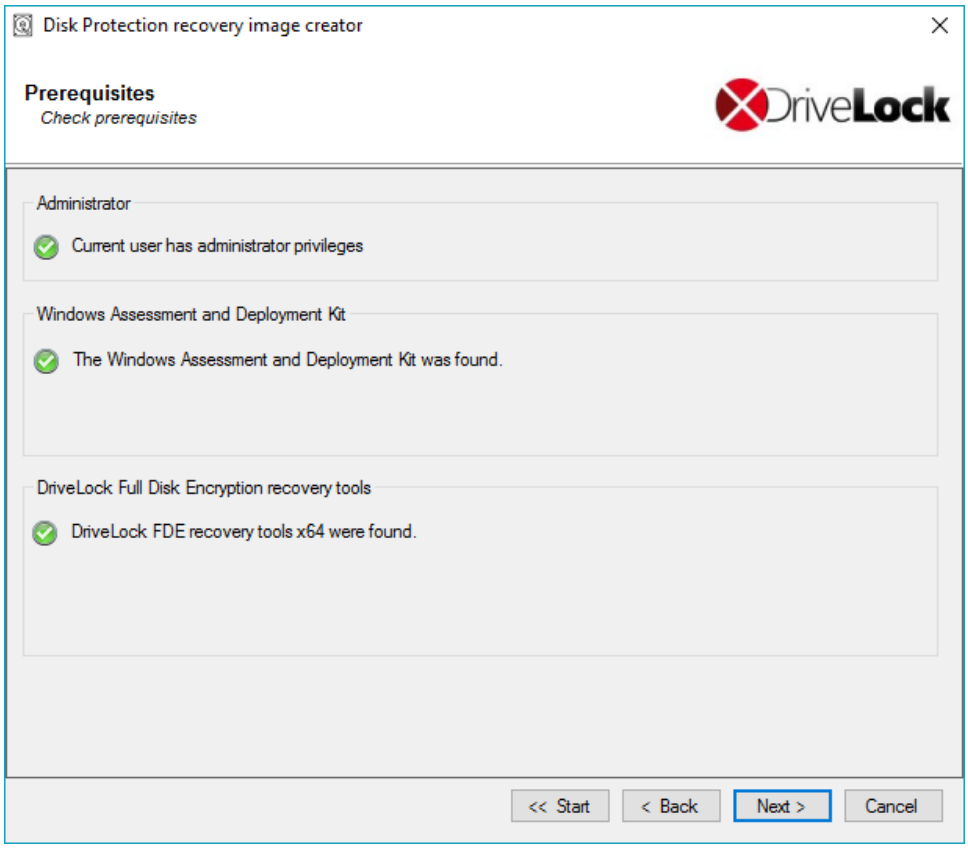


Das Windows ADK muss für die weiteren Schritte installiert sein.

Klicken Sie **Next**.

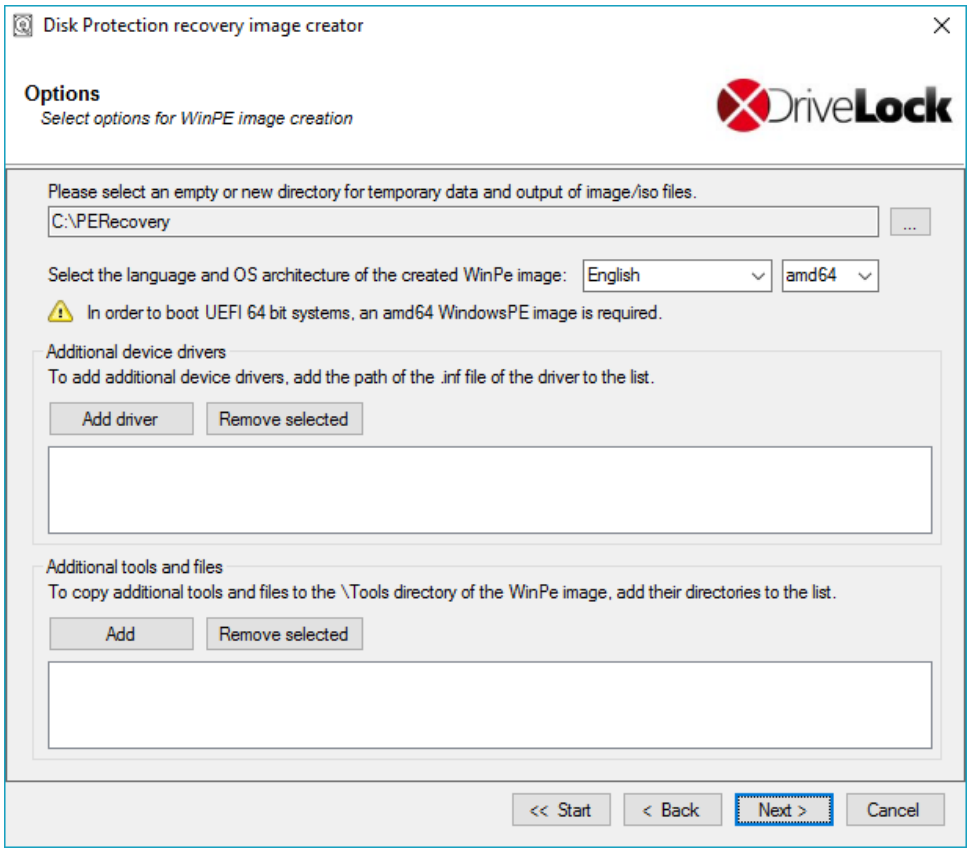


Aktivieren Sie die Option "*Accept license*" und klicken Sie **Next**.



Stellen Sie sicher, dass alle Vorbedingungen erfüllt und mit einem grünen Haken versehen sind.

Klicken Sie **Next**.

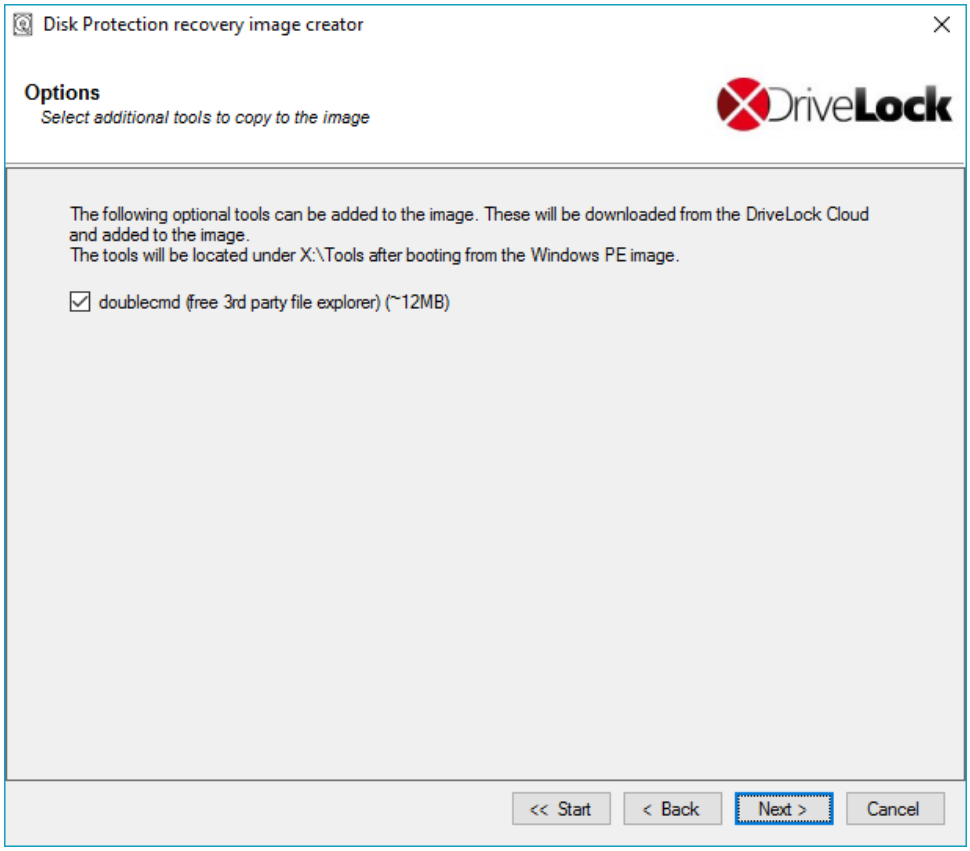


Nun geben Sie bitte das Verzeichnis an, in das die Ausgabedateien geschrieben werden sollen. Weiterhin wählen Sie die Sprache und die Zielarchitektur der zu verwendenden Windows PE Umgebung aus.

Für UEFI Systeme ist zwingend die Architektur "amd64" auszuwählen.

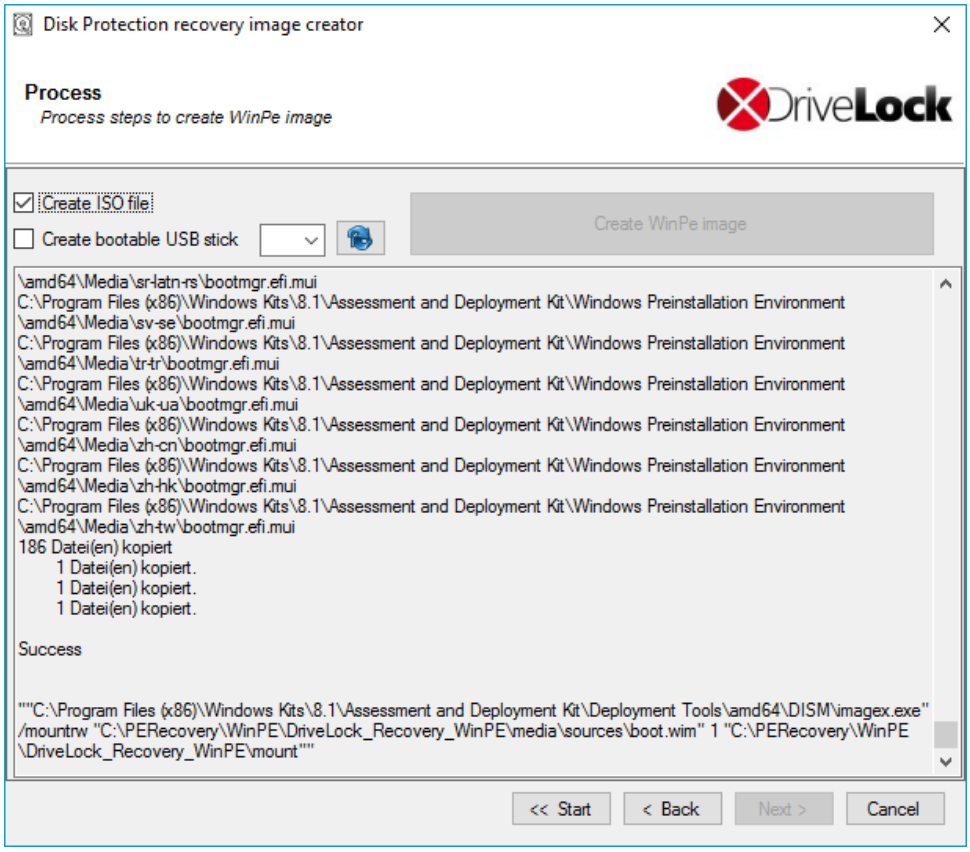
Sie können nun noch zusätzliche Treiber und weitere Tools angeben, die zur Windows PE Umgebung hinzugefügt werden sollen. Das können weitere Festplattentreiber oder jegliche andere Tools sein, die ohne einer Installation ausgeführt werden können (z.B. Antivirus-Scanner, Backup-Tools, weitere Dritt-Hersteller-Werkzeuge, etc.).

Wenn Sie alle gewünschten Änderungen vorgenommen haben, klicken Sie **Next**.



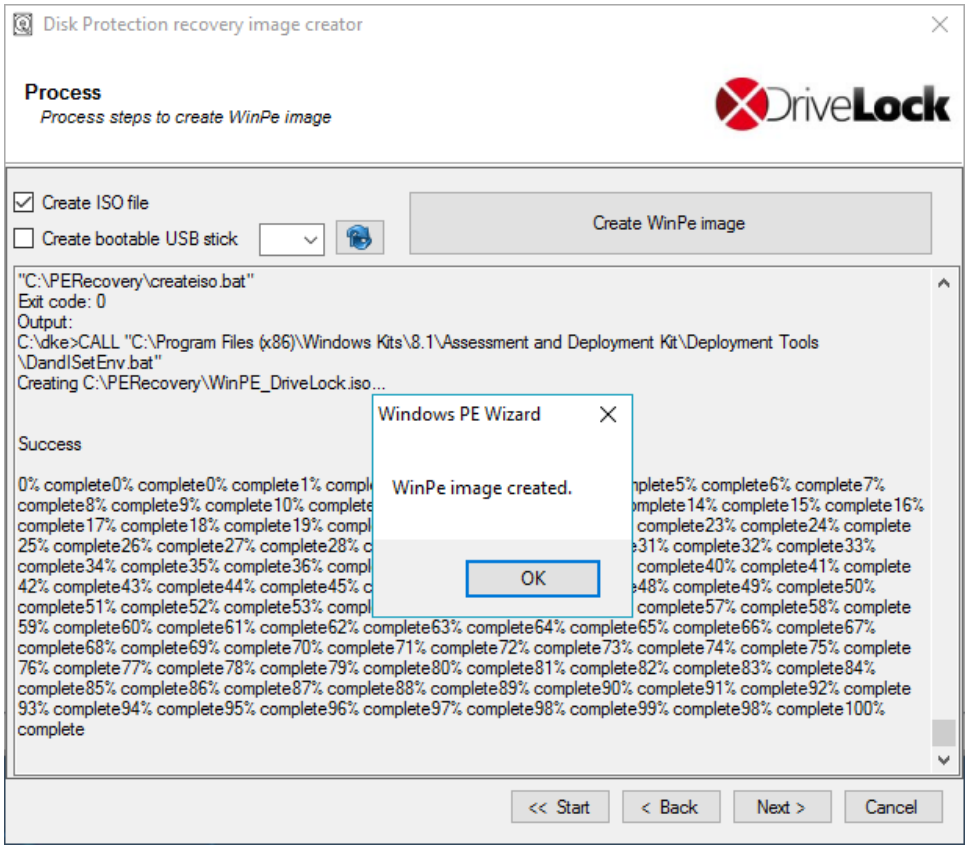
Zusätzlich können Sie nun noch einen frei verfügbaren Datei-Explorer hinzufügen, der von unserem Cloud-CDN zur Verfügung gestellt wird.

Klicken Sie nun **Next**.



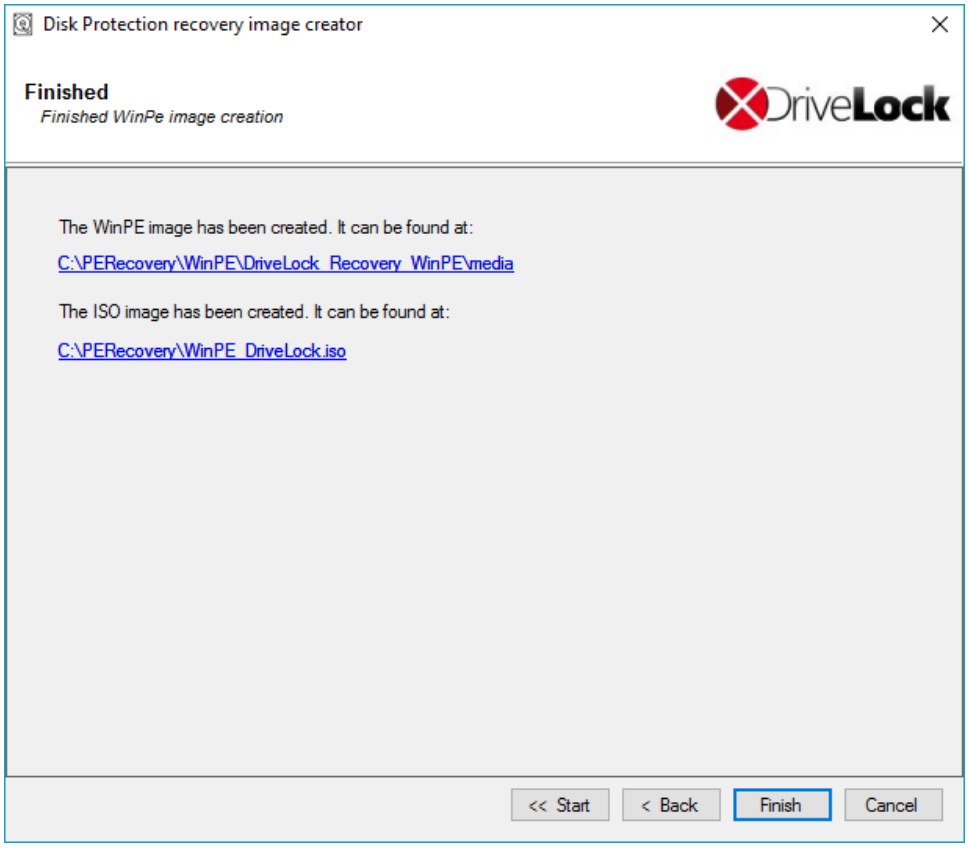
Nun wählen Sie aus, ob Sie eine bootfähige ISO-Datei oder einen bootfähigen USB-Stick erstellen möchten. Wenn Sie keine Auswahl treffen, wird lediglich eine Dateistruktur erzeugt, die Sie selbst manuell auf ein bootfähiges Medium kopieren müssen.

Starten Sie den automatischen Vorgang, indem Sie **Create WinPe image** klicken.



Sobald der Vorgang abgeschlossen ist, erscheint eine entsprechende Meldung.

Klicken Sie **Ok** und **Next**.



Wenn der Vorgang beendet ist, werden Ihnen die Links zum jeweiligen Verzeichnis angezeigt.

Klicken Sie **Finish**, um den Assistenten zu beenden.

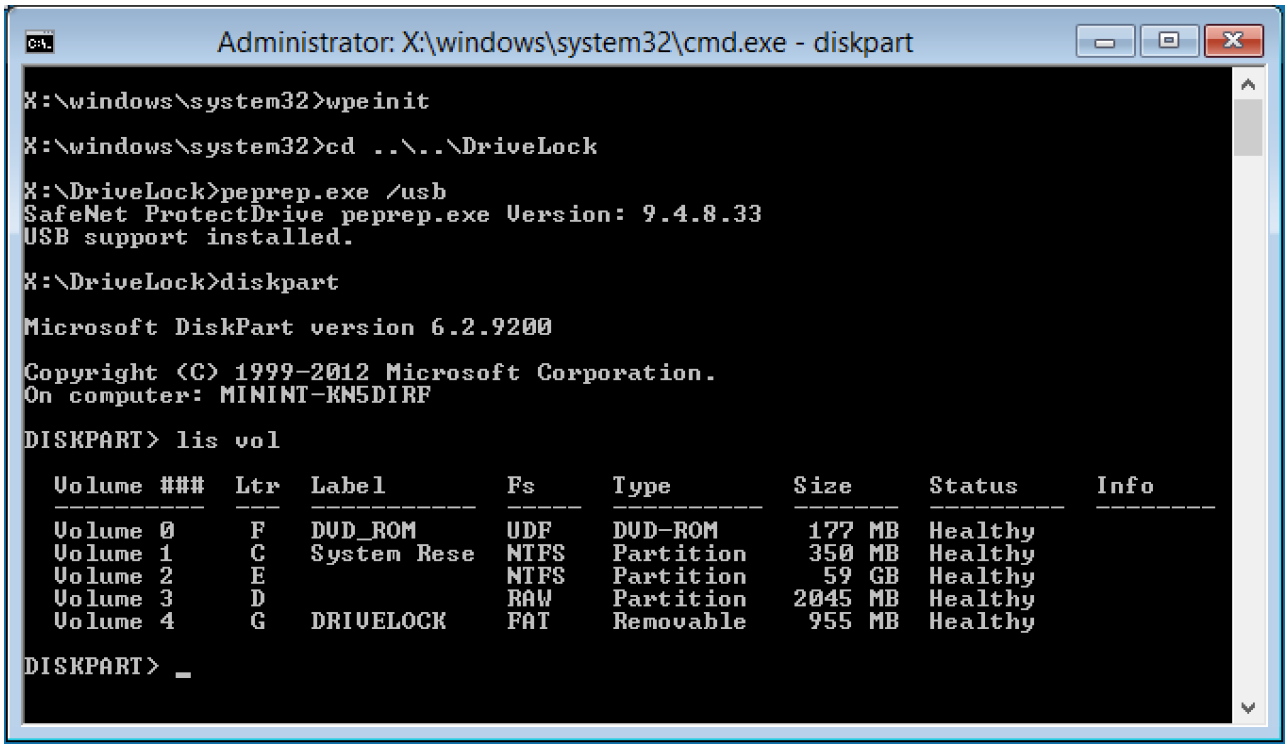
Diese Wiederherstellungs-CD enthält nun alle für die Wiederherstellung notwendigen Werkzeuge, Treiber und Wiederherstellungsdateien, die für einen Zugriff notwendig sind.

6.4.3.3 Wiederherstellung der Festplatte

Bevor Sie die Wiederherstellung starten können, stellen Sie sicher dass folgende Bedingungen erfüllt sind:

- Die notwendige *.pke Datei für den benötigten Computer wurde erstellt und auf einen USB-Stick kopiert (siehe Erstellung der notwendigen Dateien für die Entschlüsselung).
- Ein bootfähiges Windows PE Wiederherstellungsmedium wurde erstellt (siehe Erstellen einer Wiederherstellungs-CD)

Booten Sie nun den Rechner vom Wiederherstellungsmedium. Danach sehen Sie ein Kommandozeilen-Fenster mit einer Liste der verfügbaren Laufwerke (Volumes). Um diese Liste wieder anzuzeigen, verwenden Sie diesen Befehl: `echo lis vol | diskpart`



Verschlüsselte Laufwerke werden in der Spalte `Fs` als *RAW* angezeigt. Merken Sie sich nun den Laufwerksbuchstaben des USB-Sticks, welcher die Wiederherstellungsdatei enthält (ggf. den Stick einstecken und die Liste neu anzeigen lassen).

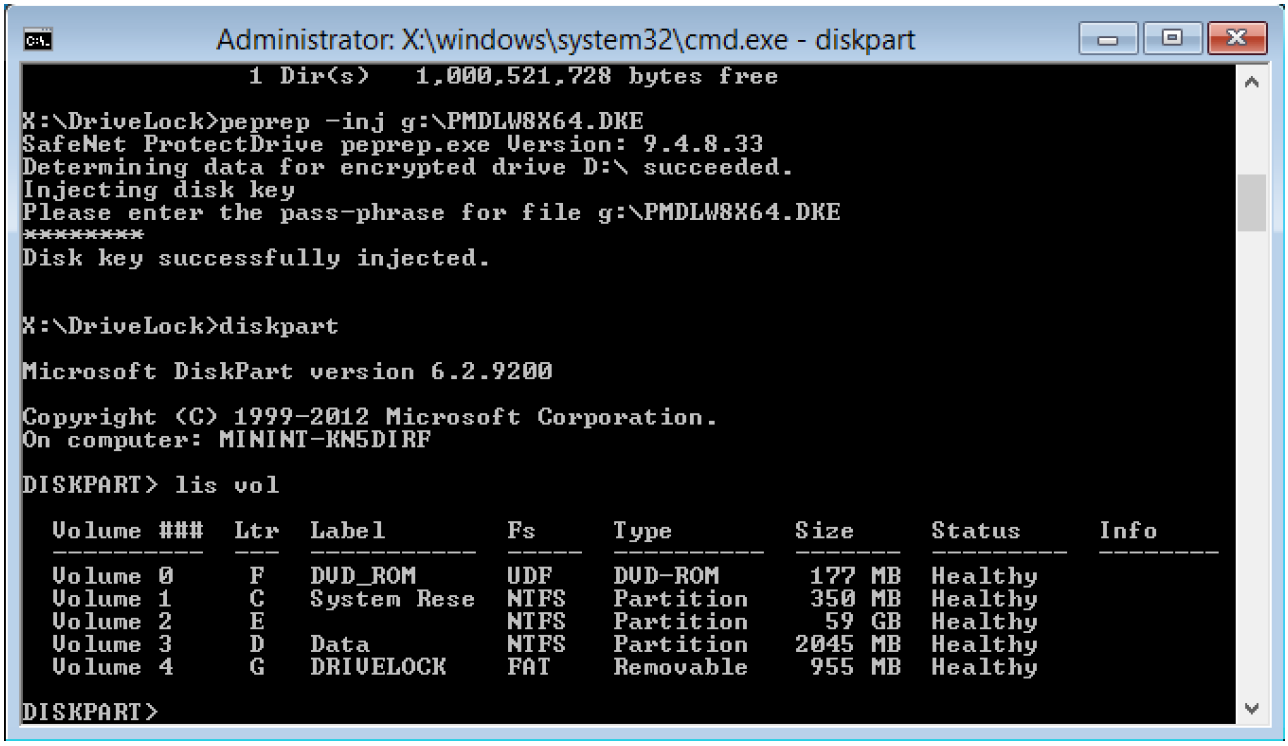
Geben Sie den Befehl `cd X:\DriveLock` *ein.*

Der folgende Befehl dient nun dazu, den Wiederherstellungsschlüssel für die Entschlüsselung dem System bekannt zu machen:

`peprep -inj <USB drive letter>:\<path to disk key file>`

In diesem Beispiel lautet der Befehl also `peprep -inj G:\PMDLW8X84.DKE`. Geben Sie nun das Kennwort ein, welches Sie bei der Erstellung der DKE-Datei verwendet haben.

Führen Sie den Befehl `echo lis vol | diskpart` erneut aus, um zu sehen ob der Wiederherstellungsschlüssel erfolgreich hinzugefügt wurde.



War die Aktion erfolgreich, wird das Laufwerk nicht mehr als *RAW* angezeigt.

Geben Sie `Exit` ein, um DISKPART zu verlassen.

Nun haben Sie Zugriff auf das Laufwerk (sofern kein schwerwiegenderer Fehler vorliegt) und können wichtige Dateien kopieren oder versuchen, die Festplatte zu reparieren.

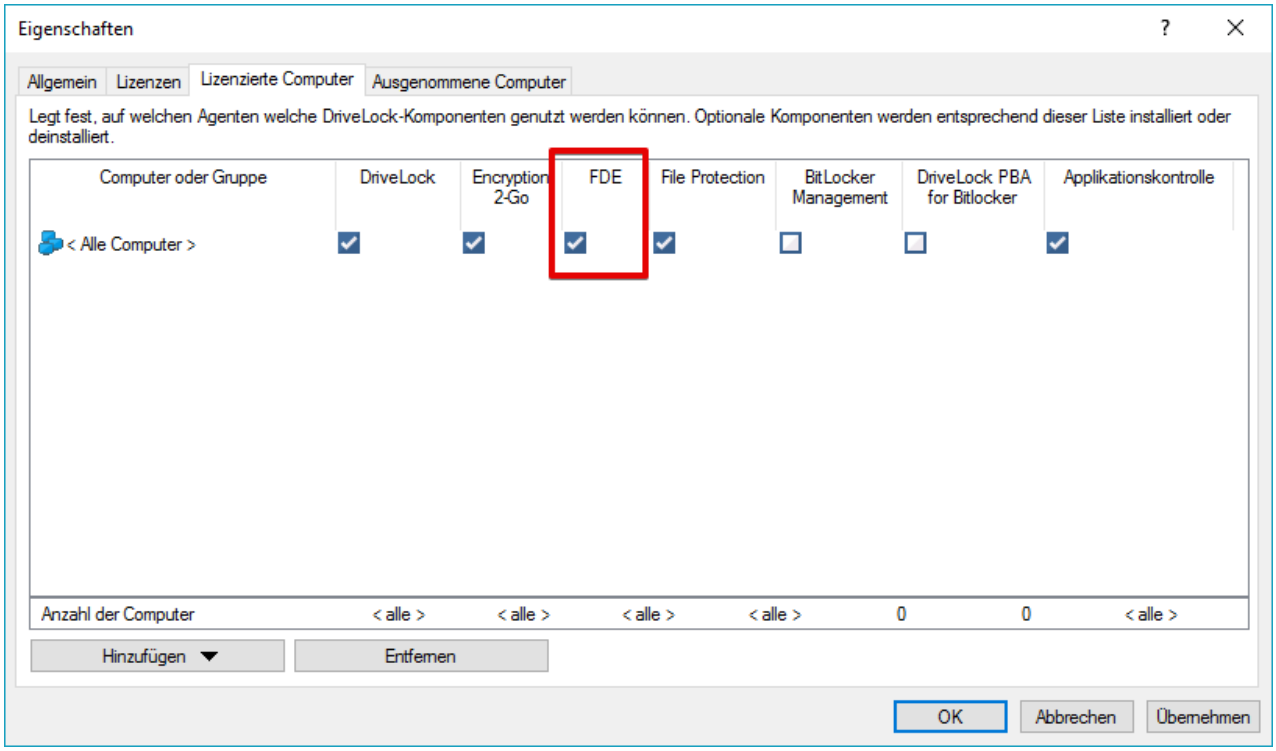
6.5 Deinstallation DriveLock Disk Protection

Disk Protection kann so konfiguriert werden, dass es alle zuvor verschlüsselten Festplatten am Client-Computer entschlüsselt, die Pre-Boot-Authentifizierung entfernt und DriveLock Full Disk Encryption deinstalliert.

Bitte beachten Sie, dass Änderungen an der Konfiguration üblicherweise alle Computer betrifft, welche über eine DriveLock Richtlinie mit dieser Konfiguration versorgt werden. Sofern Sie nur einzelne Computer deinstallieren möchten, finden Sie zusätzliche Hinweise im Abschnitt „Deinstallation / Überschreiben von Einstellungen / Umkonfiguration einzelner Systeme“.

6.5.1 Vollständige Deinstallation von DriveLock Disk Protection

Wenn auf einem oder mehreren Computer Disk Protection deinstalliert werden soll, erfolgt das über die FDE Lizenz (unter *Globale Einstellungen – Lizenz*) durch Entfernen des Hakens in der Spalte FDE:



Die Installation/Deinstallation der Disk Protection wird über die Lizenz gesteuert, die in einer den Computern zugewiesenen DriveLock Richtlinie aktiviert oder deaktiviert ist.

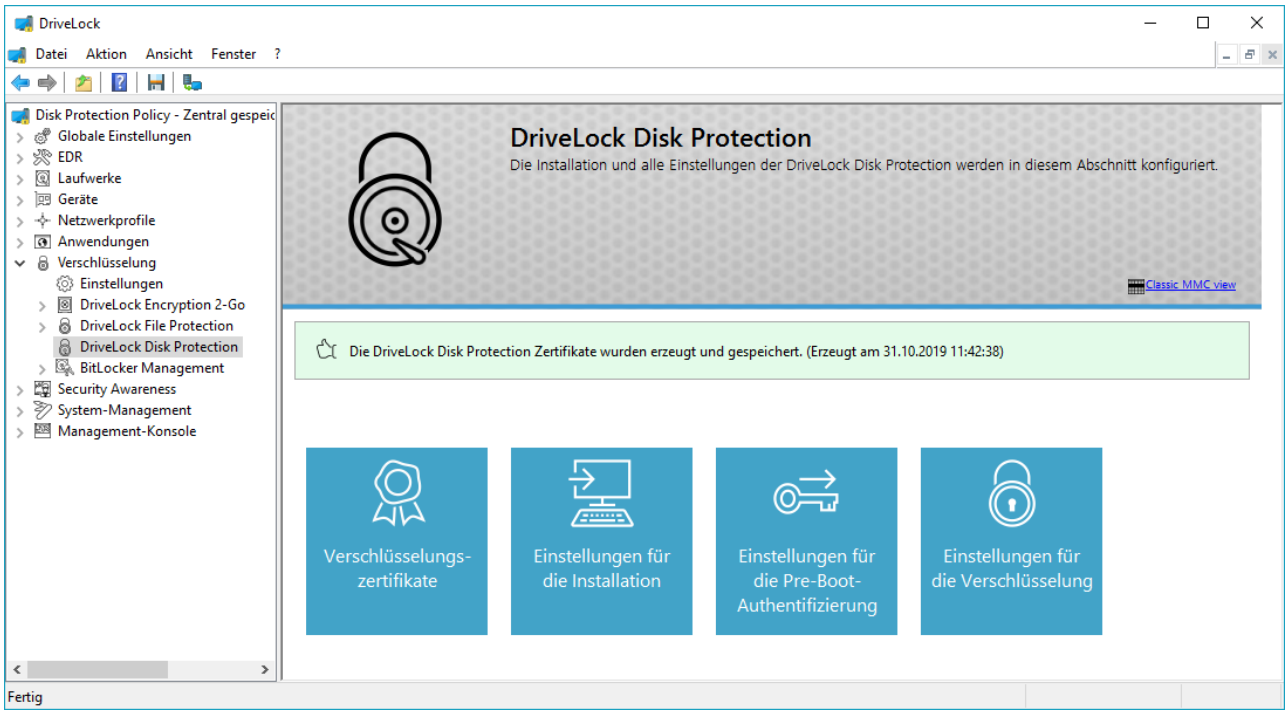
Wenn der Agent die neue Konfiguration mit deaktivierter FDE Lizenzoption bekommt, startet er mit der

1. Entschlüsselung aller verschlüsselten Laufwerke
2. Deaktivierung der Pre-Boot-Authentifizierung
3. Deinstallation der DriveLock Disk Protection

Das Disk Protection Installationspaket *DLFde_<Version>.pkg* muss separat entfernt werden, wenn es lokal auf dem Client installiert wurde.

6.5.2 Entschlüsseln der Festplatten

Man kann Disk Protection so konfigurieren, zunächst alle zuvor verschlüsselten Laufwerke zu entschlüsseln.



Um die Verschlüsselung auf Client-Computern zu deaktivieren, klicken Sie auf **Einstellungen für die Verschlüsselung**.

Deaktivieren Sie *"Lokale Festplatten auf Agenten-Computern verschlüsseln"* und klicken Sie auf **OK**, um das Fenster zu schließen.

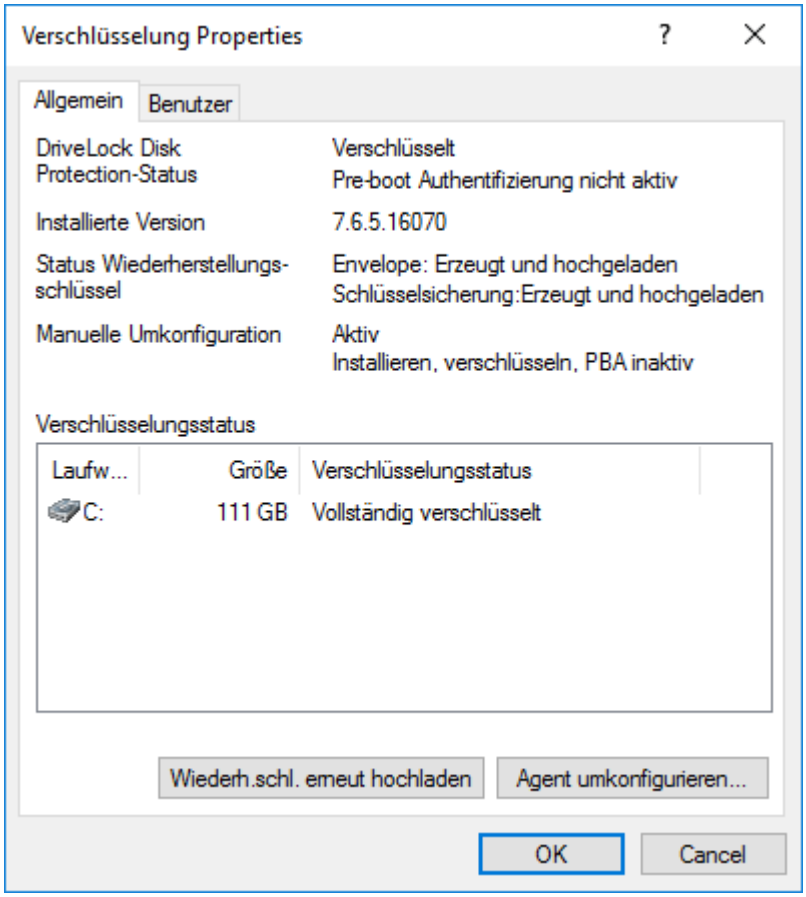
Wenn der Agent die neue Konfiguration bekommt, startet er mit der Entschlüsselung aller verschlüsselten Festplatten.

> Disk Protection und die Pre-Boot Authentifizierung werden dabei nicht von den Client-Computern entfernt.

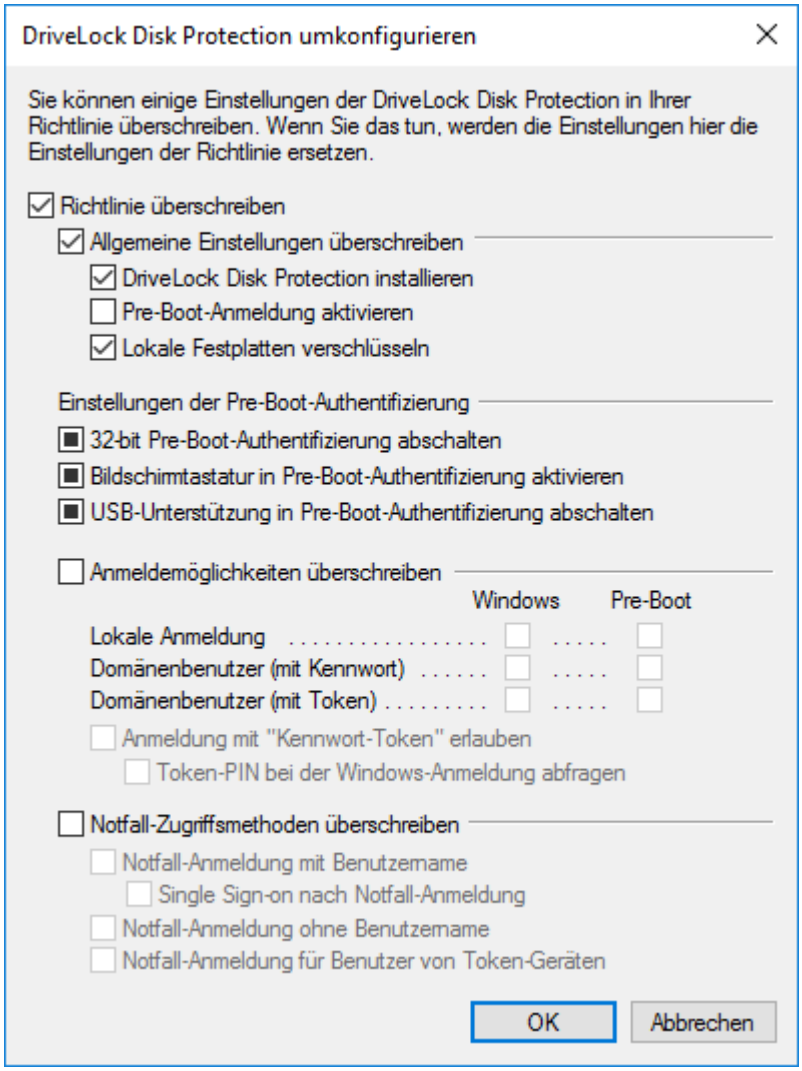
6.5.3 Deinstallation / Überschreiben von Einstellungen / Umkonfiguration einzelner Systeme

Wenn Sie Änderungen an der Disk Protection Konfiguration nur auf ganz bestimmten Computern vornehmen möchten (z.B. Deinstallation Disk Protection, Entschlüsselung der Festplatten), kann unabhängig von der zentralen Konfiguration die Einstellung speziell für einen einzelnen Agenten überschrieben werden. Dies geht mit Hilfe der Agenten-Fernkontrolle.

Verbinden Sie sich zuerst mit einem DriveLock-Agenten und wählen aus dem Kontextmenü *DriveLock Disk Protection Eigenschaften*.

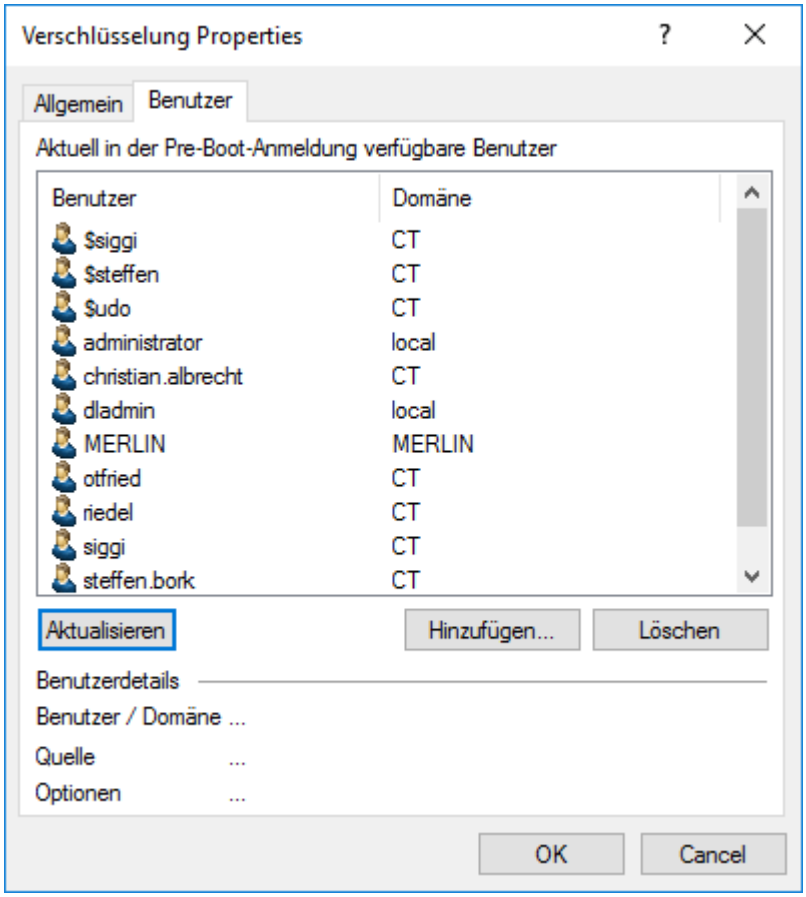


Nun klicken Sie auf **Agent umkonfigurieren.**



Markieren Sie *Richtlinie überschreiben* - Abweichend von der zentralen Richtlinie können Sie jetzt Rechner-spezifische Einstellungen konfigurieren, die nur für den gerade verbundenen Computer gelten.

Welche Benutzer in der PBA des Rechners hinterlegt sind, sehen Sie auf dem Reiter *Benutzer*. Sie können einzelne Benutzer hinzufügen oder löschen.



6.6 Benutzeranmeldung

Wenn die Systemrichtlinie so konfiguriert wurde, dass die Pre-Boot-Authentifizierung deaktiviert ist, dann findet keines der Inhalte in diesem Kapitel eine Anwendung. In diesem Fall erhält der Benutzer den Standard Windows-Domänen-Authentifizierungs-Dialog und die normale Windows Anmeldung wird angewandt.

6.6.1 UEFI Pre-Boot Authentifizierung

Weitere Informationen zur UEFI Pre-Boot Authentifizierung finden Sie im BitLocker Management Handbuch auf DriveLock.help. Hier finden Sie die aktuelle Information zur DriveLock PBA.

Die nachfolgenden Abschnitte beschreiben das Systemverhalten, wenn die DriveLock PBA auf einem UEFI-System installiert wurde.

Im Gegensatz zu früheren Versionen ist eine Verwendung von Funktionstasten nicht mehr notwendig.

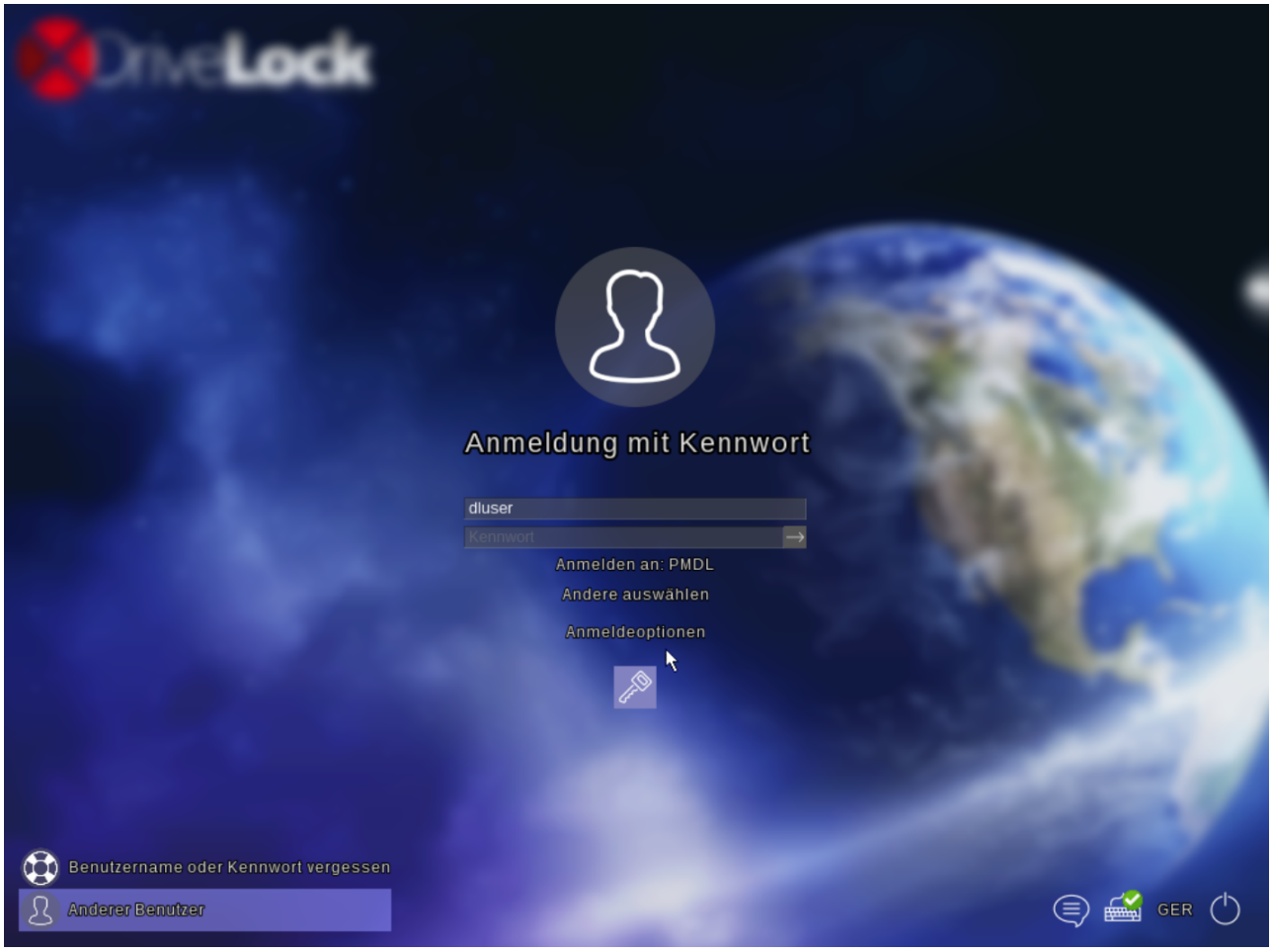
Nachdem ein Rechner mit aktivierter PBA gestartet wurde, erscheint zunächst eine kurze Textanzeige "DriveLock Pre-Boot Authentication" und anschließend der Startbildschirm:

Drücken Sie eine beliebige Taste oder klicken Sie mit der Maus, um wie unter Windows 10 zum Anmeldebildschirm zu gelangen.

Informationen zu den Hot-Keys sind im Kapitel Abkürzungs- und Funktionstasten in der BitLocker-Management-Dokumentation.

Haben Sie eine dieser Funktionen über die Kommandozeile permanent aktiviert oder deaktiviert, können Sie mit Hilfe der Hotkeys diese einmal wieder deaktivieren bzw. aktivieren.

6.6.1.1 Authentifizierung mit Benutzername und Passwort

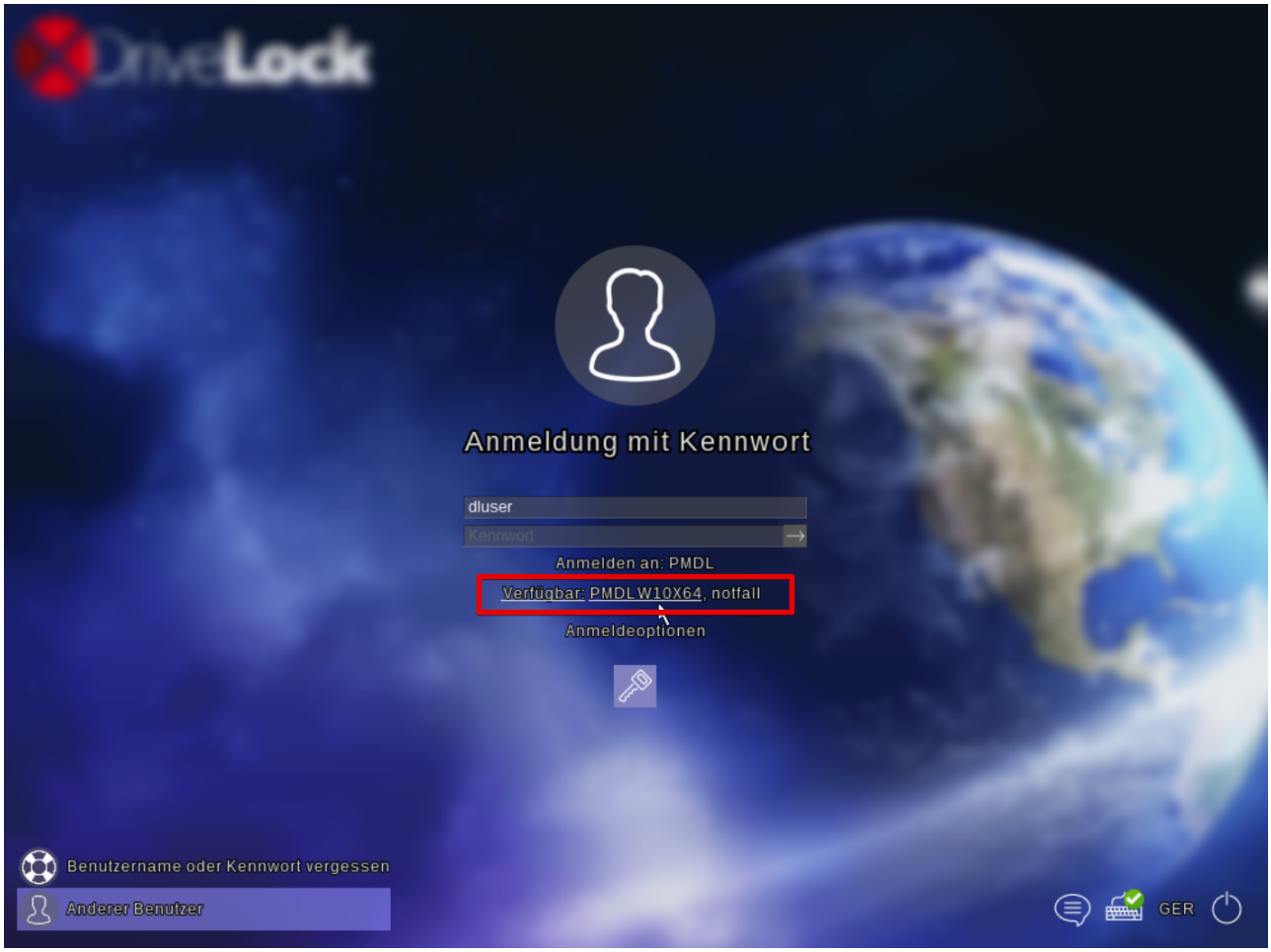


Die DriveLock PBA unterstützt sowohl die Auswahl mit der Maus, als auch die Navigation mit der Tastatur.

> Möchten Sie ausschließlich die Tastatur verwenden, navigieren Sie mit Hilfe der TAB-Taste zum nächsten Element. Mit ENTER oder der Leertaste wählen Sie das aktive Element aus. Mit ESC können Sie die Anzeige des Hilfetextes schließen.

Geben Sie zur Anmeldung den unter Windows eingerichteten Benutzernamen und das dazugehörige Passwort in die entsprechenden Felder ein. Die aktive Domäne wird nach "*Anmelden an:*" angezeigt.

Klicken Sie auf **Andere auswählen**, erscheint eine Liste aller bekannten Domänen inklusive des lokalen Rechners und eventuell manuell eingerichteter Domänen:



Nach der Eingabe des richtigen Passwortes, startet die Anmeldung nach Drücken der Eingabetaste oder durch einen Klick auf das Pfeil-Symbol rechts neben dem Passwortfeld.

Die DriveLock PBA erlaubt die Auswahl von anderen Tastaturlayouts. Die Liste der verfügbaren Layouts kann über das Symbol der aktuell eingestellten Sprache rechts unten aufgerufen werden:

Wählen Sie so das gewünschte Tastaturlayout aus. Beim nächsten Start wird sofort das bisher ausgewählte Layout voreingestellt.

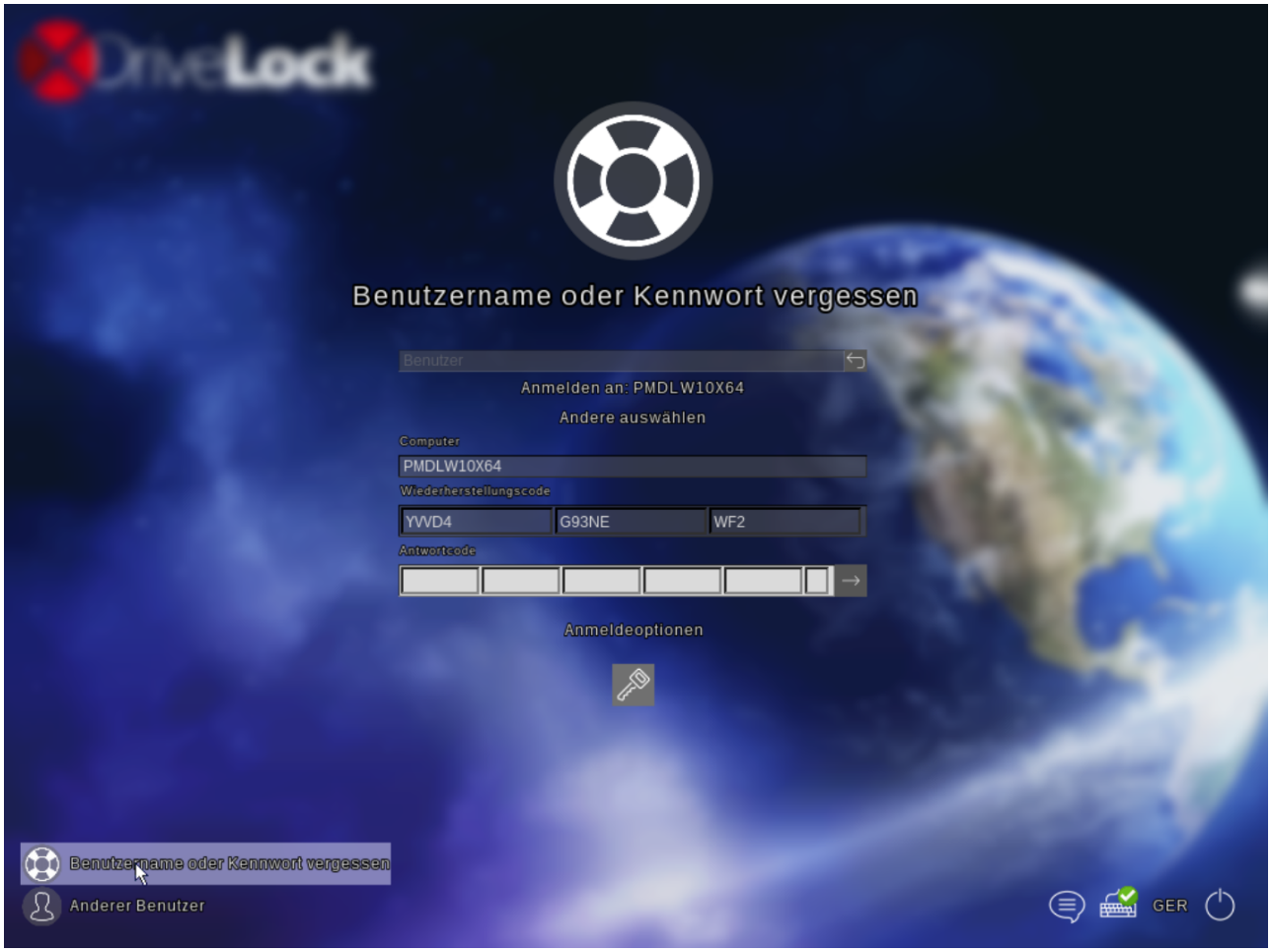
Wurde in der Richtlinie die Option für die virtuelle Tastatur (On-Screen Keyboard) aktiviert, können Sie über das Tastatur-Symbol steuern, ob Ihnen bei Auswahl eines Eingabefeldes die virtuelle Tastatur angezeigt wird oder nicht:

Damit ist auch auf Tablets, die nur über einen Touch-Screen und keine physikalische Tastatur verfügen, eine Anmeldung innerhalb der DriveLock PBA möglich.

> Sie müssen das Benutzer- oder Passwort-Eingabefeld aktiviert haben, damit die Tastatur eingeblendet wird.

> Das zuvor eingestellte Tastaturlayout hat Auswirkungen darauf, welche Tasten Ihnen die virtuelle Tastatur anzeigt.

Haben Sie Ihr Windows-Passwort vergessen, klicken Sie links unten auf **Benutzername oder Kennwort vergessen**. Danach erscheint der Dialog für die Notfallanmeldung:

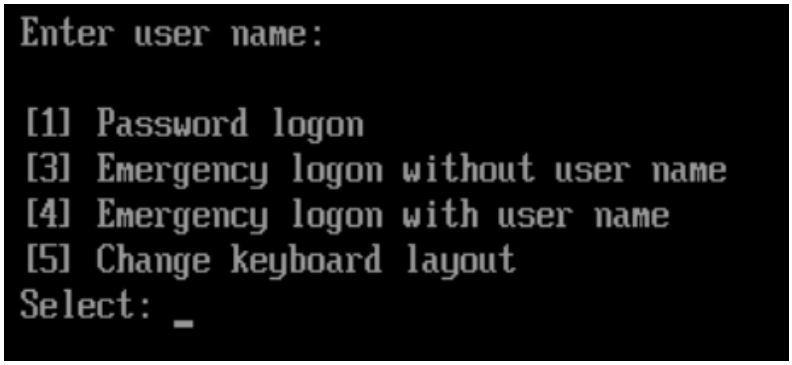


Stellen Sie zunächst bitte sicher, dass die richtige Domäne ausgewählt ist (in der Regel keine lokale Anmeldung).

Die weiteren Schritte zur Notfall-Anmeldung sind im Kapitel Notfall Anmeldeverfahren beschrieben.

Über das Schalter-Symbol unten rechts können Sie entweder das System herunterfahren/beenden oder zum Textmodus ohne grafische Anzeige wechseln.

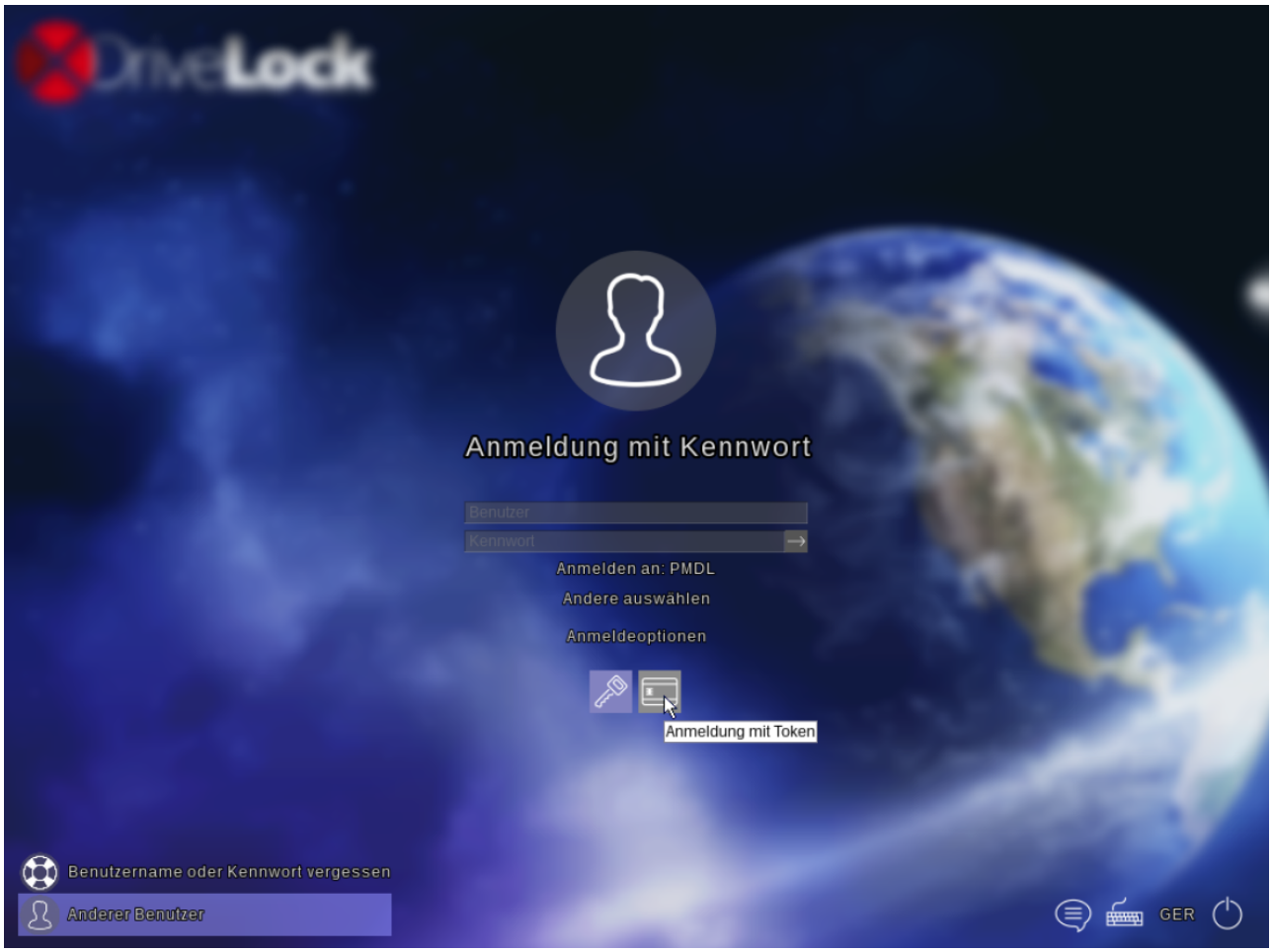
Im Textmodus steht Ihnen für die Anmeldung bzw. die Notfall-Anmeldung nur eine einfache Konsole zur Verfügung:



Wählen Sie hier die gewünschte Option über die Eingabe der angezeigten Zahl aus und geben Sie die geforderten Daten ein.

6.6.1.2 Smartcard Authentifizierung

Die DriveLock PBA erlaubt auch die Authentifizierung über Smartcards bzw. bestimmte eTokens.

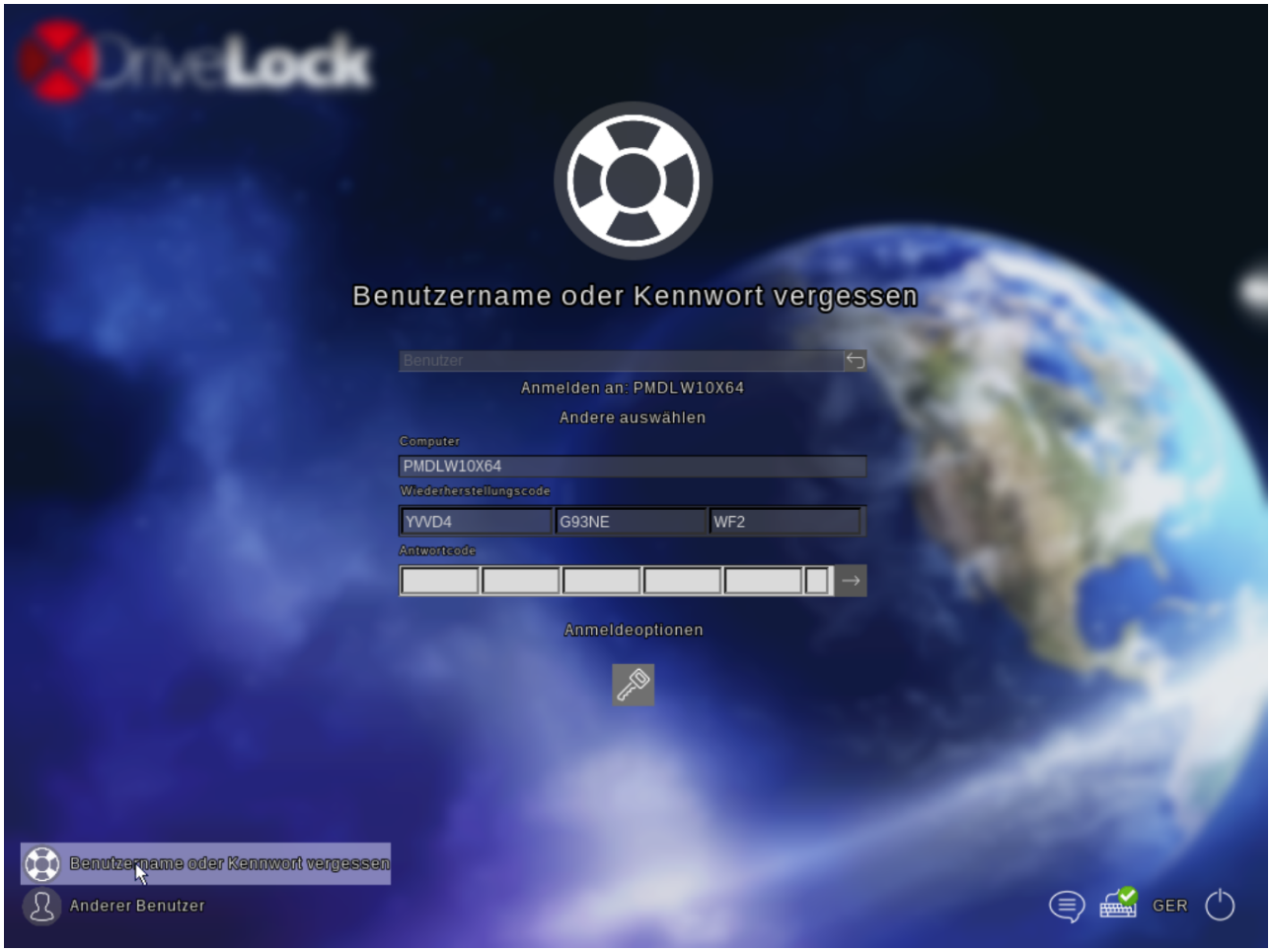


> Der Technische Artikel "*TA - Supported Smart Cards and Tokens in PBA.pdf*", welcher sich auch auf dem DriveLock ISO-Datenträger befindet, enthält alle derzeit unterstützen Smartcards und Tokens.

Wenn in der DriveLock Richtlinie die entsprechenden Anmeldeoptionen aktiviert wurden, können über die angezeigten Symbole diese analog zur Windows-Anmeldung ausgewählt werden.

Geben Sie nun die PIN für die Smartcard oder den Token ein und drücken Sie die ENTER-Taste um sich damit anzumelden.

Sollten Sie Ihre PIN vergessen haben, klicken Sie links unten auf **Benutzername oder Kennwort vergessen**. Danach erscheint der Dialog für die Notfallanmeldung:



Stellen Sie zunächst bitte sicher, dass die richtige Domäne ausgewählt ist (in der Regel keine lokale Anmeldung) und das kein Benutzername eingegeben ist.

Die weiteren Schritte zur Notfall-Anmeldung sind im Kapitel Notfall Anmeldeverfahren beschrieben.

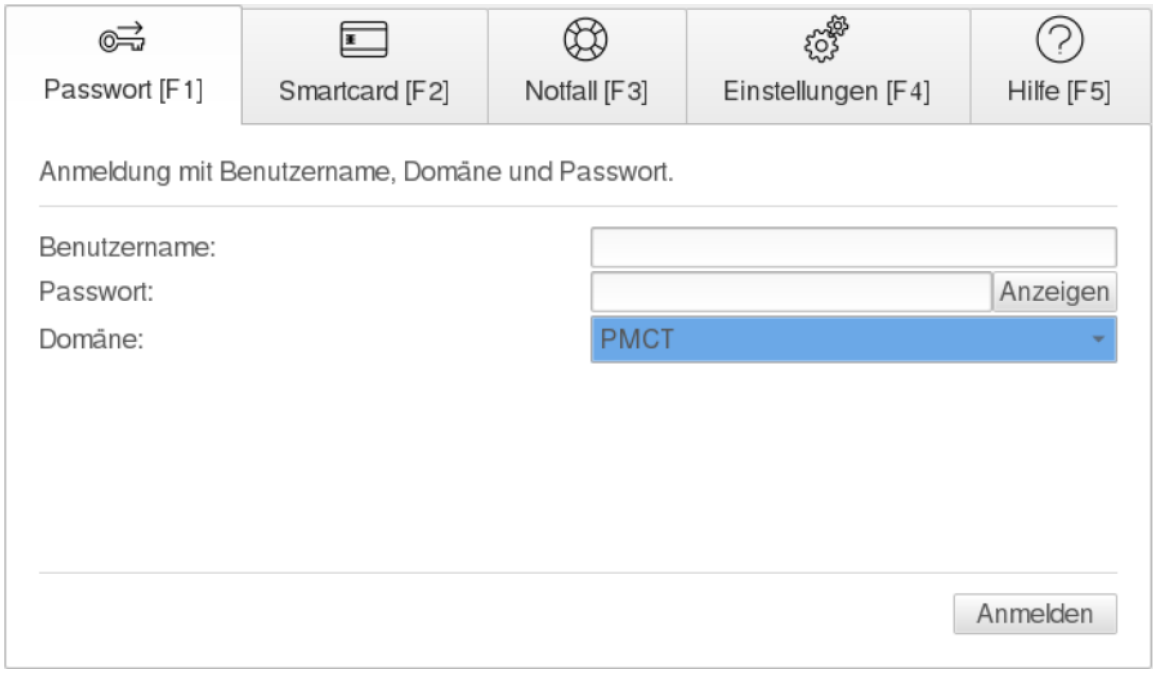
6.6.2 BIOS Pre-Boot Authentifizierung

Die nachfolgenden Abschnitte beschreiben das Systemverhalten, wenn die Disk Protection PBA auf einem Legacy-BIOS System installiert wurde.

> Mit Hilfe der am Bildschirm angezeigten Funktionstasten können Benutzer zu den jeweiligen Ansichten/Funktionen wechseln.

6.6.2.1 Authentifizierung mit Benutzername, Passwort und Domänenname

Wenn entweder die Authentifizierungs-Methoden Lokale Anmeldung oder Domänenbenutzer (mit Kennwort) aktiviert sind, wird DriveLock Disk Protection den Bildschirm wie unten anzeigen:



Wenn beide Authentifizierungs-Optionen *Lokale Anmeldung* und/oder *Domänenbenutzer (mit Kennwort)* aktiviert sind, wird durch Drücken der Funktionstaste **F2** zum Smartcard Anmeldebildschirm umgeschaltet.

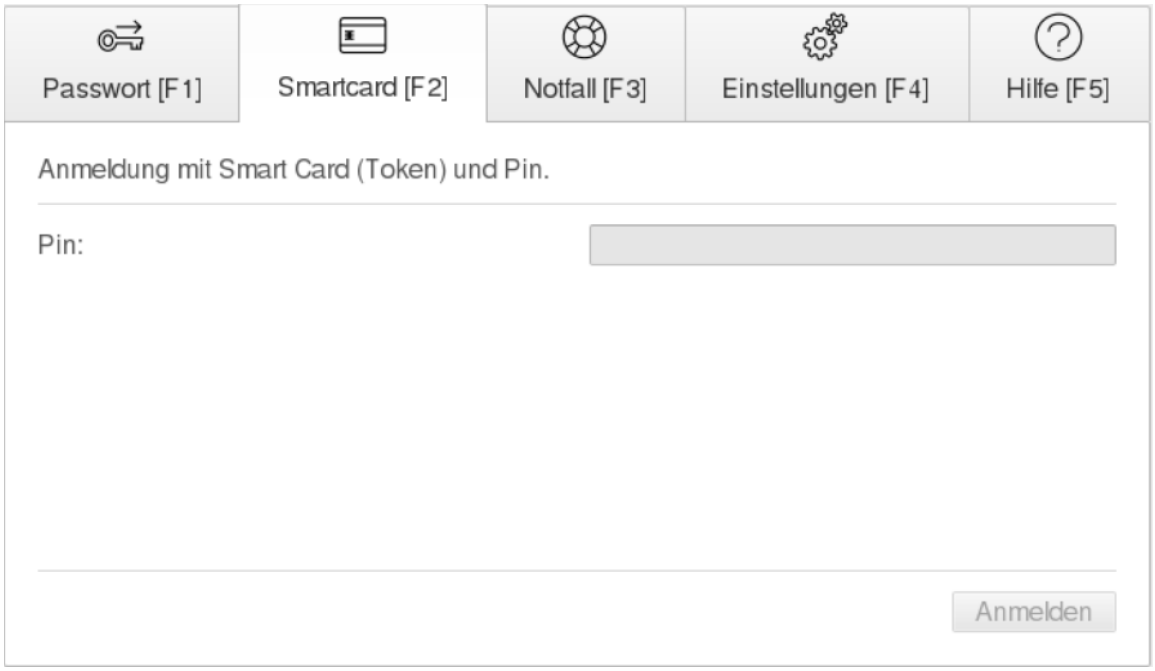
Das Feld *Domäne* enthält alle relevanten Domänen, wenn *Domänenbenutzer (mit Kennwort)* Option ausgewählt wurde. Der lokale Systemname kann ebenfalls in diesem Feld eingetragen sein. Benutzen Sie den [Pfeil-hoch] und [Pfeil-runter] um durch die Liste der verfügbaren Domänennamen zu blättern.

Beachten Sie, dass im Fall von aufeinanderfolgenden, fehlerhaften Pre-Boot Authentifizierungsversuchen die Sperr-Richtlinie erzwungen wird, um ein Erraten des Passwortes zu verhindern. Öffnen Sie unter Windows das Ereignisprotokoll des Systems, um weitere Details zu den fehlerhaften Login-Versuchen und anderen Ereignissen zu entnehmen.

Wenn der Benutzer sich nicht mehr an dem System anmelden kann (z.B. er erinnert sich nicht an das korrekte Passwort), kann das *Notfall Anmeldeverfahren mit Benutzername* gestartet werden. Siehe Kapitel „Notfall Anmeldeverfahren“ für weitere Informationen.

6.6.2.2 Authentifizierung mit Smartcard/Token und PIN

Wenn die Disk Protection Authentifizierungs-Methoden Domänenbenutzer (mit Token) oder Zugriff mit Shared Key aktiviert sind, dann sieht das Pre-Boot-Authentifizierungs-Fenster wie unten abgebildet aus:



Wenn beide Authentifizierungs-Optionen *Lokale Anmeldung* und/oder *Domänenbenutzer (mit Kennwort)* aktiviert sind, wird durch Drücken der Funktionstaste **F1** zum Benutzernamen/Passwort/Domänennamen Bildschirm umgeschaltet.

An diesem Punkt kann sich der Benutzer mit seiner Smartcard/Token und PIN am System authentifizieren. Bitte beachten Sie, dass in dem Fall von aufeinanderfolgenden fehlerhaften Pre-Boot Authentifizierungsversuchen die Sperr-Richtlinie erzwungen wird, um ein Erraten der PIN zu verhindern (Öffnen Sie das *Ereignisprotokoll* des Systems, um weitere Details zu den fehlerhaften Login-Versuchen und anderen Ereignissen zu entnehmen).

Wenn der Benutzer sich nicht an seine korrekte PIN erinnert und sich deshalb nicht am System anmelden kann, kann das *Notfall Anmeldeverfahren für Token Benutzer* gestartet werden. Siehe Kapitel „Notfall Anmeldeverfahren“ für mehr Informationen zur Notfall-Anmeldung.

6.6.3 Windows-Authentifizierung

Jedes Mal wenn sich ein Benutzer erfolgreich manuell an Windows anmeldet, wird das jeweils aktuellste Windows-Passwort der Pre-Boot Benutzerdatenbank hinzugefügt. Das gleiche passiert, wenn ein Benutzer sein persönliches Passwort unter Windows ändert.

Das Verhalten der Anmeldung hängt von der Einstellung in der DriveLock Richtlinie ab:

- *Automatisch - Single Sign-On Modus ist eingeschaltet*: der Benutzer wird automatisch bei Windows angemeldet.
- *Manuell - Single Sign-On Modus ist ausgeschaltet*: der Windows-Anmelde-Bildschirm angezeigt und der Benutzer muss sich mit seinen persönlichen Anmeldeinformationen anmelden.

Teil VII

DriveLock Encryption 2-Go

7 DriveLock Encryption 2-Go

DriveLock ist mit zusätzlichen Verschlüsselungsfähigkeiten ausgestattet, die die Verschlüsselung von vertraulichen Daten auf einfache, schnelle und sichere Weise ermöglichen.

Die DriveLock Festplattenverschlüsselung (DriveLock Disk Protection, FDE) verschlüsselt komplette Festplatten in Computern und bietet zusätzlich eine sichere Pre-Boot-Authentifizierung. Diese wird in einem anderen Kapitel des Handbuches beschrieben.

DriveLock Encryption 2-Go beinhaltet im Gegensatz zur Festplattenverschlüsselung die sichere Verschlüsselung externer Datenträger (wie z.B. USB-Sticks oder SD-Karten und das sichere Löschen von Dateien mit Hilfe standardisierter, irreversibler Verfahren.

Dieses Kapitel beschreibt die vielfältigen Möglichkeiten der Verschlüsselung externer Datenträger, insbesondere die Konfiguration der Verschlüsselungsparameter. Die Verwendung verschlüsselter Medien bzw. das Verschlüsseln von externen Laufwerken durch den Benutzer wird im DriveLock Benutzerhandbuch erläutert.

Mit DriveLock können Sie entweder

- die **Container-basierte (DriveLock Encryption 2-Go)** Verschlüsselung, so wie in vorhergehenden DriveLock Versionen, oder
- die **Datei-basierte (DriveLock File Protection)** Verschlüsselung, so wie bisher nur mit dem DriveLock File Protection Add-on oder
- die **Container-basierte und Datei-basierte** Verschlüsselung parallel nutzen und die Anwender entscheiden lassen.

Öffnen Sie in der DriveLock Richtlinie **Verschlüsselung / Einstellungen / Verfügbare Verschlüsselungsmethoden** und wählen die gewünschte Option.

Um DriveLock File Protection mit Netzwerk Laufwerken zu nutzen benötigen Sie weiterhin eine Lizenz für DriveLock File Protection.

Mehr Informationen zu DriveLock File Protection finden Sie im Kapitel DriveLock File Protection.

7.1 Wie funktioniert die DriveLock Verschlüsselung

Verschlüsselte Laufwerke werden als einzelne Container Dateien realisiert. Der Zugriff auf diese Dateien ist passwortgeschützt; ein administratives Masterpasswort stellt den Zugriff auf die Daten sicher, falls das Benutzerpasswort verloren gegangen ist. Zusätzlich gibt es bei DriveLock die Möglichkeit, das Passwort mit Hilfe eines Offline-Verfahrens zurückzusetzen.

Verschlüsselte Daten scheinen aus zufälligen Buchstaben und Zahlen zu bestehen. Innerhalb eines verschlüsselten Laufwerks sind auch Datei- und Verzeichnisnamen ebenso wie freier Platz verschlüsselt. Die Verschlüsselungsmethode definiert, auf welche Art und Weise Daten auf dem jeweiligen Laufwerk verschlüsselt werden.

Auf neueren Systemen erfolgt die Ver- und Entschlüsselung durch bereits im Prozessor vorhandene Verschlüsselungsalgorithmen (AES NI), was zu einer deutlichen Verbesserung der Geschwindigkeit dabei führt (ca. 4x schneller).

7.1.1 DriveLock Verschlüsselungsverfahren

DriveLock unterstützt folgende Verschlüsselungsverfahren:

- *AES* (empfohlen) - Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptoverfahren, welches als Nachfolger für DES bzw. 3DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt gegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch

Rijndael-Algorithmus genannt.
DriveLock verwendet eine Schlüssellänge von 256 Bits, (AES-256), welche nach aktuellem Stand der Technik als ausreichend sicher für die Verschlüsselung vertraulicher Informationen angesehen wird.

- *Triple DES* - Symmetrisches Verschlüsselungsverfahren, das auf dem klassischen → DES basiert, jedoch mit der doppelten Schlüssellänge arbeitet (112 Bit). Die zu verschlüsselnden Daten werden mit einer dreifachen Kombination des klassischen DES verschlüsselt. Aufgrund der Schlüssellänge gilt Triple-DES derzeit noch als sicheres Verfahren im Gegensatz zum einfachen DES, der durch Brute-Force-Attacken (bloßes Probieren von Schlüsseln) angreifbar ist.
- *Blowfish* - Dieser sehr schnelle Algorithmus bietet besonders bei 32-Bit-Prozessoren eine gute Leistung. Ein Vorteil von Blowfish ist seine variable Schlüssellänge von 32 bis zu 448 Bits. Blowfish gilt als sehr sicher. Der Algorithmus wurde 1994 zum ersten Mal vorgestellt
- *Twofish* - Twofish ist der AES-Beitrag von Counterpane Systems, der Firma von Bruce Schneier. Der Algorithmus benutzt eine Blockgröße von 128 Bit und kann mit Schlüsseln von 128 bis 256 Bit betrieben werden. Twofish ist sehr schnell; auf einem Pentium wird ein Byte in 18 CPU-Takten verschlüsselt. Twofish wurde bisher sehr intensiv geprüft, ohne dass Schwachstellen gefunden worden wären.
- *CAST 5* - CAST ist eine symmetrische Blockchiffre mit 64 Bit Blocklänge und einer Schlüssellänge von 40-128 Bit. Der CAST Algorithmus wurde nach seinen Entwicklern Carlisle Adams und Stafford Tavares benannt und 1996 zum Patent angemeldet. Wegen seiner höheren Geschwindigkeit gegenüber DES ist CAST auch für Echtzeitanwendungen geeignet. Schlüssellängen von 80 bis 128 Bit werden als CAST-5 bezeichnet.
- *Serpent* -- ist ein symmetrischer Verschlüsselungsalgorithmus, der von den Kryptografen Ross Anderson, Eli Biham und Lars Knudsen entwickelt wurde. Dieser Algorithmus war ein Kandidat für den Advanced Encryption Standard und gehörte mit Twofish, Rijndael, MARS und RC6 zu den fünf Finalisten des AES-Standard-Ausscheidungsverfahrens. Gegensatz zu den beiden anderen als hoch-sicher eingestuften Kandidaten der letzten Runde, MARS und Twofish, wurde Serpent bezüglich seiner Sicherheit nicht kritisiert und es wurde angenommen, dass dieser der sicherste Verschlüsselungsalgorithmus der fünf Finalisten sei.

Mit einem Hash Algorithmus verschlüsselt DriveLock das Passwort, mit welchem das verschlüsselte Laufwerk ver- bzw. entschlüsselt wird. DriveLock unterstützt folge Hash Verfahren:

- *SHA* - Das NIST (National Institute of Standards and Technology) entwickelte zusammen mit der NSA (National Security Agency) eine zum Signieren gedachte sichere Hash-Funktion als Bestandteil des Digital Signatur Algorithms (DSA) für den Digital Signature Standard (DSS). Die Funktion wurde 1994 veröffentlicht. Diese als Secure Hash Standard (SHS) bezeichnete Norm spezifiziert den sicheren Hash-Algorithmus (SHA) mit einem Hash-Wert von 160 Bit Länge für Nachrichten mit einer Größe von bis zu 264 Bit. Der Algorithmus ähnelt im Aufbau dem von Ronald L. Rivest entwickelten MD4. Der sichere Hash-Algorithmus existiert zunächst in zwei Varianten, SHA-0 und SHA-1, die sich in der Anzahl der durchlaufenen Runden bei der Generierung des Hashwertes unterscheiden. Das NIST hat im August 2002 drei weitere Varianten („SHA-2“) des Algorithmus veröffentlicht, die größere Hash-Werte erzeugen. Es handelt sich dabei um den SHA-256, SHA-384 und SHA-512 wobei die angefügte Zahl jeweils die Länge des Hash-Werts (in Bit) angibt.
- *RIPEMD-160* - RIPEMD-160 wurde von Hans Dobbertin, Antoon Bosselaers und Bart Preneel in Europa entwickelt und 1996 erstmals publiziert. Es handelt sich dabei um eine verbesserte Version von RIPEMD, welcher wiederum auf den Design Prinzipien von MD4 basiert und in Hinsicht auf seine Stärke und Performanz dem populäreren SHA-1 gleicht. Da die Entwicklung von RIPEMD-160 offener war als die von SHA-1, ist es wahrscheinlicher, dass dieser Algorithmus weniger Sicherheitslücken aufweist.
- *WHIRLPOOL* – WHIRLPOOL ist eine kryptologische Hash-Funktion, die von Vincent Rijmen und Paulo S. L. M. Barreto entworfen wurde. Sie wurde nach der Whirlpool-Galaxie im Sternbild der Jagdhunde benannt. Whirlpool gehört zu den vom Projekt NESSIE empfohlenen kryptografischen Algorithmen und wurde von der ISO mit ISO/IEC 10118-3:2004 standardisiert.

7.1.2 DriveLock Verschlüsselungsarten

DriveLock unterscheidet zwei Arten von Laufwerken:

- Laufwerke basierend auf einer Datei (Container-Datei)
- Laufwerke basierend auf einer existierenden Partition

Die DriveLock Container-Datei ist eine Datei mit der Dateiendung *.dlv. Sie kann auf allen Typen von Speichermedien oder auf einer Netzwerkfreigabe gespeichert werden. Zur Nutzung eines Containers verbindet DriveLock diesen mit einem vordefinierten oder freien Laufwerksbuchstaben, so dass dieser wie jedes andere Laufwerk innerhalb des Windows Explorer verwendet werden kann.

Die DriveLock Partition ist eine normale Partition, welche von DriveLock verschlüsselt wird. Es ist möglich, Diskettenlaufwerke, ZIP Laufwerke, USB- / FireWire-Festplatten und USB-Speichersticks sowie andere Massenspeichergeräte zu verschlüsseln.

Bei bestimmten Hardware Speichermedien ist das Erstellen einer verschlüsselten Partition nicht möglich. Bitte kontaktieren Sie hierzu den Hersteller des Speichermediums.

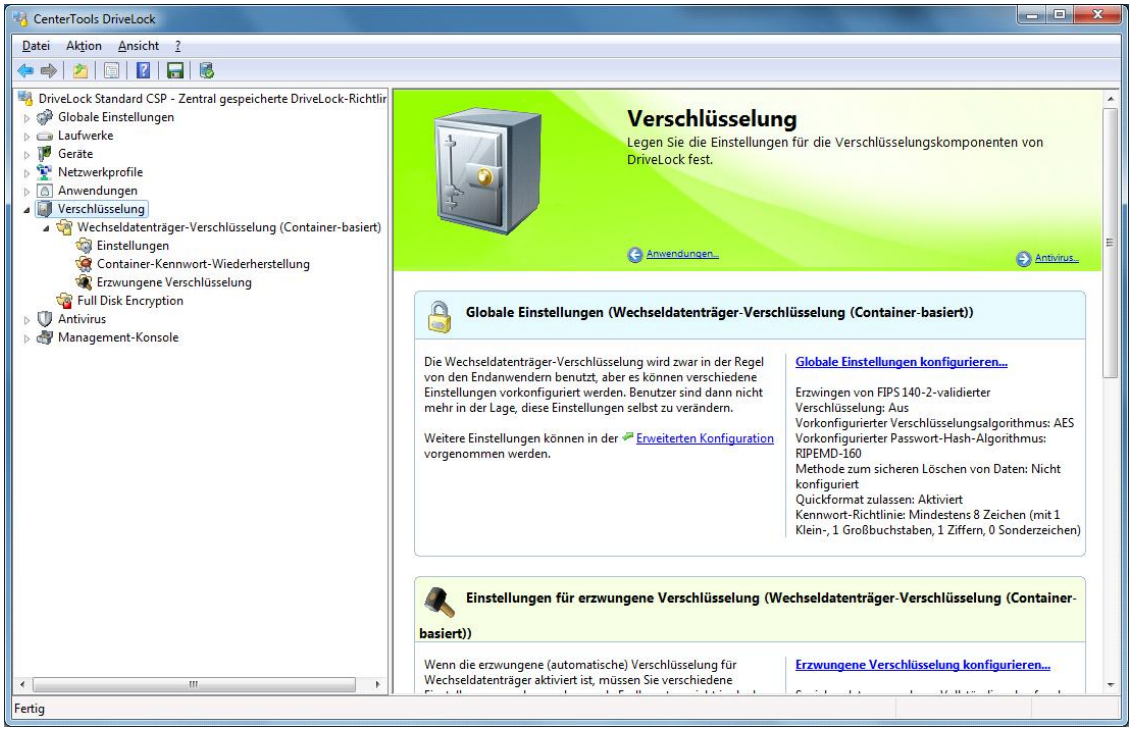
Das Laufwerk, welches die Windows Betriebssystem Dateien enthält (typischerweise C:\), kann nicht über diesen Weg verschlüsselt werden. Es muss die DriveLock Disk Protection verwendet werden, wenn es nötig ist, auch die System Partition zu verschlüsseln.

7.2 Konfiguration der DriveLock Verschlüsselung

Vor Nutzung der DriveLock Container-basierten Verschlüsselung muss ein Administrator verschiedene Einstellungen vornehmen.

7.2.1 Konfiguration in der Basiskonfiguration

Wenn die Basiskonfiguration aktiviert ist, können Sie darüber die grundlegenden Verschlüsselungseinstellungen konfigurieren. Klicken Sie dazu auf **Verschlüsselung** im linken Navigationsbaum.

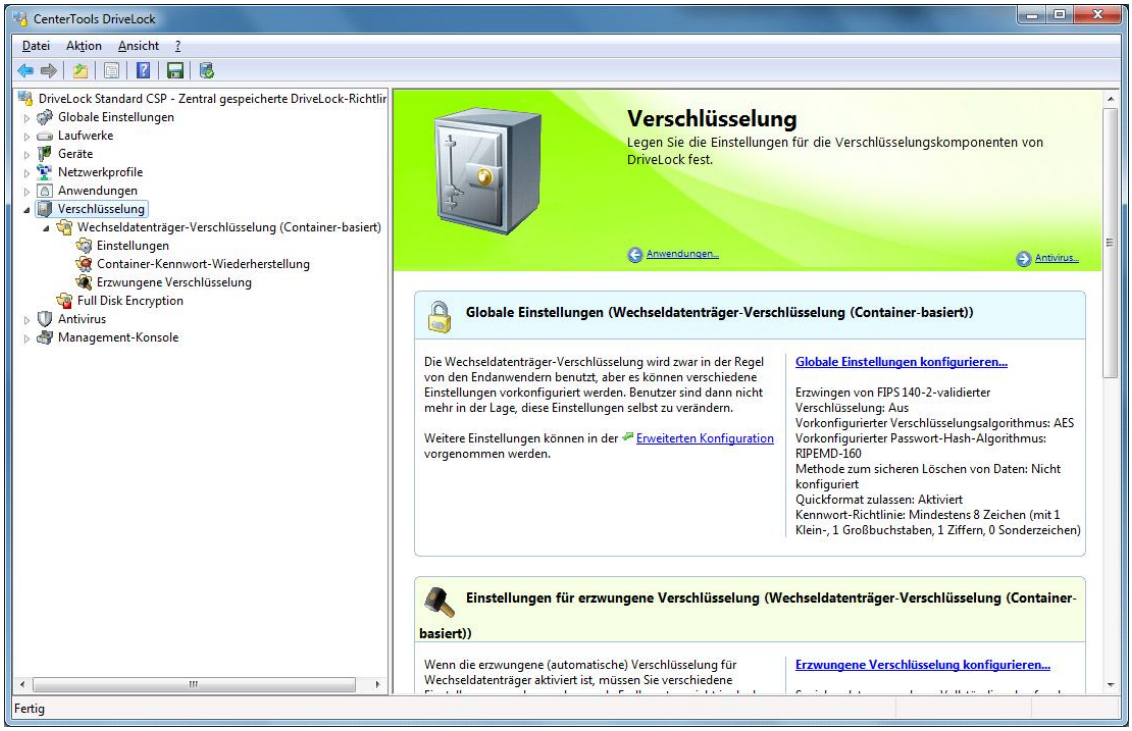


Sie können über die folgenden vier Sektionen entsprechende Einstellungen vornehmen:

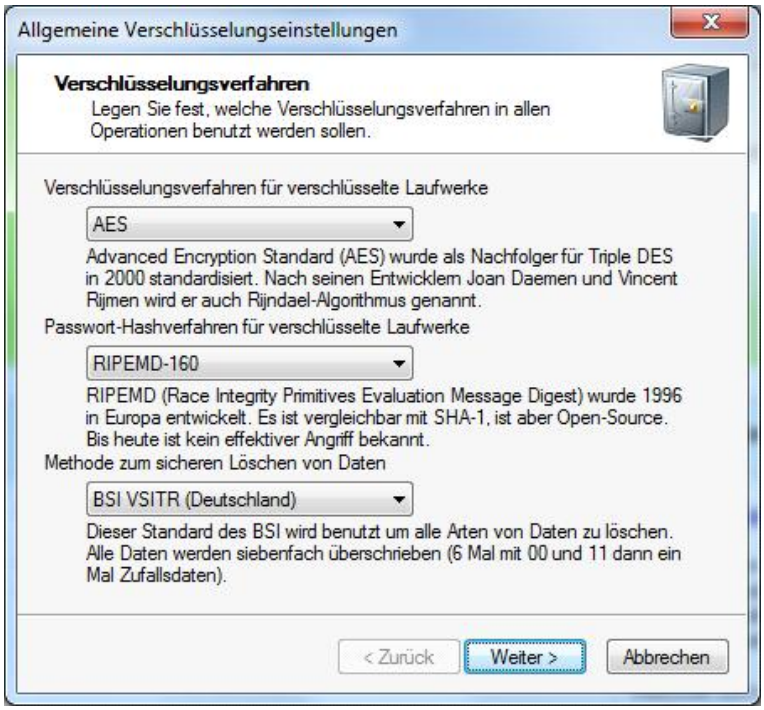
- Globale Einstellungen für die Verschlüsselung von Wechseldatenträgern
- Einstellungen für die erzwungene Verschlüsselung
- Konfiguration der Passwortwiederherstellung für verschlüsselte Medien
- Konfiguration der DriveLock Disk Protection (diese Einstellungen werden im Abschnitt „**DriveLock Disk Protection**“ des Administrationshandbuches beschrieben).

7.2.1.1 Globale Einstellungen

Globale Einstellungen legen fest, welche Optionen für Benutzer verfügbar sind, wenn sie selbst einen verschlüsselten Container anlegen, ein Laufwerk verschlüsseln oder eine verschlüsselte CD/DVD erstellen.

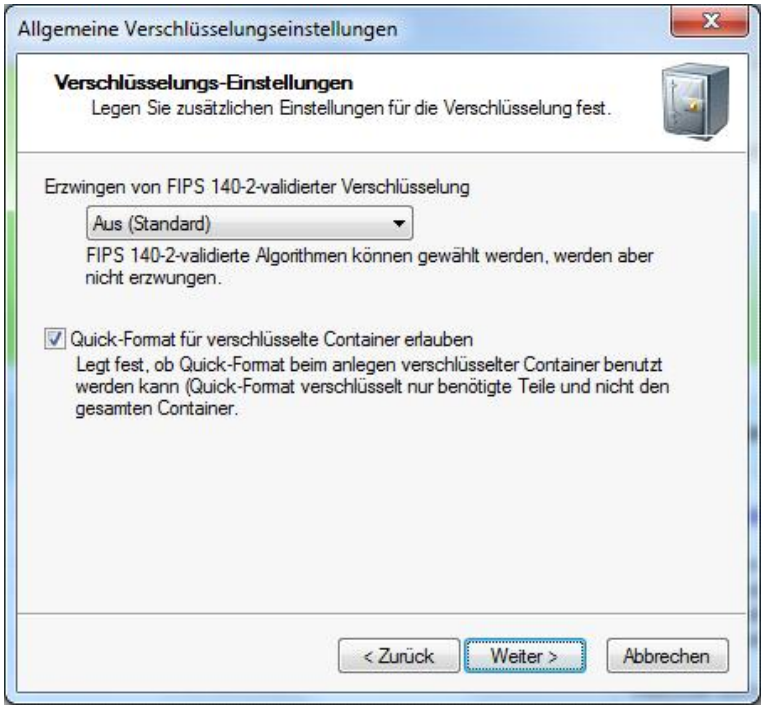


Klicken Sie auf **Globale Einstellungen konfigurieren**, um diese zu konfigurieren. Es startet der Assistent zur Konfiguration der globalen Einstellungen.



Wählen Sie hier die verschiedenen Verfahren für die Verschlüsselung, die Erzeugung von Hashwerten für Passwörter und die Methode für das sichere Löschen von Daten über die entsprechenden Listen aus.

Klicken Sie **Weiter**, um fortzufahren.



Wenn Ihr Unternehmen es erfordert, FIPS 140-2 zertifizierte Algorithmen zu verwenden, können Sie dies hier konfigurieren.

Standardmäßig ist der FIPS-Modus deaktiviert (**Aus**). Anwender können bei Bedarf FIPS 140-2 zertifizierte Verfahren auswählen, sind aber nicht dazu gezwungen. Es muss allerdings eine stimmige Konfiguration sein, d.h. wähle ich als Verschlüsselungsalgorithmus AES (FIPS-Modus) muss auch hier FIPS auf *Ein* oder *Ein (Nicht-FIPS-Verschlüsselung ausschalten)* ausgewählt sein.

Wenn Sie den FIPS-Modus aktivieren, wählen Sie eine der folgenden beiden Optionen:

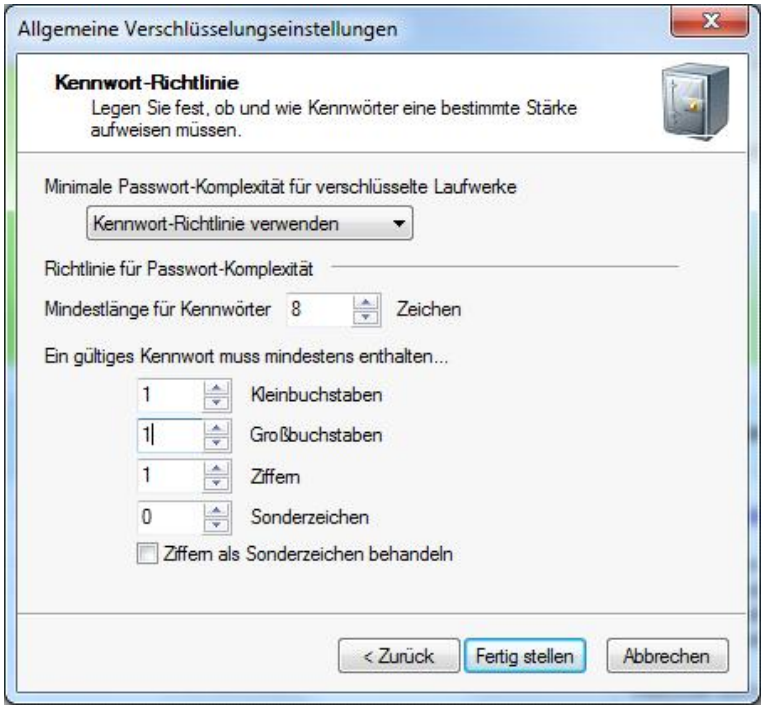
- *Ein*: Wählen Sie diese Einstellungen, um auch auf Container bzw. verschlüsselte Laufwerke zuzugreifen, die nicht mit FIPS 140-2 zertifizierten Verfahren verschlüsselte wurden. Wenn ein Benutzer einen neuen verschlüsselten Container erstellt, wird jedoch ein FIPS 140-2 zertifiziertes Verfahren verwendet.
- *Ein (Nicht-FIPS-Verschlüsselung ausschalten)*: Verwenden Sie diese Option, wenn Sie sicherstellen müssen, dass ausschließlich FIPS 140-2 zertifizierte Verfahren sowohl für die Ver- als auch für die Entschlüsselung angewendet werden können. Jeder mit Nicht- FIPS 140-2 zertifizierten Verfahren verschlüsselte Container bzw. Laufwerk kann jetzt nicht mehr entschlüsselt werden.

Um den Zeitraum zum Erstellen eines verschlüsselten Containers zu verkürzen, wählen Sie die Option "**Aktiviert**". Dadurch wird nicht der komplette verschlüsselter Container durch den DriveLock Agenten mit Null-Werten initialisiert, sondern es werden nur die wirklich benötigten Daten verschlüsselt. Dadurch kann es sein, dass zuvor unverschlüsselter Inhalt solange mit entsprechenden Verfahren wiederherstellbar ist, bis er durch verschlüsselten Inhalt überschrieben wird.

Quick-Format führt systembedingt nur auf Windows 7 (oder neuer) Betriebssystemen zu einer spürbaren Beschleunigung.

Klicken Sie **Weiter**, um fortzufahren.

Die minimal erforderliche Passwortkomplexität für verschlüsselte Laufwerke sollte so definiert werden, dass sie den Firmenrichtlinien entspricht. Die Komplexität wird auf Basis der verwendeten Zeichen sowie der Passwortlänge berechnet.



Wenn Sie Ihre eigene Passwortkomplexitäts-Richtlinie erstellen möchten, wählen Sie *„Kennwort-Richtlinie verwenden“* aus und konfigurieren anschließen diese. Weitere Informationen finden Sie im Abschnitt „Einstellungen zur Verschlüsselungsstärke“.

Eine Passwortkomplexitäts-Richtlinie enthält alle Anforderungen, die ein Benutzerpasswort erfüllen muss, wenn es erstellt wird. Diese enthält die Mindestanzahl an Zeichen und die Anzahl der Sonderzeichen, die ein Passwort enthalten muss.

Sofern Ihre Richtlinien es erfordern, dass Zeichen verwendet werden sollen, die sowohl eine Zahl also auch ein Sonderzeichen sein dürfen, aktivieren Sie die Option „**Ziffern als Sonderzeichen behandeln**“ und geben Sie die Anzahl der benötigten Zeichen an.

Klicken Sie **Fertig stellen**, um die Einstellungen zu sichern.

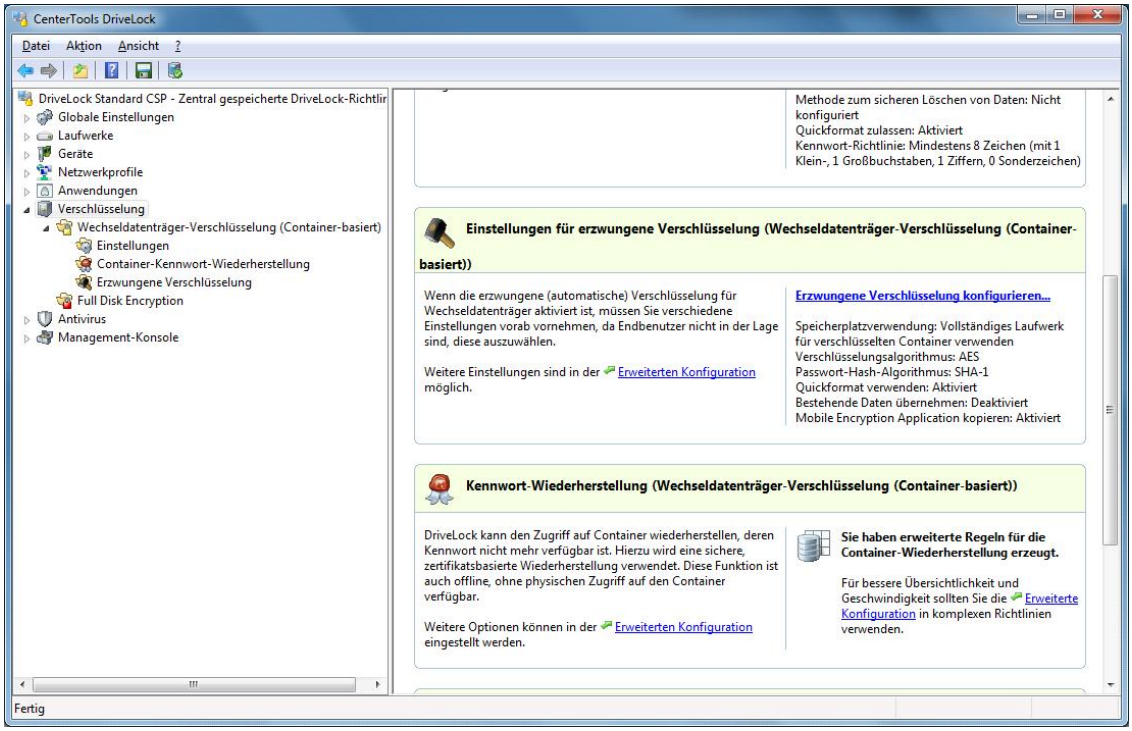
Um erweiterte Einstellungen vorzunehmen, klicken Sie auf den Link **Erweiterten Konfiguration**.

7.2.1.2 Erzwungene Verschlüsselung

Aktivieren sie die erzwungene Verschlüsselung mit *DriveLock Encryption 2-Go* in der Richtlinie unter:
Verschlüsselung/ Einstellungen / Methode für die erzwungene Verschlüsselung
Selektieren Sie **DriveLock Encryption 2-Go**.

Sie können für die erzwungenen Verschlüsselung auch *DriveLock File Protection* verwenden (siehe Erzwungene Verschlüsselung mit File Protection).

Die Einstellungen für die erzwungene Verschlüsselung legen fest, wie Wechseldatenträger automatisch verschlüsselt werden.



Klicken Sie auf **Erzwungene Verschlüsselung** konfigurieren, um die grundlegenden Einstellungen vorzunehmen.

Wählen Sie das zu verwendende Verschlüsselungsverfahren aus und konfigurieren Sie einen Hash-Algorithmus.

Um den Zeitraum zum Erstellen eines verschlüsselten Containers zu verkürzen, wählen Sie die Option "**Aktiviert**". Dadurch wird nicht der komplette verschlüsselter Container durch den DriveLock Agenten mit Null-Werten initialisiert, sondern es werden nur die wirklich benötigten Daten verschlüsselt. Dadurch kann es sein, dass zuvor unverschlüsselter Inhalt solange mit entsprechenden Verfahren wiederherstellbar ist, bis er durch verschlüsselten Inhalt überschrieben wird.

Quick-Format führt systembedingt nur auf Windows 7 (oder neuer) Betriebssystemen zu einer spürbaren Beschleunigung.

Die folgenden weiteren Einstellungen sind verfügbar:

- *Bestehende Daten erhalten:* Wählen Sie diese Option, wenn DriveLock alle unverschlüsselten Dateien erhalten und mit verschlüsseln soll. Dazu wird ein temporäres Verzeichnis (Standardmäßig im Benutzerprofil von Windows) erstellt, der verschlüsselte Container dort erzeugt, die vorhandenen Daten vom Laufwerk dort hinein kopiert und zum Schluss der Container komplett auf den Wechseldatenträger verschoben.
- *Mobile Encryption Anwendung auf unverschl. Teil kopieren:* Sie haben außerdem die Möglichkeit, festzulegen, ob die Mobile Encryption Anwendung auf Wechseldatenträger während der automatischen Verschlüsselung kopiert werden soll. Dies ermöglicht die Nutzung auch auf Rechnern, auf denen DriveLock nicht installiert ist.

Wählen Sie eine der folgenden Optionen für die Speicherplatz-Verwendung:

- *Vollständiges Laufwerk für verschlüsselten Container verwenden:* Aus technischer Sicht muss DriveLock die voraussichtliche maximale Größe des verschlüsselten Containers berechnen, wenn die Daten erhalten bleiben sollen. Das kann dazu führen, dass etwas Speicherplatz nicht von dem verschlüsselten Laufwerk verwendet wird. Wenn Sie erreichen möchten, dass der Container den kompletten verfügbaren Speicherplatz verwenden kann, aktivieren Sie diese Funktionalität. In Verbindung mit dieser Option wird DriveLock den kompletten restlichen verfügbaren Speicherplatz (sofern verfügbar) auffüllen. Dazu erstellt DriveLock eine versteckte Systemdatei in entsprechender Größe.
- *Unverschlüsselten Bereich auf Laufwerk freilassen:* Wählen Sie diese Option, wenn Sie nicht den vollständigen Platz auf einem Laufwerk für die Verschlüsselung verwenden möchten. Geben Sie eine Größe an und legen Sie fest, ob die Zahl als absoluter Wert oder als Prozentwert verstanden werden soll.

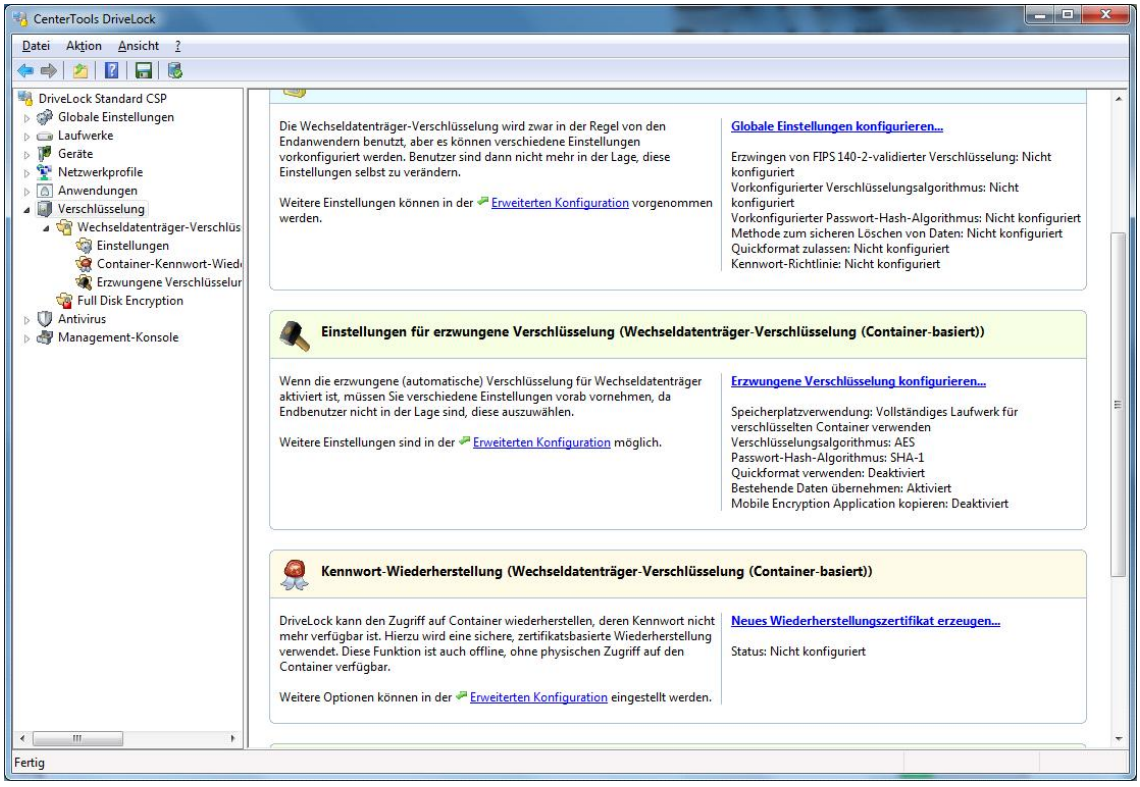
Klicken Sie **Fertig stellen**, um die Einstellungen zu übernehmen.

Um erweiterte Einstellungen vorzunehmen, klicken Sie auf den Link **Erweiterten Konfiguration**.

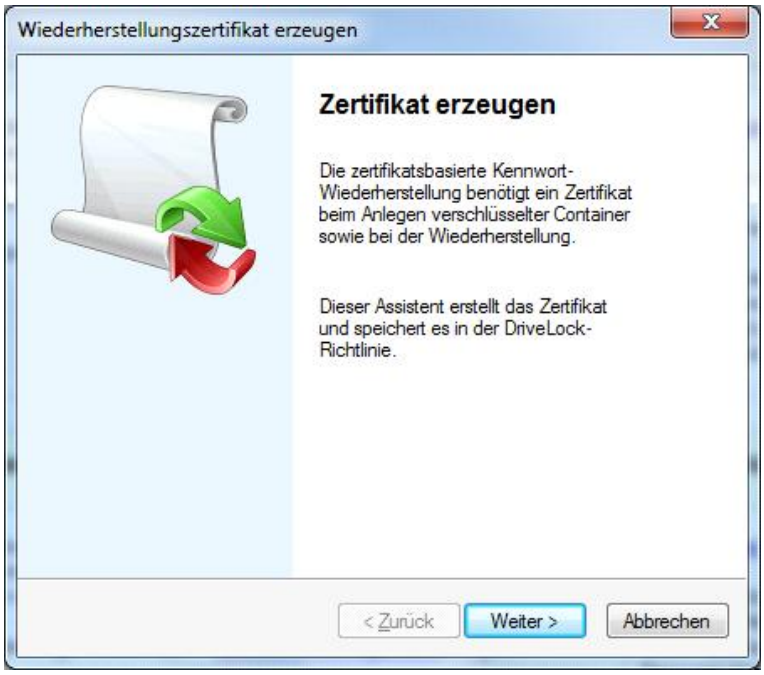
7.2.1.3 Passwort Recovery

Dieser Abschnitt beschreibt die beiden notwendigen Konfigurationsschritte, um später bei Bedarf das Passwort bei einem verschlüsselten Container (zum Beispiel bei einem zwangsverschlüsselten USB-Stick) zurücksetzen zu können.

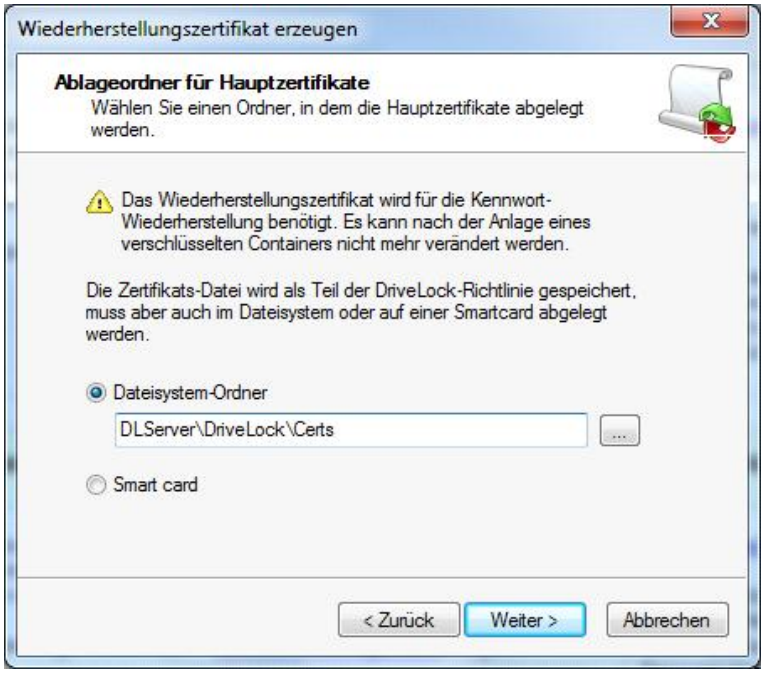
Damit Sie die Funktionalität der Offline-Passwort-Wiederherstellung nutzen zu können, müssen Sie vor der Erstellung des ersten verschlüsselten Containers ein Hauptzertifikat bestehend aus einem öffentlichen und privaten Schlüsselpaares erzeugen.



Klicken Sie dazu auf **Neues Wiederherstellungszertifikat erzeugen**. Dadurch wird der Assistent für die Erzeugung des Hauptzertifikates gestartet.



Klicken Sie **Weiter**.

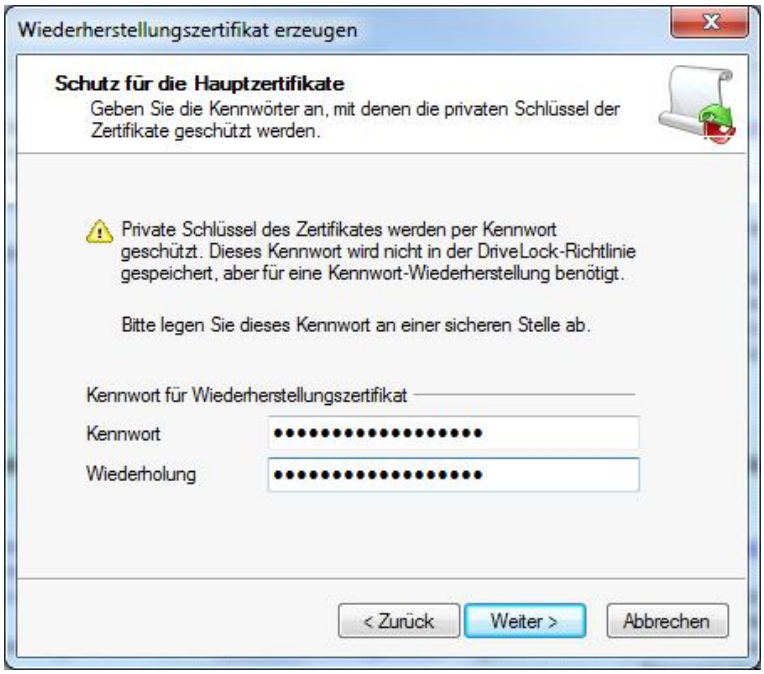


Geben Sie entweder den Ordner an, wo Sie die Zertifikats-Datei abspeichern möchten oder wählen Sie alternativ eine Smartcard als Speicherort.

Klicken auf **Weiter**.

Sofern Sie eine Smartcard zur Speicherung verwenden, werden Sie abhängig von der verwendeten Karte nun gebeten, die Karte einzulegen und auszuwählen.

Stellen Sie sicher, dass diese Datei an einem sicheren Ort abgespeichert wird, da sie für die Passwort-Wiederherstellung dringend benötigt wird.



Geben Sie nun das Passwort für den Zugriff auf den privaten Schlüsselbereich des Zertifikates an.

Sie müssen das Passwort aus Sicherheitsgründen zweifach eingeben. Um Fortzufahren, klicken Sie auf **Weiter**.

Stellen Sie sicher, dieses Passwort nicht zu vergessen. Sie sollten dieses ebenso an einem anderen sicheren Ort aufbewahren (z.B. in einem Tresor).

Es dauert einige Sekunden, um das Hauptzertifikat zu erzeugen. Anschließend werden Sie benachrichtigt, wenn der Prozess abgeschlossen ist und die Datei an dem zuvor angegebenen Ort abgespeichert wurde.

Sofern eine Smartcard zur Speicherung verwendet wird, werden Sie aufgefordert, die PIN für den Zugriff auf die Smartcard einzugeben.

Klicken Sie auf **Fertig stellen**.

Nachdem das Zertifikat erzeugt wurde, wechselt der Status in der DriveLock Management Konsole auf „*Konfiguriert*“.

Sobald das Zertifikat erzeugt und der erste verschlüsselte Container erstellt wurde, darf kein neues Zertifikat mehr erstellt werden, da das alte damit überschrieben wird und somit für eine Wiederherstellung nicht mehr verwendet werden kann.

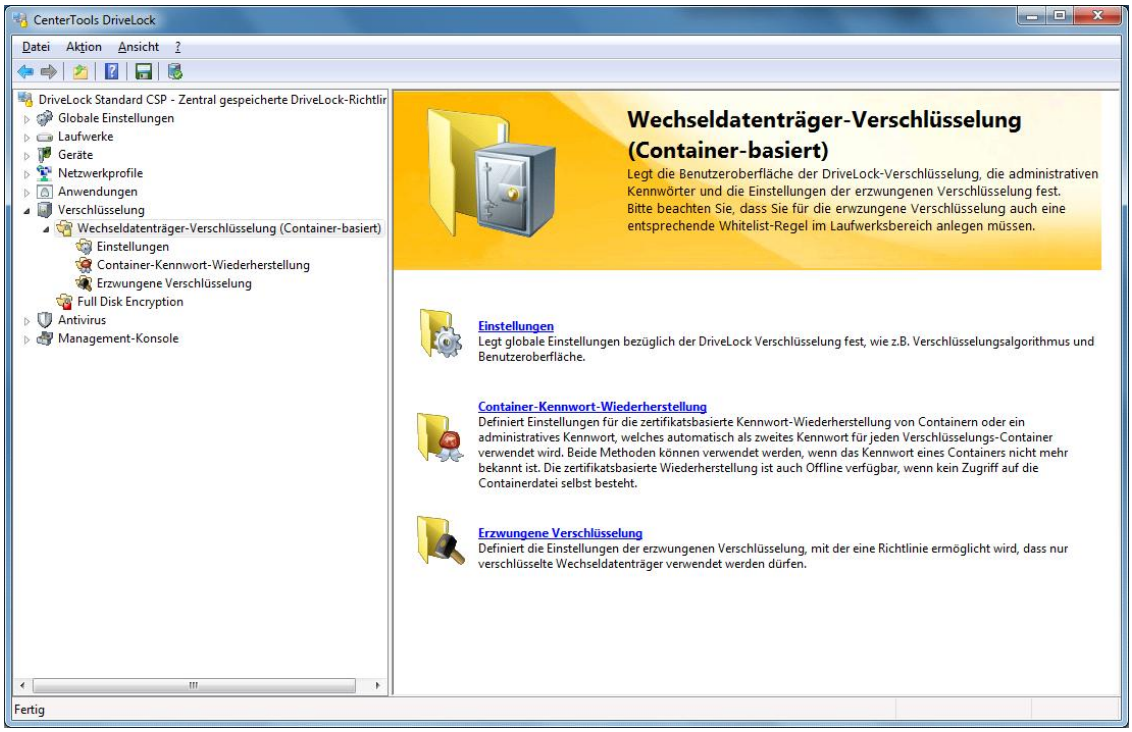
Wenn Sie auf **Wiederherstellungszertifikat anzeigen** klicken, erhalten Sie zusätzliche Informationen über das Hauptzertifikat.

Das Zertifikat wird ebenfalls in dem privaten Zertifikatsspeichers des aktuellen Benutzers gespeichert.

Um erweiterte Einstellungen vorzunehmen, klicken Sie auf den Link **Erweiterten Konfiguration**.

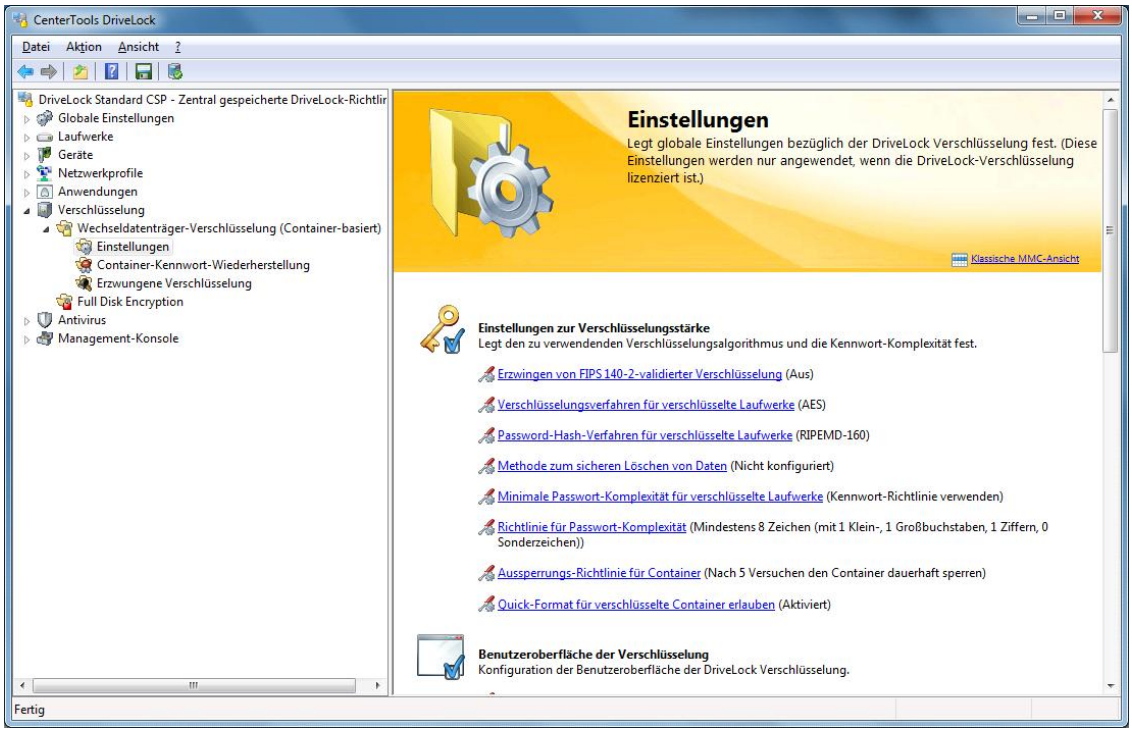
7.2.2 Konfiguration der erweiterten Einstellungen

Klicken Sie auf **Verschlüsselung** und **Wechseldatenträger-Verschlüsselung (Container-basiert)** um zum Konfigurationsfenster zu gelangen.



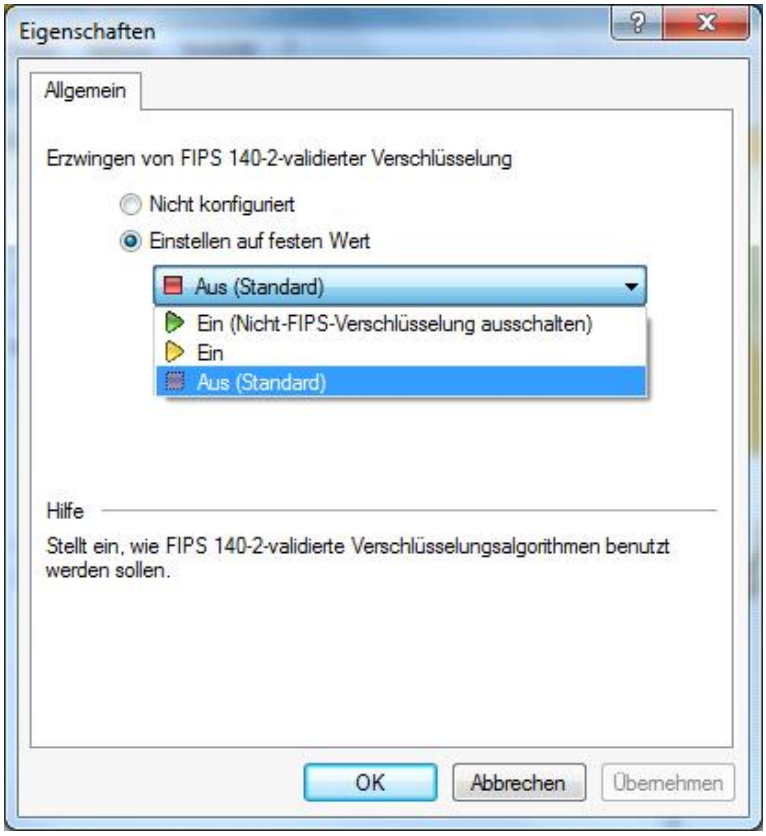
7.2.2.1 Konfiguration globaler Parameter

Klicken Sie auf **Einstellungen** zur Konfiguration globaler Parameter für die Verschlüsselungsfunktionen.



7.2.2.1.1 Einstellungen zur Verschlüsselungsstärke

Erzwingen von FIPS 140-2 zertifizierter Verschlüsselung



Wenn Ihr Unternehmen es erfordert, FIPS 140-2 zertifizierte Algorithmen zu verwenden, können Sie dies hier konfigurieren.

Standardmäßig ist der FIPS-Modus deaktiviert (**Aus**). Anwender können bei Bedarf FIPS 140-2 zertifizierte Verfahren auswählen, sind aber nicht dazu gezwungen.

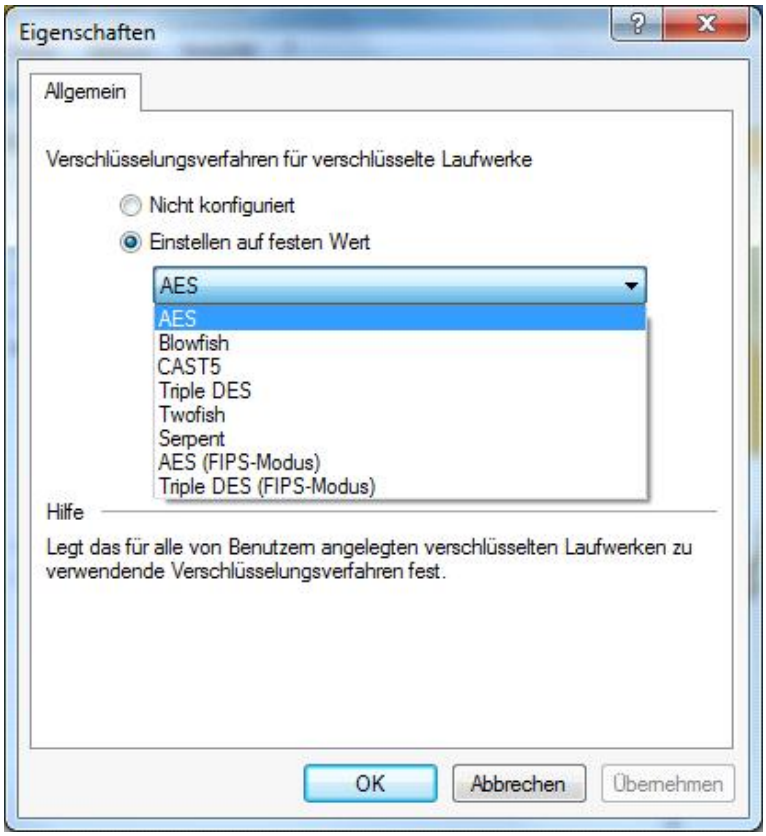
Wenn Sie den FIPS-Modus aktivieren, wählen Sie eine der folgenden beiden Optionen:

- *Ein*: Wählen Sie diese Einstellungen, um auch auf Container bzw. verschlüsselte Laufwerke zuzugreifen, die nicht mit FIPS 140-2 zertifizierten Verfahren verschlüsselte wurden. Wenn ein Benutzer einen neuen verschlüsselten Container erstellt, wird jedoch ein FIPS 140-2 zertifiziertes Verfahren verwendet.
- *Ein (Nicht-FIPS-Verschlüsselung ausschalten)*: Verwenden Sie diese Option, wenn Sie sicherstellen müssen, dass ausschließlich FIPS 140-2 zertifizierte Verfahren sowohl für die Ver- als auch für die Entschlüsselung angewendet werden können. Jeder mit Nicht- FIPS 140-2 zertifizierten Verfahren verschlüsselte Container bzw. Laufwerk kann jetzt nicht mehr entschlüsselt werden.

Klicken Sie auf **OK**, um die Einstellung zu speichern.

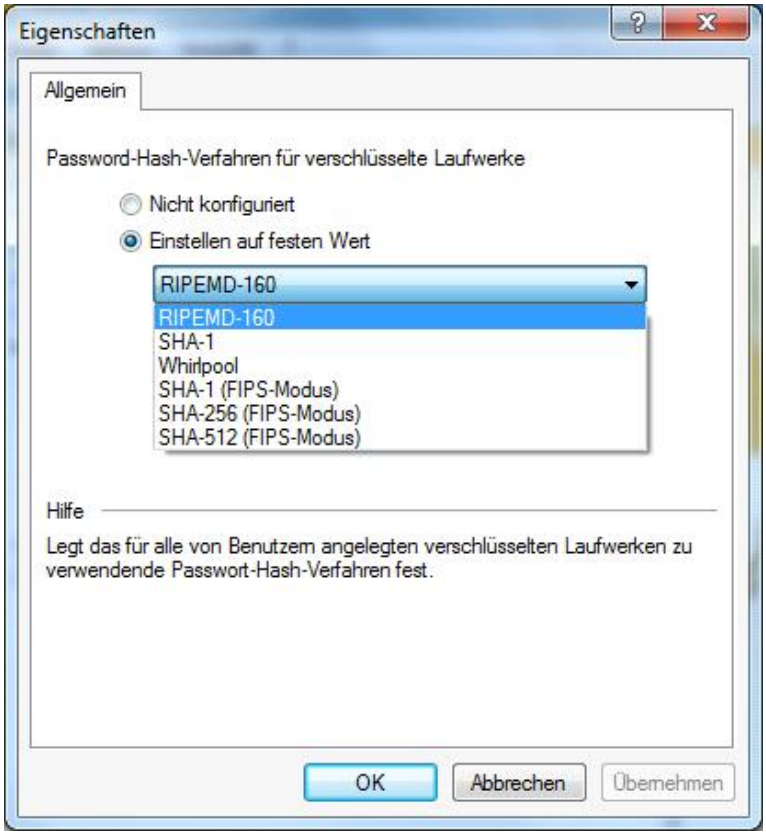
Verschlüsselungsverfahren

Konfigurieren Sie den zu verwendenden Verschlüsselungsalgorithmus. Diese sind im Kapitel "DriveLock Verschlüsselungsverfahren" beschrieben.



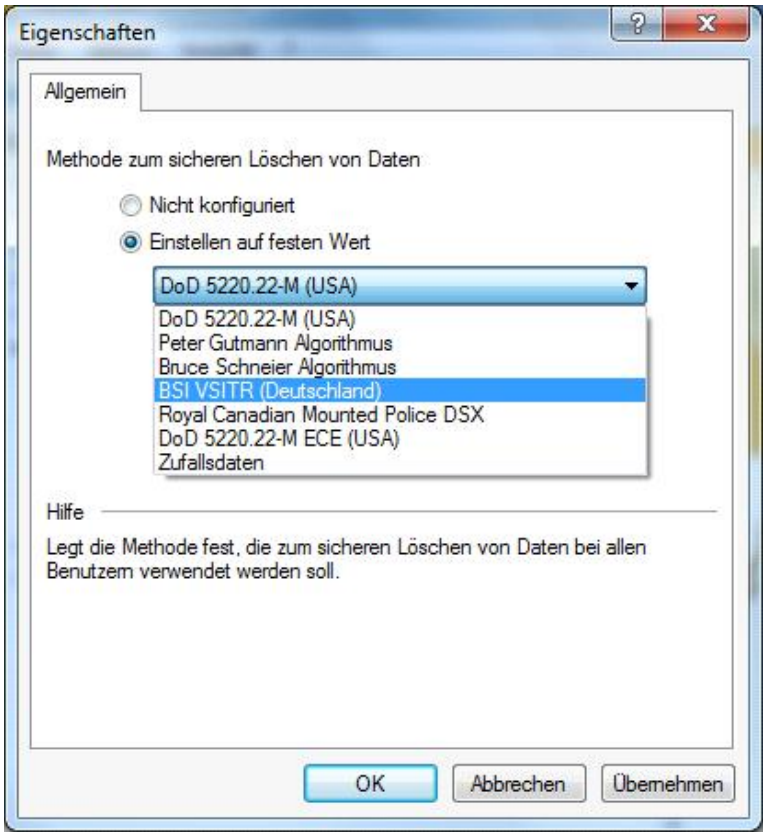
Passwort-Hash-Verfahren

Definieren Sie den zum Einsatz kommenden Hash Algorithmus. Alle Hash Algorithmen sind im Abschnitt „DriveLock Verschlüsselungsverfahren“ beschrieben.



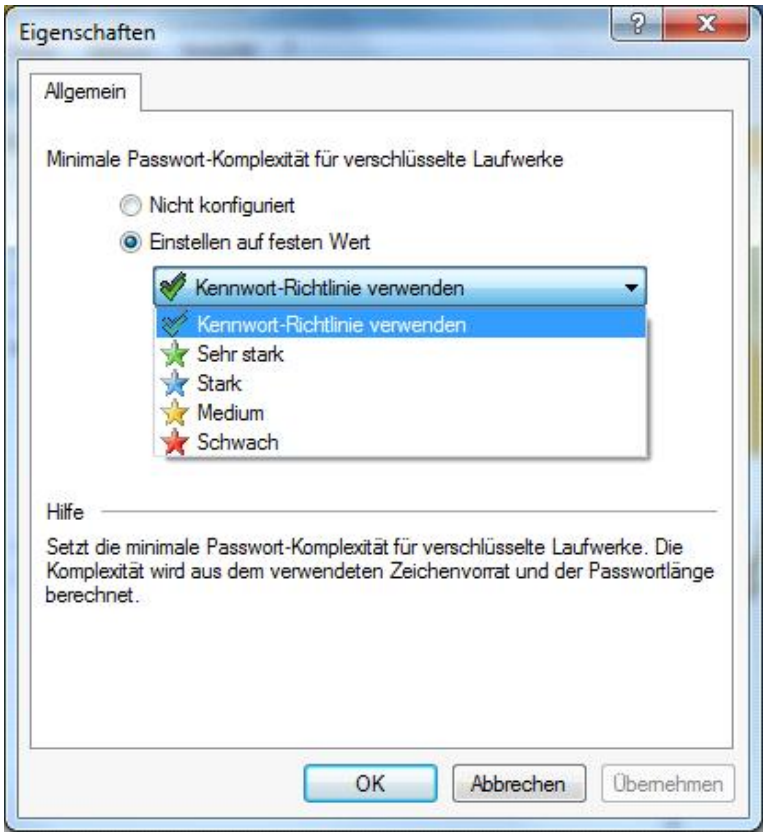
Methode zum sicheren Löschen von Dateien

Sie können festlegen, wie Daten auf sichere Weise gelöscht werden.



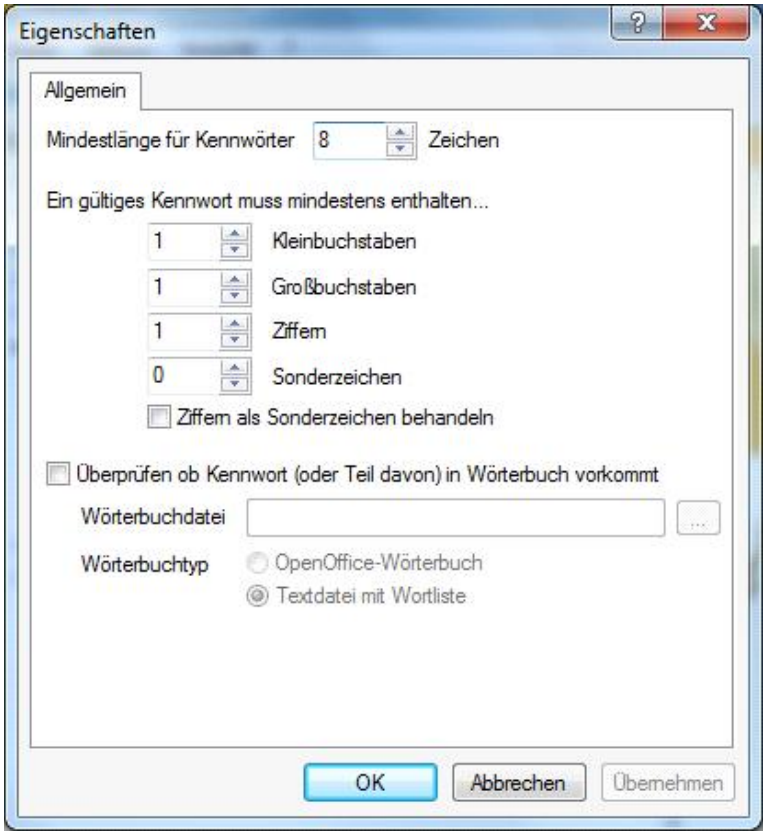
Minimale Passwortkomplexität für verschlüsselte Laufwerke

Die minimal erforderliche Passwortkomplexität für verschlüsselte Laufwerke sollte so definiert werden, dass sie den Firmenrichtlinien entspricht. Die Komplexität wird auf Basis der verwendeten Zeichen sowie der Passwortlänge berechnet. Wenn Sie Ihre eigene Passwortkomplexitäts-Richtlinie erstellen möchten, wählen Sie *„Richtlinie für Passwort-Komplexität“* aus und konfigurieren anschließen diese. Weitere Informationen finden Sie im folgenden Abschnitt.



Richtlinie für Passwort-Komplexität

Eine Passwortkomplexitäts-Richtlinie enthält alle Anforderungen, die ein Benutzerpasswort erfüllen muss, wenn es erstellt wird. Diese enthält die Mindestanzahl an Zeichen und die Anzahl der Sonderzeichen, die ein Passwort enthalten muss. DriveLock kann ein Benutzerpasswort auch verweigern, wenn es in einem Wörterbuch vorkommt (Passwort Wörterbuch Überprüfung).



Sofern Ihre Richtlinien es erfordern, dass Zeichen verwendet werden sollen, die sowohl eine Zahl also auch ein Sonderzeichen sein dürfen, aktivieren Sie die Option „**Ziffern als Sonderzeichen behandeln**“ und geben Sie die Anzahl der benötigten Zeichen an.

Ein Wörterbuch kann entweder ein Wörterbuch-Datei aus OpenOffice sein oder eine normale Textdatei, die pro Zeile ein Wort enthält. DriveLock wird mit OpenOffice Wörterbüchern für die vier folgenden Sprachen ausgeliefert: Englisch, Deutsch, Niederländisch und Französisch. Sie können die DIZ-Dateien in dem DriveLock Installationsordner finden, auf dem Client, auf dem die DriveLock Management Konsole installiert wurde (z.B. *„DictGerman.diz“)*.

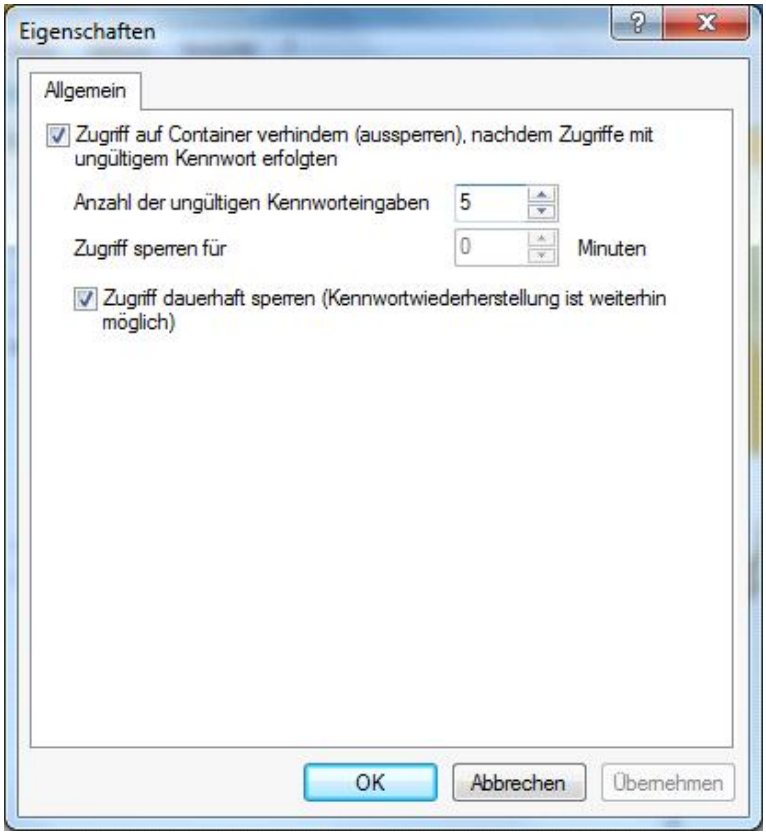
Wenn Sie die Datei aus dem Dateisystem auswählen, stellen Sie sicher, dass sich die Datei auf allen Agenten Computern an exakt der gleichen Stelle befindet, da der Agent an dem angegebenen Ort sucht.

Sie können die Datei auch dem Richtliniendateispeicher hinzufügen und wählen dazu *„Richtliniendateispeicher…“* aus und wählen die Dateien aus dem Ort aus. Dateien im Richtliniendateispeicher werden Anhand eines Sterns („*“) am Anfang des Dateinamens identifiziert und werden automatisch auf den Client kopiert. Weitere Informationen zu dem Richtliniendateispeicher finden Sie im Kapitel "Richtliniendateispeicher verwenden".

Wenn Sie das Wörterbuch verwenden um Passwörter zu überprüfen, beachten Sie dass auch Passwörter verweigert werden, indem ein Teil des Passwortes im Wörterbuch vorkommt (z.B.: das Wörterbuch enthält „es“, Passwörter wie „Essen“, „vergessen“ oder „Sessel“ werden nicht erlaubt).

Aussperrungs-Richtlinie für Container

Die Aussperrungs-Richtlinie hilft Brute-Force Angriffe zu unterbinden, indem ein Container nach einer definierten Anzahl von Versuchen ein Passwort einzugeben für eine angegebene Anzahl von Minuten oder für immer gesperrt wird.

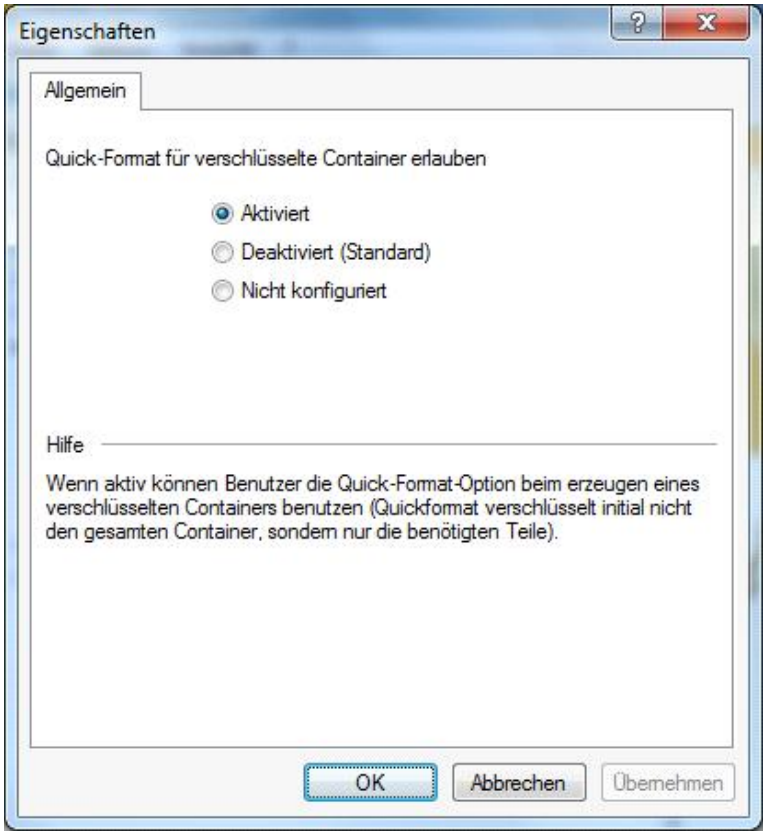


Sie haben folgende Optionen:

- Zugriff auf Container verhindern (aussperren), nachdem Zugriffe mit ungültigem Kennwort erfolgten
    - Anzahl der ungültigen Kennworteingaben
    - Zugriff sperren für x Minuten
- Zugriff dauerhaft sperren (Kennwortwiederherstellung ist weiterhin möglich): In diesem Fall kann ein Container nach x fehlgeschlagenen Anmeldeversuchen nur durch eine Kennwortwiederherstellung zurückgesetzt werden.

Die Aussperrungs-Richtlinie setzt Container-Dateien (.DLV) voraus, die in der Version 7.0 erstellt wurden, oder von einem 7.0 Agenten aktualisiert wurden. DriveLock aktualisiert automatisch eine Container-Datei, wenn diese erfolgreich geladen wird. Außerdem wird eine aktuelle DLMobile.exe (DriveLock Mobile Encryption Anwendung benötigt) – *Erweiterte Konfiguration – Verschlüsselung – Wechseldatenträger-Verschlüsselung… - Einstellungen – Mobile Encryption Anwendung nicht automatisch auf neuere Version aktualisieren…* - auf - Deaktiviert setzen (Standard). Anschließend wird die DLMobile.exe auch aktualisiert.

Quick-Format für verschlüsselte Laufwerke



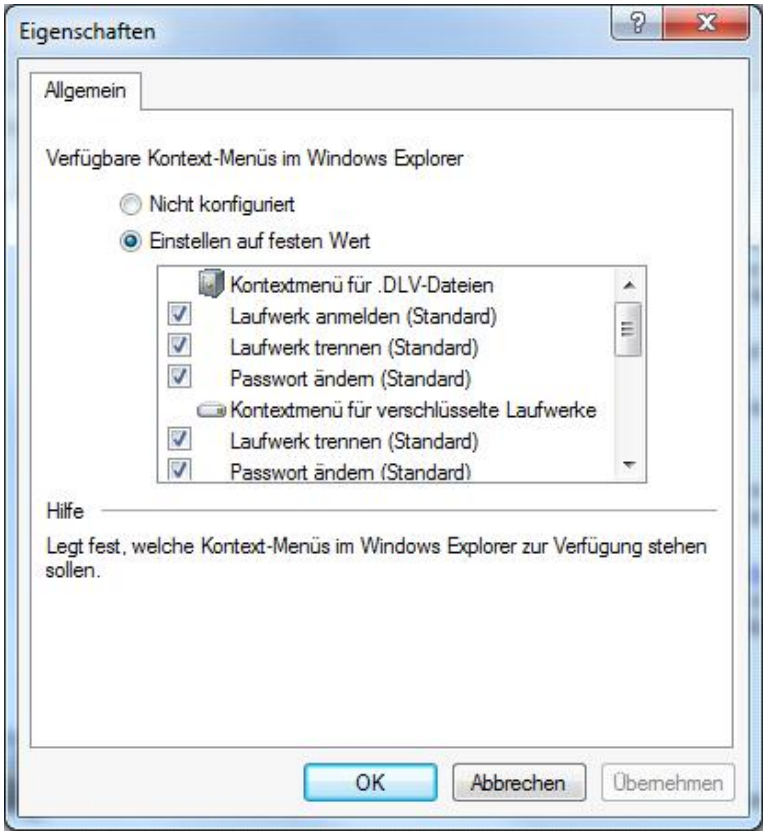
Um den Zeitraum zum Erstellen eines verschlüsselten Containers zu verkürzen, wählen Sie die Option “Aktiviert”. Dadurch wird nicht der komplette verschlüsselter Container durch den DriveLock Agenten mit Null-Werten initialisiert, sondern es werden nur die wirklich benötigten Daten verschlüsselt. Dadurch kann es sein, dass zuvor unverschlüsselter Inhalt solange mit entsprechenden Verfahren wiederherstellbar ist, bis er durch verschlüsselten Inhalt überschrieben wird.

Quick-Format führt nur auf Windows 7 (oder neuer) Betriebssystemen zu einer spürbaren Beschleunigung.

7.2.2.1.2 Verschlüsselung aus Benutzersicht

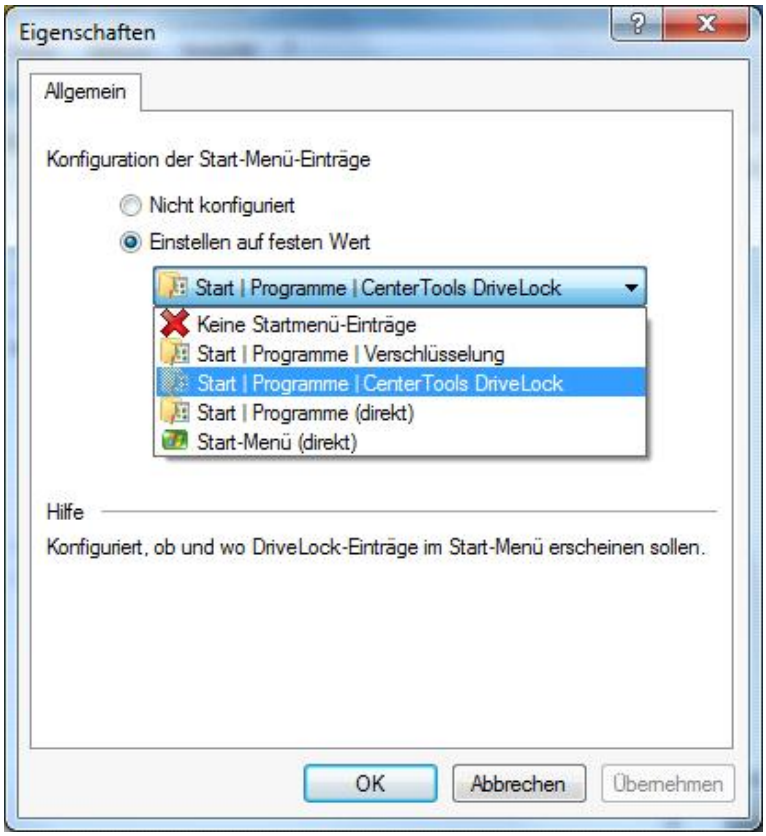
Verfügbare Kontextmenüs im Windows Explorer

Diese Einstellungen legen alle über das Kontextmenü verfügbaren Optionen fest. Die Einstellung „*Nicht konfiguriert*“ aktiviert alle Optionen.



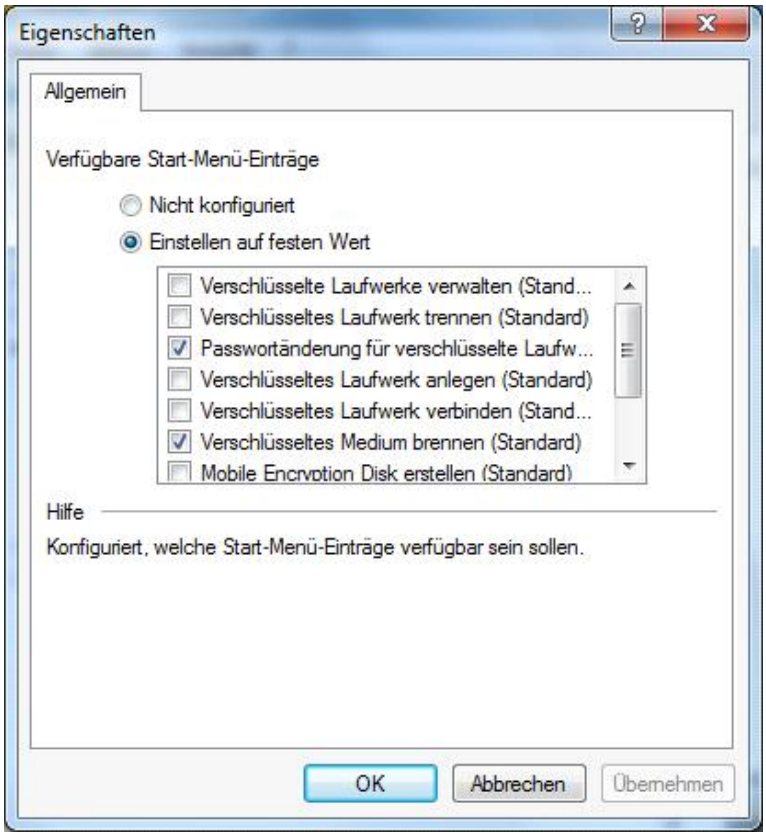
Konfiguration des Startmenüs

Sie können definieren, ob die DriveLock Startmenüeinträge angezeigt und wie diese angeordnet werden sollen. *„Nicht konfiguriert*“ erstellt den Standardeintrag *„Start – Programme – DriveLock*”.



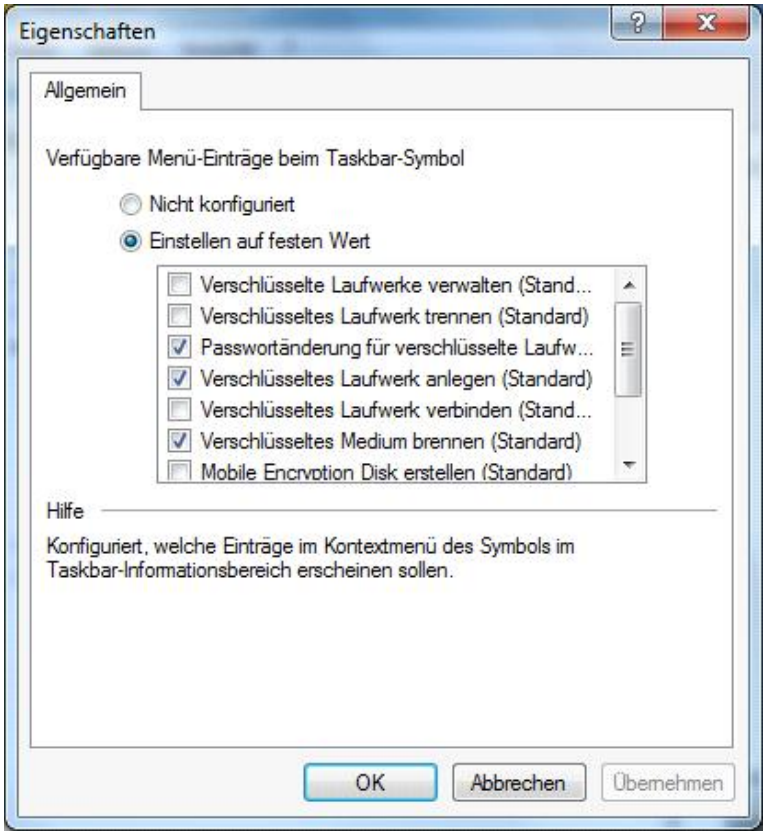
Verfügbare Einträge im Startmenü

Diese Option definiert die Startmenüeinträge, die angezeigt werden sollen („*Nicht konfiguriert*“ aktiviert alle Einträge).



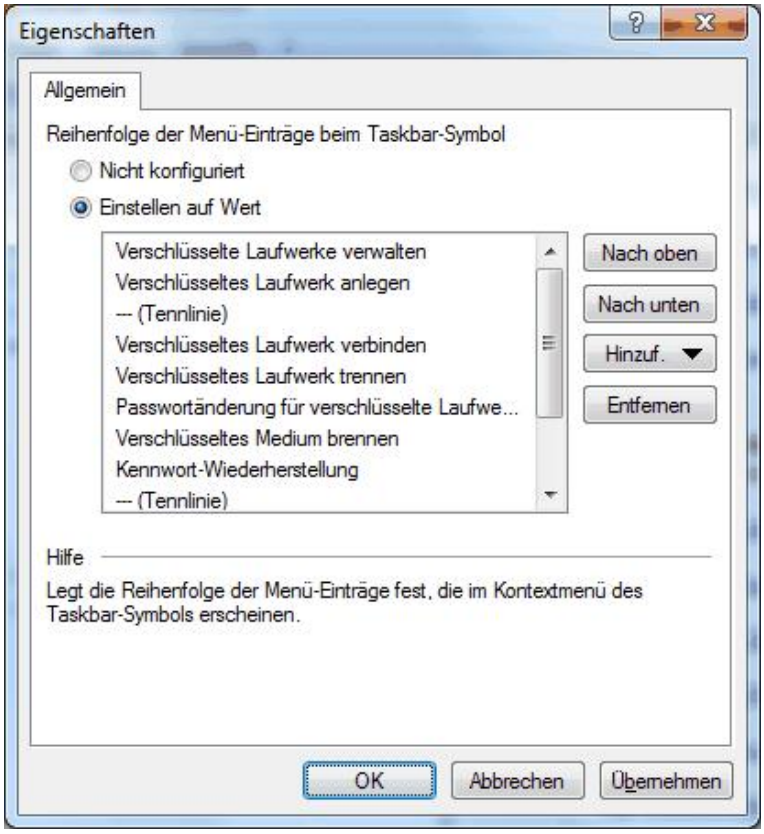
Verfügbare Menü-Einträge beim Taskbar-Symbol

Sie können definieren, ob alle Menüpunkte bei Nutzung des Taskleisten-Symbols angezeigt werden sollen („*Nicht konfiguriert*“ aktiviert alle Einträge).



Reihenfolge der Menü-Einträge beim Taskbar-Symbol

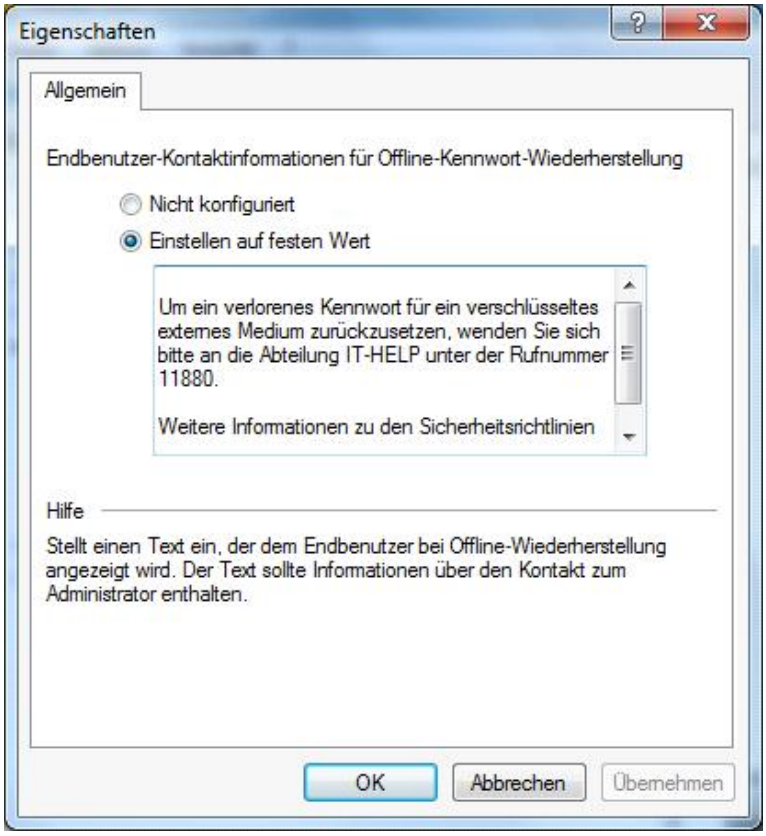
Sie können definieren, in welcher Reihenfolge die Menüpunkte bei Nutzung des Taskleisten-Symbols angezeigt werden sollen („*Nicht konfiguriert*“ aktiviert die Standard-Reihenfolge).



Um die Reihenfolge der Elemente zu ändern, markieren Sie das gewünschte Element und klicken Sie auf **Nach oben** oder **Nach unten**. Klicken Sie **Entfernen**, um das markierte Element zu löschen. Um Elemente wie zum Beispiel eine Trennlinie hinzuzufügen, klicken Sie auf **Hinzufügen**.

Endbenutzer-Kontaktinformationen für Offline-Kennwort-Wiederherstellung

Wenn ein Benutzer sein persönliches Kennwort für den Zugriff auf den Container bzw. das verschlüsselte Laufwerk vergessen hat, kann er über das Symbol in der Taskleiste oder das Startmenü den Assistenten zur Passwort-Wiederherstellung aufrufen. Dort wird ihm am Anfang ein Text angezeigt, der über diesen Menüpunkt frei vorgegeben werden kann.

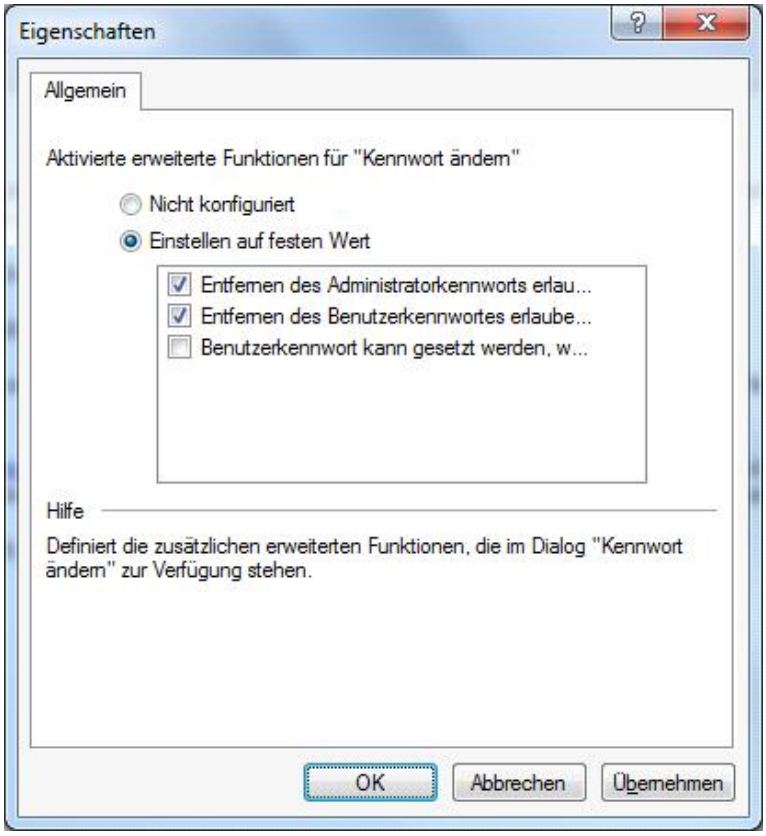


Aktivieren Sie „**Einstellen auf festen Wert**“ und geben den gewünschten Text in das Dialogfenster ein.

Aktivierte erweiterte Funktionen für „*Kennwort ändern*“

Wenn ein Benutzer sein persönliches Kennwort für den Zugriff auf den Container bzw. das verschlüsselte Laufwerk vergessen hat, kann er über das Symbol in der Taskleiste oder das Startmenü den Assistenten

- Entfernen des Administratorkennworts erlauben: Wenn ein Benutzerkennwort vorhanden ist, kann man über diese Funktion das Administratorkennwort entfernen. Es bleibt ein Container, den man nur noch mit dem persönlichen Kennwort öffnen kann.
- Entfernen des Benutzerkennwortes erlauben: Wenn ein Administratorpasswort vorhanden ist, kann man über diese Funktion sein persönliches Kennwort entfernen. Es bleibt ein Container, den man nur noch mit dem Administratorpasswort öffnen kann. Hierzu muss man sein Benutzerpasswort eingeben.
- Benutzerkennwort kann gesetzt werden, wenn ein Administratorkennwort definiert ist: Wenn es ein Administratorpasswort gibt, kann man ein zusätzliches persönliches Passwort setzen ohne dass man ein altes Passwort kennen muss.



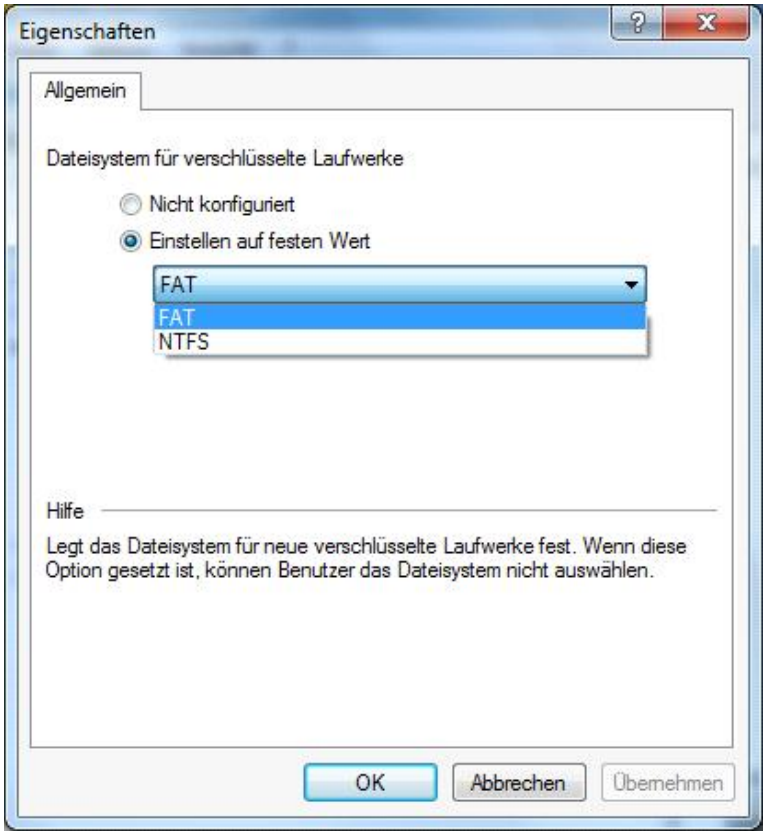
Aktivieren Sie „**Einstellen auf festen Wert**“ und wählen Sie die gewünschten Optionen aus, die einem Benutzer zur Verfügung stehen.

7.2.2.1.3 Einstellungen für verschlüsselte Laufwerke

Dateisystem für verschlüsselte Laufwerke

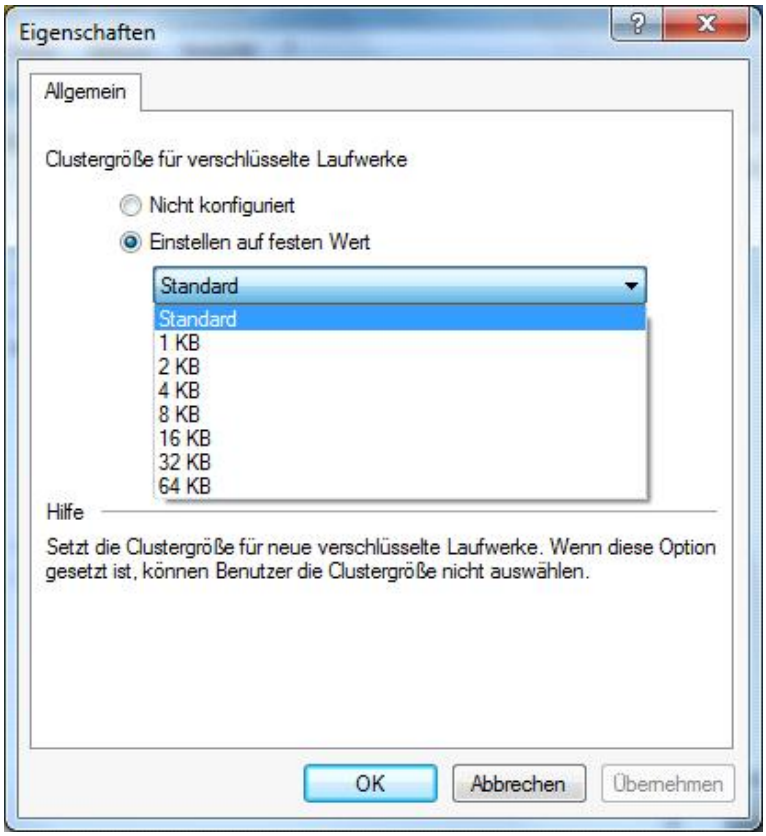
Das Dateisystem für neue verschlüsselte Laufwerke kann FAT oder NTFS sein.

Bei der Wahl von FAT wird automatisch FAT32 festgelegt, wenn die Laufwerksgröße 40 MB übersteigt (ansonsten FAT).



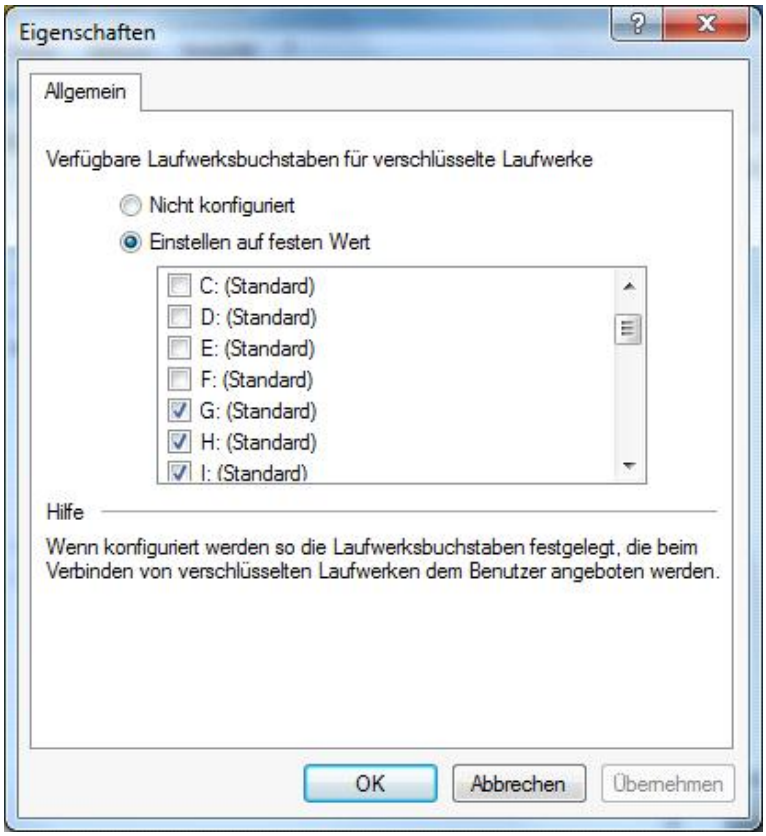
Clustergröße für verschlüsselte Laufwerke

Stellen Sie hier die Clustergröße für verschlüsselte Laufwerke ein.



Verfügbare Laufwerksbuchstaben für verschlüsselte Laufwerke

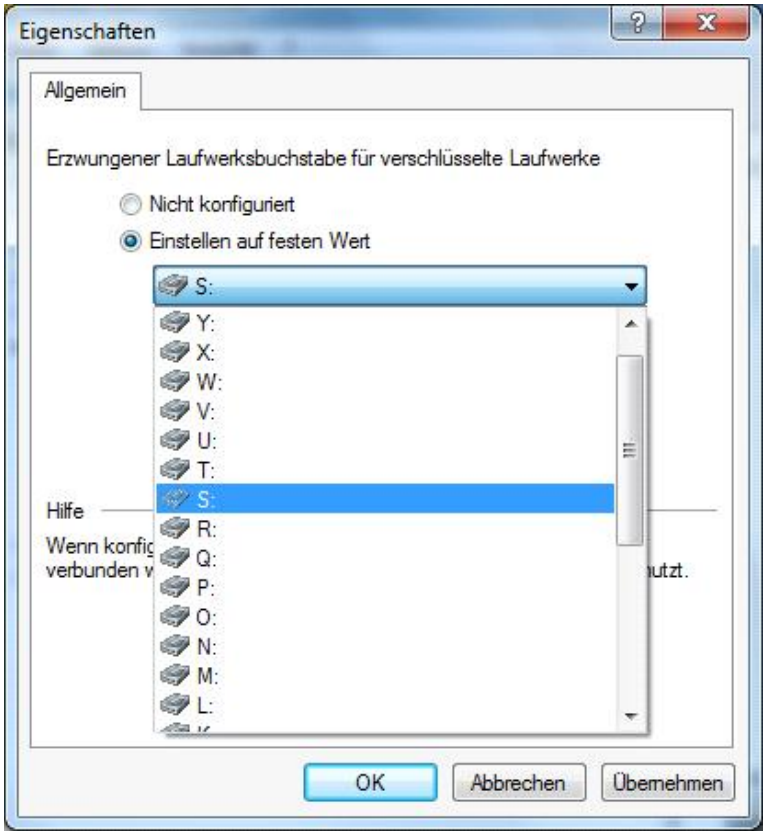
Konfigurieren Sie hier die Laufwerksbuchstaben, die automatisch an verschlüsselte Laufwerke vergeben werden.



Diese Funktionalität ist insbesondere dann hilfreich, wenn bereits bestimmte Laufwerksbuchstaben zum Beispiel durch Netzwerkfreigaben belegt sind.

Erzwungener Laufwerksbuchstabe für ein verschlüsseltes Laufwerk

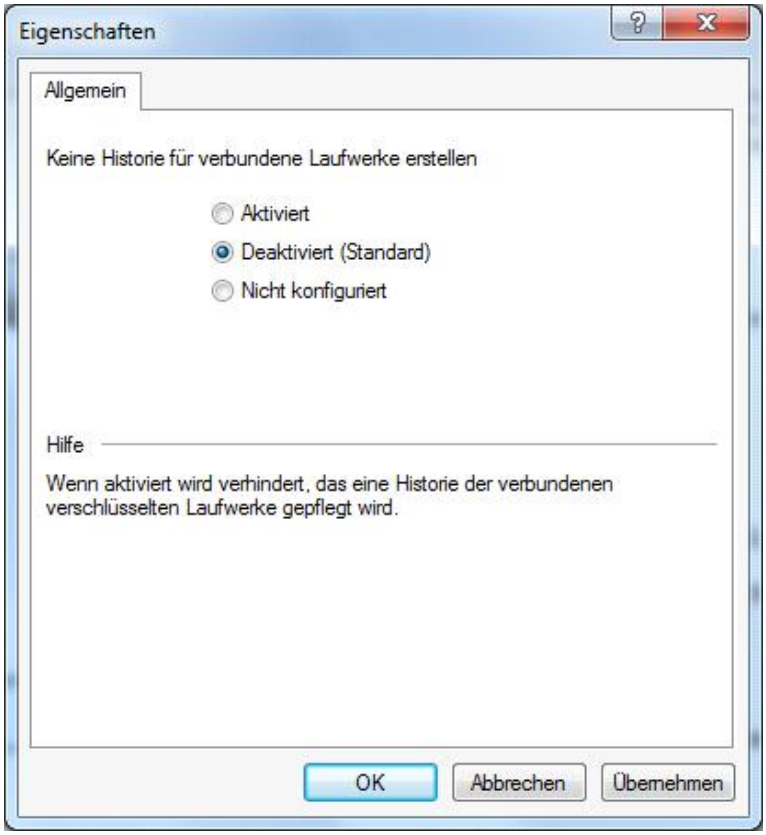
Durch Aktivieren dieser Einstellung kann nur ein verschlüsseltes Laufwerk mit dem definierten Buchstaben verbunden werden.



7.2.2.1.4 Einschränkungen für Benutzer

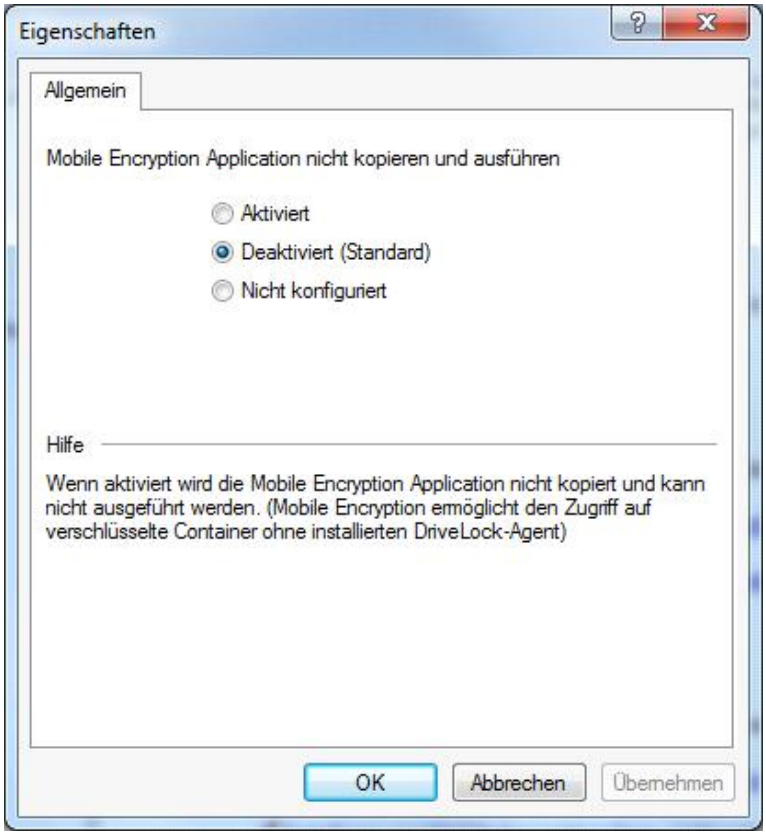
Keine Historie für verbundene Laufwerke erstellen

Diese Option verhindert die Verlaufserstellung verbundener Datenträger.



Erstellung von Mobile Encryption Disks nicht zulassen

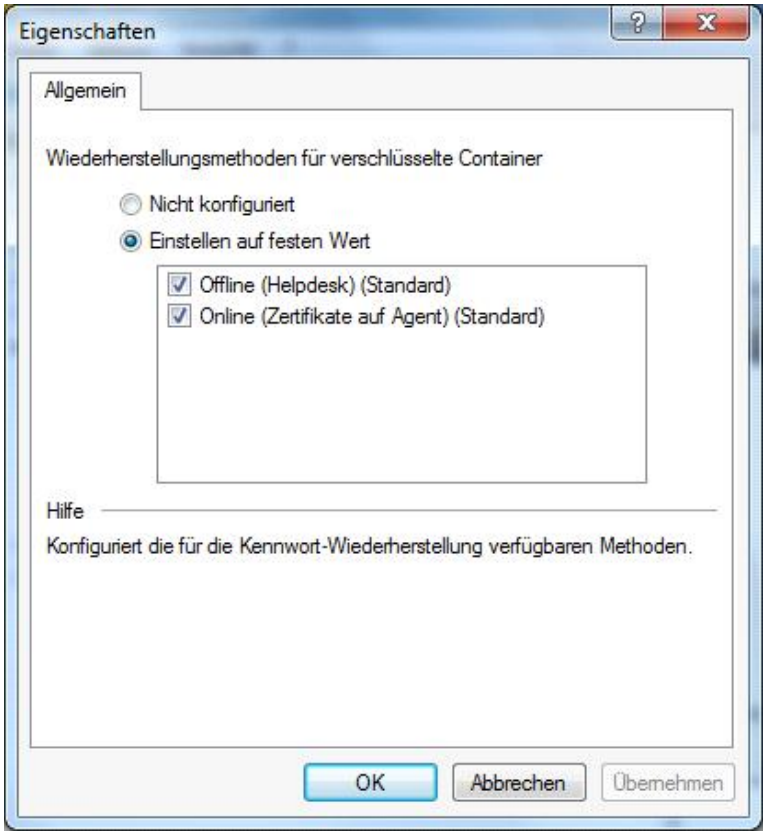
Die Mobile Encryption Anwendung (MEA) wird zur Entschlüsselung von Daten auf einem Rechner benötigt, der keinen DriveLock Agenten installiert hat. DriveLock kann die MEA zusammen mit einer Autostart-Datei auf ein Laufwerk kopieren, wenn darauf eine verschlüsselte Container-Datei abgelegt wird. Deaktivieren Sie diese Option, wenn dies für den Benutzer nicht möglich sein soll.



Wiederherstellungsmethoden für verschlüsselte Container

DriveLock stellt für die Wiederherstellung verlorengegangener Passwörter bei verschlüsselten Containern zwei Methoden zur Verfügung:

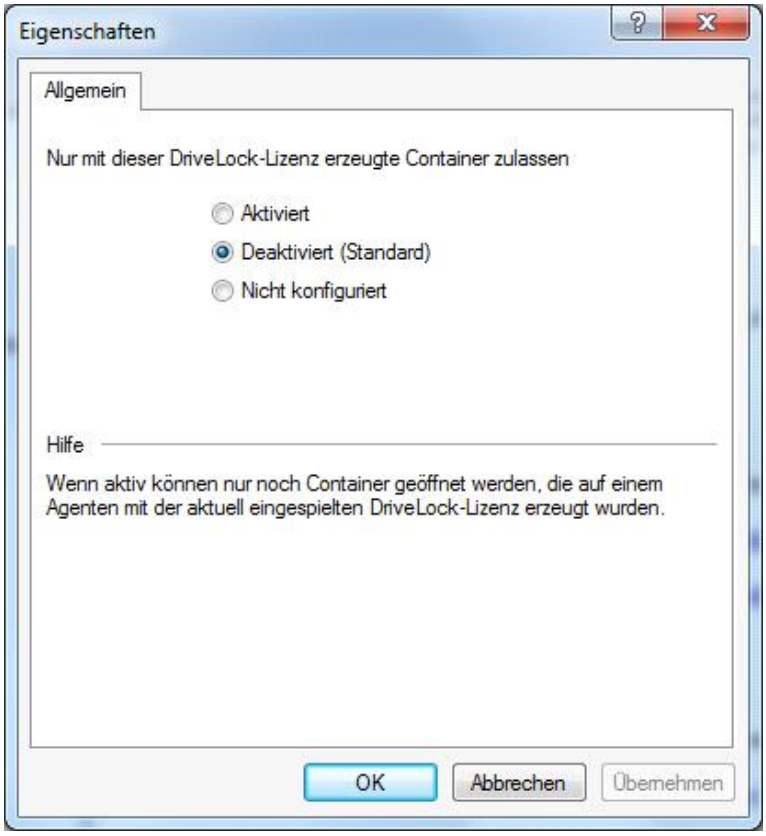
- *Offline-Wiederherstellung über ein Challenge-Response-Verfahren*:
  Mit Unterstützung eines Assistenten kann das Passwort eines verschlüsselten Containers zurückgesetzt werden, auch wenn der Computer derzeit nicht mit dem Firmennetzwerk verbunden ist.
- *Online-Wiederherstellung über lokal installierte Zertifikate*:
  Ist diese Option aktiviert, kann ein Passwort auch ohne ein Challenge-Response-Verfahren zurückgesetzt werden, vorausgesetzt das dafür notwendige Zertifikat mit privatem und öffentlichem Schlüsselpaar ist lokal auf dem entsprechenden Rechner verfügbar.



Um die Wiederherstellungsmethoden auszuwählen, die im Wiederherstellungs-Assistenten verfügbar sein sollen, aktivieren Sie die Option *„Einstellen auf festen Wert“* und markieren Sie den jeweiligen Eintrag.

Nur mit dieser DriveLock-Lizenz verschlüsselte Container zulassen

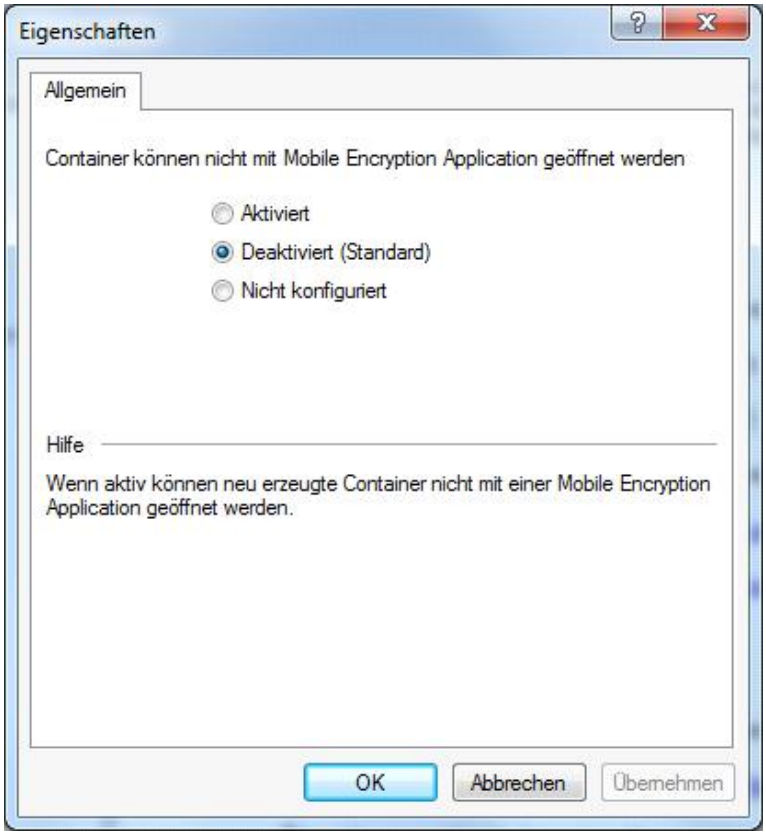
Normalerweise kann DriveLock jeden verschlüsselten Container öffnen, egal wo und mit welcher Lizenz dieser erzeugt wurde.



Wenn Sie diese Option aktivieren, kann DriveLock nur noch Container öffnen, die von einem Agenten mit der gleichen Lizenz wie der gerade konfigurierten verschlüsselt wurden.

Container können nicht mit Mobile Encryption Application geöffnet werden

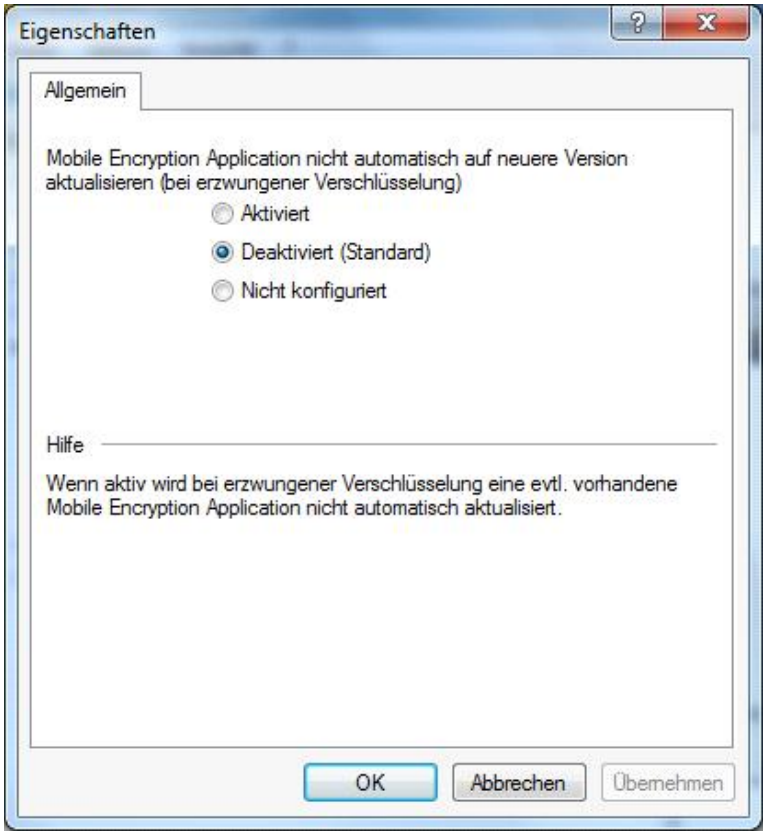
Die Mobile Encryption Anwendung dient dazu, verschlüsselte Laufwerke oder Container auch auf Systemen zu entschlüsseln, auf denen kein DriveLock installiert ist.



Um zu verhindern, dass verschlüsselte Container oder Laufwerke mit Hilfe der MEA verwendet werden können, die in Ihrem Unternehmen erzeugt wurden, aktivieren Sie diese Option.

Mobile Encryption Anwendung nicht automatisch auf neuere Version aktualisieren

Normalerweise überprüft DriveLock beim Verbindungsversuch, ob die auf einem Wechseldatenträger vorhandene MEA der aktuellen Version entspricht und ersetzt sie ggf. automatisch mit der aktuellsten Version.



Möchten Sie dieses Standardverhalten abschalten, wählen Sie die Option „**Aktiviert**“.

7.2.2.2 Konfiguration der Kennwort-Wiederherstellung

Dieser Abschnitt beschreibt die beiden notwendigen Konfigurationsschritte, um später bei Bedarf das Passwort bei einem verschlüsselten Container (zum Beispiel bei einem zwangsverschlüsselten USB-Stick) zurücksetzen zu können.

Wenn keine dieser beiden Optionen konfiguriert ist, gibt es keinen Weg, das existierende Passwort zurückzusetzen oder auf das verschlüsselte Laufwerk ohne Passwort des Benutzers zuzugreifen.

Für die Kennwort-Wiederherstellung über das Challenge-Response-Verfahren im Offline-Fall muss ein DriveLock Enterprise Service installiert und verfügbar sein.

Wenn ein verschlüsselter Container erstellt wird (z.B. bei einer Zwangsverschlüsselung eines USB-Sticks), erzeugt der DriveLock Agent die Wiederherstellungsinformationen lokal und sendet diese anschließend an den DriveLock Enterprise Service. Von dort werden diese Informationen im Falle einer Offline-Wiederherstellung durch den Administrator abgerufen. Der genaue Vorgang einer Offline-Wiederherstellung wird im Kapitel „Passwort-Wiederherstellung verschlüsselter Containerdateien“ beschrieben.

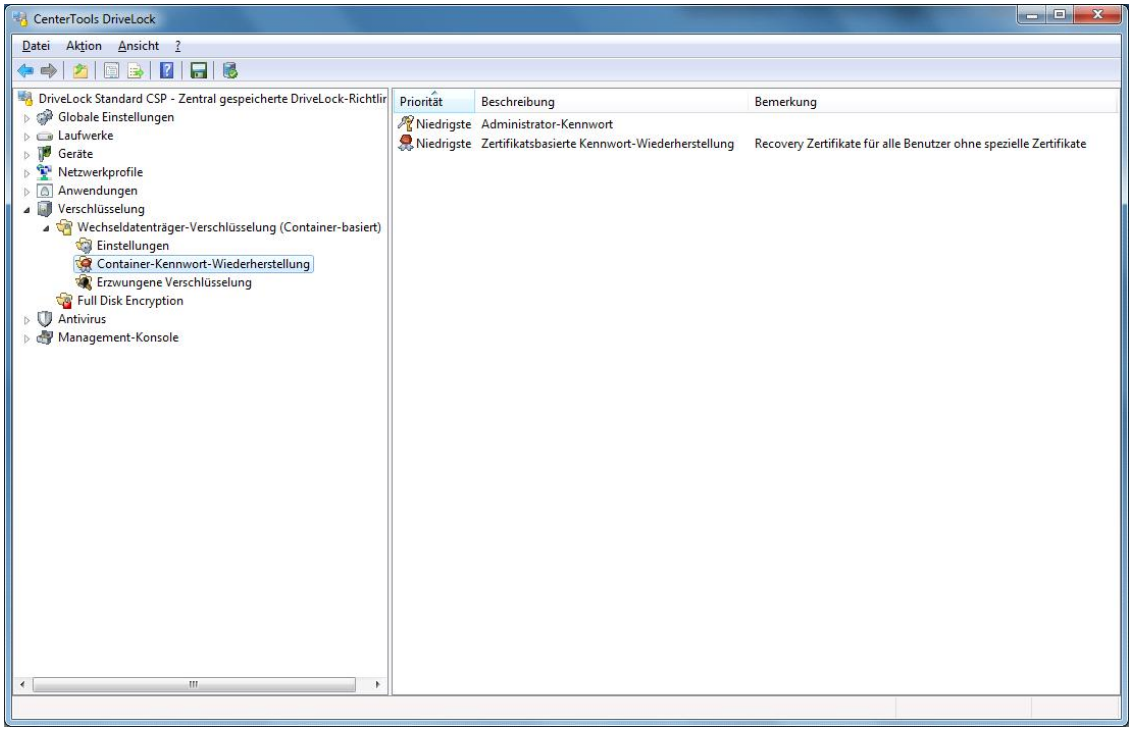
Besteht keine Online-Verbindung zum DriveLock Enterprise Service, werden die Wiederherstellungsinformationen an den DriveLock Enterprise Service gesendet, sobald dieses wieder zur Verfügung steht. Bis die Daten in der DriveLock Datenbank aktualisiert werden, können bis zu 30 Minuten vergehen.

7.2.2.2.1 Konfiguration von Administratorpasswörtern

Zusätzlich zum Passwort des Benutzers können separate Administratorpasswörter konfiguriert werden. Für den Fall, dass der Benutzer sein Passwort vergessen hat, kann der Administrator darüber auf das verschlüsselte Laufwerk

zugreifen oder das bestehende Benutzerpasswort zurücksetzen. Hierfür sollte immer ein sehr komplexes Passwort verwendet werden.

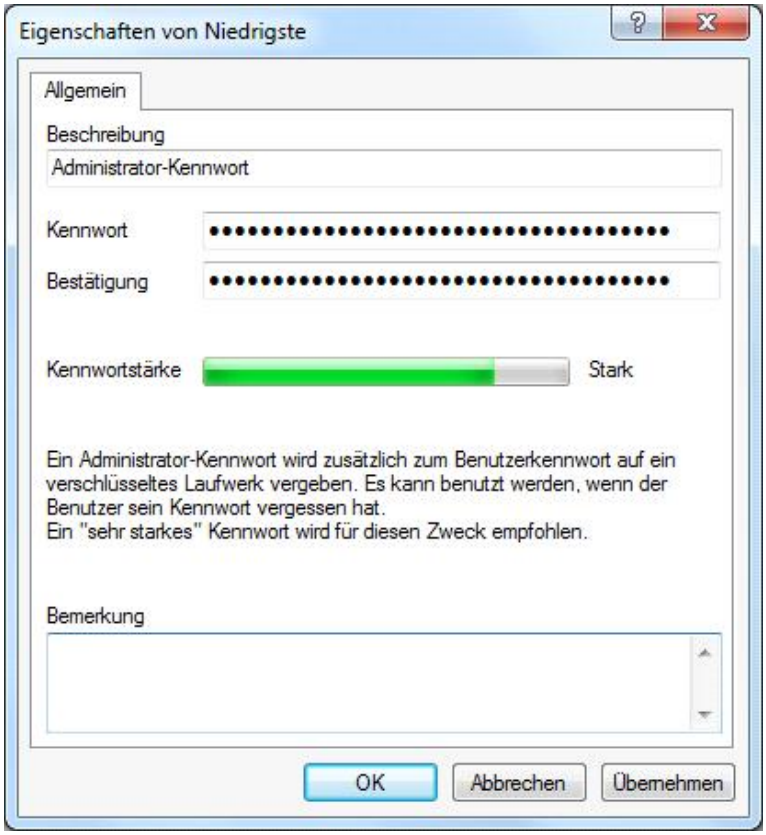
Klicken Sie auf **Container-Kennwort-Wiederherstellung** im Navigationsbereich.



Administrator-Kennungen werden durch das Symbol gekennzeichnet.

Standardmäßig ist zunächst ein Administrator-Kennwort vorhanden (Beschreibung **Administrator-Kennwort**), welches für alle verschlüsselte Container verwendet wird (sofern konfiguriert). Dieses Kennwort hat die Priorität „Niedrigste“ und kann nicht gelöscht werden.

Doppel-Klicken Sie auf **Administrator-Kennwort**, um den Dialog zur Eingabe eines zentralen Passwortes zu öffnen.



Geben Sie ein Passwort ein und klicken Sie **OK**, um das Fenster zu schließen.

Berücksichtigen Sie die folgenden Regeln zur Maximierung der Passwortstärke:

- Verwendung von Zahlen (0 bis 9)
- Verwendung von Großbuchstaben (A bis Z)
- Verwendung von Kleinbuchstaben (a bis z)
- Verwendung von Sonderzeichen (+"*ç%&/()=?è!é:£;:_,.-öä$ü¨^# etc.)
- Mindestpasswortlänge von 8 Zeichen
- Passwort darf nicht erraten werden können
- Passwort darf in keinem Wörterbuch gelistet sein

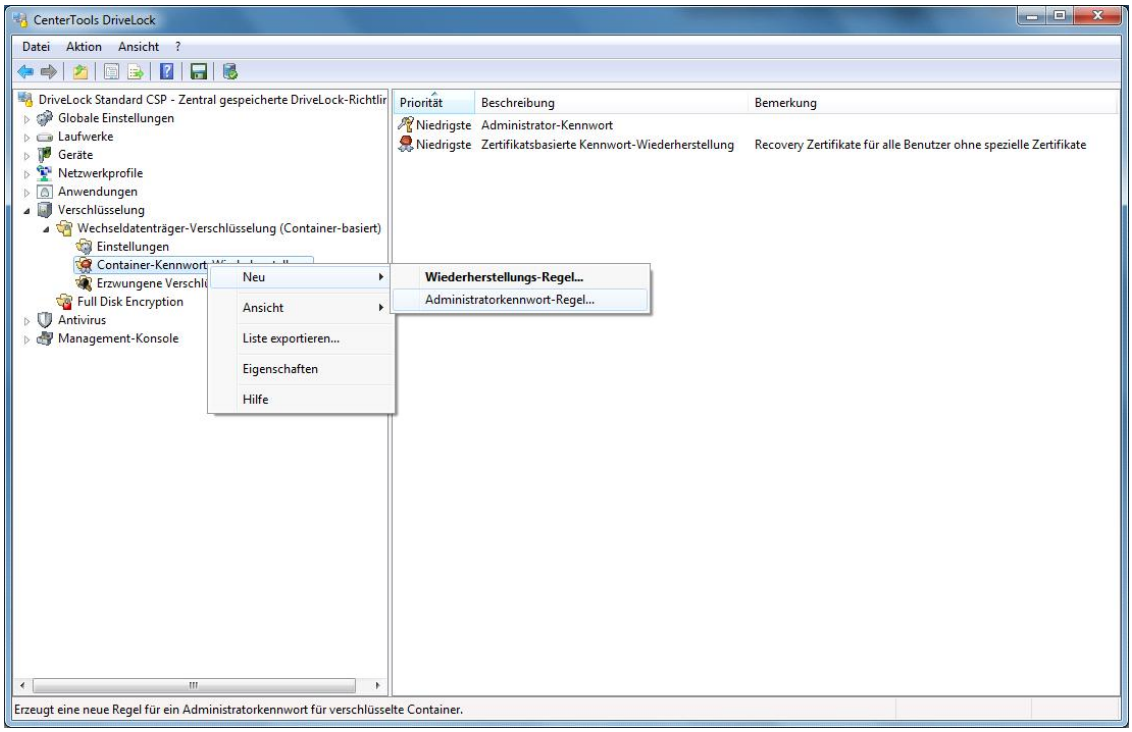
Für höchstmögliche Sicherheit wird ein sehr starkes Passwort für die Nutzung als Administratorpasswort empfohlen. Der Indikator kann dabei sicherstellen, ob ein Passwort hierfür den Anforderungen entspricht.

Stellen Sie sicher, diese administrativen Passwörter nicht zu vergessen. Sie sollten diese ebenso an einem anderen sicheren Ort aufbewahren (z.B. in einem Tresor).

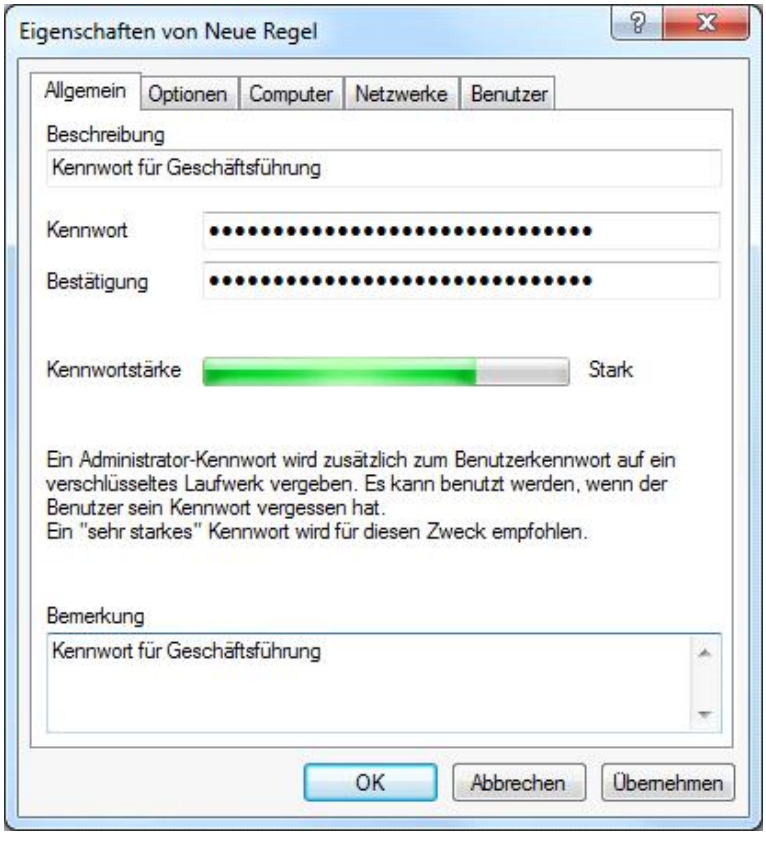
Zusätzlich zu diesem Default-Passwort können Sie nun weitere Passwörter anlegen. Da es bei diesen möglich ist, die Verwendung auf bestimmte Benutzer/Benutzergruppen, Computer oder Netzwerkverbindungen einzuschränken, sind Sie zum Beispiel in der Lage, für Geschäftsführer andere Wiederherstellungskennwörter zu verwenden, als für Mitarbeiterinnen der Buchhaltung.

Es ergeben sich aber noch weitaus mehr Anwendungsfälle für unterschiedliche Kennungen, da DriveLock diese Kennungen auch verwendet, um im Unternehmensnetzwerk die Verwendung von verschlüsselten externen Laufwerken (z.B: USB-Sticks) einfach und für den Benutzer transparent zu halten, so dass dieser nicht extra ein persönliches

Passwort eingeben muss, um Zugang zu seinem verschlüsselten Laufwerk zu erhalten. Wenn Sie nun zum Beispiel für die USB-Sticks der Geschäftsführung andere Kennungen verwenden als für die USB-Sticks deren Assistentinnen, dann können Geschäftsführer ihre eigenen Sticks verwenden, ohne dass nach einem Passwort gefragt wird, währen die Assistentinnen die Sticks ihrer Geschäftsführer nur mit dem entsprechenden persönlichen Passwort benutzen dürfen (und andersherum).

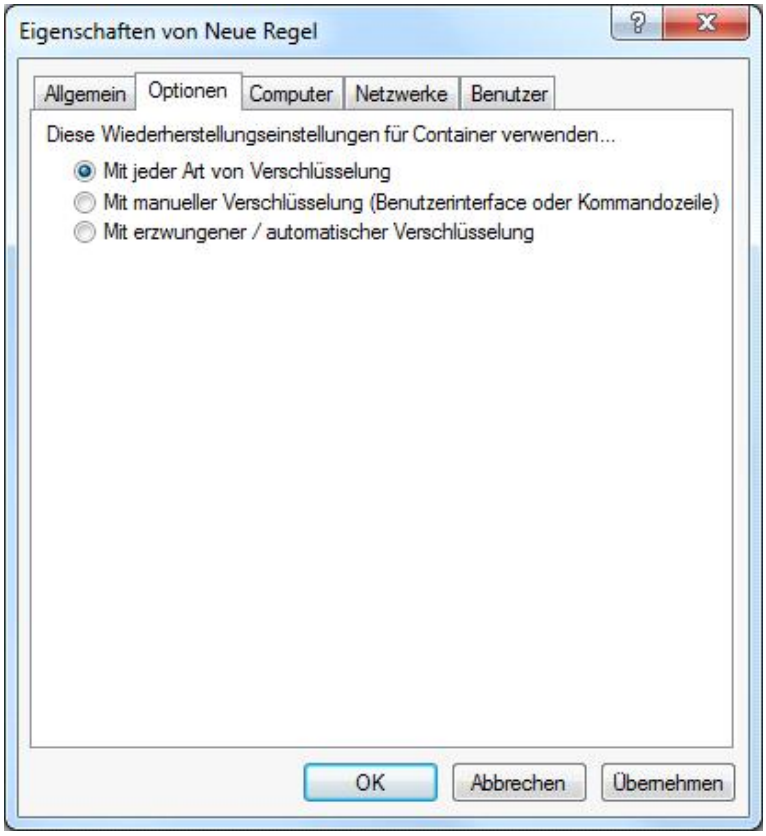


Rechtsklicken Sie auf **Container-Kennwort-Wiederherstellung** und wählen **Neu: Administratorkennwort-Regel** aus dem Kontextmenü.



Geben Sie eine Beschreibung und ein sicheres Passwort ein.

Wählen Sie den Reiter **Optionen**.



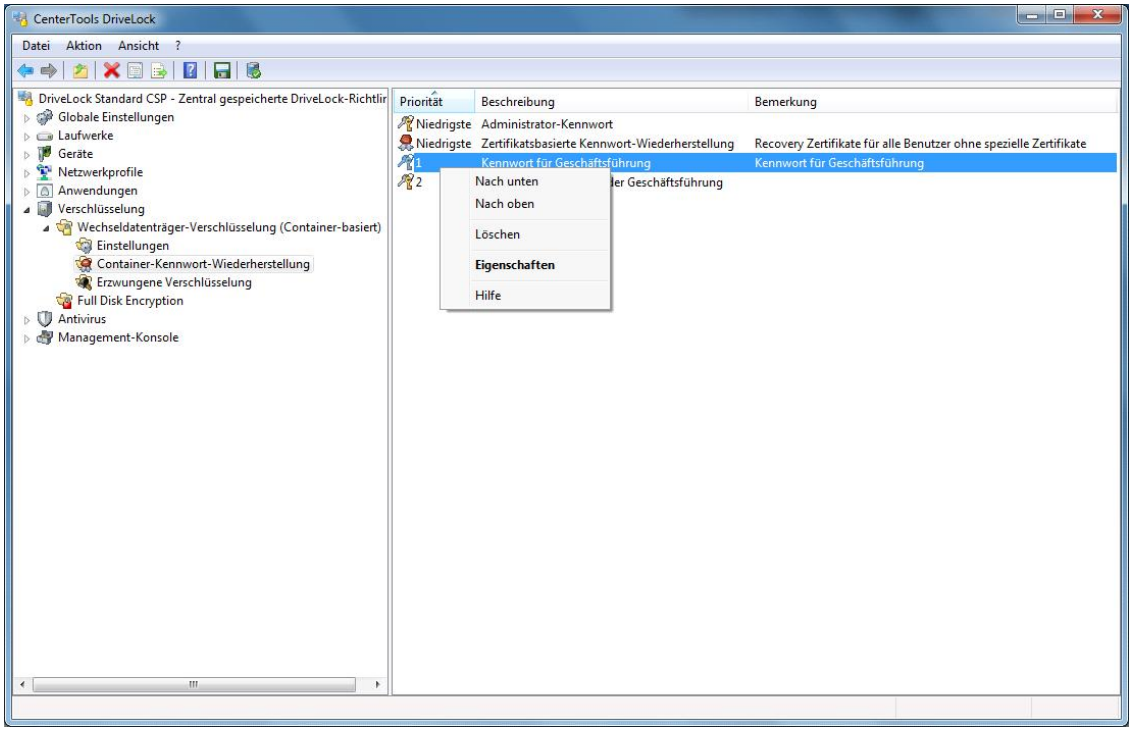
Folgende Optionen stehen zur Verfügung:

- *Mit manueller Verschlüsselung (…)* – Diese Kennung wird nur verwendet, wenn die Verschlüsselung durch einen Benutzer über Kommandozeile oder durch das Benutzerinterface von DriveLock erfolgt.
- *Mit erzwungener / automatischer Verschlüsselung* – Diese Kennung wird nur verwendet, wenn die Verschlüsselung automatisch durch DriveLock erfolgt (sog. erzwungene Verschlüsselung)
- *Mit jeder Art von Verschlüsselung* – Diese Kennung wird immer verwendet.

Über Einstellungen auf den Reitern **Computer**, **Netzwerke** und **Benutzer** können Sie nun festlegen, für welche der gleichnamigen Bereiche diese Kennung verwendet werden soll. Die Funktionsweise ist dabei die gleiche wie auch an vielen anderen Stellen bei DriveLock (z.B. bei Laufwerks-Regeln) und wird daher hier nicht detaillierter Beschrieben.

Klicken Sie auf OK, um die getroffenen Einstellungen zu übernehmen. Die neue Kennung wird anschließend in der Detailansicht rechts angezeigt.

Die erste zusätzliche Kennung erhält dabei die Priorität 1, jede weitere eine um eins erhöhte Priorität als die höchste vorhandene.



Rechts-klicken Sie auf einen Eintrag und wählen Sie **Nach unten** oder **Nach oben**, um die Reihenfolge der Priorisierung anzupassen. Über **Löschen** können Sie eine vorhandene Kennung löschen.

Wenn Sie ein bereits verwendetes Administratorpasswort löschen, ist darüber weder eine Kennwort-Wiederherstellung noch eine automatische Anmeldung mehr möglich.

7.2.2.2.2 Erzeugen des Offline-Wiederherstellungszertifikates

Damit Sie die Funktionalität der Offline-Passwort-Wiederherstellung nutzen können, müssen Sie vor der Erstellung des ersten verschlüsselten Containers ein Hauptzertifikat bestehend aus einem öffentlichen und privaten Schlüsselpaares erzeugen. Hierzu können durchaus auch mehrere Zertifikate angelegt werden, die über Computer / Netzwerke / Benutzer gefiltert werden können. Dies ist dann sinnvoll, wenn sich der Benutzerkreis unterscheidet, die eine Wiederherstellung verschlüsselter Daten durchführen dürfen. Es sollte aber mindestens das Standard-Wiederherstellungszertifikat mit der Priorität *Niedrigste* erzeugt werden.

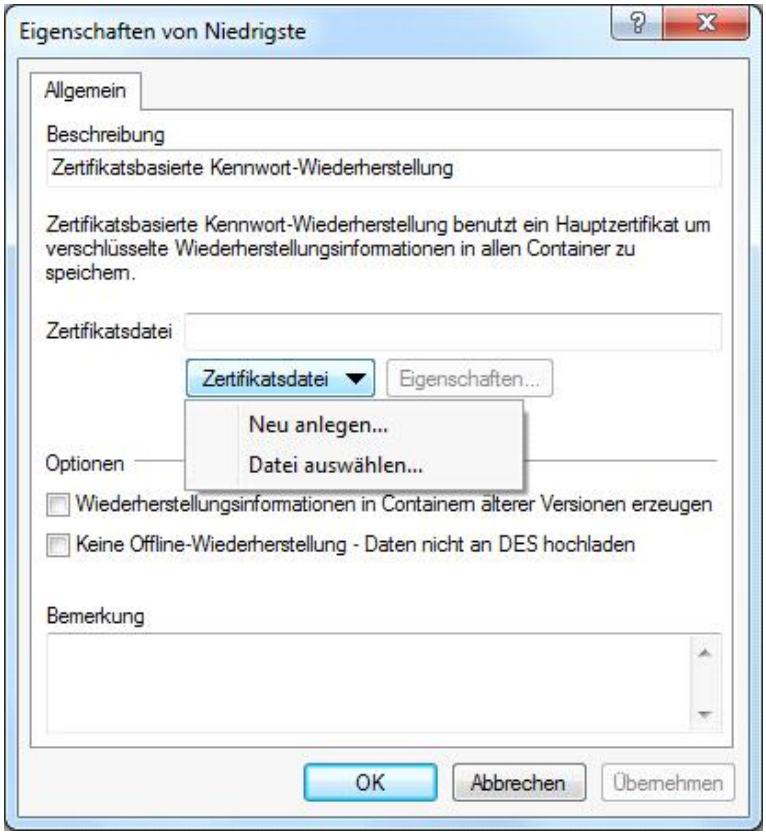
Beispiel: Gerade in großen Umgebungen kann es bevorzugt werden, ein Standard-Zertifikat zu erstellen, welches für alle verwendet wird. Lediglich für den Vorstand gibt es ein eigenes Wiederherstellungszertifikat. Das Standard-Zertifikat erhält der IT-Helpdesk, damit für alle Mitarbeiter außer dem Vorstand, das Passwort von verschlüsselten Containern zurückgesetzt werden kann. Nur der IT-Sicherheitsbeauftragte und der IT-Enterprise Administrator erhalten das Wiederherstellungszertifikat des Vorstands, damit auch hier eine Wiederherstellung möglich ist. Mit dieser Maßnahme wurde der Kreis der Personen, die potentiell Zugriff auf vertrauliche Daten haben (die des Vorstands), weiter eingeschränkt.

Bei der Passwort-Wiederherstellung (siehe auch „Passwort-Wiederherstellung verschlüsselter Containerdateien“) muss dann das passende Wiederherstellungs-Zertifikat ausgewählt werden, wenn Zertifikate mit mehreren Prioritäten erstellt wurden.

Wiederherstellungszertifikate werden durch das Symbol gekennzeichnet.

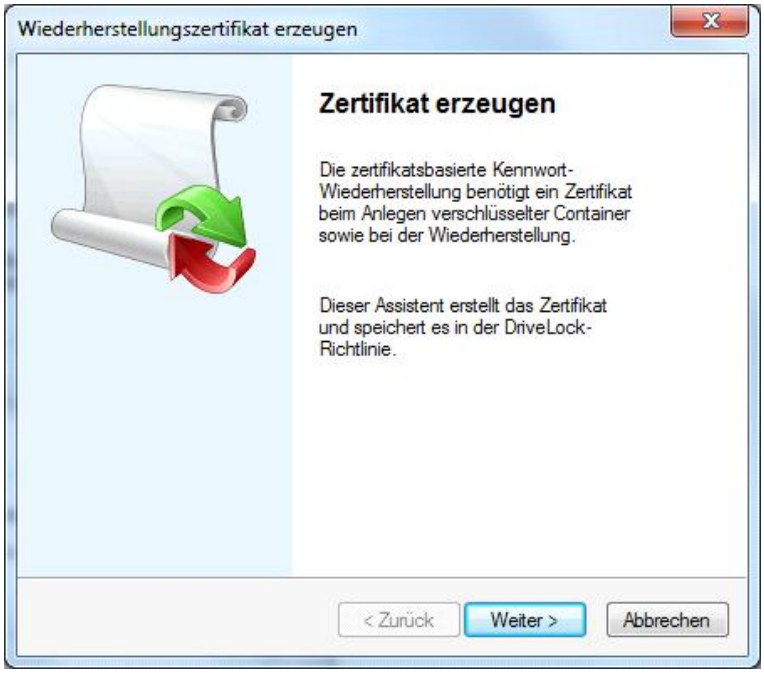
Standardmäßig ist zunächst ein Zertifikatseintrag vorhanden (Beschreibung **Zertifikatsbasierte Kennwort-Wiederherstellung**), welcher für alle verschlüsselte Container verwendet wird (sofern konfiguriert). Dieses Zertifikat hat die Priorität „Niedrigste“ und kann nicht gelöscht werden.

Doppel-Klicken Sie auf **Zertifikatsbasierte Kennwort-Wiederherstellung** (Priorität Niedrigste), um das Standard-Zertifikat zu erzeugen.

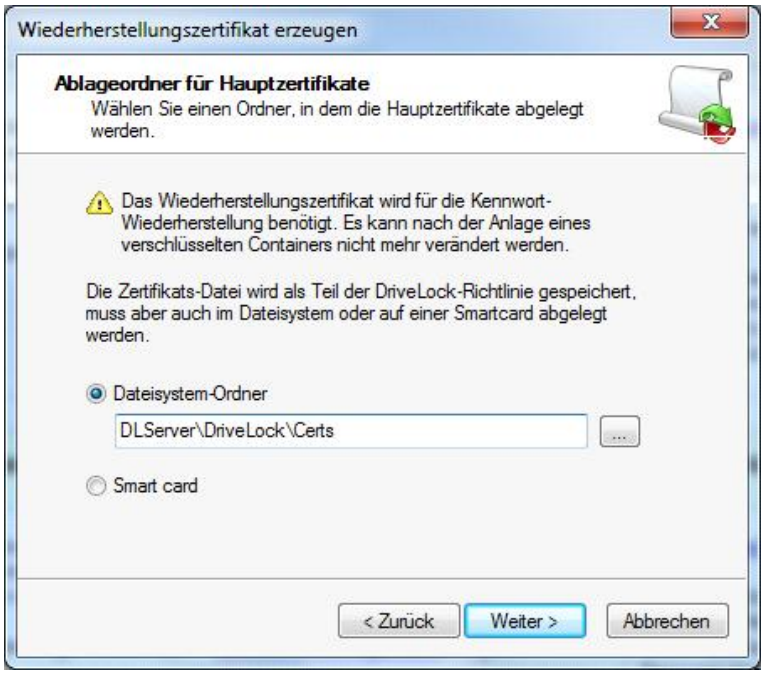


Am Anfang ist hier noch keine Zertifikatsdatei angegeben. Klicken Sie auf **Zertifikatsdatei** und wählen Sie „**Neu anlegen”** aus dem Drop-Down Menu aus.

Dadurch wird der Assistent für die Erzeugung des Hauptzertifikates gestartet.



Klicken Sie **Weiter**.

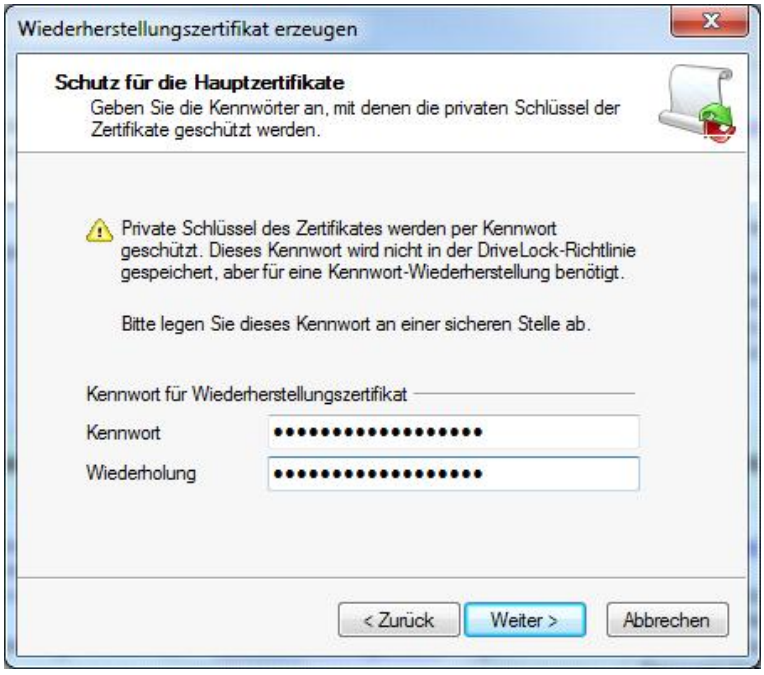


Geben Sie entweder den Ordner an, wo Sie die Zertifikats-Datei abspeichern möchten oder wählen Sie alternativ eine Smartcard als Speicherort.

Klicken auf **Weiter**.

Sofern Sie eine Smartcard zur Speicherung verwenden, werden Sie abhängig von der verwendeten Karte nun gebeten, die Karte einzulegen und auszuwählen.

Stellen Sie sicher, dass diese Datei an einem sicheren Ort abgespeichert wird, da sie für die Passwort-Wiederherstellung dringend benötigt wird.



Geben Sie nun das Passwort für den Zugriff auf den privaten Schlüsselbereich des Zertifikates an.

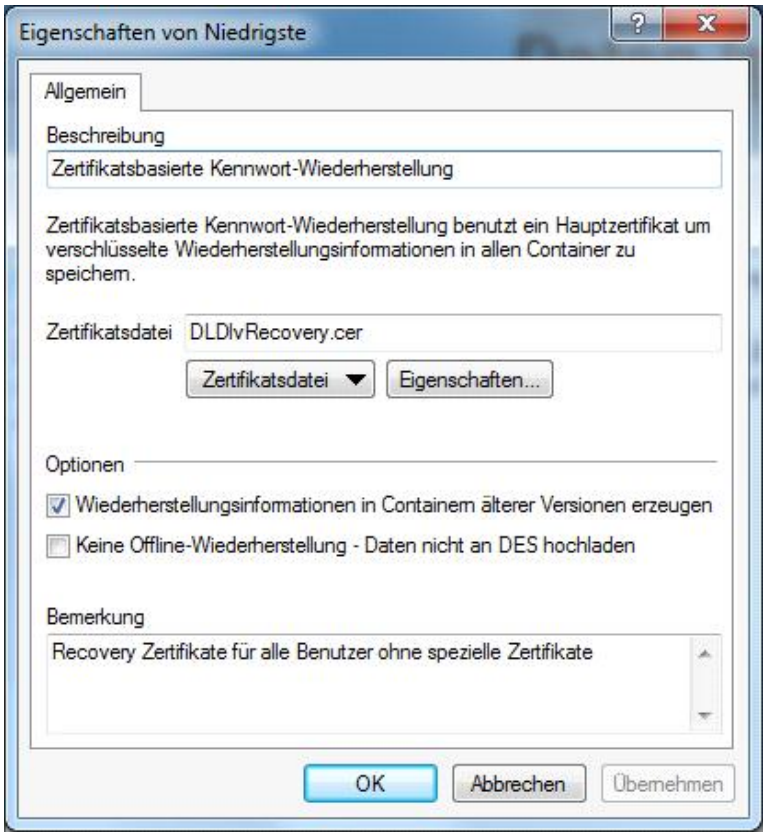
Sie müssen das Passwort aus Sicherheitsgründen zweifach eingeben. Um Fortzufahren, klicken Sie auf **Weiter**.

Stellen Sie sicher, dieses Passwort nicht zu vergessen. Sie sollten dieses ebenso an einem anderen sicheren Ort aufbewahren (z.B. in einem Tresor).

Es dauert einige Sekunden, um das Hauptzertifikat zu erzeugen. Anschließend werden Sie benachrichtigt, wenn der Prozess abgeschlossen ist und die Datei an dem zuvor angegebenen Ort abgespeichert wurde.

Sofern eine Smartcard zur Speicherung verwendet wird, werden Sie aufgefordert, die PIN für den Zugriff auf die Smartcard einzugeben.

Klicken Sie auf **Fertig stellen**.



Die soeben erzeugte Zertifikatsdatei wird nun angezeigt.

Sobald das Zertifikat erzeugt und der erste verschlüsselte Container erstellt wurde, darf kein neues Zertifikat mehr erstellt werden, da das alte damit überschrieben wird und somit für eine Wiederherstellung nicht mehr verwendet werden kann.

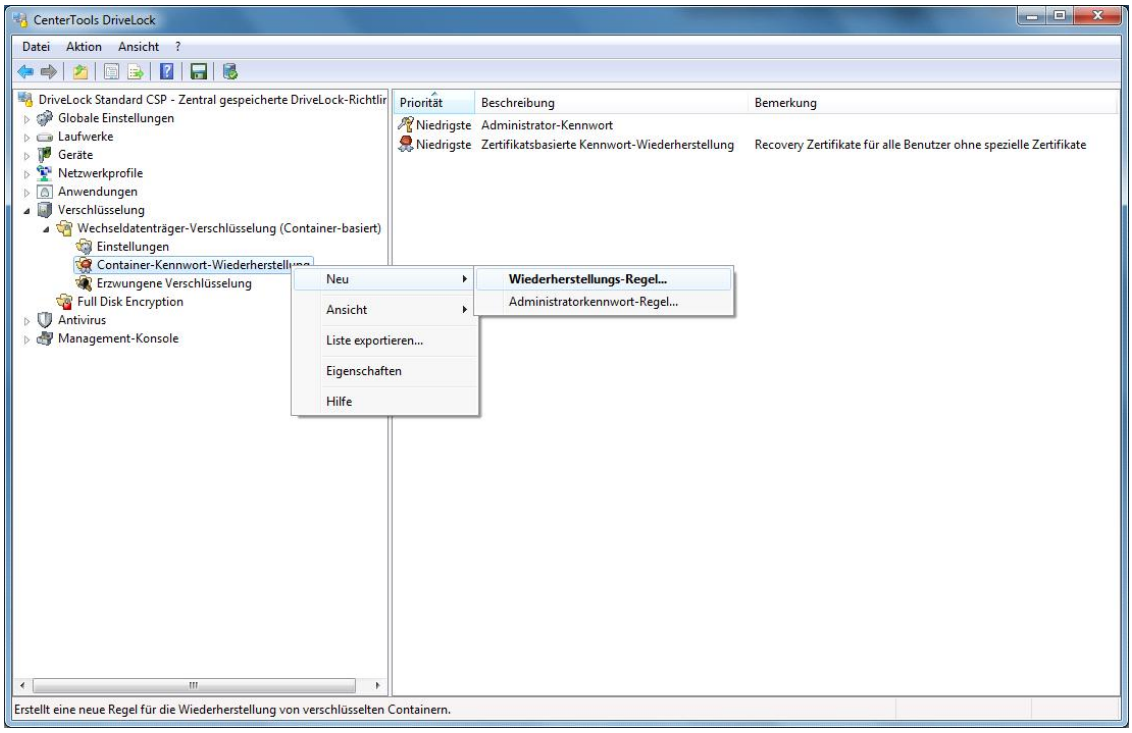
Wenn Sie auf **Eigenschaften** klicken, erhalten Sie zusätzliche Informationen über das Hauptzertifikat.

Das Zertifikat wird ebenfalls in dem privaten Zertifikatsspeichers des aktuellen Benutzers gespeichert. Der öffentliche Schlüssel des Zertifikates wird auch innerhalb des lokalen Richtliniendateispeichers abgelegt.

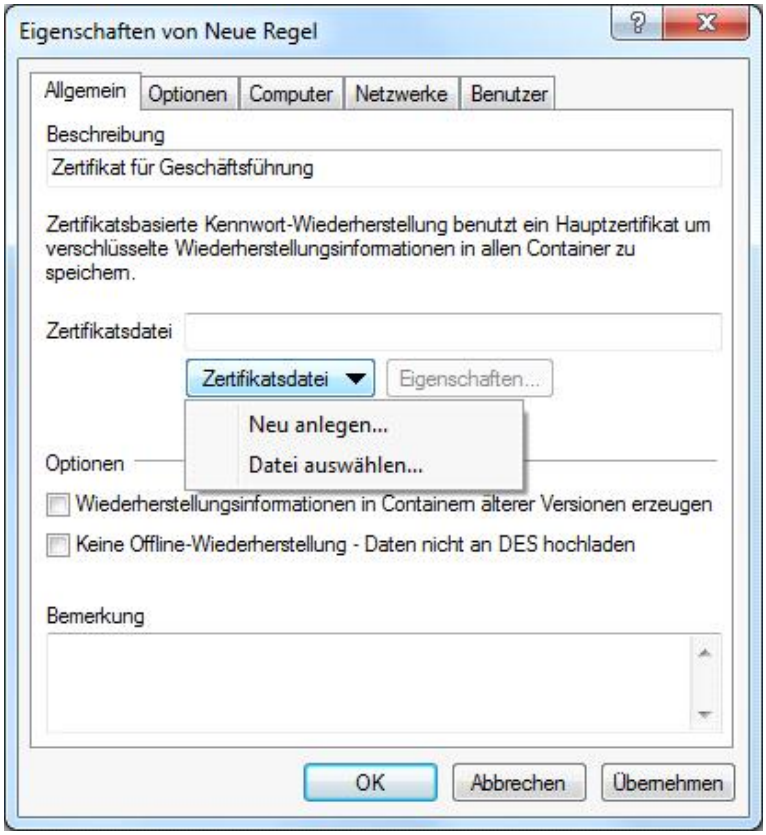
Wenn Sie den Erstellungs-Assistenten abgebrochen haben oder es während der Erstellung zu einem Problem gekommen ist, wird DriveLock die entsprechende Meldung anzeigen und Sie müssen das Hauptzertifikat erneut erzeugen.

Wenn Sie bisher mit einer älteren DriveLock Version verschlüsselte Container erzeugt haben, ist es sinnvoll, die Option *„Wiederherstellungsinformationen in Containern älterer Versionen erzeugen“* zu aktivieren. In diesem Fall überprüft DriveLock jedes Mal wenn ein Container als Laufwerk verbunden wird, ob bereits eine Wiederherstellungsinformation vorhanden ist und erzeugt gegebenenfalls diese Information. Anschließend werden die zur Wiederherstellung nötigen Daten auch an den DriveLock Enterprise Service übertragen.

Sofern der DriveLock Enterprise Service in Ihrer Umgebung nicht verwendet wird oder Sie die Übertragung der Wiederherstellungsdaten an den DriveLock Enterprise Service nicht möchten, können Sie dieses Verhalten durch Aktivieren der Option *„Keine Offline-Wiederherstellung – Daten nicht an DES hochladen“* verhindern.



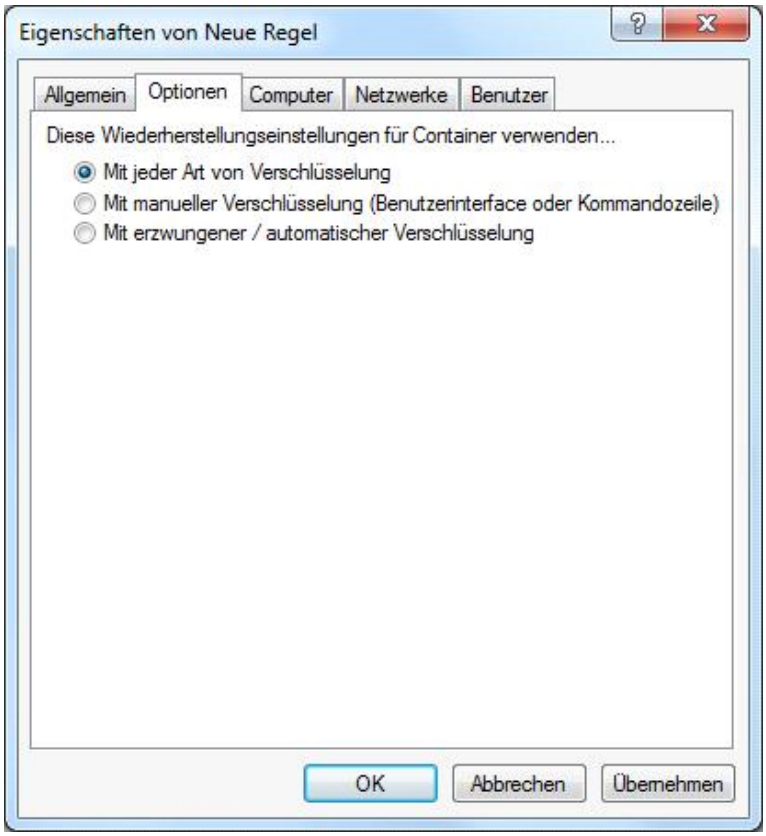
Rechtsklicken Sie auf **Container-Kennwort-Wiederherstellung** und wählen **Neu: Wiederherstellungs-Regel** aus dem Kontextmenü, um ein weiteres Zertifikat zu erzeugen.



Am Anfang ist hier noch keine Zertifikatsdatei angegeben. Klicken Sie auf **Zertifikatsdatei** und wählen Sie „**Neu anlegen**" aus dem Drop-Down Menu aus.

Dadurch wird der Assistent für die Erzeugung des Hauptzertifikates gestartet. Der Ablauf ist nun der gleiche wie bei der Erzeugung des Zertifikates für die niedrigste Priorität.

Wählen Sie den Reiter **Optionen**.



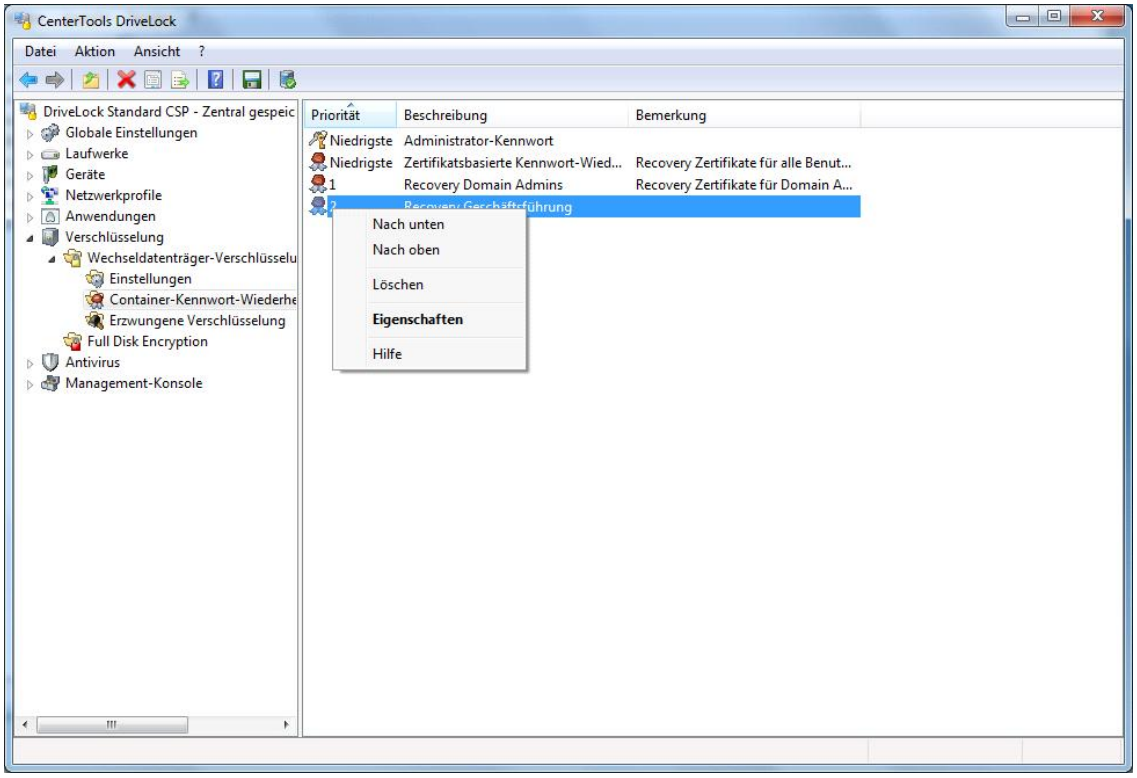
Folgende Optionen stehen zur Verfügung:

- *Mit manueller Verschlüsselung (...)* – Dieses Zertifikat wird nur verwendet, wenn die Verschlüsselung durch einen Benutzer über Kommandozeile oder durch das Benutzerinterface von DriveLock erfolgt.
- *Mit erzwungener / automatischer Verschlüsselung* – Dieses Zertifikat wird nur verwendet, wenn die Verschlüsselung automatisch durch DriveLock erfolgt (sog. erzwungene Verschlüsselung)
- *Mit jeder Art von Verschlüsselung* – Dieses Zertifikat wird immer verwendet.

Über Einstellungen auf den Reitern **Computer**, **Netzwerke** und **Benutzer** können Sie nun festlegen, für welche der gleichnamigen Bereiche dieses Zertifikat verwendet werden soll. Die Funktionsweise ist dabei die gleiche wie auch an vielen anderen Stellen bei DriveLock (z.B. bei Laufwerks-Regeln) und wird daher hier nicht detaillierter beschrieben.

Klicken Sie auf **OK**, um die getroffenen Einstellungen zu übernehmen. Das neue Zertifikat wird anschließend in der Detailansicht rechts angezeigt.

Das erste zusätzliche Zertifikat erhält dabei die Priorität 1, jedes weitere eine um eins erhöhte Priorität als die höchste vorhandene.



Rechts-klicken Sie auf einen Eintrag und wählen Sie **Nach unten** oder **Nach oben**, um die Reihenfolge der Priorisierung anzupassen. Über **Löschen** können Sie ein vorhandenes Zertifikat löschen.

Wenn Sie ein bereits verwendetes Zertifikat löschen, ist darüber keine Kennwort-Wiederherstellung mehr möglich.

7.2.2.3 Konfiguration zur Erzwingung der Verschlüsselung

Aktivieren sie die erzwungene Verschlüsselung mit *DriveLock Encryption 2-Go* in der Richtlinie unter:
Verschlüsselung/ Einstellungen / Methode für die erzwungene Verschlüsselung
Selektieren Sie **DriveLock Encryption 2-Go**.

Sie können für die erzwungenen Verschlüsselung auch *DriveLock File Protection* verwenden (siehe Erzwungene Verschlüsselung mit File Protection).

Bevor USB-Datenträger automatisch verschlüsselt werden können (erzwungene Verschlüsselung), müssen Grundeinstellungen getroffen werden.

Diese beinhalten u.a. den Verschlüsselungsalgorithmus und andere Rahmenbedingen, wie z.B. die Übernahme bestehender Daten von einem unverschlüsseltem Stick bei der Verschlüsselung oder die Größe des verschlüsselten Bereiches. Hierzu können verschiedene Regeln für bestimmte Benutzer oder Computer angelegt werden, oder auch Regeln, die nur bei bestimmten Netzwerkverbindungen angewendet werden.

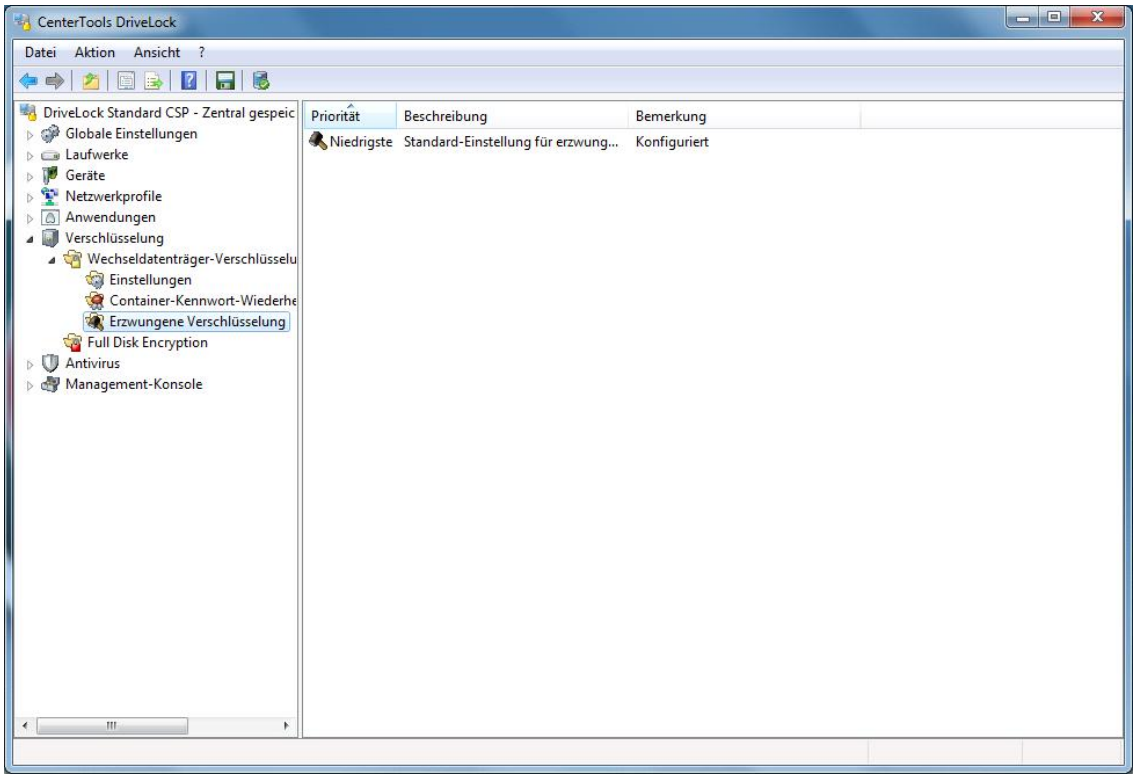
Falls gewünscht, können auch bis zu drei verschiedene dieser Regeln zu einer Benutzerauswahl zusammengefasst werden. Diese wird dem Benutzer angezeigt (z.B. beim Einstecken eines USB-Sticks) und dieser wählt aus den angebotenen Optionen die für ihn passende Verwendungsoption aus.

Beispiele:

- Alle USB-Sticks sollen mit AES verschlüsselt werden.
- Nur die USB-Sticks des Vorstandes sollen mit AES (FIPS-mode) verschlüsselt werden.

- Der Benutzer soll selbst entscheiden können, ob er den Stick komplett oder nur 50% der verfügbaren Kapazität für die Verschlüsselung nutzt.
- Der Benutzer kann zwischen den beiden Optionen „USB-Laufwerk komplett verschlüsseln“ und „Laufwerk unverschlüsselt nach Bestätigung eines Sicherheitshinweises lesend nutzern“ auswählen.

Zur Konfiguration der Einstellungen für die erzwungene Verschlüsselung klicken Sie auf **Erzwungene Verschlüsselung** im Navigationsbereich.

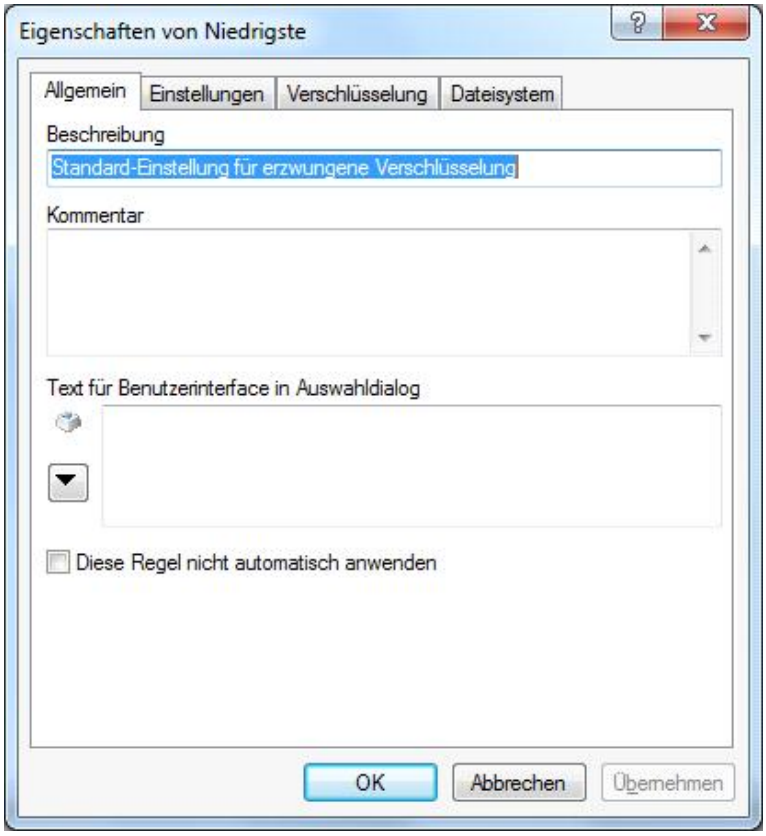


7.2.2.3.1 Einstellungsoptionen für alle Regeln der automatischen Verschlüsselung

Führen Sie einen Doppelklick auf den Eintrag **Standard-Einstellung für erzwungene Verschlüsselung** aus.

Die Standard-Einstellung mit der Priorität „**Niedrigste**“ ist immer vorhanden und kann auch nicht gelöscht werden. Wenn Sie die automatische Verschlüsselung verwenden möchten, müssen Sie entweder die Standard-Einstellungen festlegen, oder mindestens eine eigene Verschlüsselungs-Regel.

Die folgenden Parameter können auch bei allen weiteren Verschlüsselungs-Regeln, die Sie anlegen, konfiguriert werden.



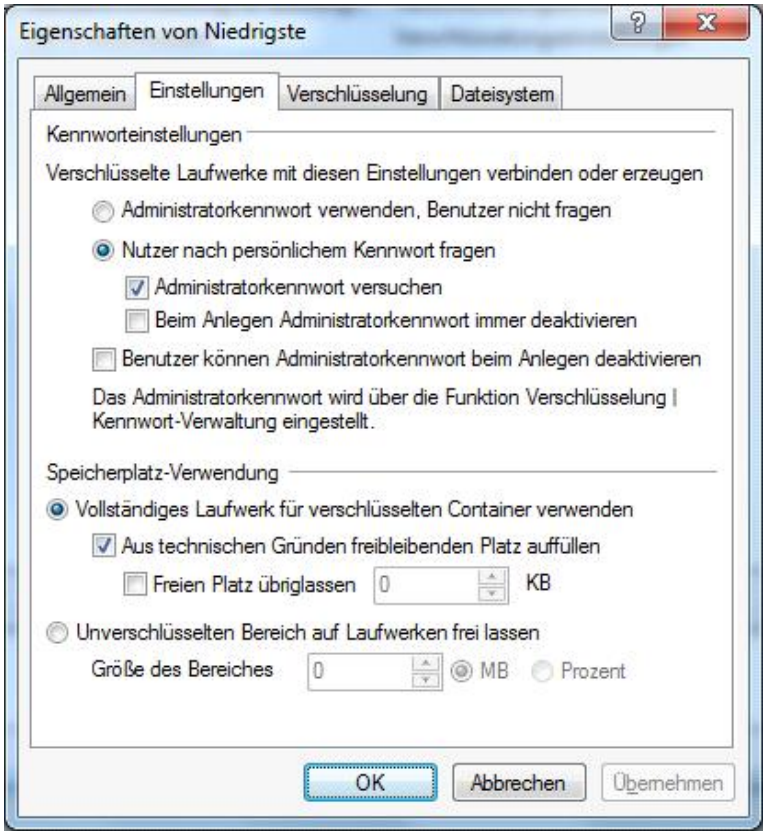
Der Beschreibungstext wird in der DriveLock Management Konsole angezeigt und dient Ihnen zur Unterscheidung der verschiedenen Regeln. Gleiches gilt auch für den Kommentar, den Sie eingeben können.

Die folgenden beiden Optionen spielen nur eine Rolle, wenn Sie zusätzlich auch noch eine Benutzerauswahl erstellen, bei der diese Verschlüsselungs-Regel verwendet wird.

Das Textfeld „**Text für Benutzerinterface in Auswahldialog**“ enthält den Text, der für die Schaltfläche innerhalb des Benutzerauswahldialogs angezeigt wird (siehe dazu auch Abschnitt „Eine Benutzerauswahl definieren“). Sie können an dieser Stelle auch eine vorher konfigurierte mehrsprachige Benachrichtigung auswählen, in dem Sie auf das Symbol klicken.

Die Option „**Diese Regel nicht automatisch anwenden**“ muss aktiviert werden, wenn diese Regel innerhalb einer Benutzerauswahl verwendet wird. In diesem Fall möchten Sie ja nicht, dass die Regel sofort nach dem Verbinden des Laufwerkes aktiv wird und die automatische Verschlüsselung beginnt (bzw. der Verschlüsselungsassistent startet), sondern dass zunächst der Benutzerauswahldialog erscheint und der Benutzer die gewünschte Option selbst auswählt.

Wählen Sie nun den Reiter **Einstellungen**.



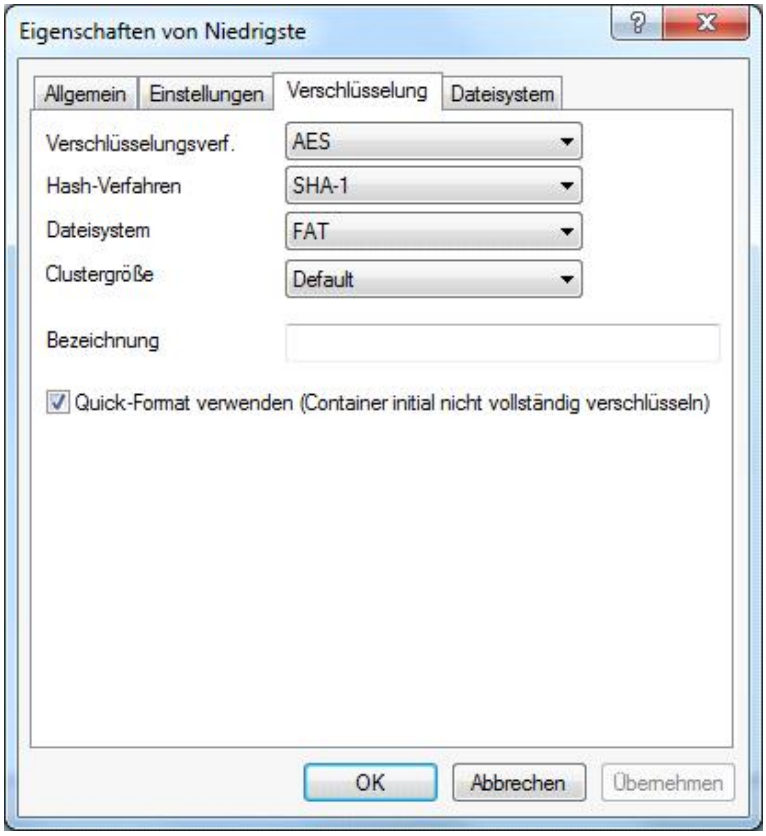
Die folgenden allgemeinen Einstellungen sind verfügbar:

- *Administratorkennwort verwenden, Benutzer nicht fragen:* Bei Aktivierung dieser Option wird das Administratorpasswort verwendet wie in Abschnitt „Konfiguration eines Administratorpassworts“ beschrieben. Benutzer können kein eigenes Passwort verwenden.
- *Nutzer nach persönlichem Kennwort fragen:* Bei dieser Einstellung wird der Benutzer nach seinem Passwort gefragt.
    - *Administratorkennwort versuchen*: Der Benutzer wird idealerweise gar nicht seinem Passwort gefragt. Die Verschlüsselung ist damit zu 100% transparent für den Benutzer. Dies setzt voraus, dass unter *Container-Kennwort-Wiederherstellung* ein *Administrator-Kennwort* gesetzt ist. Kann DriveLock einen Container nicht automatisch laden (weil z.B. das *Administrator-Kennwort* nicht übereinstimmt), wird der Benutzer nach seinem Passwort gefragt.
    - *Beim Anlegen Administratorkennwort immer deaktivieren:* Sobald der Benutzer sein persönliches Kennwort festgelegt hat, wird beim Anlegen des verschlüsselten Containers das Administratorkennwort gelöscht. Dadurch kann auf die verschlüsselten Daten nur noch durch Eingabe des Benutzerkennwortes zugegriffen werden.
- *Benutzer können Administratorkennwort beim Anlegen deaktivieren:* Wählen Sie diese Option, wenn es Benutzern ermöglicht werden soll, „private“ Containerdateien ohne Administrator-Zugang zu erzeugen. Wenn Sie zusätzlich noch die Option „*Administratorkennwort verwenden, Benutzer nicht fragen*“ aktivieren, muss ein Anwender beim Erzeugen die Option „Privat“ extra auswählen und kann dann erst ein persönliches Kennwort eingeben.
- *Vollständiges Laufwerk für verschlüsselten Container verwenden:* DriveLock verwendet den kompletten verfügbaren Speicherplatz für die Verschlüsselung. Aus technischer Sicht muss DriveLock die voraussichtliche maximale Größe des verschlüsselten Containers berechnen, wenn die Daten erhalten bleiben sollen. Das kann dazu führen, dass etwas Speicherplatz nicht von dem verschlüsselten Laufwerk verwendet wird.

- *Aus technischen Gründen freibleibenden Platz auffüllen* : Wenn Sie erreichen möchten, dass der Container den kompletten verfügbaren Speicherplatz verwenden kann, aktivieren Sie diese Funktionalität. In Verbindung mit dieser Option können Sie DriveLock veranlassen, den kompletten restlichen verfügbaren Speicherplatz (sofern verfügbar) aufzufüllen. Dazu erstellt DriveLock eine versteckte Systemdatei in entsprechender Größe.
- *Freien Platz übriglassen x KB* : In manchen Windows 7 Umgebungen, müssen wenige KB frei bleiben, damit überhaupt auf das Laufwerk zugegriffen werden kann.

- *Unverschlüsselten Bereich auf Laufwerk freilassen:* Wählen Sie diese Option, wenn Sie nicht den vollständigen Platz auf einem Laufwerk für die Verschlüsselung verwenden möchten. Geben Sie eine Größe an und legen Sie fest, ob die Zahl als absoluter Wert oder als Prozentwert verstanden werden soll.

Wählen Sie nun den Reiter **Verschlüsselung**.



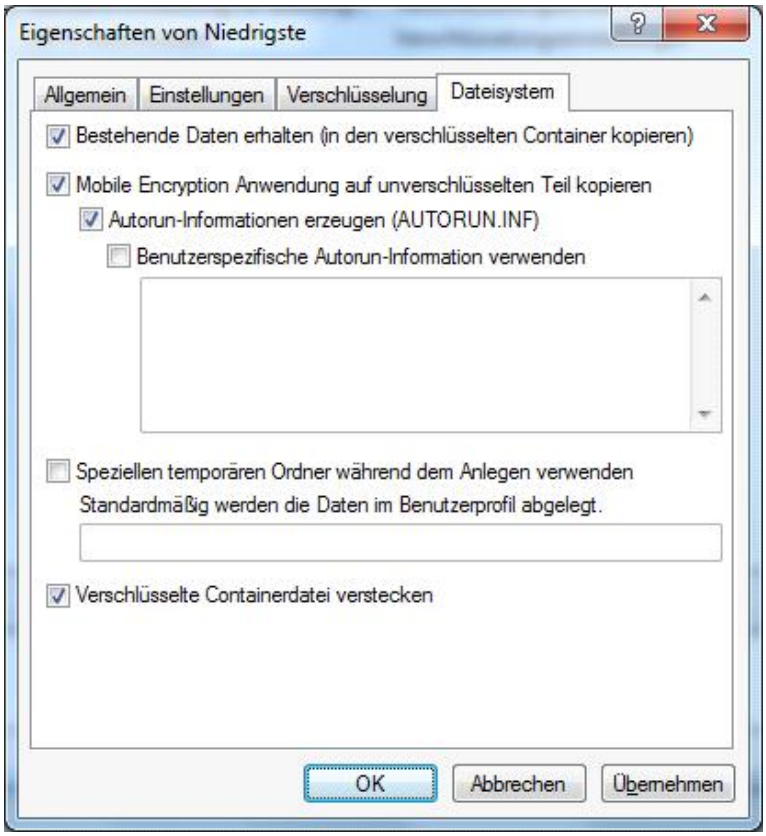
Die folgenden weiteren Einstellungen sind verfügbar:

- *Verschlüsselungsverf.:* Wählen Sie einen Verschlüsselungsalgorithmus, der für die Ver- und Entschlüsselung verwendet werden soll.
- *Hash-Verfahren:* Wählen Sie den Hash Algorithmus, der für die Ver- und Entschlüsselung verwendet werden soll.
- *Dateisystem:* Legt das Dateisystem fest, das innerhalb eines Containers zum Einsatz kommt. Wählen Sie zwischen FAT und NTFS.
- *Clustergröße:* Definiert die Clustergröße für neue verschlüsselte Laufwerke.
- *Bezeichnung:* Konfiguriert den zu verwendenden Namen für das verbundene verschlüsselte Laufwerk.
- *Quick-Format verwenden:* Um den Zeitraum zum Erstellen eines verschlüsselten Containers zu verkürzen, wählen Sie die Option “Aktiviert”. Dadurch wird nicht der komplette verschlüsselter Container durch den DriveLock Agenten mit Null-Werten initialisiert, sondern es werden nur die wirklich benötigten Daten

verschlüsselt. Dadurch kann es sein, dass zuvor unverschlüsselter Inhalt solange mit entsprechenden Verfahren wiederherstellbar ist, bis er durch verschlüsselten Inhalt überschrieben wird.

Quick-Format führt nur auf Windows 7 (oder neuer) Betriebssystemen zu einer spürbaren Beschleunigung.

Wählen Sie nun den Reiter **Dateisystem**.

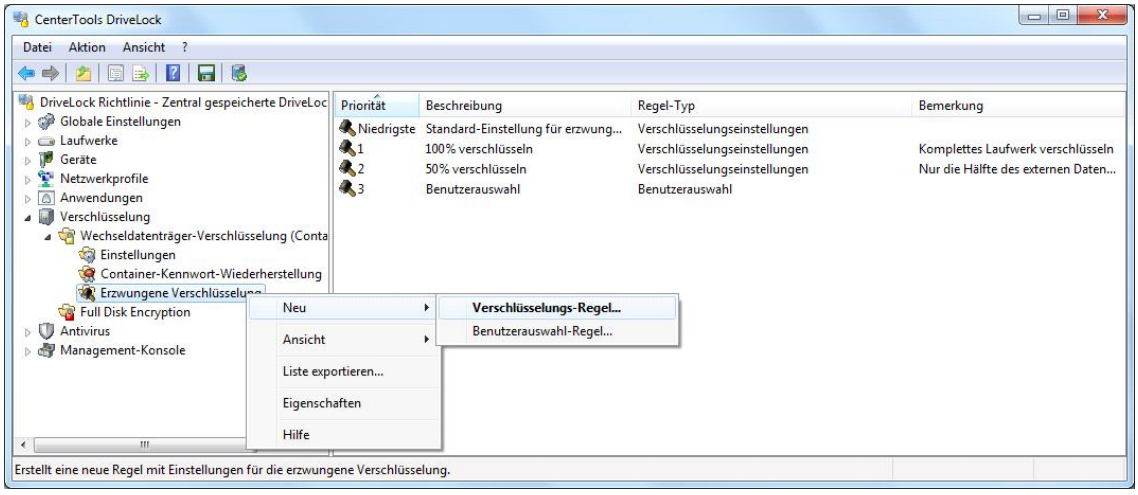


Die folgenden weiteren Einstellungen sind verfügbar:

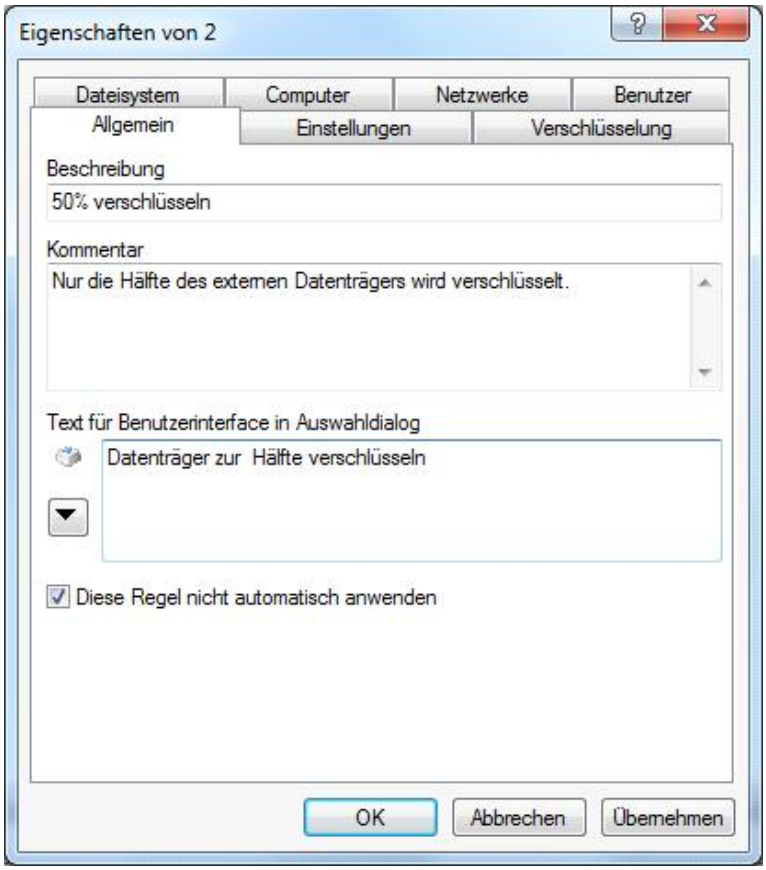
- *Bestehende Daten erhalten:* Wählen Sie diese Option, wenn DriveLock alle unverschlüsselten Dateien erhalten und mit verschlüsseln soll. Dazu wird ein temporäres Verzeichnis (Standardmäßig im Benutzerprofil von Windows) erstellt, der verschlüsselte Container dort erzeugt, die vorhandenen Daten vom Laufwerk dort hinein kopiert und zum Schluss der Container komplett auf den Wechseldatenträger verschoben. Sie können auch festlegen, dass dieses temporäre Verzeichnis an einem von Ihnen festgelegtem Platz erstellt wird (Option „**Speziellen temporären Ordner während dem Anlegen verwenden**“).
- *Mobile Encryption Anwendung auf unverschl. Teil kopieren:* Sie haben außerdem die Möglichkeit, festzulegen, ob die Mobile Encryption Anwendung auf Wechseldatenträger während der automatischen Verschlüsselung kopiert werden soll. Dies ermöglicht die Nutzung auch auf Rechnern, auf denen DriveLock nicht installiert ist. Zusätzlich kann eine **Autorun.inf** Datei mit angelegt werden, worin auch benutzerspezifische Inhalte konfiguriert werden können.
- *Speziellen temporären Ordner während dem Anlegen verwenden:* Sollen vorhandene Daten auf dem Stick übernommen werden, so können Sie hier ein Verzeichnis angeben, in dem das Verzeichnis mit dem temporären Container angelegt werden soll.
- *Verschlüsselte Containerdatei verstecken:* Wenn diese Option aktiviert ist, wird die Datei *EEDATA.DLV* als „Versteckt“ markiert.

Klicken Sie **OK**, um die Einstellungen zu übernehmen.

7.2.2.3.2 Mehrere Verschlüsselungs-Regeln anlegen



Rechtsklicken Sie auf **Erzwungene Verschlüsselung** und wählen **Neu -> Verschlüsselungs-Regel** aus dem Kontextmenü, um eine weitere Einstellungsregel zu erzeugen.

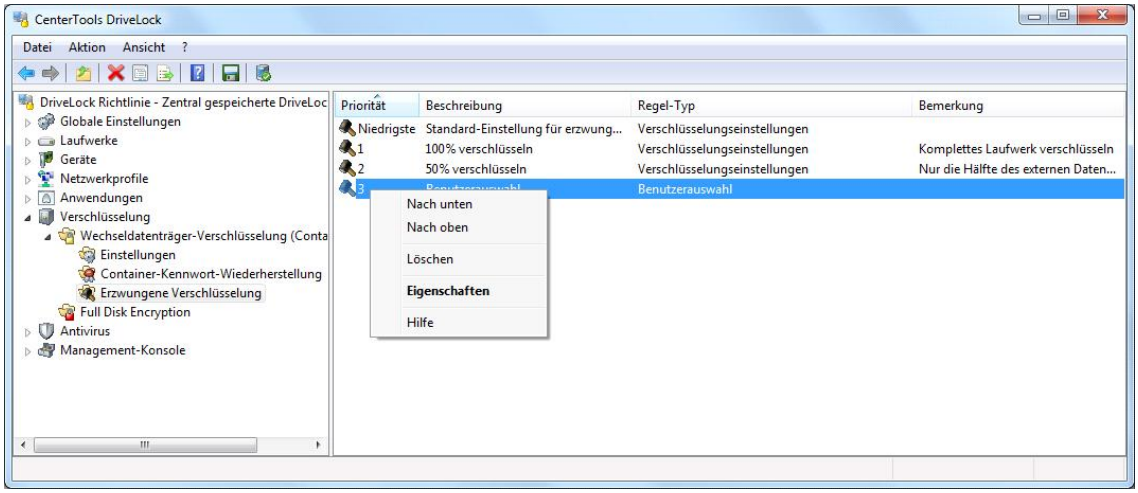


Bei den Reitern **Einstellungen**, **Verschlüsselung** und **Dateisystem** legen Sie die gleichen Parameter wie bei den Standard-Einstellungen fest.

Über Einstellungen auf den Reitern **Computer**, **Netzwerke** und **Benutzer** können Sie nun festlegen, für welche der gleichnamigen Bereiche diese Verschlüsselungs-Regel verwendet werden soll. Die Funktionsweise ist dabei die gleiche wie auch an vielen anderen Stellen bei DriveLock (z.B. bei Laufwerks-Regeln) und wird daher hier nicht detaillierter beschrieben. Dadurch können Sie z.B. für unterschiedliche Benutzergruppen verschiedene Optionen zur automatischen Verschlüsselung konfigurieren.

Klicken Sie auf **OK**, um die getroffenen Einstellungen zu übernehmen. Die neue Einstellungsregel wird anschließend in der Detailansicht rechts angezeigt.

Die erste zusätzliche Regel erhält dabei die Priorität 1, jede weitere eine um eins erhöhte Priorität als die höchste vorhandene.

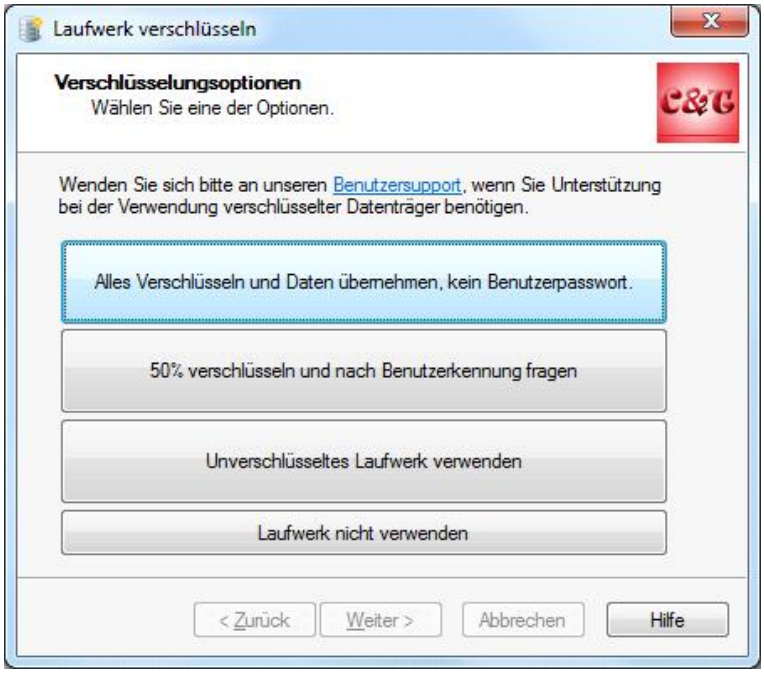


Rechts-klicken Sie auf einen Eintrag und wählen Sie **Nach unten** oder **Nach oben**, um die Reihenfolge der Priorisierung anzupassen. Über **Löschen** können Sie eine vorhandene Regel löschen.

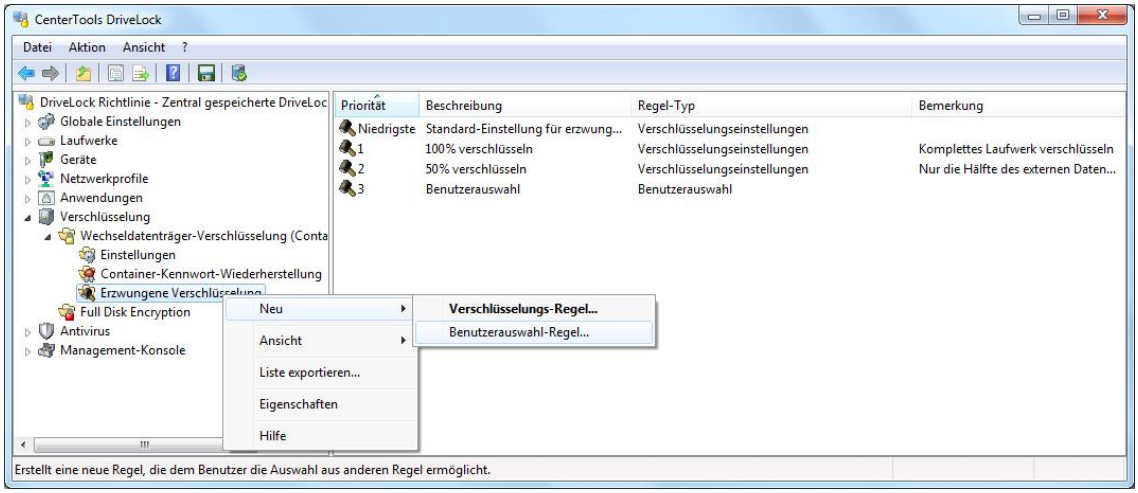
7.2.2.3.3 Eine Benutzerauswahl definieren

Eine Benutzerauswahl legt fest, welche Verschlüsselungs- bzw. Verwendungsoptionen ein Benutzerauswahldialog enthält, wenn er dem Benutzer nach dem Verbinden eines Laufwerkes angezeigt wird.

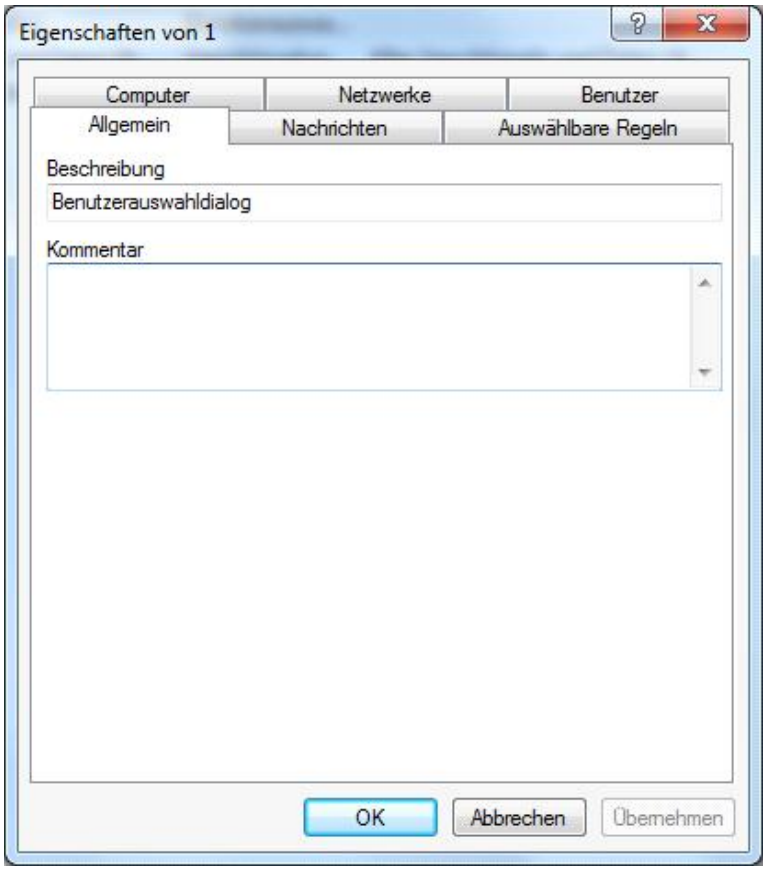
Ein derartiger Dialog kann zum Beispiel wie folgt aussehen:



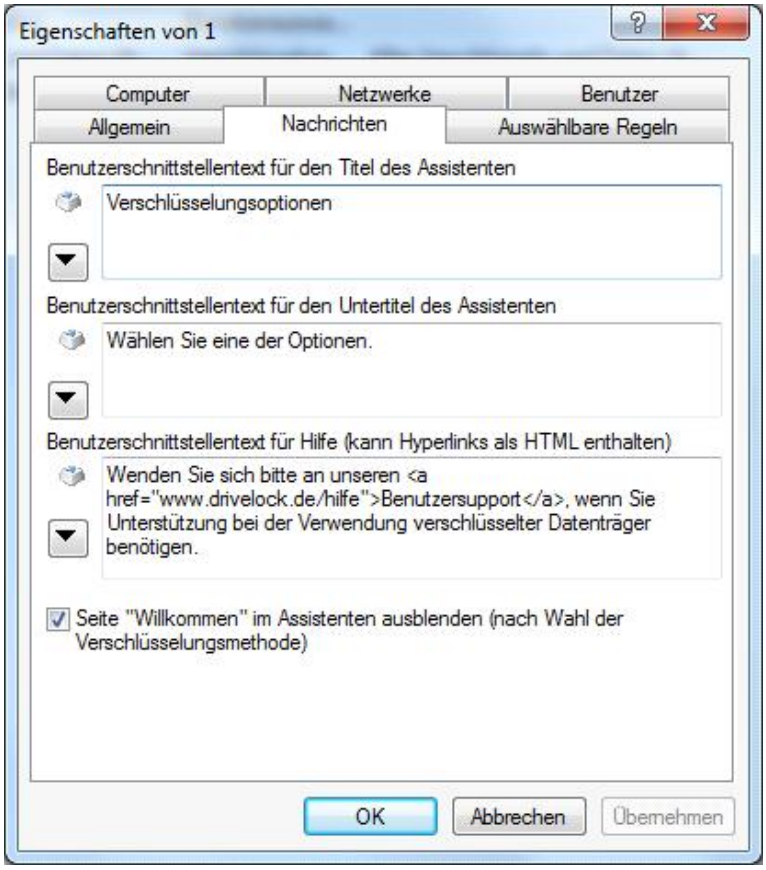
Im Folgenden wird dieser Benutzerdialog konfiguriert.



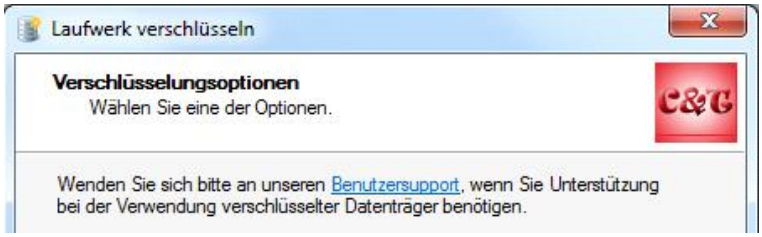
Rechtsklicken Sie auf **Erzwungene Verschlüsselung** und wählen **Neu: Benutzerauswahl-Regel** aus dem Kontextmenü, um eine Benutzerauswahl zu erzeugen.



Geben Sie eine Beschreibung und einen Kommentar (optional) ein. Wählen Sie nun den Reiter **Nachrichten**.



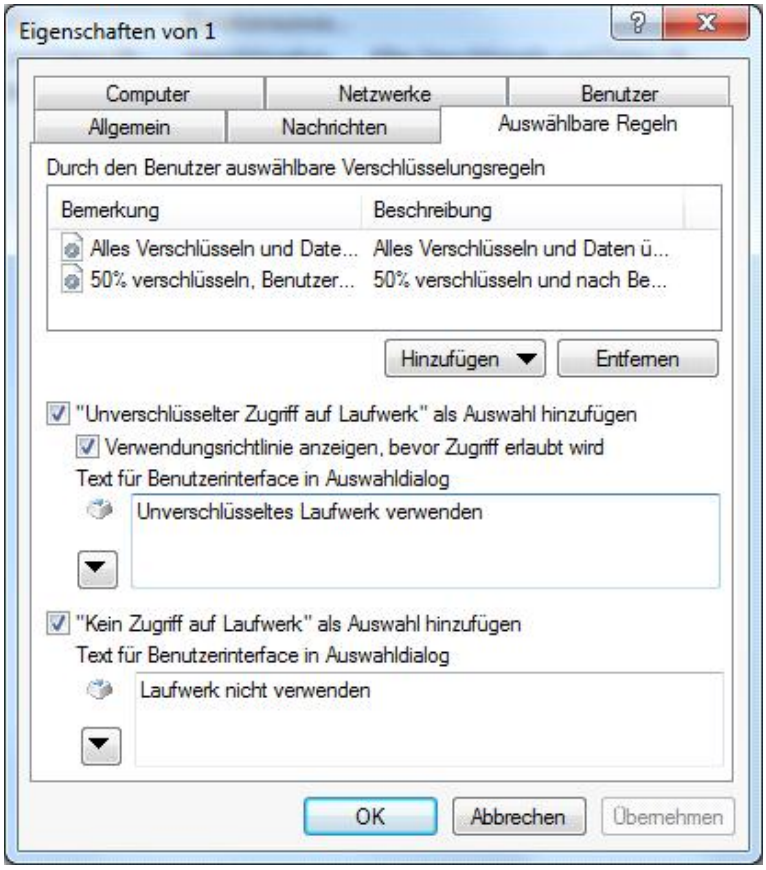
Hier werden die oberen drei Elemente Titel, Untertitel und Hilfetext konfiguriert:



Alle drei Texte können entweder wie angezeigt direkt eingegeben oder als zuvor definierte mehrsprachige Benutzernachricht durch einen Klick auf das Symbol ausgewählt werden.

Aktivieren Sie die Option „**Seite „Willkommen“ im Assistenten ausblenden…**“, um die Anzeige der Willkommensseite zu unterdrücken, wenn die vom Benutzer ausgewählte Option den Assistenten zur Verschlüsselung startet.

Zur Konfiguration der Auswahloptionen wählen Sie den Reiter **Auswählbare Regeln**.



Im oberen Bereich können Sie über die Schaltfläche Hinzufügen bis zu drei vorher angelegte Verschlüsselungs-Regeln konfigurieren. Die Reihenfolge, in der Sie die Regeln hinzufügen, bestimmt auch die Reihenfolge, wie sie im Benutzerauswahldialog angezeigt werden.

Bitte beachten Sie an dieser Stelle, dass neben der untersten im Beispiel aktivierten Option maximal drei weitere Auswahloptionen konfiguriert werden können. D.h. wenn die Option *„„Unverschlüsselter Zugriff auf Laufwerk“ als Auswahl hinzufügen*“ gewählt wurde, können Sie selbst maximal noch zwei weitere Verschlüsselungsregeln oben hinzufügen, da diese Option als dritte Auswahloption zählt.

Haben Sie die Option „„**Unverschlüsselter Zugriff auf Laufwerk“ als Auswahl hinzufügen**“ aktiviert und der Benutzer wählt diese Auswahloption aus, erhält der angemeldete Benutzer Lese- und Schreibzugriff auf das Laufwerk, auch wenn in der Laufwerksregel selbst der Zugriff als generell überhaupt nicht oder als nur lesender Zugriff konfiguriert wurde. Aktivieren Sie die Option „**Verwendungsrichtlinie anzeigen, bevor Zugriff erlaub wird**“, um nach Auswahl dieser Alternative durch den Benutzer vor der Freischaltung noch eine Verwendungsrichtlinie anzuzeigen.

Im Gegensatz dazu stellt die letzte Option „„**Kein Zugriff auf Laufwerk“ als Auswahl hinzufügen**“ quasi die „Abbrechen“-Schaltfläche dar. Wählt der Benutzer diese Auswahloption, wird das Laufwerk entsprechend den Zugriffsberechtigungen, die in der Laufwerks-Whitelist-Regel konfiguriert wurden, verbunden. Die gleichen Berechtigungen werden auch verwendet, wenn der Benutzer einen der Verschlüsselungs-Assistenten vorzeitig beendet.ie gleichen Berechtigungen werden auch verwendet, wenn der Benutzer einen der Verschlüsselungs-Assistenten vorzeitig beendet.

Über Einstellungen auf den Reitern **Computer**, **Netzwerke** und **Benutzer** können Sie nun festlegen, für welche der gleichnamigen Bereiche diese Benutzerauswahl verwendet werden soll. Die Funktionsweise ist dabei die gleiche wie auch an vielen anderen Stellen bei DriveLock (z.B. bei Laufwerks-Regeln) und wird daher hier nicht detaillierter beschrieben. Dadurch können Sie z.B. für unterschiedliche Benutzergruppen verschiedene Dialoge konfigurieren.

Klicken Sie auf **OK**, um die getroffenen Einstellungen zu übernehmen. Die neue Regel wird anschließend in der Detailansicht rechts angezeigt.

Rechts-klicken Sie auf einen Eintrag und wählen Sie **Nach unten** oder **Nach oben**, um die Reihenfolge der Priorisierung anzupassen. Über **Löschen** können Sie eine vorhandene Benutzerauswahl löschen.

Stellen Sie sicher, dass sich eine Benutzerauswahl in der Reihenfolge (Priorität) immer über der ersten Verschlüsselungs-Regel befindet (= niedrigere Nummer).

Möchten Sie im Benutzerauswahldialog ein eigenes Logo rechts oben anzeigen lassen, benötigen Sie dieses als Bitmap der Größe 48x48 Pixel. Sobald diese Datei mit dem festen Namen „DLWizardLogo.bmp“ in den Richtliniendateispeicher geladen wurde, ersetzt der DriveLock Agent das Standardlogo durch diese Grafik.

7.3 Wiederherstellung verschlüsselter Containerdateien

Für den Fall, dass ein Benutzer das Passwort für den Zugriff auf die verschlüsselten Daten vergessen hat oder dieses Passwort aus anderen Gründen nicht mehr verfügbar ist, steht neben der Verwendung der Administrator-Kennung zum Verbinden des Laufwerkes ein weiterer Wiederherstellungsmechanismus zur Verfügung. Dieser besitzt gegenüber den bisherigen Möglichkeiten zwei entscheidende Vorteile:

- Das Passwort kann auch dann zurückgesetzt werden, wenn der Computer sich aktuell nicht im Unternehmensnetzwerk befindet.
- Die Administrator-Kennung muss ggf. nicht mehr übermittelt werden bzw. die Containerdatei muss nicht zu einer Person gesendet werden, die Kenntnis von der Administrator-Kennung besitzt.

Das eingesetzte Challenge-Response-Verfahren ähnelt sehr stark dem Verfahren zur temporären Offline-Freigabe für den Zugriff auf gesperrte Laufwerke oder Geräte. Auf Seite des Benutzers steht ein Assistent zur Verfügung, der den Benutzer bei der Wiederherstellung unterstützt. Der Administrator oder ein Helpdesk-Mitarbeiter verwendet die DriveLock Management Konsole, um den angeforderten Response-Code zu erzeugen.

7.3.1 Passwort-Wiederherstellung durch den Benutzer

Die nötigen Schritte werden im DriveLock Benutzerhandbuch beschrieben.

7.3.2 Wiederherstellen verschlüsselter Laufwerke und Verzeichnisse

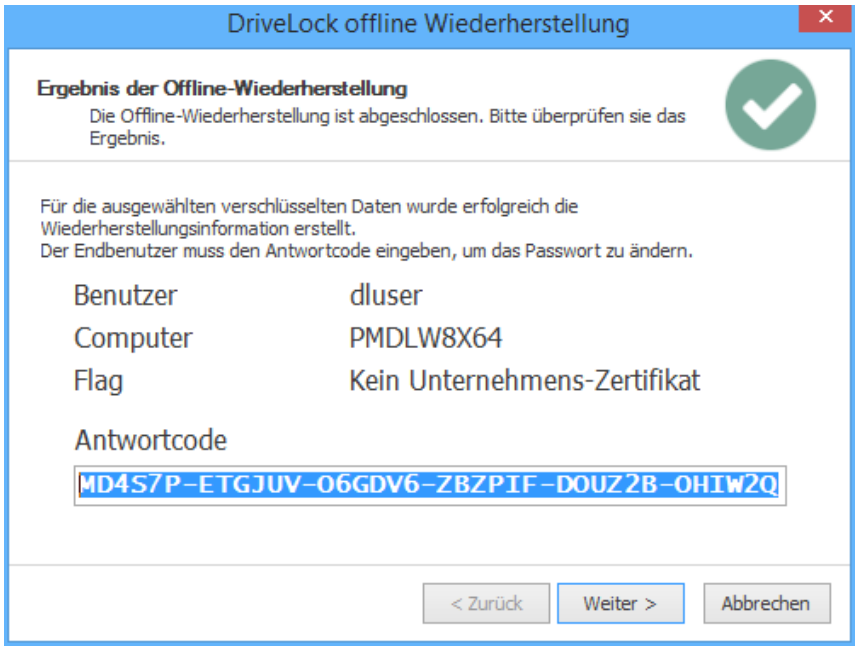
Die Offline-Wiederherstellung unterscheidet sich bei verschlüsselten Laufwerken (Containern) und Verzeichnissen für den Administrator nicht.

Um den Zugriff auf verschlüsselte Laufwerke (Container) oder Verzeichnisse wiederherzustellen, nachdem ein Passwort vergessen oder ein Zertifikat verloren ging, wird eine sogenannte Offline-Wiederherstellung mit Hilfe eines Challenge-Response Verfahrens durchgeführt. Dabei sind der Benutzer und der Administrator (oder Support-Mitarbeiter(-in)) involviert.

Das Challenge-Response Verfahren beruht auf der Überprüfung eines Anforderungscodes (Challenge) und der Generierung eines Antwortcodes (Response), welches wiederum überprüft wird. Wenn beide Codes korrekt sind, kann der Zugriff wiederhergestellt bzw. erneuert werden (z.B. durch das Vergeben eines neuen Passwortes). Der Anforderungscode wird vom Benutzer mit Hilfe eines Assistenten generiert, an den Administrator übermittelt und durch diesen auf Gültigkeit überprüft. Ist der Code in Ordnung, wird vom System ein Antwortcode generiert, durch den Administrator an den Benutzer übermittelt und durch diesen mit Hilfe des Assistenten wieder überprüft.

Um die Offline-Wiederherstellung durchzuführen, folgen Sie als Administrator / Support-Mitarbeiter(in) diesen Schritten:

1. In der *DriveLock Management Konsole (MMC)* unter **Betrieb /** Abschnitt *Verschlüsselungs-Wiederherstellung* bzw. im *DriveLock Control Center (DCC)* im Funktionsbereich **Helpdesk** öffnen Sie **Container-Kennwort-Wiederherstellung** oder **Wiederherstellung verschlüsselter Ordner**.
2. Geben Sie den *Anforderungscode* ein, der Ihnen vom Benutzer übermittelt wurde.
3. Klicken Sie auf **Weiter bzw. Suchen**. Der Anforderungscode wird nun in der DriveLock Datenbank gesucht. Bei mehr als einem Treffer wählen Sie den richtigen Ordner bzw. Container aus.
4. Geben als nächstes das Wiederherstellungszertifikat (als Zertifikatsdatei DLDlvRecover.PFX, von Smartcard oder aus dem Zertifikatsspeicher) und ggf. das korrekte Passwort an.
5. Anschließend wird der generierte Antwortcode angezeigt. Übermitteln Sie diesen Code an den Benutzer und beenden den Assistenten



Wenn Sie den privaten Schlüssel verloren haben, ist eine Wiederherstellung nicht länger möglich.

Teil VIII

DriveLock File Protection

8 DriveLock File Protection

DriveLock File Protection ist eine zentral verwaltete, transparente Dateiverschlüsselung für Verzeichnisse, welche vollständig in die DriveLock Management Konsole integriert ist.

Um die DriveLock File Protection zu verwenden, benötigen Sie eine Lizenz für alle Computer, auf denen diese Verschlüsselung zum Einsatz kommen soll.

DriveLock File Protection ist eine sogenannte File & Folder Verschlüsselung. Damit lassen sich im Gegensatz zur Container-basierten Verschlüsselung (DriveLock Encryption 2-Go) einzelne Dateien innerhalb vorher bestimmter Dateien verschlüsseln. Dabei wird der Inhalt einer Datei verschlüsselt, die Dateistruktur und der Dateiname bleiben unverändert, so dass die Datei im Windows Explorer zunächst wie eine ganz normale, unverschlüsselte Datei erscheint. Erst wenn diese Datei auf einem Computer ohne DriveLock File Protection mit dem dazugehörigen Programm (z.B. Microsoft Word) geöffnet wird, kann man die Verschlüsselung erkennen.

8.1 Wie funktioniert DriveLock File Protection?

Die Funktionsweise von DriveLock File Protection ist sehr einfach: Zunächst wird ein Verzeichnis "*verschlüsselt*", d.h. es wird als Verzeichnis markiert, in dem Dateien ausschließlich verschlüsselt abgelegt werden. Dann wird festgelegt, welcher Benutzer dieses Verzeichnis benutzen kann, d.h. für welchen Benutzer DriveLock File Protection im Hintergrund automatisch und vom Benutzer unbemerkt die Dateien beim Speichern verschlüsselt und beim Öffnen entschlüsselt.

Hinweis:
Folgende Ordner sind von der Verschlüsselung ausgeschlossen:
- das Windows-Verzeichnis, typischerweise C:\Windows
- das Verzeichnis \Program Files und \Program Files (x86)

Die Erstellung von verschlüsselten Unterordnern ist unterhalb des Benutzerverzeichnisses erlaubt,
in der Regel C:\Benutzer<Benutzername>
und in
- <Benutzername>\Desktop
- <Benutzername>\Dokumente

jedoch nicht in
- Alle Benutzer\Anwendungsdaten und <Benutzername>\Anwendungsdaten
- <Benutzername>\Start-Menü

Versucht ein Benutzer, diese Ordner zu verschlüsseln, wird eine entsprechende Fehlermeldung angezeigt: "Der gewählte Ordner kann nicht verschlüsselt werden. Diverse Systemordner können aus Gründen der Kompatibilität und Stabilität nicht verschlüsselt werden."

Auf allen Computern, auf denen DriveLock File Protection aktiv ist, wird bei jedem Zugriff auf ein Verzeichnis geprüft, ob es sich um ein markiertes (verschlüsseltes) Verzeichnis handelt. Erkennt DriveLock ein derartiges Verzeichnis, prüft es die Berechtigungen des aktuellen Benutzers und führt ggf. automatisch eine Ver- bzw. Entschlüsselung durch.

Besondere Prozesse, wie zum Beispiel die Durchführung eines Backups oder die Synchronisation von Verzeichnissen können von der automatischen Ver- bzw. Entschlüsselung ausgenommen werden. Damit wird eine Beinträchtigung bestehender Systemroutinen vermieden.

Für die Authentifizierung der Benutzer können zwei verschiedene Alternativen verwendet werden:

- *Passwort*: Für den Zugriff auf ein verschlüsseltes Verzeichnis muss ein Passwort eingeben werden
- *Zertifikat*: Die Authentifizierung erfolgt über ein im Windows Zertifikatsspeicher oder auf einer Smartcard / einem Token hinterlegtes Benutzerzertifikat

Die für eine Verwaltung von Zertifikaten üblicherweise verwendete Public-Key Infrastruktur (PKI) ist für DriveLock File Protection nicht notwendig, da DriveLock bereits alle Funktionen dafür mitbringt.

> Wenn Sie bereits über eine Active Directory PKI und Benutzerzertifikate verfügen, können Sie selbstverständlich diese für die Authentifizierung von Benutzern für DriveLock File Protection verwenden.

Sämtliche Ver- und Entschlüsselungsvorgänge erfolgen im Hintergrund, ohne dass ein Benutzer davon etwas mitbekommt. Auf neueren Systemen erfolgt dieser Vorgang durch bereits im Prozessor vorhandene Verschlüsselungsalgorithmen (AES NI), was zu einer deutlichen Verbesserung der Geschwindigkeit dabei führt (ca. 4x schneller).

Die Verwaltung verschlüsselter Verzeichnisse auf zentralen Laufwerken (z.B. Shares, NAS) erfolgt zentral über die DriveLock Management Konsole durch den IT-Administrator. Die Vergabe von Berechtigungen für die Entschlüsselung kann durch eine oder mehrere Personen der Fachabteilung (z.B. die Personalverwaltung) getrennt erfolgen. Dadurch wird zum einen der IT-Administrator von diesen zusätzlichen Aufgaben entlastet, zum anderen kann diesem Administrator auch der Zugriff entzogen werden, so dass auch er nicht in der Lage ist Dateien in diesen Verzeichnissen zu entschlüsseln.

Neben diesen sogenannten zentral verwalteten Verzeichnissen können die Benutzer auch eigene Verzeichnisse bestimmen (bzw. anlegen) und dort Dateien sicher verschlüsselt speichern (z.B. als privates lokales Verzeichnis, auf einem USB-Stick oder als Verzeichnis bei Dropbox oder einem anderen Cloud-Dienstleister). Auch hier können zusätzliche Benutzer autorisiert werden, die diese Dateien dann entschlüsseln bzw. Dateien verschlüsselt dort ablegen können.

> In diesem Handbuch wird die Verwaltung zentraler Verzeichnisse beschrieben. Das *DriveLock Benutzerhandbuch* zeigt, wie private Verzeichnisse erstellt und verwendet werden.

8.2 Unterstützte Verschlüsselungsverfahren

DriveLock File Protection unterstützt folgende Verschlüsselungsverfahren:

- *AES* (empfohlen) - Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptoverfahren, welches als Nachfolger für DES bzw. 3DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt gegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch Rijndael-Algorithmus genannt.
  DriveLock verwendet eine Schlüssellänge von 256 Bits, (AES-256), welche nach aktuellem Stand der Technik als ausreichend sicher für die Verschlüsselung vertraulicher Informationen angesehen wird.
- *Triple DES* - Symmetrisches Verschlüsselungsverfahren, das auf dem klassischen → DES basiert, jedoch mit der doppelten Schlüssellänge arbeitet (112 Bit). Die zu verschlüsselnden Daten werden mit einer dreifachen Kombination des klassischen DES verschlüsselt. Aufgrund der Schlüssellänge gilt Triple-DES derzeit noch als sicheres Verfahren im Gegensatz zum einfachen DES, der durch Brute-Force-Attacken (bloßes Probieren von Schlüsseln) angreifbar ist.
- *IDEA*: Der IDEA-Algorithmus (International Data Encryption Algorithm) wurde 1990 als ein Gemeinschaftsprojekt zwischen der ETH Zürich und der Ascom Systec AG von James L. Massey und Xueija Lai entwickelt. IDEA ist ein symmetrischer Algorithmus und gehört zu den Blockchiffren. Der Algorithmus benutzt einen 128-Bit langen Schlüssel. Bei der Verschlüsselung wird der Klartext in 64 Bit große Blöcke unterteilt und der Schlüssel in Teilstücke zu je 16 Bit zerlegt. Die Verschlüsselung geschieht durch Kombination der logischen Operation XOR, der Addition modulo 216 und der Multiplikation modulo 216+1. Die Kombination dieser drei Operationen aus unterschiedlichen algebraischen Gruppen soll ein hohes Maß an Sicherheit gewährleisten.

Mit einem Hash Algorithmus verschlüsselt DriveLock das Passwort, mit welchem das verschlüsselte Laufwerk ver- bzw. entschlüsselt wird. DriveLock unterstützt folge Hash Verfahren:

- *SHA* - Das NIST (National Institute of Standards and Technology) entwickelte zusammen mit der NSA (National Security Agency) eine zum Signieren gedachte sichere Hash-Funktion als Bestandteil des Digital Signatur Algorithms (DSA) für den Digital Signature Standard (DSS). Die Funktion wurde 1994 veröffentlicht. Diese als Secure Hash Standard (SHS) bezeichnete Norm spezifiziert den sicheren Hash-Algorithmus (SHA) mit einem Hash-Wert von 160 Bit Länge für Nachrichten mit einer Größe von bis zu 264 Bit. Der Algorithmus ähnelt im Aufbau dem von Ronald L. Rivest entwickelten MD4. Der sichere Hash-Algorithmus existiert zunächst in zwei Varianten, SHA-0 und SHA-1, die sich in der Anzahl der durchlaufenen Runden bei der Generierung des Hashwertes unterscheiden. Das NIST hat im August 2002 drei weitere Varianten („SHA-2“) des Algorithmus veröffentlicht, die größere Hash-Werte erzeugen. Es handelt sich dabei um den SHA-256, SHA-384 und SHA-512 wobei die angefügte Zahl jeweils die Länge des Hash-Werts (in Bit) angibt.
- *RIPEMD-160* - RIPEMD-160 wurde von Hans Dobbertin, Antoon Bosselaers und Bart Preneel in Europa entwickelt und 1996 erstmals publiziert. Es handelt sich dabei um eine verbesserte Version von RIPEMD, welcher wiederum auf den Design Prinzipien von MD4 basiert und in Hinsicht auf seine Stärke und Performanz dem populäreren SHA-1 gleicht. Da die Entwicklung von RIPEMD-160 offener war als die von SHA-1, ist es wahrscheinlicher, dass dieser Algorithmus weniger Sicherheitslücken aufweist.
- *WHIRLPOOL* – WHIRLPOOL ist eine kryptologische Hash-Funktion, die von Vincent Rijmen und Paulo S. L. M. Barreto entworfen wurde. Sie wurde nach der Whirlpool-Galaxie im Sternbild der Jagdhunde benannt. Whirlpool gehört zu den vom Projekt NESSIE empfohlenen kryptografischen Algorithmen und wurde von der ISO mit ISO/IEC 10118-3:2004 standardisiert.

8.3 File Protection einrichten

Bevor die DriveLock File Protection verwendet werden kann, sind einige Entscheidungen zu treffen und die daraus resultierenden Konfigurationsschritte durchzuführen.

Folgende Fragen sind dabei zu beantworten:

- Wie verwalte ich die Benutzerzertifikate für die Authentifizierung?
- Welche Einstellungen gelten für die Ver- bzw. Entschlüsselung?
- Welche Funktionen stehen dem Benutzer auf seinem Computer zur Verfügung?
- Wie soll die Verzeichnisstruktur aussehen, in dem die Daten bzw. Dateien verschlüsselt abgelegt werden?

Für die Verwaltung von Benutzerzertifikaten stehen Ihnen insbesondere die folgenden Möglichkeiten offen:

- Die Verwaltung erfolgt durch den Benutzer - ein persönliches (selbst signiertes) Zertifikat kann vom Benutzer in der DriveLock Anwendung erstellt werden.
- Die Verwaltung erfolgt durch DriveLock, die Benutzerzertifikate (öffentlicher Schlüssel) werden in der Datenbank von DriveLock gespeichert
- Benutzerzertifikate werden in einer vorhandenen PKI im Microsoft Active Directory außerhalb von DriveLock verwaltet
- Die Zertifikate der Benutzer werden in einer mit Microsoft Windows kompatiblen Umgebung außerhalb von DriveLock verwaltet.

Die Verwaltung durch DriveLock wird im Kapitel "Benutzer und Zertifikate verwalten" erklärt.

Die verschiedenen Optionen für die Ver- und Entschlüsselung und die Konfiguration der Benutzeroptionen beschreibt das Kapitel "Richtlinienkonfiguration für Clients".

Das Kapitel "Verschlüsselte Laufwerke zentral verwalten" beschreibt das Anlegen und Verwalten von zentral verwalteten Verzeichnissen.

8.3.1 Master-Zertifikat für die Schlüsselverwaltung einrichten

Bevor Sie mit Hilfe des DriveLock Enterprise Service eigene Zertifikate verwalten können, müssen Sie, ggf. pro Mandant, ein Master-Zertifikat erstellen bzw. einrichten, mit Hilfe dessen alle weiteren Benutzer-Zertifikate signiert und ausgestellt werden können.

In den Servereigenschaften legen Sie fest, ob sie das Master-Zertifikat des Mandanten **root** für alle Mandanten verwenden oder für jeden Mandanten eine eigenes Master-Zertifikat erstellen wollen.
Öffnen Sie **DriveLock Enterprise Services / Server /** Doppel-Klick **<Servername> / Optionen** und markieren Sie entsprechend **Mandantenfähiges Zertifikatsmanagement aktivieren**.

So erstellen Sie ein Master-Zertifikat für die DriveLock File Protection:

1. Öffnen Sie **DriveLock Enterprise Services / Mandanten**
   Rechts-Klick **<Mandantenname> / Alle Aufgaben / MasterZertifikat konfigurieren**.
   Sollte die Zertifikatsverwaltung noch nicht eingerichtet worden sein, erscheint ein Einrichtungsassistent.
2. Klicken Sie **Weiter**.
3. Möchten Sie ein bereits vorhandenes eigenes Zertifikat verwenden, wählen Sie die Option "*Bestehendes Master-Zertifikat verwenden*" und klicken Sie auf "...", um die Zertifkatsdatei auszuwählen. Anschließend geben Sie das Kennwort für den Zugriff auf das in der Datei enthaltene Zertifikat ein und klicken **Weiter**.
   Fahren Sie mit Schritt 5 fort.
   Möchten Sie ein neues selbst-signiertes Zertifikat erstellen, wählen Sie die Option "*Neues Master-Zertifikat erstellen*" und klicken Sie auf **Weiter**.
4. Geben Sie im folgenden Dialog die Angaben für das Zertifikat vollständig ein und klicken Sie **Weiter**.

5. Nun wird das Zertifikat in der DriveLock Datenbank gespeichert. Klicken Sie auf **Fertig stellen**, wenn das Speichern des Zertifikates erfolgreich beendet wurde. Sofern dabei ein Fehler aufgetreten ist, erhalten Sie

statt der Erfolgsmeldung einen entsprechenden Fehlerhinweis. Führen Sie in diesem Fall den Assistenten erneut aus.

Sobald Sie ein Master-Zertifikat erstellt und den Assistenten beendet haben, wird auf dem entsprechenden Server die Zertifikats- und Schlüsselverwaltung aktiviert und der DriveLock Enterprise Service neu gestartet.

8.3.2 Zertifikatsverwaltung konfigurieren

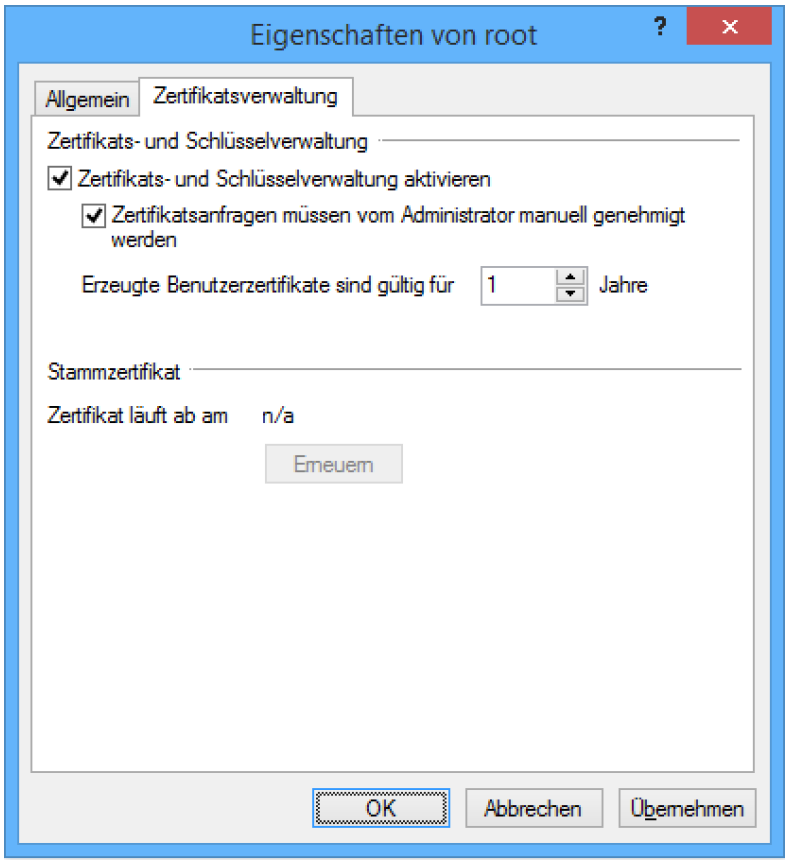
Durch die Einrichtung eines Master-Zertifikates wird die Zertifikats- und Schlüsselverwaltung des DriveLock Enterprise Services automatisch aktiviert. Sie können diese Einstellung jederzeit wieder deaktivieren bzw. aktivieren.

Ebenfalls zu den Einstellungen der Zertifikatsverwaltung gehört die Konfiguration des Systemverhaltens bei der Erzeugung und Erneuerung von Benutzerzertifikaten. Sie können hierbei zwischen den folgenden beiden Optionen wählen:

- Benutzerzertifikate werden nach dem Antrag automatisch und sofort erstellt und an den erstellenden Benutzer übertragen. (Standardeinstellung)
- Ein Administrator muss Benutzerzertifikate erst genehmigen, bevor der Benutzer das von ihm beantragte Zertifikat verwenden kann.

Um die Einstellungen der Zertifikatsverwaltung zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie **DriveLock Enterprise Services /** Doppel-Klick **<Mandantenname> / Zertifikatsverwaltung**.



2. Um die Zertifikatsverwaltung zu aktivieren, markieren Sie die Option "*Zertifikats- und Schlüsselverwaltung aktivieren*".
3. Sollen alle Benutzerzertifikate zunächst durch den Administrator geprüft und freigegeben werden, aktivieren Sie die Option "*Zertifikatsanfragen müssen vom Administrator manuell genehmigt werden*".

4. Stellen Sie die Gültigkeitsdauer der Benutzerzertifikate auf den gewünschten Wert (in Jahren) ein.
5. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

8.3.3 Richtlinienkonfiguration für Clients

Die Einstellungen für die Ver- und Entschlüsselung von Dateien und das Verhalten von DriveLock File Protection auf dem Client-Computer werden innerhalb einer DriveLock Richtlinie vorgenommen.

Verwenden Sie die DriveLock Management Konsole, um eine vorhandene Richtlinie zum Bearbeiten zu öffnen:

1. Klicken Sie im Navigationsbereich auf **Richtlinien**.
2. Rechts-klicken Sie im linken Bereich auf eine Richtlinie und wählen Sie **Bearbeiten...** .
3. Nachdem sich die Richtlinie in einem neuen Fenster geöffnet hat, klicken Sie dort im Navigationsbereich auf **Verschlüsselung -> File Protection**

Hier können Sie nun die folgenden Schritte durchführen:

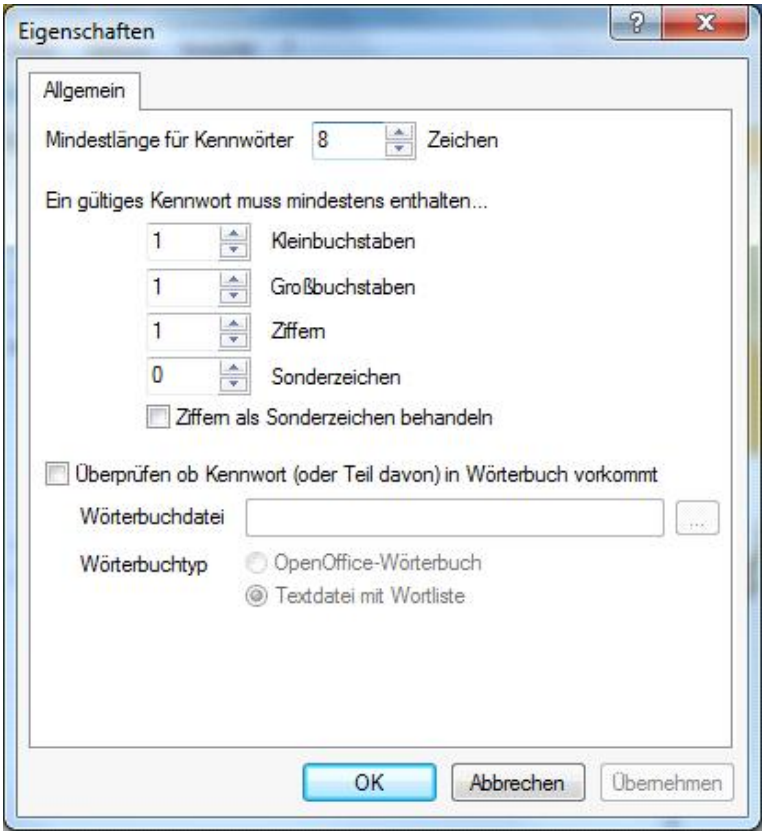
- Einstellungen zur Verschlüsselung konfigurieren
- Benutzeroberfläche der Verschlüsselung konfigurieren
- Einstellungen für verschlüsselte Laufwerke konfigurieren
- Zusätzliche Einstellungen konfigurieren
- Wiederherstellungszertifikat erzeugen
- Erzwungene Verschlüsselung verwenden

8.3.3.1 Einstellungen zur Verschlüsselung konfigurieren

Um die Verschlüsselungseinstellungen zu konfigurieren, klicken Sie im Navigationsbreich auf den Knoten **File Protection** und anschließend auf **Einstellungen**.

Um die verschiedenen Einstellungen vorzunehmen, klicken Sie auf eine der folgenden Optionen im linken Bereich:

- *Verschlüsselungsalgorithmus für verschlüsselte Ordner*: Hier legen Sie den Algorithmus fest, der für die Ver- und Entschlüsselung verwendet wird (die Algorithmen sind im Kapitel "Unterstützte Verschlüsselungsverfahren" beschrieben).
- *Hash-Algorithmus für Passwörter bei verschlüsselten Ordnern*; Hier legen Sie den Algorithmus fest, der für die Erzeugung der Passwort-Hashes verwendet wird (die Algorithmen sind im Kapitel "Unterstützte Verschlüsselungsverfahren" beschrieben).
- *Minimale Passwort-Komplexität für verschlüsselte Ordner*: Die minimal erforderliche Passwortkomplexität für verschlüsselte Laufwerke sollte so definiert werden, dass sie den Firmenrichtlinien entspricht. Die Komplexität wird auf Basis der verwendeten Zeichen sowie der Passwortlänge berechnet. Wenn Sie Ihre eigene Passwortkomplexitäts-Richtlinie erstellen möchten, wählen Sie „*Richtlinie für Passwort-Komplexität*“ aus und konfigurieren anschließen diese.
- *Richtlinie für Passwort-Komplexität*: Sofern Ihre Richtlinien es erfordern, dass Zeichen verwendet werden sollen, die sowohl eine Zahl also auch ein Sonderzeichen sein dürfen, aktivieren Sie die Option „*Ziffern als Sonderzeichen behandeln*“ und geben Sie die Anzahl der benötigten Zeichen an.



Ein Wörterbuch kann entweder ein Wörterbuch-Datei aus OpenOffice sein oder eine normale Textdatei, die pro Zeile ein Wort enthält. DriveLock wird mit OpenOffice Wörterbüchern für die vier folgenden Sprachen ausgeliefert: Englisch, Deutsch, Niederländisch und Französisch. Sie können die DIZ-Dateien in dem DriveLock Installationsordner finden, auf dem Client, auf dem die DriveLock Management Konsole installiert wurde (z.B. „*DictGerman.diz*“).

Wenn Sie die Datei aus dem Dateisystem auswählen, stellen Sie sicher, dass sich die Datei auf allen Agenten Computern an exakt der gleichen Stelle befindet, da der Agent an dem angegebenen Ort sucht.

Sie können die Datei auch dem Richtliniendateispeicher hinzufügen und wählen dazu „*Richtliniendateispeicher...*“ aus und wählen die Dateien aus dem Ort aus. Dateien im Richtliniendateispeicher werden Anhand eines Sterns („*“) am Anfang des Dateinamens identifiziert und werden automatisch auf den Client kopiert. Weitere Informationen zu dem Richtliniendateispeicher finden Sie im Kapitel "Richtliniendateispeicher verwenden".

Wenn Sie das Wörterbuch verwenden um Passwörter zu überprüfen, beachten Sie dass auch Passwörter verweigert werden, indem ein Teil des Passwortes im Wörterbuch vorkommt (z.B.: das Wörterbuch enthält „es“, Passwörter wie „Essen“, „vergessen“ oder „Sessel“ werden nicht erlaubt).

8.3.3.2 Benutzeroberfläche der Verschlüsselung konfigurieren

Um die Verschlüsselungseinstellungen zu konfigurieren, klicken Sie im Navigationsbreich auf den Knoten **File Protection** und anschließend auf **Einstellungen**.

Um die verschiedenen Einstellungen vorzunehmen, klicken Sie auf eine der folgenden Optionen im linken Bereich:

- *Verfügbare Kontext-Menüs im Windows Explorer*: Um die verfügbaren Kontextmenü-Einträge festzulegen, die ein Benutzer nach einem Rechts-Klick auf ein verschlüsseltes Verzeichnis angezeigt bekommt, klicken Sie auf

Einstellen auf festen Wert und wählen Sie aus den drei Optionen aus. Ist *Nicht konfiguriert* ausgewählt, werden alle Einträge angezeigt.

- *Konfiguration der Start-Menü-Einträge*: Um die Ebene der verfügbaren Startmenü-Einträge festzulegen, die ein Benutzer nach einem Klick auf das Windows Start-Symbol angezeigt bekommt, klicken Sie auf **Einstellen auf festen Wert** und wählen Sie aus den Optionen aus. Ist *Nicht konfiguriert* ausgewählt, werden die Einträge unter Alle Programme / DriveLock File Protection angezeigt.
- *Verfügbare Start-Menü-Einträge*: Um die verfügbaren Startmenü-Einträge festzulegen, die ein Benutzer nach einem Klick auf das Windows Start-Symbol angezeigt bekommt, klicken Sie auf **Einstellen auf festen Wert** und wählen Sie aus den Optionen aus. Ist *Nicht konfiguriert* ausgewählt, werden alle Einträge angezeigt.
- *Verfügbare Menü-Einträge beim Taskbar-Symbol*: Um die verfügbaren Tasksymbol-Menüeinträge festzulegen, die ein Benutzer nach einem Rechts-Klick auf das DriveLock Taskleisten-Symbol angezeigt bekommt, klicken Sie auf **Einstellen auf festen Wert** und wählen Sie aus den Optionen aus. Ist *Nicht konfiguriert* ausgewählt, werden alle Einträge angezeigt.
- *Reihenfolge der Menü-Einträge beim Taskbar-Symbol*: Um die Reihenfolge verfügbaren Tasksymbol-Menüeinträge festzulegen, die ein Benutzer nach einem Rechts-Klick auf das DriveLock Taskleisten-Symbol angezeigt bekommt, klicken Sie auf **Einstellen auf festen Wert**. Wählen Sie einen Eintrag aus und klicken Sie auf **Nach oben** oder **Nach unten**, um den ausgewählten Eintrag zu verschieben. Wählen Sie einen Eintrag aus und klicken Sie auf **Entfernen**, um einen Eintrag zu löschen. Um eine Trennlinie hinzuzufügen, wählen Sie einen Eintrag aus und klicken Sie auf **Hinzuf.**. Ist *Nicht konfiguriert* ausgewählt, werden alle Einträge in einer Standardreihenfolge angezeigt.
- *Endbenutzer-Kontaktinformationen für Offline-Wiederherstellung*: Um den Text festzulegen, die ein Benutzer nach einem Rechts-Klick auf das DriveLock Taskleisten-Symbo und der Auswahl der Option "*Verschlüsselten Ordner wiederherstellen*" angezeigt bekommt, klicken Sie auf **Einstellen auf festen Wert** und geben Sie den gewünschten Text in das Textfeld ein. Ist *Nicht konfiguriert* ausgewählt, wird kein Text angezeigt.
- *Format von Benutzeranzeigenamen*: Um das Format der Benutzerliste festzulegen, die ein Benutzer bei der Verwaltung berechtigter Benutzer angezeigt bekommt, klicken Sie auf **Einstellen auf festen Wert** und wählen Sie aus den Optionen aus. Ist *Nicht konfiguriert* ausgewählt, werden die Benutzer im Format *[Nachname], [Vorname]* angezeigt.
- *Keine Nachrichten für automatisch verbundene verschlüsselte Ordner anzeigen*: Um die Anzeige von Popup-Meldungen durch DriveLock beim automatischen Verbinden verschlüsselter Laufwerke zu unterdrücken, aktivieren Sie die Option *Aktiviert*. Ist *Nicht konfiguriert* oder *Deaktiviert* ausgewählt, werden Popup-Fenster angezeigt.
- *Optionen zum Speichern von Kennwörtern verschlüsselter Ordner*: Hier stellen Sie ein, ob und wie Benutzer ihr Kennwort beim Öffnen verschlüsselter Ordner speichern dürfen. Sie können *Speichern verbieten, zulassen* oder *nur für die aktive Sitzung zulassen*. Wenn Sie für *aktive Sitzung* auswählen, wird das Passwort gelöscht, sobald sich der Benutzer abmeldet, gilt dafür aber für alle verschlüsselten Ordner, die mit dem selben Passwort geschützt sind. Damit erleichtern Sie Anwendern das Arbeiten mit mehreren verschlüsselten Ordner bei trotzdem hoher Sicherheit.

8.3.3.3 Einstellungen für verschlüsselte Laufwerke konfigurieren

Um die Verschlüsselungseinstellungen zu konfigurieren, klicken Sie im Navigationsbereich auf den Knoten **File Protection** und anschließend auf **Einstellungen**.

Um die verschiedenen Einstellungen vorzunehmen, klicken Sie auf eine der folgenden Optionen im linken Bereich:

- *Verfügbare Wiederherstellungsverfahren für verschlüsselte Ordner*: Um festzulegen welche Wiederherstellungsoptionen einem Benutzer zur Verfügung stehen, klicken Sie auf **Einstellen auf festen Wert** und wählen Sie aus den Optionen aus. Ist *Nicht konfiguriert* ausgewählt, werden alle Optionen angezeigt.
- *Intervall zwischen Überprüfungen auf Zertifikatswiederruf*: Um den Zeitraum festzulegen, innerhalb dessen keine erneute Überprüfung des Benutzerzertifikates auf einen erfolgten Rückruf desselben erfolgt, klicken Sie auf **Einstellen auf festen Wert** und wählen Sie aus den Optionen aus. Ist *Nicht konfiguriert* ausgewählt, beträgt das Intervall 24 Stunden.
- *Zugriff auf Dateien in verschlüsselten Ordnern*: Um festzulegen, wie sich DriveLock File Protection verhalten soll, wenn ein Benutzer keine Berechtigung zur Ver-/Entschlüsselung hat, klicken Sie auf **Einstellen auf festen Wert** und wählen Sie aus den Optionen aus. Ist *Nicht konfiguriert* ausgewählt, wird der Zugriff auf das Verzeichnis verweigert. Folgende Optionen stehen zur Auswahl und verhalten sich wie folgt:
  - *Verweigern*: Benutzer ohne Berechtigungen können nicht auf das Verzeichnis zugreifen, auch wenn Sie entsprechende Windows-Berechtigungen hätten. Er erscheint die Windows-Meldung "*Zugriff verweigert*".
  - *Erlauben für Administratoren*: Benutzer ohne Berechtigungen können nur darauf zugreifen, wenn Sie der Gruppe der Administratoren

Wird der Zugriff ohne Berechtigungen ermöglicht, verhält sich das Verzeichnis wie ein ganz normales Windows-Verzeichnis, d.h. Dateien werden beim Öffnen nicht entschlüsselt, beim Schreiben aber auch nicht verschlüsselt. Bei berechtigten Benutzern geht DriveLock File Protection aber innerhalb eines verschlüsselten Verzeichnisses immer von einer verschlüsselten Datei aus und würde auch eine unverschlüsselte Datei entschlüsseln, was dazu führt, dass ein berechtigter Benutzer mit dieser Datei nichts anfangen kann und diese ggf. beim Schreiben komplett unbrauchbar macht.

- *Automatisches Verbinden von verschlüsselten Ordnern*: Um festzulegen, wie sich DriveLock File Protection beim Verbinden verschlüsselter Laufwerke verhalten soll, klicken Sie auf **Einstellen auf festen Wert** und wählen Sie aus den Optionen aus. Ist *Nicht konfiguriert* ausgewählt, gilt die Option *An (Dialog bei Bedarf anzeigen)*. Folgende Optionen stehen zur Auswahl und verhalten sich wie folgt:
  - *An (Dialog bei Bedarf anzeigen)*: DriveLock File Protection versucht, den Ordner mit Hilfe des im Zertifikatsspeicher vorhandenen Benutzerzertifikats oder mit einem zuvor gespeicherten Passwort zu verbinden. Hat der Benutzer keine Berechtigung oder stimmt das Passwort nicht, öffnet sich ein Fenster und der Benutzer kann eine Authentisierungsmethode auswählen. Diese Option ist sinnvoll, wenn Passwörter nicht gespeichert werden dürfen, oder Benutzerzertifikate nicht im Zertifikatsspeicher von Windows sondern auf externen Medien wie z.B. Smartcards oder Token gespeichert sind.
  - *Nur vollautomatisch, keine Dialoge anzeigen*: DriveLock File Protection versucht, den Ordner mit Hilfe des im Zertifikatsspeicher vorhandenen Benutzerzertifikats oder mit einem zuvor gespeicherten Passwort zu verbinden. Hat der Benutzer keine Berechtigung oder stimmt das Passwort nicht, wird der Benutzer als nicht berechtigt angesehen.
  - *Aus*: Es erfolgt keine automatische Verbindung mit einem verschlüsselten Verzeichnis. Der Benutzer wird solang als unberechtigter Benutzer angesehen, bis er einen Rechts-Klick auf das Verzeichnis durchführt und den Menüeintrag *Verschlüsselten Ordner verbinden* auswählt.

8.3.3.4 Zusätzliche Einstellungen konfigurieren

Um die Verschlüsselungseinstellungen zu konfigurieren, klicken Sie im Navigationsbreich auf den Knoten **File Protection** und anschließend auf **Einstellungen**.

Um die verschiedenen Einstellungen vorzunehmen, klicken Sie auf eine der folgenden Optionen im linken Bereich:

- *Dateien und Ordner, die von der automatischen Verbindung ausgenommen sind*: Um Verzeichnisse festzulegen, bei denen DriveLock keinen Versuch einer automatischen Verbindung unternehmen soll, klicken Sie auf **Einstellen auf feste Liste** und bearbeiten Sie die Liste der gewünschten Verzeichnisse oder Dateien mit Hilfe der Schaltflächen **Hinzufügen**, **Löschen** und **Bearbeiten**.
- *Namen von Backup-Programmen (mit Zugriff nur auf verschlüsselte Dateien)*: Um Programme festzulegen, welche auch ohne Berechtigung Zugriff auf verschlüsselte Verzeichnisse haben müssen, klicken Sie auf **Einstellen auf feste Liste** und bearbeiten Sie die Liste der gewünschten Programme mit Hilfe der Schaltflächen **Hinzufügen**, **Löschen** und **Bearbeiten**. Geben Sie dabei den kompletten Programmnamen ohne Pfad an, (z.B. *backup.exe*). Standardmäßig werden bereits die Programme von Dropbox, OneDrive und Google Drive berücksichtigt.

> - Lange Dateinamen werden vom Treiber nicht unterstützt um Backup-Programme zu erkennen. Geben sie stattdessen dier ersten sieben Zeichen an, z.B. BACKUP.EXE (echter 8.3 Dateiname) aber MYBACKU für MyBackupBackupAndRestore.exe.

8.3.3.5 Erzwungene Verschlüsselung

Für die erzwungene Verschlüsselung von externen Datenträgern können Sie statt der Container Verschlüsselung (siehe DriveLock Encryption 2-Go) auch die Dateiverschlüsselung verwenden. Bei großen Datenträgern beschleunigt das die Initialisierung deutlich, weil nicht erst ein Container angelegt werden muss, sondern nur die zu kopierenden Dateien verschlüsselt werden. Außerdem können sie so mehrere Ordner mit unterschiedlichen Berechtigungen anlegen lassen, z.B. einen Ordner mit Unternehmenszertifikat, auf den alle Zertifikatsinhaber transparent zugreifen können, einen Ordner mit Benutzername und Passwort nur für den Besitzer und einen Ordner für unverschlüsselte Daten.

Erzwungene Verschlüsselung mit DriveLock File Protection verwenden

1. Aktivieren sie die erzwungene Verschlüsselung mit *DriveLock File Protection* in der Richtlinie unter:
   Verschlüsselung/ Einstellungen / Methode für die erzwungene Verschlüsselung
   Selektieren Sie **DriveLock File Protection**. Damit wird für alle neuen unverschlüsselten Laufwerke, für die in einer Regel die erzwungene Verschlüsselung aktiviert ist, die Datei- und Ordner basierte Verschlüsselung verwendet. Wollen Sie ihre Benutzer zwischen Container-basierte oder die Datei- und Order basierte Verschlüsselung auswählen lassen. Markieren Sie **Entscheidung durch den Benutzer.**
2. Konfigurieren Sie die Verschlüsselungseinstellungen unter **Erzwungenen Verschlüsselung**.
   Legen Sie mit **Rechte Maus Klick / Neu** eine oder ggf. mehrere neue Verschlüsselungsregeln an für unterschiedliche Benutzergruppen an.
   a. Im Konfigurationsdialog für die Regel erstellen Sie unter *Allgemein* eine kurze Beschreibung für die Regel.
   b. Im Reiter **Dateisystem** konfigurieren Sie, ob **bestehende Daten erhalten** bleiben sollen und in den konfigurierten Ordner verschoben/verschlüsselt werden sollen und legen fest ob die **Mobile Encryption Anwendung** auf das Laufwerk kopiert werden soll. Wenn Sie **bestehende Daten erhalten** hier nicht auswählen, werden alle vorhandenen Daten gelöscht, bevor der Stick verschlüsselt wird.
   c. Im Reiter **Einstellungen** legen Sie die Art der Berechtigungen und der Verschlüsselung fest und vergeben einen Namen für den verschlüsselten Ordner. Unter Erweiterte Einstellungen können sie die Namen für weitere Ordner vergeben und festlegen, ob diese stattdessen bei der Initialisierung die vorhandenen unverschlüsselten Daten aufnehmen sollen.
   d. In den Reitern **Computer, Netzwerke** und **Benutzer** legen Sie fest für wen und wo die Regel gelten soll.

e. Legen Sie die Priorität fest mit der die Regel angewendet werden soll. Es wird immer die zutreffende Regel mit der höchsten Priorität verwendet.

Benutzerauswahl der Verschlüsselungsregel (Optional)

Analog erstellen Sie neue Benutzerauswahlregeln und fügen dort Verschlüsselungsregeln hinzu, wenn Anwender selbst eine geeignete Verschlüsselungsregel auswählen sollen. Hier müssen Sie die Priorität so festlegen dass die Regel vor den Verschlüsselungsregeln zur Anwendung kommt.

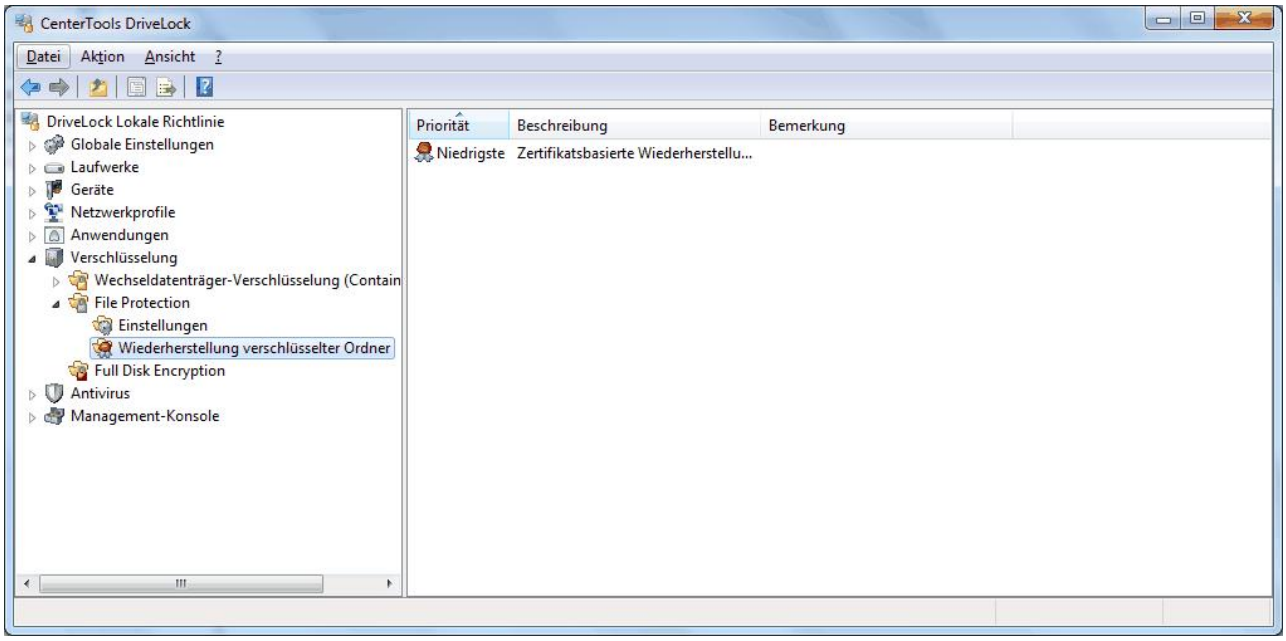
> Haben Sie **Entscheidung durch den den Benutzer** konfiguriert, erscheint zuerst der Auswahldialog für die Verschlüsselungsmethode und dann der Dialog mit den Benutzerauswahlregeln. Achten sie darauf, die in beiden Dialogen verfügbaren Optionen nur einmal zu markieren.

8.3.3.6 Einstellungen für die Wiederherstellung verschlüsselter Laufwerke konfigurieren

Damit Sie die Funktionalität der Offline-Passwort-Wiederherstellung nutzen können, müssen Sie vor der Erstellung des ersten verschlüsselten Verzeichnisses ein Hauptzertifikat bestehend aus einem öffentlichen und privaten Schlüsselpaares erzeugen. Hierzu können durchaus auch mehrere Zertifikate angelegt werden, die über Computer / Netzwerke / Benutzer gefiltert werden können. Dies ist dann sinnvoll, wenn sich der Benutzerkreis unterscheidet, die eine Wiederherstellung verschlüsselter Daten durchführen dürfen. Es sollte aber mindestens das Standard-Wiederherstellungszertifikat mit der Priorität *Niedrigste* erzeugt werden.

> Beispiel: Gerade in großen Umgebungen kann es bevorzugt werden, ein Standard-Zertifikat zu erstellen, welches für alle verwendet wird. Lediglich für den Vorstand gibt es ein eigenes Wiederherstellungszertifikat. Das Standard-Zertifikat erhält der IT-Helpdesk, damit für alle Mitarbeiter außer dem Vorstand, das Passwort von verschlüsselten Verzeichnisse zurückgesetzt werden kann. Nur der IT-Sicherheitsbeauftragte und der IT-Enterprise Administrator erhalten das Wiederherstellungszertifikat des Vorstands, damit auch hier eine Wiederherstellung möglich ist. Mit dieser Maßnahme wurde der Kreis der Personen, die potentiell Zugriff auf vertrauliche Daten haben (die des Vorstands), weiter eingeschränkt.

Um die Einstellungen für die Wiederherstellung verschlüsselter Laufwerke zu konfigurieren, klicken Sie im Navigationsbreich auf den Knoten **File Protection** und anschließend auf **Wiederherstellung verschlüsselter Ordner**.



Bei der Wiederherstellung verschlüsselter Verzeichnisse (siehe auch „Wiederherstellung verschlüsselter Verzeichnisse“) muss dann das passende Wiederherstellungs-Zertifikat ausgewählt werden, wenn Zertifikate mit mehreren Prioritäten erstellt wurden.

Wiederherstellungszertifikate werden durch das Symbol gekennzeichnet.

Standardmäßig ist zunächst ein Zertifikatseintrag vorhanden (Beschreibung **Zertifikatsbasierte Wiederherstellung**), welcher für alle verschlüsselte Verzeichnisse verwendet wird (sofern konfiguriert). Dieses Zertifikat hat die Priorität „*Niedrigste*“ und kann nicht gelöscht werden.

Um ein Standard-Wiederherstellungszertifikat zu erstellen, führen Sie folgende Schritte durch:

- Doppel-Klicken Sie auf **Zertifikatsbasierte Wiederherstellung (Priorität Niedrigste)**.
- Klicken Sie auf Zertifikatsdatei und wählen Sie „**Neu anlegen**” aus dem Drop-Down Menu aus. Dadurch wird der Assistent für die Erzeugung des Hauptzertifikates gestartet.
- Klicken Sie **Weiter**.
- Geben Sie entweder den Ordner an, wo Sie die Zertifikats-Datei abspeichern möchten oder wählen Sie alternativ eine Smartcard als Speicherort.
- Klicken auf **Weiter**.
- Sofern Sie eine Smartcard zur Speicherung verwenden, werden Sie abhängig von der verwendeten Karte nun gebeten, die Karte einzulegen und auszuwählen.

Stellen Sie sicher, dass diese Datei an einem sicheren Ort abgespeichert wird, da sie für die Passwort-Wiederherstellung dringend benötigt wird.

- Geben Sie nun das Passwort für den Zugriff auf den privaten Schlüsselbereich des Zertifikates an. Sie müssen das Passwort aus Sicherheitsgründen zweifach eingeben.
- Um Fortzufahren, klicken Sie auf **Weiter**. Es dauert einige Sekunden, um das Hauptzertifikat zu erzeugen. Anschließend werden Sie benachrichtigt, wenn der Prozess abgeschlossen ist und die Datei an dem zuvor angegebenen Ort abgespeichert wurde.

Stellen Sie sicher, dieses Passwort nicht zu vergessen. Sie sollten dieses ebenso an einem anderen sicheren Ort aufbewahren (z.B. in einem Tresor).

- Sofern eine Smartcard zur Speicherung verwendet wird, werden Sie aufgefordert, die PIN für den Zugriff auf die Smartcard einzugeben.
- Klicken Sie auf **Fertig stellen**.

Die soeben erzeugte Zertifikatsdatei wird nun angezeigt.

Sobald das Zertifikat erzeugt und der erste verschlüsselte Container erstellt wurde, darf kein neues Zertifikat mehr erstellt werden, da das alte damit überschrieben wird und somit für eine Wiederherstellung nicht mehr verwendet werden kann.

Wenn Sie auf **Eigenschaften** klicken, erhalten Sie zusätzliche Informationen über das Hauptzertifikat.

Das Zertifikat wird ebenfalls in dem privaten Zertifikatsspeichers des aktuellen Benutzers gespeichert. Der öffentliche Schlüssel des Zertifikates wird auch innerhalb des lokalen Richtliniendateispeichers abgelegt.

Wenn Sie den Erstellungs-Assistenten abgebrochen haben oder es während der Erstellung zu einem Problem gekommen ist, wird DriveLock die entsprechende Meldung anzeigen und Sie müssen das Hauptzertifikat erneut erzeugen.

Wenn Sie bisher schon ohne ein Hauptzertifikat verschlüsselte Verzeichnisse verwendet haben, ist es sinnvoll, die Option *„Wiederherstellungsinformationen zu bestehenden Ordnern hinzufügen“* zu aktivieren. In diesem Fall überprüft DriveLock jedes Mal wenn ein Verzeichnis verbunden wird, ob bereits eine Wiederherstellungsinformation vorhanden ist und erzeugt gegebenenfalls diese Information. Anschließend werden die zur Wiederherstellung nötigen Daten auch an den DriveLock Enterprise Service übertragen.

Sofern der DriveLock Enterprise Service in Ihrer Umgebung nicht verwendet wird oder Sie die Übertragung der Wiederherstellungsdaten an den DriveLock Enterprise Service nicht möchten, können Sie dieses Verhalten durch Aktivieren der Option *„Keine Offline-Wiederherstellung – Daten nicht an DES hochladen“* verhindern.

Rechtsklicken Sie auf **Wiederherstellung verschlüsselter Ordner** und wählen **Neu -> Wiederherstellungs-Regel** aus dem Kontextmenü, um ein weiteres Zertifikat zu erzeugen.

Am Anfang ist hier noch keine Zertifikatsdatei angegeben. Klicken Sie auf **Zertifikatsdatei** und wählen Sie **„Neu anlegen”** aus dem Drop-Down Menu aus.

Dadurch wird wieder der Assistent für die Erzeugung des Hauptzertifikates gestartet. Der Ablauf ist nun der gleiche wie bei der Erzeugung des Zertifikates für die niedrigste Priorität.

Über Einstellungen auf den Reitern **Computer**, **Netzwerke** und **Benutzer** können Sie nun festlegen, für welche der gleichnamigen Bereiche dieses Zertifikat verwendet werden soll. Die Funktionsweise ist dabei die gleiche wie auch an vielen anderen Stellen bei DriveLock (z.B. bei Laufwerks-Regeln, siehe Kapitel "Computer Gültigkeitsbereich", "Netzwerk Profile" und "Benutzer- und Gruppenprüfung") und wird daher hier nicht detaillierter beschrieben.

Klicken Sie auf **OK**, um die getroffenen Einstellungen zu übernehmen. Das neue Zertifikat wird anschließend in der Detailansicht rechts angezeigt.

Das erste zusätzliche Zertifikat erhält dabei die Priorität 1, jedes weitere eine um eins erhöhte Priorität als die höchste vorhandene.

Rechts-klicken Sie auf einen Eintrag und wählen Sie **Nach unten** oder **Nach oben**, um die Reihenfolge der Priorisierung anzupassen. Über **Löschen** können Sie ein vorhandenes Zertifikat löschen.

Wenn Sie ein bereits verwendetes Zertifikat löschen, ist darüber keine Wiederherstellung mehr möglich.

8.3.3.7 Unternehmenszertifikat

Verschlüsselte Ordner mit einem Unternehmenszertifikat können von jedem Anwender verbunden werden, der Zugriff auf den zugehörigen privaten Schlüssel im Windows Zertifikats-Speicher hat. In dem Fall prüfte DriveLock beim Verbinden eines verschlüsselten Ordners als erstes ob es den Ordner mit dem Unternehmenszertifikat entschlüsseln kann und der Ordner wird ohne weitere Benutzereingaben verbunden. Andernfalls wird der Benutzer nach seinen Zugangsdaten gefragt.

DriveLock erstellt die Unternehmenszertifikate nicht - Sie können den öffentlichen Schlüssel eines Zertifikat (*.cer), das Sie besitzen, hinzufügen. Den privaten Schlüssel (*.pfx) müssen Sie selbst im Windows Zertifikats-Speicher (Benutzer- oder Computerkonto) hinterlegen.

Technisch sind Unternehmenszertifikat und Wiederherstellungszertifikat sehr ähnlich und werden auf die selbe Art konfiguriert (siehe vorhergehendes Kapitel).

Unternehmenszertifikat erstellen

Um ein neues Unternehmenszertifikat in einer Richtlinie anzulegen öffnen Sie **Verschlüsselung / File Protection / Wiederherstellung verschlüsselter Ordner / Neu / Unternehmenszertifikat / Allgemein,** erstellen eine Beschreibung und importieren ein Zertifikat.

Markieren Sie **Aktiviert** um das Zertifikat beim Erstellen / Aktualisieren von Ordnern zu verwenden.

Im Reiter **Optionen** markieren Sie die gewünschte Art der Verwendung.

> Zum Ausprobieren können Sie z.B. ein Wiederherstellungszertifikat als Unternehmenszertifikat verwenden. Importieren Sie DLFfeRecovery.cer in die Richtline und DLFfeRecovery.pfx in den Windows Zertifikats-Speicher.

Unternehmenszertifikat erneuern

DriveLock kümmert sich nicht um das Ablaufdatum eines Unternehmenszertifikats, Sie können damit weiterhin verschlüsselte Ordner erstellen und verbinden. Jedoch können Sie jederzeit neue Unternehmenszertifikate zur Richtlinie hinzufügen und abgelaufenen Zertifikate aus der Richtlinie entfernen.

> Wenn Sie ein Unternehmenszertifikat aus dem Windows Zertifikats-Speicher löschen, können Sie mit diesem Schlüssel den verschlüsselten Ordner nicht mehr verbinden. Wenn das der einzige Schlüssel für den Ordner war kann eine neues Unternehmenszertifikat nicht mehr hinzugefügt werden.

8.4 Benutzer und Zertifikate verwalten

Bevor Benutzer und Zertifikate in DriveLock File Protection verwaltet werden können, müssen Sie einige Einstellungen konfigurieren. Dies wird in den Kapiteln "Master-Zertifikat für die Schlüsselverwaltung einrichten"und "Zertifikatsverwaltung konfigurieren" beschrieben.

8.4.1 Wie funktioniert die Benutzerverwaltung?

Die Benutzerverwaltung in DriveLock File Protection hilft Ihnen, ohne eine bereits vorhandene Public-Key-Infrastruktur (PKI) Benutzer und deren zugehörige Zertifikate zu verwalten.

Die integrierte Benutzerverwaltung wird nicht benötigt, wenn

- Sie bereits eine Microsoft Active Directory Umgebung haben, in denen auch Benutzerzertifikate verwaltet werden
- Sie eine andere PKI im Einsatz haben, die mit Microsoft Windows kompatibel ist
- Sie ausschließlich mit Passwörtern (nicht Windows-Passwörter) als Authentifizierung arbeiten möchten

Der große Vorteil, Benutzerzertifikate als Authentisierungshilfsmittel für die DriveLock File Protection zu verwenden, liegt darin, dass damit eine vollkommen transparente Ver- und Entschlüsselung ermöglicht wird, ein Benutzer nichts davon merkt und somit in keinster Weise in seiner üblicher Arbeitsweise beeinträchtigt wird. Bei jedem Zugriff auf ein verschlüsseltes Verzeichnis prüft DriveLock File Protection, ob im Zertifikatsspeicher des Benutzers ein Benutzerzertifikat vorhanden ist und dieses für die automatische Authentifizierung verwendet werden kann.

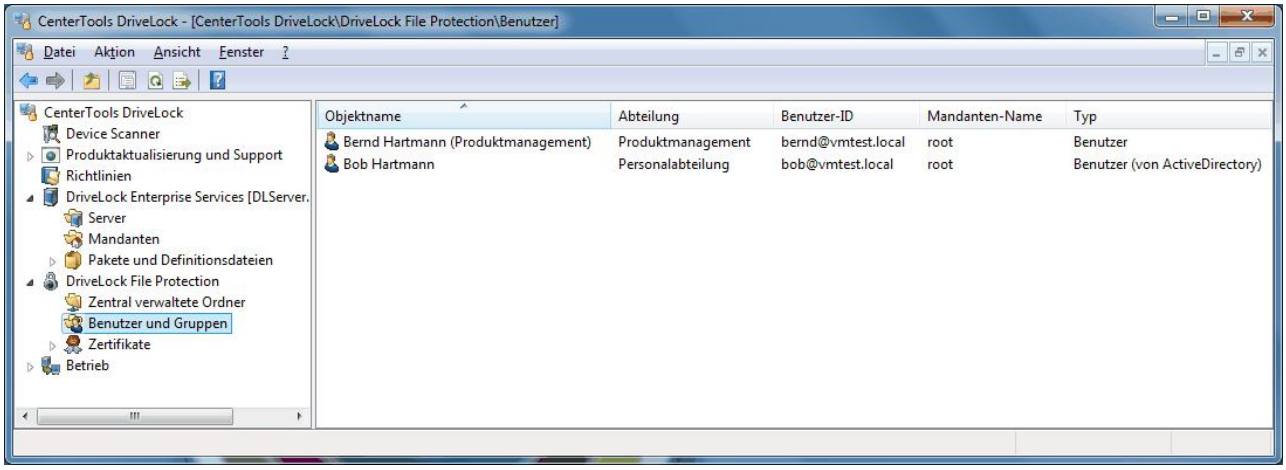
Damit Sie sich nicht mit dem Thema PKI auseinandersetzen müssen, sind alle für eine einfache, schnelle und übersichtliche Verwaltung von Benutzern und deren Zertifikate notwendigen Funktionen in DriveLock File Protection bereits integriert. Benutzer können selbst Zertifikate beantragen, beantragte Zertifikate können automatisch genehmigt, erstellt und im Benutzerzertifikatsspeicher des Betriebssystems abgelegt werden. Sie als IT-Administrator können Benutzer hinzufügen, bearbeiten und löschen, können Zertifikate ändern, zurücknehmen, löschen und aus dem Active Directory oder von Datei oder anderem Medium hinzufügen.

> Zwischen einem Benutzer und einem Zertifikat besteht in DriveLock File Protection eine enge Beziehung. So wie es keinen Benutzer ohne Zertifikat geben kann, kann es kein Zertifikat ohne einen dazu gehörenden Benutzer geben. Beide bilden also eine Einheit. Beantragt ein Benutzer ein Zertifikat, legt DriveLock automatisch auch einen entsprechenden Benutzer an. Ebenso können Sie als IT-Administrator keinen Benutzer anlegen, ohne ein passendes Zertifikat zu haben.

Die DriveLock PKI speichert und verwaltet nicht die privaten Schlüssel der Benutzerzertifikate. Anwender müssen ihr Zertifikat mit privatem Schlüssel (PFX-Datei) mit der DriveLock Anwendung aus dem Windows Zertifikatsspeicher exportieren und sicher aufbewahren. Sie müssen das Zertifikat wieder in den Windows Zertifikatsspeicher importieren um auf ihre verschlüsselten Ordner von einem anderen Computer zuzugreifen.

8.4.2 Benutzer verwalten

Die Benutzer werden mit Hilfe der DriveLock Management Konsole verwaltet. Sie gelangen zur DriveLock File Protection Benutzerverwaltung, in dem Sie im Navigationsbereich auf **DriveLock File Protection** und dann auf **Benutzer und Gruppen** klicken.



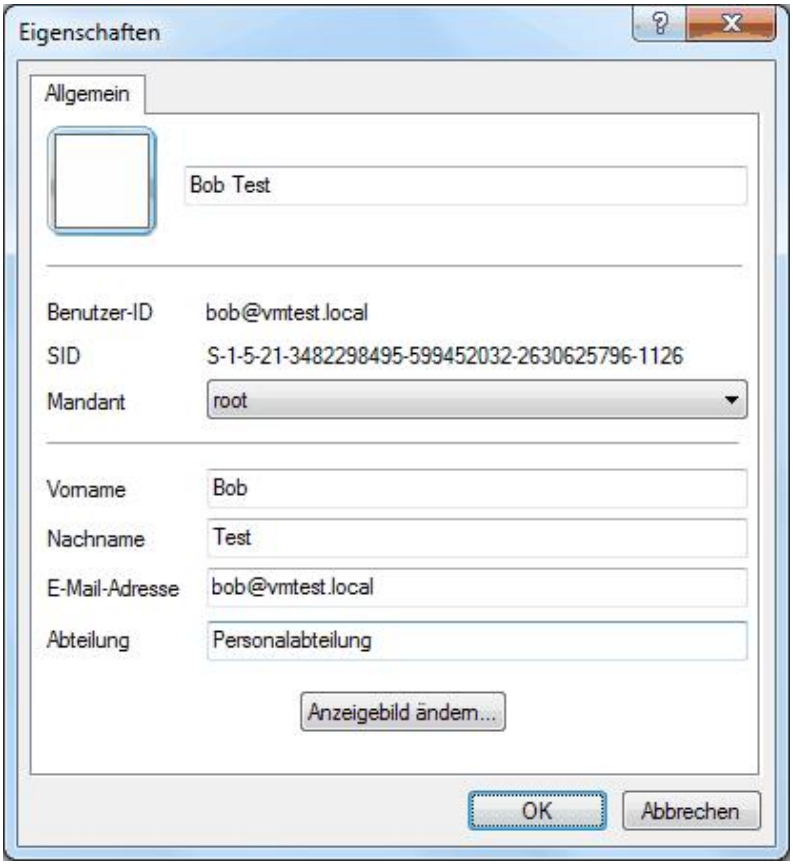
Die rechte Seite zeigt Ihnen eine Übersicht über alle in der DriveLock Datenbank gespeicherten Benutzer an.

Um die angezeigten Einträge nach einer anderen Spalte (Standard ist *Objektname*) zu sortieren, klicken Sie auf eine der Spaltenüberschriften. Um die Reihenfolge von Auf- nach Absteigend bzw. von Ab- nach Aufsteigend zu ändern, klicken Sie ein weiteres Mal auf diese Spaltenüberschrift.

Bitte beachten Sie, dass Sie als Administrator mit Hilfe dieser Benutzerverwaltung keine Zertifikate erzeugen können. Sie können hier lediglich bestehende Zertifikate einer PKI importieren, zu denen dann auch der entsprechende Benutzer angelegt wird. DriveLock File Protection Zertifikate erzeugen kann nur ein Benutzer selbst. Wie das funktioniert, ist im *DriveLock Benutzerhandbuch* beschrieben.

Um einen Benutzer mit einem vorhandenen Zertifikat anzulegen (d.h. ein Zertifikat zu importieren), führen Sie folgende Schritte durch:

- Rechts-klicken Sie auf **Benutzer** im Navigationsbereich oder auf eine leere Stelle in der Detailansicht rechts
- Im Kontextmenü klicken Sie auf **Neu** und wählen
    - *Benutzer aus Active Directory*, wenn Sie aus dem Microsoft AD einen Benutzer mit vorhandenem Zertifikat auswählen möchten. In diesem Fall erscheint der Standarddialog zu Auswahl von Objekten aus dem Active Directory und Sie können einen Benutzer auswählen.
    - *Benutzer von Zertifikat*, wenn Sie ein Zertifikat in Form eine Zertifikatsdatei (*.cer) vorliegen haben. In diesem Fall können Sie diese Zertifikatsdatei über den Dateiauswahldialog öffnen.
- Nach dem Einlesen des Zertifikates öffnet sich das Eigenschaften-Fenster des Benutzers:



- Sofern aus dem Zertifikat die Daten bereits ausgelesen werden konnten, sind die passenden Eingabefelder bereits mit diesen Werten gefüllt. Bitte tragen Sie fehlende Informationen wie z.B. E-Mail-Adresse oder Abteilung noch ein.
- *Optional*: In Umgebungen mit mehr als einem DES und verschiedenen Mandanten, kann der neue Benutzer für einen bestimmten Mandanten angelegt werden. Wählen Sie in diesem Fall aus der Dropdown-Liste Mandant den richtigen Mandant aus. Belassen Sie ansonsten diesen Eintrag unverändert.
- *Optional*: Sie können auch ein beliebiges Anzeigebild aus einer Grafikdatei hinzufügen. Da dieses Bild an verschiedenen Stellen bei der Benutzerauswahl angezeigt wird, kann es die Auswahl des richtigen Benutzers insbesondere bei gleichen Namen erleichtern. Klicken Sie dazu auf **Anzeigebild ändern** und wählen Sie eine passende Grafikdatei aus. Klicken Sie auf **Öffnen**. Konnte die Datei als Anzeigebild verwendet werden, wird dieses neue Bild nun links oben bei den Benutzereigenschaften angezeigt.
- Klicken Sie auf **OK**, um den Benutzer anzulegen und die Änderungen zu speichern. In der Detailansicht rechts wird der neue Benutzer nun angezeigt.

> Wenn ein Benutzer selbst ein Zertifikat beantragt/erstellt, wird automatisch ein entsprechender Benutzer angelegt.

Um die Eigenschaften eines Benutzers zu ändern oder anzusehen, doppel-klicken Sie auf den gewünschten Eintrag:

- Der Reiter *Verwaltete Ordner* zeigt alle zentral verwaltete Verzeichnisse, für die dieser Benutzer Berechtigungen hat.
- Der Reiter *Zertifikate* zeigt die Zertifikate, die diesem Benutzer zugeordnet und die in der Datenbank gespeichert sind.

Um einen Benutzer zu löschen, Rechts-klicken Sie auf den gewünschten Eintrag und wählen Sie **Benutzer löschen** aus dem Kontextmenü aus.

> Weitere Informationen zu zentral verwalteten Ordnern finden Sie unter "Verschlüsselte Laufwerke zentral verwalten". Die Verwaltung von Zertifikaten wird in Kapitel "Zertifikate verwalten" beschrieben.

8.4.3 Gruppen verwalten

DriveLock File Protection Gruppen sind ein Satz von DriveLock Benutzern. DriveLock Gruppen können zu zentral verwalteten verschlüsselten Ordner zugewiesen werden. Jedes mal wenn DriveLock Benutzer zu einer DriveLock Gruppe hinzugefügt oder daraus entfernt werden, passt der DriveLock Enterprise Server im Hintergrund die korrespondierenden Benutzer bei allen zentral verwalteten Ordner an, die diese DriveLock Gruppe zugeordnet haben.

> DriveLock Gruppen verhalten sich anders als Windows (AD) Gruppen. Für AD Gruppen werden die Berechtigungen zum Zugriffszeitpunkt geprüft. Da Gruppen jedoch keine Zertifikate besitzen können und sich nicht authentifizieren können, muss DriveLock die entsprechenden Benutzer einzeln den jeweiligen Ordnern zuweisen. Es kann ca. 15 Minuten dauern bis diese Zuweisung abgeschlossen ist.

Um eine neue Gruppe anzulegen rechts-klicken Sie **Benutzer und Gruppen / Neu**.

Sie können entweder eine neue DriveLock **Gruppe** anlegen und die gewünschten DriveLock Benutzer hinzufügen oder Sie importieren eine bestehende Gruppe aus dem **Group from Active Directory** (AD). Beim Import aus dem AD werden die Mitglieder der AD Gruppe unter folgenden Bedingungen zur DriveLock Gruppe hinzugefügt:

- der AD Benutzer existiert bereits als DriveLock Benutzer => der Benutzer wird einfach zur DriveLock Gruppe hinzugefügt
- der AD Benutzer besitze ein gültiges Zertifikat => ein neuer DriveLock Benutzer wird erzeugt und dann zur DriveLock Gruppe hinzugefügt
- der AD Benutzer besitzt kein gültiges Zertifikat => ein Hinweis wird angezeigt und der Benutzer wird nicht hinzugefügt

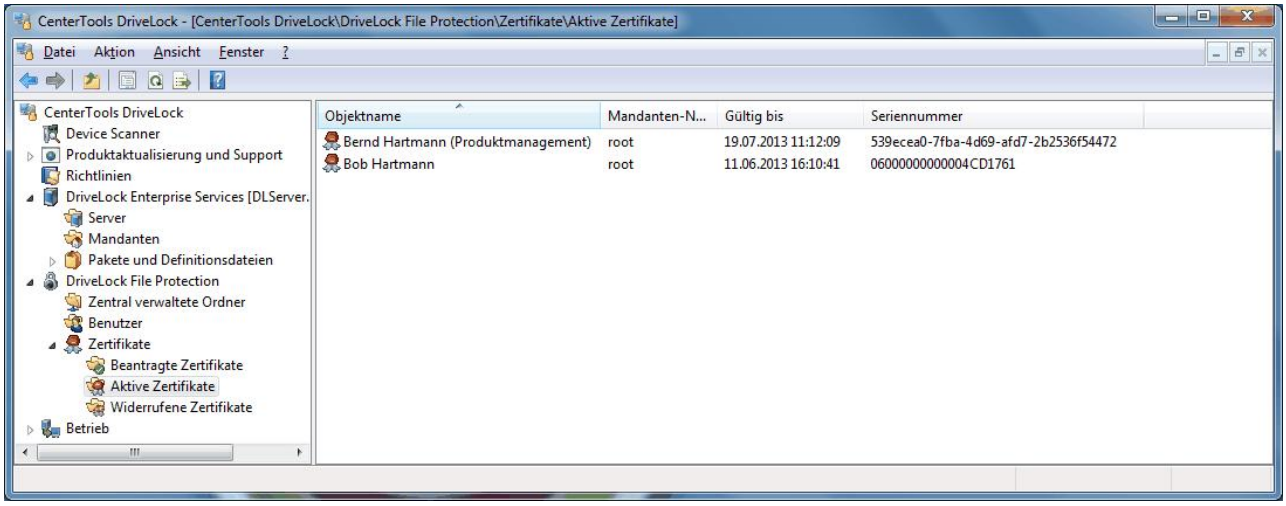
Im Eigenschaften-Dialog der neuen Gruppe können Sie nun auf dem Reiter **Allgemein** den Gruppennamen vergeben/anpassen und den richtigen Mandanten auswählen. Auf dem Reiter **Benutzer** können Sie Benutzer des Mandanten hinzufügen/anpassen. Mindestens einen Benutzer müssen Sie als **Gruppenadministrator** markieren. Mit **OK** speichern Sie die neue Gruppe.

> Sobald die Gruppe angelegt ist kann nur noch ein Gruppenadministrator mittels der DriveLock Anwendung weitere Benutzer hinzufügen und Administrator-Berechtigungen vergeben oder entziehen. Mehr dazu ist im DriveLock Benutzerhandbuch beschrieben.

Öffnen Sie den Eigenschaftendialog einer DriveLock Gruppe um Informationen zu den Gruppenmitgliedern und den zugewiesenen zentral verwalteten Ordner zu erhalten. Als DriveLock Administrator können Sie in Ausnahmefällen, falls der Gruppen-Administrator nicht verfügbar ist, Benutzer oder verwaltetet Ordern aus der Gruppe entfernen.

8.4.4 Zertifikate verwalten

Die Zertifikate werden mit Hilfe der DriveLock Management Konsole verwaltet. Sie gelangen zur DriveLock File Protection Zertifikatsverwaltung, in dem Sie im Navigationsbereich auf **DriveLock File Protection** und dann auf **Zertifikate** klicken.



Es wird zischen den folgenden drei Kategorien unterschieden:

- *Beantragte Zertifikate*: Hier sehen Sie alle Zertifikate, die durch Benutzer beantragt oder verlängert wurden und von einem Administrator (z.B. Ihnen) noch nicht bearbeitet wurden. Ein Zertifikatsantrag kann hier entweder abgelehnt oder angenommen werden.

> Die Genehmigung von Zertifikaten ist nur dann notwendig, wenn Sie in den Einstellungen des DES die entsprechende Option aktiviert haben (siehe "Zertifikatsverwaltung konfigurieren"). Ansonsten enthält diese Liste niemals Zertifikate.

- *Aktive Zertifikate*: Diese Übersicht zeigt alle derzeit aktiven Zertifikate, die in der DriveLock Datenbank gespeichert sind. Hier können Sie Zertifikate ansehen, den öffentlichen Teil exportieren und Zertifikate löschen oder widerrufen.
- *Widerrufene Zertifikate*: Diese Liste zeigt Ihnen alle Zertifikate, die widerrufen wurden. Durch den Widerruf wird ein Zertifikat als ungültig gekennzeichnet, aber noch nicht aus der Datenbank gelöscht. Hier können Sie widerrufene Zertifikate ansehen, den öffentlichen Teil exportieren und den Widerruf zurücknehmen (ein Zertifikat wird dann wieder als *aktiv* gekennzeichnet).

Klicken Sie auf eine der drei Kategorien, um sich alle zu dieser Kategorie gespeicherten Zertifikate anzeigen zu lassen.

Die rechte Seite zeigt Ihnen jeweils eine Übersicht über alle in der DriveLock Datenbank gespeicherten Zertifikate an.

Um die angezeigten Einträge nach einer anderen Spalte (Standard ist *Objektname*) zu sortieren, klicken Sie auf eine der Spaltenüberschriften. Um die Reihenfolge von Auf- nach Absteigend bzw. von Ab- nach Aufsteigend zu ändern, klicken Sie ein weiteres Mal auf diese Spaltenüberschrift.

Um Zertifikatsanträge zu bearbeiten, gehen Sie folgendermaßen vor:

- Klicken Sie auf **Beantragte Zertifikate** im Navigationsbereich.
- Rechts-klicken Sie auf den Zertifikatseintrag, den Sie bearbeiten möchten.
- Um den Antrag zu akzeptieren und das Zertifikat auszustellen, wählen Sie im Kontextmenü **Alle Aufgaben -> Antrag akzeptieren**. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird aktiviert.

  oder

- Um den gestellten Zertifikatsantrag abzulehnen und das Zertifikat nicht auszustellen, wählen Sie im Kontextmenü **Alle Aufgaben -> Antrag ablehnen**. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird gelöscht.

Um ein aktives Zertifikat zu widerrufen, führen Sie folgende Schritte aus:

- Klicken Sie auf **Aktive Zertifikate** im Navigationsbereich.
- Rechts-klicken Sie auf den Zertifikatseintrag, den Sie bearbeiten möchten.
- Wählen Sie im Kontextmenü **Alle Aufgaben -> Widerrufen...** aus.
- Wählen Sie einen Grund für den Widerruf aus der Dropdown-Liste aus.
- Optional: Geben Sie im Textfeld *Bemerkung* weitere Informationen zum Widerruf dieses Zertifikates ein.
- Klicken Sie **OK**, um das Zertifikat endgültig zu widerrufen. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird als widerrufen markiert.

oder

- Klicken Sie **Abbrechen**, um den Vorgang zu beenden und das Zertifikat nicht zu widerrufen.

Um ein widerrufenes Zertifikat erneut zu aktivieren, führen Sie folgende Schritte aus:

- Klicken Sie auf **Widerrufene Zertifikate** im Navigationsbereich.
- Rechts-klicken Sie auf den Zertifikatseintrag, den Sie bearbeiten möchten.
- Wählen Sie im Kontextmenü **Alle Aufgaben -> Widerrufen aufheben** aus.
- Klicken Sie **Ja**, um das Zertifikat endgültig zu aktivieren. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird aktiviert.

oder

- Klicken Sie **Nein**, um den Vorgang zu beenden und das Zertifikat nicht zu aktivieren.

Um ein Zertifikat zu exportieren, führen Sie folgende Schritte aus:

- Klicken Sie auf **Aktive Zertifikate** im Navigationsbereich.

oder

- Klicken Sie auf **Widerrufene Zertifikate** im Navigationsbereich.
- Rechts-klicken Sie auf den Zertifikatseintrag, den Sie exportieren möchten.
- Wählen Sie im Kontextmenü **Zertifikat exportieren...** aus.
- Wählen Sie ein Verzeichnis und einen Dateinamen, um den öffentlichen Bereich des Zertifikates in einer Datei (Endung *.cer*) zu speichern.

> Diese Zertifikatsdatei kann von einem Benutzer verwendet werden, um den im Zertifikatsbesitzer (d.h. der Benutzer von dem dieses Zertifikat generiert wurde) für ein bestimmtes privates Verzeichnis zu autorisieren. Dieser Vorgang wird im DriveLock Benutzerhandbuch beschrieben.

Um ein aktives Zertifikat zu löschen, führen Sie folgende Schritte aus:

- Klicken Sie auf **Aktive Zertifikate** im Navigationsbereich.
- Rechts-klicken Sie auf den Zertifikatseintrag, den Sie bearbeiten möchten.
- Wählen Sie im Kontextmenü **Alle Aufgaben -> Zertifikat löschen** aus.
- Klicken Sie **Ja**, um das Zertifikat endgültig zu löschen. Der Listeneintrag des Zertifikats wird entfernt, das Zertifikat wird gelöscht.

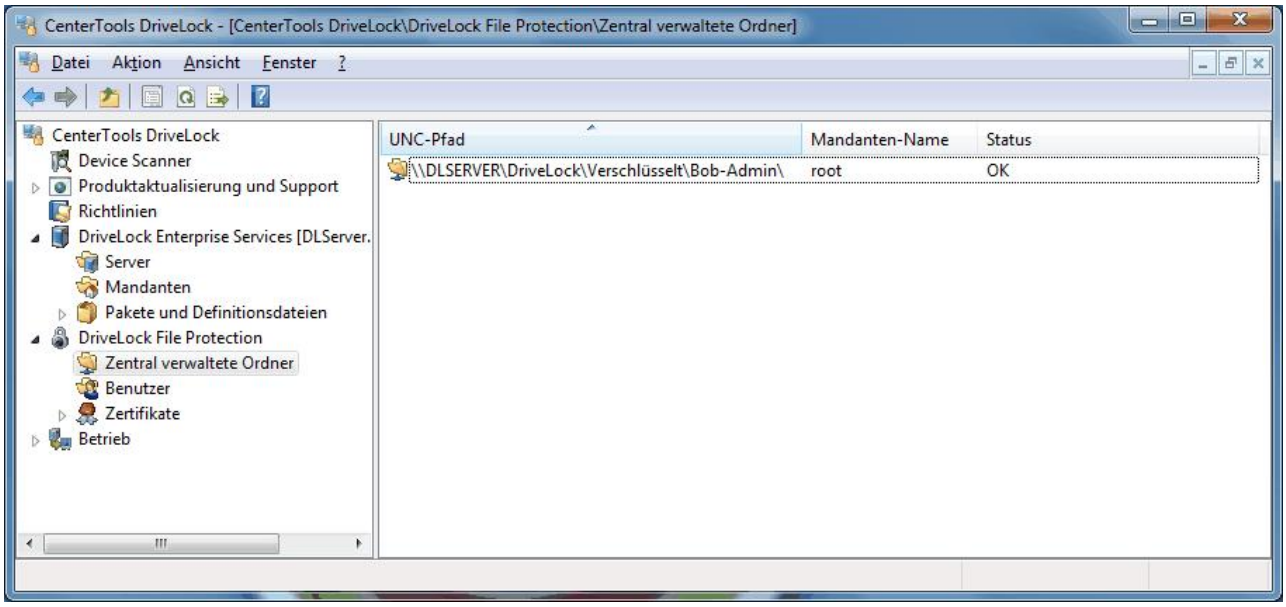
oder

- Klicken Sie **Nein**, um den Vorgang zu beenden und das Zertifikat nicht zu löschen.

Bitte beachten Sie, dass das Löschen von Zertifikaten nicht den in der Datenbank gespeicherten Benutzer löscht. Es ist jedoch nicht mehr möglich, diesen Benutzer für den Zugriff auf ein zentral verwaltetes Verzeichnis zu autorisieren. Bereits eingerichtete Berechtigungen bleiben davon unberührt, so lange der Benutzer sein Benutzerzertifikat im Zertifikatsspeicher von Windows gespeichert hat. Um bereits eingerichtete Berechtigungen unwirksam werden zu lassen, widerrufen Sie bitte das gewünschte Zertifikat.

8.5 Verschlüsselte Laufwerke zentral verwalten

Mit Hilfe der *MMC* verwalten Sie verschlüsselte Verzeichnisse an zentraler Stelle. Sie gelangen zur Verwaltung der Verzeichnisse, in dem Sie im Navigationsbereich auf **DriveLock File Protection** und dann auf **Zentral verwaltete Ordner** klicken.



Die rechte Seite zeigt Ihnen eine Übersicht über alle in der DriveLock Datenbank gespeicherten Verzeichnisse und deren Status an.

Um die angezeigten Einträge nach einer anderen Spalte (Standard ist *UNC-Pfad*) zu sortieren, klicken Sie auf eine der Spaltenüberschriften. Um die Reihenfolge von Auf- nach Absteigend bzw. von Ab- nach Aufsteigend zu ändern, klicken Sie ein weiteres Mal auf diese Spaltenüberschrift.

Hier können Sie neue Verzeichnisse anlegen und Benutzerberechtigungen einmalig einrichten, Berechtigungen bestehender Verzeichnisse ändern oder ansehen (sofern Sie als Benutzer selbst die Berechtigung als Verzeichnisadministrator haben) oder Verzeichniseinträge löschen.

Wenn Sie ein neues zentral verwaltetes Verzeichnis anlegen, beachten Sie bitte folgendes:

- Es können keine bestehenden Verzeichnisse zentral verwaltet und verschlüsselt werden. Erstens ist in den meisten Fällen auf einem Server kein DFP Dienst installiert, der für eine asynchrone Verschlüsselung sorgen könnte und zweitens können während der Zeitdauer der Initialverschlüsselung auftretende Konfliktsituationen technisch nicht ausreichend genug gelöst werden (z.B. wenn erst ein Teil der Dateien bereits verschlüsselt ist oder eine größere Datei gerade verschlüsselt wird und ein anderen Benutzer von seinem Computer aus auf diese Datei zugreift).
- Die Benutzer, die beim Anlegen des Verzeichnisses für den Zugriff autorisiert werden, erhalten Administrationsrechte für dieses Verzeichnis. Administrationsrechte erlauben es, weitere Benutzer zu berechtigen bzw. Berechtigungen zu entfernen. Somit können Sie als IT-Administrator die Verwaltung der

autorisierten Benutzer bereits beim Anlegen des Verzeichnisses an einen oder mehrere Benutzer der Fachabteilung abgeben.

8.5.1 Neues verschlüsseltes Laufwerk anlegen

Sie benötigen für das Verzeichnis bzw. das Netzlaufwerk, in dem Sie das neue verschlüsselte Verzeichnis anlegen möchten, Schreibrechte.

Um ein neues verschlüsseltes Verzeichnis anzulegen, führen Sie folgende Schritte durch:

- Rechts-klicken Sie auf **Zentral verwaltete Ordner** im Navigationsbereich oder auf eine leere Stelle in der Detailansicht rechts
- Im Kontextmenü klicken Sie auf **Neu** und wählen **Zentral verwalteter Ordner**.

- Optional: Die Einstellungen *Erzeugen für Mandant* und *Primärer Server* müssen nur angepasst werden, wenn in Ihrer Umgebung mehr als ein DES verfügbar ist und ein anderer DES als der zentrale Service verwendet werden soll, oder Sie mehr als einen Mandanten eingerichtet haben und nicht der Standard-Mandant *root* verwendet werden muss. In den meisten Fällen dürfte keine Änderung dieser Vorgaben notwendig sein.
- Geben Sie in das Textfeld Pfad des neuen zentral verwalteten Ordners den UNC-Pfad für das neue Verzeichnis an.

oder

- Klicken Sie auf die Schaltfläche "..." und wählen Sie über den Auswahldialog das gewünschte Verzeichnis aus. Klicken Sie auf **Neues Verzeichnis**, um im zuvor ausgewählten Ordner ein neues Verzeichnis anzulegen und wählen Sie dieses aus. Klicken Sie auf **OK**, um die Auswahl zu übernehmen.
- Vergewissern Sie sich, dass der nun angezeigte UNC-Pfad korrekt ist und klicken Sie **Weiter**.
- Um einen bestimmten Benutzer zu suchen, geben Sie einen Suchtext in das obere Suchfeld ein. Nachdem Sie mindestens drei Buchstaben eingegeben haben, werden automatisch nur noch in der Datenbank vorhandene aktive Benutzer angezeigt, die den Suchtext im Namen beinhalten. Alternativ können Sie **Suchen** klicken, um die Suche manuell zu starten.

- Wählen Sie nun eine oder mehrere angezeigte Benutzer aus. Diese erhalten nach der Einrichtung administrative Berechtigungen für dieses Verzeichnis.
- Klicken Sie auf **Weiter**. Der neue Ordner wird nun angelegt und die Berechtigungen eingetragen. Anschließend erhalten Sie eine Rückmeldung, ob dieser Vorgang erfolgreich abgeschlossen werden konnte.
- Klicken Sie **Fertig stellen**.

8.5.2 Zugriffsberechtigungen ändern

Die Zugriffsberechtigungen für ein verschlüsseltes Verzeichnis können entweder durch die DriveLock Benutzeroberfläche, über das Kontextmenü im Windows Explorer oder über die DriveLock Management Konsole geändert werden. Für die Änderung benötigt der durchführende Benutzer administrative Berechtigungen für dieses Verzeichnis.

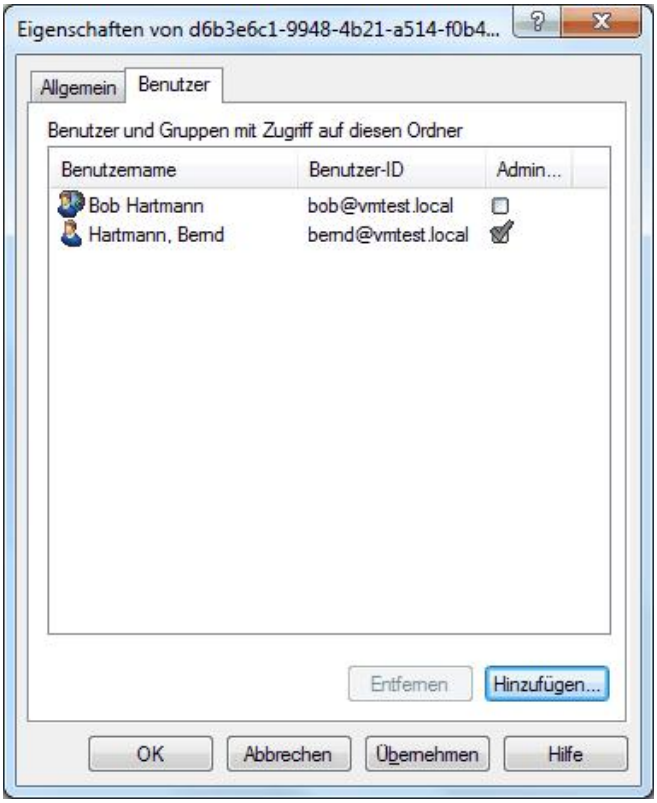
Um als Administrator über den Windows Explorer die Zugriffsberechtigungen zu ändern, rechts-klicken Sie auf das Verzeichnis und wählen Sie *Eigenschaften und Benutzer des verschlüsselten Ordners.*

Um als Administrator über die DriveLock Management Konsole die Zugriffsberechtigungen für ein bestehendes zentral verwaltetes Verzeichnis zu ändern, gehen Sie folgendermaßen vor:

- Klicken Sie auf **Zentral verwaltete Ordner** im Navigationsbereich.
- Rechts-klicken Sie auf das gewünschte Verzeichnis in der Detailansicht und wählen Sie **Ordner verwalten**.

oder

- Doppelklicken Sie auf das gewünschte Verzeichnis, wählen Sie den Reiter *Benutzer* und klicken Sie auf **Verwalten**.
- Sofern bei den Informationen *<Anmelden um Daten zu sehen>* angezeigt wird, müssen Sie sich zunächst noch Authentifizieren. Klicken Sie dazu auf **Anmelden** und wählen Sie das Zertifikat, welches für den Zugriff benötigt wird, aus.
- Wählen Sie den Reiter *Benutzer*.



- Um einen Benutzer den Zugriff zu entziehen, wählen Sie den gewünschten Benutzer aus und klicken Sie auf **Entfernen**.
- Um einen neuen Benutzer zu berechtigen, klicken Sie auf **Hinzufügen**.
- So fügen Sie einen Benutzer aus dem Windows Active Directory hinzu:
    - Aktivieren Sie die Option *Windows-Benutzer (mit Zertifikat)*.
    - Um den Benutzer auszuwählen, klicken Sie auf die Schaltfläche "..." und wählen Sie aus dem Active Directory den gewünschten Benutzer.
    - Klicken Sie auf **Fertig stellen**. Der ausgewählte Benutzer wird als normaler Benutzer (also ohne administrative Berechtigung) hinzugefügt.
- So fügen Sie einen Benutzer aus der DriveLock Datenbank hinzu:
    - Aktivieren Sie die Option *DriveLock File Protection-Benutzer (mit Zertifikat)*.
    - Klicken Sie auf **Weiter**.
    - Wählen Sie nun eine oder mehrere angezeigte Benutzer aus. Diese erhalten nach der Einrichtung normale Berechtigungen für dieses Verzeichnis.
    - Klicken Sie auf **Fertig stellen**.
- Um das Fenster zu schließen, klicken Sie **OK**.

8.6 Wiederherstellung verschlüsselter Verzeichnisse

Sie benötigen die Wiederherstellung verschlüsselter Verzeichnisse, wenn kein Benutzer mehr auf ein verschlüsseltes Verzeichnis zugreifen und die Daten entschlüsseln kann. Dies kann entweder durch den Verlust der entsprechenden Benutzerzertifikate oder das Vergessen eines Passwortes geschehen.

Um den Zugriff auf verschlüsselte Laufwerke wiederherzustellen, nachdem ein Passwort vergessen oder ein Zertifikat verloren ging, wird eine sogenannte Offline-Wiederherstellung mit Hilfe eines Challenge-Response Verfahrens durchgeführt. Dabei sind der Benutzer und der Administrator (oder Support-Mitarbeiter(-in)) involviert.

Das Challenge-Response Verfahren beruht auf der Überprüfung eines Anforderungscodes (Challenge) und der Generierung eines Antwortcodes (Response), welches wiederum überprüft wird. Wenn beide Codes korrekt sind, kann der Zugriff wiederhergestellt bzw. erneuert werden (z.B. durch das Vergeben eines neuen Passwortes). Der Anforderungscode wird vom Benutzer mit Hilfe eines Assistenten generiert, an den Administrator übermittelt und durch diesen auf Gültigkeit überprüft. Ist der Code in Ordnung, wird vom System ein Antwortcode generiert, durch den Administrator an den Benutzer übermittelt und durch diesen mit Hilfe des Assistenten wieder überprüft.

Die für die Wiederherstellung durch den Benutzer durchzuführenden Schritte werden im *DriveLock Benutzerhandbuch* beschrieben.

Die für die Wiederherstellung durch den Administrator (oder Support-Mitarbeiter(-in)) sind identisch zur Wiederherstellung verschlüsselter Laufwerke und werden in Wiederherstellen verschlüsselter Laufwerke und Verzeichnisse beschrieben.

8.7 Reporting und Analyse

Auswertungen, Berichte und Statistiken lassen sich mit Hilfe des DriveLock Control Centers durchführen. Mehr Informationen dazu finden Sie im DriveLock Control Center Handbuch.

Teil IX

Terminalserver

9 Terminalserver

DriveLock unterstützt die Verwendung auf Terminalservern. Die Module Laufwerke und Applikationen können auf einem Terminalserver verwendet werden. Da es verschiedenste Verbindungsmöglichkeiten zwischen einem Client und dem Terminalserver gibt, wird in den folgenden Kapiteln ganz spezifisch auf die unterschiedlichen Szenarien eingegangen und deren Unterschiede erklärt. Teilweise gibt es dort Einschränkungen, bei anderen wird der volle Funktionsumfang unterstützt.

9.1 Verbindungsarten

Unterstütze Funktionen je nach Verbindungsart (nur Laufwerksverbindungen):

Funktion	FAT-Clients	Windows XP/Vista/7 Embedded Client	Virtual-Clients	Linux V6 Thin-Clients des Herstellers Wyse	Thin-Clients anderer Hersteller
Berechtigungen anhand von Benutzer / Gruppen	Ja	Ja	Ja	Ja	Ja
Freigabe anhand des verbundenen Laufwerksbuchstaben	Ja	Ja	Ja	Ja	Ja
Freigaben anhand der Hardwaredaten inkl. Seriennummer	Ja	Ja	Ja	Ja	Nein
Dateisystemfilter	Ja	Ja	Ja	Ja	Ja
Dateisystemfilter inkl. Header Überprüfung	Ja	Ja	Ja	Ja	Ja
Dateiprotokollierung	Ja	Ja	Ja	Ja	Ja
Schattenkopie	Ja	Ja	Ja	Ja	Ja
Benötigt DriveLock-Agent lokal	Ja	Ja	Ja	Spezielles Plug-In für Wyse Linux V6	Nein
Benötigt DriveLock-Agent auf dem TS	Nein	Nein	Der Virtual-Client wird anstatt des Terminalservers verwendet.	Ja	Ja

Wenn die Applikationskontrolle auf dem Terminalserver verwendet werden soll, wird unabhängig von der obigen Tabelle immer der DriveLock-Agent auf dem Terminalserver benötigt.

9.1.1 FAT-Clients / Desktop-Clients

Ein FAT-Client bzw. ein Desktop-Client ist ein normaler Computer mit Windows XP oder höher. Der FAT-Client stellt eine Verbindung mit dem Terminalserver her. Der DriveLock-Agent wird bereits auf dem FAT-Client installiert, somit findet die Kontrolle genau dort statt, wo ein Gerät angeschlossen wird. Der Benutzer darf nur die Geräte in seiner Terminalserversitzung verwenden, die auch lokal durch den DriveLock-Agenten freigegeben sind.

Befinden sich die FAT-Clients in der einer Domäne, kann die Konfiguration über Gruppenrichtlinie erfolgen. Ansonsten empfehlen wir die Verwendung von zentral gespeicherten Richtlinien.

9.1.2 Windows Embedded-Clients

Ein Windows Embedded-Client ist ein spezieller Computer mit Windows XP Embedded oder höher. Der Windows Embedded-Client stellt eine Verbindung mit dem Terminalserver her. Der DriveLock-Agent wird bereits auf dem Embedded-Client installiert bzw. in das Image integriert. Somit findet die Kontrolle genau dort statt, wo ein Gerät angeschlossen wird. Der Benutzer darf nur die Geräte in seiner Terminalserversitzung verwenden, die auch lokal durch den DriveLock-Agenten freigegeben sind.

Befinden sich die Windows Embedded-Clients in der einer Domäne, kann die Konfiguration über Gruppenrichtlinie erfolgen. Ansonsten empfehlen wir die Verwendung von zentral gespeicherten Richtlinien.

9.1.3 Virtual-Clients

Ein Virtual-Client ist ein virtueller Computer mit Windows XP oder höher. Ein Thin-Client (oder jeder andere beliebige Client) stellt eine Verbindung mit dem virtuellen Computer her. Der DriveLock-Agent wird auf dem virtuellen Client installiert. Über ein USB-Mapping Treiber werden alle lokal angeschlossenen USB-Geräte in den virtuellen Computer verbunden. Der Benutzer darf nur die Geräte in seinem virtuellen Client verwenden, die dort auch durch den DriveLock-Agenten freigegeben sind.

Befinden sich die virtuellen Clients in der einer Domäne, kann die Konfiguration über Gruppenrichtlinie erfolgen. Ansonsten empfehlen wir die Verwendung von zentral gespeicherten Richtlinien.

9.1.4 Thin-Clients anderer Hersteller

Ein Thin-Client ist ein speziell abgespeckter Computer mit einem proprietären Betriebssystem. Ein Thin-Client stellt eine Verbindung mit dem Terminalserver her. Der DriveLock-Agent wird auf dem Terminalserver installiert. Der Benutzer darf nur die Geräte in seiner Terminalserversitzung verwenden, die dort auch durch den DriveLock-Agenten freigegeben sind.

Befinden sich die Terminalserver in der einer Domäne, kann die Konfiguration über Gruppenrichtlinie erfolgen. Ansonsten empfehlen wir die Verwendung von zentral gespeicherten Richtlinien.

9.1.5 Linux Thin-Clients des Herstellers Wyse

Ein Wyse Thin-Client ist ein speziell abgespeckter Computer mit einem Linux Betriebssystem. Dieser Thin-Client stellt eine Verbindung mit dem Terminalserver her. Der DriveLock-Agent wird auf dem Terminalserver installiert. Der Benutzer darf nur die Geräte in seiner Terminalserver-Sitzung verwenden, die dort auch durch den DriveLock-Agenten freigegeben sind.

Der Unterschied zu den Thin-Clients anderer Hersteller liegt im verwendeten Betriebssystem. Aktuell gibt es für Wyse Linux V6 ein zusätzliches Plug-In für den ICA-Channel, damit die Hardwaredaten von USB-Datenträgern über eine Virtual ICA-Channel-Erweiterung dem DriveLock-Agent am Terminalserver übergeben werden können. Damit ist es möglich Laufwerks-Whitelist-Regeln in vollem Umfang zu erstellen, d.h. mit Hersteller/Produkt ID + Seriennummern.

> Das Plug-In für den Wyse Linux V6 Thin-Client (nur ICA-Protokoll!) erhalten Sie auf Anfrage von unserem Support (support@drivelock.de).

Befinden sich die Terminalserver in der einer Domäne, kann die Konfiguration über Gruppenrichtlinie erfolgen. Ansonsten empfehlen wir die Verwendung von zentral gespeicherten Richtlinien.

9.2 Terminalserver-Regeln

Ist erst einmal klar, wie die Umgebung aufgebaut ist, und welche Verbindungsarten es gibt, kann man an die Konfiguration gehen. Je nach Verbindungsart findet die Konfiguration clientseitig oder serverseitig statt.

Als nächstes muss man sich ein Berechtigungskonzept überlegen. Was soll gesperrt werden und wie sehen Ausnahmen davon aus? Wie weit geht man ins Detail? Reicht eine Freigabe nach Benutzern/Gruppen, nach verbundenen Laufwerksbuchstaben, nach Hardwaredaten oder einer Kombination dessen.

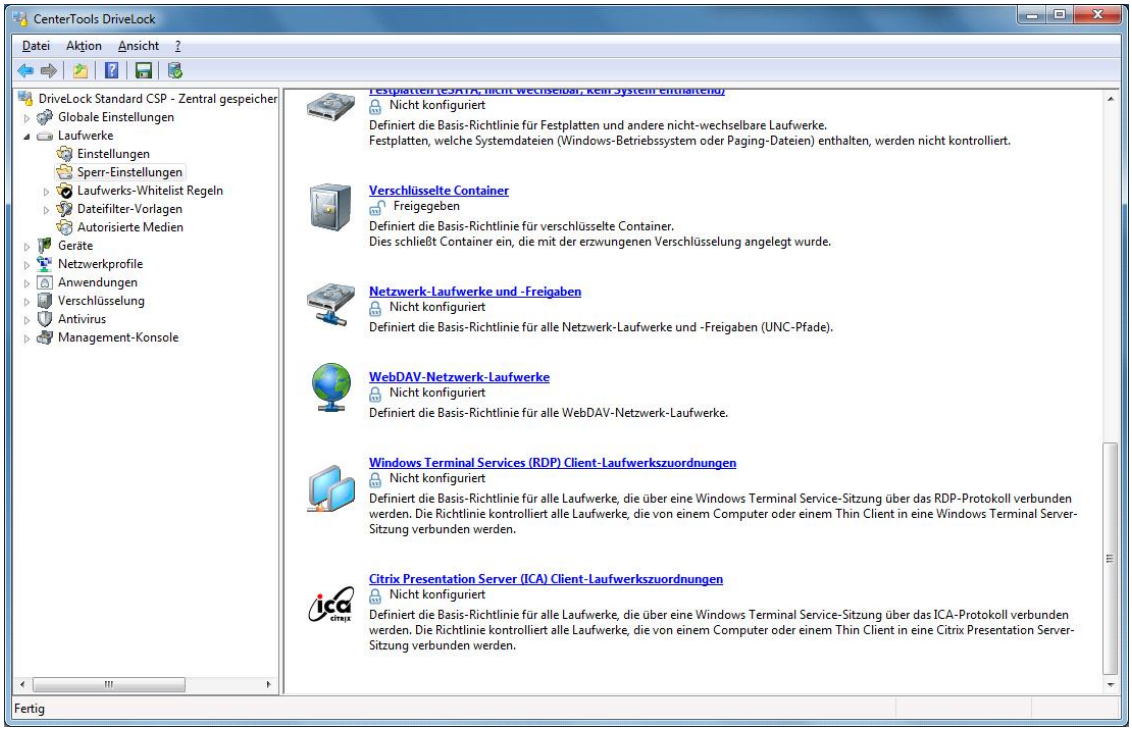
Eine weitere Unterscheidung gilt den Whitelist-Regeln. Es können mindestens Berechtigungen anhand des verbundenen Laufwerkbuchstabens am Terminalserver vergeben werden. Das Vergeben von Berechtigungen basierend auf einzelne Laufwerke anhand der Hardwaredaten (z.B. USB-Stick Kingston DataTraveler) geht nur unter bestimmten Voraussetzungen.

Generell empfiehlt es sich die Konfiguration von Terminalservern und Clients zu trennen, z.B. durch eine separate Gruppenrichtlinie.

9.2.1 Globale Berechtigungen

Im einfachsten Fall, können Berechtigungen auf alle verbunden Laufwerke eines Clients vergeben werden. Dabei spielt es keine Rolle ob das verbundene Laufwerk ein CD/DVD-Laufwerk, eine Festplatte, oder ein USB-Stick ist. Die Berechtigungen werden für all diese verbunden Laufwerke anhand von Benutzern oder Gruppen umgesetzt. Hierbei wird nach Verbindungsprotokoll unterschieden: Erweiterte Konfiguration – Laufwerke – Sperr-Einstellungen

- Windows Terminal Services (RDP) Client-Laufwerkszuordnungen: Alle Verbindungen über RDP, Windows-Standard.
- Citrix Presentation Server (ICA) Client-Laufwerkszuordnungen: Alle Verbindungen über ICA, Citrix-Standard. Setzt Citrix Presentation Server 4.5 (64-Bit) oder XEN 5 oder höher voraus.

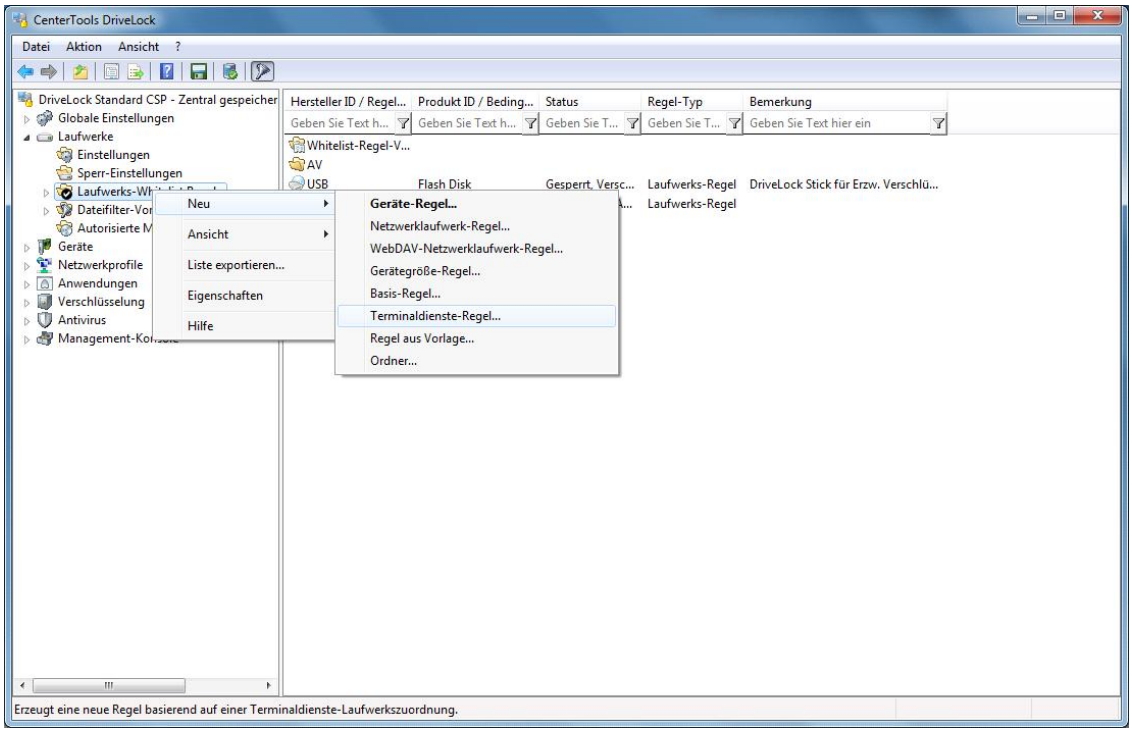


9.2.2 Basierend auf den verbunden Laufwerksbuchstaben

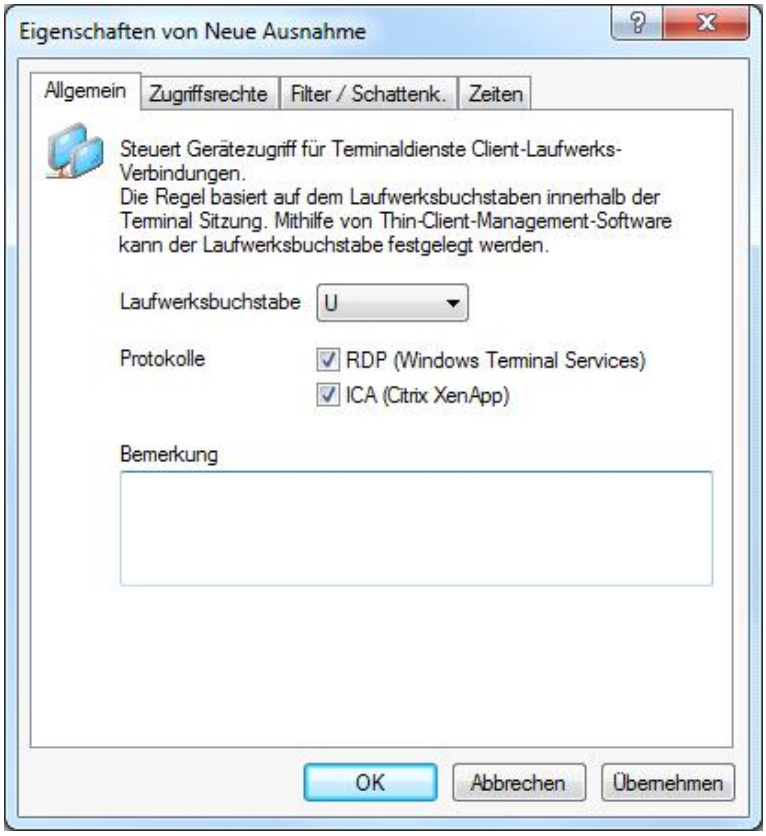
Um Laufwerke zu sperren, müssen Sie die Terminalserver Umgebung so konfigurieren, dass vordefinierte Laufwerksbuchstaben für bestimme Laufwerkstypen (z.B. USB-Wechseldatenträger) verwendet werden. Normalerweise kann man das auf Thin-Client Seite einstellen. Anschließend können Sie eine Terminaldienste-Regel erstellen, um auf diesen Laufwerksbuchstaben Berechtigungen oder zeitliche Einschränkungen festzulegen.

Beispiel: Ein Benutzer stellt eine Verbindung mit einem Terminalserver her. Als Client hat er einen Thin-Client. Der Administrator hat an allen Thin-Clients eingestellt, dass USB-Laufwerke immer als Laufwerk U: innerhalb der Terminalserversitzung verbunden werden. Der Administrator erstellt in DriveLock eine Terminaldienste-Regel für das Laufwerk U: und vergibt darauf Berechtigungen für eine Gruppe. Damit kann über die Gruppe der Zugriff auf USB-Laufwerke geregelt werden.

Um eine Ausnahme basierend auf den verbunden Laufwerksbuchstaben zu erstellen, navigieren Sie zu **Laufwerke: Laufwerks-Whitelist-Regeln**, dann mit Rechtsklick darauf auf **Neu –> Terminaldienste-Regel**:



Anschließend wählen Sie dazu aus dem Dropdown-Menü einen Buchstaben und aktivieren Sie das dazu passende Protokoll, das in Ihrer Umgebung verwendet wird. Berechtigungen werden auf dem Reiter *Zugriffsrechte* vergeben:



9.2.3 Basierend anhand der Hardwaredaten

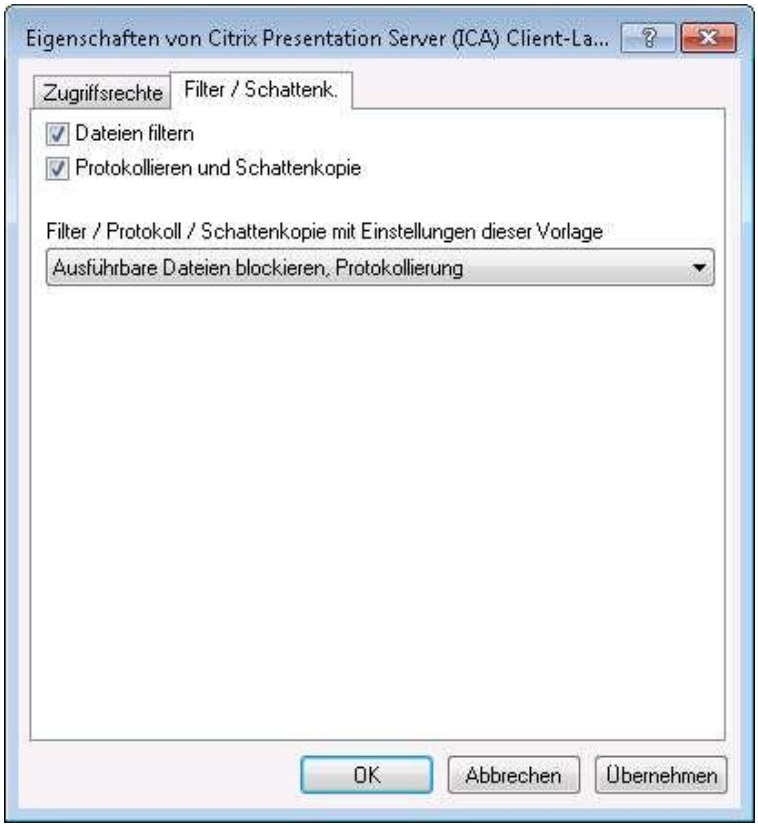
Wenn Sie eine Whitelist-Regel anhand der Hardwaredaten erstellen möchten, die Verbindungsart es erlaubt, können Sie wie gewohnt eine Regel erstellen: *Laufwerke –> Laufwerks-Whitelist Regeln –> Geräte-Regel* und verbinden Sie sich anschließend mit dem Client oder dem Terminalserver, je nach Verbindungsart, und wählen das freizugebende Laufwerk aus. Anschließend vergeben Sie noch die Berechtigungen auf dem Reiter *Zugriffsrechte*.

9.2.4 Dateifilter

Mithilfe des Dateifilters lassen sich Zugriffe anhand der Dateitypen (PDF, DOCX, etc.) einschränken und protokollieren.

Der Dateifilter kann in allen Regeln verwendet und zugewiesen werden. Generell gilt, der clientseitige Dateifilter ist leistungsfähiger als serverseitig. Einschränkungen aufgrund der Verbindungsarten können Sie der Übersichtstabelle in Kapitel „Verbindungsarten“ entnehmen.

Ein Dateifilter kann auf alle Arten von Regeln angewendet werden. Im Folgenden Beispiel verwenden wir eine Dateifilter-Vorlage (die ausführbare Dateien sperrt), und wenden diesen serverseitig auf Verbindungen an, die über das Protokoll ICA hergestellt werden: *Laufwerke –> Sperr-Einstellungen –> Citrix Presentation Server (ICA) Client-Laufwerkszuordnungen –> Reiter Filter /Schattenk*.



Anschließend gibt es folgende Optionen:

- *Dateien filtern*: Dateitypen werden anhand der gewählten Dateifilter-Vorlage zugelassen/gesperrt.
- *Protokollieren und Schattenkopie*: Operationen (Lesen, Schreiben) werden protokolliert und können später mit dem DCC ausgewertet werden.
- *Filter / Protokoll / Schattenkopie mit Einstellungen dieser Vorlage <Auswahl>*: Auswahl der Dateifilter-Vorlage, deren Einstellungen verwendet werden. Es wird nur der Filtern/Protokollieren Teil der Vorlage angewendet, entsprechend gesetzten vorhergehenden Optionen, z.B. Setzt man Dateien filter und wählt eine Vorlage Ausführbare Dateien blockieren, Protokollierung wird u.A. .EXE blockiert, aber keine Protokollierung vorgenommen.

9.3 Applikationskontrolle

Die Applikationskontrolle ist besonders interessant, wenn es darum geht den Terminalserver abzusichern. Damit ist es für den Administrator ein Leichtes, Zugriff auf bestimmte Programme zu unterbinden. Auch Systemprogramme, wie die cmd.exe, wscript.exe, cscript.exe, mmc.exe und dergleichen können für Standardbenutzer gesperrt werden. Die Ausführung durch Administratoren ist weiterhin möglich.

Die Konfiguration erfolgt hier identisch zur Client-Konfiguration.

DriveLock Administration