



DriveLock Administration 2022.1

30.03.2022

© 2022 DriveLock SE





Inhaltsverzeichnis

Teil I		Konventionen	5
Teil II		Hinweise zu diesem Handbuch	7
Teil III		Laufwerke und Geräte kontrollieren	9
	1	Laufwerke kontrollieren	10
		Laufwerke in der Basiskonfiguration sperren	11
		Laufwerkssperre aktivieren	12
		Einfache Laufwerksregeln definieren	
		Erweiterte Einstellungen zum Sperren von Laufwerken	20
		Allgemeine Einstellungen zur Laufwerkssperrung	20
		Globale Sicherheits-Einstellungen für die Kontrolle von Laufwerken	20
		Konfiguration von Benutzermeldungen	22
		Angepasste Benutzerbenachrichtigungen	22
		Einstellungen der Dateihash-Erzeugung	23
		Laufwerks-Identifikations-Dateien	24
		Schattenkopie-Einstellungen	27
		S.M.A.R.T. Festplatten-Selbstüberwachung	27
		Erweiterte Einstellungen zur Kontrolle von Laufwerken	28
		Laufwerkssperre aktivieren	28
		Laufwerksregeln definieren	31
		Whitelist-Regeln verwalten	32
		Whitelist-Vorlagen erstellen	34
		Geräte-Regel	36
		Sperren und Überwachen von CD/DVD-Brennern	38
		Laufwerkslisten-Regel erstellen	41
		Netzwerklaufwerk-Regel	42
		WebDAV-Netzwerklaufwerk-Regel	44
		Gerätegröße-Regel	45
		Basis-Regel	47
		Terminaldienste-Regel	48
		Regeln basierend auf einer Regelvorlage erstellen	48
		Hardware-ID-Regel	49
		Zusätzliche Einstellungen bei Whitelist-Regeln konfigurieren	50
		Dateizugriff einschränken und überwachen	51
		Laufwerksbuchstaben zuweisen	51
		Regelspezifische Benutzermeldungen einrichten	52
		Weitere Optionen	54
		Ausführung von eigenen Kommandos	57
		Dateifilter konfigurieren	60
		Datei-Typdefinitionen erstellen	60
		Dateitypen-Gruppen erstellen	63
		Neue Dateifilter-Vorlage erstellen	65
		Dateifilter-Vorlage verwenden	74
		Dateifilter-Vorlage für verschlüsselte Laufwerke (Encryption 2-Go)	75
		Laufwerkslisten erstellen	76
		Medien-Autorisierung verwenden	79
		Datenubertragung mit Hilfe von Schattenkopien überwachen	82
		Allgemeine Schattenkopie-Einstellungen festlegen	82
		Allgemeine Einstellungen	83
		Client-Einstellungen für Schättenkopien	84



		Ausnahmen bei Schattenkopien	84
		Einstellungen für das Hochladen auf den zentralen	86
		Schättenkopie-Server Zeitliche Einschränkungen	86
		Netzwerkeinschränkungen	87
		Verschlüsselung	88
		Schattenkonien in Laufwerksregeln konfigurieren	80
		Schattenkopien in Ladiwerksregen königdheren	92
	C		92 0E
	Z	Gerate kontromeren	95
		Geräte in der Basiskonfiguration sperren	96
		Erweiterte Einstellungen zum Sperren von Geräten	104
		Allgemeine Einstellungen zur Gerätesperrung	105
		Konfiguration von Benutzermeldungen	105
		Erweiterte Einstellungen zur Kontrolle von Geräten	106
		Gerätesperrungaktivieren	106
		Detaillierte Kontrolle von iTunes und iTunes-synchronisierten Geräte	110
		Konfigurieren der Schnittstellen COM und LPT	114
		Geräteregeln definieren	114
		Gerätelisten verwenden	118
		Bluetooth-Geräte	122
		Computervorlagen verwenden	122
		Computervorlage erstellen	123
		Erstellen einer Computervorlage anhand des aktuellen Systems	124
		Erstellen einer Computervorlage von einem anderen Rechner	124
		Erzeugen einer leeren Vorlage	124
		Computervorlagen verwenden	125
		Bearbeiten der Geräteliste in der Computervorlage	125
		Neue Geräte in die Computervorlage importieren	126
		Geräte aus einer Computervorlage exportieren	127
		Zugriffsrechte innerhalb einer Computervorlage definieren	128
		Aktivieren einer Computervorlage	129
		Anzeige der durch eine Computervorlage definierten Geräte	129
Teil IV		Netzwerkprofile	131
	1	Allgemeine Netzwerknrofil-Finstellungen	135
	-		100
		Benutzerbenachrichtigung einrichten	135
		WIFI Verbindungen bei LAN-Anbindung verhindern	136
	-	VPN-Clients von Drittanbietern einsetzen	137
	2	Netzwerkverbindungen festlegen	138
		Active Directory Standort	140
		Netzwerkverbindung anhand IP-Einstellungen festlegen	141
		Netzwerkadapter	143
		Geographische Position	143
		Drahtlosnetzwerk mit SSID	143
		Besondere Netzwerkverbindung	144
		Befehlszeile	145
	3	Konfigurationsprofile erstellen	146
		Internet Explorer Proxy Einstellungen	148
		MSN Messenger Einstellungen	149
		Weitere Aktionen bei Erkennung von Netzwerken	149
	Δ	Whitelist-Regel für eine Netzwerkverhindung einrichten	151
	-		1.71
	5	Benutzerspezifische Netzwerkprofile erstellen	151
Teil V		DriveLock File Protection	153
	1	Wie funktioniert DriveLock File Protection?	154



2	Linke wet "Ante Manager III" and the second a large second	
_	Unterstutzte verschlusselungsverfahren	155
3	File Protection einrichten	156
	Master-Zertifikat für die Schlüsselverwaltung einrichten	157
	Zertifikatsverwaltung konfigurieren	158
	Richtlinienkonfiguration für Clients	159
	Einstellungen zur Verschlüsselung konfigurieren	159
	Benutzeroberfläche der Verschlüsselung konfigurieren	160
	Einstellungen für verschlüsselte Laufwerke konfigurieren	161
	Zusätzliche Einstellungen konfigurieren	162
	Erzwungene Verschlüsselung	163
	Einstellungen für die Wiederherstellung verschlüsselter Laufwerke	104
	konfigurieren Unterrehmenssertifiket	164
		100
4		107
	Wie funktioniert die Benutzerverwaltung?	167
	Benutzer verwalten	168
	Gruppen verwalten	170
_	Zertifikate verwalten	170
5	Verschlusselte Laufwerke zentral verwalten	1/3
	Neues verschlusseltes Laufwerk anlegen	174
	Neues verschlusseltes Laufwerk anlegen Zugriffsberechtigungen ändern	174 175
6	Neues verschlusseltes Laufwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse	174 175 176
6 7	Neues verschlusseltes Laufwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse	174 175 176 177
6 7	Neues verschlusseltes Laufwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver	174 175 176 177 178
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten	174 175 176 177 178 179
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients	174 175 176 177 178 179 180
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients	174 175 176 177 178 179 180 180
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients Virtual-Clients	174 175 176 177 178 179 180 180 180
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients Virtual-Clients Thin-Clients anderer Hersteller	174 175 176 177 178 179 180 180 180 180 180
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients Virtual-Clients Thin-Clients anderer Hersteller Linux Thin-Clients des Herstellers Wyse	174 175 176 177 178 179 180 180 180 180 180 180
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients Virtual-Clients Thin-Clients des Hersteller Linux Thin-Clients des Herstellers Wyse Terminalserver-Regeln	174 175 176 177 178 179 180 180 180 180 180
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients Virtual-Clients Thin-Clients anderer Hersteller Linux Thin-Clients des Herstellers Wyse Terminalserver-Regeln Globale Berechtigungen	174 175 176 177 178 179 180 180 180 180 180 180 181
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients Virtual-Clients Thin-Clients anderer Hersteller Linux Thin-Clients des Herstellers Wyse Terminalserver-Regeln Globale Berechtigungen Basierend auf den verbunden Laufwerksbuchstaben	174 175 176 177 178 179 180 180 180 180 180 180 180 181 181
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients Virtual-Clients Thin-Clients anderer Hersteller Linux Thin-Clients des Herstellers Wyse Terminalserver-Regeln Globale Berechtigungen Basierend auf den verbunden Laufwerksbuchstaben Basierend anhand der Hardwaredaten	174 175 176 177 178 179 180 180 180 180 180 181 181 181 181
6 7 1	Neues verschlusseltes Lautwerk anlegen Zugriffsberechtigungen ändern Wiederherstellung verschlüsselter Verzeichnisse Reporting und Analyse Terminalserver Verbindungsarten FAT-Clients / Desktop-Clients Windows Embedded-Clients Virtual-Clients Thin-Clients anderer Hersteller Linux Thin-Clients des Herstellers Wyse Terminalserver-Regeln Globale Berechtigungen Basierend auf den verbunden Laufwerksbuchstaben Basierend anhand der Hardwaredaten Dateifilter	174 175 176 177 178 179 180 180 180 180 180 181 181 181 181 181
	4	 Master-Zertifikat für die Schlüsselverwaltung einrichten Zertifikatsverwaltung konfigurieren Richtlinienkonfiguration für Clients Einstellungen zur Verschlüsselung konfigurieren Benutzeroberfläche der Verschlüsselung konfigurieren Einstellungen für verschlüsselte Laufwerke konfigurieren Zusätzliche Einstellungen konfigurieren Einstellungen für die Wiederherstellung verschlüsselter Laufwerke konfigurieren Unternehmenszertifikat Benutzer und Zertifikate verwalten Wie funktioniert die Benutzerverwaltung? Benutzer verwalten Gruppen verwalten Zertifikate verwalten S Verschlüsselte Laufwerke zentral verwalten





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, Netzwerkprofile, File Protection, 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, Encryption (beinhaltet BitLocker Management, Disk Protection, Encryption 2-Go, 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 Laufwerke und Geräte kontrollieren





3 Laufwerke und Geräte kontrollieren

3.1 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

3.1.1 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 <u>"Erweiterte Einstellungen</u> zum Sperren von Laufwerken").

3.1.1.1 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".



CriveLock					-	
🛒 Datei Aktion Ansicht Fenster	r ?					- 8 ×
🗢 🔿 🖄 📓 🖌 🌄						
DriveLock - Zentral gespeicherte O Globale Einstellungen Globale Einstellungen O Globale Einstellungen O Globale Einstellungen O Verschlusselung O Verschlüsselung Security-Awareness System-Management Management-Konsole		Laufwerke Jedes an den Computer angeschlossene Gerät, dieser Kategorie konfiguierten Richtlinien verwa Bitte beachten Sie, dass einige Kameras, Scanne Geräte, die nicht über einen Laufwerksbuchstab	das über einen Laufwerksbuchstaben angespro ltet. er und Medienabspielgeräte über die Kategorie en angesprochen werden.	chen wird (z.B. USB-SI "Geräte" verwaltet w	tick usw), wird über (erden müssen. Dies g	Aie in ilt für alle
	Sperr-Einstellung Legt die Basisrichtlinie für al Beginnen Sie mit Ihrer Konfi Ihrem Netzwerk kontrolliert Der verwendete Bus-Typ (U Laufwerkstyp (z.B. CD-ROM Weitere Optionen sind in der	gen le Laufwerke eines bestimmten Typs fest. guration hier, um zu bestimmen, wie Laufwerke in werden sollen. i8, 1394 oder SD) besitzt eine höhere Priorität als der r ^{Ja} <u>Erweiterten Konfiguration</u> verfügbar.	Line and Lin	aufwerke	b	
			Drive type	Status	Options	
			Distatutinaurie se CD-ROM-Laufwerke USB-angeschlossene Laufwerke FireWire (1394)-angeschlossene Laufwerke SD-Karten-Laufwerke (SD Bus) Andere Wechseldatenträger Festplatten (eSATA, nicht wechselbar) Verschlüsselte Laufwerke Netzwerk-Laufwerke und -Freigaben WebDAV-basierende Netzwerklaufwerke	Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert		×
< >>	<u> </u>					
Fertig						

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.

Allgemein	Optionen		
USB-ang	eschlossene Laufwerke		
0	Erlauben		
0	Sperren für alle Benutzer (Stan	dard)	
0	Sperren, aber Zugriff für definie	nte Benutzer und (Gruppen erlauben
	Benutzer oder Gruppe	Lese	en Schre
	Se DriveLockAdmins		
	Hinzufügen y Entfemen		

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".

Allgemein Optionen	
Dateifilter und Schatter	nkopie
Dateien filtem	
Protokollieren und S	Schattenkopie
Filter / Protokoll / Scha	attenkopie mit Einstellungen dieser Vorlage
Nur Office Dokumente	•
Erzwungene Verschlüs	selung
Verschlüsselung en	zwingen
Verschlüsselung en Verschlüsse	zwingen Ite Laufwerke automatisch verschlüsseln
Verschlüsselung er. Unverschlüsse Senutzerbenachrichtig	zwingen Ite Laufwerke automatisch verschlüsseln ung
 Verschlüsselung er. Unverschlüsse Benutzerbenachrichtig Benutzer muss Ven 	zwingen te Laufwerke automatisch verschlüsseln ung vendungsrichtlinie akzeptieren, bevor Regel aktiv wird
 Verschlüsselung er. Unverschlüsse Benutzerbenachrichtig Benutzer muss Ven Speziellen Text bei 	zwingen Ite Laufwerke automatisch verschlüsseln ung vendungsrichtlinie akzeptieren, bevor Regel aktiv wird Benutzerbenachrichtigung anzeigen
 Verschlüsselung er. Unverschlüsse Benutzerbenachrichtig Benutzer muss Ven Speziellen Text bei Benutzerinformation 	zwingen te Laufwerke automatisch verschlüsseln ung vendungsrichtlinie akzeptieren, bevor Regel aktiv wird Benutzerbenachrichtigung anzeigen n wenn diese Regel aktiviert wird
 Verschlüsselung er. Unverschlüsse Benutzerbenachrichtig Benutzer muss Ven Speziellen Text bei Benutzerinformatio 	zwingen te Laufwerke automatisch verschlüsseln ung vendungsrichtlinie akzeptieren, bevor Regel aktiv wird Benutzerbenachrichtigung anzeigen n wenn diese Regel aktiviert wird
 Verschlüsselung er. Unverschlüsse Benutzerbenachrichtig Benutzer muss Ven Speziellen Text bei Benutzerinformatio 	zwingen te Laufwerke automatisch verschlüsseln ung vendungsrichtlinie akzeptieren, bevor Regel aktiv wird Benutzerbenachrichtigung anzeigen n wenn diese Regel aktiviert wird

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 **x**, um das Popup-Fenster zu schließen. Verwenden Sie die kleinen blauen Pfeilsymbole **v** und **a**, um die Laufwerksdetails ein- bzw. auszuschalten.



GenterTools DriveLock					- • • ×
Datei Aktion Ansicht ?					
DivieLock Standard Policy - Zentral gespe Globale Einstellungen GE Einstellungen Sperr-Einstellungen Dotterführer-Vorlagen Datefführer-Vorlagen		Laufwerke Jedes an den Compute usw), wird über die in Bitte beachten Sie, das müssen. Dies gilt für al	r angeschlossene Gerät, das über einen La dieser Kategorie konfigurierten Richtlinien s einige Kameras, Scanner und Medienabsp le Geräte, die nicht über einen Laufwerksbu	ufwerksbuchstaben angesprochen wird verwaltet. vielgeräte über die Kategorie "Geräte" + chstaben angesprochen werden.	(z.B. USB-Stick verwaltet werden
Autorisierte Medien J Geräte Y Netzwerkprofile		G Globale Einstellungen			🕤 Geräte
 Q erschlüsselung Q Antivirus Q Antivirus Management-Konsole 	Sperr-Einstellunge Legt die Basisrichtlinie für alle Beginnen Sie mit Ihrer Konfig Laufwerkein Ihrem Netzwerk Der verwendete Bus-Typ (USI als der Laufwerkstyp (z.B. CD- Weitere Optionen sind in der	n Laufwerke eines bestimmten Typ uration hier, um zu bestimmen, w kontrolliert werden sollen. 1, 1394 oder SD) besitzt eine höher ROM). Proveiterten Konfiguration verfü	s fest. ie e Priorität igbar. USB-ange	schlossene Laufwerke	
	Whitelist-Regeln				
	Die Laufwerks-White-List Regeln definieren Ausnahmen der Basis-	<u>Whitelist-Regel erstellen</u> Produkt Hersteller	Status	Bemerkung	Aktionen
< III >	Richtlinie. Aufgrund von eindeutigen Laufwerks-Identifikations- Merkmalen bestimmen die	USB Flash Disk LEXAR JUMPDRIVE SECURE	Gesperrt, Verschlüsselt Gesperrt mit Ausnahmen, Dateifilter, Protokoll	DriveLock Stick für Erzw. Verschlüsselung	
ertig					

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)

There is a second the second s					
2 2 8					
veLock Standard Policy - Zentral gespe Globale Einstellungen Laufwerke Sperr-Einstellungen Sperr-Einstellungen Datefilter-Vorlagen Autoristerte Medien		Laufwerke Jedes an den Compute usw), wird über die in Bitte beachten Sie, das müssen. Dies gilt für al	er angeschlossene Gerät, das über einen La dieser Kategorie konfigurierten Richtlinien s einige Kameras, Scanner und Medienabsp lle Geräte, die nicht über einen Laufwerksbu	ufwerksbuchstaben angesprochen wird verwaltet. Jielgeräte über die Kategorie "Geräte" chstaben angesprochen werden.	(z.B. USB- verwaltet v
Geräte		Globale Einstellungen			€) Ger
Anwendungen					
Verschlüsselung Antivirus	Sperr-Einstellunge	n			
	Laufwerke in Ihrem Netzwerk	kontrolliert werden sollen.		2	
	Laufwerke in Ihrem Netzwerk Der verwendete Bus-Typ (USI als der Laufwerkstyp (z.B. CD Weitere Optionen sind in der	kontrolliert werden sollen. 8, 1394 oder SD) besitzt eine höher -ROM). <u>P Erweiterten Konfiguration</u> verfü	re Priorität	eschlossene Laufwerke	
	Laufwerke in Ihrem Netzwerk Der verwendete Bus-Typ (US) als der Laufwerkstyp (z.B. CD) Weitere Optionen sind in der Whitelist-Regeln	kontrolliert werden sollen. 3, 1394 oder SD) besitzt eine höher ROM). <i>P</i> Enveiterten Konfiguration verfü	re Priorităt ügbar. USB-anq	eschlossene Laufwerke	
	Laufwerke in Ihrem Netzwerk Der verwendete Bus-Typ (US) als der Laufwerkstyp (z.B. CD) Weitere Optionen sind in der Whitelist-Regeln Die Laufwerks-White-List Regeln definieren	kontrolliert werden sollen. 3. 1394 oder SD) besitte eine höher ROM). # Enweiterten Konfiguration verfu Whitelist-Regel erstellen Ded tab. Unstation	iggar.	eschlossene Laufwerke	
	Laufwerke in Ihrem Netzwerk Der verwendete Bus-Typ (US) als der Laufwerkstyp (z.B. CD Weitere Optionen sind in der Whitelist-Regeln Die Laufwerks-White-List Regeln definieren Ausnahmen der Basis- Richtlinie.	kontrolliert werden sollen. 3.1340 oder SD) besitte eine höher ROM). Fuweiterten Konfiguration verfu Whitelist-Regel erstellen Produkt Hersteller USB Flach Dick	re Priorität ügbər. USB-anq USB-anq Status Geopert Verschlüsselt	eschlossene Laufwerke	Aktionen

3.1.1.2 Einfache Laufwerksregeln definieren

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



Algemein	Zugriffsrech	te Optionen	
Hersteller	ID 🗌		
Produkt IC)		
Bemerkun	g		
Symbol	finierte Serien	nummern zulassen	Lingförag
Symbol	finierte Serien	 nummern zulassen Bemerkung 	Hinzufügen)
Symbol	finierte Serien	• nummern zulassen Bemerkung	Hinzufügen) Entfernen
Symbol	finierte Serien	nummern zulassen Bemerkung	Hinzufügen Entfernen Bearbeiten
Symbol	finierte Serien	nummern zulassen Bemerkung	Hinzufügen Entfemen Bearbeiten

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).



nstallierte l	Laufwerke	Device Scanner Datenbar	nk		
Zurzeit inst	allierte L <mark>au</mark> fw	verke / Geräte 🔘 lokal) auf	dlwin 7x64	Verbinden
Laufw	Bus	Hersteller	Prod	ukt	Seriennummer
1	NETWORH FLOPPY SAS	 \vmware-host\Share VMware, 	d GEN VMw NEC	IERIC_FLOP vare Virtual S VMWar VM	6&3b4c39bd&
	USB	LEXAR	JUM	PDRIVE SE	302ac203025
Aktualisie	ren				

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.



	Zugriffsrech	te Optionen	
Hersteller	ID LEXAR		
Produkt I[JUMPD	RIVE SECURE	
Bemerkun Symbol	g	▼	
Seri	ennummer	Bemerkung	Hinzufügen
1000	ac2030256 <mark>4</mark> 2	•••	Entfernen
302			
302			Bearbeiten

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

Algemein	Zugriffsrechte	Optionen		
Sperr-Ein	st <mark>ellun</mark> gen			
0	Erlauben			
0	Sperren für alle Be	enutzer		
0	Sperren, aber Zug	priff für definierte B	enutzer und Grup	pen erlauben
	Benutzer oder G	iruppe	Lesen	Schre
	StriveLockAr	dmins		
		Entformer		
	Hinzufügen 🔫	Chuemen		

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".

Allgemein	Zugriffsrechte	Optionen	
Dateifilter	und Schattenkor	pie	
Z Dateie	n filtem		
Protok	ollieren und Scha	attenkopie	
Filter / Pro	tokoll / Schatter	nkopie mit Einstellungen dieser Vorlage	
Nur Office	e Dokumente		•
Erzwunge	ne Verschlüsselu	ing	_
Versch	lüsselung erzwin	gen	
🗌 Ur	nverschlüsselte L	aufwerke automatisch verschlüsseln	
Benutzerb Benutz Spezie	enachrichtigung er muss Verwen llen Text bei Ber	aufwerke automatisch verschlüsseln dungsrichtlinie akzeptieren, bevor Regel aktiv v nutzerbenachrichtigung anzeigen	vird
Benutzerb Benutz Spezie Benut	enachrichtigung er muss Verwen llen Text bei Ber zerinformation w	aufwerke automatisch verschlüsseln dungsrichtlinie akzeptieren, bevor Regel aktiv v nutzerbenachrichtigung anzeigen enn diese Regel aktiviert wird	vird
Benutzerb Benutz Spezie Benut	enachrichtigung er muss Verwen llen Text bei Ber zerinformation w	aufwerke automatisch verschlüsseln dungsrichtlinie akzeptieren, bevor Regel aktiv v nutzerbenachrichtigung anzeigen enn diese Regel aktiviert wird	vird

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.



3.1.2 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.

3.1.2.1 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.

3.1.2.1.1 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.



Allereneite			
Administratore	en den Zugriff auf alle Laufwerke	erlauben	
	Aktiviert		
	Deaktiviert (Standard)		
	Nicht konfiguriert		
Hilfe Aktivieren Sie	diese Option um allen Administra edauben, lst dies deaktiviert dürt	atoren den Zugriff auf die fen nur die Benutzer welch	ie in
Laufwerke zu der Liste: -erla	ubte Benutzer- aufgeführt sind a	uf die Laufwerke zugreifen	
Laufwerke zu der Liste: -erla	ubte Benutzer- aufgeführt sind a	uf die Laufwerke zugreifen	

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.

F	
romati	eren und Auswerren von Wechseidatentragem
B	enutzer oder Gruppe
	nzufügen
Hi	



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**.

3.1.2.1.2 Konfiguration von Benutzermeldungen

3.1.2.1.2.1 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.

Ilgemein	Laufwerkszugriff Temporäre Freigabe	
Benutz	erdefinierte Nachrichten verwenden	
Laufw	erk gespert Nachricht (%DRV% ersetzt mit Laufw.buchstabe)	
	Der Zugriff auf das Laufwerk %DRV% wurde gespent.	*
Test		-
Test		*
Nachri verwei	icht wenn Neustart benötigt wird um Laufwerk wieder zu nden (%DRV% ersetzt mit Laufwerksbuchstaben)	
	Bitte starten Sie den Rechner neu, um das Laufwerk %DRV% verwenden zu können.	*
Test		*

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").

3.1.2.1.3 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.

3.1.2.1.4 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.



 Default company policy - Zentri Globale Einstellungen EDR Laufwerke Einstellungen Sperr-Einstellungen Sperr-Einstellungen Laufwerks-Whitelist-Reg Dateifilter-Vorlagen Laufwerkslisten Autorisierte Medien Merzwerkprofile 	Einstellung Enter text here Protokollieren von Laufwerksaktivitäten (verbinden / entfern Laufwerke freigeben wenn Dienst gestoppt wird (Nur Windo Administratoren den Zugriff auf alle Laufwerke erlauben Schattenkopie-Einstellungen Formatieren und Auswerfen von Wechseldatenträgern Angepasste Benutzer-Benachrichtigungen Einstellungen der Dateihash-Erzeugung Einstellungen der Festplatten-Selbstüberwachung (S.M.A.R.T.) Einstellungen für Laufwerks-Identifikations-Dateien	Wert Enter text he Nicht konfig Nicht konfig Nicht konfig Nicht konfig Nicht konfig Nicht konfig Nicht konfig Nicht konfig	guriert i guriert i guriert i guriert guriert guriert guriert guriert guriert
 Anwendungen Verschlüsselung Microsoft Defender Security Awareness Inventarisierung und Schwai System-Management Management-Konsole 	Properties ? Allgemein Sicherheit Laufwerks-IdDateien können benutzt werden, um Herstellerdaten und Seriennummer von Laufwerken bereitzustellen (z.B. wenn diese Daten Grund von Beschränkungen nicht übermittelt werden). Diese Daten haben eine höhere Priorität als Hardware-Daten. Image: Laufwerks-Identifikations-Dateien benutzen (sofem vorhanden) Sicherheits- und Kompatibilitäts-Modus Sehr sicher (könnte mit Citrix-ICA-basierten Thin Clients nicht funktionieren) Image: Mittel sicher (funktioniert in den meisten Thin-Client-Umgebur Niedrig sicher (funktioniert überall) Laufwerks-Identifikations-Dateien automatisch erzeugen (wird m aktuellen Hardware-Daten gefüllt, nicht auf Thin-Clients) Laufwerks-Identifikations-Datei-Hashlisten aktivieren (wenn eine Hashliste Teil der Laufwerks-Identifikations-Datei Hashlisten aktivieren (wenn eine Hashliste Teil der Laufwerks-Identifikations-Datei St, werden nu Dateien erlaubt, deren Hashwert dem der Liste entspricht; alle a Dateien werden blockiert) Dateien sind ab Erzeugung gültig für 24 Tude	× hfig hfig hfig hfig hfig hfig hfig hfig	guriert (guriert (guriert (guriert (guriert (guriert (guriert (guriert (guriert (guriert (
< >	OK Cancel A	pply	

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.



Active Directory / Lokale Computer	
Konfigurationsdateien	Laufwerks-Identifikations-Datei X
 Richtlinienzuweisungen DriveLock Enterprise Services [dlserver] Server Mandanten Produkt-Pakete und -Dateien Agenten-Push-Installation DriveLock Cloud OriveLock File Protection 	Laufwerks-Identifikations-Datei erzeugen auf
Betrieb Agenten-Fernkontrolle	Revision
Netzwerk-Pre-Boot-Computer	Seriennummer
	Nur bereits existierende Dateien erlauben (Hashliste generieren)
	□ Laufwerksdaten gültig bis 10.07.2020 ∨ 09:52:38 🜲
	Digitale Signatur von Volume-Daten
	Zeitfikat auswählen OK Abbrechen K Abbrechen Laufwerks- Identifikations-Datei erzeugen

3.1.2.1.5 Schattenkopie-Einstellungen

Bitte sehen Sie im Kapitel <u>"Schattenkopien in Laufwerksregeln konfigurieren</u>" für Informationen zum Konfigurieren und zur Verwendung von Schattenkopien nach.

3.1.2.1.6 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:



Allgemein		
 Festplatten-Selbstübe S.M.A.R.TFunktione Status lesen alle 	erwachung aktivieren (benutzt eingebaute ien) 60 💓 min	

3.1.2.1.7 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.

3.1.2.2 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).



Optionen	Laufwerke		Befehle
Allgemein	Filter / Schattenk.	Nachrichten	
SB-angeschlossene	laufwerke		
Edauben	Ladiweike		
Sperren f ür all	e Benutzer (Standard)		
 Sperren, aber 	Zugriff für definierte Benutz	er und Grup	open erlauben
Benutzer og	ler Gruppe	Lesen	Schre
S VMTES			
Lingthingon	Entfemen		

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.

Allgemein	Filter / Schattenk.	Nachrichten	
Optionen	Laufwerke	Befehle	
Buchstabe von ve	rbundenen Laufwerken ändem	auf ersten Freien aus:	
A:		e.	
B :			
C:			
D:			
E:			
V F:			
G :			
₩ H:			
J:			
L.			
N.			
P.			
Q:			
R:			
		-	

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

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

3.1.2.3 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.

3.1.2.3.1 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.

CenterTools DriveLoc	:k	-					
Datei Aktion Ansic	ht ?						
🗢 🏟 🖄 🛅 🗟	2 🖬 🗟 🔈						
 DriveLock Standard F Globale Einstellur Laufwerke Einstellungen Sperr-Einstell 	Policy - Zentral gespe ngen n ungen	Hersteller I Geben Sie Whitelis	D / Regel Produkt ID / Bedingung S Text h 7 Geben Sie Text hier ein 7 G t-Regel-V	itatus Seben Sie T 🍸	Regel-Typ Geben Sie T Y	Bemerkung Geben Sie Text hier ein 🌱	
⊿ White	hitelist-Reaeln	•	Geräte-Regel	rt mit A	Laufwerks-Regel		
→ AV → 💱 Dateifilter	Ansicht		Netzwerklaufwerk-Regel	geben rt	Netzwerklaufw Laufwerksgröß		
Autorisier Filler Geräte	Liste exportieren		Gerätegröße-Regel	rt	Basisregel		
Netzwerkprot	Eigenschaften		Basis-Regel				
 Anwendunge Verschlüsselu 	Hilfe		Terminaldienste-Regel Regel aus Vorlage				
▷ ♥ Antovirus ▷ ♥ Management-Ko	onsole		Ordner				
<) ·						
Erzeugt einen neuen Ord	ner zur Ablage von Wh	nitelist-Regel	in.				

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**.



genschaft	2n		
Allgemein	Zugriffsrechte		
Name	Hersteller-Regeln		
Bemerkun	g		
verzeicht	is aller hersteller spezillschen win	iteist-negelfi	
			-
	0.11		

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.

Datei Aktion Ansicht ?	
(+ - +) 2 D = 1 = 1 1 2 1 2 2 2 2 2 2	
[™] DiveLock Standard Policy - Zentral gespe Hersteller ID / Regel Produkt ID / Bedingung [™] Gibaba Einstellungen Geben Sie Text h [™] Geben Sie Text hier ein [™] Gibaba Einstellungen Geben Sie Text h [™] Geben Sie Text hier ein	Status Regel-Typ Bernerkung Image: Status Geben Sie T Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status
Whitelist-Regel-Vorlagen Neu	• Geräte-Regel
	 Netzwerklaufwerk-Regel WebDAV-Netzwerklaufwerk-Regel Gerätegröße-Regel
Autorisierte Medien Am Raster ausrichten	Basis-Regel
Verate Eigenschaften Verate	Terminaldienste-Regel
> 🛆 Anwendungen Hilfe	Regel aus Vorlage
Management-Konsole	
Fügt eine neue Basis-Regel (basierend auf Laufwerks-Typ oder -Verbindung) ein.	

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**.



CenterTools DriveLock						
Datei Aktion Ansicht ?	-					
← ⇒ 2 × □ ≥ 2 = 8	68	0				
 Statistics of the second sec	Image: Second Secon	egel Produkt ID / Bedingung St. Y Geben Sie Text hier ein Y Geben gel-V Flash Disk Geben CD/DVD-Optionen anzeigen Alle Aufgaben Hiffe Hiffe	stus Regel-Typ ben Sie T Y Geben Sie T Y spert, Versc Laufwerks-Rege egeben Netzwerklaufw. Verschieben Sperren Freigeben	Bemerkung Geben Sie Text hier ein DriveLock Stick für Erzw. Ver	rschlū	
<►						
Verschiebt das gewählte Element in einen ande	ren Ordner.					

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

el-Ordner wahlen			
Wählen Sie den Ziel-Ordner	für die Whitel	ist-Regel	
Laufwerks-Whitelist-Regelr AV Hersteller-Regeln Lexar	18		
		ок	Abbrechen

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

3.1.2.3.2 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 Regel nzu 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.



3.1.2.3.3 Geräte-Regel

CenterTools DriveLock		• ×
Datei Aktion Ansicht ?		
🗢 🔿 🖄 🖾 🗟 🔛 🚳 🚺	P	
DriveLock Standard Policy - Zentral gespe DriveLock Standard P	Image: Status Regel-Typ Bemerkung Geben Sie Text h Geben Sie Text h Geben Sie T Geben Sie Text hier ein Image: Status Geben Sie T Geben Sie Text hier ein Image: Status Image: Status Geben Sie T Geben Sie Text hier ein Image: Status Image: Status Geben Sie T Geben Sie Text hier ein Image: Status Image: Status Gesperit, Versc Laufwerks-Regel DriveLock Stick für Erzw. Verschlü Image: Status Geräter-Regel Verks-Regel DriveLock Stick für Erzw. Verschlü Image: Status Geräter-Regel Verks-Regel Verks-Regel Image: Status	
∢ ► Erstellt ein neues Objekt in diesem Container.		

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.

Welzweike	Benutzer	Laufwerke Nachrichten		Optioner	n Befehle	
Allgemein	Zugriffsred	chte Filter / Schattenk.		Zeiten	Computer	
Hersteller ID	LEXAR					
Produkt ID	JUMPDRIVE SECURE					
Bemerkun <mark>g</mark>						
Symbol	erte Serienn] ummern zulass	en			
Serienn	ummer	Bemerkung		Hin	zufügen	
	302ac203025642				Entfemen	
302ac2				Be	arbeiten	
302ac2						
302ac2						


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.

nstallierte Lai	Jfwerke De	vice Scanner Datenban	k	
Zurzeit install	ierte Laufwer	ke / Geräte 💿 lokal	(auf dlwin 7x64	Verbinden
Laufwerk	Bus	Hersteller	Produkt	Seriennummer
1	NETWO FLOPPY SAS	∖vmware-host∖Sha VMware,	GENERIC_FLOPP VMware Virtual S	6&3b4c39bd&
denter la construction de la construcción de la	USB	LEXAR	JUMPDRIVE SEC.	
Aktualisiere	n			

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.

nstallierte Laufwerke Der	vice Scanner Datenbank	
Computer	Hersteller	Produkt
Salle > DLSERVER DLWIN7X64	Dell	GENERIC_FLOPPY_DR VIRTUAL DISK DVD-ROM GDR-T10N I
	 NECVMWar PLDS WMware 	VMware IDE CDR10 DVD+-RW DU-8A2S VMware Virtual S
	Revision 3000	

Die weiteren Konfigurationsmöglichkeiten werden im Abschnitt <u>"Zusätzliche Einstellungen bei Whitelist-Regeln</u> <u>konfigurieren</u>" beschrieben.

3.1.2.3.4 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.



Optionen	CD/DVD		Befehle
Allgemein	Filter / Schattenk.	1	Nachrichten
)-ROM-Laufwerke © Erlauben © Sperren für al	le Benutzer (Standard)		
Sperren, aber Benutzer or	der Gruppe	Lesen	Schre
Somane Source Drive Lo	en-Benutzer ckAdmins	N	
Hinzufügen	Entfemen		

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.

ScenterTools DriveLock		
Datei Aktion Ansicht ?		
🗢 🔿 🙎 🞇 🕞 📓 🐻		
 DriveLock Standard Policy - Zentral gespe Globale Einstellungen Laufwerke Sperr-Einstellungen Sperr-Einstellungen Matorisierte Medien Autorisierte Medien Anwendungen Verschlüszelung Verschlüszelung Management-Konsole 	Hersteller ID / Regel Produkt ID / Bedingung Status Regel-Typ Bemerkung Geben Sie Text Geben Sie Text hier ein Geben Sie T Geben Sie Text hier ein Whitelist-Regel-V AV GUB Flash Disk Gespert, Versc Laufwerks-Regel DriveLock Stick für Erzw. Verschlü GELEXAR JUMPDRIVE SECURE Gespert, Versc Laufwerks-Regel DriveLock Stick für Erzw. Verschlü Medien mit defin S12 MB - 1024 MB Gespert Laufwerksgröß CD-ROM-meter Basistregel	
۲ <u>اا</u>		
Wenn aktiviert, wird die Registerseite "CD/DVD	" angezeigt.	
· · · · · · · · · · · · · · · · · · ·		

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".



Allgemein Filter / Schattenk. Nachrichten Optionen CD/DVD Befehle DVD-Brennen wird über die Schreib-Rechte auf der Seite "Allgemein" für ezu jede CD/DVD-Brennsoftware kontrolliert. Bit beachten Sie das dduch für eine Liste der unterstützten Software. CD/DVD-Brennsoftware kontrolliert. Bit handbuch für eine Liste der unterstützten Software. nn Brennen blockiert ist, wird der CD/DVD-Brenner dem Benutzer in seiner ware nicht mehr angezeigt ("Soft-Blocking"), sollte eine Software trotzdem inen wollen, wird dies mit "Zugriff verweiget" verhindet ("Hard-Blocking") m-Einstellungen Wenn Brennen blockiert ist, wird der CD/DVD-Brennsoftware kontrolliert. Bit Handbuch für eine Liste der unterstützten Software soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) (seine Benutzerbenachrichtigungen anzeigen n Windows XP eingebaute Brennfunktion abschalten (mmer) Wein Brenzen dei Wis zustand ändem (letztes Zeichen wird "=" wenn Brenutzer gespert ist fersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "=" wenn Brenutzer gespert ist	Filter / Schattenk.
Optionen CD/DVD Befehle Nachrichten Optionen CD/D (DVD-Brennen wird über die Schreib-Rechte auf der Seite "Allgemein" für ezu jede CD/DVD-Brennsoftware kontrolliert. Bitte beachten Sie das idduch für eine Liste der unterstützten Software. CD/DVD-Brennen wird über die Schreib-Rechte auf nahezu jede CD/DVD-Brennsoftware kontrolliert. Bit Handbuch für eine Liste der unterstützten Software. nn Brennen blockiert ist, wird der CD/DVD-Brenner dem Benutzer in seiner ware nicht mehr angezeigt ("Soft-Blocking"), sollte eine Software trotzdem nem wollen, wird dies mit "Zugriff verweigert" verhindet ("Hard-Blocking") mr-Einstellungen Wenn Brennen blockiert ist, wird der CD/DVD-Brenner Soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) Keine Benutzerbenachrichtigungen anzeigen in Windows XP eingebaute Brennfunktion abschalten (mmer) Soft-Blocking deaktivieren (CD/DVD-Brenner nicht versteenen wollen, wird dies mit "Zugriff verweigert" ver Soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) Soft-Blocking deaktivieren (CD/DVD-Brenner nicht versteenen wollen, wird dies mit "Zugriff verweigert" ver Soft-Blocking deaktivieren (CD/DVD-Brenner nicht versteenen wollen, wird dies mit "Zugriff verweigert" ver Soft-Blocking deaktivieren (CD/DVD-Brenner nicht versteenen wollen, wird dies mit "Zugriff verweigert" ver Soft-Blocking deaktivieren (CD/DVD-Brenner nicht versteenen wollen, wird dies mit "Zugriff verweigert" ver Benutzer und Support-Informationen Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemelde- en Benutzer gespert ist Mindows XP eingebaute Brennfunktion absch Hersteller-Informationen je nach Zustand ändem wenn Brennen erdault sonst "d")	
 ∠DVD-Brennen wird über die Schreib-Rechte auf der Seite "Allgemein" für nezu jede CD/DVD-Brennsoftware kontrolliert. Bitte beachten Sie das nabuch für eine Liste der unterstützten Software. cD/DVD-Brennsoftware kontrolliert. Bitte beachten Sie das nabuch für eine Liste der unterstützten Software. cm Brennen blockiert ist, wird der CD/DVD-Brenner dem Benutzer in seiner tware nicht mehr angezeigt ("Soft-Blocking"), sollte eine Software trotzdem Software nicht mehr angezeigt ("Soft-Blocking"), sollte eine Software trotzdem Software nicht mehr angezeigt ("Soft-Blocking"), sollte eine Software trotzdem Software nicht mehr angezeigt ("Soft-Blocking"), sollte eine Software nicht mehr angezeigt ("Soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) Keine Benutzerbenachrichtigungen anzeigen In Windows XP eingebaute Brennfunktion abschalten (immer) nutzer- und Support-Informationen — Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemeldeten Benutzer gespent ist Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "=" wenn Brennen erdel wits sont "#") 	DVD Befehle
enn Brennen blockiert ist, wird der CD/DVD-Brenner dem Benutzer in seiner ftware nicht mehr angezeigt ("Soft-Blocking"), sollte eine Software trotzdem ernen wollen, wird dies mit "Zugriff verweigert" verhindert ("Hard-Blocking") err-Einstellungen Soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) Keine Benutzerbenachrichtigungen anzeigen In Windows XP eingebaute Brennfunktion abschalten (immer) nutzer- und Support-Informationen Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemelde- ten Benutzer gespent ist Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "="	uf der Seite "Allgemein" fü itte beachten Sie das 4.
berr-Einstellungen Sperr-Einstellungen Soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) Soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) Keine Benutzerbenachrichtigungen anzeigen Soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) In Windows XP eingebaute Brennfunktion abschalten (immer) Keine Benutzerbenachrichtigungen anzeigen In Windows XP eingebaute Brennfunktion abschalten (immer) In Windows XP eingebaute Brennfunktion abschalten (immer) Benutzer- und Support-Informationen Benutzer- und Support-Informationen Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemeldeten Benutzer gespert ist Hardware-Revision zu "Lock" ändem, wenn Brenzen erdault sont "#") Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "=" W Hersteller-Informationen je nach Zustand ändem	nner dem Benutzer in sein ollte eine Software trotzde verhindert ("Hard-Blocking
Soft-Blocking deaktivieren (CD/DVD-Brenner nicht verstecken) Keine Benutzerbenachrichtigungen anzeigen In Windows XP eingebaute Brennfunktion abschalten (immer) enutzer- und Support-Informationen Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemeldeten Benutzer gespent ist Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "=" wenn Brennen erlauft sonst "#")	
Keine Benutzerbenachrichtigungen anzeigen In Windows XP eingebaute Brennfunktion abschalten (immer) enutzer- und Support-Informationen Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemeldeten Benutzer gespent ist Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "="" wenn Brennen endault*")	icht verstecken)
In Windows XP eingebaute Brennfunktion abschalten (immer) Image: Windows XP eingebaute Brennfunktion abschalten (immer) enutzer- und Support-Informationen Benutzer- und Support-Informationen Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemeldeten Benutzer gespent ist Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemeldeten Benutzer gespent ist Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "="" wenn Brennen endault sond "#") Image: Windows XP eingebaute Brennfunktion abschalten (mersteller-Informationen in the sond "#")	
enutzer- und Support-Informationen Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemelde- ten Benutzer gespent ist Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "=" wenn Brennen efaultet sonst "#") Benutzer und Support-Informationen Hardware-Revision zu "Lock" ändem, wenn Bre ten Benutzer gespert ist Wenn Brennen efaultet sonst "#")	halten (immer)
Hardware-Revision zu "Lock" ändem, wenn Brennen für den angemelde- ten Benutzer gespert ist Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "=" Wenn Brennen edaubt sonst "#") wenn Brennen edaubt sonst "#")	
Hersteller-Informationen je nach Zustand ändem (letztes Zeichen wird "=" Wenn Brennen edaubt sonst "#") wenn Brennen edaubt sonst "#")	ennen für den angemelde
	n (letztes Zeichen wird "=
ompatibilitäts-Optionen Kompatibilitäts-Optionen	
CD/DVD-Schreiboperationen nicht filtem (Brennen nicht sperren)	nen nicht sperren)
Low-level-Gerätetreiber nicht filtem	

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.



3.1.2.3.5 Laufwerkslisten-Regel erstellen

🦪 DriveLock	Herst	eller	ID / Regeltyp		Produkt IE) / Bedingung			Serienni
Device Scanner	Gebe	n Sie	Text hier ein	7	Geben Sie	Text hier ein	<	7	Geben S
 Produktaktualisierung und Support Lokale Computer-Richtlinie Globale Einstellungen Laufwerke Einstellungen 	₩ ₩ Cr	hiteli: iveLo	st-Regel-Vorlagen ock Laufwerke	_	Zugelasse	ne DriveLock Laufv	verke		
Geräte-Regel			Neu		•	1			
Laufwerkslisten-Regel			Liste exportieren						
Netzwerklaufwerk-Regel									
WebDAV-Netzwerklaufwerk-Regel			Ansicht		•				
Gerätegröße-Regel			Symbole anordne	n	•				
Verschlüsselte Medien-Regel			Am Raster ausrich	nter	n				
Basis-Regel			Eigenschaften						
Terminaldienste-Regel			Hilfe						
Regel aus Vorlage		-		_		1			
Ordner									
Hardware-ID-Regel									
📑 Richtlinien									

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



Nachrichten Verschlüsselung Optionen Befehle Allgemein Zugriffsrechte Filter / Schattenk. Zeiten Computer Beschreibung DriveLock Laufwerke	Netzwerke	e Be	nutzer	La	ufwerke		Awarene	ss
Allgemein Zugriffsrechte Filter / Schattenk. Zeiten Computer Beschreibung DriveLock Laufwerke Laufwerksliste Zugelassene DriveLock Laufwerke Es wurde eine Laufwerkslisten-Regel für alle Laufwerke mit einem passender Eintrag in der gewählten Laufwerksliste gewählt. Komment: Alle DriveLock SE intem zugelassenen Laufwerke	Nachrichte	n Ve	rschlüsselu	ng	Optio	nen	Befeł	nle
Beschreibung DriveLock Laufwerke Laufwerksliste Zugelassene DriveLock Laufwerke Es wurde eine Laufwerkslisten-Regel für alle Laufwerke mit einem passender Eintrag in der gewählten Laufwerksliste gewählt. Komment: Alle DriveLock SE intern zugelassenen Laufwerke	Algemein	Zugriffsrech	nte Filte	r / Schi	attenk.	Zeiter	Comp	outer
Laufwerksliste Zugelassene DriveLock Laufwerke Es wurde eine Laufwerkslisten-Regel für alle Laufwerke mit einem passender Eintrag in der gewählten Laufwerksliste gewählt. Komment: Alle DriveLock SE intern zugelassenen Laufwerke	Beschreibung	DriveLock	Laufwerke					
Laufwerksliste Zugelassene DriveLock Laufwerke Es wurde eine Laufwerkslisten-Regel für alle Laufwerke mit einem passender Eintrag in der gewählten Laufwerksliste gewählt. Komment: Alle DriveLock SE intem zugelassenen Laufwerke								
Es wurde eine Laufwerkslisten-Regel für alle Laufwerke mit einem passender Eintrag in der gewählten Laufwerksliste gewählt. Komment: Alle DriveLock SE intern zugelassenen Laufwerke	Laufwerksliste	e Désalante l	- Aundra					
s wurde eine Laufwerkslisten-Regel für alle Laufwerke mit einem passender Eintrag in der gewählten Laufwerksliste gewählt.								
Komment: Alle DriveLock SE intern zugelassenen Laufwerke	Eintrag in der	newählten La	a fundadiat	ar and i	Cool work	o mic om	om pussoi	TO OT 1
Komment: Alle DriveLock SE intern zugelassenen Laufwerke	_	QUINTER LEGIT LE	Buiwerksiist	e gewa	hlt.			
Komment: Alle DriveLock SE intern zugelassenen Laufwerke		gewaniten Et	BuiwerKsiist	e gewa	hlt.			
Komment: Alle DriveLock SE intern zugelassenen Laufwerke		gewannen L	BuiwerKsiist	e gewa	hlt.			
		gewaniten Lt	aui werk siist	e gewa	hit.			
	Komment;		ock SE inte	e gewa m zuge	hlt.	Laufwe	rke	
	Komment;	Alle DriveL	ock SE inte	e gewa m zuge	hlt. Iassenen	Laufwe	rke	
	Kommenti	Alle DriveL	ock SE inte	e gewa m zuge	hlt. Iassenen	Laufwe	rke	
	Kommenti	Alle DriveL	ock SE inte	e gewa m zuge	hlt.	Laufwe	rke	
	Kommenti	Alle DriveL	ock SE inte	m zuge	hlt. Iassenen	Laufwe	rke	
	Kommenti	Alle DriveL	ock SE inte	m zuge	hlt. Iassenen	Laufwe	rke	
	Komment;	Alle DriveL	ock SE inte	m zuge	hlt.	Laufwe	rke	
	Kommenti	Alle DriveL	ock SE inte	m zuge	hlt.	Laufwe	rke	
	Komment;	Alle DriveL	ock SE inte	m zuge	lassenen	Laufwe	rke	
	Komment;	Alle DriveL	ock SE inte	m zuge	lassenen	Laufwe	rke	
()K Abbrechen Ubernehme	Komment;	Alle DriveL	ock SE inte	m zuge	hlt.	Laufwe	rke	

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

3.1.2.3.6 Netzwerklaufwerk-Regel

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



CenterTools DriveLock			-				- 0 ×
Datei Aktion Ansicht ?							
🗢 🏟 🖄 🖾 🗟 🖬 🖬	1 8 2						
 DriveLock Standard Policy - Ze Globale Einstellungen Laufwerke Einstellungen Sperr-Einstellungen 	ntral gespe	Hersteller ID / Regel Geben Sie Text h 🌱 📆 Whitelist-Regel-V 🏐 AV 🔗 USB	Produkt ID / Beding Geben Sie Text h 🍸 Flash Disk	Status Geben Sie T 🍸 Gespert, Versc	Regel-Typ Geben Sie T 🍸 Laufwerks-Regel	Bemerkung Geben Sie Text hier ein	
(aufwerks-Whitelist-Ewhitelist-Ewhitelist-Vorlagen Grate Autorisierte Medien Autorisierte Medien Anwendungen Verchlüsselung Anwendungen Anwen	Ansich Liste er Eigens Hilfe	t	Geräte-Regel Netzwerklaufwerk-Rr WebDAV-Netzwerkla Gerätegröße-Regel Basis-Regel Terminaldienste-Reg Regel aus Vorlage Ordner	egel ufwerk-Regel el	verks-Regel		
Erstellt ein neues Objekt in diesem (Container.						

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

		Vetzwerke	Benutzer	Optionen
Allgemein	Zugi	iffsrechte	Filter / Schattenk.	Zeiten
Server	DLSERV	ER		
Freigabe	DriveLoc	k		
Bemerku <mark>n</mark> g				
Symbol	0.	•		

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



letzwerkfreigabe auswählen	
🔺 📬 Netzwerk	
▲ 🜉 DLSERVER	
DriveLock	
🖻 🎍 netlogon	
🖻 📜 sysvol	E
▷ 🖳 DLWIN7X64	
🕑 🖳 vmware-host	+
rdner: DriveLock (\DLSERVER)	

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 <u>"Zusätzliche Einstellungen bei Whitelist-Regeln</u> <u>konfigurieren</u>" beschrieben.

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

3.1.2.3.7 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.

Datei Aktion Anxicht ? Image: Status Regel-Typ Bemerkung Geben Sie Text h Geben Sie T Geben Sie T Image: Status Regel-Typ Bemerkung Image: Status Geben Sie Text h Geben Sie T Geben Sie T Image: Status Geben Sie Text h Geben Sie T Geben Sie Toxt hier ein Image: Status Status Gegent Versc Laufwerks-Regel Image: Status Status Gegent Versc Laufwerks-Regel Image: Status Neuwerkspröfie USB Flash Disk Gegent, Versc Laufwerks-Regel Image: Neuwerkspröfie Neuwerkspröfie Neuwerkspröfie Neuwerkspröfie Gestats: Regel Image: Neuwerkspröfie Hilfe Hilfe Terminadimste-Regel Regel aus Vorlag Image: Neuwerkspröfie Hilfe Regel aus Vorlag Ordner Ordner Image: Neuwerkspröfie Hilfe Regel aus Vorlag Ordner Ordner Image: Neuwerkspröfie Hilfe Regel aus Vorlag Ordner Ordner Image: Neuwe	CenterTools DriveLock			x
Image: Second	Datei Aktion Ansicht ?			
DriveLock Standard Policy - Zentral geper Hersteller ID / Regel Produkt ID / Beding Status Regel Typ Bemerkung Geben Sie Test h Ceben Sie Test h Geben Sie Test h Gestegrieße-Regel Gerate-Regel Gerate-Regel Basin Regel aus Vorlage Ordner Gerate-Regel Regel aus Vorlage Ordner	🗢 🔿 🖄 🔝 🗟 🖬 🕷	3 🗩		
Datefilier-Voltagen Ansicht Ansicht Ansicht Geräte experiment. Gerätes Regel Gerä	DriveLock Standard Policy - Zentral g Ø Globale Einstellungen Gebale Einstellungen Geser-Einstellungen Ser-Einstellungen O Laufwerks-Whitelist-Reaeln	gespe Hersteller ID / Regel Geben Sie Text h GW Whitelist-Regel-V. WSB	Produkt ID / Beding Status Regel-Typ Bemerkung Ø Geben Sie Text h Ø Geben Sie T Ø Geben Sie Text hier ein " Flash Disk Gesperrt, Versc Laufwerks-Regel DriveLock Stick für Erzw. Verschlü	
Ansicht Ansicht Netwerkaurwerk-Regel Gerätersteinen Ansicht Liste exportieren Gerätegröße-Regel Basis-Regel Regel aus Vorlage Ordner *	Dateifilter-Vorlagen	Neu 🕨	Geräte-Regel	
Netzwekprofile Anwendungen Grätegröße-Regel Gerätegröße-Regel Basis-Regel Regel aus Vorlage Ordner Tertellt ein neues Objekt in diesem Container.	⊳ 🗗 Geräte	Ansicht 🕨	Netzwerklautwerk-Regel	
Verschlüsselung Antivirus Management-Konsole File Hilfe Basis-Regel Regel aus Vorlage Ordner Tertellt ein neues Objekt in diesem Container.	▷ 1 Netzwerkprofile L ▷ ③ Anwendungen	Liste exportieren	Gerätegröße-Regel	
Management-Konsole Hife Hife Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel ternulaldenste-Kegel Regel aus Vorlage Ordner ternulaldenste-Kegel tern	Verschlüsselung E	Eigenschaften	Basis-Regel	
Indersor Conlige Ordner	Anuvirus Management-Konsole	Hilfe	Terminaldienste-Regel	
III III Erstellt ein neues Objekt in diesem Container.			Ordner	
Erstellt ein neues Objekt in diesem Container.	<	•		
	Erstellt ein neues Objekt in diesem Conta	ainer.		

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



Computer	Netzwerke	Benutzer	Optionen
Allgemein	Zugriffsrechte	Filter / Schattenk.	Zeiten
Server-URL h	ttps://mediacenter.gm	x.net	
Bemerkung V	VebDAV Laufwerk GN	IX Mediacenter	
Symbol	? •		

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

Die weiteren Konfigurationsmöglichkeiten werden im Abschnitt <u>"Zusätzliche Einstellungen bei Whitelist-Regeln</u> <u>konfigurieren</u>" beschrieben.

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

3.1.2.3.8 Gerätegröße-Regel

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



CenterTools Drivel ock								0 <u></u> X
Datai Altion Ancisht 2								
		ล						
DriveLock Standard Policy - Zer Globale Einstellungen	ntral gespe	Hersteller ID / Regel	Produkt ID / Beding	Status	Regel-Typ	Bemerkung	-1	
∠ → Laufwerke		Geben Sie Text h Y	Geben Sie Text h Y	Geben Sie T 🍸	Geben Sie T 🍸	Geben Sie Text hier ein	1	
instellungen		Whitelist-Regel-V						
Sperr-Einstellungen	ala	USB	Flash Disk	Gesperrt, Versc	Laufwerks-Regel	DriveLock Stick für Erzw. Verschlü		
Dateifilter-Vorlagen	Neu	•	Geräte-Regel		verks-Regel			
Autorisierte Medien	Ansich		Netzwerklaufwerk-Re	gel				
Fill Geräte	Ansien	. ,	WebDAV-Netzwerkla	ufwerk-Regel				
▷ ▲ Anwendungen	Liste ex	cportieren	Gerätegröße-Regel					
Verschlüsselung	Eigense	chaften	Basis-Regel					
Management-Konsole	Hilfe		Terminaldienste-Reg	el				
p eg management konsole			Regel aus Vorlage					
		_	Oraner					
Costallitaria annua Obialitaria dianan C	•							
Erstellt ein neues Objekt in diesem C	ontainer.							

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

	e Benutzer	Lauf	werke	Nachrichten	Optione	n Befehle
Allgemeir	Zugriffsre	echte	Filter	/ Schattenk.	Zeiten	Computer
F	iteuert Gerätez st die Größe in Regel aktiviere	rugriff ar nerhalb n, wenn	hand d des Ben Gerät g	er Größe des G eiches, wird die rößer als (>=)	erätes. e Regel akt 512	tiviert.
			und	kleiner als (<)	1024	
F	emerkung					
	111 428 10 829	82 62				
)iese Regel für	Laufwe	rke akti	vieren, die ver	b <mark>unden s</mark> in	d über:
)iese Regel für	· Laufwe wire)	irke akti	vieren, die verl	bunden sin	d über:
)iese Regel für	Laufwe wire)	erke <mark>akt</mark> i	vieren, die verl	bunden sin	d über:
)iese Regel für	Laufwe wire) ≦	irke akti	vieren, <mark>d</mark> ie verl	bunden sin	d über:

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 <u>"Zusätzliche Einstellungen bei Whitelist-Regeln</u> <u>konfigurieren</u>" beschrieben.

3.1.2.3.9 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.



Netzwerke	Benutzer	Laufwerk	e Nachrichter	Optioner	Befehle
Allgemein	Zugriffsred	hte Fil	er / Schattenk.	Zeiten	Computer
Ver bes Ger	iniert eine Ba schlusses. wenden Sie e chränkungen ätetyp oder -a	sis-Regel a ine solche angeben v anschluss	nhand des Gerät Regel, wenn Sie vollen. Diskettenla	etyps bzw. Zeit-oder Co ufwerke	omputer-
Ben	nerkung		CD-ROM-L	urwerke aufwerke	Â
			USB-anges Firewire (13 SD-Karten- Andere We Festplatten Verschlüsse Netzwerk-L WebDAV-N	ichlossene La 194) angesch Laufwerke (S ichseldatentri (eSATA, nich elte Laufwerk aufwerke letzwerklaufv	autwerk lossene SD-Bus) äger ht wech te werke ↓
					<u>.</u>

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 <u>"Zusätzliche Einstellungen bei Whitelist-Regeln</u> <u>konfigurieren</u>" beschrieben.

3.1.2.3.10 Terminaldienste-Regel

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

3.1.2.3.11 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.



CenterTools DriveLock							- 0 X
Datei Aktion Ansicht ?							
♦ ♦ 2 0 0 0 0 0 0 0]					
 DriveLock Standard Policy - Ze Globale Einstellungen Eaufwerke Einstellungen E	entral gespe	Hersteller ID / Regel Geben Sie Text h Whitelist-Regel-V AV USB	Produkt ID / Beding Geben Sie Text h 🍸 Flash Disk	Status Geben Sie T 🍸 Gesperrt, Versc	Regel-Typ Geben Sie T 🍸 Laufwerks-Regel	Bemerkung Geben Sie Text hier ein	
Dateifilter-Vorlagen	Neu	•	Geräte-Regel		verks-Regel		
Autorisierte Medien Øeräte Netzwerkprofile Anwendungen	Ansicht Liste exp	>	Netzwerklaufwerk-Re WebDAV-Netzwerkla Gerätegröße-Regel	egel ufwerk-Regel			
Antivirus Management-Konsole	Hilfe		Terminaldienste-Reg Regel aus Vorlage Ordner	el			
Erstellt ein neues Objekt in diesem	Container.						
	an an connul						

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 <u>"Zusätzliche Einstellungen bei Whitelist-Regeln</u> <u>konfigurieren</u>" beschrieben.

DriveLock	Herst	eller I	D / Regeltyp	_	Produkt ID) / Bedingung		Serienni
 Produktaktualisierung und Support Dokale Computer-Richtlinie Globale Einstellungen Laufwerke Einstellungen 	Geber	n Sie hitelis iveLo	Text hier ein st-Regel-Vorlagen ck Laufwerke	7	Geben Sie Zugelasse	Text hier ein ne DriveLock Laufwerke	4	Geben S
Geräte-Regel			Neu		•	1		
Laufwerkslisten-Regel			Liste exportieren					
Netzwerklaufwerk-Regel								
WebDAV-Netzwerklaufwerk-Regel	Ansicht •							
Gerätegröße-Regel			Symbole anordne	n	•			
Verschlüsselte Medien-Regel			Am Raster ausrich	nter	n			
Basis-Regel			Eigenschaften					
Terminaldienste-Regel			Hilfe					
Regel aus Vorlage		-		_		1		
Ordner								
Hardware-ID-Regel								
📑 Richtlinien								

3.1.2.3.12 Hardware-ID-Regel



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

	Eige	enschafte	en vo	n Ne	ue Aus	nahr	ne	?	×	
Netzwerk	e	Benutz	er	La	ufwerke		Av	warene	ess	
Nachrichte	en	Verschlüsselur			ng Optionen			Befehle		
Allgemein	Zugr	iffsrechte	Filter	/ Schattenk. Zeiter			en	n Computer		
Hardware-ID										
Diese Art vor "USBSTOR\ Migration vor Bemerkung	n Rege Disk Ve n ander	In basiert au endor_Produ ren Endgerä	f der V uct'') ur itesiche	Vindow nd dien erheitslo	s-Hardwa t der Kom ssungen a	are-ID apatibil auf Dr	(z.B. lität be iveLo	ei der ck.		
Symbol	9	~								
Nur defini	erte Se	riennummer	n zulas	sen						
Serienn	ummer	Ber	nerkun	g			Hin	zufüge	en	
				_			Bea	intferne arbeite	en	
			Oł	(Abbre	echen		Übem	ehmen	

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.

3.1.2.3.13 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.



3.1.2.3.13.1 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.

	Benutzer	Laufwerke	Nachrichten	Optionen	Befehle
Allgemein	Zugriffsred	hte Filter	/ Schattenk.	Zeiten	Computer
Einstellun	igen von "Sp en filtern kollieren und	err-Einstellung Schattenkopi	jen" verwender ie t Einstellungen i	l	-
Reihe	. Filtervorla	ge	t Einstellungen i	ulesel vollag	c
1 2	Alle Office Zertifikat-	e Dokumente Dateien erlaut	pen		
Hinzufü	igen	ntfemen			•

Wenn Sie einen eigenen Filter angeben möchten, deaktivieren Sie "Einstellungen von "Sperr-Einstellungen" 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 述, 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.

3.1.2.3.13.2 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.



Allgemein	Zugriffsred	hte	Filter .	/ Schattenk.	Zeiten	Computer
Vetzwerke	Benutzer	Laufwerke		Nachrichten	Optioner	Befehle
Buchstab	e von verbu	ndene	n Laufw	erken ändern a	uf ersten Fr	eien aus:
A:						*
B:						
D:						
E:						
📝 F:						
G :						E
H:						
K:						
E L:						
M :						
V N:						
0:						
Q:						
R :						*
-					0.024	

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

3.1.2.3.13.3 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.



	Eigenschaft	ten von Lexa	ar	? ×					
Allgemein Zu	griffsrechte Filte	r / Schattenk.	Zeiten	Computer					
Netzwerke	Benutzer	Laufwerke	1	Awareness					
Nachrichten	Verschlüsselu	ng Optic	onen	Befehle					
Speziellen Tex	bei Benutzerbenad	hrichtigung anze	eigen						
Benutzerinformation wenn diese Regel aktiviert wird									
Bitte beachten Sie unsere Datenschutzbestimmungen.									
Bitte beachten Sie unsere Datenschutzbestimmungen.									
Benachrichtigu	ng anzeigen wenn	Zugriff erlaubt wi	ird						
Keine Benachr	ichtigung anzeigen	(Laufwerk ignorie	eren)						
Keine Ereigniss	e für dieses Laufwe	erk erzeugen							
	0	K Abbr	echen	Ü <u>b</u> ernehmen					

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.



Eigenschaften von Lexar ? ×												
Allgemein Zug	iffsrechte Fi	ter / Sch	attenk.	Zeiten	Computer							
Netzwerke	Benutzer	La	aufwerke	1	Awareness							
Nachrichten	Nachrichten Verschlüsselung Optionen											
 Speziellen Text bei Benutzerbenachrichtigung anzeigen Benutzerinformation wenn diese Regel aktiviert wird Bitte beachten Sie unsere Datenschutzbestimmungen. 												
Bitte beachten Sie unsere Datenschutzbestimmungen. Mehrsprachige Benachrichtigung												
E Nachri	cht löschen											
K Nachri	cht testen											
Keine Ereignisse	TUP DESES LAUP	werk erze	ugen									
		ок	Abbre	echen	Ü <u>b</u> ernehmen							

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".

3.1.2.3.13.4 Weitere Optionen

Verschlüsselung

Mit Hilfe der Reiters "Verschlüsselung" können Sie Einstellungen zur erzwungenen Verschlüsselung festlegen.



Eigenschafte	n von	Lexar						?	Х
Netzwerk	e	Benutz	er	La	ufwerke		A	waren	ess
Allgemein	Zugi	riffsrechte	Filte	r / Scha	ttenk.	Zei	iten	Cor	nputer
Nachrichte	n	Verschl	üsselu	ng	Optio	nen	Befehle		
Verschlüs	selung	erzwingen							
Unvers	schlüss	selte Laufwe	rke au	tomatis	ch versch	lüsse	In		
B	eim ers	sten Schreib	zugriff	verschli	isseln				
Strenger Test auf verschlüsseltes Medium (nur DriveLock-Dateien dürfen vorhanden sein)									
Versch	Verschlüsselte Medien nicht automatisch verbinden								
🔥 Kor	figurie	ren Sie: Ver	schlüss	elung	Erzw	unge	ene V	erschl.	
		-							
			0	ĸ	Abbr	echer	n	Übern	ehmen

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.



Eigenschafte	n von Le:	xar					?	×	
Netzwerk	е	Benutz	ter	L	aufwerke		Awaren	less	
Allgemein	Zugriffs	rechte	Filter	r / Scha	attenk.	Zeiten	Co	mputer	
Nachrichte	n	Versch	lüsselur	ng	Optic	onen	Befehle		
Medien-Autorisierung erforderlich (Nur CD/DVD-Laufwerke) Ausnahmen für Laufwerkstyp und -buchstabe Diese Regel nicht anwenden bei Laufwerken vom Typ CD/DVD-ROM Festplatte Wechseldatenträger Diese Regel nicht anwenden bei Laufwerksbuchstaben A: C: E: G: B: D: F: H:									
<								>	
Aktionen beir	n Verbinde	en —							
System ü	berprüfen,	bevor Z	ugriff a	uf Lauf	werk gew	ahrt wird			
Тур	Beschre	eibung							
							Hinzufi	ügen	
							Bearbe	eiten	
							Löso	hen	
			0	ĸ	Abbr	echen	Überr	nehmen	

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

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.



Bes	hreibung
Ber	utzer überprüfen
Ner	n ein Laufwerk verbunden wird, überprüfen ob
01	Vindows-Dienst gestartet ist
0	ateisystem-Filter mit Laufwerk verbunden ist
@ E	enutzerdefinierte Befehl "Erfolg" zurückmeldet Befehlszeile
	%FILESTG%*CheckUserParam.cmd
	Der Rückgabecode des Befehls muss Null für Erfolg und Nicht-Null im Fehlerfall sein

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.

3.1.2.3.13.5 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



	Zugriffsreck	nte Filter	/ Schattenk.	Zeiten	Computer
Netzwerke	Benutzer	Laufwerke	Nachrichten	Optionen	Befehle
Befehl au	sführen, wenr	n Laufwe <mark>r</mark> k v	e <mark>rbunde</mark> n und g	espent wird	
Dereniaz	Gile				
🔲 Im Be	enutzerkontex	t ausführen (Interaktiver Ben	utzer)	
Defeld av	-f"leave wave	- I - Annale in	والمراجعة والمراجعة	-	4
Defeniau	stunren, went	n Laurwerk v	erbunden und n	icht gespen	t wird
VEU EC		Lleer Derem			
AFILE3		euserralam.	und		<
Im Be	enutzerkontex	t ausführen (Interaktiver Ben	utzer)	
Befehl au	sführen, wenr	n Laufwerk g	etrennt wird		
Befehlsz	eile				
Coronioz] <] []
	enutzerkontex	t ausführen (Interaktiver Ben	utzer)	
I Im Be				,	
i im Be					
m Be					

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

Nigemein	Zugriffsred	chte F	ilter / Schattenk.	Zeiten	Computer	
letzwerke	Benutzer	Laufwer	ke Nachrichten	Optionen	Befehle	
Befehl au	usführen, wen	nn Laufwe	rk verbunden und g	espent wird		
Befehlsz	zeile					
					<	
Im Be	enutzerkonte	xt ausführ	en (Interaktiver Ben	utzer)	19 - 25 H - Ch	
Defelel av	of these was	un laufuun	de under medane under	isht saasaat		
Defet	usiuniren, wen	IT Laurwe	ik verbunden und n	icht gespen	WIG	
VEILEC	tene TG?*Ued⇒	tal learPar	am omd			
70FILE3		leuserrai	am.cmu		2	In den Text einfügen
	anutzarkonta	xt austuhr	en (Interaktiver Ben	utzer)		en a general en
Im B	CHULZCIKONIC		1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1			Laufwerksbuchstabe
Befehl au	usführen, wer	nn L <mark>au</mark> fwe	rk getrennt wird		9	Laufwerksbuchstabe Laufwerkgröße (Bytes)
Befehl au Befehlsz	usführen, wer zeile	nn L <mark>au</mark> fwe	rk getrennt wird		ł	Laufwerksbuchstabe Laufwerkgröße (Bytes) Produkt-ID
Befehl au Befehlsz	usführen, wer zeile	nn Laufwe	rk getrennt wird		र	Laufwerksbuchstabe Laufwerkgröße (Bytes) Produkt-ID Hersteller-ID
Befehl au Befehlsz	usführen, wer zeile enutzerkonte	nn Laufwe xt ausführ	rk getrennt wird en (Interaktiver Ben	utzer)	<	Laufwerksbuchstabe Laufwerkgröße (Bytes) Produkt-ID Hersteller-ID Seriennummer
Befehl au Befehlsz	usführen, wer zeile enutzerkonte	nn Laufwe	rk getrennt wird en (Interaktiver Ben	utzer)	<	Laufwerksbuchstabe Laufwerkgröße (Bytes) Produkt-ID Hersteller-ID Seriennummer
Befehl au Befehlsz	usführen, wer zeile enutzerkonte	nn Laufwe	rk getrennt wird en (Interaktiver Ben	utzer)	<.	Laufwerksbuchstabe Laufwerkgröße (Bytes) Produkt-ID Hersteller-ID Seriennummer Anzeigename
inweis: Um	skripte (VBS	n Laufwe xt ausführ 5, JS) ausz	rk getrennt wird en (Interaktiver Ben zuführen, benutzen	utzer) Sie die Befe	< hlszei	Laufwerksbuchstabe Laufwerkgröße (Bytes) Produkt-ID Hersteller-ID Seriennummer Anzeigename Benutzername

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.



3.1.2.4 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.

3.1.2.4.1 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.



CenterTools DriveLock				
Datei Aktion Ansicht ?				
🗢 🔿 🖄 🛅 🗟 👔	8 2	•		
BriveLock Standard Policy -	Zentr <mark>al g</mark> espe	Dateierweiterung	en Bemerkung	*
👂 🧼 Globale Einstellungen		Geben Sie Text hie	er ein 🌱 Geben Sie Text hier ein 🌱	
⊿ 📾 Laufwerke		386	Erzeugt von vordefiniertem Inhalt	
Einstellungen		ACCDB	Erzeugt von vordefiniertem Inhalt	
Sperr-Einstellungen	Pagala	ACCDE	Erzeugt von vordefiniertem Inhalt	
A Dateifilter-Vorlagen	Regelli	ACCDR	Erzeugt von vordefiniertem Inhalt	=
Datei-Typdefir***		ACCDT	Erzeuat von vordefiniertem Inhalt	
🜍 Dateitypen-Gr	Neu	•	Datei-Typdefinition lefiniertem Inhalt	
Autorisierte Medi	Alle Aufgal	ben 🕨	Erzeugt von vordefiniertem Inhalt	
▶ 10 Geräte	Andrew		Erzeugt von vordefiniertem Inhalt	
Netzwerkprofile	Ansicht		Erzeugt von vordefiniertem Inhalt	
▷ Anwendungen	Liste export	tieren	Erzeugt von vordefiniertem Inhalt	
Verschlüsselung	.		Erzeugt von vordefiniertem Inhalt	
Antivirus	Eigenschaf	ten	Erzeugt von vordefiniertem Inhalt	
p my Management-Konsol	Hilfe		Erzeugt von vordefiniertem Inhalt	
			Erzeugt von vordefiniertem Inhalt	
		BUP	Erzeugt von vorderiniertem innait	
		CUR CURA	Erzeugt von vorderiniertem Innart	
			Erzeugt von vordenniertem Inhalt	
			Erzeugt von vordefiniertem Inhalt	
			Erzeugt von vordefiniertem Inhalt	
		DOC	Erzeugt von vordefiniertem Inhalt	
		DOT	Frzeugt von vordefiniertem Inhalt	
		DSS	Erzeugt von vordefiniertem Inhalt	
		DWG	Erzeugt von vordefiniertem Inhalt	
		EXE	Erzeugt von vordefiniertem Inhalt	
		FLT	Erzeugt von vordefiniertem Inhalt	
		🔢 GIF	Erzeugt von vordefiniertem Inhalt	
		👫 GZ	Erzeugt von vordefiniertem Inhalt	
<	۲	ICO 📑	Erzeugt von vordefiniertem Inhalt	+
Erzeugt eine neue Datei-Typdefir	nition für den I	nhaltsfilter.		

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.

	Typdefinit	tion Test	
Dateitypde	finition gült	tig für Dateiendunger	
Dateityp	Bes	chreibung	Hinzufügen
JPEG	JPE	EG Image	Entfemen
3emerkun, Erzeugt v	g on vordefin	iertem Inhaltsfilter	

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

Anschließen aktivieren Sie den Reiter Typdefinition.



	Typdefinitio	n Test			
Dateity Dateiir	rp auf Basis v nhalt wird geg	on Inhaltsprü jen <mark>s</mark> tatische	ifung erkenner Regeln geprü	n ft.	
Start	-Position	Länge	Inhalt		
C	000	3	FF D8 FF		
Hinzu	fügen)	Entfernen	Bearbeite	n]	
Beim I	nhaltstest	müssen a muss eine	lle Regeln gült der Regeln g	ig sein (AND) ültig sein (OF) ()
Dateity	p mithilfe kur	idenspezifisc	her DLL erken	inen	
~	ateipfad				
DLL-D Funkti	onsname				

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.

Startposition	0×0000	(Bytes ab Dateianfang)
Länge	4	(Bytes)
Erwarteter Inha	It ab Startposition	
🔿 Text	Ðľ≁±	
Hex-Bytes	D0 CF 1A B1	

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.

3.1.2.4.2 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.



CenterTools DriveLock							
Datei Aktion Ansicht ?							
🗢 🔿 🖄 💿 🗟 🖬 🚳 💆							
BriveLock Standard Policy - Zentral gespe	Beschreibung	Dateierweiterungen	Bemerkung				
 Globale Einstellungen Globale Einstellungen Globale Einstellungen 	Geben Sie Text hier ei	ein Y Geben Sie Text hier ein Y Geb	Geben Sie T Y				
Einstellungen	Archive Audio-Dateien	ZIP; KAK; ISO; CAB; AKJ; ACE; Z; L MP3: MP4: M4P: M4A: WMA: WA	(vordefiniert) (vordefiniert)				
Sperr-Einstellungen	Ausführbare Dateie	n EXE; SCR; PIF; DLL; BAT; COM; JS;	(vordefiniert)				
a 🎲 Dateifilter-Vorlagen	Bilder	JPG; BMP; GIF; TIFF; JPEG; PNG; T	(vordefiniert)				
Catei-Typdefinitionen	Temporäre Dateier	TMP; TEMP; .	(vordefiniert)				
Autorisierte Medier Neu	•	Dateitypen-Gruppe	(vordefiniert)				
Geräte Alle Aufg Metzwerkprofile	jaben 🕨	AVI; VOB; IFO; BOP; WMV; MPEG; VMDK: VMSN: VHD	(vordefiniert) (vordefiniert)				
Anwendungen Ansicht	•						
Verschlüsselung Of Antivirus	ortieren						
Management-Konsole Eigensch	aften						
Hilfe							
<							
Legt eine neue Dateitypen-Gruppe an, die in Da	ateifilter-Vorlagen benu	zt werden kann.					

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

Vlgemein	Verknüpfungen	
Beschreibu	ng Zertifikatsdateien	
Enthaltene	Dateitypen (Erweiterungen)	
Dateityp	Beschreibung	Hinzufügen
CER CRL CRL CRT	Security Certificate Certificate Revocation List Security Certificate Security Certificate	Entfemen
3emerkung]	

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.



Dateityp	Beschreibung	
BOSDX OTF	OpenSearch Description File OpenType Font file	
P10 P12 P7B	Certificate Request Personal Information Exchange PKCS #7 Certificates	
Р7С Р7М	Digital ID File PKCS #7 MIME Message	
P7R P7S	Certificate Request Response PKCS #7 Signature	
PARTIAL	Partial Download Dial-Up Phonebook	
PCH	Unbekannter Dateityp	-

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.

3.1.2.4.3 Neue Dateifilter-Vorlage erstellen

Datei Aktion Ansicht ?	
Beschreibung Beschreibung Beschreibung Bemerkung Gebale Einstellungen Geben Sie Text hier ein Geban Sie Text hier ein Geben Sie Text hier ein Alle Office Dokumente Alles Protokollieren Alle Strötkollieren Ausführbare Dateien blockieren und Shadow Read Betriffert-Materian Datei-Typedefinitionen	
The Dat Neu Vorlage	
Dat Ansicht Ansicht	
▷ IP Geräte Liste exportieren	
Xetzwerkp Anwendun Eigenschaften	
Werschlüss Hilfe Hilfe	
Neue Vorlage hinzufügen.	

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



Ausnahmen	Weitere	Computer	Netzwerke	Benutzer	Verknüpfungen
Allgemein	Lese-Filt	er Schr	eib-Filter	Protokoll	Schattenkopie
Vorlagenbeso	chreibung	Zertifikat-Da	teien erlaube	n	
Bemerkung					
Lesezugriff a	auf Zertifika	itsdateien.			*
					÷

Geben Sie einen Namen in das Feld "**Vorlagenbeschreibung**" und optional eine Bemerkung als Beschreibung ein. Als nächstes aktivieren Sie den Reiter **Lese-Filter**.



usnahmen Weitere Co	mputer Netzwer	ke Benutzer	Verknüpfungen	
Allgemein Lese-Filter	Schreib-Filter	Protokoll	Schattenkopie	
eim Lesen von Dateien	 Alle Endung Nur definier Definierte E Gleiche Ein 	gen erlauben te Endungen ei indungen nicht stellungen beim teien	tauben ertauben I Schreiben	
Dateityp Beschreib	ung		Hinzufügen	
			Dateiendungen. Archive Audio-Dateien Ausführbare Dat Bilder Office-Dokumer Temporäre Date Text-Dokumente	eien nte ien

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.



	Weitere Co	mputer	Netzwerk	e Ben	utzer	Verknüpfungen
Allgemein	Lese-Filter	Schn	eib-Filter	Protok	oll	Schattenkopie
Beim Lesen v	von Dateien	© A	lle Endunge ur definierte efinierte En leiche Einst	n erlaul Endun dungen ellunge	gen er nicht n beim	lauben erlauben Schreiben
Dateityp	Beschreib	ung	en von Date	len		Hinzufügen 🚽
S Gruppe	Zertifikats	dateien				Entfernen

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.



Ausnahmen	Weitere	Com	puter	Netzwer	ke	Benutzer	Verknüpfungen
Allgemein	Lese-Filt	er	Schre	eib-Filter	F	rotokoll	Schattenkopie
Beim Schreib	en von Da	teien	G	leiche Ein:	stell	ung wie bei	Lesen
			() A	ie Endung	jen to E	enaupen odupgen er	Jauban
			0.0	efinierte F		nden nicht	edauben
Definierte Da	teienduna	en hei	m Sch	reiben von	D=	teien	enadber)
Dateityp	Besch	reibur	ng				Hinzufügen 👻
Gruppe	Zertifi	catsda	ateien				Entfernen
							… Einge- bauter
	20.0422	10.00	1.000	6 ·····	15.	1	Inhaltsfilter

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.



Ausnahmen	Weitere	Computer	Netzwerke	Benutzer	Verknüpfungen
Allgemein	Lese-Filt	er Schr	eib-Filter	Protokoll	Schattenkopie
Protokollierte	Dateien	C Keine			
		Alle			
		⊙ Vom W	echseldater	träger gelese	ne Dateien
		O Zum W	echseldater	träger gesch	iebene Dateien
Protokollierte	Zustände	Alle			
) Erfolg 🛞	erlaubter Zu	griff)	
) Fehler (verweigertei	Zugriff)	

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 <u>"Schattenkopien in Laufwerksregeln</u> <u>konfigurieren</u>" beschrieben.

Wählen Sie den Reiter "Weitere".



Algemein	Lese-Filt	er Schr	eib-Filter	Protokoll	Schatten	kopie
Ausnahmen	Weitere	Computer	Netzwerk	te Benutz	er Verknüp	fungen
Beim Lese	en Zugriff v	verbieten aut	f Dateien g	rößer		KB
Beim Sch	reiben Zug	riff verbieter	n auf Dateie	en größer	0	KB
Auditudetete					122	
	٦ 		0000000			
Beim Lese	ezugntt: An	chivdatelen	scannen			
	vorteosch	tato Apoleiud	a sperren			
1.001.0.14	rongesend		ateien spei	TOT		
Beim Sch	reibzugriff:	Archivdatei	en scanner	1		
Versch	nachtelte A	vchivdateier	n sperren			
Kennv	vortgeschü	tzte Archivd	lateien spei	ren		

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".



Allgemein	Lese-Filt	er Schr	eib-Filter	Protokoll	Schattenkopie
Ausnahmen	Weitere	Computer	Netzwerk	e Benutzer	Verknüpfungen
 Regel ist Regel ist Regel ist 	auf allen C nur auf gev auf gewähl	omputern ak wählten Corr ten Comput	tiv nputern akti ern nicht ak	v tiv, aber auf a	llen anderen
Compu	ter	*	1		1.000 1.00
	Server				
	Server				

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".


Augemein	Lese-Filt	ter Schr	eib-Filter	Protokoll	Schattenkopie
Ausnahmen	Weitere	Computer	Netzwerke	e Benutzer	Verknüpfungen
 Regel ist Regel ist Regel ist 	bei allen N nur bei gev bei gewähl	etzwerkverb vählten Netz ten Netzwer	indungen al werkverbind kverb. nicht	div dungen aktiv aktiv, aber b	ei allen anderen
Verbin	dung / Star	ndort			

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".



Allgemein	Lese-Filt	ter Schn	eib-Filter	Protokoll	Schattenkopie
Ausnahmen	Weitere	Computer	Netzwerk	e Benutzer	Verknüpfungen
Regel ist Regel ist Regel ist	aktiv für all aktiv nur fü bei gew. B	e Benutzeru ürgewählte B enutzem /G	und Gruppe Benutzer un ìruppen nic	n Id Gruppen ht aktiv, aber	bei allen anderen
Benutz	er oder Gru	ippe	0.00		
	CEOCICI MIN				

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.

3.1.2.4.4 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.



Optione	en	Laufwerke	Befehle
Allgemein	1	Filter / Schattenk.	Nachrichten
Dateien filte Protokollier Filter / Prot	em en und So tokoll / So	shattenkopie	an diagar Vadaga
Reihe	Filtervor	age	en uieser vonage
1	Alle Offic	e Dokumente	
Hinzufüg	en)	Entfernen	
Hinzufüg	en)	Entfemen	

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 1 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.

3.1.2.4.5 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.

3.1.2.5 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.

• 🔿 🖄 🗒 🗟 🚺 🚺	r .					
🛿 DriveLock		Beschreibung	^		Anzahl von La	Bemerkung
🔞 Device Scanner		Geben Sie Text	hier ei	in 🍸	Geben Sie T 🍸	Geben Sie Text hier ein
 	l Support ie t-Regeln	Zugelassene	e Drive	Lock Laufwerke	2	Alle von DriveLock SE zugelassene
□ Whiteist-Regention	-vonagen					
C Laufwerkslister	·					
Autorisierte M	Neu	۱.	1	Laufwerksliste		
▷ Geräte ▷ -∲- Netzwerkprofile	Ansicht	•				
Anwendungen	Liste export	ieren	I 1			
 Ø Verschlüsselung Ø DriveLock Web Se 	Eigenschaft	en				
B Security-Awarene	Hilfe		I 1			
System-Management						
Management-Konsole						
🗇 Richtlinien						
Richtlinienzuweisungen						

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



Eig	enschaften von Zugelassene DriveLock Laufwerke 🛛 ? 🛛 🗙
Allgemein Laufwer	rke Verknüpfungen
Beschreibung	Zugelassene DriveLock Laufwerke
Geräteklasse	【 Laufwerke 🗸 🗸
Kommentar	Alle von DriveLock SE zugelassenen externen Laufwerke
	OK Abbrechen Übernehmen

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.



Eigens	chaften von Zugel	assene DriveLock	Laufwerke ? ×
Allgemein Laufwerke	Verknüpfungen		
Hersteller	Produkt	Seriennummer	Bemerkung
Sony	Flash Disk Storage Media	fbf1101122200001 5a0812080001025	
Eigenschaften Ak	tivieren Hinzufügen	Entfemen Importi	eren 🔻 Exportieren 🔻
		ОК	Abbrechen Übernehmen

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.

3.1.2.6 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.



Zeiten	Computer	Netzwerke	Optionen	Befehle
Allgeme	in	Zugriffsrechte	Filter / Sc	hattenk.
Beschreibun Kommentar	9			
Regeltyp	 ◯ Jede Aux ◯ Jede Vid O Spezifisc Medien- 	dio CD eo DVD / CD hes Medium Information		*
	Medie	ninformation ciplosed		-

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.

ktuell eingelegte	e Medien	🔘 lokal	auf Agent	dlwin 7x64	Verbinden
Laufwerk	Besch	ireibung			
ØD	Medie	n-Name: CDR	OM Seriennumme	r: BUF8/EUF Anzał	11 litel:

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



Zeiten	Computer	Netzwerke	Optionen	Befehle
Allgemein		priffsrechte	Filter / Sc	hattenk.
Beschreibung	DriveLock CD			
Kommentar	DriveLock Insta	llations-CD		
Regeltyp	⊚ Jede Audio C ⊚ Jede Video D	D IVD / CD		
	Spezifisches	Medium		
	Medien-Infon	mation		
	Medien-Nam Seriennumm Anzahl Titel Anzahl Audio CDDB-Disc-I	e CDROM er B0F87E 1 p-Titel 0 ID 000000	и EOF 00	м Ш. •
	Medieninfo	ormation einlese	n	
	-			

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 "<u>Zusätzliche Einstellungen bei</u> <u>Whitelist-Regeln konfigurieren</u>" beschrieben.

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

CenterTools DriveLock	Ad address + Asylants + Martines	
Datei Aktion Ansicht ?		
🗢 🔿 🞽 🗙 🗊 🗟 🔽 🖬 🔞		
 DriveLock Standard Policy - Zentral gespe Globale Einstellungen Eusfwerke Einstellungen Sper-Einstellungen Whitelist-Regel-Vorlagen AV Hersteller-Regeln Leafwerks-Whiteler-Regeln Dattorisierte Medien Mattorisierte Medien Verschlüsselung Verschlüsselung Wanagement-Konsole 	Beschreibung Status Geben Sie Text hier ein Geben Sie T Y Drive Alle Aufgaben Freigeben Eigenschaften Hiffe	
Enthält die Aktionen, die an dem Element durch	II chgeführt werden können.	



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.

3.1.2.7 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.

3.1.2.7.1 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.



3.1.2.7.1.1 Allgemeine Einstellungen

Zentrale Speicherung	Zeiten	Netzwerke
Allgemein	Optionen	Ausnahmen
okaler Speicherort für Schatt	tenkopien (auf Agenter	ı) ———
Standard		
Speichert die Dateie	n im Benutzerprofil für a	ille Benutzer.
Fest vorgegebener P	fad	
Speicherbeschränkungen —		
Dateien mit bis zu	5000 🌲 KE	Größe kopieren
📃 Schattenkopien kopi	eren nur 1000	KB der Quelldatei
🔽 Auf Agent nicht mehr	als 100 🚔 Me	3 Platz belegen
Einstellungen für Speicherber	einigung	
Bereinigung läuft alle 5	Minuten	
Altere Dateien zuerst	Größere Dat	eien zuerst
🗾 Dateien löschen, die	älter als 0	Tage sind

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.



3.1.2.7.1.2 Client-Einstellungen für Schattenkopien

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

Zentrale Speicherung	Zeiten	Netzwerke
Allgemein	Optionen	Ausnahmen
iff auf Schattenkopien a	auf den Agenten	
📃 Lokale Freigabe au	uf allen Agenten:	
Dateien nach Uplo	ad zu zentralem Speiche	erort lokal nicht löscher
	as to contratem operate	sient fortain nont food for

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.

3.1.2.7.1.3 Ausnahmen bei Schattenkopien

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



Zentrale Speicherung	Zeiten	Netzwerke
Allgemein	Optionen	Ausnahmen
Gewählte Prozesse von So Diese Prozesse auch	chattenkopie und Protol von Dateifilter ausnehm	kollierung ausschließer en
Prozessname	Beschreibung	
DLAvScan.exe	Antivirus command li	ne utility
Hinzufügen Entfe Gewählte Benutzer von So Diese Benutzer auch	emen Bearbeiten chattenkopie und Protok von Dateifilter ausnehm	collierung ausschließe en
Hinzufügen Entfe Gewählte Benutzer von So Diese Benutzer auch Benutzer	emen Bearbeiten chattenkopie und Protok von Dateifilter ausnehm	collierung ausschließe en
Hinzufügen Entfe Gewählte Benutzer von So Diese Benutzer auch Benutzer MT AUTHORITY\S	emen Bearbeiten chattenkopie und Protok von Dateifilter ausnehm YSTEM	collierung ausschließer en
Hinzufügen Entfe Gewählte Benutzer von So Diese Benutzer auch Benutzer MT AUTHORITY\S Hinzufügen Entfe	emen Bearbeiten chattenkopie und Protok von Dateifilter ausnehm YSTEM	collierung ausschließe en

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.

Austuhrbarer Prozess	
Prozess-Datei (.EXE-Datei))
DLAvScan.exe	
Bemerkung	
Antivirus command line util	ility
Vordefinierte Anwendung	
Vordefinierte Anwendung F-Secure Antivirus	
Vordefinierte Anwendung Vordefinierte Anwendung	

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.



3.1.2.7.1.4 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.

Allgemein	Option	nen	Ausnahmen
Zentrale Speicherur	ng	Zeiten	Netzwerke
chattenkopien zu zentra	alem Speicher	ort hochladen	
Nicht hochladen			
O Zu Netzwerkfreig	gabe		
UNC-Pfad der N	letzwerkfreigal	be	
\\DLServer\Dri	veLock\Shad	ows	
Ein gültiges Ben	utzerkonto wir	d zum Hochla	den benötigt:
Benutzer	domāne\ben	utzerkennung	
Kennwort	•••••		
Bestätigung	•••••		
Dateien werden alle	60 💌	Minuten hoc	hgeladen
	ОК	Abb	rechen Überneh

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).

3.1.2.7.1.5 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.



Allgemein				1	Optio	onen			_	1	Ausr	ahm	en
Zentrale S	peicl	neru	ng	1		Z	eiter	1	[í	Ne	etzwe	erke
chladen zum	Serv	rer n	ur zu	i gei	wähl	ten Z	eiter	n					
	0	2	4	6	8	10	12	14	16	18	20	22	
Alle													
Montag													
Dienstag													
Mittwoch													
Donnerstag								Ħ	11	Ħ	ŤŤ		
Freitag													
Samstag													
Sonntag													
		© F	Rege	ak ak	tiv		Π	o F	lege	l nic	ht ak	ctiv	
	-	-					14	-					

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**".

3.1.2.7.1.6 Netzwerkeinschränkungen

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



Zentrale Speicherung Zeiten Netz Hochladen zum Server bei allen Netzwerkverbindungen Hochladen zum Server nur bei gewählten Netzwerkverbindung Hochladen zum Server nicht bei gewählten Netzwerkverbindung Verbindung / Standort Image: CenterTools	7	Optionen	Ausnahmen
Hochladen zum Server bei allen Netzwerkverbindungen Hochladen zum Server nur bei gewählten Netzwerkverbindung Hochladen zum Server nicht bei gewählten Netzwerkverbindun Verbindung / Standort CenterTools	Zentrale Speicherung	Zeiten	Netzwerke
Verbindung / Standort) Hochladen zum Server b) Hochladen zum Server n) Hochladen zum Server n	ei allen Netzwerkverbin ur bei gewählten Netzw iicht bei gewählten Netz	dungen erkverbindungen werkverbindungen
CenterTools	Verbindung / Standort	Ŧ	
Hinzufügen			

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.

3.1.2.7.1.7 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.



	Prope	erties		?	×
Allgemein	Option	nen	Au	snahmen	n
Zentrale Speicherung	Zeiten	Netzwerk	ke Ve	erschlüss	elung
Schattenkopien sind imn für den verwendeten Sc	ner verschlüselt hlüssel können	t. Zusätzliche konfiguriert	e Sicherhe werden:	itsmaßna	hmen
Keine zusätzliche Sic	herheit ("unve	rschlüsselt")			
Kennwortsicherheit					
Kennwort					
Bestätigen					
Zertifikatsbasierte Sic Öffentliche Schlüssel verwendet. Private S in Management Comp	cherheit folgender Zert chlüssel sind e	ifikate werde rforderlich, u	en zur Vers m Schatte	chlüsselu nkopien :	ung später
 Zertifikatsbasierte Sic Öffentliche Schlüssel verwendet. Private S in Management Cons Beschreibung 	cherheit folgender Zert chlüssel sind e sole zu entschlü	ifikate werde rforderlich, u isseln. Dateiname	en zur Vers m Schatte	chlüsselu nkopien :	ung später
 Zertifikatsbasierte Sic Öffentliche Schlüssel verwendet. Private S in Management Cons Beschreibung DriveLock even 	cherheit folgender Zert chlüssel sind e sole zu entschlü	ifikate werde forderlich, u isseln. Dateiname DLEventEnc	en zur Vers m Schatte	chlüsselu nkopien :	ung später
Zertifikatsbasierte Sic Öffentliche Schlüssel verwendet. Private S in Management Cons Beschreibung DriveLock even DriveLock even	cherheit folgender Zert chlüssel sind e sole zu entschlü t paramete t paramete	ifikate werde nforderlich, u isseln. Dateiname DLEventEnc DLEventEnc	en zur Vers m Schatte crypt1.cer crypt2.cer	chlüsselu nkopien :	ung später
Zertifikatsbasierte Sic Öffentliche Schlüssel verwendet. Private S in Management Cons Beschreibung DriveLock even DriveLock even DriveLock even DriveLock even	cherheit folgender Zert chlüssel sind e sole zu entschlü t paramete t paramete t paramete	ifikate werde forderlich, u isseln. Dateiname DLEventEnc DLEventEnc DLEventEnc	en zur Vers m Schatte crypt1.cer crypt2.cer crypt3.cer	chlüsselu nkopien :	ung später
Zertifikatsbasierte Sic Öffentliche Schlüssel verwendet. Private S in Management Cons Beschreibung DriveLock even DriveLock even DriveLock even DriveLock even DriveLock even DriveLock even	cherheit folgender Zert chlüssel sind e sole zu entschlü t paramete t paramete t paramete t paramete	ifikate werde rforderlich, u isseln. Dateiname DLEventEnc DLEventEnc DLEventEnc	en zur Vers m Schatte srypt1.cer srypt2.cer srypt3.cer	ichlüsselu nkopien :	ung später

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

3.1.2.7.2 Schattenkopien in Laufwerksregeln konfigurieren

Um die Erstellung von Schattenkopien zu aktivieren, muss zunächst eine Dateifilter-Vorlage erstellt werden. Bitte lesen Sie das Kapitel <u>"Neue Dateifilter-Vorlage erstellen</u>" für mehr Informationen.

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



Adananmen	Weitere C	omputer	Netzwerke	Benutzer	Verknüpfungen
Allgemein	Lese-Filter	Schn	eib-Filter	Protokoll	Schattenkopie
Schattenkop	ie 💿 Nich	t ersteller	1		
	🔘 Für a	alle Dateie	en		
	🔘 Für g	elesene	Dateien		
	Für generation wie der Genera	eschrieb	ene Dateien		
Schatten	copie nur für a	usgewäh	Ite Dateitype	en erstellen	
Keine	Schattenkopi	e fur gew	vahite Dateit	ypen (Ausnal	nmeliste)
Dateity	Besch	hreibung			Hinzufügen
					Entfernen

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.



Netzwerke	Benutzer	Laufwerke	Nachrichten	Optionen	Befehle
Allgemein	Zugriffsred	hte Filter	/ Schattenk.	Zeiten	Computer
Einstellun	gen von "Sp en filtern kollieren und	err-Einstellung Schattenkop	jen" verwenden je		
Filter / Pr	otokoll / Sch . Filtervorla	lattenkopie mi lige	t Einstellungen (dieser Vorlag	ge
1	Schatten	- kopien erzeug	ien		
Hinzufü	gen) E	intfermen		1	

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.

Eigenschaft	en von LEX	CAR			? 🔀
Netzwerke	Benutzer	Laufwerke	Nachrichten	Optionen	Befehle
Allgemein	Zugriffsrec	hte Filter.	/ Schattenk.	Zeiten	Computer
Einstellun	gen von "Sp en filtern kollieren und otokoll / Sch	err-Einstellung Schattenkopi attenkopie mi	jen" verwender ie t Finstellungen) dieser Vorla	ne
Reib	Filtervorta	atterikopie mi	(Einstellungen	ulesel voliaj	yc
Hinzufü	gen. Er	ntfernen	zulassen, Proto	Koillerung	
	<u></u>				



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.

3.1.2.7.3 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.



CenterTools DriveLock - [CenterTools DriveLock\Betrieb\Sch	attenkopien (\\DLServer\DriveLo	ck\Shadows)]		
Natei Aktion Ansicht Fenster ?				- 5 ×
CenterTools DriveLock CenterTools DriveLock CenterTools DriveLock CenterTools DriveLock CenterTools DriveLock Strain of Support CenterTools DriveLock Enterprise Services [DLServer] CenterTools DriveLock Centerprise Services [DLServer] CenterTools DriveLock Strain of Content of CenterTools DriveLock Strain of CenterTools DriveLock DriveLock Strain of CenterTools DriveLock Strain of CenterTools DriveLock Strain of CenterTools DriveLock DriveLock DriveLock DriveLock Strain of CenterTools DriveLock Driv	Dateiname Geben Sie Text hier ein Orkelock/, Zatasheet.pdf Drivelock/, Zatasheet.pdf Demo, HTML.bt Geheiminformationen.doc	Datum Zeit Größe Gebe Geb Geb Geb	Benutzer Computer Image: Seben Sie T Image: Geben Sie T Geben Sie T VMTEST/bernd DLWIN7X64 VMTEST/bernd DLWIN7X64 VMTEST/bernd DLWIN7X64 DLWIN7X64 DLWIN7X64	Gerate-Identifikation Zugriffstyp ▼ Geben Sie Text h ▼ Gebe ▼ LEXAR JUMPDRIVE Schreiben LEXAR JUMPDRIVE Schreiben LEXAR JUMPDRIVE Schreiben LEXAR JUMPDRIVE Schreiben

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

CenterTools DriveLock - [CenterTools DriveLock\Betrieb\Sch	attenkopien (\\D	LServer\DriveLock	Shadows)]						
Notei Aktion Ansicht Fenster ?									- 5 ×
ConterTeels Drivel esk	Dut		0*	7.1	00			0	7
T Device Scanner	Dateiname	1.1		Zeit	Grose	Benutzer	Computer	Gerate-Identifikation	Zugriffstyp
Produktaktualisierung und Support	Geben Sie Text	nierein	r Gebe r	Gebe	Geben Sie T Y	Geben Sie T Y	Geben Sie T	Geben Sie Text n Y	Gebe Y
🔯 Richtlinien	Bringle	Löschen	2012	15:52:07	10,1 KB	VMTEST\bernd	DLWIN7X64	LEXAR JUMPDRIVE	Schreiben
DriveLock Enterprise Services [DLServer]	Demo I	Casardattan	2012	15:51:59	336 Bytes	VMTEST\bernd	DLWIN7X64	LEXAR JUMPDRIVE	Schreiben
a 🦏 Betrieb	Geheim	Eigenscharten	2012	15:51:58	26,0 KB	VMTEST\bernd	DLWIN7X64	LEXAR JUMPDRIVE	Schreiben
Schattenkopien (\DLServer\DriveLock\Shadows)		Hilfe							
• • • • • •	_								
Öffnet die Eigenschaften des aktuellen Objekts.									

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.



Geheime Daten	.docx	
Größe	10,1 KB	
Zugriffsdatum	09.01.2012 15:52:07	
Zugriff an Computer	DLWIN7X64	
Zugriff von Benutzer	VMTEST\bernd	
Zugriffstype	Schreiben	
Speicherort	E:	
Geräte-Hersteller	LEXAR	
Geräte-Produktkennung	JUMPDRIVE SECURE	
Geräte-Seriennummer	302ac203025642261005	
C	Schattenkopie extrahieren	

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

CenterTools DriveLock - [CenterTools DriveLock/Betrieb\Sc Date: Aktion Ansicht Fenster ? Amount Provide Pro	hattenkopien (\\DLServer\DriveLow	:k\Shadows)]						- 8 ×
CenterTools DriveLock CenterTools DriveLock CenterTools DriveLock CenterTools DriveLock CenterTools DriveLock Richtlinien Agenten-Fernkontrolle Agenten-Fernkontrolle Agenten-Fernkontrolle Agenten-Fernkontrolle Ordner / Agent auswählen Ansicht Neues Fenster hier offnen Attualisieren Liste exportieren Eigenschaften Hilfe Dffnet die Eigenschaften des attuellen Obiekts.	Dateiname Geben Sie Text hier ein Geheime Daten.docx DriveLock_7_Datasheet.pdf Demo_HTMLtat Geheiminformationen.doc	Datum Gebe 9 09.01.2012 09.01.2012 09.01.2012 09.01.2012 09.01.2012 09.01.2012	Zeit Gebe ¥ 15:52:07 15:52:02 15:51:58	Große Geben Sie T 7 10,1 KB 273 KB 336 Bytes 26,0 KB	Benutzer Geben Sie T Y VMTEST\bernd VMTEST\bernd VMTEST\bernd VMTEST\bernd	Computer Geben Sie T., G DLWIN7X64 DLWIN7X64 DLWIN7X64 DLWIN7X64	Geräte-Identifikation	Zugriffstyp Gebe T Schreiben Schreiben Schreiben Schreiben
							14 million 19 million	

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



Algemein	Zugriffsrech	ite				
Statistik —	<u>)</u> .	- 53) 				-
Anzahl Dat	eien	4				
Alteste Dat	ei von	09.01.2012 15:	51:58			
Neueste D	atei von	09.01.2012 15:	52:07			
Option <mark>e</mark> n						
Maximale /	Anzahl anzuz	eigender <mark>Dat</mark> eien	50000	×		
Timeout beim Laden de		r Dateien	10	×	min	

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.

3.2 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 "<u>Gerätesperrung aktivieren</u>" 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".

3.2.1 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.



tei Aktion Ansicht ?				
1 21 21 20 30				
DriveLock Standard Policy - Zentral gespe Globale Einstellungen Laufwerke Ceräte Netzwerkprofile Anwendungen Verschlüsselung Management-Konsole	Geräte Alle Geräte, bei denen es sich Geräte werden nach Ihrer jewe Blackberrys). Jedes Gerät ist g Jede Geräteklasse in DriveLock Wittelist-Regeln. @ Lautweite.	iicht um ein Laufw ligen Gerätekateg nau einer Geräte-1 besitzt eine globa	erk handelt, werden anhand Ihrer Geräte-Kategori orie kontrolliert und erkannt (z.B. USB-Controller, B Klasse zugeordnet, ähnlich der Klassen im Window Je Konfigurationsmöglichkeit als auch einen eigene	e kontrolliert. Iuetooth-Geräte odi vs Geräte-Manager. en Bereich für <u>en Anwendungen.</u>
	Sperr-Einstellungen Konfiguration der Geräte-Sperr-Einstellungen von DriveLock. In der Standard-Einstellung kontrolliert DriveLock keine Geräte-Kategori Wird eine Geräte-Kategorie "aktiviert", als, die Option "Geräte dieser Tyj sperren/ melden" wird aktiviert, werden von DriveLock alle Geräte dieser Type gespert, solange keine Whitelist für diese definiert ist. Weitere Gerätekkassen sind in der "Erweiterten Konfiguration verfügba	a. 15 5	Windows Mobile-Geräte Image: Anderna Status: Geräte werden von DriveLock nicht konfiguriert.	X
		Drive type Bluetooth-A Infrarot-Schr Scanner und Windows Me Palm OS-Gee	dater Geräte werden von DriveLock ni Nicht konfiguriert Wihtelist-Regeln aktiviert Kameras Wihtelist-Regeln aktiviert Biele-Geräte Geräte werden von DriveLock ni Nicht konfiguriert Geräte werden von DriveLock ni Nicht konfiguriert Geräte werden von DriveLock ni Nicht konfiguriert	cht kontrolliert - cht kontrolliert - cht kontrolliert -

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

Allgemein	
	Windows Mobile Handhelds und Smartphones
	Geräte dieses Typs sperren / melden
	📝 Ereignisse für Geräte dieses Typs melden
	V Systemgeräte dieses Typs nicht sperren
	Geräte dieser Klasse werden nicht gespert: DriveLock erkennt kein Gerät dieses Typs und spert Geräte dieser Klasse auch nicht.

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.



n
Windows Mobile Handhelds und Smartphones
🕼 Gerāte dieses Typs sperren / melden
📝 Ereignisse für Geräte dieses Typs melden
✓ Systemgeräte dieses Typs nicht sperren
Geräte dieser Klasse werden gespent: Nur Geräte dieses Typs, die über Computer-Vorlagen oder Regeln in der Geräte-"White-list" definiert sind, werden erlaubt.
Anderungen gelten nicht für Geräte die bereits mit einem Computer verbunden sind. Ein Reboot ist nötig, um die Änderungen für alle Geräte zu aktivieren.

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.



ei Ak <u>t</u> ion <u>A</u> nsicht <u>?</u>			
🔿 🚈 🔝 🔜 🚳			
DriveLock Standard Policy - Zentral gespe DiveLock Standard Policy - Zentral gespe Gatate Perate Netwerkprofile Anwendungen Verschlüsselung Verschlüsselung Management-Konsole	Geräte Alle Geräte, bei denen es sich ni Geräte werden nach Ihrer jeweili Blackberrys), Jedes Gerät ist gen Jede Geräteklasse in DriveLock i Whitelist-Regeln.	cht um ein Laufwe gen Gerätekateg au einer Geräte-l esitzt eine globa	erk handelt, werden anhand Ihrer Geräte-Kategorie kontrolliert. orie kontrolliert und erkannt (28. USB-Controller, Bluetooth-Geräte odk Klasse zugeordnet, ähnlich der Klassen im Windows Geräte-Manager. Ie Konfigurationsmöglichkeit als auch einen eigenen Bereich für Anwendungen.
	Sperr-Einstellungen		
	V Konfiguration der Geräte-Sperr-Einstellungen von DriveLock.		Windows Mobile-Geräte
	V Konfiguration der Geräte-Sperr-Einstellungen von DriveLock. In der Standard-Einstellung kontrolliert DriveLock keine Geräte-Kategorie. Wird eine Geräte-Kategorie "aktiviert", d.h. die Option "Geräte dieses Typs gesperren / melden" wird aktiviert, werden von DriveLock alle Geräte dieses Typs gesperren / solange keine Whitelist für diese definiert ist. Weitere Geräteklassen sind in der # <u>Erweiterten Konfiguration</u> verfügbar.	-	Windows Mobile-Geräte Image: Status: Whitelist-Regeln aktiviert
	Konfiguration der Geräte-Sperr-Einstellungen von DriveLock. In der Standard-Einstellung kontrolliert DriveLock keine Geräte-Kategorie. Wird eine Geräte-Kategorie "aktiviert", d.h. die Option "Geräte dieses Typs geperren / melden" wird aktiviert, werden von DriveLock alle Geräte dieses Typs gesperre, solange keine Whitelist für diese definiert ist. Weitere Geräteklassen sind in der ≈ <u>Erweiterten Konfiguration</u> verfügbar.	Crive type	Windows Mobile-Geräte X Image: Imag
	Konfiguration der Geräte-Sperr-Einstellungen von DriveLock. In der Standard-Einstellung kontrolliert DriveLock keine Geräte-Kategorie. Wird eine Geräte-Kategorie "aktiviert", d.h. die Option "Geräte dieses Typs sperren / melden" wird aktiviert, werden von DriveLock alle Geräte dieses Typs gesperre, Joalnage keine Whitelist für diese definiert ist. Weitere Geräteklassen sind in der ²⁰ Erweiterten Konfiguration verfügbar.	Drive type	Windows Mobile-Geräte X Image: Status Whitelist-Regel aktiviert Status: Whitelist-Regel aktiviert Whitelist-Regel erstellen Enveiterte Konfiguration Typ Bezeichnung Status Bemerkung Aktionen
	Konfiguration der Geräte-Sperr-Einstellungen von DriveLock. In der Standard-Einstellung kontrolliert DriveLock keine Geräte-Kategorie. Wird eine Geräte-Kategorie "aktiviert", d.h. die Option "Geräte dieses Typs sperren / melden" wird aktiviert, werden von DriveLock alle Geräte dieses Typs gespert, solange keine Whitelist für diese definiert ist. Weitere Geräteklassen sind in der ≈ <u>Erweiterten Konfiguration</u> verfügbar.	Drive type Bluetoeth-A	Windows Mobile-Geräte X Image: Status: Whitelist-Regel aktiviert Whitelist-Regel erstellen Enveitente Konfiguration Typ Bezeichnung Status: Bemerkung Aktionen
	Konfiguration der Geräte-Sperr-Einstellungen von DriveLock. In der Standard-Einstellung kontrolliert DriveLock keine Geräte-Kategorie. Wird eine Geräte-Kategorie "aktiviert", d.h. die Option "Geräte dieses Typs sperren / melden" wird aktiviert, werden von DriveLock alle Geräte dieses Typs gespert, solange keine Whitelist für diese definiert ist. Weitere Geräteklassen sind in der P <u>Enveiterten Konfiguration</u> verfügbar.	Drive type Eluetooth-A Infrarot-Schr Scanner und Windows Md	Windows Mobile-Geräte X Image: Status: Whitelist-Regel aktiviert Whitelist-Regel erstellen Enweiterte Konfiguration Typ Bezeichnung Status Bemerkung Aktionen
	Konfiguration der Geräte-Sperr-Einstellungen von DriveLock. In der Standard-Einstellung kontrolliert DriveLock keine Geräte-Kategorie. Wird eine Geräte-Kategorie "aktiviert", d.h. die Option "Geräte dieses Typs sperren / melden" wird aktiviert, werden von DriveLock alle Geräte dieses Typs gespert, solange keine Whitelist für diese definiert ist. Weitere Geräteklassen sind in der # <u>Enveiterten Konfiguration</u> verfügbar.	Drive type Eluetooth-A Infrarot-Schn Scanner und Windows Mi Windows Mi Palm 05-cei	Windows Mobile-Geräte X Image: Status: Whitelist-Regel aktiviert Whitelist-Regel erstellen Erweiterte Konfiguration Typ Bezeichnung Status Bemerkung Aktionen

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

Allgemein	Zug	riffsrechte	
Beschreibu	ung	HTC USB Sync	
Geräteklas	se	Windows Mobile Handhelds und Sma	artphones 🔹 👻
Bemerkung	9		
Optionen	F	Geräte bei Benutzerwechsel nicht neu star	ten
Тур (0	Bus	
		Bus-Bezeichnung	
	0	Einzelgerät Hardware ID	
		USB\Vid_0BB4&Pid_00CE	
		Zusätzliche (kompatible) Hardware IDe	
		zusatziicile (kuinpatible) haluwale ibs	
		Zusatziiche (Kompatible) Haldwale ibs	Neu
			Neu Entfemen
			Neu Entfemen Bearbeiten

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.

<u>Beispiel</u>: 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.

nstallierte Gerate	Hardware-Da	tenbank	Device Scanner Datenbank	
Hersteller	*	Produkt		<u>^</u>
Hewlett-Packard		HTC Sr	nartPhone USB Sync	
HHP		HTC U	SB Sync	
Hitachi Maxell Lte	Hitachi Maxell Ltd.		PC USB Sync	
HTC		Pocket	PC USB Sync	
Intermec		Pocket	PC USB Sync	
ITRONIX		Pocket	PocketPC USB Sync	
JVC		Pocket	PC USB Sync	
Legend	E	Pocket	PC USB Sync	
LGE		Pocket	PC USB Sync	
Linkup Systems		Pocket	PC USB Sync	
MEI		Pocket	PC USB Sync	
Microsoft Corpora	ation	Pocket	PC USB Sync	
MITAC		Pocket	PC USB Sync	
MMT		Pocket	PC USB Sync	
Motorola	+	Pocket	PC USB Sync	+
Import 💌		Hardware	ID USB\Vid_0BB4&Pid_00CE	
Import 🔻		Hardware	D USB\Vid_0BB4&Pid_00CE	

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.

Allgemein	Zugriffsrechte
Sperr-Eins	tellungen
⊚ E	dauben
🔘 S	perren für alle Benutzer
<u>ی</u> ۵	perren, aber Zugriff für definierte Benutzer und Gruppen erlauben
	Benutzer oder Gruppe
	S Domänen-Benutzer
	Hinzufügen) Entfemen

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.



d CenterTools DriveLock			
Datei Aktion Ansicht ?			
DriveLock Standard Policy - Zentral gespe > Globale Einstellungen > Torestore > Foreste > Netzwerkprofile > Netzwerkprofile > Netzwerkprofile > Werschlüsselung > Wandenklüsselung > Management-Konsole	Geräte He Geräte, bei denen es sich nic Geräte werden nach Ihrer jeweitg Blackberrys), Jedes Gerät ist gen Jede Geräteldasse in DriveLock b Whitelist-Regeln. C Jaurez	ht um ein Laufwerk handelt, werden anhand Ihrer Geräte-Kategorie kontrolliert. en Gerätekategorie kontrolliert und erkannt (z.B. USB-Controller, Bluetooth-Geräte u einer Geräte-Klasse zugeordnet, ähnlich der Klassen im Windows Geräte-Manag sitzt eine globale Konfigurationsmöglichkeit als auch einen eigenen Bereich für	oder jer.
	Sperr-Einstellungen Konfiguration der Gesäte-Sper-Einstellungen von DriveLock. In der Standard-Einstellung kontrolliert DriveLock keine Geräte Kategorie. Wird eine Gesäte-Kategorie "aktiviert", d.h. die Option "Gesäte dieses Typs geperner) / melden" wird aktiviert, werden von DriveLock alle Gesäte dieses Typs gestern, von Stander Kaine Whitelia für diese definiert ist. Weitere Geräteklassen sind in der <i>P</i> <u>Enveiterten Konfiguration</u> verfügbar.	Windows Mobile-Geräte Àndern Status: Whitelist-Regel naktiviert Drive type Buetooth-A Impart Status Buetooth-A Senarcund Ymail Status Buetooth-A Senarcund Ymail Status Berefkonz Mark Senarcund Windows M BackBern-Gerate	Akt
		Geräte werden von DriveLock nicht kontrolliert -	

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.



				-
Netzwerk-Kreu	st ob Netzwerk-Kreuz	Bridging	Bridaina auf den	
Agenten erla	ubt sein soll.			L
ViFi-Verbindun	g <mark>en sperren, wenn de</mark>	r Computer mit de	m LAN verbunden	ist
Wenn aktiviert Computer mit e	, werden alle Wireless inem (Ethernet) LAN v	-LAN-Adapter ges verbunden ist.	spent, während de	r

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.

3.2.2 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.



3.2.2.1 Allgemeine Einstellungen zur Gerätesperrung

3.2.2.1.1 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.

Allaemein		
Benutzerd	efinierte Nachricht verwenden	
Gerät ges	pent Nachricht (%DEV% ersetzt mit Gerätenamen)	
1	Das Gerät %DEV% wurde aufgrund Unternehmensrichtlinien gesperit.	*
Test		÷
Nachricht	für Gerät benötigt Neustart (%DEV% ersetzt mit Gerätename	n)
	-	
Test		÷

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").



3.2.2.1.2 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.

3.2.2.2 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 <u>"Konfigurieren der Schnittstellen COM</u> 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.

3.2.2.3 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
- Les ezeichen
- Notizen
- Alle übertragenen Dateien und Synchronisationsdaten auditieren : Dies kommt der Dateiprotokollierung im Dateifilter gleich, d.h. jeglicher Datenaustausch wird protokolliert.



Vigemein Filter / Audit	Nachrichten
Synchronisation von	selektierten Datentypen immer verhindern
V Musik	🔽 Kontakte
Videos	Kalender
Bilder	📝 e Mail-Konten
Anwendungen (Ap	ops) 📃 Lesezeichen
Hörbücher	Notizen
eBooks (und PDF-	-Dateien)
Alle übertragenen Dar Systemdateien und	teien und Synchronisationsdaten auditieren d -objekte auditieren
Alle übertragenen Dai Systemdateien und	teien und Synchronisationsdaten auditieren d -objekte auditieren

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:

VIgemein	Filter / Audit Nachrichten
V Spezie	llen Text bei Benutzerbenachrichtigung anzeigen
Benut	zerinformation wenn diese Regel aktiviert wird
پ ا	Bitte beachten Sie die Unternehmensrichtlinien bei der Verwendung von iPhones.
Dennel	7
Benaci	nnontigung anzeigen wenn Zugnt enaubt wird
Keine	nnontigung anzeigen wenn zugnit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren)
Keine Keine	nnontigung anzeigen wenn zugnit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren) Ereignisse für dieses Laufwerk erzeugen
Keine I	nnentigung anzeigen wenn zugmit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren) Ereignisse für dieses Laufwerk erzeugen
Keine I	nnentigung anzeigen wenn zugnit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren) Ereignisse für dieses Laufwerk erzeugen
v Benaci Keine I Keine I	nnentigung anzeigen wenn zugnit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren) Ereignisse für dieses Laufwerk erzeugen
v Benaci	nnentigung anzeigen wenn zugnit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren) Ereignisse für dieses Laufwerk erzeugen
Keine I	nnentigung anzeigen wenn zugnit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren) Ereignisse für dieses Laufwerk erzeugen
Keine I	nnentigung anzeigen wenn zugnit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren) Ereignisse für dieses Laufwerk erzeugen
v Benaci	nnentigung anzeigen wenn zugnit enaubt wird Benachrichtigung anzeigen (Laufwerk ignorieren) Ereignisse für dieses Laufwerk erzeugen

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.

Vigemein	
Tunes-Soft	wareeinschränkungen
۲	Nicht konfiguriert
0	Einstellen auf festen Wert
Hilfe	 Geräte-Synchronisierung Verschlüsselte Gerätesicherungen erzwinger Neue Geräte nicht registrieren (Standard) Geräte nicht automatisch synchronisieren (St Softwareaktualisierung Nicht nach i Tunes-Aktualisierungen suchen
Schränkt d	en Zugriff auf verschiedene Funktionen in iTunes ein.



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.

3.2.2.4 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.

igenschaften von Serielle Schnittstellen (COM)	Eigenschaften von Parallele Schnittstellen (LPT)
 Serielle Schnittstellen (COM) Serielle Schnittstellen (COM) werden nicht über "White-list"-Regeln gespert. Stattdessen werden sie wie Wechseldatenträger behandelt. Erlauben Sperren für alle Benutzer Sperren aber Zunriff für definierte Benutzer und Gruppen erlauben 	Parallele Schnittstellen (LPT) Parallele Schnittstellen (LPT) Parallele Schnittstellen (LPT) werden nicht über "White-list"-Regeln gespert. Stattdessen werden sie wie Wechseldatenträger behandelt. © Erlauben © Sperren für alle Benutzer © Sperren aber Zugriff für definierte Benutzer und Gruppen erlauben
Benutzer oder Gruppe	Benutzer oder Gruppe
Hinzufügen) Entfemen	Hinzufügen) Entfemen
OK Abbrechen Übernehmen	OK Abbrechen Übernehmen

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.

3.2.2.5 Geräteregeln definieren

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



CenterTools DriveLock) 🗙
Datei Aktion Ansicht	?		
🗢 🔿 🖄 🗔 🔒 🛛	8 2 6 4		
 DriveLock Standard Policy Globale Einstellungen Laufwerke Einstellungen Geräte Einstellungen Geräte Geräte Geräte Geräte- Geräte-	r - Zentral gespe Geben \overrightarrow{V} Gr Geben \overrightarrow{V} Gr Geben \overrightarrow{V} Gr Gerät H H H egeln chnittstellen es-synchronisier	Schreibung Hardware-ID Status Bemerkung uben Sie Text hier ein Y Geben Sie Text hier ein Y Geben Sie Text hier ein Y Geben Sie Text hier ein Y IC USB Sync USB\Vid_0B84 Erlaubt für Liste von Konten	
Windows N	Nobile Handhelc		
Palm OS	Template-Regeln anzeigen		
Mobiltel	Neu	Gerät oder Bus	
Netzwerkprofile Anwendungen	Ansicht	•	
Verschlüsselung Antinimus	Liste exportieren		
Management-Kons	Eigenschaften		
	Hilfe		
L			
<			
Erzeugt einen neuen Eintrag fü	ir ein Gerät oder einen Bus.		

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.

Netzwer	ke	Benutze	r	Optionen
Allgemein	Zugriffsre	Zugriffsrechte Zeiten		
Beschreibung	HTC Titan			
Geräteklasse	Windows Mobile Handhelds und Smartphones			
Bemerkung				
Typ 🔘	Bus	zerwechse	a hichi neu sia	
Typ O	Bus Bus-Bezeichnun Einzelgerät Hardware ID USB\Vid 0BB4	Pid 0A50)	*
Typ 🔘	Bus Bus-Bezeichnun Einzelgerät Hardware ID USB/Vid_0BB4 Zusätzliche (korr	serwechse %Pid_0A50 patible) Ha) ardware IDs	
Typ 💮	Bus Bus-Bezeichnun Einzelgerät Hardware ID USB\Vid_0BB4 Zusätzliche (kom	g &Pid_0A50 apatible) Ha) ardware IDs	
Typ 💮	Bus-Bezeichnun Einzelgerät Hardware ID USB\Vid_0BB4 Zusätzliche (kom	9 8Pid_0A50) ardware IDs	Neu

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.

<u>Beispiel</u>: 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.



ristallierte Gerate	Hardware	-Datenbank	Device Scanner Da	tenbank	
Zurzeit installierte	Geräte	Iokal	⊚ auf Agent		Verbinden
Gerätebezeichn	ung		Hardwar	e-ID	

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.



Installierte Geräte Hardw	vare-Da	tenbank	Device Scanner Date	nbank
Hersteller	•	Produk	t	
Acer Labs Inc. Askey Asus BCOM CASIO Cesscom CMCS Compal Compaq Cyberbank Dell Computer Corp. E-TEN Freedom Scientific FUJITSU	III.			
Fujitsu Siemens	-			
Import 🔻		Hardware	e ID	

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.

3.2.2.6 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

🛒 DriveLock	Beschre	ibung	Geräteklasse	Anzahl von Ge	Bemerkung	
🔞 Device Scanner	Geben S	Sie Text hier ein 🌱	Geben Sie Text hier ein 🍸	Geben Sie T 🍸	Geben Sie Text hier ein	7
 ▷ @ Produktaktualisierung und Support ▲ □ Lokale Computer-Richtlinie ▷ @ Globale Einstellungen 	🚔 Andi	roid Company Devices le Company Devices ne Devices	Android-Geräte Apple-Geräte Scapper und Kameras	1 1 0		
▷ ④ Laufwerke ▲ Ì Geräte	A Print	ter MUC Office	Drucker	2		
 Einstellungen Sperr-Einstellungen Computer (Vorlagen) 						
Computer (vorlagen) Geräte-Whitelist-Regeln Adapter und Schnittstellen						
Geräte Geräte Gräntphones						
Geräteli Neu	•	Geräteliste				
Anwendur Ansicht Arsicht	•					
▷ 🚱 DriveLock Liste exportieren						
▷ III Security-A ▷ III System-M Eigenschaften						
Managem Hilfe]				

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



E	Eigenschaften von Android Company Devices ? ×
Allgemein Geräte	Verknüpfungen
Beschreibung	Android Company Devices
Geräteklasse	🏟 Android-Geräte 🗸 🗸
Kommentar	
	OK Abbrechen Ü <u>b</u> ernehmen

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.



Eig	enschaften von Ar	ndroid Company [Devices ? ×
Allgemein Geräte Ve	knüpfungen		
Hersteller	Produkt	Hardware-ID (oder	Bemerkung
	VMware Virtual S	1	Data
Eigenschaften Akt	ivieren Hinzufügen	Entfemen Importie	eren 🔻 Exportieren 💌
		ОК	Abbrechen Übernehmen

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.

	Eigenschat	ften von N	eue Regel	? ×
Zeiten	Computer	Netzwerke	Benutzer	Optionen
Allgemein	Zugriffsrechte	e Filter /	Schattenk.	Awareness
Beschreibung	Sicherheitseinste	ellungen für An	droid Smartphon	es
Geräteklasse	🌲 Android-Gera	äte		~
Corritoliato				
Android Comp	any Devices			~
Comment				
Comment				
		OK	Abbrechen	Übernehmen

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.



3.2.3 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).

3.2.4 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

CenterTools DriveLock				
Datei Aktion Ansicht	?			
🗢 🏟 🖄 🗔 🔒 🚺	2 🖬 🚳 🛛			
BriveLock Standard Policy - Zentral ges		Vorlagen-Name	Status	
Globale Einstellunge	'n	Geben Sie Text hier ein	Geben Sie Text hier ein	
 Geräte Einstellungen Sperr-Einstellung Computer (Vorla 	gen) Beneln	Bell Computer Corp. Latitude E6500	Geräte gesperit	
Netzwerkprofile	Template-Reg	jeln anzeigen		
 Anwendungen Verschlüsselung 	Eigenschaften			
Antivirus	Hilfe			
Zeigt bzw. versteckt die durc	h (Computer-)Ten	nplates erzeugten Regeln.		

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.

3.2.4.1 Computervorlage erstellen

CantarTools Drivel ock						
Datei Aktion Anricht 2			And in case of the local division of the loc			
		2				
Drivel ock Standard Policy - Z	entral gespe	Vorlagen-Name	*	5		
Globale Einstellungen		Geben Sie Text hier	ein	Geben Sie Text hier ein	7	
Laufwerke		BDell Computer C	Corp. Latitude E6500	Geräte gesperrt		
Gerate				-		
Sperr-Einstellungen						
Computer (Vorlagen)	Neu		Computer (Vorlage)			
Netzwerkprofile			comparer (romage)			
> 🙆 Anwendungen	Ansicht	•				
Verschlüsselung	Liste expo	ortieren				
Management-Konsole	Eigensch	aften				
	Hilfe					
-						
•	Þ					
Neue Vorlage für einen Computer	hinzufügen.					

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



3.2.4.1.1 Erstellen einer Computervorlage anhand des aktuellen Systems

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

Vlgemein	Geräte	Zugriffsrechte	
/orlagen-1	lame	Acer Inspire	
Vorlage	e aktiviere	n (Zugriff auf Geräte in dieser Vorlage erlauben)	
Bemerkun	9		

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 "<u>Computervorlagen verwenden</u>", wenn Sie weitere Geräte hinzufügen und die Berechtigungen konfigurieren möchten.

3.2.4.1.2 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 "<u>Computervorlagen verwenden</u>", wenn Sie weitere Geräte hinzufügen und die Berechtigungen konfigurieren möchten.

3.2.4.1.3 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.



3.2.4.2 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.

Allgemein Ge	räte Zugriffsrechte		
Тур	Beschreibung 🔺	Hardware-ID	*
Gerät	Bluetooth Device (Personal Area Network) Bluetooth Device (RFCOMM Protocol TDI) Broadcom NetXtreme 57xx Gigabit Controller Communications port (COM1) Conexant D110 MDC V.92 Modem Dell Wireless 1450 Dual Band WLAN Mini-P. Dell Wireless 350 Bluetooth Module Intel(R) 82801FB/FBM USB Universal Host Intel(R) 82801FB/FBM USB Universal Host Intel(R) 82801FB/FBM USB Universal Host Intel(R) 82801FB/FBM USB Universal Host Intel(R) 82801FB/FBM USB Universal Host	BTH\MS_BTHPAN BTH\MS_RFCOMM PCI\VEN_14E4&DEV_16778 ACPI\PNP0501 PCI\VEN_8086&DEV_266D8 PCI\VEN_8086&DEV_266D8 USB\Vid_413c&Pid_8103ℜ PCI\VEN_8086&DEV_2658 PCI\VEN_8086&DEV_2659 PCI\VEN_8086&DEV_265A PCI\VEN_8086&DEV_265B	E
Gerät Gerät Gerät Gerät Gerät Gerät Bigenschafter	Intel(R) 82801FB/FBM USB2 Enhanced Ho Sigma Tel C-Major Audio SMC IrCC - Fast infrared port Standard Modem over Bluetooth link Texas Instruments PCI GemCore based Sma.	PCI/VEN_8086&DEV_265C PCI/VEN_8086&DEV_266E& ACPI/SMCF010 BTHENUM\{00001103-0000 PCI/VEN_104C&DEV_8038 men Import ▼	•

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

3.2.4.2.1 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.



Beschreibung	Texas Instruments PCI GemCore based SmartCard controller
Geräteklasse	🗒 Smartcard-Lesegeräte 🔹
Bemerkung	
Гур 🔘	Bus Bus-Bezeichnung Einzelgerät Hardware ID PCI/VEN_104C&DEV_8038
	Zusätzliche (kompatible) Hardware IDs
	Neu Entfemen

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 "<u>Geräteregeln definieren</u>").

3.2.4.2.2 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.



Igemein Ge	erate Zugriffsrechte		
Тур	Beschreibung 🔺	Hardware-ID	*
📥 Gerät	Bluetooth Device (Personal Area Network)	BTH\MS_BTHPAN	
🚖 Gerät	Bluetooth Device (RFCOMM Protocol TDI)	BTH\MS_RFCOMM	
Gerät	Broadcom NetXtreme 57xx Gigabit Controller	PCI\VEN_14E4&DEV_1677&	
(Nur In	Communications port (COM1)	ACPI\PNP0501	
Gerät	Conexant D110 MDC V.92 Modem	PCI\VEN_8086&DEV_266D&	-
🚖 Gerät	Dell Wireless 1450 Dual Band WLAN Mini-P	PCI\VEN_14E4&DEV_4324&	=
猪 Gerät	Dell Wireless 350 Bluetooth Module	USB\Vid_413c&Pid_8103ℜ	
Gerät	Intel(R) 82801FB/FBM USB Universal Host	PCI\VEN_8086&DEV_2658	
Gerät	Intel(R) 82801FB/FBM USB Universal Host	PCI\VEN_8086&DEV_2659	
Gerät	Intel(R) 82801FB/FBM USB Universal Host	PCI\VEN_8086&DEV_265A	
Gerät	Intel(R) 82801FB/FBM USB Universal Host	PCI\VEN_8086&DEV_265B	
Gerät	Intel(R) 82801FB/FBM USB2 Enhanced Ho	PCI\VEN_8086&DEV_265C	
🖌 Gerät	Sigma Tel C-Major Audio	PCI\VEN_8086&DEV_266E&	
🖉 Gerät	SMC IrCC - Fast infrared port	ACPI\SMCF010	
🕼 Gerät	Standard Modem over Bluetooth link	BTHENUM\{00001103-0000	
🛗 Gerät	Texas Instruments PCI GemCore based Sma	PCI\VEN_104C&DEV_8038	-
idenschafte	Deaktivieren Hinzufügen Entferr	en Import T Evnot	-
igensenance			<u> </u>
		Von lokalem Com	outer
		Von Agent	

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.

3.2.4.2.3 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.



Allgemein Ge	räte Zugriffsrechte		
Тур	Beschreibung 🔺	Hardware-ID	
🚖 Gerät	Bluetooth Device (Personal Area Network)	BTH\MS_BTHPAN	
📥 Gerät	Bluetooth Device (RFCOMM Protocol TDI)	BTH\MS_RFCOMM	
📥 Gerät	Broadcom NetXtreme 57xx Gigabit Controller	PCI\VEN_14E4&DEV_1677&	
🖓 (Nur In	Communications port (COM1)	ACPI\PNP0501	
Gerät	Conexant D110 MDC V.92 Modem	PCI\VEN_8086&DEV_266D&	
🚖 Gerät	Dell Wireless 1450 Dual Band WLAN Mini-P	PCI\VEN_14E4&DEV_4324&	E
😵 Gerät	Dell Wireless 350 Bluetooth Module	USB\Vid_413c&Pid_8103ℜ	
Gerät	Intel(R) 82801FB/FBM USB Universal Host	PCI\VEN_8086&DEV_2658	
🖗 Gerät	Intel(R) 82801FB/FBM USB Universal Host	PCI\VEN_8086&DEV_2659	
Gerät	Intel(R) 82801FB/FBM USB Universal Host	PCI\VEN_8086&DEV_265A	
🖗 Gerāt	Intel(R) 82801FB/FBM USB Universal Host	PCI\VEN_8086&DEV_265B	
Gerät	Intel(R) 82801FB/FBM USB2 Enhanced Ho	PCI\VEN_8086&DEV_265C	
💐 Gerät	SigmaTel C-Major Audio	PCI\VEN_8086&DEV_266E&	
🖉 Gerät	SMC IrCC - Fast infrared port	ACPI\SMCF010	
Gerāt	Standard Modem over Bluetooth link	BTHENUM\{00001103-0000	
🛗 Gerät	Texas Instruments PCI GemCore based Sma	PCI\VEN_104C&DEV_8038	-
-			
Eigenschafter	Deaktivieren Hinzufügen Entfem	en Import 🔻 Export	
		Na	ch Hardware-Datenbar

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.

3.2.4.2.4 Zugriffsrechte innerhalb einer Computervorlage definieren

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

Algemeir	Geräte	Zugriffsrechte					
C Erlaul	ben						
Sperr	en, aber Zu	u <mark>griff für d</mark> efinierte	e Benutzer un	d Gruppen erlau	ben		
Ber	nutzer oder	Gruppe					
22	Domänen-	Benutzer					
C	zufügen	Entfernen]				
Hina							
Hin				OK		-	lle en ele en el



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.

3.2.4.2.5 Aktivieren einer Computervorlage

genschafte	en von N	eue Vorlage	[8] ×
Allgemein	Geräte	Zugriffsrechte	
Vorlagen-N	lame	Dell Computer Corp. Latitude E6400	Ĵ
Vorlage	e aktiviere	n (Zugriff auf Geräte in dieser Vorlage erlaub	pen)
Bemerkung	9		
		ОК	Abbrechen Übernehme

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.

3.2.4.2.6 Anzeige der durch eine Computervorlage definierten Geräte

Ng CenterTools DriveLock
Date: Aktion Ansicht ?
DriveLock Standard Policy - Zentral gespe Vorlagen-Name Status
© Globale Einstellungen Geben Sie Text hier ein Image: Computer Corp. Latitude E6400 Geräte erlaubt © Gräte Geräte Image: Computer Corp. Latitude E6500 Geräte erlaubt © Gräte Geräte Image: Computer Corp. Latitude E6500 Geräte gesperit © Gräte Malagter und Schnitstellen Image: Computer Corp. Latitude E6500 Geräte gesperit © Gräte Mitritus Image: Computer Corp. Latitude E6500 Geräte gesperit © Gräte Vinitistellen Image: Computer Corp. Latitude E6500 Geräte gesperit © Gräte Vinitistellen Image: Computer Corp. Latitude E6500 Geräte gesperit © Malagter und Schnitstellen Image: Computer Corp. Latitude E6500 Geräte gesperit © Gräte Template-Regeln anzeigen Image: Computer Corp. Latitude E6500 Geräte Geräte Geräte Geräter © Management-Konsole Image: Computer Corp. Latitude E6500 Image: Computer Corp. Latitude E6500 Image: Computer Corp. Latitude E6500
۲ ــــــــــــــــــــــــــــــــــــ



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 IV Netzwerkprofile





4 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.



CenterTools DriveLock	
Datei Aktion Ansicht ?	
🗢 🔿 🖄 🖬 🖬 😸	
DriveLock Standard CSP - Zentral gespeicher Globale Einstellungen Globale Einstellungen Garate Grave Verschüsselung Verschüsselung Management-Konsole	Netzwerkprofile Konfiguration von Netzwerkverbindungen / Standorten und dazugehörigen Konfigurationsprofile. Laufwerks- oder Geräte-Whitelist-Regeln konfiguriert werden, um einzelne Geräte nur in speziellen Netzwerken zuzulassen.
	Einstellungen Konfiguriert das globale Verhalten von DriveLock beim Verwalten von verschiedenen Netzwerken. Verbindungen / Standorte Definiert Netzwerkverbindungen. Anhand der Verbindungen ermittelt ein DriveLock Agent, mit welchem Netzwerk er verbunden ist. Netzwerkverbindungen können anhand der IP-Konfiguration (Subnetz, DNS-Domänen-Name), Active Directory Standort, WLAN Netzwerkschlüssel (SSID) oder anderer, spezieller Parameter identifiziert werden.
<)	Konfigurationsprofile Konfigurationsprofile können verwendet werden, um spezielle Parameter (z.B. HTTP Proxy Server) auf Client Computern zu ändern, wenn diese mit bestimmten Netzwerken verbunden sind. Dazu kann jede Netzwerkverbindung mit einem speziellen Konfigurationsprofil verbunden werden.
Fertig	

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:



Allgemein	Zugriffsrec	hte F	Filter / Sc	hattenk.	Zeiten	Computer
Netzwerke	Benutzer	Laufwe	rke N	achrichten	Optione	n Befehle
 Regel ist Regel ist 	nur bei gewä bei gewählter	hlten Net n Netzwe	zwerkve erkverb. r	nicht aktiv, a	aktiv aber bei all	en anderen
Verbind	dung / Stando	ort				

- 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.



4.1 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 "<u>Benutzerspezifische Netzwerkprofile erstellen</u>" nach.

4.1.1 Benutzerbenachrichtigung einrichten

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



igenschaften	8 X
Allgemein	
Methode der Benutzerbenachrichtigung	
Sprechblasentipp anzeigen	
 Dialogfenster anzeigen 	
🔘 Keine	
V Symbol im Infobereich anzeigen	
Anzeigedauer	10 sec.
Vorschau	
DIVELICA	
HTMLText HTMLText	
9:00	
OK	hen Ubernehmen

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,

4.1.2 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.



genschaften	2	×
Allgemein		
WiFi-Verbindur	igen sperren, wenn der Computer mit einem LAN verbund	len ist
	Aktiviert	
	 Deaktiviert (Standard) 	
	Nicht konfiguriert	
Wenn aktiviert Computer mit e	, werden alle Wireless-LAN-Adapter gespent, während de inem (Ethernet) LAN verbunden ist.	F
	OK Abbrechen Übern	ehmen

4.1.2.1 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.

<u>Beispiel</u>: 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:



agomont	Adapter	Reaktion	Verknüpfu	ngen		
Vetzwerk	/erbindung	wird erkann	t anhand vo	on Einem aus	s	
Schnitt	stellen-Nar	me (z.B. "Lo	kale Verbind	dung")		
Name						
V Netzwe	erkadapter	Name (Har	lware-Bezei	chnung)		
Adapte	emame	Drittanbie	ter VPN LAN	4		
Adapte	ertyp					
Adapte	ertvo	[··				~
☑ Diese 1 □ Diese 1	Verbindung Verbindung	nicht als L nicht als W	AN erkenner /i-Fi / WLAN	ı Lerkennen		

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.

4.2 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

ei Aktion Ansich	?						
DriveLock Standard C: Globale Einstellung Laufwerke Geräte Netzwerkprofile Einstellungen	5P - Zentral gespeicher gen	Beschrei Geben S Centi Centi McD Centi	ibung ^ ie Text hier ein erTools onald Islands ne (kein Netzwerk)	Typ Geben Sie Text h Active Directory-St Geographische Posi Spezielle Verbindung	Status Geben Y Zugelassen Gesperrt b Zugelassen	Konfigurationsprofil Geben Sie Text hier ein <kein profil="" zugeordnet=""> <kein profil="" zugeordnet=""> <kein profil="" zugeordnet=""></kein></kein></kein>	7
C Konfigurat	Neu	•	Active Directory-Stando	ort			
Anwendunger Verschlüsselur	Ansicht	×	Netzwerkverbindung				
Antivirus	Liste exportieren		Netzwerkadapter Geographische Position				
my wanagement-	Eigenschaften		Wireless-LAN SSID				
	Hilfe		Spezielle Verbindung				
III	→ F	-					

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:



Algemein	Reaktion	Verknüpfungen	
Wenn der	Computer m	it dieser Netzwerkverbindung	verbunden wird
0	Verbindung :	zulassen	
0	Verbindung :	sperren bis zum nächsten Neu	ustart
0	Verbindung :	sperren bis zu manuellem Eing	griff
0	Computer he	runterfahren	
			27.8 T. F.

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.

4.2.1 Active Directory Standort

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



	Reaktion	Verknüpfungen	
AD Stando	ort-Name	CenterTools	
Domänen-	GUID	11adb49f-3b7d-48b1-838f-8dde33739378	
Symbol		-	
Konfigurat Bemerkun	ionsprofil	<kein profil="" zugeordnet=""></kein>	•
Firmennet	zwerk		*
			×

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.

4.2.2 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.



Aigemein	IP-Einstel	lungen	Reaktion	Verknüpfunge	en	
Beschreib	ung	IP-Ne	zwerk			
Symbol			•			
Konfigurat	ionsprofil	kein	Profil zugeo	rdnet>		•
Bemerkun	g					
						^
						~

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.

Algemein	IP-Einstellunge	en Reaktion	Verknüpfun	gen	
Vetzwerkv	verbindung wird	erkannt anhar	nd von Einem	aus	
V IP-Sub	netz (IP-Adresse	und Subnetz	Maske)		
IP-Adr	esse 1	92 . 168 .	10 . 5		
Subne	tz-Maske 2	55 . 255 .	255 . 0		
Primäre	m DNS Domän	en-Namen			
Domār	nenname				
Standa	rdgateway				
IP-Adr	esse 1	92 . 168 .	10 . 100		
DHCP-	Server-Adresse				
IP-Adr	esse	21 - V	81		
Diese V	/ethindung nich	tale I AN ertre	nnen		
Diese	Verbindung nich	t als Wi-Fi / W	'L <mark>AN erkenne</mark>	n	
Finstellun	nen übernehme		EST		
Cinateliuni	gen übernerline	VOIT VIVIT	Cal		



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.

4.2.3 Netzwerkadapter

Die Einstellung für Netzwerkadapter wird in Verbindung mit VPN-Client von Drittanbietern benötigt und wird im Abschnitt "<u>VPN-Clients von Drittanbietern einsetzen</u>" beschrieben.

4.2.4 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**:

ng	McDonald Islands			
ler	🔲 Guatemala			
	Guemsey			
	🔲 Guinea			
	🕅 Guinea-Bissau			
	C Guyana			
	🔄 Haiti			
	V Heardinsel und McDonaldinseln			
nsprofil	<kein profil="" zugeordnet=""></kein>			
	4			
	nsprofil			

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).

<u>Beispiel</u>: 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.

4.2.5 Drahtlosnetzwerk mit SSID

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



Allgemein	Reaktion	Verknüpfungen	
Drahtlosne	tzwerk-SSI)	
CENTERI	MUC		•
Symbol		-	
Konfigurati	onsprofil	<pre><kein profil="" zugeordnet=""></kein></pre>	•
Bemerkun	9		
			*
			*

Geben Sie anschließend die SSID in das entsprechende Feld ein.

4.2.6 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.


Allgemein	Reaktion	Verknüpfungen	
Netzwerkv	verbindung v omputer nich eine definiert	vird von DriveLock erkannt, wenn t mit einem Netzwerk verbunden ist e Netzwerkverbindung konfiguriert	t (Offline) ist
Symbol		-	
Ko <mark>n</mark> figurati	ionsprofil	<kein profil="" zugeordnet=""></kein>	Ŧ
Bemerkun	g		
			*
			-

4.2.7 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.



	Reaktion	Verknüpfungen	
Beschreib	ung	Security Test	
Befehl <mark>s</mark> zei	le		
Symbol		-	
Konfigurat	ionsprofil	<kein profil="" zugeordnet=""></kein>	÷
Bemerkun	g		
			^
			+
Uinusia: F)ie Anwendu	ng muss Exit code 1 zurückgeben,	wenn der Computer

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"*).

4.3 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.

Detei Aktion Ansicht ? Detei Aktion Ansicht ? Divielock Standard CSP - Zentral gespichter Divielock Standard CSP - Zentral gespichter Detei Aktion Standard CSP - Zentral gespichter Detei Standard
Image: Second and CSP - Zentral gespeicht Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung
Orverlack Standard CSP - Zentral gespreicher Geben Sie Tot hier ein Geben Sie Tot hier ei
Globale Einstellungen Geben Sie Text hier ein Geben Sie Text hier ein Geben Sie Text hier ein Geben Sie Text hier ein In dieser Ansicht werden keine Elemente angezeigt. Netwerkprofile Verbindungen / Sandorte Verschüsselung Ansicht Ansicht Eigenschaften Hiffe Hiffe Erzeugt ein neues Konfigurationsprofil.
In dieser Ansicht werden keine Elemente angezeigt. Netzwerkprofile Verschlüsselungen Ansicht Iste exportieren Eigenschaften Hife Hife Erzeugt ein neues Konfigurationsprofil.
Konfigurationsprofile Anwendungen Neu Konfigurationsprofile Ansicht Ansicht Eigenschaften Hilfe
Anwendungen Neu Verschlüsselung Ansicht Liste exportieren Eigenschaften Hiffe
Verschlüsselur Verschlüsselur Management-K Liste exportieren Eigenschaften Hilfe Hilfe Erzeugt ein neues Konfigurationsprofil.
Management-K Eigenschaften Hilfe Hilfe Hilfe Erzeugt ein neues Konfigurationsprofil.
Eigenschaften Hilfe
Hilfe
۲ الت المراجع ا Erzeugt ein neues Konfigurationsprofil.
Erzeugt ein neues Konfigurationsprofil.

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

Allgemein	Proxy	MSN Messenger	Weitere	Verknüpfungen	
Beschreibu	ung		2111		
Bemerkun	9				
	99 99				~
					Ŧ

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



4.3.1 Internet Explorer Proxy Einstellungen

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

Allgemein	Proxy	MSN Messenger	Weitere	Verknüpfung	en
Proxy-E	Ein <mark>s</mark> tellun	gen verändern			
Automatiso Manuelle I Einstell Automa Adres	che Konf Einstellur ungen al atisches se	iguration überschreil Igen zu verwende, a utomatisch erkennei Konfigurations-Skrip	bt manuelle automatisch n t verwende	e Einstellungen he Konfiguratio en	ı. Um n abschalten
-		••••••••			
Proxy-S	berver im	LAN verwenden			
Adres	se			Port	
					Erweitert
Pro	oxy-Serv	er für lokale Adresse	n umgehe	n	
Einstellur	aan üha	mahman			
	igen ube	menmen			

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.



4.3.2 MSN Messenger Einstellungen

Nigemein	Proxy	MSN Messenger	Weitere	Verknüpfungen	1
MSN N	lessenge	er-Einstellungen verä	indem		
Automa	atische A	nmeldung			
🗌 Pe	rsönliche	e Statusnachricht ve	rändem		
N	achricht				
S	mbol	o 🖪 💿 🖁	0	0	
Pe	rsönliche	es Anzeigebild verär	idem		
Γ					
Einstellur	igen übe	mehmen			

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.

4.3.3 Weitere Aktionen bei Erkennung von Netzwerken

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



Algemein	Proxy	MSN Messenger	Weitere	Verknüpfungen	
Bearbeitur V Co	ng von G mputer-F enutzer-R	ruppenrichtlinien Richtlinien aktualisie ichtlinien aktualisier	ren wenn \ en wenn V	Verbindung erkannt Verbindung erkannt v	wird wird
🔽 Standa	ard-Druck	er verändem			
Micro	soft XPS	Document Writer			÷

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.



4.4 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:

	Zugriffsred	chte Filte	r / Schattenk.	Zeiten	Computer
Netzwerke	Benutzer	Laufwerke	Nachrichten	Optionen	Befehle
Regel ist Regel ist Regel ist	bei allen Net nur bei gewä bei gewählte	zwerkverbind ihlten Netzw en Netzwerkv	dungen aktiv erkverbindungen rerb. nicht aktiv, a	aktiv aber bei aller	n anderen
Verbin	dung / Stand	lort	n		

- 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.

4.5 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.

Netzwerkprofile





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**.

genschaften		8 ×
Allgemein		
Benutzem erla	uben, persönliche Netzwerk-Profi	e zu verwalten
	Aktiviert (Standard)	
	Oeaktiviert	
	Nicht konfiguriert	
Wenn aktiviert Agenten-Benu	, können Benutzer persönliche N tzerinterfaces verwalten.	etzwerkprofile mit Hilfe des
	ОК	Abbrechen Übernehmen

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 V DriveLock File Protection





5 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.

5.1 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></benutzername>
und in
- <benutzername>\Desktop</benutzername>
- <benutzername>\Dokumente</benutzername>
jedoch nicht in
 Alle Benutzer\Anwendungsdaten und <benutzername>\Anwendungsdaten</benutzername>
- <benutzername>\Start-Menü</benutzername>
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.

5.2 Unterstützte Verschlüsselungsverfahren

DriveLock File Protection unterstützt folgende Verschlüsselungsverfahren:

 AES (empfohlen) - Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptoverfahren, welches als Nachfolger f
ür 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 verbzw. 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.

5.3 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.

5.3.1 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:

- 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.

Zertifikatsdetails Füllen Sie alle Fe	eingeben elder aus, um das neue Zertifikat anlegen zu können.
Das Master-Zertifikat Benutzeranfragen ver	wird auf dem Server erstellt und gespeichert und für alle nwendet.
Zertifikatsname	DriveLock File Protection Master Certificate
Organisationseinheit	Certs
Organisation	Spectre
Standort	Munich
Bundesland	
Land	Deutschland
	Sector Sect

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.

5.3.2 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.

Eigenschaften von root 🛛 📍 🎴	<
Allgemein Zertifikatsverwaltung Zertifikats- und Schlüsselverwaltung Zertifikats- und Schlüsselverwaltung aktivieren Zertifikatsanfragen müssen vom Administrator manuell genehmigt werden Erzeugte Benutzerzertifikate sind gültig für 1 🚔 Jahre	-
Stammzertifikat Zertifikat läuft ab am n/a Emeuem	_
OK Abbrechen O <u>b</u> ernehme	n

- 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.

5.3.3 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

5.3.3.1 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.



Che Te parte a comp	
Mindestlänge für Kenn	wöiter 8 🚔 Zeichen
Ein gültiges Kennwort	muss mindestens enthalten
1	Kleinbuchstaben
1 😫	Großbuchstaben
1	Ziffem
0	Sonderzeichen
Ziffern	als Sonderzeichen behandeln
🗖 Überprüfen ob Ken	nwort (oder Teil davon) in Wörterbuch vorkommt
Uberprüfen ob Ken Wörterbuchdatei	nwort (oder Teil davon) in Wörterbuch vorkommt
Überprüfen ob Ken Wörterbuchdatei Wörterbuchtyp	nwort (oder Teil davon) in Wörterbuch vorkommt
Überprüfen ob Ken Wörterbuchdatei Wörterbuchtyp	nwort (oder Teil davon) in Wörterbuch vorkommt OpenOffice-Wörterbuch Textdatei mit Wortliste
Überprüfen ob Ken Wörterbuchdatei Wörterbuchtyp	nwort (oder Teil davon) in Wörterbuch vorkommt OpenOffice-Wörterbuch © Textdatei mit Wortliste
Uberprüfen ob Ken Wörterbuchdatei Wörterbuchtyp	nwort (oder Teil davon) in Wörterbuch vorkommt OpenOffice-Wörterbuch (a) Textdatei mit Wortliste

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).

5.3.3.2 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.

5.3.3.3 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.

5.3.3.4 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.

5.3.3.5 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

- 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.
- 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.

5.3.3.6 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.

Notes Tools DriveLock			and the second	l	- 0 - X		
Datei Aktion Ansicht ?							
BriveLock Lokale Richtlinie	Priorität	Beschreibung	Bemerkung				
 Globale Einstellungen Laufwerke Geräte Anwendungen Werschlüsselung Werschlüsselung Wechseldatenträger-Verschlüsselung (Contain File Protection Einstellungen Wiederherstellung verschlüsselter Ordner Full Disk Encryption Management-Konsole 	2 Niedrigste	Zertifikatsbasierte Wiederherstellu					
< •				1			



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.

5.3.3.7 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.

5.4 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.

5.4.1 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.

5.4.2 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.

🖏 CenterTools DriveLock - [CenterTools DriveLock\DriveLock File Protection\Benutzer]						
Datei Aktion Ansicht Eenster ?						
CenterTools DriveLock	Objektname	Abteilung	Benutzer-ID	Mandanten-Name	Тур	
 Produktaktualisierung und Support Produktaktualisierung und Support Richtlinien DriveLock Enterprise Services [DLServer. Server Mandanten Pakete und Definitionsdateien DriveLock File Protection Zentral verwaltete Ordner Benutzer und Gruppen Etriëb 	& Bernd Hartmann (Produktmanagement) & Bob Hartmann	Produktmanagement Personalabteilung	bernd@vmtest.local bob@vmtest.local	root	Benutzer Benutzer (von ActiveDirectory)	

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:



	Bob Test				
Benutzer-ID SID	bob@vmtest.local S-1-5-21-3482298495-599452032-2630625796-1126				
Mandant	root				
Vomame	Bob				
Nachname	Test				
E-Mail-Adresse	bob@vmtest.local				
Abteilung	Personalabteilung				
	Anzeigebild ändem				

- 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.

5.4.3 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 g
 ültiges Zertifikat => ein neuer DriveLock Benutzer wird erzeugt und dann zur DriveLock Gruppe hinzugef
 ügt
- 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.

5.4.4 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.



🙀 CenterTools DriveLock - [CenterTools DriveLock\DriveLock File Protection\Zertifikate\Aktive Zertifikate]					
Batei Aktion Ansicht Fenster ?					
🗇 🔿 🔁 🖻 🛯 💀 🔢					
CenterTools DriveLock	Objektname	Mandanten-N	Gültig bis	Seriennummer	
 Device Scanner Produktaktualisierung und Support Richtlinien DiveLock Enterprise Services [DLServer. Server Mandanten Pakete und Definitionsdateien DriveLock File Protection Zentral verwaltete Ordner Benutzer Zertifikate Artive Zertifikate Widerrufene Zertifikate Widerrufene Zertifikate Widerrufene Zertifikate Widerrufene Zertifikate Widerrufene Zertifikate 	Bernd Hartmann (Produktmanagement)	root	19.07.2013 11:12:09 11.06.2013 16:10:41	539ecea0-7fba-4d69-afd7-2b2536f54472 0600000000004CD1761	

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.

5.5 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.

 CenterTools DriveLock Device Scanner Produktaktualisierung und Support Richtlinien DriveLock Enterprise Services [DLServer,	UNC-Pfad	Mandanten-Name	Status
Mandanten Pakete und Definitionsdateien DriveLock File Protection Zentral verwaltete Ordner Benutzer Zertifikate Betrieb		root	OK

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.

5.5.1 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.

Daten (Wäl zen	des zentral verwalteten Ordners nlen Sie den Pfad, Mandanten und primären Server des neuen ral verwalteten Ordners.
5	Pfad des neuen zentral verwalteten Ordners
and a	\\DLSERVER\DriveLock\Verschlüsselt\
	Erzeugen für Mandant
	root
	Primärer Server (für die Verwaltung des Ordners)
	DLServer.vmtest.local

- 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.

5.5.2 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.



gemein Benutzer			
enutzer und Gruppen mit 2	Zugriff auf diesen Ordner		
Benutzemame	Benutzer-ID	Admin	
Bob Hartmann & Hartmann, Bernd	bob@vmtest.local bernd@vmtest.local	0 1	
	Entfernen	Hinzufügen	

- 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**.

5.6 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.

5.7 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.





Terminalserver





6 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.

6.1 Verbindungsarten

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 Terminalserver s verwendet.	Ja	Ja

Unterstütze Funktionen je nach Verbindungsart (nur Laufwerksverbindungen):

Wenn die Applikationskontrolle auf dem Terminalserver verwendet werden soll, wird unabhängig von der obigen Tabelle immer der DriveLock-Agent auf dem Terminalserver benötigt.

6.1.1 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.

6.1.2 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.

6.1.3 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.

6.1.4 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.

6.1.5 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.

6.2 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.

6.2.1 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.





6.2.2 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:

CenterTools DriveLock				- 🗆 💌 🗙
Datei Aktion Ansicht ?				
🗢 🔿 🖄 🛅 🗟 👔	a 🛛 🕹 D			
Anvendungen Anvendung	Intral gespeicher H Heu Intral gespeicher H G G W Heu Intral gespeicher H G G G G G G G G G G G G G G G G G G G	Hersteller ID Seben Sie Tr Whitelist- AV USB + +	D/ Regel Produkt ID / Beding Status Regel-Typ Bemerkung Fexth Y Geben Sie Text h Y Geben Sie T Y Geben Sie Text hier ein Y Flash Disk Gesperrt, Versc Laufwerks-Regel DriveLock Stick für Erzw. Verschlü Geräte-Regel Netzwerklaufwerk-Regel Laufwerks-Regel DriveLock Stick für Erzw. Verschlü Netzwerklaufwerk-Regel Gerätegröße-Regel Basis-Regel Easis-Regel Terminaldienste-Regel Regel aus Vorlage Ordner Ordner	
< III	• .	Ultranta 1		
Erzeugt eine neue Regel basierend	auf einer Terminal	Idienste-Lai	autwerkszuordnung.	

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:



Allgemein	Zugriffsrechte	Filter / Schattenk	Zeiten
	Steuert Gerätezug /erbindungen. Die Regel basiert a Ferminal Sitzung. I kann der Laufwerk Laufwerksbuchsta Protokolle Bemerkung	niff für Terminaldienst auf dem Laufwerksbu Mithilfe von Thin-Clie (sbuchstabe festgele be U RDP (Windo V RDP (Windo	te Client-Laufwerks- uchstaben innerhalb der nt-Management-Software egt werden. www.reminal Services) enApp)
		OK	Abbrachan Dibamahma

6.2.3 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*.

6.2.4 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.



Zugriffsrechte	Filter / Schattenk.	
📝 Dateien filte	0	
Protokolliere	1 und Schattenkopie	
Filter / Protokol	/ Schattenkopie mit Einstellungen dieser Vorlage	
Ausführbare D	teien blockieren, Protokollierung	•

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.

6.3 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.





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

Weitere in diesem Dokument aufgeführte tatsächliche Produktund Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

DriveLock and others are either registered trademarks or trademarks of DriveLock SE or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

© 2022 DriveLock SE

